MATEMATYKA OLIMPIJSKA

$\star$

Algebra i Teoria Liczb

Adam Neugebauer

STYCZEŃ 2018

OPRACOWANIE GRAFICZNE

Autor

Wydanie XV

(rozszerzone)

Przedmowa

Mathematik ist die Königin der Wissennschaften und
die Zahlentheorie die Königin der Mathematik.
(Carl Friedrich Gauss)

Przedstawiamy kolejne wydanie pierwszego, z powstających czterech, skryptu z MATEMATYKI OLIMPIJSKIEJ.

Skrypt ten – ż ó ł t y – przedstawia podstawowe pojęcia i metody elementarnej *Algebry i Teorii Liczb*. Kolejnymi są lub będą: skrypt z i e l o n y – *Geometria* (cytowany jako $\mathbb{GEO}$), skrypt c z e r w o n y – *Kombinatoryka* (cytowany jako $\mathbb{KOM}$) i skrypt n i e b i e s k i – *Równania i Nierówności* (cytowany jako $\mathbb{RIN}$). Zamiarem pomysłodawców jest, by mogły one służyć nauczycielom i uczniom zajmującym się Olimpiadą Matematyczną. Byłoby też dobrze, gdyby matematykę elementarną, w objętości zakreślonej przez te skrypty, znali studenci kierunków nauczycielskich uniwersytetów.

Przy wyborze przedstawionego materiału kierujemy się, oprócz pierwotnego wymogu "elementarności", względami "stosowalności" w matematyce olimpijskiej: większość omawianych tematów inspirowana była przez zadania olimpijskie (krajowe i międzynarodowe). Szczegółowy spis treści i indeks dają dostatecznie dobre wyobrażenie, na ile należy przy tym rozszerzyć i pogłębić wykładane w szkołach średnich treści teorioliczbowe i algebraiczne.

Skrypt jest w zasadzie samowystarczalny: zaczyna się od **liczb naturalnych**. Dążąc do **krzywych eliptycznych**, po drodze mówi o jednoznaczności rozkładu na **czynniki nierozkładalne** w **pierścieniu** liczb całkowitych i **pierścieniu wielomianów**, **kongruencjach**, **ułamkach łańcuchowych**, **formach kwadratowych**, **ciągach rekurencyjnych**, **pierścieniach kwadratowych**, i o **równaniach diofantycznych**, w szczególności o **równaniu indyjskim**. Centralnym rozdziałem skryptu jest rozdział 5: badanie reszt z dzielenia liczb całkowitych przez ustaloną liczbę m – **moduł** – dostarcza mocnego narzędzia teorioliczbowego – **arytmetyki modulo** m – z którym powinni oswajać się już gimnazjaliści.

W krótkiej bibliografii, którą uzupełnić należy o rozmaite zbiory zadań z Olimpiad Matematycznych, pokazujemy kilka źródeł dających możliwość rozszerzenia i pogłębienia wiedzy algebraicznej i teorioliczbowej.

W indeksie zamieszczamy również terminy zaledwie wspomniane w tekście. Powinno to rozbudzać ciekawość Czytelników i zachęcać do samodzielnych poszukiwań w literaturze.

Znaczek $\square$ oznacza koniec dowodu twierdzenia lub wskazuje, że dowód opuszczamy. Znaczek $\lozenge$ oznacza koniec rozwiązania zadania lub koniec przykładu. Czasami zamiast *wtedy i*

tylko wtedy, gdy piszemy "iff" (ang. *if and only if*). Używamy też skrótu "b.s.o." zamiast *bez straty ogólności*.

Skrypt należy zacząć czytać od *Elementarza* (rozdział 2) następnie przejść do *Arytmetyki Modularnej* (rozdział 5), stopniowo, gdy pojawia się potrzeba, zapoznając się z materiałem rozdziałów 1, 3 i 4. Kolejność czytania dalszych rozdziałów jest w zasadzie dowolna.

Rozdziały 2, 3 i 4 (w planie: wszystkie) kończą się zestawami zadań treningowych i wskazówkami/rozwiązaniami. Proponowana kolejność działań:

(0) dobrze zrozum matematyczną treść zadania i wykonaj e k s p e r y m e n t y rachunkowe,

(1) szukaj rozwiązania (nie rezygnuj przed upływem jednej godziny!),

(2) czytaj (z ołówkiem w ręce) pokazaną wskazówkę/rozwiązanie uzupełniając wszystkie szczegóły, i porównaj z rozwiązaniem własnym (jeżeli takowe masz),

(3) spróbuj znaleźć uogólnienie,

(4) zreferuj kolegom.

Autor wraz z konsultantem skryptu (którym jest pani Beata Bogdańska – współautor pozostałych części serii "Matematyka Olimpijska") ma nadzieję, że skrypt okaże się przydatny w trudnej pracy nad "otwieraniem" tego co w głowach młodzieży, dzięki zbiorowemu i (zapewne niezamierzenie) solidarnemu wysiłkowi dorosłych, zostało "zamknięte", mianowicie c i e k a w o ś c i ś w i a t a. Matematyka, jako królowa nauk, jest z pewnością jednym z lepszych (może najlepszym) "otwieraczem" młodych umysłów, a w jej ramach teoria liczb, jako królowa matematyki, wyróżnia się szczególną "ostrością".

APEL

Szanowni Czytelnicy!

Nasze skrypty z Matematyki Olimpijskiej są ciągle w trakcie tworzenia. Mimo naszych wysiłków z pewnością pozostało w nich jeszcze sporo do poprawienia. W związku z tym zwracamy się do Was z apelem o:

(1) krytyczne czytanie,

(2) informowanie o zauważonych błędach i innych niedostatkach zarówno merytorycznych jak i dydaktycznych (adres: **koloroweskrypty @ gmail.com**).

Bylibyśmy bardzo wdzięczni za wzięcie sobie do serca tego apelu. Nasze reakcje na Wasze uwagi zamieszczamy na stronie **sites.google.com/site/koloroweskrypty**.

Tabliczka chronologiczna

Euklides z Aleksandrii	(ok. 365 p.n.e. - ok. 300 p.n.e.)
Eratostenes z Cyreny	(275 p.n.e. - 194 p.n.e.)
Diofantos z Aleksandrii	(III - IV wiek n.e.)
Brahmagupta	(598 - 660)
Bhaskara	(1114 - 1185)
Leonardo Pisano Bigollo zw. **Fibonacci**	(ok. 1170 - ok. 1240)
Niccolò Fontana zw. **Tartaglia**	(ok. 1499 - 1557)
François **Viète**	(1540 - 1603)
Claude Gaspard **Bachet de Méziriac**	(1581 - 1638)
Pierre de **Fermat**	(1601 - 1665)
Isaac **Newton**	(1643 - 1727)
Jakob **Bernoulli**	(1654 - 1705)
Leonhard **Euler**	(1707 - 1783)
Étienne **Bézout**	(1730 - 1783)
Joseph-Louis **Lagrange**	(1736 - 1813)
Adrien Marie **Legendre**	(1752 - 1833)
Sophie **Germain**	(1776 - 1831)
Carl Friedrich **Gauss**	(1777 - 1855)
August Ferdinand **Möbius**	(1790 - 1868)
Peter Gustav **Lejeune-Dirichlet**	(1805 - 1859)
Joseph **Liouville**	(1809 - 1882)
Évariste **Galois**	(1811 - 1832)
James Joseph **Sylvester**	(1814 - 1897)
Pafnucy **Czebyszew**	(1821 - 1894)
Gotthold **Eisenstein**	(1823 - 1852)
Leopold **Kronecker**	(1823 - 1891)
Richard **Dedekind**	(1831 - 1916)
François Édouard **Lucas**	(1842 - 1891)
Georg **Frobenius**	(1849 - 1917)
Adolf **Hurwitz**	(1859 - 1919)
Kurt **Hensel**	(1861 - 1941)
David **Hilbert**	(1862 - 1943)
Hermann **Minkowski**	(1864 - 1909)
Jacques **Hadamard**	(1865 - 1963)
Charles **de la Vallée Poussin**	(1866 - 1962)
Srinivasa **Ramanujan**	(1887 - 1920)

Liczby pierwsze $3 \leqslant p \leqslant 2011$ i ich pierwiastki pierwotne

p	g	g'	p	g	p	g	p	g	p	g	p	g	p	g	p	g
3	2	-1	**173**	2	**397**	5	**641**	3	**887**	5	**1163**	5	**1451**	2	**1721**	3
5	2	-2	**179**	2	**401**	3	**643**	11	**907**	2	**1171**	2	**1453**	2	**1723**	3
7	3	-2	**181**	2	**409**	21	**647**	5	**911**	17	**1181**	7	**1459**	5	**1733**	2
11	2	-3	**191**	19	**419**	2	**653**	2	**919**	7	**1187**	2	**1471**	6	**1741**	2
13	2	-2	**193**	5	**421**	2	**659**	2	**929**	3	**1193**	3	**1481**	3	**1747**	2
17	3	-3	**197**	2	**431**	7	**661**	2	**937**	5	**1201**	11	**1483**	2	**1753**	7
19	2	-4	**199**	3	**433**	5	**673**	5	**941**	2	**1213**	2	**1487**	5	**1759**	6
23	5	-2	**211**	2	**439**	15	**677**	2	**947**	2	**1217**	3	**1489**	14	**1777**	5
29	2	-2	**223**	3	**443**	2	**683**	5	**953**	3	**1223**	5	**1493**	2	**1783**	10
31	3	-7	**227**	2	**449**	3	**691**	3	**967**	5	**1229**	2	**1499**	2	**1787**	2
37	2	-2	**229**	6	**457**	13	**701**	2	**971**	6	**1231**	3	**1511**	11	**1789**	6
41	6	-6	**233**	3	**461**	2	**709**	2	**977**	3	**1237**	2	**1523**	2	**1801**	11
43	3	-9	**239**	7	**463**	3	**719**	11	**983**	5	**1249**	7	**1531**	2	**1811**	6
47	5	-2	**241**	7	**467**	2	**727**	5	**991**	6	**1259**	2	**1543**	5	**1823**	5
53	2	-2	**251**	6	**479**	13	**733**	6	**997**	7	**1277**	2	**1549**	2	**1831**	3
59	2	-3	**257**	3	**487**	3	**739**	3	**1009**	11	**1279**	3	**1553**	3	**1847**	5
61	2	-2	**263**	5	**491**	2	**743**	5	**1013**	3	**1283**	2	**1559**	19	**1861**	2
67	2	-4	**269**	2	**499**	7	**751**	3	**1019**	2	**1289**	6	**1567**	3	**1867**	2
71	7	-2	**271**	6	**503**	5	**757**	2	**1021**	10	**1291**	2	**1571**	2	**1871**	14
73	5	-5	**277**	5	**509**	2	**761**	6	**1031**	14	**1297**	10	**1579**	3	**1873**	10
79	3	-2	**281**	3	**521**	3	**769**	11	**1033**	5	**1301**	2	**1583**	5	**1877**	2
83	2	-3	**283**	3	**523**	2	**773**	2	**1039**	3	**1303**	6	**1597**	11	**1879**	6
89	3	-3	**293**	2	**541**	2	**787**	2	**1049**	3	**1307**	2	**1601**	3	**1889**	3
97	5	-5	**307**	5	**547**	2	**797**	2	**1051**	7	**1319**	13	**1607**	5	**1901**	2
101	2	-2	**311**	17	**557**	2	**809**	3	**1061**	2	**1321**	13	**1609**	7	**1907**	2
103	5	-2	**313**	10	**563**	2	**811**	3	**1063**	3	**1327**	3	**1613**	3	**1913**	3
107	2	-3	**317**	2	**569**	3	**821**	2	**1069**	6	**1361**	3	**1619**	2	**1931**	2
109	6	-6	**331**	3	**571**	3	**823**	3	**1087**	3	**1367**	5	**1621**	2	**1933**	5
113	3	-3	**337**	10	**577**	5	**827**	2	**1091**	2	**1373**	2	**1627**	3	**1949**	2
127	3	-9	**347**	2	**587**	2	**829**	2	**1093**	5	**1381**	2	**1637**	2	**1951**	3
131	2	-3	**349**	2	**593**	7	**839**	11	**1097**	3	**1399**	13	**1657**	11	**1973**	2
137	3	-3	**353**	3	**599**	7	**853**	2	**1103**	5	**1409**	3	**1663**	3	**1979**	2
139	2	-4	**359**	7	**601**	7	**857**	3	**1109**	2	**1423**	3	**1667**	2	**1987**	2
149	2	-2	**367**	6	**607**	3	**859**	2	**1117**	2	**1427**	2	**1669**	2	**1993**	5
151	6	-5	**373**	2	**613**	2	**863**	5	**1123**	2	**1429**	6	**1693**	2	**1997**	2
157	5	-5	**379**	2	**617**	3	**877**	2	**1129**	11	**1433**	3	**1697**	3	**1999**	3
163	2	-4	**383**	5	**619**	2	**881**	3	**1151**	17	**1439**	7	**1699**	3	**2003**	5
167	5	-2	**389**	2	**631**	3	**883**	2	**1153**	5	**1447**	3	**1709**	3	**2011**	3

Spis treści

1 Pojęcia podstawowe **1**
- 1.1 Liczby naturalne . . . 1
  - 1.1.1 Kilka zasad podstawowych . . . 1
  - 1.1.2 Zasada Indukcji Matematycznej . . . 3
- 1.2 Działania algebraiczne . . . 6
- 1.3 Grupa . . . 8
- 1.4 Pierścień przemienny. Ciało . . . 9
- 1.5 Liczby zespolone . . . 11

2 Elementarz **18**
- 2.1 Największy wspólny dzielnik w pierścieniu $\mathbb{Z}$ . . . 18
  - 2.1.1 Podzielność i dzielenie z resztą w $\mathbb{Z}$ . . . 18
  - 2.1.2 Ideały w pierścieniu $\mathbb{Z}$ . . . 20
  - 2.1.3 Największy wspólny dzielnik . . . 22
  - 2.1.4 Zasadnicze Twierdzenie Arytmetyki . . . 24
  - 2.1.5 Najmniejsza wspólna wielokrotność . . . 25
  - 2.1.6 Algorytm Euklidesa . . . 26
- 2.2 Równanie $ax + by = n$ . . . 28
  - 2.2.1 Twierdzenie Brahmagupty-Bachet'a . . . 28
  - 2.2.2 Twierdzenie Sylvestera . . . 29
- 2.3 Liczby pierwsze . . . 31
  - 2.3.1 Istnienie i jednoznaczność rozkładu na czynniki pierwsze . . . 31
  - 2.3.2 Sito Eratostenesa. Twierdzenie Euklidesa . . . 32
  - 2.3.3 Kilka pytań dotyczących liczb pierwszych . . . 34
- 2.4 Wykładniki p-adyczne . . . 36
  - 2.4.1 Definicje. Formuła Legendre'a . . . 36
  - 2.4.2 Lemat o zwiększaniu wykładnika p-adycznego . . . 38
- 2.5 Trójki pitagorejskie . . . 42
  - 2.5.1 Trik . . . 42
  - 2.5.2 Trójki pitagorejskie . . . 43
- 2.6 Zadania dodatkowe . . . 44
  - 2.6.1 Treści zadań . . . 44
  - 2.6.2 Wskazówki i rozwiązania . . . 48

3 Wielomiany **64**
- 3.1 Pierścień wielomianów . . . 64
- 3.2 Siedem idei podstawowych . . . 66
  - 3.2.1 Pierwsza idea: twierdzenie Bézout'a . . . 66
  - 3.2.2 Druga idea: algorytm dzielenia z resztą . . . 68

3.2.3 Trzecia idea: twierdzenie Lagrange'a i o jednoznaczności . . . 70
3.2.4 Czwarta idea: pierwiastki wymierne . . . 72
3.2.5 Piąta idea: postać kanoniczna trójmianu kwadratowego . . . 73
3.2.6 Szósta idea: Wielomian jako funkcja rzeczywista . . . 75
3.2.7 Siódma idea: wzory Viète'a . . . 77
3.3 Jednoznaczność rozkładu w pierścieniu wielomianów . . . 81
3.3.1 Podzielność w pierścieniu wielomianów . . . 82
3.3.2 Ideał. Największy wspólny dzielnik . . . 83
3.3.3 Zasadnicze twierdzenie arytmetyki wielomianów . . . 84
3.3.4 Wielomiany nierozkładalne . . . 85
3.3.5 Jednoznaczność rozkładu . . . 85
3.4 Dalsze twierdzenia o wielomianach . . . 86
3.4.1 Zawartość wielomianu . . . 86
3.4.2 Wielomiany nierozkładalne w $\mathbb{Q}[X]$ . . . 89
3.4.3 Zasadnicze Twierdzenie Algebry . . . 92
3.4.4 Rozkłady w pierścieniu $\mathbb{C}[X]$ i $\mathbb{R}[X]$ . . . 94
3.4.5 Pierwiastki wielomianu $X^n - 1$ . . . 95
3.4.6 Wielomiany cyklotomiczne . . . 97
3.4.7 Rozwiązywanie równań stopnia 3 i 4 . . . 98
3.4.8 Wzory Viète'a . . . 101
3.4.9 Wielomiany palindromiczne . . . 104
3.4.10 Wielomian interpolacyjny Lagrange'a . . . 105
3.4.11 Funkcje wymierne. Ułamki proste . . . 106
3.4.12 Funkcje wymierne jako funkcje . . . 108
3.5 Wielomiany wielu zmiennych . . . 108
3.5.1 Definicje . . . 108
3.5.2 Tożsamość Sophie Germain . . . 110
3.5.3 Jeszcze dwie faktoryzacje . . . 111
3.6 Zadania dodatkowe . . . 112
3.6.1 Treści zadań . . . 112
3.6.2 Wskazówki/rozwiązania . . . 118

4 Funkcje arytmetyczne 143
4.1 Sumy potęg dzielników . . . 143
4.1.1 Funkcja τ . . . 144
4.1.2 Funkcja σ . . . 145
4.2 Funkcja φ Eulera . . . 146
4.3 Splot Dirichlet'a i odwracanie Möbiusa . . . 147
4.3.1 Splot Dirichlet'a . . . 147
4.3.2 Twierdzenie Möbiusa o odwracaniu . . . 148
4.4 Piętnaście zadań dodatkowych . . . 150
4.4.1 Treści zadań . . . 150
4.4.2 Rozwiązania wybranych ćwiczeń i zadań dodatkowych . . . 151

5 Arytmetyka modularna 157
5.1 Wstęp do teorii kongruencji . . . 157
5.1.1 Definicja i cechy podzielności . . . 157
5.1.2 Motywacja: równania diofantyczne . . . 160
5.1.3 Twierdzenie Schura . . . 161

5.1.4 Kongruencje liniowe 162
5.1.5 Odwracanie modulo m 163
5.2 Twierdzenie Eulera, Fermat'a i Wilsona 164
5.2.1 Zupełne i zredukowane układy reszt 164
5.2.2 Twierdzenie Eulera 165
5.2.3 Małe twierdzenie Fermat'a 166
5.2.4 Twierdzenie Wilsona 167
5.3 Układy kongruencji liniowych 168
5.3.1 Twierdzenie chińskie o resztach 169
5.3.2 Zadanie o długiej igle 171
5.3.3 Uogólnione twierdzenie chińskie o resztach 172
5.4 Pierścień klas reszt modulo m 175
5.4.1 Działania na warstwach modulo m 176
5.4.2 Grupa $(\mathbb{Z}/m)^*$ warstw odwracalnych 177
5.4.3 Ciało $\mathbb{Z}/p$ 178
5.4.4 Pierwiastki kongruencji wielomianowych 178
5.4.5 Kongruencje wielomianowe modulo p 181
5.4.6 Ważne zastosowanie twierdzenia chińskiego 181
5.5 Rząd elementu grupy w teorii liczb 183
5.5.1 Podgrupy i twierdzenie Lagrange'a 183
5.5.2 Podstawowe własności rzędu elementu 184
5.5.3 Rząd elementu w grupie $(\mathbb{Z}/m, +)$ 186
5.5.4 Rząd elementu w grupie $((\mathbb{Z}/m)^*, \cdot)$ 186
5.5.5 O liczbach pierwszych w ciągach arytmetycznych 189
5.5.6 Twierdzenie Zsigmondy'*ego* 191
5.6 Pierwiastki pierwotne 195
5.6.1 Definicja i uwagi wstępne 195
5.6.2 Twierdzenie o istnieniu pierwiastków pierwotnych 197
5.6.3 Jeszcze kilka przykładów 199
5.6.4 Indeks 201
5.6.5 Dwa słowa o liczbach Carmichaela 202
5.7 Reszty kwadratowe i prawo wzajemności 203
5.7.1 Reszty i niereszty kwadratowe modulo p 203
5.7.2 Symbol Legendre'a 204
5.7.3 Kryterium Eulera 204
5.7.4 Kryterium Gaussa 206
5.7.5 Prawo wzajemności reszt kwadratowych 208
5.7.6 Prawo wzajemności a ciągi arytmetyczne 211
5.7.7 Trójmian kwadratowy modulo p 213
5.7.8 Kilka zadań 214
5.7.9 Liczba lokalnie kwadratowa jest kwadratem (globalnym) 217
5.8 Kongruencje modulo p^n. Liczby p-adyczne 218
5.8.1 Reszty kwadratowe modulo p^n 219
5.8.2 Lemat Hensela 220
5.8.3 Jedno interesujące zadanie 221
5.8.4 Dwa słowa o liczbach p-adycznych 222

6 Dodatkowe wiadomości o wielomianach 224
6.1 Pochodna wielomianu . . . 224
6.1.1 Funkcja wielomianowa . . . 224
6.1.2 Definicja pochodnej . . . 225
6.1.3 Twierdzenia Rolle'*a* i Lagrange'*a* . . . 225
6.1.4 Wzór Maclaurina i wzór Taylora . . . 226
6.1.5 Pochodna a pierwiastki wielokrotne . . . 227
6.2 Wielomiany symetryczne . . . 227
6.2.1 Definicja . . . 228
6.2.2 Twierdzenie Newtona . . . 229
6.2.3 Wyróżnik . . . 230
6.2.4 Funkcje tworzące . . . 230
6.3 Liczby algebraiczne i przestępne . . . 232
6.3.1 Wielomian minimalny liczby algebraicznej . . . 232
6.3.2 Uwalnianie się od niewymierności w mianowniku . . . 233
6.3.3 Pierścień liczb algebraicznych całkowitych . . . 234
6.3.4 Nierozkładalność wielomianów cyklotomicznych . . . 236
6.3.5 Liczby przestępne . . . 238
6.3.6 Twierdzenie Liouville'*a* . . . 238
6.4 O zerach wielomianów wielu zmiennych . . . 240
6.4.1 Combinatorial Nullstellensatz . . . 241
6.4.2 Kilka zastosowań . . . 244
6.4.3 Twierdzenia Chevalley'*a* i Warninga . . . 245
6.5 Wielomiany i liczby Bernoulli'*ego* . . . 248
6.5.1 Sumowanie potęg . . . 248
6.5.2 Wielomiany i liczby Bernoulli'*ego* . . . 248

7 Aproksymacje diofantyczne 250
7.1 Twierdzenie Dirichlet'*a* . . . 250
7.2 Ciągi Farey'*a* . . . 251
7.3 Ułamki łańcuchowe . . . 253
7.3.1 Kanoniczne rozwinięcia. Reguła Eulera . . . 253
7.3.2 Nieskończone ułamki łańcuchowe . . . 256
7.3.3 Złota liczba. Twierdzenie Hurwitza . . . 259
7.3.4 Grupa $\mathbf{GL}_2(\mathbb{Z})$ . . . 261
7.3.5 Równoważność liczb . . . 262
7.3.6 Niewymierności kwadratowe . . . 263
7.3.7 Okresowe ułamki łańcuchowe . . . 265
7.3.8 Twierdzenia Lagrange'*a* i Galois'*a* . . . 267

8 Sumy kwadratów 270
8.1 Jedna ważna tożsamość . . . 270
8.2 Sumy dwóch kwadratów . . . 272
8.2.1 Twierdzenie Fermat'*a*-Eulera . . . 272
8.2.2 Drugi dowód twierdzenia Fermat'*a*-Eulera . . . 274
8.2.3 Twierdzenie o przedstawieniu . . . 275
8.2.4 Funkcja $r(n)$ . . . 276
8.3 Nieco geometrii w teorii liczb . . . 277
8.3.1 Kraty w płaszczyźnie . . . 277

8.3.2 Dyskretne podgrupy płaszczyzny . . . 278
8.3.3 Twierdzenie Minkowskiego o figurze wypukłej . . . 280
8.3.4 Dwa zastosowania . . . 281
8.3.5 Liczby naturalne postaci $x^2 + 2y^2$ i $x^2 + 3y^2$ . . . 283
8.3.6 Liczby pierwsze postaci $x^2 + 5y^2$ . . . 285
8.4 Binarne formy kwadratowe . . . 287
8.4.1 Wyróżnik formy . . . 288
8.4.2 Równoważność form . . . 288
8.4.3 Lemat Lagrange'*a* . . . 290
8.4.4 Redukcja form dodatnio-określonych . . . 291
8.5 Sumy więcej niż dwóch kwadratów . . . 293
8.5.1 Twierdzenie o sumach czterech kwadratów . . . 294
8.5.2 Uwagi o sumach trzech kwadratów . . . 296
8.6 Dodatek. Piąty dowód TFE . . . 297

9 Arytmetyka ciągów rekurencyjnych 301
9.1 Klasyczny ciąg Fibonacci'*ego* . . . 301
9.1.1 Wzór Binet'*a* . . . 302
9.1.2 Kilka tożsamości . . . 302
9.1.3 Dwie interpretacje ciągu (f_n) . . . 304
9.1.4 Ciąg (f_n) jest NWD-ciągiem . . . 304
9.2 Metoda Eulera i metoda funkcji tworzących . . . 305
9.2.1 Metoda Eulera . . . 305
9.2.2 Pierścień formalnych szeregów potęgowych . . . 308
9.2.3 Metoda funkcji tworzących . . . 309
9.3 Ciągi Lucas'*a* . . . 309
9.3.1 Przestrzeń $\mathcal{R}ek(P, Q)$ . . . 310
9.3.2 Definicja ciągów Lucas'*a* . . . 310
9.3.3 Kilka tożsamości . . . 311
9.3.4 Podzielność wyrazów ciągów Lucas'*a* . . . 312
9.4 Ilustracja geometryczna . . . 313
9.4.1 Macierze odwzorowań liniowych . . . 313
9.4.2 Wyznacznik odwzorowania liniowego . . . 315
9.4.3 Pola trójkątów . . . 315
9.4.4 Ogólny wzór Cassini'*ego* . . . 316
9.5 Ciągi rekurencyjne modulo p . . . 317
9.5.1 Warstwy "zespolone" modulo p . . . 317
9.5.2 $\mathbb{F}_p(\iota)$ jest ciałem . . . 319
9.5.3 Dwa słowa o grupie multyplikatywnej $\mathbb{F}_p(\iota)^*$ . . . 320
9.5.4 Wzory Eulera-Binet'*a* modulo p . . . 321
9.5.5 Okresowość ciągów rekurencyjnych modulo p . . . 322

10 Pierścienie kwadratowe 325
10.1 Pierścień liczb całkowitych Gaussa . . . 326
10.1.1 Definicja i podstawowe własności . . . 326
10.1.2 Dzielenie z resztą i podzielność w $\mathbb{Z}[\,i\,]$ . . . 327
10.1.3 Algorytm Euklidesa w $\mathbb{Z}[\,i\,]$ . . . 330
10.1.4 Liczby pierwsze w $\mathbb{Z}[\,i\,]$ . . . 330
10.1.5 Twierdzenie o jednoznaczności rozkładu w $\mathbb{Z}[\,i\,]$ . . . 332

10.1.6 Rozkład liczb pierwszych wymiernych w $\mathbb{Z}[i]$ . . . 335
10.2 Pierścienie kwadratowe . . . 336
10.2.1 Jedności w $\mathbb{Z}[\tau_D]$ . . . 337
10.2.2 Dzielenie z resztą w $\mathbb{Z}[\tau_D]$ . . . 337
10.2.3 Podzielność, NWD i ideały w $\mathbb{Z}[\tau_D]$ . . . 340
10.2.4 Dig'*owość* pierścieni kwadratowych . . . 342
10.2.5 Wnioski z dig'*owości* . . . 342
10.2.6 Związek z formami kwadratowymi . . . 344
10.2.7 Jednoznaczność rozkładu . . . 347
10.2.8 Pierścienie $\mathbb{Z}[\tau_{-2}]$, $\mathbb{Z}[\tau_{-3}]$ i $\mathbb{Z}[\tau_{-5}]$ . . . 349
10.3 Teoria podzielności w dig'*ach* . . . 354
10.3.1 Dziedziny całkowitości . . . 354
10.3.2 Relacja podzielności. Relacja stowarzyszenia . . . 355
10.3.3 Ideał. Dziedzina ideałów głównych . . . 356
10.3.4 Największy wspólny dzielnik . . . 357
10.3.5 Elementy nierozkładalne i pierwsze w $\mathcal{R}$ . . . 357
10.3.6 Jednoznaczność rozkładu w dig'*ach* . . . 358
10.4 Jedności rzeczywiste . . . 360
10.4.1 Lemat o równaniu $x^2 - Dy^2 = 1$ . . . 360
10.4.2 Jedności fundamentalne . . . 361
10.4.3 Pierścienie typu (-1) i $(+1)$ . . . 364

11 Równania diofantyczne 365
11.1 Metody podstawowe . . . 365
11.1.1 Wykorzystanie nierówności . . . 365
11.1.2 Metoda zstępowania . . . 366
11.1.3 Wykorzystanie kongruencji . . . 367
11.1.4 Wykorzystanie jednoznaczności rozkładu . . . 369
11.2 Wielkie Twierdzenie Fermat'*a* . . . 371
11.2.1 Twierdzenia Fermat'*a* . . . 372
11.2.2 Twierdzenie Sophie Germain . . . 374
11.2.3 Metoda Eulera dowodu WTF(3) . . . 375
11.2.4 Równanie $x^3 + y^3 + z^3 = w^3$ . . . 377
11.3 Równanie Ramanujana . . . 378
11.4 Równanie indyjskie . . . 383
11.4.1 Twierdzenie podstawowe . . . 383
11.4.2 Interpretacje . . . 386
11.4.3 Równanie *anty*-indyjskie . . . 388
11.4.4 Ogólne równanie indyjskie . . . 389
11.4.5 Kilka zadań . . . 390
11.5 Punkty wymierne na prostych i na stożkowych . . . 391
11.6 Krzywe sześcienne . . . 398
11.6.1 Postać normalna. Przykłady . . . 398
11.6.2 Krzywe eliptyczne . . . 402
11.6.3 Metoda siecznych-stycznych . . . 403
11.6.4 Równania $y^2 = x^3 + 1$ i $y^2 = x^3 - 1$ . . . 406
11.6.5 Dodawanie punktów krzywej eliptycznej . . . 409

12 Kilka wiadomości dodatkowych **412**
12.1 Część całkowita i ułamkowa liczby rzeczywistej 412
12.1.1 Podstawowe własności 412
12.1.2 Twierdzenie Beatty'*ego* 414
12.1.3 Zadania z częścią ułamkową 415
12.2 Zapis pozycyjny liczb 417
12.2.1 Zapis pozycyjny liczb naturalnych 417
12.2.2 Zapis pozycyjny liczb rzeczywistych 419
12.3 Ułamki egipskie 421
12.3.1 Skończone sumy ułamków egipskich 421
12.3.2 Szeregi harmoniczne 425
12.3.3 Liczby harmoniczne. Twierdzenie Wolstenholme'*a* 429
12.4 Współczynniki dwumienne 431
12.4.1 Wielomiany Newtona 432
12.4.2 Twierdzenie Lucas'*a* 432
12.4.3 Twierdzenie Wolstenholme'*a*-Glaishera 434
12.5 Rozmieszczenie liczb pierwszych 436
12.5.1 Dwa twierdzenia Czebyszewa 436
12.5.2 Twierdzenie o liczbach pierwszych 440

Literatura **441**

Indeks **442**

Rozdział 1

Pojęcia podstawowe

Ich bin der Meinung [...] *daß man zu einer strengen und völlig befriedigenden Begründung des Zahlbegriffs kommen kann, und zwar durch eine Methode, die ich die axiomatische nennen will.*
(David Hilbert)

W rozdziale tym przypominamy podstawowe fakty dotyczące liczb naturalnych oraz poznajemy definicje najważniejszych struktur algebraicznych takich jak grupa, pierścień i ciało. W końcu rozdziału poznajemy nowy rodzaj liczb: liczby zespolone.

1.1 Liczby naturalne

Zakładamy, że Czytelnik jest dobrze zaznajomiony z pojęciem **liczby całkowitej**. Zbiór wszystkich liczb całkowitych

$$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

oznaczamy przez $\mathbb{Z}$. Dodatnie elementy tego zbioru nazywamy **liczbami naturalnymi**. Zbiór liczb naturalnych oznaczamy symbolem $\mathbb{N}$. W niektórych podręcznikach zero uważa się za liczbę naturalną. Nam będzie wygodniej "zaczynać" liczby naturalne od 1.

1.1.1 Kilka zasad podstawowych

Najważniejszym faktem dotyczącym liczb naturalnych jest Zasada Minimum. Jest ona w istocie aksjomatem (czyli twierdzeniem przyjmowanym bez dowodu).

Zasada minimum *Każdy niepusty podzbiór zbioru liczb naturalnych zawiera (dokładnie jedną) liczbę najmniejszą.*

Standardowe zastosowania Zasady Minimum w rozumowaniach teorioliczbowych zobaczymy w dowodach twierdzeń T2.14 i T2.16. Teraz pokażemy na prostym przykładzie, jak to działa. Wybieramy w tym celu dowód niewymierności $\sqrt{n}$, gdzie $n \in \mathbb{N}$ nie jest kwadratem:

ZADANIE 1.1 Udowodnić, że jeżeli liczba naturalna n nie jest kwadratem żadnej liczby całkowitej, to nie jest też kwadratem żadnej liczby wymiernej.

Rozwiązanie. Załóżmy, nie wprost, że istnieją takie ułamki $\frac{a}{b}$, że $a, b \in \mathbb{N}$ i że zachodzi równość $\sqrt{n} = \frac{a}{b}$, czyli równość $nb^2 = a^2$. Rozważmy więc (niepusty!) zbiór mianowników wszystkich takich ułamków $\frac{a}{b}$. Niech b_0 będzie najmniejszą liczbą w tym zbiorze. Wówczas

$$\frac{nab_0}{ab_0} = n = \frac{ka^2}{kb_0^2}$$

dla pewnego $a \in \mathbb{N}$ i dowolnej liczby $k \in \mathbb{N}$. Stąd

$$n = \frac{nab_0 - ka^2}{ab_0 - kb_0^2} = \frac{a}{b_0} \cdot \frac{nb_0 - ka}{a - kb_0} = \sqrt{n} \cdot \frac{nb_0 - ka}{a - kb_0} \tag{1.1}$$

na mocy zasady **odejmowania proporcji stronami** i założenia $\sqrt{n} = a/b_0$. Podnosząc równość (1.1) obustronnie do kwadratu i upraszczając przez n, dostajemy

$$n = \left(\frac{nb_0 - ka}{a - kb_0}\right)^2.$$

Połóżmy w tej równości k wyznaczone (jednoznacznie) z nierówności $k^2 < n < (k+1)^2$. Wówczas $kb_0 < a < kb_0 + b_0$, skąd $0 < a - kb_0 < b_0$ i widzimy, że dodatni mianownik $a - kb_0$ ułamka $\frac{nb_0 - ka}{a - kb_0}$ jest mniejszy niż b_0. Sprzeczność. $\Diamond$

Przykład. Dowodzimy: *Liczba* 1 *jest najmniejszą liczbą naturalną.* Rzeczywiście, jeżeli istnieją liczby naturalne mniejsze niż 1, to niech (Zasada Minimum!) n_0 będzie najmniejszą liczbą naturalną mniejszą niż 1. Wówczas $n_0^2 < n_0 < 1$. Sprzeczność. Q.e.d. $\Diamond$

Czytelnik zechce z pewnością udowodnić prawdziwość kolejnej zasady:

ZASADA SKWANTOWANIA *Jeżeli liczby całkowite a, b spełniają warunek $a > b$, to $a \geqslant b + 1$. W szczególności: jeżeli $c \in \mathbb{Z}$ i $c > 0$, to $c \geqslant 1$.*

Przykładowe zastosowanie Zasady Skwantowania widzimy w rozwiązaniu takiego zadania:

ZADANIE 1.2 Udowodnić, że jeżeli dla liczb naturalnych a, b, c, d, k, l zachodzi równość $bc - ad = 1$ i nierówności $\frac{a}{b} < \frac{k}{l} < \frac{c}{d}$, to $k \geqslant a + c$ i $l \geqslant b + d$.

Rozwiązanie. Nierówność $\frac{a}{b} < \frac{k}{l}$ daje $0 < bk - al$. Stąd, ponieważ mamy do czynienia z liczbą całkowitą, dostajemy $1 \leqslant bk - al$. Mnożąc tę nierówność przez c znajdujemy

$$c \leqslant c(bk - al) = bck - acl = (1 + ad)k - acl,$$

skąd $a(cl - dk) + c \leqslant k$, czyli $a + c \leqslant k$ (bo $cl - dk > 0$, więc $cl - dk \geqslant 1$). Podobnie, mnożąc nierówność $cl - dk \geqslant 1$ przez b, dostaniemy nierówność $b + d \leqslant l$. $\Diamond$

Często stosujemy również Zasadę Maksimum:

ZASADA MAKSIMUM *Każdy niepusty i ograniczony (od góry) zbiór liczb naturalnych zawiera dokładnie jeden element największy.*

ZADANIE 1.3 Udowodnić Zasadę Maksimum korzystając z Zasady Minimum.

R o z w i ą z a n i e. Niech X będzie niepustym i ograniczonym podzbiorem zbioru liczb naturalnych. To znaczy, że istnieje takie $a \in \mathbb{N}$, że dla każdego $x \in X$ mamy $x \leqslant a$. Niech $Y = \{y \in \mathbb{N} : \forall_{x \in X}\, y \geqslant x\}$ będzie zbiorem wszystkich ograniczeń górnych zbioru X. Zbiór Y jest niepusty, bo $a \in Y$. Zawiera zatem element najmniejszy. Oznaczmy go m. Wówczas

$$m \geqslant x$$

dla każdego $x \in X$, bo $m \in Y$. Twierdzimy, że m należy do X i jest, wobec tego, największym elementem zbioru X. Gdyby $m \notin X$, to wszystkie nierówności $m \geqslant x$ byłyby ostre i wtedy (na mocy Zasady Skwantowania) mielibyśmy $m - 1 \geqslant x$ dla każdego $x \in X$. To jednakże jest niemożliwe, bo m jest najmniejszym elementem zbioru Y. $\Diamond$

Ćwiczenie 1.1 Udowodnić Zasadę Minimum korzystając z Zasady Maksimum.

1.1.2 Zasada Indukcji Matematycznej

Zasada Indukcji Matematycznej jest (logicznie) równoważna Zasadzie Minimum, ale często bywa wygodniejsza w stosowaniu.

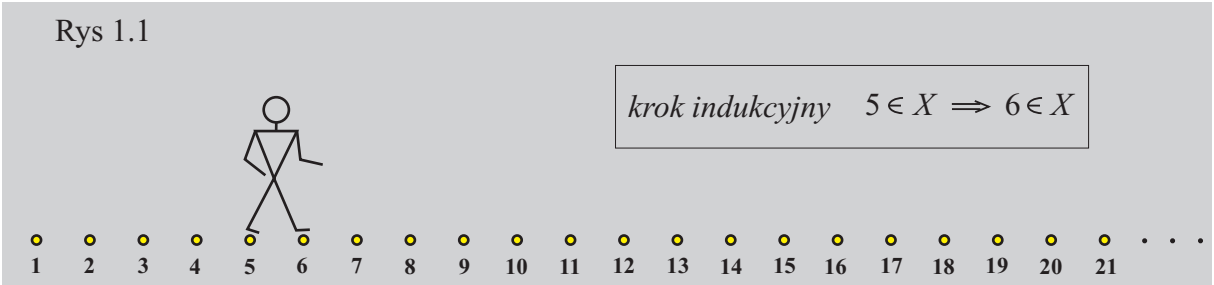
ZASADA INDUKCJI MATEMATYCZNEJ *Niech $X \subseteq \mathbb{N}$ będzie podzbiorem zbioru liczb naturalnych. Załóżmy, że spełnione są warunki:*

$$\text{(B)}\quad \boxed{1 \in X}, \qquad \text{(I)}\quad \boxed{k \in X \Rightarrow k+1 \in X}.$$

Wówczas $X = \mathbb{N}$.

Podzbiór X zbioru liczb naturalnych nazwiemy **podzbiorem induktywnym**, gdy spełnia warunek (I). Zasada Indukcji Matematycznej mówi po prostu, że *zawierający liczbę* 1 *podzbiór induktywny zbioru liczb naturalnych jest c a ł y m zbiorem liczb naturalnych* $\mathbb{N}$.

Rys 1.1



P r z y k ł a d. Udowodnimy, że *suma wszystkich liczb naturalnych niewiększych niż n wynosi* $\frac{n(n+1)}{2}$. Oznaczmy tę sumę przez S_n. Mamy udowodnić, że zbiór

$$X = \left\{ k \in \mathbb{N} : S_k = \frac{k(k+1)}{2} \right\}$$

jest całym zbiorem liczb naturalnych. W pierwszym kroku sprawdzamy, czy zbiór X spełnia warunek (B) (zwany **warunkiem bazowym**). Tę część rozumowania nazywamy **bazą**

rozumowania indukcyjnego. W aktualnym przypadku warunek bazowy jest spełniony (bowiem $1 = \frac{1\cdot 2}{2}$). Sprawdzenie zachodzenia warunku (I), czyli induktywności zbioru X, nazywa się **krokiem indukcyjnym** rozumowania indukcyjnego. Załóżmy więc, że liczba naturalna k należy do X. Wówczas, w aktualnym przypadku,

$$S_{k+1} = S_k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2},$$

więc $k+1 \in X$. Dzięki ZIM (Zasadzie Indukcji Matematycznej) widzimy, że $X = \mathbb{N}$. $\Diamond$

Podobnie dowodzimy tez poniższego ćwiczenia:

Ćwiczenie 1.2 Udowodnić, że dla każdej liczby naturalnej $n > 1$:

1. $1^2 + 2^2 + 3^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$,

2. $1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \dfrac{n(4n^2-1)}{3}$,

3. $\dfrac{1\cdot 3\cdot 5\cdot \ldots \cdot (2n-1)}{2\cdot 4\cdot 6\cdot \ldots \cdot 2n} < \dfrac{1}{\sqrt{3n+1}}$,

4. $\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}} = 2\cos\dfrac{\pi}{2^{n+1}}$ (n pierwiastków),

5. $\dfrac{1}{1+x} + \dfrac{2}{1+x^2} + \dfrac{4}{1+x^4} + \ldots + \dfrac{2^n}{1+x^{2^n}} = \dfrac{2^{n+1}}{1-x^{2^{n+1}}} - \dfrac{1}{1-x}$ dla $|x| \neq 1$.

Ćwiczenie 1.3 Udowodnić poniższe wersje ZIM:

(1) *Jeżeli podzbiór $X \subseteq \mathbb{N}$ spełnia warunki*

$$\text{(B)} \quad \boxed{\boxed{1 \in X}}, \qquad \text{(IU)} \quad \boxed{\boxed{\{1, \ldots, k\} \subseteq X \;\Rightarrow\; k+1 \in X}},$$

to X jest c a ł y m zbiorem liczb naturalnych.

(2) *Jeżeli podzbiór $X \subseteq \mathbb{N}$ spełnia warunki*

$$\text{(B1-2)} \quad \boxed{\boxed{1,\, 2 \in X}}, \qquad \text{(I2)} \quad \boxed{\boxed{k \in X \;\Rightarrow\; k+2 \in X}},$$

to X jest c a ł y m zbiorem liczb naturalnych.

ZADANIE 1.4 Udowodnić, że zbiór $\mathcal{G} = \{0, 1, \ldots, 1023\}$ da się rozbić na sumę takich dwóch r o z ł ą c z n y c h r ó w n o l i c z n y c h podzbiorów $\mathcal{A}$, $\mathcal{B}$, że dla każdego $k = 1, 2, \ldots, 9$ suma k-tych potęg liczb zbioru $\mathcal{A}$ równa jest sumie k-tych potęg liczb zbioru $\mathcal{B}$.

R o z w i ą z a n i e. Po pierwsze dobrze jest się domyślić, że jest to zadanie dające się rozwiązać za pomocą indukcji. Mianowicie oznaczymy przez X zbiór takich liczb naturalnych n, dla których zbiór $\mathcal{G}(n) = \{0, 1, \ldots, 2^{n+1}-1\}$ można przedstawić w postaci sumy takich dwóch równolicznych podzbiorów $\mathcal{A}(n)$ i $\mathcal{B}(n)$, że dla każdego $k = 1, 2, \ldots, n$ suma k-tych potęg

liczb zbioru $\mathcal{A}(n)$ równa jest sumie k-tych potęg liczb zbioru $\mathcal{B}(n)$. Nasze zadanie polega na udowodnieniu, że $9 \in X$. Wykażemy przez indukcję nierównie więcej: $X = \mathbb{N}$.

Korzystając z Zasady Indukcji zdefiniujemy zbiory $\mathcal{A}(n)$ i $\mathcal{B}(n)$ dla każdego $n \in \mathbb{N}$. Niech $\mathcal{A}(1) = \{0,\, 3\}$ i $\mathcal{B}(1) = \{1,\, 2\}$ (to jest **baza definicji indukcyjnej**). Następnie definiujemy

$$\mathcal{A}(n+1) = \mathcal{A}(n) \cup [\mathcal{B}(n) + 2^{n+1}], \quad \mathcal{B}(n+1) = \mathcal{B}(n) \cup [\mathcal{A}(n) + 2^{n+1}]. \tag{1.2}$$

[Używamy tu wygodnego skrótu $\mathcal{X} + a = \{x + a : x \in \mathcal{X}\}$ dla dowolnego podzbioru $\mathcal{X} \subseteq \mathbb{N}$ i dowolnej liczby $a \in \mathbb{N}$.] To jest **krok indukcyjny definicji indukcyjnej** (= określenie obiektu "następnego" za pomocą "poprzedniego" lub "poprzednich"). Mamy więc na przykład:

$$\mathcal{A}(2) = \mathcal{A}(1) \cup [\mathcal{B}(1) + 4] = \{0,\, 3\} \cup [\{1,\, 2\} + 4] = \{0,\, 3\} \cup \{5,\, 6\} = \{0,\, 3,\, 5,\, 6\},$$
$$\mathcal{B}(2) = \mathcal{B}(1) \cup [\mathcal{A}(1) + 4] = \{1,\, 2\} \cup [\{0,\, 3\} + 4] = \{1,\, 2\} \cup \{4,\, 7\} = \{1,\, 2,\, 4,\, 7\}.$$

Łatwo, przez indukcję(!), sprawdzić, że zbiory $\mathcal{A}(n)$, $\mathcal{B}(n)$ są r o z ł ą c z n e i r ó w n o l i c z n e. Czytelnik powinien bezwzględnie to zrobić.

Pozostało nam sprawdzenie, że $\sum_{x\in\mathcal{A}(n)} x^k = \sum_{x\in\mathcal{B}(n)} x^k$ dla wszystkich $n \in \mathbb{N}$ i wszystkich $1 \leqslant k \leqslant n$. Robimy to, oczywiście, za pomocą indukcji matematycznej, której baza jest po prostu równością $0 + 3 = 1 + 2$.

Dla wykonania kroku indukcyjnego ustalmy liczby naturalne $k \leqslant n+1$. Mamy wtedy

$$\sum_{x\in\mathcal{A}(n+1)} x^k = \sum_{x\in\mathcal{A}(n)} x^k + \sum_{x\in\mathcal{B}(n)} (x + 2^{n+1})^k = \sum_{x\in\mathcal{A}(n)} x^k + \sum_{x\in\mathcal{B}(n)} \sum_{s=0}^{k} \binom{k}{s} x^{k-s} 2^{(n+1)s} =$$
$$\sum_{x\in\mathcal{A}(n)} x^k + \sum_{s=0}^{k} \binom{k}{s} 2^{(n+1)s} \sum_{x\in\mathcal{B}(n)} x^{k-s} = \sum_{x\in\mathcal{G}(n)} x^k + \sum_{s=1}^{k} \binom{k}{s} 2^{(n+1)s} \sum_{x\in\mathcal{B}(n)} x^{k-s}.$$

Pierwsza równość wynika z (1.2), druga z twierdzenia o dwumianie (por. (1.7)), trzecia z przemienności sumy, a czwarta z równości $\mathcal{G}(n) = \mathcal{A}(n) \sqcup \mathcal{B}(n)$ (suma rozłączna, zob. $\mathbb{KOM}$). Dokładnie tak samo dostaniemy

$$\sum_{x\in\mathcal{B}(n+1)} x^k = \sum_{x\in\mathcal{G}(n)} x^k + \sum_{s=1}^{k} \binom{k}{s} 2^{(n+1)s} \sum_{x\in\mathcal{A}(n)} x^{k-s}.$$

Założenie indukcyjne, czyli równości $\sum_{x\in\mathcal{A}(n)} x^{k-s} = \sum_{x\in\mathcal{B}(n)} x^{k-s}$ dla wszystkich $s = 1, \ldots, k$ (przy czym w przypadku $s = k$ równość ta oznacza, po prostu równość mocy $|\mathcal{A}(n)| = |\mathcal{B}(n)|$) daje więc równość $\sum_{x\in\mathcal{A}(n+1)} x^k = \sum_{x\in\mathcal{B}(n+1)} x^k$. W ten sposób zadanie jest rozwiązane. $\Diamond$

Rozwiązując poniższe zadanie również należy postawić tezę ogólną (*dla dowolnego* n) a następnie udowodnić ją za pomocą ZIM.

ZADANIE HALMOSA. W pewnym miasteczku mieszka 345 zamężnych matematyczek. Każda z nich wie w każdej chwili czy mąż innej jest wierny czy nie, nic nie wie jednak o swoim mężu. Prawo tego miasteczka wymaga aby każdy, kto jest w stanie p r z e p r o w a d z i ć d o w ó d niewierności swojego partnera, zastrzelił go na specjalnym miejscu straceń tego samego dnia o zachodzie słońca. Każda matematyczka jest absolutnie inteligentna i absolutnie prawomyślna.

Pewnego dnia pani burmistrz (jedyna niezamężna w miasteczku) ogłosiła, że w miasteczku są niewierni mężowie. Zakazała porozumiewania się paniom matematyczkom w rzeczonej sprawie, jednocześnie nakazując przeprowadzanie rozumowań dowodowych. W rzeczywistości w miasteczku było 40 niewiernych mężów. Co się stanie w miasteczku po ogłoszeniu pani burmistrz?

Czasami niezbędne jest stosowne wzmocnienie tezy, która staje się założeniem w kroku indukcyjnym:

Ćwiczenie 1.4 Udowodnić za pomocą indukcji, że dla dowolnej liczby naturalnej n zachodzi nierówność

$$h_n(2) := 1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} < 2.$$

Wskazówka. Łatwiej dowodzić nierówności mocniejszej: $h_n(2) \leqslant 2 - \frac{1}{n}$.

ZADANIE 1.5 Udowodnić, że Zasada Minimum jest równoważna Zasadzie Indukcji.

Rozwiązanie. (1) Dowodzimy najpierw, że z ZIM wynika ZM. Postępujemy nie wprost. To znaczy, załóżmy, że zbiór $Y \subseteq \mathbb{N}$ jest podzbiorem niepustym bez elementu najmniejszego. Zdefiniujmy podzbiór $X \subseteq \mathbb{N}$:

$$X = \{n \in \mathbb{N} : \{1, 2, \ldots, n\} \cap Y = \varnothing\}.$$

Jasne, że $1 \in X$ (bo $\{1\} \cap Y = \varnothing$, bowiem w przeciwnym przypadku liczba 1 byłaby elementem najmniejszym w Y). Zatem X spełnia warunek bazowy ZIM. Sprawdzimy, że X jest podzbiorem induktywnym: Niech $k \in X$. Wówczas $\{1, \ldots, k\} \cap Y = \varnothing$, więc, gdyby $\{1, \ldots, k, k+1\} \cap Y \neq \varnothing$, to liczba $k+1$ musiałaby należeć do Y i byłaby wtedy elementem najmniejszym w Y. Ponieważ założyliśmy, że w Y nie ma elementu najmniejszego, więc musi być $\{1, \ldots, k, k+1\} \cap Y = \varnothing$, czyli $k+1 \in X$. Zatem, na mocy ZIM, $X = \mathbb{N}$. To oznacza, że $Y = \varnothing$. Uzyskana sprzeczność kończy rozumowanie.

(2) Dowodzimy teraz, że z ZM wynika ZIM. Załóżmy, że $X \subseteq \mathbb{N}$ spełnia warunki (B) i (I) i że, nie wprost, $X \neq \mathbb{N}$. Wówczas $Y = \mathbb{N} \setminus X$ jest niepusty. Ma więc element najmniejszy n_0. Wtedy $n_0 - 1$ jest liczbą naturalną (!) należącą do X. Więc $n_0 = (n_0 - 1) + 1 \in X$, bo X jest induktywny. Sprzeczność. $\Diamond$

1.2 Działania algebraiczne

Podstawowym pojęciem w algebrze jest pojęcie działania (dwuargumentowego). **Algebra** jest działem matematyki badającym **struktury algebraiczne**, czyli zbiory z działaniami.

Definicja 1.1 Niech A będzie dowolnym zbiorem. Funkcję $f : A \times A \longrightarrow A$, która każdej uporządkowanej parze (α, β) elementów zbioru A przyporządkowuje element $f(\alpha, \beta)$ tego samego zbioru, nazywamy **działaniem dwuargumentowym** w zbiorze A. Na oznaczenie działania używamy jakiegoś specjalnego znaczka, na przykład $+, \cdot, \times, \circ, *$ (itp.), i zamiast $+(\alpha, \beta)$ (itp.) piszemy $\alpha + \beta$ (itp.). Element $\alpha * \beta \in A$ nazywamy **wynikiem** działania $*$ na parze $(\alpha, \beta) \in A \times A$.

Definicja 1.2 Działanie $* : A \times A \longrightarrow A$ nazywamy **łącznym**, gdy

$$\alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma \tag{1.3}$$

dla dowolnych α, β, $\gamma \in A$. Działanie $*$ nazywamy **przemiennym**, gdy

$$\alpha * \beta = \beta * \alpha \tag{1.4}$$

dla dowolnych α, $\beta \in A$.

P r z y k ł a d 1. Każdy zna działania **dodawania** i **mnożenia** w zbiorze $\mathbb{Z}$ liczb całkowitych. Działania te są łączne i przemienne. Również łączne i przemienne są działania dodawania i mnożenia w zbiorze $\mathbb{Q}$ liczb wymiernych oraz w zbiorze $\mathbb{R}$ liczb rzeczywistych. Działanie $\triangleright : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ dane wzorem $a \triangleright b = 2a + b$ nie jest ani łączne ani przemienne. Na przykład $1 \triangleright 2 = 4 \neq 5 = 2 \triangleright 1$. Oraz $1 \triangleright (2 \triangleright 3) = 2 + (2 \triangleright 3) = 2 + (4 + 3) = 9$, a $(1 \triangleright 2) \triangleright 3 = (2 + 2) \triangleright 3 = 8 + 3 = 11$. Działania $- : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ i $:: \mathbb{R}_{>0} \times \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0}$ odejmowania liczb rzeczywistych i dzielenia dodatnich liczb rzeczywistych nie są ani przemienne ani łączne. Działanie $\triangle: \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ dane wzorem $x \triangle y = \frac{x+y}{2}$ jest przemienne ale nie jest łączne. $\Diamond$

U w a g a. Łączność działania jest w pewnym sensie bardziej podstawową jego własnością niż przemienność. Jeżeli dane działanie $*$ jest łączne, to można jednoznacznie zdefiniować wartość "iloczynu" trzech czynników $\alpha * \beta * \gamma$ jako $\alpha * (\beta * \gamma)$ lub $(\alpha * \beta) * \gamma$. Podobnie ma się rzecz z "iloczynem" $\alpha_1 * \alpha_2 * \ldots * \alpha_n$, gdzie tylko porządek α_i jest istotny. W szczególności, gdy wszystkie α_i są równe α dostajemy n-tą "potęgę" α^n. Prawidłowo należy ją określić indukcyjnie ($\alpha^1 = \alpha$ i $\alpha^{n+1} = \alpha^n * \alpha$) i zapisywać jakoś tak: α^{*n}.

Ćwiczenie 1.5 Niech X będzie dowolnym zbiorem niepustym i niech $\mathcal{B}ij(X)$ oznacza zbiór wszystkich bijekcji zbioru X na zbiór X. W zbiorze $\mathcal{B}ij(X)$ określamy działanie **składania**: Jeżeli f, $g \in \mathcal{B}ij(X)$, to $f \circ g$ jest zdefiniowane przez $(f \circ g)(x) = f(g(x))$ dla każdego $x \in X$. Udowodnić, że w ten sposób z d e f i n i o w a l i ś m y działanie i że jest ono ł ą c z n e, ale (gdy $|X| > 2$) n i e j e s t p r z e m i e n n e.

Definicja 1.3 Jeżeli w pewnym zbiorze B zadane są dwa działania $\wedge$ i $\vee$, to mówimy, że działanie $\vee$ jest **rozdzielne względem działania** $\wedge$, gdy

$$u \vee (v \wedge w) = (u \vee v) \wedge (u \vee w) \tag{1.5}$$

dla dowolnych u, v, $w \in B$.

P r z y k ł a d 2. Działanie mnożenia liczb jest rozdzielne względem działania dodawania liczb (to znaczy, że $a \cdot (b + c) = a \cdot b + a \cdot c$ dla dowolnych liczb a, b, c).

Ćwiczenie 1.6 W zbiorze $\mathcal{P}(X)$ wszystkich podzbiorów danego zbioru X znane są działania $\cap$ **przekroju** czyli **iloczynu teoriomnogościowego** oraz $\cup$ **sumy teoriomnogościowej**. Uzasadnić, że każde z nich jest rozdzielne względem drugiego.

Definicja 1.4 Element $\varepsilon \in A$ nazywamy **elementem neutralnym** działania $*$ w zbiorze A, gdy dla dowolnego $\alpha \in A$ zachodzą równości:

$$\varepsilon * \alpha = \alpha * \varepsilon = \alpha. \tag{1.6}$$

P r z y k ł a d 3. Jasne, że liczba 0 jest elementem neutralnym dodawania liczb (naturalnych, całkowitych, wymiernych, rzeczywistych), liczba 1 jest elementem neutralnym mnożenia liczb. Zbiór pusty $\varnothing \in \mathcal{P}(X)$ jest elementem neutralnym sumy teoriomnogościowej, zbiór "pełny" $X \in \mathcal{P}(X)$ jest elementem neutralnym iloczynu teoriomnogościowego w $\mathcal{P}(X)$. $\Diamond$

Ćwiczenie 1.7 Udowodnić, że działanie ma c o n a j w y ż e j jeden element neutralny.

1.3 Grupa

Wprowadzimy teraz bardzo ważne pojęcie grupy.

Definicja 1.5 Zbiór Γ wraz z działaniem $* : \Gamma \times \Gamma \longrightarrow \Gamma$ nazywamy **grupą**, gdy spełnione są następujące prawa:

(1) działanie $*$ jest łączne, tzn. $\alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma$ dla wszystkich $\alpha, \beta, \gamma \in \Gamma$,

(2) działanie $*$ ma element neutralny ε, tzn. $\alpha * \varepsilon = \varepsilon * \alpha = \alpha$ dla wszystkich $\alpha \in \Gamma$,

(3) dla każdego $\alpha \in \Gamma$ istnieje taki element $\widetilde{\alpha} \in \Gamma$, że $\alpha * \widetilde{\alpha} = \widetilde{\alpha} * \alpha = \varepsilon$.

Ćwiczenie 1.8 Jeżeli $\alpha \in \Gamma$, to element $\widetilde{\alpha}$, którego istnienie zapewnia punkt (3), nazywa się **elementem odwrotnym** do α lub **odwrotnością** α. Udowodnić, że dany element grupy ma dokładnie jedną odwrotność. Oznaczamy ją α^{-1}.

Ćwiczenie 1.9 Udowodnić, że odwrotność odwrotności danego elementu równa jest temu elementowi: $(\alpha^{-1})^{-1} = \alpha$.

Ćwiczenie 1.10 Dowieść, że jeśli α, β są elementami grupy, to $(\alpha * \beta)^{-1} = \beta^{-1} * \alpha^{-1}$.

U w a g a. Gdy zadanym działaniem $*$ w grupie jest **dodawanie** oznaczane symbolem $+$, to mówimy, że ta grupa jest grupą **typu addytywnego**. W takim przypadku element neutralny ε nazywa się **zerem** i zazwyczaj oznacza symbolem 0, element odwrotny do α nazywa się **elementem przeciwnym** do α, i oznacza symbolem $-\alpha$. Równości z aksjomatów D1.5(1), D1.5(2) i D1.5(3) w tym przypadku mają postać:

(1) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$,

(2) $0 + \alpha = \alpha + 0 = \alpha$,

(3) $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$.

Definicja 1.6 Jeżeli $(\Gamma, *)$ jest grupą i działanie $*$ jest przemienne, to grupę $(\Gamma, *)$ nazywamy **grupą przemienną**, czyli **komutatywną** lub **grupą abelową**.

Ćwiczenie 1.11 Sprawdzić, że następujące zbiory ze wskazanymi działaniami są grupami abelowymi: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\{+1, -1\}, \cdot)$, $(\mathbb{R}_{>0}, \cdot)$.

P r z y k ł a d. Najważniejszy przykład grupy spotykamy w ćwiczeniu C1.5. Odwrotnością bijekcji $f \in \mathcal{B}ij(X)$ jest, oczywiście, bijekcja odwrona f^{-1}. Elementem neutralnym zaś jest **identyczność** na X, oznaczana zazwyczaj Id_X. Grupa $(\mathcal{B}ij(X), \circ)$ nazywa się **grupą bijekcji** zbioru X. Grupa ta jest grupą abelową wyłącznie w przypadku, gdy $|X| \leqslant 2$. W przypadku gdy X jest zbiorem skończonym i zawiera n elementów, na przykład $X = \{1, 2, \ldots, n\}$, zbiór $\mathcal{B}ij(X)$ oznaczamy symbolem S_n, jego elementy nazywamy **permutacjami**, a samą grupę $(S_n, \circ)$ nazywamy n-tą **grupą symetryczną**. Ponieważ element $\sigma \in S_n$ jest funkcją określoną na zbiorze $[\,n\,] := \{1, 2, \ldots, n\}$, więc zadajemy ją wypisując w jednej linii elementy zbioru $[\,n\,]$ a tuż pod nimi ich obrazy:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

Zbiór S_n ma $n!$ (*silnia*) elementów. $\Diamond$

Ćwiczenie 1.12 Niech $\sigma, \tau \in S_7$ będą zadane przez

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 1 & 2 & 4 & 5 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 6 & 1 & 3 & 2 & 4 \end{pmatrix}.$$

Wyznaczyć następujące elementy grupy S_7: $\sigma \circ \tau$, $\tau \circ \sigma$, σ^4, τ^{-1}, $\sigma^{-3} := (\sigma^{-1})^3$.

Ćwiczenie 1.13 Niech α będzie elementem grupy $(\Gamma, *)$. Niech funkcja $f_\alpha : \Gamma \longrightarrow \Gamma$ będzie zadana przez $f_\alpha(\xi) = \alpha * \xi$. Dowieść, że f_α jest bijekcją zbioru Γ. Dowieść też, że

$$f_\alpha \circ f_\beta = f_{\alpha * \beta}, \quad \text{oraz} \quad (f_\alpha)^{-1} = f_{\alpha^{-1}}$$

dla dowolnych $\alpha, \beta \in \Gamma$.

1.4 Pierścień przemienny. Ciało

Pierścienie, jakie występują w dużych ilościach w elementarnej teorii liczb, należą do klasy pierścieni przemiennych z jedynką.

Definicja 1.7 Zbiór $\mathcal{R}$ wraz z dwoma działaniami: $+$ zwanym **dodawaniem** i $\cdot$ zwanym **mnożeniem** i dwoma wyróżnionymi elementami: 0 zwanym **elementem zerowym** lub **zerem**, i 1 zwanym **jedynką**, nazywa się **pierścieniem przemiennym z jedynką**, gdy

(1) $(\mathcal{R}, +)$ jest grupą abelową z elementem neutralnym 0,

(2) mnożenie $\cdot$ jest rozdzielne względem dodawania $+$,

(3) mnożenie $\cdot$ jest łączne i przemienne,

(4) jedynka 1 jest elementem neutralnym mnożenia.

P r z y k ł a d 1. Znane nam przykłady pierścieni (przemiennych z jedynką):

- **pierścień liczb całkowitych** $(\mathbb{Z}, +, \cdot, 0, 1)$,
- **pierścień liczb wymiernych** $(\mathbb{Q}, +, \cdot, 0, 1)$,
- **pierścień liczb rzeczywistych** $(\mathbb{R}, +, \cdot, 0, 1)$. $\Diamond$

ZADANIE 1.6 Udowodnić, że w każdym pierścieniu zachodzą równości

$$\textbf{(1)} \quad \alpha \cdot 0 = 0, \qquad \textbf{(2)} \quad (-\alpha) \cdot (-\beta) = \alpha \cdot \beta.$$

R o z w i ą z a n i e. (1) Mamy

$$\alpha \cdot 0 + \alpha \cdot 0 = \alpha \cdot (0 + 0) = \alpha \cdot 0.$$

Pierwsza z tych równości wynika z rozdzielności mnożenia względem dodawania, druga z faktu, że 0 jest elementem neutralnym dodawania. Dodajmy teraz $-(\alpha \cdot 0)$ do lewej strony tej równości:

$$-(\alpha \cdot 0) + [\alpha \cdot 0 + \alpha \cdot 0] = [-(\alpha \cdot 0) + \alpha \cdot 0] + \alpha \cdot 0 = 0 + \alpha \cdot 0 = \alpha \cdot 0.$$

Dodając ten sam element $-(\alpha \cdot 0)$ do prawej strony dostajemy 0. W ten sposób równość (1) jest udowodniona. Dla sprawdzenia równości (2), zauważmy, że:

$$(-\alpha) \cdot \beta + \alpha \cdot \beta = (-\alpha + \alpha) \cdot \beta = 0 \cdot \beta = \beta \cdot 0 = 0.$$

Widzimy stąd, że $(-\alpha) \cdot \beta$ jest elementem przeciwnym do $\alpha \cdot \beta$. Zatem

$$(-\alpha) \cdot (-\beta) = -(\alpha \cdot (-\beta)) = -((-\beta) \cdot \alpha) = -(-(\beta \cdot \alpha)) = \beta \cdot \alpha = \alpha \cdot \beta.$$

Takiego typu proste manipulacje z aksjomatami pierścienia w dalszym ciągu będziemy pozostawiali Czytelnikowi. $\Diamond$

U w a g a. Gdy α jest elementem pierścienia $\mathcal{R}$ i n jest liczbą całkowitą, to definiujemy $n\alpha \in \mathcal{R}$ następująco: $0\alpha = 0$, $1\alpha = \alpha$, $(n+1)\alpha = n\alpha + \alpha$ dla $n \in \mathbb{N}$, oraz $n\alpha = -(-n)\alpha$, gdy $n < 0$.

Ćwiczenie 1.14 Niech α, β będą dowolnymi elementami pierścienia. Udowodnić szczegółowo (przez indukcję), że dla $m, n \in \mathbb{Z}$ prawdziwe są równości: **(1)** $n(m\alpha) = (nm)\alpha$, **(2)** $(n+m)\alpha = n\alpha + m\alpha$, **(3)** $n(\alpha + \beta) = n\alpha + n\beta$, **(4)** $(n\alpha) \cdot \beta = \alpha \cdot n\beta = n(\alpha \cdot \beta)$.

Ćwiczenie 1.15 Niech α będzie elementem pierścienia. Zdefiniować przez indukcję n-tą potęgę, α^n dla wykładnika naturalnego n. Następnie udowodnić przez indukcję, że $(\alpha^m)^n = \alpha^{mn}$ dla dowolnych $m, n \in \mathbb{N}$.

Ćwiczenie 1.16 Udowodnić przez indukcję, że dla dowolnych elementów α, β pierścienia p r z e m i e n n e g o i dowolnej liczby $n \in \mathbb{N}$ zachodzą równości (piszemy $\varphi\psi$ zamiast $\varphi \cdot \psi$):

$$(\alpha + \beta)^n = \alpha^n + \binom{n}{1}\alpha^{n-1}\beta + \ldots + \binom{n}{n-1}\alpha\beta^{n-1} + \beta^n, \tag{1.7}$$

$$\alpha^n - \beta^n = (\alpha - \beta)(\alpha^{n-1} + \alpha^{n-2}\beta + \ldots + \alpha\beta^{n-2} + \beta^{n-1}). \tag{1.8}$$

Definicja 1.8 Element $\eta \in \mathcal{R}$ danego pierścienia $\mathcal{R}$ nazywamy **elementem odwracalnym** lub **jednością**, gdy istnieje taki element $\xi \in \mathcal{R}$, że $\eta\xi = 1$. W takiej sytuacji element ξ nazywamy **odwrotnością** η i oznaczamy $\xi = \eta^{-1}$. Zbiór wszystkich elementów odwracalnych pierścienia $\mathcal{R}$ oznaczamy symbolem $\mathcal{R}^*$.

Ćwiczenie 1.17 Udowodnić, że jeżeli $\mathcal{R}$ jest pierścieniem przemiennym z jedynką, to zbiór $\mathcal{R}^*$ z działaniem $\cdot$ jest grupą abelową, zwaną **grupą jedności pierścienia** $\mathcal{R}$.

Ćwiczenie 1.18 Wyznaczyć grupy jedności pierścieni $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

Definicja 1.9 Element α pierścienia $\mathcal{R}$ nazywamy **dzielnikiem zera**, gdy $\alpha \neq 0$ i istnieje taki różny od zera element $\beta \in \mathcal{R}$, że $\alpha\beta = 0$. Pierścień nie zawierający żadnych dzielników zera nazywa się **dziedziną całkowitości**. W dziedzinach całkowitości (zwanych też **pierścieniami bez dzielników zera**) zachodzi więc prawo: $\boxed{\alpha\beta = 0 \Rightarrow \alpha = 0 \ \textit{lub} \ \beta = 0.}$

Poznamy teraz definicję ciała:

Definicja 1.10 Pierścień przemienny z jedynką nazywa się **ciałem**, gdy każdy jego różny od zera element jest odwracalny. Jeżeli α jest niezerowym elementem ciała, to jego odwrotność oznaczamy α^{-1} lub $\frac{1}{\alpha}$. Konsekwentnie piszemy również $\frac{\alpha}{\beta}$ zamiast $\alpha\beta^{-1}$.

Przykład. Z ćwiczenia C1.18 widzimy, że pierścienie $\mathbb{Q}$ i $\mathbb{R}$ są ciałami. $\Diamond$

Ćwiczenie 1.19 Udowodnić, że ciało jest dziedziną całkowitości.

Ćwiczenie 1.20 Udowodnić, że skończona dziedzina całkowitości jest ciałem.

1.5 Liczby zespolone

Matematyka w żaden sposób nie potrafi obejść się bez liczb zespolonych. Również matematyka "olimpijska" wyraźnie kuleje bez tych liczb. Należy więc przyswoić sobie podstawową wiedzę ich dotyczącą. Im wcześniej tym lepiej.

Liczby rzeczywiste utożsamiamy z punktami prostej – **osi liczbowej**. Podobnie, liczby zespolone utożsamimy z punktami płaszczyzny.

Definicja 1.11 Napis postaci $a + bi$, gdzie $a, b \in \mathbb{R}$ nazywamy **liczbą zespoloną**. Zbiór liczb zespolonych oznaczamy symbolem $\mathbb{C}$. W zbiorze tym wykonujemy działania **dodawania** i **mnożenia** następująco:

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \tag{1.9}$$

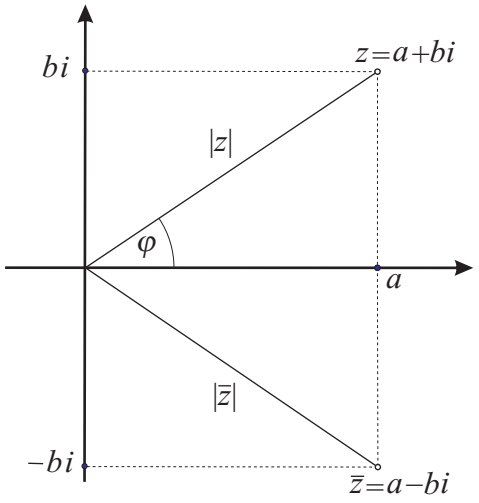
$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i. \tag{1.10}$$

Dodawanie i mnożenie liczb zespolonych jest łatwe: mówi o tym reguła:

rób to co w szkole pamiętając, że $i^2 = -1$.

Wygodnym jest utożsamiać liczbę zespoloną $z = a + bi$ z punktem płaszczyzny o współrzędnych kartezjańskich (a, b). W takiej sytuacji odciętą a nazywamy **częścią rzeczywistą** liczby z i oznaczamy $a = \operatorname{Re} z$, a rzędną b nazywamy **częścią urojoną** liczby z i oznaczamy $b = \operatorname{Im} z$. Utożsamiamy też liczbę rzeczywistą a z liczbą zespoloną $a + 0i$. W ten sposób traktujemy zbiór $\mathbb{R}$ liczb rzeczywistych jako podzbiór zbioru liczb zespolonych $\mathbb{C}$.

Geometrycznie, $\mathbb{R}$ pokrywa się z osią odciętych, zwaną w tym kontekście **osią rzeczywistą**. Oś rzędnych nazywamy wtedy **osią urojoną**. Liczby zespolone leżące na osi urojonej nazywa się **liczbami czysto urojonymi**.



Rys. 1.2

Niech $z = a + bi$ będzie liczbą zespoloną. Kładziemy:

$$\overline{z} = a - bi, \qquad |z| = \sqrt{a^2 + b^2}.$$

Liczbę $\overline{z}$ nazywamy liczbą **sprzężoną** do z; z geometrycznego punktu widzenia, $\overline{z}$ jest odbiciem punktu z w osi rzeczywistej. Liczba rzeczywista $|z|$ nazywa się **modułem** liczby z; oznacza ona odległość punktu (a, b) od początku układu współrzędnych.

Ćwiczenie 1.21 Sprawdzić, że $z + \overline{z} = 2 \operatorname{Re} z$ i $z - \overline{z} = 2i \operatorname{Im} z$ dla dowolnej liczby zespolonej z.

Ćwiczenie 1.22 Udowodnić tożsamości:

$$\textbf{(1)}\quad \overline{z + w} = \overline{z} + \overline{w}, \qquad \textbf{(2)}\quad \overline{z \cdot w} = \overline{z} \cdot \overline{w}, \tag{1.11}$$

$$\textbf{(3)}\quad z \cdot \overline{z} = |z|^2, \qquad \textbf{(4)}\quad |z \cdot w| = |z| \cdot |w|. \tag{1.12}$$

Ćwiczenie 1.23 Dowieść i podać interpretację geometryczną następującej **nierówności trójkąta**: $|z + w| \leqslant |z| + |w|$ dla dowolnych $z, w \in \mathbb{C}$. *Wskazówka.* Rysunek 1.3*a*.

Ćwiczenie 1.24 Sprawdzić, że jeżeli $z = a + bi \neq 0$, to liczba

$$z^{-1} := \frac{a}{|z|^2} + \frac{-b}{|z|^2} i = \frac{\overline{z}}{|z|^2}$$

jest **odwrotnością** liczby z w tym sensie, że $z \cdot z^{-1} = z^{-1} \cdot z = 1$.

Fakt, że każda niezerowa liczba zespolona z ma odwrotność z^{-1} (oznaczaną też oczywiście $\frac{1}{z}$) pokazuje, że w zbiorze $\mathbb{C}$ wykonalne jest **dzielenie** liczb (nie przez zero!). W praktyce dzielenie polega na mnożeniu licznika i mianownika przez liczbę sprzężoną do mianownika:

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}\, i.$$

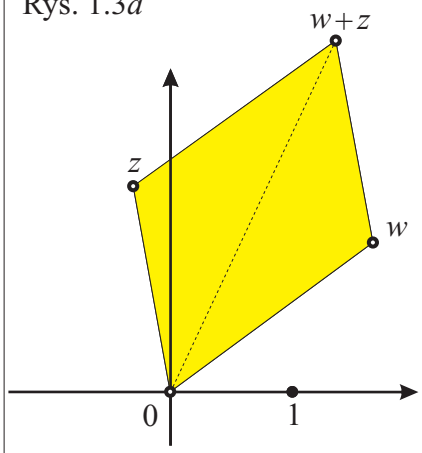
Ćwiczenie 1.25 Uzasadnić, że $|z/w| = |z|/|w|$. Oraz, że niezerowa liczba $z \in \mathbb{C}$ ma moduł równy 1 wtedy i tylko wtedy, gdy $z^{-1} = \overline{z}$.

Ćwiczenie 1.26 Niech $z = 2 + 3i$, $w = 4 - i$. Narysować z, $\overline{z}$, $z + w$, z^2, zw, $\overline{z}^3 w^{-2}$ i zbiór $\{kz + lw : k, l \in \mathbb{Z}\}$.

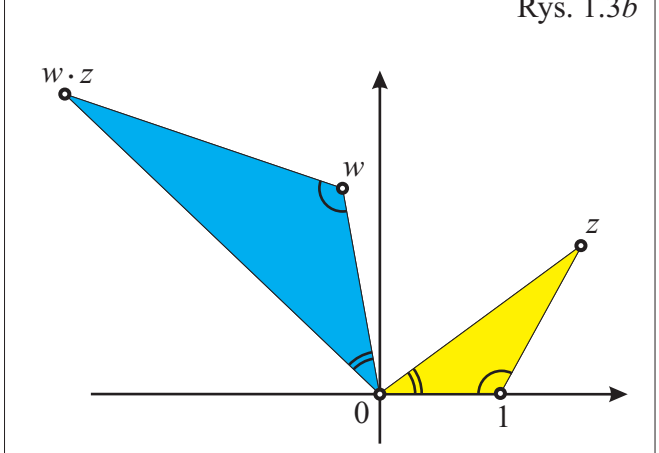
Ćwiczenie 1.27 Udowodnić, że zbiór $\mathbb{C}$ wraz z wprowadzonymi działaniami dodawania i mnożenia jest ciałem. W szczególności w $\mathbb{C}$ nie ma dzielników zera. To znaczy, że jeżeli $zw = 0$, to $z = 0$ lub $w = 0$, porównaj D1.9.

Chcemy teraz zobaczyć geometryczną interpretację dodawania i mnożenia liczb zespolonych.

Rys. 1.3*a*



Rys. 1.3*b*



Z formuły (1.9) łatwo wywnioskować, że punkt płaszczyzny odpowiadający sumie $w + z$ jest jednoznacznie wyznaczony przez warunek: *punkty odpowiadające liczbom* 0, w, $w + z$, z *są wierzchołkami równoległoboku*, zobacz rysunek 1.3*a*. Widzimy stąd i z **zasady równoległoboku** dodawania wektorów, że przekształcenie $A_w : z \longmapsto w + z$ polegające na dodawaniu ustalonej liczby zespolonej w do zmiennej liczby z jest, z geometrycznego punktu widzenia, **translacją**, która przesuwa punkt 0 w punkt w.

Aby zobaczyć interpretację geometryczną mnożenia liczb zespolonych użyjemy **współrzędnych biegunowych** (r, φ) niezerowego (tzn. różnego od początku układu) punktu (a, b), który utożsamiamy z liczbą zespoloną $z = a + bi$. Tutaj $r = |z|$ jest modułem liczby z, zaś φ jest miarą kąta między dodatnią częścią osi rzeczywistej i półprostą h_{0z}. Kąt ten nazywamy **argumentem** liczby z i oznaczamy $\operatorname{Arg} z$. Liczbę φ definiujemy z dokładnością do 2π. Jeżeli $\operatorname{Arg} z = \varphi$, to, z elementarnej trygonometrii, mamy (porównaj rysunek 1.2):

$$z = |z| \cos \varphi + i|z| \sin \varphi = |z|(\cos \varphi + i \sin \varphi). \tag{1.13}$$

Taki zapis nazywamy **postacią trygonometryczną** liczby zespolonej z.

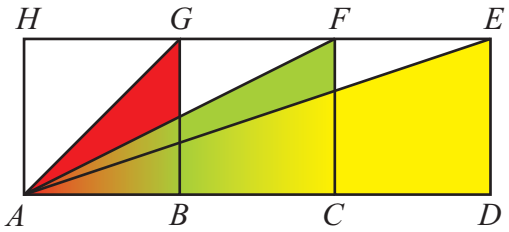
Pomnóżmy dwie liczby zespolone zadane w postaci trygonometrycznej:

$$\begin{aligned}|z|(\cos\varphi + i\sin\varphi)\cdot|w|(\cos\psi + i\sin\psi)\\ &= |z|\cdot|w|\left[(\cos\varphi\cos\psi - \sin\varphi\sin\psi) + i(\cos\varphi\sin\psi + \sin\varphi\cos\psi)\right]\\ &= |zw|\left[\cos(\varphi+\psi) + i\sin(\varphi+\psi)\right].\end{aligned}$$

Ostatnia równość wynika z drugiej tożsamości (1.12) i z elementarnej trygonometrii, zobacz $\mathbb{GEO}$ T2.29. Wnioskujemy stąd, że zachodzi następująca r e g u ł a m n o ż e n i a:

mnożąc liczby zespolone mnożymy ich moduły i dodajemy ich argumenty.

Używając tej reguły z łatwością rozwiążemy ćwiczenie:



Rys. 1.4

Ćwiczenie 1.28 Niech $ABGH$, $BCFG$ i $CDEF$ będą kwadratami, zobacz rysunek 1.4. Wykazać, że suma miar kątów: $\sphericalangle DAE$, $\sphericalangle CAF$, $\sphericalangle BAG$ jest równa 90°. *Wskazówka.* Pomnożyć: $(3+i)(2+i)(1+i)$.

Z reguły mnożenia widzimy, że przekształcenie $M_w : z \longmapsto wz$, tzn. mnożenie przez ustaloną niezerową liczbę zespoloną w jest, z geometrycznego punktu widzenia, złożeniem $J_0^\lambda \circ R_0^\varphi$ dwóch przekształceń płaszczyzny: **obrotu** wokół punktu $0=(0,0)$ o kąt $\varphi = \operatorname{Arg} w$, i **jednokładności** o środku 0 i skali $\lambda = |w|$. Zobacz rysunek 1.3*b*, gdzie widać dwa podobne trójkąty $\triangle(0)(1)(z)$ i $\triangle(0)(w)(zw) = M_w(\triangle(0)(1)(z))$. W szczególności, mnożenie przez i jest obrotem wokół 0 o kąt prosty (przeciwnie do ruchu wskazówek zegara). Podobnie, mnożenie przez $-i$ jest obrotem o kąt prosty, tym razem zgodnie z ruchem wskazówek zegara.

Innym wnioskiem z reguły mnożenia jest ***wzór de Moivre'a***

$$(\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi. \tag{1.14}$$

W następnych trzech ćwiczeniach widzimy sympatyczne zastosowania wzoru de Moivre'*a*:

Ćwiczenie 1.29 Przedstawić w postaci $a+bi$ liczby: $(1+i)^{2011}$, $(1+\sqrt{3}\,i)^{2010}$.

Ćwiczenie 1.30 Zapisać w postaci $a+bi$: $(1+i\operatorname{tg}\varphi)^n$, $(1+\cos\varphi+i\sin\varphi)^n$.

Ćwiczenie 1.31 Używając wzoru dwumiennego (zobacz (1.7)) i wzoru de Moivre'*a* udowodnić, że dla dowolnego $x\in\mathbb{R}$ zachodzą równości

$$\begin{aligned}\sin 3x &= -4\sin^3 x + 3\sin x\\ \cos 5x &= 16\cos^5 x - 20\cos^3 x + 5\cos x.\end{aligned}$$

Wnioskiem z reguły mnożenia jest fakt, że dla liczby zespolonej $w = |w|(\cos\varphi + i\sin\varphi)$, $w \neq 0$, istnieje d o k ł a d n i e n **pierwiastków n-tego stopnia z liczby** w:

$$\boxed{z_k = \sqrt[n]{|w|}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right).} \tag{1.15}$$

Należy tak długo przyglądać się liczbom z_k, aż stanie się jasne, że tworzą wierzchołki pewnego n-kąta foremnego i każda z nich spełnia warunek $z_k^n = w$. Patrz rysunek 1.5*a*.

Ćwiczenie 1.32 Udowodnić, że jeżeli $az^2 + bz + c = 0$ dla pewnych liczb zespolonych $a \neq 0$, b, c, to

$$z = \frac{-b + \sqrt{\Delta}}{2a},$$

gdzie $\sqrt{\Delta}$ oznacza jeden z pierwiastków stopnia drugiego z liczby $\Delta := b^2 - 4ac$.

Ćwiczenie 1.33 Uzasadnić, że każdy pierwiastek równania kwadratowego

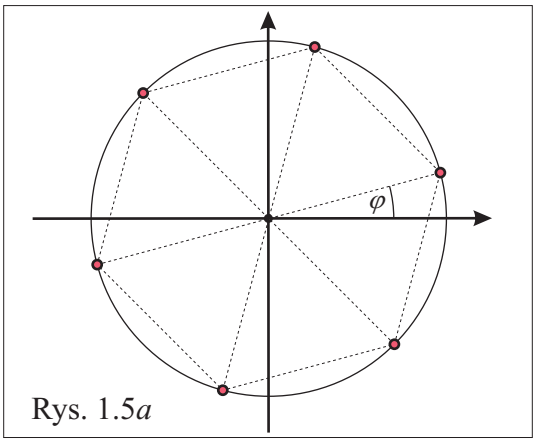
$$z^2 - 2(\cos\varphi)z + 1 = 0,$$

przy dowolnym parametrze $\varphi \in \mathbb{R}$, jest liczbą zespoloną o module 1.

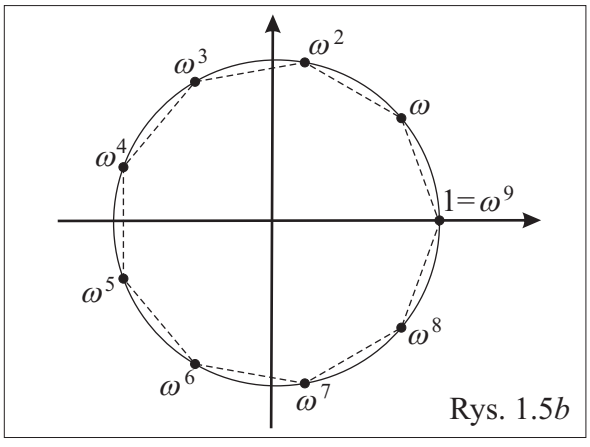
Ćwiczenie 1.34 Narysować 6-elementowy zbiór pierwiastków stopnia 6 z liczby i. *Wskazówka.* Zaznaczony na rysunku 1.5*a* kąt φ ma miarę $\pi/12$.

Szczególnie sympatycznym jest zbiór wszystkich pierwiastków n-tego stopnia z liczby 1.

Ćwiczenie 1.35 Udowodnić, że zbiór $\mu_n(\mathbb{C})$ wszystkich pierwiastków stopnia n z 1 jest grupą względem mnożenia.



Rys. 1.5*a*



Rys. 1.5*b*

Ćwiczenie 1.36 Udowodnić, że grupa $(\mu_n(\mathbb{C}), \cdot)$ jest grupą cykliczną (grupę Γ nazywamy **grupą cykliczną**, gdy istnieje taki element $\omega \in \Gamma$, że zachodzi równość zbiorów $\Gamma = \{\omega^n : n \in \mathbb{Z}\}$). Patrz rysunek 1.5*b*, gdzie pokazano przypadek $n = 9$.

Liczby zespolone, dzięki swojej "budowie" pozwalają zgrabnie uzasadniać tożsamości trygonometryczne, zobacz na przykład C1.31. Inny przykład widzimy w rozwiązaniu kolejnego zadania:

ZADANIE 1.7 Udowodnić, że dla dowolnego $x \neq 2l\pi$ zachodzi równość

$$\frac{1}{2} + \sum_{k=1}^{N} \cos kx = \frac{\sin(N+\frac{1}{2})x}{2\sin\frac{x}{2}}.$$

Rozwiązanie. Weźmy liczbę zespoloną $z = \cos x + i\sin x$ i niech $w = \cos\frac{x}{2} + i\sin\frac{x}{2}$ będzie (jednym z dwóch) pierwiastkiem kwadratowym z liczby z. Dzięki wzorowi de Moivre'*a* wiemy, że rozważana suma jest częścią rzeczywistą liczby

$$\frac{1}{2}\sum_{k=-N}^{N} z^k = \frac{1}{2}z^{-N}\sum_{k=0}^{2N} z^k = \frac{1}{2}z^{-N}\frac{z^{2N+1}-1}{z-1} = \frac{w(z^{N+1}w^{-1} - z^{-N}w^{-1})}{2w(zw^{-1}-w^{-1})},$$

czyli liczby

$$\frac{w^{2N+1} - \overline{w^{2N+1}}}{2(w-\overline{w})} = \frac{2i\sin(2N+1)\frac{x}{2}}{2\cdot 2i\sin\frac{x}{2}}.$$

Radzimy Czytelnikowi tak długo sprawdzać napisane równości, aż wszystko będzie dla niego całkowicie jasne. ◊

Ćwiczenie 1.37 Udowodnić, że dla każdego $x \neq 2l\pi$ zachodzi równość

$$\sum_{k=0}^{N} \sin kx = \frac{\sin\frac{Nx}{2}\,\sin\frac{(N+1)x}{2}}{\sin\frac{x}{2}}.$$

Liczby zespolone są też wygodnym narzędziem w planimetrii. Wynika to z prostoty zapisywania obrotów. Widzieliśmy to w C1.28, zobaczymy i teraz, patrz też $\mathbb{GEO}$:

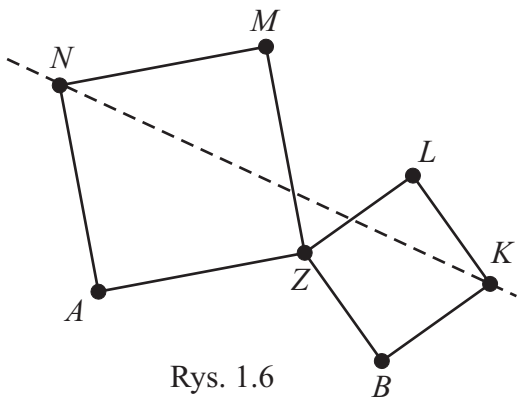
ZADANIE 1.8 (***Zadanie o zakopanym skarbie.***) Na płaszczyźnie dane są ustalone dwa punkty A, B i zmienny punkt Z. Niech $ZBKL$ i $AZMN$ będą dwoma kwadratami zorientowanymi przeciwnie do ruchu wskazówek zegara. Udowodnić, że wszystkie proste l_{NK} przechodzą przez ten sam punkt (są współpękowe).

Rozwiązanie. Po utożsamieniu płaszczyzny, w której leżą te kwadraty z płaszczyzną zespoloną, będziemy uważać wszystkie występujące w zadaniu punkty za liczby zespolone. Wówczas

$$N = A + i(Z-A), \quad K = B - i(Z-B).$$

Wobec tego środek odcinka $\overline{NK}$ utożsamiamy z liczbą zespoloną

$$\frac{N+K}{2} = \frac{A+B+i(B-A)}{2}.$$

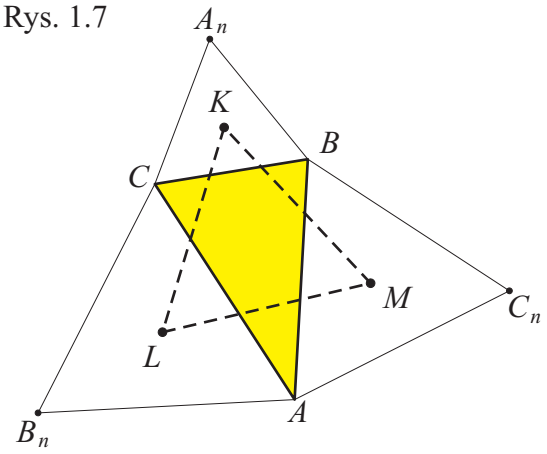


Rys. 1.6

Widzimy więc, że środek odcinka $\overline{NK}$ nie zależy od wyboru punktu Z i przez ten środek przechodzą (oczywiście) wszystkie proste l_{NK}. ◊

ZADANIE 1.9 (***Zadanie o trójkątach Napoleona***) Na zewnątrz danego trójkąta $\triangle ABC$, na jego bokach, zbudowano trójkąty równoboczne $\triangle BCA_n$, $\triangle CAB_n$ i $\triangle ABC_n$. Udowodnić, że środki ciężkości tych trójkątów są wierzchołkami trójkąta równobocznego.

Rys. 1.7



Rozwiązanie. Podobnie jak wyżej, utożsamiamy punkty płaszczyzny z liczbami zespolonymi. Oznaczmy $\omega = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$. Mnożenie przez ω jest więc obrotem o kąt 60°. Wobec tego, patrz rysunek 1.7,

$$A_n = C + \omega(B - C), \tag{1.16}$$
$$B_n = A + \omega(C - A), \tag{1.17}$$
$$C_n = B + \omega(A - B). \tag{1.18}$$

Chcemy zaś uzasadnić, że zachodzi równość

$$\omega(L - K) = M - K. \tag{1.19}$$

Ponieważ środek ciężkości K jest średnią arytmetyczną odpowiednich wierzchołków, więc, na mocy równości (1.16), $3K = A_n + B + C = (1+\omega)B + (2-\omega)C$. Podobnie, z równości (1.17) i (1.18) dostajemy $3L = (1+\omega)C + (2-\omega)A$ i $3M = (1+\omega)A + (2-\omega)B$. Korzystając z tych równości i (łatwej do zobaczenia – sprawdzić!) równości $\omega^2 + 1 = \omega$, po prostych rachunkach, dostaniemy równość $\omega(3L - 3K) = 3M - 3K$, czyli (1.19). $\Diamond$

Rozdział 2

Elementarz

Euclid, whose fame rests on the portion of his E l e m e n t s
that forms the foundation of g e o m e t r y studied in high school,
seems to have made original contributions to n u m b e r t h e o r y,
while his geometry was largely a compilation of previous results.
(Richard Courant)

W tym rozdziale przedstawiamy podstawowe pojęcia i twierdzenia elementarnej teorii liczb. Najważniejsze idee pochodzą zapewne od E u k l i d e s a.

2.1 Największy wspólny dzielnik w pierścieniu $\mathbb{Z}$

W tym paragrafie zbieramy i systematyzujemy wstępne wiadomości o podzielności liczb całkowitych. Przekonamy się, że najważniejszym narzędziem służącym do badania podzielności liczb całkowitych jest tak zwane d z i e l e n i e z r e s z t ą, zobacz twierdzenie T2.2. Z twierdzenia tego wynikają kolejno wnioski:

- ✓ każdy ideał w $\mathbb{Z}$ jest ideałem głównym, zobacz T2.3,
- ✓ każde dwie (niezerowe) liczby całkowite mają NWD , zobacz T2.4,
- ✓ NWD da się przedstawić w postaci kombinacji liniowej, zobacz T2.6,
- ✓ prawdziwe jest Zasadnicze Twierdzenie Arytmetyki, zobacz T2.7,
- ✓ każde dwie (niezerowe) liczby całkowite mają NWW , zobacz T2.8.

Paragraf zakończymy prezentacją algorytmu Euklidesa, który redukuje (beznadziejnie trudne w szkole) zadanie wyznaczania NWD do kilku prostych dzieleń z resztą.

2.1.1 Podzielność i dzielenie z resztą w $\mathbb{Z}$

Zaczynamy od podstawowej definicji. Zwróćmy uwagę, że w tej definicji n i e występują ułamki.

Definicja 2.1 Niech a, b będą liczbami całkowitymi. Mówimy, że a **dzieli** b, gdy istnieje taka liczba $q \in \mathbb{Z}$, że $b = a \cdot q$. Zapisujemy to tak: $a|b$. Mówimy również w takiej sytuacji, że b jest **wielokrotnością** a, lub że a jest **dzielnikiem** b.

Podstawowe własności **relacji podzielności** w pierścieniu liczb całkowitych $\mathbb{Z}$ zawarte są w naszym pierwszym twierdzeniu.

TWIERDZENIE 2.1 *Dla dowolnych liczb całkowitych* a, b, c, d *zachodzą:*

(1) $a|a,\ 1|a,\ (-1)|a,\ a|0,$

(2) *jeżeli* $a|b$ *i* $b|c,$ *to* $a|c,$

(3) *jeżeli* $a|b$ *i* $b|a,$ *to* $a = \pm b,$

(4) *jeżeli* $a|b$ *i* $a|c,$ *to* $a|b \pm c$ *i* $a|bd,$

(5) *jeżeli* $a^k|b^k,$ *dla* $k \geqslant 1,$ *to* $a|b.$ □

Ćwiczenie 2.1 Udowodnić prawdziwość wszystkich, z wyjątkiem ostatniej, tez.

Ćwiczenie 2.2 Uzasadnić szczegółowo, że jeżeli $a|b$ i $b \neq 0,$ to $|a| \leqslant |b|$.

Jeden wniosek z tezy T2.1(4) jest tak c z ę s t o wykorzystywany w rozumowaniach, że stosujemy go w dalszym ciągu prawie "mimochodem", czasami nazywając ***Zasadą Podstawową***:

ZASADA PODSTAWOWA *Jeżeli* a_i, x_i, b_j, y_j *oraz* c *są liczbami całkowitymi i*

$$a_1x_1 + a_2x_2 + \ \ldots\ + a_nx_n = b_1y_1 + b_2y_2 + \ \ldots\ + b_my_m + c,$$

a wszystkie liczby a_i, b_j *są podzielne przez daną liczbę całkowitą* $d,$ *to* $d|c.$

P r z y k ł a d. Udowodnimy, że liczba $A_n = 5^{2n} + 1$ jest, dla każdej liczby naturalnej n, podzielna przez 2, ale nie jest podzielna przez 4. Rzeczywiście, wzór dwumienny daje:

$$A_n = \left(5^2\right)^n + 1 = (1 + 8 \cdot 3)^n + 1 = 1 + \sum_{k=1}^{n} \binom{n}{k} 8^k \cdot 3^k + 1 = 2 + \sum_{k=1}^{n} \binom{n}{k} 8^k \cdot 3^k,$$

skąd $2|A_n$. Gdyby $4|A_n,$ to, na mocy Zasady Podstawowej, mielibyśmy $4|2$. ◊

Oznaczmy przez $D(a)$ zbiór wszystkich dzielników liczby całkowitej a. Jasne, że $D(0) = \mathbb{Z}$. Jeżeli a, b są liczbami całkowitymi, to oznaczmy

$$D(a, b) = D(a) \cap D(b).$$

Zbiór $D(a, b)$ jest więc po prostu zbiorem wszystkich **wspólnych dzielników** liczb a i b. Na przykład, ponieważ

$$D(-30) = \{\pm1, \pm2, \pm3, \pm5, \pm6, \pm10, \pm15, \pm30\} \quad \text{i} \quad D(21) = \{\pm1, \pm3, \pm7, \pm21\},$$

więc $D(-30, 21) = \{-1,\ +1,\ -3,\ +3\}$.

Zauważmy, że zbiór $D(a,\ b)$ jest zbiorem nieskończonym w jednym tylko przypadku: gdy $a = b = 0$. W każdym innym przypadku jest to zbiór n i e p u s t y (jeżeli $a \neq 0,$ to $a \in D(a,\ b)$, zob. T2.1(1)) i s k o ń c z o n y (jeżeli $a \neq 0,$ to $D(a,\ b) \subseteq [\,-|a|;\ |a|\,]$, zob. C2.2), a jego największy element (istniejący na mocy zasady maksimum) nazywa się (w szkole) największym wspólnym dzielnikiem liczb całkowitych a i b.

Arcyważnym narzędziem w teorii liczb całkowitych jest **dzielenie z resztą**.

TWIERDZENIE 2.2 (***Dzielenie z resztą w*** $\mathbb{Z}$) *Jeżeli* $a, b \in \mathbb{Z}$ *i* $b \neq 0$, *to istnieje dokładnie jedna taka para liczb* $q, r \in \mathbb{Z}$, *że*

$$\boxed{a = qb + r \quad oraz \quad 0 \leqslant r < |b|.} \tag{2.1}$$

D O W Ó D. Rozważmy zbiór $X = \{a - xb : x \in \mathbb{Z},\, a - xb \geqslant 0\}$. Zbiór ten jest niepusty (dlaczego?). Niech $r = a - qb$ będzie najmniejszą liczbą zbioru X. Jasne, że $0 \leqslant r < |b|$. W ten sposób uzasadniliśmy i s t n i e n i e liczb q i r. Załóżmy teraz, że pary (q_1, r_1) i (q_2, r_2) spełniają narzucone warunki. Wtedy $a = q_1 b + r_1 = q_2 b + r_2$. Stąd $(q_1 - q_2)b = r_2 - r_1$, więc $|q_1 - q_2| \cdot |b| = |r_2 - r_1|$. Ale $|r_2 - r_1| < |b|$, bo $0 \leqslant r_1, r_2 < |b|$. Wobec tego $|q_1 - q_2| = 0$. Zatem $q_1 = q_2$, a więc i $r_1 = r_2$. Widzimy zatem j e d y n o ś ć liczb q, r. □

Liczba q nazywa się (niepełnym) **ilorazem**, a liczba r, **resztą** z dzielenia a przez b. Możliwymi resztami z dzielenia liczb całkowitych przez daną liczbę naturalną m są liczby

$$0, 1, 2, \ldots, m - 1.$$

Ten układ liczb nazywa się **standardowym zupełnym układem reszt modulo** m.

Ćwiczenie 2.3 Niech $n \in \mathbb{Z}$ będzie liczbą nieparzystą. Wyznaczyć resztę z dzielenia liczby $3n^3 + 2n^2 + n - 1$ przez 8.

Ćwiczenie 2.4 Wyznaczyć resztę z dzielenia liczby $2^{2009} + 1$ przez 7.

2.1.2 Ideały w pierścieniu $\mathbb{Z}$

Ideały w zbiorze (pierścieniu) liczb całkowitych $\mathbb{Z}$ grają ważną rolę przy badaniu relacji podzielności w tym zbiorze.

Definicja 2.2 Podzbiór $I \subseteq \mathbb{Z}$ nazywamy **ideałem**, gdy zawiera liczbę 0 oraz spełnia poniższe dwa warunki:

(1) jeżeli $a \in I$ i $b \in I$, to $a + b \in I$,

(2) jeżeli $k \in \mathbb{Z}$ i $a \in I$, to $ka \in I$.

P r z y k ł a d. Ustalmy dowolną liczbę całkowitą a. Zbiór

$$(a) := \{ka : k \in \mathbb{Z}\} = \{\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots\}$$

wszystkich wielokrotności liczby a jest ideałem. Warunek (1) mówi bowiem po prostu, że suma dwóch wielokrotności liczby a jest wielokrotnością liczby a: $ka + la = (k + l)a$. Zaś warunek (2) mówi, że wielokrotność wielokrotności liczby a jest wielokrotnością liczby a: $k(la) = (kl)a$. Zauważmy, że jeżeli $a, b \in I$, to $a - b = a + (-1)b \in I$. Zauważmy wreszcie, że $(1) = (-1) = \mathbb{Z}$ oraz $(0) = \{0\}$. Ideał (0) nazywamy **ideałem zerowym**. ◊

Definicja 2.3 Ideał (a) nazywa się **ideałem głównym** generowanym przez a, zaś samą liczbę a nazywamy **generatorem** tego ideału.

Ćwiczenie 2.5 Dowieść, że dla dowolnych liczb całkowitych a, b:

$$a|b \iff (b) \subseteq (a).$$

Teza ćwiczenia C2.5 pozwala zastępować relację podzielności liczb relacją inkluzji ideałów. W szczególności, $(a) = (b)$ wtedy i tylko wtedy, gdy $a = \pm b$, zobacz T2.1(3).

Ćwiczenie 2.6 Udowodnić, że przekrój (= część wspólna = iloczyn teoriomnogościowy) dowolnej rodziny ideałów jest ideałem.

Ćwiczenie 2.7 Udowodnić, że jeżeli zawierający 0 podzbiór zbioru $\mathbb{Z}$ spełnia warunek (1) definicji D2.2, to jest on ideałem. *Wskazówka.* Udowodnić przez indukcję, że jeżeli $a \in I$, to $na \in I$ dla każdego $n \in \mathbb{N}$.

Niech dane będą dwie liczby całkowite a, b. Zdefiniujemy zbiór

$$(a, b) := \{ax + by : x, y \in \mathbb{Z}\}. \tag{2.2}$$

Element $ax+by$ tego zbioru nazywamy **kombinacją liniową** liczb a i b. Kombinacja liniowa jest więc po prostu sumą pewnej wielokrotności liczby a i pewnej wielokrotności liczby b. Zbiór (a, b) nazywamy **ideałem generowanym przez liczby** a, b. Możemy używać takiej terminologii, bowiem:

Ćwiczenie 2.8 Dowieść, że zbiór (a, b) jest ideałem.

Najważniejszym wnioskiem z możliwości dzielenia z resztą w pierścieniu liczb całkowitych $\mathbb{Z}$ jest fakt, że k a ż d y ideał w tym pierścieniu jest zbiorem wielokrotności pewnej liczby, czyli jest ideałem głównym. Rozumowanie, które prowadzi do tego wniosku, jest laboratoryjnie czystym przykładem pięknego kawałka matematyki olimpijskiej.

TWIERDZENIE 2.3 *Jeżeli $I \subseteq \mathbb{Z}$ jest ideałem, to istnieje jedyna taka liczba całkowita nieujemna d, że $I = (d) := \{qd : q \in \mathbb{Z}\}$.*

D O W Ó D. Jeżeli ideał I jest ideałem zerowym, czyli zawiera tylko jeden element 0, to $I = (0)$. Jeżeli nie jest ideałem zerowym, to zawiera jakąś liczbę $b \neq 0$ i wtedy zawiera też liczby dodatnie (bo zawiera liczby b i $-b = (-1) \cdot b$, a któraś z nich jest dodatnia). Niech d będzie n a j m n i e j s z ą d o d a t n i ą liczbą w zbiorze I. Taka liczba istnieje na mocy Zasady Minimum. Pokażemy, że każda liczba $a \in I$ jest wielokrotnością d. Podzielmy w tym celu a przez d z resztą:

$$a = qd + r, \qquad 0 \leqslant r < d.$$

Wówczas $r = a - qd \in I$, bo $a \in I$ i $qd \in I$. Ale d jest najmniejszą dodatnią liczbą w zbiorze I, a $0 \leqslant r < d$, stąd $r = 0$, czyli $a = qd$. Wykazaliśmy w ten sposób, że $I \subseteq (d)$. Ponieważ zawieranie $(d) \subseteq I$ jest oczywiste, więc $I = (d)$. □

U w a g a. Twierdzenie T2.3 może być (i zazwyczaj jest) wyrażone tak: *pierścień $\mathbb{Z}$ liczb całkowitych jest* ***dziedziną ideałów głównych*** (skrót: **dig**).

Ćwiczenie 2.9 Dane są dowolne liczby całkowite $a_1, a_2, \ldots, a_n$. Udowodnić, że zbiór

$$(a_1, a_2, \ldots, a_n) := \{a_1x_1 + a_2x_2 + \ldots + a_nx_n : x_1, x_2, \ldots, x_n \in \mathbb{Z}\}$$

jest n a j m n i e j s z y m ideałem zawierającym liczby $a_1, a_2, \ldots, a_n$. Nazywamy go **ideałem generowanym** przez te liczby.

2.1.3 Największy wspólny dzielnik

Najważniejszym pojęciem elementarnej teorii liczb jest pojęcie największego wspólnego dzielnika. Przyjęta niżej (zobacz D2.4) definicja tego pojęcia jest, jak się okaże, równoważna, ze wspomnianą w ustępie 2.1.1, definicją szkolną.

Definicja 2.4 Załóżmy, że a, b są, nie równymi jednocześnie 0, liczbami całkowitymi. Liczbę naturalną d nazywamy **największym wspólnym dzielnikiem** liczb a i b, gdy

(1) $d \in D(a, b)$ (d jest wspólnym dzielnikiem),

(2) jeżeli $e \in D(a, b)$, to $e|d$ (d jest wielokrotnością każdego wspólnego dzielnika).

Łatwo widzieć, że co najwyżej jedna liczba dodatnia d spełnia powyższe warunki: gdyby d_1 też je spełniała, to $d_1|d$ i $d|d_1$, skąd $d = d_1$. Udowodnimy więc teraz, że dla dowolnych dwóch niezerowych liczb całkowitych istnieje ich największy wspólny dzielnik.

TWIERDZENIE 2.4 *Dla dowolnych, nie równych jednocześnie* 0*, liczb całkowitych* a, b *istnieje największy wspólny dzielnik liczb* a, b*.*

DOWÓD. Rozważmy ideał (a, b) generowany przez liczby a, b, zobacz (2.2). Ponieważ każdy ideał w $\mathbb{Z}$ jest główny, zobacz T2.3, więc istnieje taka liczba dodatnia d, że

$$(a, b) = (d).$$

Sprawdzamy, że tak wyznaczona liczba d spełnia warunki D2.4(1) i D2.4(2):

(1) Ponieważ $a \in (a, b)$ (bo $a = a \cdot 1 + b \cdot 0$), a $(a, b) = (d)$, więc $a \in (d)$, czyli $d|a$. Podobnie sprawdzamy, że $d|b$.

(2) Ponieważ $d \in (d) = (a, b)$, a zbiór (a, b) składa się ze wszystkich kombinacji liniowych $ax + by$, więc

$$d = ax_0 + by_0 \tag{2.3}$$

dla pewnych $x_0, y_0 \in \mathbb{Z}$. Niech teraz $e|a$ i $e|b$ dla pewnej liczby całkowitej e. Wtedy $a = ke$ i $b = le$, skąd, dzięki (2.3), $d = (ke)x_0 + (le)y_0 = e(kx_0 + ly_0)$. Więc $e|d$. □

Widzimy więc, że dokładnie jedna liczba naturalna d spełnia warunki (1), (2) definicji D2.4. Tę, jednoznacznie wyznaczoną, liczbę oznaczamy symbolem

$$\mathrm{NWD}\,(a, b).$$

Łatwo sprawdzić, że jest to ta sama liczba, którą tak nazywaliśmy w szkole. Mianowicie:

TWIERDZENIE 2.5 *Jeżeli* a, b *są, nie równymi jednocześnie* 0*, liczbami całkowitymi, to* $\mathrm{NWD}\,(a, b)$ *jest największą liczbą w zbiorze* $D(a, b)$ *wspólnych dzielników liczb* a *i* b*.*

DOWÓD. Niech $d = \mathrm{NWD}\,(a, b)$ i niech d_1 oznacza największą liczbę w $D(a, b)$. Wtedy $d \leqslant d_1$, bo d_1 jest największy. Jednocześnie $d_1|a$ i $d_1|b$ (bo d_1 jest wspólnym dzielnikiem), więc $d_1|d$ (bo d spełnia warunek D2.4(2)). Zatem, zob. C2.2, $d_1 \leqslant d$. Przeto $d_1 = d$. □

Definicja 2.5 Jeżeli $\mathrm{NWD}\,(a,\,b)=1,$ to mówimy, że liczby $a,\,b$ są **względnie pierwsze**. Piszemy też $a\perp b$ dla wskazania, że liczby $a,\,b$ są względnie pierwsze.

Liczby całkowite $a,\,b$ są więc względnie pierwsze wtedy i tylko wtedy, gdy 1 jest ich j e d y n y m w s p ó l n y m dzielnikiem dodatnim.

Ćwiczenie 2.10 Udowodnić, że dla dowolnych liczb całkowitych $a,\,b$ zachodzi

$$\mathrm{NWD}\,(a,\,a+b)|b.$$

Wywnioskować stąd, że dwie kolejne liczby całkowite są względnie pierwsze.

Ćwiczenie 2.11 Wybrano $n+1$ liczb ze zbioru $\{1,\,2,\,3,\,\ldots,\,2n\}$. Udowodnić, że znajdą się wśród nich dwie liczby względnie pierwsze. (***Zagadka Erdősa***)

ZADANIE 2.1 Udowodnić, że jeśli $n,\,m\in\mathbb{N}$ i m jest nieparzysta, to

$$\mathrm{NWD}\,(2^m-1,\,2^n+1)=1.$$

R o z w i ą z a n i e. Niech $d=\mathrm{NWD}\,(2^m-1,\,2^n+1)$. Wtedy d jest liczbą nieparzystą(!) i mamy $2^m-1=dx,\,2^n+1=dy$ dla pewnych liczb naturalnych $x,\,y$. Na mocy wzoru dwumiennego mamy

$$2^{mn}=(dx+1)^n=du+1\quad\text{i}\quad 2^{nm}=(dy-1)^m=dv-1, \tag{2.4}$$

gdzie

$$u=\sum_{k=0}^{n-1}\binom{n}{k}d^{n-k-1}x^{n-k},\quad v=\sum_{l=0}^{m-1}\binom{m}{l}(-1)^l d^{m-l-1}y^{m-l}.$$

Dzięki równościom (2.4) mamy $du+1=dv-1$. Stąd $2=d(v-u)$. Więc $d=1$. $\lozenge$

ZADANIE 2.2 Liczby $F_n=2^{2^n}+1$, dla $n\in\mathbb{Z}_{\geq 0}$, nazywamy **liczbami Fermat'a**. Udowodnić ***Twierdzenie Goldbacha***: *Dwie różne liczby Fermat'*a *są względnie pierwsze.*

R o z w i ą z a n i e. Niech $n=m+r$ i $r>0$. Wówczas mamy

$$F_n=2^{2^n}+1=2^{2^{m+r}}+1=(2^{2^m})^{2^r}+1=(F_m-1)^{2^r}+1.$$

Na mocy wzoru dwumiennego, podobnie jak w poprzednim zadaniu, dostajemy więc

$$F_n=(F_m-1)^{2^r}+1=(A\cdot F_m+1)+1=A\cdot F_m+2$$

przy pewnym $A\in\mathbb{N}$. Z otrzymanej równości $F_n=AF_m+2,$ na mocy Zasady Podstawowej, wnosimy, że każdy wspólny dzielnik liczb F_n i F_m jest dzielnikiem 2. Ponieważ jednak liczby Fermat'*a* są nieparzyste, więc jedynym dodatnim wspólnym dzielnikiem F_n i F_m jest 1. $\lozenge$

Fakt, że największy wspólny dzielnik dwóch liczb całkowitych $a,\,b$ da się przedstawić w postaci kombinacji liniowej $ax+by$ tych liczb, jest tak ważny, że zapiszemy go jeszcze raz:

TWIERDZENIE 2.6 (***Twierdzenie Gaussa-Bézout'a***) *Dla niezerowych liczb całkowitych* a, b *istnieją liczby całkowite* x, y, *dla których*

$$\boxed{\text{NWD}\,(a,\,b) = ax + by.} \tag{2.5}$$

W szczególności: $a \perp b$ *wtedy i tylko wtedy, gdy* $ax + by = 1$ *dla pewnych* $x,\, y \in \mathbb{Z}$. □

Kolejne cztery ćwiczenia rozwiązuje się bardzo łatwo korzystając z przedstawienia największego wspólnego dzielnika w postaci (2.5):

Ćwiczenie 2.12 Jeżeli d jest największym wspólnym dzielnikiem a, b oraz $a = da'$ i $b = db'$, to $\text{NWD}\,(a',\, b') = 1$.

Ćwiczenie 2.13 Jeżeli $\text{NWD}\,(a,\, b) = 1$ oraz $c|a$, to $\text{NWD}\,(c,\, b) = 1$.

Ćwiczenie 2.14 Jeżeli $\text{NWD}\,(a,\, b) = \text{NWD}\,(c,\, b) = 1$, to $\text{NWD}\,(ac,\, b) = 1$.

Ćwiczenie 2.15 Udowodnić przez indukcję względem n, $m \geqslant 0$, że jeżeli liczby całkowite a, b są względnie pierwsze, to $\text{NWD}\,(a^n,\, b^m) = 1$ dla dowolnych n, $m \in \mathbb{Z}_{\geq 0}$.

Można również mówić o największym wspólnym dzielniku dowolnych układów liczb:

Ćwiczenie 2.16 Zdefiniować $\text{NWD}\,(a_1,\, a_2,\, \ldots,\, a_s)$ i wykazać, że jest on równy (z dokładnością do znaku) generatorowi ideału $(a_1,\, a_2,\, \ldots,\, a_s)$, zobacz też C2.9.

2.1.4 Zasadnicze Twierdzenie Arytmetyki

Jesteśmy teraz w stanie udowodnić tak zwane ***Zasadnicze Twierdzenie Arytmetyki*, ZTA**. Niektórzy nazywają je również twierdzeniem Gaussa, chociaż poprawniej powinno się je nazywać twierdzeniem Euklidesa – znajduje się bowiem w jego "Elementach".

TWIERDZENIE 2.7 (**ZTA**) *Niech* a, b *i* c *będą liczbami całkowitymi. Wówczas*:

$$\boxed{\textit{Jeżeli}\ \ a|bc\ \ \textit{i}\ \ \text{NWD}\,(a,\, b) = 1,\ \ \textit{to}\ \ a|c.}$$

D O W Ó D. Założenie $a \perp b$ daje, jak wiemy, równość $1 = ax+by$, przy pewnych x, $y \in \mathbb{Z}$. Mnożąc tę równość obustronnie przez c, otrzymamy $c = acx + bcy = acx + aky = a(cx + ky)$, gdzie druga równość wynika z założenia, że $bc = ak$ dla pewnego $k \in \mathbb{Z}$. Zatem $a|c$. □

Teza kolejnego ćwiczenia jest b a r d z o w a ż n a.

Ćwiczenie 2.17 Jeżeli liczby całkowite a, b są względnie pierwsze i $a|c$ i $b|c$, to $ab|c$.

ZADANIE 2.3 Udowodnić prawdziwość tezy T2.1(5).

Rozwiązanie. Niech $b^k = ca^k$. Oznaczmy $d = \mathrm{NWD}\,(a, b)$ i $a = da'$, $b = db'$. Mamy więc $d^k(b')^k = cd^k(a')^k$, skąd $(b')^k = c(a')^k$. Z C2.12 wiemy, że $\mathrm{NWD}\,(a', b') = 1$, więc z C2.15, $\mathrm{NWD}\,((a')^k, (b')^k) = 1$. Stąd i z równości $1 \cdot (b')^k = c(a')^k$, dzięki ZTA, widzimy, że $(a')^k|1$. Zatem $(a')^k = \pm 1$, czyli $a' = \pm 1$. Ostatecznie, $a = \pm d$, więc $a|b$. ◊

Następne zadanie pokazuje efektywną metodę znajdowania wszystkich wymiernych pierwiastków wielomianów o współczynnikach całkowitych.

ZADANIE 2.4 Jeżeli liczba wymierna $\frac{h}{k}$ dana w postaci **ułamka nieskracalnego** (to znaczy takiego, że $\mathrm{NWD}\,(h, k) = 1$) jest pierwiastkiem wielomianu

$$f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

o współczynnikach całkowitych, to $k|a_n$, a $h|a_0$.

Rozwiązanie. Jeżeli $f(\frac{h}{k}) = 0$, to, po wymnożeniu przez k^n, dostajemy równość

$$a_0k^n + a_1k^{n-1}h + a_2k^{n-2}h^2 + \ldots + a_{n-1}kh^{n-1} + a_nh^n = 0.$$

Z tej równości, dzięki Zasadzie Podstawowej, wnosimy, że $h|a_0k^n$ oraz $k|a_nh^n$. Wiedząc z C2.15, że $\mathrm{NWD}\,(h, k^n) = 1$ oraz $\mathrm{NWD}\,(k, h^n) = 1$, wnioskujemy, dzięki ZTA, że $h|a_0$ oraz $k|a_n$. To kończy rozwiązanie. ◊

Ćwiczenie 2.18 Udowodnić, że liczba wymierna ma tylko jedno, z dokładnością do znaku licznika i mianownika, przedstawienie w postaci ułamka nieskracalnego.

Ćwiczenie 2.19 Udowodnić, że jeżeli przy naturalnym n, dana liczba całkowita jest n-tą potęgą liczby wymiernej, to jest też n-tą potęgą liczby całkowitej.

2.1.5 Najmniejsza wspólna wielokrotność

Czasami używamy również najmniejszej wspólnej wielokrotności dwóch (lub większej liczby) liczb całkowitych. Podamy definicję tego pojęcia dualną do definicji D2.4.

Definicja 2.6 Liczbę naturalną m nazywamy **najmniejszą wspólną wielokrotnością** niezerowych liczb całkowitych a i b, gdy

(1) $a|m$ i $b|m$ (m jest wspólną wielokrotnością),

(2) jeżeli $a|n$ i $b|n$, to $m|n$ (m jest dzielnikiem każdej wspólnej wielokrotności).

Łatwo sprawdzić, że co najwyżej jedna liczba naturalna m spełnia powyższe dwa warunki. Jeszcze łatwiej sprawdzić, że dla dowolnych dwóch niezerowych liczb całkowitych a, b istnieje ich najmniejsza wspólna wielokrotność, oznaczana $\mathrm{NWW}\,(a, b)$:

TWIERDZENIE 2.8 *Jeżeli $a, b \neq 0$ są liczbami całkowitymi i zachodzi równość*

$$(a) \cap (b) = (m), \tag{2.6}$$

to liczba $|m|$ jest najmniejszą wspólną wielokrotnością liczb a, b.

D O W Ó D. Ćwiczenie dla Czytelnika. Porównać C2.6. □

Ciekawą i ważną własność NWD i NWW podaje:

TWIERDZENIE 2.9 *Dla dowolnych liczb naturalnych* a, b *zachodzi równość:*

$$\mathrm{NWD}\,(a,\,b)\cdot\mathrm{NWW}\,(a,\,b)=ab.$$

D O W Ó D. Niech $d=\mathrm{NWD}\,(a,\,b)$ i niech $a=a'd$ i $b=b'd$. Wówczas, jak wiemy, $\mathrm{NWD}\,(a',\,b')=1$. Pokażemy, że liczba $m:=\frac{ab}{d}=a'b=ab'$ spełnia warunek D2.6(2) (bo warunek D2.6(1), oczywiście, spełnia). Niech więc $a|n$ i $b|n$ dla pewnej liczby całkowitej n. Mamy zatem dla pewnych $k,\,l\in\mathbb{Z}$

$$n=ak=bl. \tag{2.7}$$

Stąd, $ak=bl$, czyli $da'k=db'l$, więc $a'k=b'l$. Ale, $\mathrm{NWD}\,(a',\,b')=1$ i $a'|b'l$, zatem, na mocy ZTA, $a'|l$. Kładąc $l=a's$ mamy, dzięki (2.7), $n=bl=ba's=ms$. □

Ćwiczenie 2.20 Udowodnić, że dla $a,\,b,\,c\in\mathbb{Z}$ zachodzi równość

$$\mathrm{NWW}\,(a,\,\mathrm{NWW}\,(b,\,c))=\mathrm{NWW}\,(\mathrm{NWW}\,(a,\,b),\,c).$$

Ćwiczenie 2.21 Udowodnić, że (na ogół) $\mathrm{NWD}\,(a,\,b,\,c)\cdot\mathrm{NWW}\,(a,\,b,\,c)\neq abc$, ale

$$\mathrm{NWD}\,(ab,\,bc,\,ca)\cdot\mathrm{NWW}\,(a,\,b,\,c)=abc=\mathrm{NWD}\,(a,\,b,\,c)\cdot\mathrm{NWW}\,(ab,\,bc,\,ca).$$

2.1.6 Algorytm Euklidesa

Proste twierdzenie T2.10 leży u podstaw efektywnej metody (czyli **algorytmu**) wyznaczania największego wspólnego dzielnika. Ten, pochodzący od Euklidesa, algorytm jest absolutnie n a j w a ż n i e j s z y m narzędziem rachunkowym (elementarnej) teorii liczb.

TWIERDZENIE 2.10 *Jeżeli dla liczb całkowitych* a, b, q, r *zachodzi równość* $a=qb+r$, *to* $\mathrm{NWD}\,(a,\,b)=\mathrm{NWD}\,(b,\,r)$.

D O W Ó D. Dzięki Zasadzie Podstawowej z łatwością sprawdzamy, że warunek $a=qb+r$ implikuje równość $D(a,\,b)=D(b,\,r)$ zbiorów wspólnych dzielników. Stąd teza. □

TWIERDZENIE 2.11 (***Algorytm Euklidesa wyznaczania*** NWD) *Dane są liczby całkowite* a *i* b, *przy czym* $b\neq 0$. *Wykonujemy kolejne dzielenia z resztą:*

$$\begin{cases} a &= qb+r,\\ b &= q_1r+r_1,\\ r &= q_2r_1+r_2,\\ r_1 &= q_3r_2+r_3,\\ &\dots \end{cases} \tag{2.8}$$

Wówczas ciąg reszt $r,\,r_1,\,r_2,\,\dots$ *jest ściśle malejącym ciągiem liczb całkowitych nieujemnych. Ostatnia n i e z e r o w a reszta równa jest* $\mathrm{NWD}\,(a,\,b)$. □

Ćwiczenie 2.22 Udowodnić twierdzenie T2.11. *Wskazówka.* Ostatnia linijka algorytmu (2.8) ma postać $r_s = q_{s+2}r_{s+1} + 0$. Z niej: $D(r_{s+1}) = D(r_{s+1}, 0) = \cdots = D(a, b)$.

P r z y k ł a d. Ciąg oczywistych równości

$$\begin{array}{rcrcr} 17464 & = & 1 \cdot 9322 & + & 8142 \\ 9322 & = & 1 \cdot 8142 & + & 1180 \\ 8142 & = & 6 \cdot 1180 & + & 1062 \\ 1180 & = & 1 \cdot 1062 & + & 118 \\ 1062 & = & 9 \cdot 118 & + & 0 \end{array} \tag{2.9}$$

pokazuje, że $D(17464, 9322) = D(9322, 8142) = D(8142, 1180) = \ldots = D(1062, 118) = D(118, 0) = D(118)$. Wobec tego mamy: $\mathrm{NWD}\,(17464, 9322) = \mathrm{NWD}\,(9322, 8142) = \cdots = \mathrm{NWD}\,(1062, 118) = \mathrm{NWD}\,(118, 0) = 118$. ◊

Zrobimy trzy w a ż n e u w a g i dotyczące algorytmu Euklidesa:

U w a g a 1. W praktyce, zamiast wykonywać w kolejnej linii algorytmu Euklidesa dzielenie z resztą nieujemną mniejszą niż dzielnik, wygodnie jest "dzielić z resztą ujemną", jeżeli prowadzi to do mniejszych co do wartości bezwzględnej reszt. Poniższy przykład (po porównaniu z (2.9)) pokazuje wyraźnie o co chodzi:

$$\begin{array}{rcrcr} 17464 & = & 2 \cdot 9322 & - & 1\,180 \\ 9322 & = & 8 \cdot 1180 & - & 118 \\ 1180 & = & 10 \cdot 118 & + & 0 \end{array} \tag{2.10}$$

Ćwiczenie 2.23 Wyznaczyć $\mathrm{NWD}\,(234567, 765432)$.

U w a g a 2. W matematyce szkolnej, aby wyznaczyć $\mathrm{NWD}\,(a, b)$, musimy znać rozkłady liczb a, b na czynniki pierwsze. Algorytm Euklidesa pozwala wyznaczyć największy wspólny dzielnik dowolnych dwóch liczb całkowitych bez najmniejszej znajomości ich rozkładów na czynniki pierwsze (można nawet n i e w i e d z i e ć co to jest liczba pierwsza). Na przykład, trzy proste równości (2.10) wystarczają do sprawdzenia, że

$$\mathrm{NWD}\,(17464, 9322) = 118,$$

W matematyce szkolnej tymczasem wymaga się od uczniów uprzedniego rozwiązania (znacznie trudniejszego) zadania rozkładu na czynniki pierwsze:

$$9322 = 2 \cdot 59 \cdot 79, \quad 17464 = 2 \cdot 2 \cdot 2 \cdot 37 \cdot 59.$$

U w a g a 3. Algorytm Euklidesa daje jeszcze więcej: Wiemy, że największy wspólny dzielnik dwóch liczb całkowitych a i b da się zapisać jako kombinacja liniowa $ax+by$ tych liczb, zobacz (2.5). Często chcemy jednak z n a ć k o n k r e t n e x, y (a nie tylko wiedzieć, że takowe istnieją). Otóż, równości (2.8) z algorytmu Euklidesa (czytane od tyłu) dają e f e k t y w n ą (i efektowną!) metodę wyznaczania x i y. Na przykład, dzięki (2.9):

$$\begin{aligned} 118 &= 1180 - 1062 = 1180 - (8142 - 6 \cdot 1180) = -8142 + 7 \cdot 1180 = \\ &= -8142 + 7 \cdot (9322 - 8142) = 7 \cdot 9322 - 8 \cdot 8142 = \\ &= 7 \cdot 9322 - 8 \cdot (17464 - 9322) = 9322 \cdot 15 + 17464 \cdot (-8). \end{aligned}$$

Za pomocą równości (2.10) możemy to zrobić jeszcze szybciej:

$$118 = 8 \cdot 1180 - 9322 = 8 \cdot (2 \cdot 9322 - 17464) - 9322 = 9322 \cdot 15 + 17464 \cdot (-8).$$

2.2 Równanie $ax + by = n$

Niech a, b, n będą dowolnymi liczbami całkowitymi. Możemy teraz podać kompletną teorię równania $ax + by = n$.

2.2.1 Twierdzenie Brahmagupty-Bachet'a

Zajmiemy się najpierw rozwiązaniami równania $ax + by = n$ w liczbach całkowitych x, y.

TWIERDZENIE 2.12 (***Brahmagupta-Bachet***) *Niech a, b, n będą takimi liczbami całkowitymi, że istnieje $d := \mathrm{NWD}\,(a, b)$. Wówczas równanie*

$$ax + by = n \tag{2.11}$$

ma rozwiązania w liczbach całkowitych x, y wtedy i tylko wtedy, gdy $d|n$. Gdy ten warunek jest spełniony, to wszystkie rozwiązania tego równania dane są przez formuły

$$x = \frac{nx_0 - bt}{d}, \qquad y = \frac{ny_0 + at}{d}, \qquad t \in \mathbb{Z}, \tag{2.12}$$

gdzie para (x_0, y_0) jest jakimkolwiek rozwiązaniem równania $ax + by = d$.

DOWÓD. Wobec określenia ideału (a, b), zobacz (2.2), widzimy, że x, $y \in \mathbb{Z}$ spełniające równość $ax + by = n$ istnieją wtedy i tylko wtedy, gdy $n \in (a, b)$, czyli wtedy i tylko wtedy, gdy $n \in (d)$, zobacz dowód T2.4, czyli wtedy i tylko wtedy, gdy $d|n$.

Załóżmy więc, że $d|n$ i oznaczmy $n = dk$, $a = da'$, $b = db'$. Niech x_0, y_0 będą takimi liczbami całkowitymi, że $ax_0 + by_0 = d$. Takie x_0, y_0 istnieją na mocy twierdzenia Gaussa-Bézout'a T2.6 (można je, jak wiemy, wyznaczyć za pomocą algorytmu Euklidesa, zobacz U3 z ustępu 2.1.6). Mnożąc przez k znajdujemy

$$a \cdot kx_0 + b \cdot ky_0 = n. \tag{2.13}$$

Załóżmy teraz, że para (x, y) jest jakimś (całkowitoliczbowym) rozwiązaniem, czyli, że zachodzi równość $ax + by = n$. Odejmując tę równość obustronnie od równości (2.13) i porządkując wyrazy, otrzymamy $a(kx_0 - x) + b(ky_0 - y) = 0$, czyli, po podzieleniu przez d:

$$a'(kx_0 - x) = b'(y - ky_0).$$

Ale, zobacz C2.12, $\mathrm{NWD}\,(a', b') = 1$, więc, na mocy ZTA, $b'|kx_0 - x$, czyli $kx_0 - x = b't$ dla pewnego $t \in \mathbb{Z}$. Stąd $x = kx_0 - b't$. Co daje $y = ky_0 + a't$. Udowodniliśmy więc równości (2.12). Z drugiej strony, sprawdzenie, że para $(kx_0 - b't, ky_0 + a't)$ jest, dla każdego $t \in \mathbb{Z}$, rozwiązaniem równania (2.11), jest natychmiastowe. □

Ćwiczenie 2.24 Rozwiązać w liczbach całkowitych równanie $13x + 21y = 511$.

Ćwiczenie 2.25 Rozwiązać równanie $21x - 9y + 16z = 7$ w $\mathbb{Z}$. *Wskazówka.* Ponieważ $\mathrm{NWD}\,(21, 16) = 1$, więc równanie $21x + 16z = 7 + 9y$ ma rozwiązania dla każdej liczby całkowitej $y \in \mathbb{Z}$.

Ćwiczenie 2.26 Rozwiązać równanie $6x + 15y - 10z = 26$ w $\mathbb{Z}$. *Wskazówka.* Wyznaczyć najpierw wszystkie $z \in \mathbb{Z}$, dla których $3|26 + 10z$.

2.2.2 Twierdzenie Sylvestera

Które liczby dadzą się przedstawić w postaci $ax + by$ z nieujemnymi x, y? Częściowej odpowiedzi udzielił Sylvester.

Załóżmy, że a, b są danymi liczbami naturalnymi. Liczbę całkowitą n nazwiemy *osiągalną*, gdy istnieją takie liczby x, $y \in \mathbb{Z}_{\geqslant 0}$, że $n = ax + by$. Liczba 0 jest, oczywiście, osiągalna, a liczby ujemne są, oczywiście, *nieosiągalne*.

TWIERDZENIE 2.13 (***Twierdzenie Sylvestera***) *Niech* $\mathrm{NWD}\,(a, b) = 1$. *Wówczas*:

(1) *moc zbioru liczb nieosiągalnych jest równa* $\frac{1}{2}(a-1)(b-1)$;

(2) *największą liczbą nieosiągalną jest* $ab - a - b$.

DOWÓD. Załóżmy, że $a < b$ i ustawmy wszystkie liczby całkowite nieujemne w tablicy

$$\begin{array}{ccccccc} 0 & 1 & 2 & \dots & k & \dots & a-1 \\ a & a+1 & a+2 & \dots & a+k & \dots & 2a-1 \\ 2a & 2a+1 & 2a+2 & \dots & 2a+k & \dots & 3a-1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array} \tag{2.14}$$

(1) Każda kolumna tej tablicy jest ciągiem arytmetycznym o różnicy a. Rozważmy liczby

$$0 \cdot b, \quad 1 \cdot b, \quad 2 \cdot b, \quad \dots, \quad (a-1) \cdot b. \tag{2.15}$$

Wszystkie te liczby są, oczywiście, osiągalne i każda z nich stoi w innej kolumnie tablicy (2.14). Gdyby bowiem sb i tb, przy pewnych $0 \leqslant s < t \leqslant a-1$, stały w tej samej kolumnie, to liczba $tb - sb$ byłaby wielokrotnością a, co wobec nierówności $t - s \leqslant a - 1$ jest niemożliwe. Zatem, w każdej z kolumn o "nagłówku" 0, 1, …, $a-1$ stoi dokładnie jedna z liczb (2.15). Oznaczmy przez $y_k b$ liczbę z ciągu (2.15) stojącą w kolumnie o nagłówku k.

Jasne, że wszystkie liczby stojące pod liczbą $y_k b$ w k-tej kolumnie są osiągalne. Natomiast, wszystkie liczby k-tej kolumny stojące nad liczbą $y_k b$ są *nieosiągalne*. Aby to zobaczyć wystarczy (dlaczego?) udowodnić, że liczba stojąca tuż nad $y_k b$, czyli liczba $y_k b - a$, jest nieosiągalna. Załóżmy, nie wprost, że $y_k b - a$ jest osiągalna, czyli że $y_k b - a = ax + by$ dla pewnych x, $y \in \mathbb{Z}_{\geqslant 0}$. Wtedy $b(y_k - y) = a(x+1)$, co, dzięki ZTA i nieujemności x, daje $y_k - y = at > 0$. To jednakże jest niemożliwe, bo $y \geqslant 0$, a $y_k \leqslant a - 1$. Wobec tego liczba liczb nieosiągalnych w k-tej kolumnie wynosi

$$\left\lfloor \frac{y_k b}{a} \right\rfloor = \frac{y_k b - k}{a}.$$

Ostatecznie, moc zbioru liczb nieosiągalnych wynosi

$$\sum_{k=0}^{a-1} \frac{y_k b - k}{a} = \frac{b}{a} \sum_{k=0}^{a-1} y_k - \frac{1}{a} \sum_{k=0}^{a-1} k = \frac{(a-1)(b-1)}{2}.$$

(2) Największa nieosiągalna liczba stoi w pewnej kolumnie tablicy (2.14) tuż nad liczbą $(a-1)b$. Jest to więc liczba $(a-1)b - a$. □

W poniższym zadaniu pokażemy pewien rodzaj *wzajemności* uzupełniający naszą wiedzę na temat liczb osiągalnych (i nieosiągalnych):

ZADANIE 2.5 Niech, jak wyżej, $a, b \in \mathbb{N} > 0$ i $a \perp b$. Udowodnić, że liczba $n \in \mathbb{Z}$ jest osiągalna wtedy i tylko wtedy, gdy liczba $I(n) := ab - a - b - n$ jest nieosiągalna.

R o z w i ą z a n i e. Używamy oznaczeń i założeń z dowodu T2.13. Załóżmy, że liczba n stoi w k-tej kolumnie tablicy (2.14) rozszerzonej w górę do $-\infty$. Wtedy, jak wiemy, $n = y_k b + sa$ dla pewnego $s \in \mathbb{Z}$. Przy czym n jest osiągalna wtedy i tylko wtedy, gdy $s \geqslant 0$. Przy tych oznaczeniach mamy:

$$I(n) = ab - a - b - y_k b - sa = (a - 1 - y_k)b - (s + 1)a = y_l b - (s + 1)a.$$

Liczba $(a - 1 - y_k)b$ jest jedną z liczb ciągu (2.15), bo $0 \leqslant y_k \leqslant a - 1$. Oznaczyliśmy ją więc $y_l b$. Wobec tego $I(n)$ jest nieosiągalna wtedy i tylko wtedy, gdy $-(s + 1) < 0$, czyli wtedy i tylko wtedy, gdy $s \geqslant 0$, czyli wtedy i tylko wtedy, gdy n jest liczbą osiągalną. $\Diamond$

Ćwiczenie 2.27 Wskazać najmniejszą liczbę naturalną dającą się przedstawić na cztery różne sposoby w postaci $5x + 6y$ przy $x, y \in \mathbb{N}$.

Ćwiczenie 2.28 Niech a, b będą względnie pierwszymi liczbami naturalnymi. Udowodnić, że liczba nieujemnych rozwiązań równania $ax + by = n$ równa jest $\left\lfloor \frac{n}{ab} \right\rfloor$ lub $\left\lfloor \frac{n}{ab} \right\rfloor + 1$.

Ćwiczenie 2.29 W pewnej grze można zdobyć a lub b punktów w jednym "rozdaniu" ($a, b \in \mathbb{N}$, $a > b$). Wynik gry po pewnej liczbie rozdań jest sumą zdobytych punktów. Zauważono, że nie można osiągnąć wyniku 58 punktów, oraz że jeszcze dokładnie 34 inne wyniki są w tej grze nieosiągalne. Wyznaczyć a i b.

Ćwiczenie 2.30 Mamy do dyspozycji cegły o wymiarach $6 \times 14 \times 21$. Możemy, kładąc je jedną na drugiej ("leżąco", "na sztorc" i "stojąco"), budować "wieże". Wyznaczyć taką n a j m n i e j s z ą liczbę $G \in \mathbb{N}$, że da się zbudować wieże k a ż d e j wysokości $\geqslant G$.

U w a g a. Frobenius postawił p r o b l e m ogólniejszy: *Dane są względnie pierwsze liczby naturalne $a_1, \ldots, a_k$. Znaleźć taką najmniejszą liczbę całkowitą $G = G(a_1, \ldots, a_k)$, że każdą liczbę całkowitą $m \geqslant G$ można przedstawić w postaci $a_1x_1 + a_2x_2 + \cdots + a_kx_k$, gdzie liczby $x_1, \ldots, x_k$ są całkowite i nieujemne.* Z T2.13(2) wiemy, że $G(a, b) = (a - 1)(b - 1)$. Łatwo(?!) dowieść, że dla dowolnych względnie pierwszych liczb naturalnych $a_1, \ldots, a_k$ **liczba Frobeniusa** $G(a_1, a_2, \ldots, a_k)$ i s t n i e j e.

Ćwiczenie 2.31 Udowodnić, że zachodzi szacowanie $G(a, b, c) \leqslant D + (d-1)(a-1)$, gdzie $d = \mathrm{NWD}\,(b, c)$, $D = d\left(\frac{b}{d} - 1\right)\left(\frac{c}{d} - 1\right)$.

ZADANIE 2.6 Niech $a, b, c \in \mathbb{N}$ i $\mathrm{NWD}\,(a, b) = \mathrm{NWD}\,(b, c) = \mathrm{NWD}\,(c, a) = 1$. Udowodnić, że $G(ab, bc, ca) = 2abc - ab - bc - ca$.

R o z w i ą z a n i e. Niech $bcx + cay + abz = 2abc - ab - bc - ca$ dla pewnych $x, y, z \in \mathbb{Z}_{\geqslant 0}$, czyli $2abc = bc(x+1) + ca(y+1) + ab(z+1)$. Stąd, na mocy Zasady Podstawowej, $a|bc(x+1)$, $b|ca(y + 1)$, $c|ab(z + 1)$. Więc, na mocy ZTA, $a|x + 1$, $b|y + 1$ i $c|z + 1$. Przeto, na mocy C2.2, $a \leqslant x + 1$, $b \leqslant y + 1$ i $c \leqslant z + 1$. Wobec tego $2abc = bc(x + 1) + ca(y + 1) + ab(z + 1) \geqslant bca + cab + abc = 3abc$. Sprzeczność. Niech teraz $m > 2abc - ab - bc - ca$. Weźmy taką j e d y n ą liczbę $z \in \mathbb{Z}$, dla której $c|m - abz$ i $0 \leqslant z < c$ (dla dowodu istnienia takiej liczby z, rozważmy c liczb m, $m - ab$, $m - 2ab$, $\ldots$, $m - (c - 1)ab$ i zauważmy, że każda z nich daje i n n ą resztę z dzielenia przez c). Dla tej liczby z mamy więc $cn := m - abz > 2abc - ab - bc - ca - abz \geqslant 2abc - ab - bc - ca - ab(c - 1) = c(ab - b - a)$. Stąd $n > ab - b - a$, więc, na mocy Z2.5, istnieją $x, y \in \mathbb{Z}_{\geqslant 0}$, dla których $n = bx + ay$. Ostatecznie $m = cn + abz = bcx + cay + abz$. $\Diamond$

2.3 Liczby pierwsze

Liczby pierwsze są elementarnymi cegiełkami, z których zbudowane są (multyplikatywnie) liczby naturalne, zobacz T2.16. To jest podstawowy powód, dla którego interesujemy się nimi.

2.3.1 Istnienie i jednoznaczność rozkładu na czynniki pierwsze

W matematyce szkolnej definiujemy liczbę pierwszą jako taką liczbę naturalną większa od 1, która dzieli się tylko przez 1 i przez samą siebie. Definicja D2.7 jest równoważna z tą szkolną. W praktyce olimpijskiej znacznie częściej używa się c h a r a k t e r y z a c j i liczb pierwszych pokazanej w T2.15.

Definicja 2.7 Liczbę naturalną p nazywamy **liczbą pierwszą**, gdy zbiór $D(p)$ jej dzielników całkowitych ma dokładnie cztery elementy: $D(p) = \{1, -1, p, -p\}$. Zbiór liczb pierwszych oznaczamy symbolem $\mathbb{P}$. Różną od 1 liczbę naturalną nazywamy **liczbą złożoną**, gdy nie jest liczbą pierwszą. (Liczba 1 nie jest ani pierwsza ani złożona!)

Czytelnik powinien bezwzględnie rozwiązać dwa proste ćwiczenia:

Ćwiczenie 2.32 Jeżeli p jest liczbą pierwszą, to, dla danej liczby całkowitej a, albo $p|a$ albo $\mathrm{NWD}\,(p, a) = 1$.

Ćwiczenie 2.33 Udowodnić, że liczba naturalna n jest liczbą złożoną wtedy i tylko wtedy, gdy istnieją takie liczby całkowite a, b, że $1 < a, b < n$ oraz $n = ab$. Równoważnie, wtedy i tylko wtedy, gdy liczba n ma **dzielnik właściwy**, czyli gdy istnieje $a \in D(n)$ spełniające warunek $1 < a < n$.

Możemy teraz naprawić jeden z podstawowych niedostatków matematyki szkolnej: udowodnimy mianowicie twierdzenie o istnieniu i jednoznaczności rozkładu liczb naturalnych na iloczyn liczb pierwszych. W dowodzie i s t n i e n i a rozkładu liczb naturalnych na iloczyn liczb pierwszych wykorzystamy następujące podstawowe:

TWIERDZENIE 2.14 *Każda liczba naturalna $n > 1$ dzieli się przez pewną liczbę pierwszą.*

D O W Ó D. Z a ł ó ż m y, że nie. Wówczas, na mocy Zasady Minimum, istnieje najmniejsza liczba naturalna $n_0 > 1$ nie dzieląca się przez ż a d n ą liczbę pierwszą. Liczba n_0 nie jest liczbą pierwszą, gdyż dzieli się przez siebie. Jest więc liczbą złożoną. Zatem, zobacz C2.33, $n_0 = kl$ dla pewnych $1 < k, l < n_0$. Liczba k, jako mniejsza od n_0, ale większa od 1, ma dzielnik pierwszy p. Ten dzielnik p dzieli również n_0, zobacz T2.1(2). S p r z e c z n o ś ć. □

W dowodzie jednoznaczności rozkładu (i w ogóle w teorii liczb) wykorzystujemy następującą charakteryzację liczb pierwszych:

TWIERDZENIE 2.15 *Liczba naturalna $p \neq 1$ jest liczbą pierwszą w t e d y i t y l k o w t e d y, g d y dla dowolnych liczb całkowitych a, b zachodzi*

$$\boxed{p|ab \implies p|a \quad lub \quad p|b.} \tag{2.16}$$

D O W Ó D. ($\Longrightarrow$) Niech p będzie liczbą pierwszą, niech $p|ab$ i niech $p \nmid a$. Wówczas, na mocy C2.32, $\mathrm{NWD}\,(p,\, a) = 1$, więc, na mocy ZTA, $p|b$.

($\Longleftarrow$) Jeżeli p n i e jest liczbą pierwszą, to, zobacz C2.33, $p = ab$, gdzie $1 < a,\, b < p$. Wtedy $p|ab$, ale $p \nmid a$ i $p \nmid b$. Zatem p n i e spełnia warunku (2.16). □

Ćwiczenie 2.34 Udowodnić przez indukcję, że jeżeli liczba pierwsza p jest dzielnikiem iloczynu $a_1a_2 \cdot \ldots \cdot a_s$ liczb całkowitych, to jest dzielnikiem co najmniej jednego z czynników tego iloczynu.

TWIERDZENIE 2.16 (***Twierdzenie o jednoznaczności rozkładu w*** $\mathbb{N}$) *Każda liczba naturalna $n > 1$ da się w jeden i tylko jeden, z dokładnością do porządku czynników, sposób zapisać w postaci iloczynu liczb pierwszych*

$$n = p_1p_2p_3 \cdot \ldots \cdot p_s. \tag{2.17}$$

D O W Ó D. I s t n i e n i e takiego przedstawienia jest natychmiastowym wnioskiem z zasady minimum i T2.14. Istotnie, załóżmy nie wprost, że istnieją liczby naturalne nie dające się zapisać w postaci (2.17) i oznaczmy przez m najmniejszą taką liczbę. Przedstawiamy ją (dzięki T2.14 wiemy, że jest to możliwe) w postaci iloczynu $m = p_1n$, gdzie p_1 jest liczbą pierwszą, a n liczbą naturalną. Wówczas, jeżeli $n = 1$, to mamy sprzeczność, bo równość $m = p_1$ daje zapis postaci (2.17). Jeżeli zaś $n > 1$, to $n < m$ i, wobec minimalności liczby m, możemy napisać równość $n = p_2 \cdot \ldots \cdot p_s$, gdzie p_i są liczbami pierwszymi. Zatem $m = p_1n = p_1p_2 \cdot \ldots \cdot p_s$. I znowu mamy sprzeczność.

Zajmiemy się teraz j e d n o z n a c z n o ś c i ą. Załóżmy nie wprost, że istnieją liczby naturalne mające istotnie różne rozkłady na iloczyn liczb pierwszych i że m jest najmniejszą taką liczbą:

$$m = p_1p_2 \cdot \ldots \cdot p_s = q_1q_2 \cdot \ldots \cdot q_t. \tag{2.18}$$

Ponieważ $p_1|m$ czyli $p_1|q_1q_2 \cdot \ldots \cdot q_t$ więc, na mocy C2.34, $p_1|q_r$ dla pewnego $1 \leqslant r \leqslant t$. Przenumerowując możemy uznać, że $r = 1$. Jasne, że wówczas $p_1 = q_1$. Ponieważ liczba $\frac{m}{p_1} = \frac{m}{q_1} = p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_t$ jest mniejsza niż m, więc ma tylko jedno, z dokładnością do porządku czynników, przedstawienie w postaci iloczynu liczb pierwszych. Stąd $t = s$ i, po ewentualnym dalszym przenumerowaniu, $p_2 = q_2$, …, $p_s = q_s$. To jest jednakże sprzeczne z założeniem, że rozkłady (2.18) są istotnie różne. □

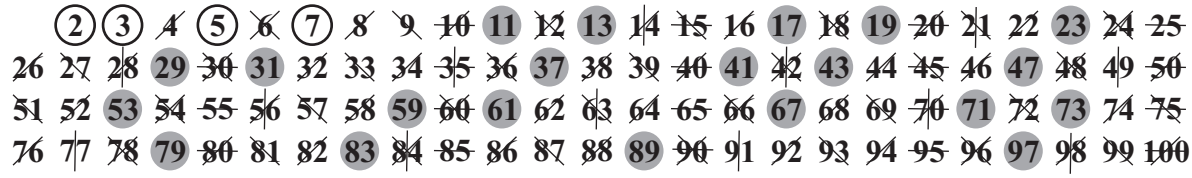
2.3.2 Sito Eratostenesa. Twierdzenie Euklidesa

Z twierdzenia T2.14 wynika, że zbiór $\mathbb{P}$ liczb pierwszych jest n i e p u s t y. Na przykład 2 jest liczbą pierwszą. W tym ustępie pokażemy najpierw metodę (algorytm) wyznaczania w s z y s t k i c h liczb pierwszych niewiększych niż dana liczba $n \in \mathbb{N}$. Następnie udowodnimy (na cztery sposoby), że zbiór $\mathbb{P}$ jest zbiorem nieskończonym.

Już w starożytności wymyślono prosty algorytm wyznaczania wszystkich liczb pierwszych mniejszych niż dana liczba naturalna n. Nazywamy go **sitem Eratostenesa**[1].

[1]Eratostenes nie wymyślił tego sita. Znalazł je w *Elementach* swojego poprzednika na stanowisku "dyrektora" Biblioteki Aleksandryjskiej, Euklidesa. Wyznaczył za to promień Ziemi (zdumiewająco dokładnie), dzięki czemu, korzystając z pomysłów Anaksagorasa i Arystarcha, mógł wyznaczyć promienie Księżyca (wcale dokładnie) i Słońca (ze znacznym błędem), a także odległości Ziemia-Księżyc (całkiem poprawnie) i Ziemia-Słońce (z dwudziestokrotnym błędem).

Polega on na tym, że mając wypisany ciąg kolejnych liczb naturalnych od 2 do n, otaczamy kółkiem liczbę 2, a następnie skreślamy (czysto automatycznie, czyli po prostu co drugą) jej właściwe wielokrotności: 4, 6, 8, itd. Pierwszą nieskreśloną liczbą jest 3. Otaczamy ją kółkiem, a następnie skreślamy jej właściwe wielokrotności 6, 9, 12, itd. Teraz pierwszą nieskreśloną liczbą jest 5 (zobacz rysunek), więc otaczamy ją kółkiem, skreślamy jej właściwe wielokrotności. Itd. Robimy to tak długo dopóki nie natrafimy na pierwszą nieskreśloną liczbę większą niż $\sqrt{n}$. Wówczas liczby otoczone kółkiem i nieskreślone są (wszystkimi!) liczbami pierwszymi z przedziału $[\,2;\,n\,]$.



Ćwiczenie 2.35 Udowodnić, że jeżeli $n > 1$ jest liczbą złożoną, to istnieje taki dzielnik pierwszy p liczby n, że $p \leqslant \sqrt{n}$. Wywnioskować stąd poprawność sita Eratostenesa.

Na powyższym rysunku widzimy jak, po czterech (bo $\sqrt{100} < 11$) krokach, odnaleźliśmy wszystkie dwadzieścia pięć liczb pierwszych $\leqslant 100$. Jednak ciągle jeszcze nie wiemy czy zbiór $\mathbb{P}$ jest skończony czy nie. Mamy więc niespodziankę:

TWIERDZENIE EUKLIDESA *Zbiór $\mathbb{P}$ liczb pierwszych n i e jest zbiorem skończonym.*

P I E R W S Z Y D O W Ó D. (wg. Euklidesa) Załóżmy, że $\mathcal{A} = \{q_1, q_2, \ldots, q_s\} \subseteq \mathbb{P}$ jest s k o ń c z o n y m (niepustym) podzbiorem. Rozważmy liczbę naturalną

$$m = 1 + q_1 q_2 \cdot \ldots \cdot q_s.$$

Liczba ta, jako większa od 1, dzieli się przez jakąś liczbę pierwszą $q \in \mathbb{P}$. Ponieważ żadna liczba pierwsza $q_i \in \mathcal{A}$ nie dzieli m, więc $q \notin \mathcal{A}$. Przeto $\mathcal{A} \neq \mathbb{P}$. Czyli: ż a d e n s k o ń c z o n y zbiór nie jest równy $\mathbb{P}$. [Trudno się nie zachwycić urodą[2] tego rozumowania!] □

D R U G I D O W Ó D. (wg. Goldbacha[3] i Pólya'*i*) Niech q_n oznacza dowolny (na przykład najmniejszy) dzielnik pierwszy n-tej liczby Fermat'*a* F_n, zobacz Z2.2. Względna pierwszość różnych liczb Fermata dowodzi, że $q_n \neq q_m$ dla $n \neq m$. □

T R Z E C I D O W Ó D. (wg. Eulera – szkic) Załóżmy, nie wprost, że $p_1, p_2, \ldots, p_s$ są w s z y s t k i m i liczbami pierwszymi. Wówczas iloczyn

$$\prod_{i=1}^{s} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \frac{1}{p_i^3} + \ldots\right)$$

[2] W pięknej książeczce [**8**] czytamy takie zdanie: *Nie wiadomo, co bardziej podziwiać w tym miejscu u Euklidesa; czy to, że greccy matematycy stawiali sobie w ogóle takie pytania, same dla siebie, z wewnętrznej potrzeby myślenia matematycznego, jakiej nie spotykamy u wcześniejszych narodów i którą też wszystkie późniejsze narody przejęły wprost od Greków; czy to, że postawili sobie właśnie to pytanie, które naiwny obserwator może łatwo przeoczyć, uważać za zbędne, trywialne i którego trudność ten dopiero zauważy, kto starał się bezskutecznie znaleźć w ciągu liczb pierwszych proste prawo, które gwarantowałoby możliwość nieograniczonego posuwania się w tym ciągu naprzód; czy to wreszcie, że umieli oni ominąć brak takiego prawa przez kunsztowny dowód, z którym dopiero co zapoznaliśmy się.*

[3] Christian Goldbach jest najbardziej znany jako autor słynnej (nie udowodnionej do dzisiaj) tak zwanej ***hipotezy Goldbacha***, według której *każda liczba parzysta $\geqslant 4$ jest sumą dwóch liczb pierwszych.*

jest, z jednej strony, równy liczbie $\prod_{i=1}^{s} \frac{1}{1-\frac{1}{p_i}}$, z drugiej zaś (dzięki istnieniu i jednoznaczności rozkładu mianowników n na czynniki pierwsze), $\sum_{n\geqslant 1} \frac{1}{n}$. Ale, zobacz twierdzenie T12.5, $\sum_{n\geqslant 1} \frac{1}{n} = \infty$. Sprzeczność. □

CZWARTY DOWÓD. (wg. Erdősa) Niech $n \geqslant 2$ będzie dowolną liczbą naturalną. Niech $s = \pi(n)$ oznacza ilość liczb pierwszych niewiększych niż n. Oznaczmy przez $p_1, p_2, \ldots, p_s$ wszystkie liczby pierwsze z przedziału $[\,1;\, n\,]$. Każdą liczbę naturalną $m \leqslant n$ przedstawiamy, na mocy ćwiczenia C2.36, jednoznacznie w postaci

$$m = k \cdot a^2 = (p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}) \cdot a^2, \tag{2.19}$$

gdzie $e_i = 0$ lub 1, bo k jest bezkwadratowa. Policzmy ile (co najwyżej) istnieje iloczynów (2.19). Ponieważ wykładniki e_i mogą przyjmować wartości 0 lub 1, więc możliwych czynników k jest co najwyżej 2^s. Możliwych zaś czynników a^2 jest co najwyżej $\sqrt{n}$. Zatem

$$n \leqslant 2^s \sqrt{n}.$$

Stąd, po zlogarytmowaniu, dostajemy $\frac{1}{2}\log n \leqslant s \log 2$, czyli

$$\pi(n) \geqslant \frac{\log n}{2 \log 2}. \tag{2.20}$$

Ponieważ funkcja $C \log n$ rośnie do nieskończoności (przy $C > 0$ i $n \to \infty$), więc zbiór $\mathbb{P}$ jest zbiorem nieskończonym. □

Ćwiczenie 2.36 Liczbę naturalną k nazywamy **bezkwadratową**, gdy nie dzieli się przez kwadrat żadnej liczby pierwszej. Dowieść, że każdą niezerową liczbę całkowitą m da się na jeden i tylko jeden sposób zapisać w postaci iloczynu $m = ka^2$, gdzie k jest liczbą bezkwadratową.

Ćwiczenie 2.37 Udowodnić, że jeżeli najmniejszy dzielnik pierwszy p liczby naturalnej n jest większy niż $\sqrt[3]{n}$, to liczba n/p jest liczbą pierwszą lub jedynką.

2.3.3 Kilka pytań dotyczących liczb pierwszych

Z twierdzenia Euklidesa wiemy, że ciąg:

$$p_1 = \mathbf{2},\ p_2 = \mathbf{3},\ p_3 = \mathbf{5},\ \ldots,\ p_{25} = \mathbf{97},\ \ldots,\ p_{168} = \mathbf{997},\ \ldots,\ p_{305} = \mathbf{2011},\ \ldots \tag{2.21}$$

(zobacz naszą tabelkę liczb pierwszych na stronie vi), którego n-tym wyrazem jest n-ta (w kolejności rosnącej) liczba pierwsza, jest ciągiem nieskończonym. Jest to ciąg bardzo "nieregularny": nie znamy żadnego sensownego wzoru na n-ty wyraz tego ciągu. To znaczy, nie znamy żadnej takiej funkcji elementarnej (wielomianu, funkcji wymiernej, wykładniczej czy ich złożeń) f, że $f(n) = p_n$. Nie znamy też żadnej takiej niestałej funkcji elementarnej g, że $g(n) \in \mathbb{P}$ dla wszystkich $n \in \mathbb{N}$. Można zadać nieskończenie wiele pytań na temat ciągu (2.21). Powiemy tu o paru takich pytaniach.

Przykład 1. W ciągu (p_n) są dowolnie duże "dziury", czyli, dla dowolnie dużej liczby N istnieje taki indeks n, że $p_{n+1} - p_n \geqslant N$. Rzeczywiście, ponieważ kolejne liczby

$$N! + 2,\ N! + 3,\ N! + 4,\ \ldots,\ N! + N$$

wszystkie są złożone, więc największy taki indeks n, że $p_n \leqslant N! + 1$, jest oczywiście dobry. Z drugiej strony, zdarzają się najmniejsze możliwe "dziury". To znaczy, istnieją takie indeksy n, że $p_{n+1} - p_n = 2$. Pary $\{p, p+2\}$ liczb pierwszych nazywamy parami **liczb pierwszych bliźniaczych**. Para $3\,756\,801\,695\,685 \cdot 2^{666\,669} \pm 1$ jest największą znaną (koniec 2013) parą liczb pierwszych bliźniaczych. N i e wiadomo czy takich "bliźniaków" jest nieskończenie wiele. Zobacz też 12.3.2 U2. ◊

P r z y k ł a d 2. Euler zwrócił uwagę świata na wielomian

$$E(X) = X^2 + X + 41,$$

który dla $x = 0, 1, 2, \ldots, 40$ przyjmuje wartości będące liczbami pierwszymi (sprawdźcie!). [Ta interesująca własność wielomianu $E(X)$ jest ściśle związana z faktem, że *pierścień kwadratowy* $\mathbb{Z}[\tau_{-163}]$ *jest* dig*'iem*, zobacz T10.10.] Oczywiście $41|E(41)$ i $41 < E(41)$, więc $E(41)$ jest liczbą z ł o ż o n ą. Nie ma w tym nic nadzwyczajnego: w Z5.3 pokazujemy, że jeżeli $f(X) = a_0 + a_1X + \cdots + a_nX^n$ jest wielomianem stopnia $\geqslant 1$ o współczynnikach całkowitych, to wartości $|f(x)|$ n i e mogą być liczbami pierwszymi dla wszystkich $x \in \mathbb{Z}$. ◊

Ćwiczenie 2.38 Udowodnić, że jeżeli liczba naturalna, której wszystkie cyfry (w dowolnym systemie pozycyjnym) są jedynkami, jest liczbą pierwszą, to liczba tych cyfr jest liczbą pierwszą (ale nie na odwrót, na przykład $(111)_7$ dzieli się przez $19 = (25)_7$).

U w a g a 1. Wśród liczb trzycyfrowych $(111)_m = m^2+m+1$, przy $2 \leqslant m \leqslant 44$, występuje, jak to można sprawdzić posługując się naszą tabelką liczb pierwszych, dokładnie 16 liczb pierwszych. Wielomian $X^2 + X + 1$ przyjmuje więc (dla argumentów całkowitych) dosyć "chętnie" wartości będące liczbami pierwszymi. Nie wiadomo jednak czy "robi" to nieskończenie wiele razy. Podobnie ma się rzecz z wielomianem $X^2 + 1$.

Wielomiany (jednej zmiennej) nie "chcą" dawać samych wartości będących liczbami pierwszymi. Próbowano więc szukać liczb pierwszych w postaci wykładniczej.

P r z y k ł a d 3. Rozważmy **liczby Mersenne'a** $M_n = 2^n - 1$. Liczba M_n na pewno jest liczbą złożoną, gdy n jest liczbą złożoną. To wynika z tożsamości "nieśmiertelnej" (1.8). Rzeczywiście, jeżeli $n = ab$, gdzie $a, b \geqslant 2$, to mamy rozkład

$$M_n = 2^{ab} - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1),$$

i oba czynniki są $\geqslant 2$. Jeżeli $n = p$ jest liczbą pierwszą, to takiego (systemowego) rozkładu nie ma. Więc jest szansa na pierwszość liczby M_p. Na przykład $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ są liczbami pierwszymi. Ale już $M_{11} = 23 \cdot 89$. Liczby M_p będące liczbami pierwszymi nazywamy **liczbami pierwszymi Mersenne'a**. Nie wiadomo czy jest ich nieskończenie wiele. Do dzisiaj (maj 2017 roku) znamy tylko 49 liczb pierwszych Mersenne'a. N a j w i ę k s z ą z nich jest $M_{74\,207\,281}$. Nie wiadomo również czy istnieje nieskończenie wiele liczb złożonych Mersenne'a, chociaż wydaje się to bardzo prawdopodobnym. Na przykład, wśród początkowych 50 000 liczb M_n występuje t y l k o 27 liczb pierwszych (największą z nich jest $M_{44\,497}$). Pewną metodę sprawdzania złożoności liczb M_p poznamy w rozdziale 5, zobacz 5.7.8 U2. ◊

Jeszcze "gorzej" ma się sprawa z liczbami $V_n := 2^n + 1$:

Ćwiczenie 2.39 Udowodnić, że jeżeli $2^n + 1 \in \mathbb{P}$, to $n = 2^k$ dla pewnego $k \in \mathbb{N}$.

P r z y k ł a d 4. Liczby V_{2^k} oznaczamy F_k i nazywamy liczbami Fermat'*a*, zobacz Z2.2. Fermat sądził, że wszystkie liczby F_k są liczbami pierwszymi. Nietrudno(?) to sprawdzić dla $k = 0, 1, 2, 3$ i 4: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$. Niemałym zaskoczeniem okazał się, udowodniony przez Eulera[4], $F a k t$: $\boxed{641|F_5.}$ Można go uzasadnić następująco: Mamy równość

$$F_5 = 2^{32} + 1 = 2^{28}(5^4 + 2^4) - (5 \cdot 2^7)^4 + 1 = 2^{28} \cdot 641 - (640^4 - 1).$$

Wystarczy teraz przywołać tożsamość $x^4 - 1 = (x + 1)(x - 1)(x^2 + 1)$ i położyć $x = 640$. Warto wiedzieć, że od czasów Eulera znaleziono (skończenie!) wiele złożonych liczb Fermat'*a* i a n i j e d n e j, poza F_0, F_1, F_2, F_3 i F_4, **liczby pierwszej Fermat'*a***. Wspomnimy jeszcze, że największą liczbą Fermat'*a*, o której udowodniono, że jest liczbą z ł o ż o n ą, jest $F_{3\,329\,780}$. Jej dzielnikiem jest liczba pierwsza(!) $386 \cdot 2^{3\,329\,781} + 1$ (lipiec 2014). Porównaj Z5.15. $\Diamond$

Ćwiczenie 2.40 Udowodnić, że jeżeli $k \in \mathbb{N}$, to liczba $F_k + F_{k-1} - 1$ ma co najmniej k różnych dzielników pierwszych. *Wskazówka.* Zastosować rozumowanie indukcyjne z wykorzystaniem tożsamości $x^4 + x^2 + 1 = (x^2 + 1 - x)(x^2 + 1 + x)$.

2.4 Wykładniki p-adyczne

Na zbiorze niezerowych liczb wymiernych działają funkcje v_p wykładników p-adycznych. Funkcji v_p jest nieskończenie wiele (tyle ile jest liczb pierwszych). Dostarczają one wygodnego sposobu myślenia o podzielności w pierścieniu $\mathbb{Z}$. Warto więc poznać najprostsze ich własności.

2.4.1 Definicje. Formuła Legendre'*a*

Zdefiniujemy najpierw funkcje v_p na zbiorze liczb całkowitych, a następnie rozszerzymy ich dziedzinę do zbioru liczb wymiernych.

Definicja 2.8 Jeżeli p jest liczbą pierwszą, a $c \neq 0$ jest liczbą całkowitą, to symbolem $v_p(c)$ oznaczamy największą liczbę całkowitą k, dla której $p^k|c$. Kładziemy też $v_p(0) = +\infty$. Liczbę $v_p(c)$ nazywamy **wykładnikiem p-adycznym** liczby $c \in \mathbb{Z}$.

Jeżeli m jest niezerową liczbą całkowitą, to biorąc rozkład (2.17) liczby $|m|$ i grupując ewentualne powtarzające się takie same czynniki w potęgę, dostajemy tak zwany **kanoniczny rozkład liczby całkowitej** na iloczyn liczb pierwszych

$$m = \pm p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}. \tag{RK}$$

Przy takim zapisie rozumiemy, że występujące w nim liczby pierwsze p_i są p a r a m i r ó ż n e. Jasne, że wykładnik e_i, z jakim występuje liczba pierwsza p_i w kanonicznym rozkładzie (RK) liczby naturalnej $|m|$ na czynniki pierwsze, jest równy wykładnikowi p_i-adycznemu liczby m. Kanoniczny rozkład liczby naturalnej n na czynniki pierwsze możemy więc zapisać:

$$\boxed{n = \textstyle\prod_p p^{v_p(n)},}$$

[4]Napisał wtedy z dumą: $2^{32} + 1$ *non esse primum inveni, sed divisibilem per numeri* 641

gdzie iloczyn rozciąga się na wszystkie liczby pierwsze, ale prawie wszystkie czynniki są równe 1. Zwrot *prawie wszystkie* znaczy: wszystkie z wyjątkiem skończenie wielu.

Ćwiczenie 2.41 Udowodnić, że $a|b$ wtedy i tylko wtedy, gdy $v_p(a) \leqslant v_p(b)$ dla każdej liczby pierwszej p.

Ćwiczenie 2.42 Udowodnić, że dodatnia liczba d jest równa $\mathrm{NWD}\,(a,b)$ wtedy i tylko wtedy, gdy $v_p(d) = \min\{v_p(a),\, v_p(b)\}$ dla każdej liczby pierwszej p. Analogicznie dla najmniejszej wspólnej wielokrotności: $v_p(\mathrm{NWW}\,(a,\,b)) = \max\{v_p(a),\, v_p(b)\}$.

Ćwiczenie 2.43 Ustalmy liczbę pierwszą p. Udowodnić, że funkcja v_p ma własności:

1. $v_p(ab) = v_p(a) + v_p(b)$,

2. $v_p(a+b) \geqslant \min\{v_p(a),\, v_p(b)\}$ (przy tym, gdy $v_p(a) \neq v_p(b)$, to zachodzi równość).

Ćwiczenie 2.44 Liczba naturalna a jest n-tą potęgą liczby naturalnej wtedy i tylko wtedy, gdy $n|v_p(a)$ dla każdej liczby pierwszej p. Udowodnić.

ZADANIE 2.7 Liczby naturalne a i b są takie, że $a^n|b^{n+1}$ dla każdej liczby naturalnej n. Udowodnić, że $a|b$.

Rozwiązanie. Niech p będzie dowolną liczbą pierwszą. Mamy wykazać, że $k \leqslant l$, gdzie $k = v_p(a)$, $l = v_p(b)$. Z założenia i C2.41 wiemy, że $nk \leqslant (n+1)l$ dla każdej liczby naturalnej n. Załóżmy, nie wprost, że $k > l$ i połóżmy $k = l + r$, $r \geqslant 1$. Wówczas, na mocy nierówności $nk \leqslant (n+1)l$, mamy $n(l+r) \leqslant (n+1)l$, skąd $n \leqslant nr \leqslant l$ dla każdego $n \in \mathbb{N}$. Ta, oczywista, sprzeczność kończy rozwiązanie. ◊

Ćwiczenie 2.45 **(1)** Obliczyć $\sum_{k=1}^{1000} v_2(k)$. **(2)** Rozłożyć na czynniki pierwsze liczbę 20!.

Po rozwiązaniu tego ćwiczenia z łatwością udowodnimy poniższe twierdzenie:

TWIERDZENIE 2.17 (***Legendre***) *Wykładnik p-adyczny liczby* $n!$ (*silnia*) *wynosi*

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ \ldots \ + \left\lfloor \frac{n}{p^k} \right\rfloor,$$

gdzie k *jest taką liczbą naturalną, że* $p^k \leqslant n < p^{k+1}$. □

Ćwiczenie 2.46 Dowieść, że $2^n \nmid n!$ dla $n \in \mathbb{N}$. Wyznaczyć zbiór $\{n \in \mathbb{N} : 2^{n-1}|n!\}$.

Funkcja v_p wykładnika p-adycznego, określona wyjściowo na zbiorze $\mathbb{Z}$ liczb całkowitych, może być rozszerzona do funkcji $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{+\infty\}$ za pomocą równości:

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b) \quad \text{oraz} \quad v_p(0) = +\infty.$$

Ćwiczenie 2.47 Udowodnić, że to określenie jest poprawne (to znaczy, że nie zależy od przedstawienia liczby wymiernej w postaci ułamka) oraz że funkcja v_p ma własności:

1. $v_p(xy) = v_p(x) + v_p(y)$,

2. $v_p(x+y) \geqslant \min\{v_p(x),\, v_p(y)\}$ (przy tym, gdy $v_p(x) \neq v_p(y)$, to zachodzi równość).

Ćwiczenie 2.48 Udowodnić, że liczba wymierna x jest liczbą całkowitą wtedy i tylko wtedy, gdy $v_p(x) \geqslant 0$ dla każdej liczby pierwszej p.

Ćwiczenie 2.49 Podać czysto arytmetyczny (to znaczy bez wykorzystywania interpretacji kombinatorycznej) dowód faktu, że liczba $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ jest liczbą całkowitą dla dowolnych liczb całkowitych $0 \leqslant k \leqslant n$. *Wskazówka.* $0! = 1$. W razie potrzeby zobacz C12.1.5.

Ćwiczenie 2.50 Udowodnić, że jeżeli p jest liczbą pierwszą, s jest dowolną liczbą naturalną, a $1 \leqslant k \leqslant p^s - 1$, to p dzieli $\binom{p^s}{k}$. *Wskazówka.* Zobacz Z12.11.

U w a g a. Określona na zbiorze $\mathbb{Q}$ funkcja v_p przyjmuje wartości w zbiorze $\mathbb{Z} \cup \{+\infty\}$, gdzie $+\infty$ jest d o d a t k o w y m elementem (n i e liczbą!) spełniającym wymagania:

$$(+\infty) + k = +\infty, \quad (+\infty) + (\infty) = +\infty \quad \text{oraz} \quad +\infty > k$$

dla dowolnej liczby całkowitej k.

2.4.2 Lemat o zwiększaniu wykładnika p-adycznego

Zastanowimy się nad zależnością wykładnika p-adycznego $v_p(x^k \pm y^k)$ liczb całkowitych postaci $x^k \pm y^k$ od wykładników p-adycznych $v_p(x \pm y)$ i $v_p(k)$.

Wprowadzimy wygodne oznaczenie: $Q_k(x,\, y) = x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1}$. Tożsamość "nieśmiertelna" (zob. (1.8)) pisze się więc tak:

$$x^k - y^k = (x-y)Q_k(x,\, y) \tag{2.22}$$

Jeżeli x, y są liczbami całkowitymi, to ta równość i teza ćwiczenia C2.43.1 pokazują, że $v_p(x^k - y^k) = v_p(x-y) + v_p(Q_k(x,\, y))$. Widzimy stąd, że wykładnik p-adyczny liczby $x^k - y^k$ jest n i e m n i e j s z y od wykładnika p-adycznego liczby $x - y$. Głównym morałem płynącym z tego ustępu jest fakt, że, przy pewnych dodatkowych założeniach, mamy pełną kontrolę nad przyrostem $v_p(x^k - y^k) - v_p(x-y) = v_p(Q_k(x,\, y))$. W dowodzie tego wyniku wykorzystamy tezy poniższych dwóch zadań.

ZADANIE 2.8 Dana jest liczba pierwsza p i liczby całkowite x, y. Udowodnić, że jeżeli $v_p(xy) = 0$, $v_p(x-y) \geqslant 1$ i $p \nmid k$, to zachodzi równość

$$v_p(x^k - y^k) = v_p(x-y). \tag{2.23}$$

R o z w i ą z a n i e. Wobec równości (2.22) wystarczy udowodnić, że $p \nmid Q_k(x,\, y)$. Założenie $v_p(x-y) \geqslant 1$ zapisujemy w postaci: $x = y + pc$, dla pewnego $c \in \mathbb{Z}$. Mamy wtedy

$$Q_k(x,\, y) = (y+pc)^{k-1} + (y+pc)^{k-2}y + \cdots + (y+pc)y^{k-2} + y^{k-1}.$$

Występujące tu czynniki $(y+pc)^s$, dzięki równości dwumiennej (1.7), zapisujemy w postaci $y^s + pC$, gdzie $C \in \mathbb{Z}$. Stąd, po uporządkowaniu, $Q_k(x,\, y) = ky^{k-1} + pD$ dla pewnego $D \in \mathbb{Z}$. Jasne, że to kończy dowód równości (2.23). Bowiem $p \nmid k$ i $p \nmid y$. $\Diamond$

ZADANIE 2.9 Dana jest liczba pierwsza nieparzysta p i liczby całkowite x, y. Udowodnić, że jeżeli $v_p(xy) = 0$ i $v_p(x-y) \geqslant 1$, to dla dowolnego $s \in \mathbb{N}$ zachodzi równość

$$v_p(x^{sp} - y^{sp}) = v_p(x^s - y^s) + 1. \tag{2.24}$$

Rozwiązanie. Rozważamy najpierw przypadek $s = 1$. Teza jest wówczas równoważna dwóm faktom: $p|Q_p(x, y)$ oraz $p^2 \nmid Q_p(x, y)$. Dla ich dowodu postępujemy tak jak wyżej z tą różnicą, że wykorzystujemy wzór dwumienny "z dokładnością do wyrazów kwadratowych": $(y + pc)^s = y^s + \binom{s}{1}pcy^{s-1} + p^2A = y^s + spcy^{s-1} + p^2A$. Dostaniemy wówczas

$$Q_p(x, y) = py^{p-1} + [(p-1) + (p-2) + \cdots + 1 + 0]\, pcy^{p-2} + p^2B.$$

Ponieważ suma $0 + 1 + \cdots + (p-1)$ jest równa $\frac{1}{2}(p-1)p$ (zob. 1.1.2 P), więc jest liczbą podzielną przez p (tutaj jest ważna nieparzystość liczby p). Wobec tego mamy $Q_p(x, y) = py^{p-1} + p^2\left[\frac{p-1}{2}cy^{p-2} + B\right]$. Stąd widać prawdziwość obu faktów. Bowiem $p \nmid y$.

Przypadek dowolnego $s \in \mathbb{N}$ sprowadza się do rozważonego: kładziemy $x_1 = x^s$, $y_1 = y^s$ i sprawdzamy założenia $v_p(x_1y_1) = 0$ oraz $v_p(x_1 - y_1) \geqslant 1$. Drugie jest spełnione, bowiem $v_p(x_1 - y_1) = v_p((x-y)Q_s(a, b)) = v_p(x-y) + v_p(Q_s(x, y)) \geqslant v_p(x-y) \geqslant 1$, a pierwsze jest spełnione, bowiem $v_p(x_1y_1) = sv_p(xy) = 0$. To kończy rozwiązanie. ♢

W twierdzeniu T2.18, które nazywać będziemy ***Lematem o Zwiększaniu Wykładnika***, dowodzimy, że, przy wypisanych założeniach, przyrost $v_p(x^k - y^k) - v_p(x-y)$ jest równy $v_p(k)$.

TWIERDZENIE 2.18 (LZW) *Niech x, $y \in \mathbb{Z}$, $k \in \mathbb{N}$ i $p \in \mathbb{P}$. Wówczas, jeżeli spełnione są warunki $v_p(xy) = 0$ i $v_p(x-y) \geqslant \frac{3}{p}$, to*

$$\boxed{\boxed{v_p(x^k - y^k) = v_p(x-y) + v_p(k).}} \tag{2.25}$$

DOWÓD. Warunek $v_p(x-y) \geqslant 3/p$ oznacza, oczywiście, że $v_p(x-y) \geqslant 1$ w przypadku gdy $p > 2$ oraz $v_p(x-y) \geqslant 2$ w przypadku gdy $p = 2$. Rozważymy osobno te dwa przypadki.

Przypadek $p > 2$. Niech $k = p^\alpha m$, gdzie $\alpha = v_p(k)$. Liczby $x_1 = x^{p^\alpha}$, $y_1 = y^{p^\alpha}$ spełniają(!) założenia $v_p(x_1y_1) = 0$, $v_p(x_1 - y_1) \geqslant 1$. Ponieważ $p \nmid m$, więc, na mocy Z2.8, $v_p(x^k - y^k) = v_p(x_1^m - y_1^m) = v_p(x_1 - y_1) = v_p(x^{p^\alpha} - y^{p^\alpha})$. Jasne, że α-krotne zastosowanie równości (2.24) daje tezę:

$$v_p(x^{p^\alpha} - y^{p^\alpha}) = v_p(x^{p^{\alpha-1}} - y^{p^{\alpha-1}}) + 1 = v_p(x^{p^{\alpha-2}} - y^{p^{\alpha-2}}) + 2 = \ldots = v_p(x-y) + \alpha.$$

Przypadek $p = 2$. Niech $k = 2^\alpha m$, $2 \nmid m$. Załóżmy najpierw, że $m = 1$. Wielokrotne zastosowanie wzoru na różnicę kwadratów daje wówczas rozkład

$$x^k - y^k = (x^{2^{\alpha-1}} + y^{2^{\alpha-1}})(x^{2^{\alpha-2}} + y^{2^{\alpha-2}}) \cdot \ldots \cdot (x^2 + y^2)(x+y)(x-y).$$

Mamy tu α czynników *z plusem* i jeden czynnik $(x-y)$. Sprawdzamy, że wykładnik 2-adyczny każdego czynnika *z plusem* równy jest 1. Tu konieczne jest (mocniejsze niż w przypadku nieparzystego p) założenie $v_2(x-y) \geqslant 2$. Rzeczywiście, jeżeli $x = 2c+1$ i $x - y = 4d$, to $x + y = 4(c-d) + 2 = 2(2c - 2d + 1)$, skąd $v_2(x+y) = 1$. Jeszcze łatwiej[5] sprawdzić,

[5]Chodzi o to, że pozostałe czynniki *z plusem* są sumami dwóch kwadratów liczb nieparzystych, a kwadrat liczby nieparzystej daje resztę 1 z dzielenia przez 4, więc suma dwóch takich kwadratów daje resztę 2 z dzielenia przez 4. Ta uwaga przydaje się w rozwiązaniu C2.51.

że wykładnik 2-adyczny pozostałych czynników *z plusem* jest równy 1. To kończy dowód równości (2.25) w tym podprzypadku. Przypadek dowolnego nieparzystego m rozpatrujemy tak jak wyżej (za pomocą (2.23)). □

Ćwiczenie 2.51 Udowodnić, że jeżeli $v_2(xy) = 0$, $v_2(x-y) \geqslant 1$, a $k \in \mathbb{N}$ jest liczbą p a r z y s t ą, to zachodzi równość

$$v_2(x^k - y^k) = v_2(x^2 - y^2) + v_2(k) - 1. \tag{2.26}$$

U w a g a. Dla n i e p a r z y s t y c h wykładników k istnieje "plusowy" wariant tożsamości nieśmiertelnej: $x^k + y^k = (x+y)(x^{k-1} - x^{k-2}y + \ldots - xy^{k-2} + y^{k-1})$ (jego prawdziwość wynika z równości (1.8) i oczywistych równości $(-y)^s = -y^s$ dla nieparzystych s). Dzięki niemu łatwo rozwiążemy poniższe ćwiczenie:

Ćwiczenie 2.52 Udowodnić następujący wariant "plusowy" lematu LZW. Mianowicie: *Jeżeli* $x, y \in \mathbb{Z}$, $v_p(xy) = 0$ *i* $v_p(x+y) \geqslant 1$, *a* k *jest liczbą n i e p a r z y s t ą, to*

$$v_p(x^k + y^k) = v_p(x+y) + v_p(k). \tag{2.27}$$

Pokażemy parę przykładów wykorzystania LZW.

P r z y k ł a d 1. Przez jaką najwyższą potęgę liczby 3 dzieli się liczba $L_n = 11\ldots1$ zapisana (w systemie dziesiętnym) za pomocą n cyfr 1? Ponieważ (zob. tożsamość nieśmiertelną)

$$9L_n = 9(10^{n-1} + 10^{n-2} + \cdots + 10 + 1) = 9 \cdot \frac{10^n - 1}{10 - 1} = 10^n - 1^n,$$

więc $v_3(9L_n) = 2 + v_3(L_n) = 2 + v_3(10-1) + v_3(n)$. Zatem $v_3(L_n) = 2 + v_3(n)$. ◊

P r z y k ł a d 2. Wyznaczymy wszystkie takie liczby naturalne n, że $3^n | 5^n + 1$. Jasne, że $n = 1$ jest dobra. Ponieważ para $(x, y) = (5, 1)$ spełnia założenia "plusowego" wariantu LZW (zob. C2.52) dla $p = 3$, więc dla każdej n i e p a r z y s t e j liczby n mamy: $v_3(5^n + 1) = v_3(6) + v_3(n)$. Gdyby więc $3^n | 5^n + 1$, mielibyśmy nierówność $n \leqslant 1 + v_3(n)$. Aby zobaczyć, że taka nierówność jest możliwa jedynie dla $n = 1$ musimy opuścić arytmetykę i wejść na teren analizy matematycznej. Mielibyśmy bowiem wówczas dla $n = 3^k \cdot m$, gdzie $3 \perp m$, jawnie fałszywą nierówność $3^k \leqslant n \leqslant 1 + k$ (dla każdego $k \in \mathbb{N}$ prawdziwa jest bowiem nierówność odwrotna $1 + k < 3^k$, co bardzo łatwo udowodnić przez indukcję!).

Również jest jasne, że n nie może być liczbą parzystą, wtedy bowiem liczba $5^n + 1$, jako równa $(24+1)^{n/2} + 1 = 3A + 2$, w ogóle nie dzieli się przez 3. ◊

P r z y k ł a d 3. W 33 OM należało udowodnić, że: *Jeżeli* a *jest liczbą naturalną parzystą, to dla dowolnego* $n \in \mathbb{N}$ *liczba* $a^{(a+1)^n} + 1$ *dzieli się przez* $(a+1)^{n+1}$ *ale nie dzieli się przez* $(a+1)^{n+2}$. Aby to udowodnić bierzemy dowolny dzielnik pierwszy p liczby $a+1$. Ponieważ a jest liczbą parzystą, więc $p > 2$. Kładąc $x = a$, $y = 1$ oraz $k = (a+1)^n$ znajdujemy się w sytuacji opisanej przez "plusowy" wariant LZW z ćwiczenia C2.52. Dostajemy więc równość

$$v_p\left(a^{(a+1)^n} + 1\right) = v_p(a+1) + v_p((a+1)^n) = v_p(a+1) + nv_p(a+1) = (n+1)v_p(a+1).$$

Jasne(?!), że to kończy dowód. ◊

Ćwiczenie 2.53 Niech $p \in \mathbb{P}_{\geqslant 5}$. Wyznaczyć $v_p\left[(p-2)^{2(p-1)} - (p-4)^{p-1}\right]$.

Ćwiczenie 2.54 Niech $A = (n-1)^{n^{n+1}} + (n+1)^{n^{n-1}}$ dla danej liczby nieparzystej $n \geqslant 3$. Wyznaczyć największą taką liczbę naturalną k, że $n^k | A$.

Ćwiczenie 2.55 Udowodnić, że dla każdej liczby naturalnej $n \geqslant 2$ zachodzi nierówność $v_2(5^n - 3^n) \leqslant 3 + \log_2 n$.

ZADANIE 2.10 Wyznaczyć wszystkie takie czwórki $(x, y, n, k) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}_{\geqslant 2}$, że $x < y$, $x \perp y$ i $3^n = x^k + y^k$.

Rozwiązanie. Po pierwsze: jasne, że $v_3(xy) = 0$ (gdy $3|x$, to dzięki Zasadzie Podstawowej widzimy, że $3|y$, co jest niemożliwe, bo $x \perp y$). Po drugie: k nie może być liczbą parzystą (parzysta potęga liczby niepodzielnej przez 3 jest kwadratem liczby niepodzielnej przez 3, a $(3u \pm 1)^2 = 9u^2 \pm 6u + 1$, więc suma dwóch parzystych potęg liczb niepodzielnych przez 3 daje resztę $1 + 1$ z dzielenia przez 3). Zatem $k = 2m + 1 \geqslant 3$ i możemy zastosować (2.27):

$$n = v_3(3^n) = v_3(x^k + y^k) = v_3(x + y) + v_3(k),$$

bo $v_3(x + y) \geqslant 1$ (ta nierówność wynika z równości $3^n = (x + y)(x^{k-1} - \cdots + y^{k-1})$, z której widać, że $x + y$ jest potęgą liczby 3 o dodatnim wykładniku). Mamy więc

$$x^k + y^k = 3^n = 3^{v_3(x+y)} \cdot 3^{v_3(k)} \leqslant (x + y)k.$$

Taka nierówność jest sprzeczna z nierównościami $x^k > kx$ i $y^k > ky$ (prawdziwymi dla $x, y \geqslant 2$ i $k \geqslant 3$). Pozostaje zbadać przypadek $x = 1$. Mamy wówczas $1 + y^k \leqslant k + ky$. Stąd:

$$k + ky \geqslant 1 + y^k = 1 + [1 + (y-1)]^k = 1 + 1 + k(y-1) + \binom{k}{2}(y-1)^2 + \ldots >$$
$$> 2 - k + ky + \frac{k(k-1)}{2}(y-1)^2,$$

bo w miejscu kropek stoją wyrazy dodatnie. Stąd, po prostych przekształceniach, $k(y-1)^2 < 4$. Ta nierówność jest możliwa tylko dla $y = 2$ (pamiętamy, że $y \geqslant 2$ i $k \geqslant 3$). W ten sposób znajdujemy jedyne rozwiązanie: $(x, y, n, k) = (1, 2, 2, 3)$. ◊

ZADANIE 2.11 Udowodnić, że jeżeli dla pewnego $k \in \mathbb{N}$ zachodzi równość $3^k - 2^k = p^n$, gdzie $p \in \mathbb{P}$, a $n \geqslant 2$, to k jest liczbą pierwszą.

Rozwiązanie. Jasne, że $p \neq 2, 3$ i $k > 1$. Pokażemy, że jeżeli $k = ab$, przy czym $a, b \geqslant 2$, to $p|a$ (i $p|b$): Mamy równość $3^k - 2^k = (3^a - 2^a)Q_b(3^a, 2^a)$. Stąd i z jednoznaczności rozkładu, mamy $3^a - 2^a = p^\alpha$, gdzie $1 \leqslant \alpha < n$. Dzięki LZW dostajemy równość

$$n = v_p(3^k - 2^k) = v_p(3^a - 2^a) + v_p(b) = \alpha + v_p(b) \qquad (*)$$

Zatem $v_p(b) \geqslant 1$. Podobnie dostajemy nierówność $v_p(a) \geqslant 1$. To oznacza, że k jest potęgą liczby pierwszej, konkretnie: $k = p^s$. Wystarczy wykazać, że $s = 1$. Załóżmy więc, nie wprost, że $s \geqslant 2$. Wówczas $k = p \cdot p^{s-1}$. W równości $(*)$ połóżmy $a = p$, $b = p^{s-1}$. Otrzymujemy $n = v_p(3^p - 2^p) + s - 1$. Wobec tego

$$(3^a)^b - (2^a)^b = 3^k - 2^k = p^n = p^{v_p(3^p - 2^p) + s - 1} = (3^p - 2^p)b.$$

Stąd dostajemy nonsensowną równość $b = Q_b(3^p, 2^p)$ (gdy $x, y \in \mathbb{N}_{\geqslant 3}$, to $Q_b(x, y)$ jest sumą b składników postaci $x^t y^{b-1-t}$, z których każdy jest większy niż 2^{b-1}). $\Diamond$

Proponujemy jeszcze trzy ćwiczenia na zastosowanie LZW[6].

Ćwiczenie 2.56 Załóżmy, że $x^k + y^k = p^n$, gdzie $x, y, k, n \in \mathbb{N}$, $2 \nmid k$ i $p \in \mathbb{P}_{>2}$. Udowodnić, że k ma co najwyżej jeden dzielnik pierwszy.

Ćwiczenie 2.57 Liczba naturalna $n \geqslant 2$ jest dzielnikiem liczby $(a-1)^k$, gdzie $k, a \in \mathbb{N}_{\geqslant 2}$. Udowodnić, że wówczas $n|(a^{n-1} + a^{n-2} + \cdots + a + 1)$.

Ćwiczenie 2.58 Wyznaczyć wszystkie $n \in \mathbb{N}$, dla których zachodzi podzielność $2^n|3^n - 1$.

2.5 Trójki pitagorejskie

W tym paragrafie poznamy jeden prosty ale ważny trik, i zobaczymy jak za jego pomocą rozwiązuje się równanie Pitagorasa.

2.5.1 Trik

Prosty ***trik***, który jest treścią kolejnego twierdzenia, jest bardzo często używany. Jest on natychmiastowym wnioskiem z jednoznaczności rozkładu. Jego rozliczne uogólnienia są bardzo ważnym motywem w całej teorii liczb.

TWIERDZENIE 2.19 (***Trik***) *Jeżeli liczby naturalne a, b są względnie pierwsze i zachodzi równość $ab = c^k$ dla pewnych $c, k \in \mathbb{N}$, to liczby a, b są k-tymi potęgami liczb naturalnych.*

DOWÓD. Niech p będzie dowolną liczbą pierwszą dzielącą a. Wówczas $p|c^k$ i, wobec założenia $a \perp b$, $p \nmid b$, czyli $v_p(b) = 0$. Zatem

$$k \cdot v_p(c) = v_p(c^k) = v_p(ab) = v_p(a) + v_p(b) = v_p(a).$$

Stąd, na mocy C2.44, a jest k-tą potęgą. Podobnie, b jest k-tą potęgą liczby naturalnej. $\square$

ZADANIE 2.12 Niech $n, m \in \mathbb{Z}$ będą takimi liczbami całkowitymi, że zachodzi równość $7n^2 - n = 8m^2 - m$. Udowodnić, że $|n - m|$ jest kwadratem liczby całkowitej.

Rozwiązanie. Równość $7n^2 - n = 8m^2 - m$ po przekształceniu daje

$$(n - m) \cdot (7(n + m) - 1) = m^2. \tag{2.28}$$

Teraz z łatwością sprawdzamy, że $\mathrm{NWD}\,(n - m, 7(n + m) - 1) = 1$. Istotnie, jeżeli liczba pierwsza p dzieli $n - m$, to, wobec równości (2.28), dzieli m^2, czyli też m. Więc dzieli też $(n - m) + 2m = n + m$. Zatem nie dzieli $7(n + m) - 1$. Na mocy triku T2.19 widzimy więc, że zarówno $|n - m|$ jak i $|7(n + m) - 1|$ są kwadratami liczb całkowitych. $\Diamond$

[6]W literaturze olimpijskiej używa się skrótu LTE (*Lifting the Exponent Lemma*)

2.5.2 Trójki pitagorejskie

Pokażemy teraz jak się rozwiązuje jedno klasyczne równanie diofantyczne stopnia 2. Rozwiązaniom tego równania w geometrii odpowiadają tak zwane trójkąty pitagorejskie.

Definicja 2.9 Rozwiązanie (x, y, z) **równania Pitagorasa**

$$x^2 + y^2 = z^2 \tag{2.29}$$

w liczbach naturalnych nazywamy **trójką pitagorejską**. Trójka pitagorejska (x, y, z) nazywa się **pierwotną trójką pitagorejską**, gdy $\mathrm{NWD}\,(x, y, z) = 1$.

U w a g a 1. Jest prawdopodobne, że jakieś ogólne metody znajdowania rozwiązań równania Pitagorasa były znane w Mezopotamii dwanaście wieków p r z e d Pitagorasem. Na przykład z tego okresu pochodzi gliniana tabliczka z zapisaną pismem klinowym trójką pitagorejską (6480, 4961, 8161). Pierwszy zaświadczony dowód twierdzenia T2.20 pochodzi od Euklidesa.

TWIERDZENIE 2.20 *Jeżeli (x, y, z) jest pierwotną trójką pitagorejską, w której x jest liczbą parzystą, to istnieją takie liczby $u, v \in \mathbb{N}$ różnej parzystości, że $u > v$, $u \perp v$ oraz:*

$$(x, y, z) = (2uv, u^2 - v^2, u^2 + v^2).$$

D O W Ó D. Niech $(x, y, z) \in \mathbb{N}$ będzie trójką pierwotną. Wówczas z jest liczbą nieparzystą, a z liczb x, y dokładnie jedna jest parzysta (dlaczego?). Połóżmy więc $z = 2n + 1$, $x = 2m$, $y = 2k + 1$. Ponieważ $x^2 = (z - y)(z + y)$, więc $m^2 = (n - k)(n + k + 1)$. Pokazujemy, że $\mathrm{NWD}\,(n - k, n + k + 1) = 1$: Gdy $d \in D(n - k, n + k + 1)$, to d dzieli sumę tych liczb i ich różnicę: $d|2n + 1$ i $d|2k + 1$. Więc $d|z$ i $d|y$. Zatem $d^2|z^2 - y^2$, stąd $d^2|x^2$, zatem $d|x$. I, dzięki założonej pierwotności trójki (x, y, z), mamy $d = \pm 1$. Stosujemy więc *trik*: znajdujemy takie liczby $u, v \in \mathbb{N}$, że $n + k + 1 = u^2$ i $n - k = v^2$. Stąd dostajemy: $z = 2n + 1 = u^2 + v^2$, $x = 2m = 2uv$ i $y = u^2 - v^2$. Przy tym u, v, jak łatwo się przekonać, są różnej parzystości i, wobec założenia pierwotności trójki (x, y, z), zachodzi $u \perp v$. □

Ćwiczenie 2.59 Uzupełnić szczegóły w powyższym dowodzie. *Wskazówka.* Uzasadnić, że kwadrat (liczby całkowitej) przy dzieleniu przez 4 daje resztę 0 lub 1.

U w a g a 2. Jeżeli (a, b, c) jest trójką pitagorejską, a $d = \mathrm{NWD}\,(a, b, c)$, to trójka $(x, y, z) = (\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ jest, oczywiście, trójką pitagorejską. Ponadto $\mathrm{NWD}\,(x, y, z) = 1$, więc (x, y, z) jest trójką pierwotną. Wobec tego każda trójka pitagorejska jest postaci

$$\boxed{(\,2duv,\, d(u^2 - v^2),\, d(u^2 + v^2)\,).} \tag{2.30}$$

Ćwiczenie 2.60 Wyznaczyć wszystkie takie trójki pitagorejskie, że $b = 15$ lub $c = 15$.

Ćwiczenie 2.61 Udowodnić, że jeśli (a, b, c) jest trójką pitagorejską, to $60|abc$.

Trójkąt prostokątny $\triangle ABC$ (zwyczajowo uznajemy $m(\sphericalangle C) = 90^\circ$) nazywa się **trójkątem pitagorejskim**, gdy długości wszystkich jego boków są liczbami całkowitymi.

Ćwiczenie 2.62 Udowodnić, że w trójkącie pitagorejskim zarówno promień r okręgu wpisanego jak i promienie r_A, r_B, r_C okręgów dopisanych, są liczbami naturalnymi. Udowodnić też, że istnieją trzy i, z dokładnością do przystawania, tylko trzy takie trójkąty pitagorejskie, że promień r okręgu w nie wpisanego jest równy 3.

Ćwiczenie 2.63 Wyznaczyć wszystkie trójkąty pitagorejskie o polu równym obwodowi, tzn., takie trójki pitagorejskie (a, b, c), że $a + b + c = ab/2$.

Ćwiczenie 2.64 Wyznaczyć wszystkie trójkąty pitagorejskie, w których przeciwprostokątna jest o 1 dłuższa niż jedna z przyprostokątnych.

Ćwiczenie 2.65 Wyznaczyć wszystkie rozwiązania równania $x^2 + y^2 = 2z^2$ w liczbach naturalnych. *Wskazówka.* Podstawić $x = u + v$, $y = u - v$.

Ćwiczenie 2.66 Udowodnić, że okręgi o równaniach $x^2 + y^2 = 1$ i $x^2 + y^2 = 2$ przechodzą przez nieskończenie wiele **punktów wymiernych** (o obu współrzędnych wymiernych), natomiast okrąg o równaniu $x^2 + y^2 = 3$ nie przechodzi przez żaden punkt wymierny.

2.6 Zadania dodatkowe

Pokazujemy zbiorek zadań do naszego *Elementarza*. Ich poziom trudności należy do przedziału [SP; IMO], a do ich rozwiązania wystarcza teoria wyłożona w tym rozdziale.

2.6.1 Treści zadań

Podział naszego zbiorku na podzbiorki jest mniej lub bardziej przypadkowy. Wszystkie oznaczenia są standardowe lub wyjaśnione.

A. Podzielność

ZADANIE 2.A0 Udowodnić, że ułamek $\frac{21n+4}{14n+3}$ jest nieskracalny dla każdego $n \in \mathbb{N}$.

ZADANIE 2.A1 Wyznaczyć cyfry x, y jeżeli wiadomo, że $13|(3\,0x0\,y03)_{10}$.

ZADANIE 2.A2 Niech x, y, z oznaczają liczby całkowite. Udowodnić, że zachodzą równoważności: **(1)** $37|2x + 15y \iff 37|3x + 4y$, **(2)** $6|x + y + z \iff 6|x^3 + y^3 + z^3$.

ZADANIE 2.A3 Niech $k, l \in \mathbb{N}$. Udowodnić, że jeżeli liczba $100kl - 1$ jest dzielnikiem liczby $(100k^2 - 1)^2$, to jest też dzielnikiem liczby $(100l^2 - 1)^2$.

ZADANIE 2.A4 Udowodnić, że jeżeli $x, y \in \mathbb{Z}$ oraz $11|x^2 + y^2$, to $11|x$ i $11|y$.

ZADANIE 2.A5 Dane są takie liczby naturalne a, b, c, że liczby $a^2 + b^2$, $b^2 + c^2$ i $c^2 + a^2$ są kwadratami (liczb naturalnych). Dowieść, że co najmniej jedna z liczb a, b, c jest podzielna przez 5.

ZADANIE 2.A6 Liczby naturalne a, b, c i m są takie, że $m|a + b$, $m|b + c$, $m|c + a$ i $m^3|abc$. Udowodnić, że $m|a$, $m|b$ i $m|c$.

ZADANIE 2.A7 Wyznacz zbiór: **(1)** $\{n \in \mathbb{N} : n + 5|n^5 + 5\}$; **(2)** $\{n \in \mathbb{N} : 5^{n-1} + 7^{n-1}|5^n + 7^n\}$.

ZADANIE 2.A8 Dana jest nieparzysta liczba naturalna k. Udowodnić, że dla każdego $n \in \mathbb{N}$ zachodzi podzielność $(1 + 2 + \cdots + n)|(1^k + 2^k + \cdots + n^k)$.

ZADANIE 2.A9 Dowieść, że istnieje dokładnie jedna taka trójka (a, b, c) liczb naturalnych, że $1 < a < b < c$ oraz $a|bc + 1$, $b|ca + 1$ i $c|ab + 1$.

ZADANIE 2.A10 Udowodnić, że jeżeli $a, b \in \mathbb{N}$ i $n \in \mathbb{N}_{\geqslant 2}$, to $(a^n - b^n) \nmid (a^n + b^n)$.

ZADANIE 2.A11 Wyznaczyć wszystkie takie pary (a, b) liczb naturalnych, że liczba ab^2+b+7 jest dzielnikiem liczby $a^2b + a + b$.

ZADANIE 2.A12 Udowodnić, że jeżeli $m, n \in \mathbb{N}$, to

$$\textbf{(1)}\ \frac{\binom{2m}{m}\binom{2n}{n}}{\binom{m+n}{n}} \in \mathbb{N}, \quad \textbf{(2)}\ \frac{(2m)!(3n)!}{(m!)^2(n!)^3} \in \mathbb{N}, \quad \textbf{(3)}\ \frac{(n!)!}{n!^{(n-1)!}} \in \mathbb{N}, \quad \textbf{(4)}\ C_n := \frac{\binom{2n}{n}}{n+1} \in \mathbb{N}.$$

[Teza **(1)** nazywa się ***Twierdzeniem Catalana***, a liczba C_n nazywa się **liczbą Catalana**.]

ZADANIE 2.A13 Dane są takie liczby całkowite $A_1, A_2, \ldots, A_s$ i $B_1, B_2, \ldots, B_s$, że dla każdej liczby naturalnej m zachodzi nierówność

$$\operatorname{card}\{t : 1 \leqslant t \leqslant s,\ m|B_t\} \leqslant \operatorname{card}\{t : 1 \leqslant t \leqslant s,\ m|A_t\}. \tag{2.31}$$

Udowodnić, że wówczas $B_1B_2 \cdot \ldots \cdot B_s | A_1A_2 \cdot \ldots \cdot A_s$.

ZADANIE 2.A14 Dane są dowolne liczby całkowite $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Udowodnić, że liczba

$$L := \prod_{1 \leqslant k < l \leqslant n} \frac{a_l - a_k}{l - k} \tag{2.32}$$

jest liczbą całkowitą.

B. NWD i NWW

ZADANIE 2.B1 Udowodnić, że jeżeli $a \neq b$ są liczbami naturalnymi, to $\operatorname{NWD}(a, b) \leqslant \frac{a+b}{3}$.

ZADANIE 2.B2 Niech $a, b \in \mathbb{N}$. Udowodnić, że $\operatorname{NWD}(a + b, \operatorname{NWW}(a, b)) = \operatorname{NWD}(a, b)$.

ZADANIE 2.B3 Udowodnić, że dla dowolnych $a, b, c \in \mathbb{Z}_{\neq 0}$ zachodzi równość

$$\frac{\operatorname{NWW}(a^2, b^2, c^2)}{\operatorname{NWW}(a, b) \cdot \operatorname{NWW}(b, c) \cdot \operatorname{NWW}(c, a)} = \frac{\operatorname{NWD}(a^2, b^2, c^2)}{\operatorname{NWD}(a, b) \cdot \operatorname{NWD}(b, c) \cdot \operatorname{NWD}(c, a)}.$$

ZADANIE 2.B4 Liczby naturalne a_n, b_n wyznaczamy z równości $a_n + b_n\sqrt{2} = (1 + \sqrt{2})^n$, dla wszystkich $n \in \mathbb{N}$. Wyznaczyć $\operatorname{NWD}(a_n, b_n)$.

ZADANIE 2.B5 Udowodnić, że dla liczb naturalnych $m \leqslant n$ zachodzi $n|\binom{n}{m}\operatorname{NWD}(m, n)$.

ZADANIE 2.B6 Niech $p > 2$ będzie liczbą pierwszą i niech a, b będą liczbami naturalnymi względnie pierwszymi. Wykazać, że liczba $\operatorname{NWD}(a + b, a^{p-1} - a^{p-2}b + \ldots - ab^{p-2} + b^{p-1})$ dzieli p.

ZADANIE 2.B7 Dowieść, że $n! = \prod_{k=1}^{n} \operatorname{NWW}(1, 2, \ldots, \lfloor n/k \rfloor)$ dla dowolnego $n \in \mathbb{N}$.

ZADANIE 2.B8 Wykazać, że istnieje nieskończenie wiele takich par (m, n) liczb naturalnych, dla których zachodzi równość $\operatorname{NWD}(m^2 + 1, n^2 + 1) = m + n$.

ZADANIE 2.B9 Niech $a \in \mathbb{N}_{\geqslant 2}$. Dowieść, że dla dowolnych $m, n \in \mathbb{N}$ zachodzi równość:

$$\boxed{\boxed{\operatorname{NWD}(a^m - 1, a^n - 1) = a^{\operatorname{NWD}(m,n)} - 1.}}$$

ZADANIE 2.B10 Ciąg $(a_n)_{n \geqslant 1}$ o wyrazach z $\mathbb{N}$ spełnia warunek $\operatorname{NWD}(a_k, a_l) = \operatorname{NWD}(k, l)$ dla dowolnych $k \neq l$. Uzasadnić, że $a_n = n$ dla każdego $n \in \mathbb{N}$.

ZADANIE 2.B11 Dowieść, że jeśli $k_1 < k_2 < \cdots < k_n \in \mathbb{N}$, to $\operatorname{NWW}(k_1, k_2, \ldots, k_n) \geqslant nk_1$.

ZADANIE 2.B12 Funkcja $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ spełnia warunki:

$$(1)\ f(x, x) = x; \quad (2)\ f(x, y) = f(y, x); \quad (3)\ f(x, y + x) = f(x, y)$$

dla dowolnych x, y. Udowodnić, że $f(m,\,n) = \mathrm{NWD}\,(m,\,n)$ dla dowolnej pary $(m,\,n) \in \mathbb{N} \times \mathbb{N}$.

ZADANIE 2.B13 Niech $0 < k \leqslant n$ będą liczbami całkowitymi. Udowodnić, że największy wspólny dzielnik liczb $\binom{n}{k}$, $\binom{n+1}{k}, \ldots, \binom{n+k}{k}$ jest równy 1.

ZADANIE 2.B14 Dane są takie liczby naturalne $a_1 < a_2 < \cdots < a_n \leqslant 1951$, że dla każdej pary $1 \leqslant i < j \leqslant n$ zachodzi nierówność $\mathrm{NWW}\,(a_i,\,a_j) > 1951$. Udowodnić, że $\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n} < 2$.

C. Dzielniki i złożoność liczb

ZADANIE 2.C1 Załóżmy, że $p < q$ są dwiema k o l e j n y m i liczbami pierwszymi nieparzystymi. Udowodnić, że liczba $p+q$ ma co najmniej trzy (niekoniecznie różne) dzielniki pierwsze.

ZADANIE 2.C2 Udowodnić, że następujące liczby są złożone (w **(3)** dla każdego $n \geqslant 2$):

$$\textbf{(1)}\quad 3^{2012} + 4^{2013}, \qquad \textbf{(2)}\quad \frac{5^{125}-1}{5^{25}-1}, \qquad \textbf{(3)}\quad f(n) := n^{2012} + n^{2011} + 1, \qquad \textbf{(4)}\quad T_n := 3^{3^n} + 1,$$

przy czym T_n ma co najmniej $2n+1$ (niekoniecznie różnych) dzielników pierwszych.

ZADANIE 2.C3 Udowodnić, że dla danej $n \in \mathbb{N}$, w przedziale $[\,\sqrt{n};\,\sqrt{n} + \sqrt[4]{n}\,]$ znajdzie się co najwyżej jeden dzielnik liczby n.

ZADANIE 2.C4 Dane są a, $d \in \mathbb{N}$, $a \geqslant 2$. Udowodnić, że liczba $a^{2d} - 1$ ma te same dzielniki pierwsze co liczba $a^d - 1$ wtedy i tylko wtedy, gdy $d = 1$ oraz $a = 2^r - 1$ przy pewnym r.

ZADANIE 2.C5 Dane są takie k, m, $n \in \mathbb{N}$, że $m \leqslant n$ i $m | n^k$. Dowieść, że $m^{m^m} | n^{n^n}$.

ZADANIE 2.C6 Załóżmy, że k, $a \in \mathbb{N}_{\geqslant 2}$. Dowieść, że jeżeli liczby $a^k - 1$ i $a - 1$ mają dokładnie te same dzielniki pierwsze, to $k = 2$ oraz $a = M_r$ (l. Mersenne'a) dla pewnego $r \in \mathbb{N}$.

ZADANIE 2.C7 Liczbę naturalną n nazywa się **liczbą Nováka**, gdy $n | 2^n + 1$. Udowodnić, że
(1) jeżeli n jest liczbą Nováka, to $2^n + 1$ również jest liczbą Nováka;
(2) NWD i NWW dwóch liczb Nováka jest liczbą Nováka;
(3) jeżeli n jest liczbą Nováka, $p \in \mathbb{P}$ i $p | 2^n + 1$, to np jest liczbą Nováka;
(4) iloczyn liczb Nováka jest liczbą Nováka;
(5) istnieje liczba Nováka mająca dokładnie 2017 dzielników pierwszych.

D. Kwadraty i inne potęgi

ZADANIE 2.D0 Udowodnić, że ani suma $x^2 + y^2$ dwóch kwadratów liczb nieparzystych, ani suma $x^2 + y^2 + z^2$ trzech kwadratów liczb nieparzystych n i e jest kwadratem (liczby całkowitej). Dowieść istnienia nieskończenie wielu takich czwórek x, y, u, w różnych nieparzystych liczb całkowitych, że liczba $x^2 + y^2 + u^2 + w^2$ jest kwadratem.

ZADANIE 2.D1 Liczba $n \in \mathbb{N}$ zapisana jest w systemie dziesiętnym za pomocą 30 cyfr równych 0 lub 6. Czy n może być kwadratem?

ZADANIE 2.D2 Czterocyfrowa (w systemie dziesiętnym) liczba naturalna $(aabb)_{10}$ jest kwadratem. Wyznaczyć cyfry a i b.

ZADANIE 2.D3 Udowodnić, że jeżeli $a^2 + a = 3b^2$ dla a, $b \in \mathbb{N}$, to $a + 1$ jest kwadratem.

ZADANIE 2.D4 Wyznaczyć wszystkie liczby naturalne n, dla których:
(1) liczba $4^n - 3^n$ jest kwadratem (liczby całkowitej);
(2) liczba $5^n - 3^n$ jest kwadratem (liczby całkowitej).

ZADANIE 2.D5 Liczby naturalne $T_n = n(n+1)/2$ nazywają się **liczbami trójkątnymi**. Udowodnić, że istnieje nieskończenie wiele liczb trójkątnych będących kwadratami (liczb całkowitych).

ZADANIE 2.D6 Udowodnić, że iloczyn dwóch, ani trzech, ani czterech kolejnych liczb naturalnych nie jest kwadratem.

ZADANIE 2.D7 Udowodnić, że jeżeli różnica dwóch kolejnych sześcianów liczb naturalnych jest kwadratem liczby naturalnej m, to m jest sumą dwóch kolejnych kwadratów liczb naturalnych.

ZADANIE 2.D8 Udowodnić, że liczba $V_n := 2^n + 1$, przy $n \in \mathbb{N}$, jest właściwą[7] potęgą liczby naturalnej wtedy i tylko wtedy, gdy $n = 3$.

ZADANIE 2.D9 Udowodnić, że liczba Mersenne'a $M_m := 2^m - 1$, przy $m \geqslant 2$, nie jest właściwą potęgą liczby naturalnej.

ZADANIE 2.D10 Wyznaczyć wszystkie takie pary (x, y) liczb naturalnych, że liczby $x^2 + 5y$ i $y^2 + 5x$ są kwadratami.

ZADANIE 2.D11 Dana jest liczba pierwsza $p > 2$ i takie liczby naturalne $x, y \leqslant (p-1)/2$, że iloczyn $x(p-x)y(p-y)$ jest kwadratem. Udowodnić, że $x = y$.

ZADANIE 2.D12 Czy istnieją takie liczby naturalne x, y, że liczby $x + 2y$, $5x + 13y$, $7x + 11y$ są kwadratami?

E. Równania diofantyczne

ZADANIE 2.E1 Udowodnić, że równanie: **(1)** $14x^2 + 197xy + 14y^2 = 2^z$ nie ma rozwiązań w liczbach całkowitych x, y, z; **(2)** $y^2 = x^5 + 4$ nie ma rozwiązań w liczbach naturalnych nieparzystych.

ZADANIE 2.E2 Dowieść, że jeżeli $a, b, c, n \in \mathbb{N}$ i $a^n + b^n = c^n$, to $\min\{a, b\} \geqslant n$.

ZADANIE 2.E3 Udowodnić, że równanie $x^3 + y^4 = z^5$ ma nieskończenie wiele rozwiązań w liczbach naturalnych x, y, z.

ZADANIE 2.E4 Udowodnić, że dla każdej liczby naturalnej n istnieje taka liczba naturalna m, że zachodzi równość $(\sqrt{2}-1)^n = \sqrt{m} - \sqrt{m-1}$.

F. Liczby pierwsze, jednoznaczność rozkładu

ZADANIE 2.F1 Wyznaczyć wszystkie takie:
(1) liczby pierwsze p, dla których $2p + 1$ i $4p + 1$ są liczbami pierwszymi;
(2) liczby pierwsze p, dla których $4p^2 + 1$ i $6p^2 + 1$ są liczbami pierwszymi;
(3) trójki (p, q, r) kolejnych liczb pierwszych, dla których $p^2 + q^2 + r^2$ jest liczbą pierwszą;
(4) liczby naturalne n, że para $(2^n - 1, 2^n + 1)$ jest parą liczb pierwszych bliźniaczych.

ZADANIE 2.F2 Niech $\gamma(n) = \mathrm{card}\{p \in \mathbb{P} : p|n\}$ (czyli $\gamma(n)$ oznacza liczbę różnych dzielników pierwszych liczby naturalnej n, na przykład $\gamma(1) = 0$, $\gamma(p) = 1$, itp.). Udowodnić, że dla każdego $m \in \mathbb{N}$ istnieją takie liczby $k, l \in \mathbb{N}$, że $m = k - l$ i $\gamma(k) = \gamma(l)$.

ZADANIE 2.F3 Załóżmy, że wszystkie wyrazy ciągu arytmetycznego $q, q + r, \ldots, q + (n-1)r$ są liczbami pierwszymi. Udowodnić, że różnica r tego ciągu jest podzielna przez iloczyn wszystkich liczb pierwszych $p < n$.

ZADANIE 2.F4 Udowodnić, że dla $n \in \mathbb{N}$ zachodzi nierówność $\sqrt[n]{n!} \leqslant \prod_{p \leqslant n} p^{1/(p-1)}$.

ZADANIE 2.F5 Niech $(p_1, p_2, p_3, \ldots) = (2, 3, 5, \ldots)$ będzie ciągiem wszystkich (ustawionych rosnąco) liczb pierwszych. Udowodnić, że dla każdego $n \geqslant 4$ zachodzi ***nierówność Bonse***

$$p_{n+1} < \sqrt{p_1 p_2 \cdot \ldots \cdot p_n}. \tag{2.33}$$

ZADANIE 2.F6 Liczby całkowite a_i spełniają nierówności $1 < a_1 < a_2 < \cdots < a_n < 2a_1$. Udowodnić, że jeżeli m jest liczbą różnych dzielników pierwszych iloczynu $a_1 a_2 \cdot \ldots \cdot a_n$, to zachodzi nierówność $(a_1 a_2 \cdot \ldots \cdot a_n)^{m-1} \geqslant (n!)^m$.

ZADANIE 2.F7 Wykazać, że zbiór $\mathbb{N}$ można przedstawić w postaci sumy pięciu parami rozłącznych podzbiorów o następującej własności: każda piątka liczb $n, 2n, 3n, 4n, 5n$, gdzie $n \in \mathbb{N}$, zawiera po jednej liczbie z każdego z tych pięciu podzbiorów.

[7] Potęgę x^m liczby całkowitej x nazywamy **właściwą** (ang. *perfect power*), gdy $m \in \mathbb{N}_{\geqslant 2}$.

ZADANIE 2.F8 Dane są nieparzyste liczby pierwsze $r < s$. Dowieść, że liczba $M_{rs} := 2^{rs} - 1$ ma co najmniej 3 różne dzielniki pierwsze.

G. Liczby bezkwadratowe

ZADANIE 2.G1 Udowodnić, że istnieje nieskończenie wiele takich liczb naturalnych bezkwadratowych n, że liczby $n+1$, $n+2$ również są bezkwadratowe.

ZADANIE 2.G2 Udowodnić, że każda liczba naturalna $n > 1$ da się przedstawić w postaci sumy dwóch liczb naturalnych bezkwadratowych.

H. Zadania addytywne

ZADANIE 2.H1 Udowodnić, że liczba naturalna m jest sumą dwóch kwadratów (liczb całkowitych) wtedy i tylko wtedy, gdy liczba $2m$ jest sumą dwóch kwadratów (liczb całkowitych).

ZADANIE 2.H2 Udowodnić, że jeżeli liczba naturalna n jest sumą trzech kwadratów liczb naturalnych, to również liczba n^2 jest sumą trzech kwadratów liczb naturalnych.

ZADANIE 2.H3 Udowodnić, że potęga 2^n $(n \in \mathbb{N})$ nie da się przedstawić w postaci sumy dwóch czy więcej kolejnych liczb naturalnych, a każda liczba naturalna nie będąca naturalną potęgą dwójki da się przedstawić w postaci takiej sumy.

ZADANIE 2.H4 Udowodnić, że każda liczba całkowita daje się na nieskończenie wiele sposobów przedstawić w postaci $\pm 1^2 \pm 2^2 \pm \cdots \pm m^2$, gdzie $m \in \mathbb{N}$, a znaki $+$, $-$ są odpowiednio dobrane.

ZADANIE 2.H5 Udowodnić, że każda liczba całkowita daje się (na nieskończenie wiele sposobów) przedstawić w postaci sumy pięciu sześcianów liczb całkowitych.

ZADANIE 2.H6 Dana jest liczba naturalna n. Udowodnić, że dla każdej liczby naturalnej $a < n!$ istnieją takie (dodatnie) dzielniki $d_1 < \cdots < d_s$ liczby $n!$, że $a = d_1 + \cdots + d_s$ i $s \leqslant n$.

I. Cztery zastosowania LZW

ZADANIE 2.I1 Niech $p \in \mathbb{P}$ i $a, n \in \mathbb{N}$. Udowodnić, że jeżeli $2^p + 3^p = a^n$, to $n = 1$.

ZADANIE 2.I2 Liczbę $n \in \mathbb{N}$ nazwiemy *ciekawą*, gdy $n | 1^n + 2^n + \cdots + 8^n$. Udowodnić, że istnieje nieskończenie wiele *ciekawych* liczb naturalnych.

ZADANIE 2.I3 Dane są takie różne liczby rzeczywiste x, y, że wszystkie liczby $x^n - y^n$, dla $n \in \mathbb{N}$, są liczbami całkowitymi. Dowieść, że $x, y \in \mathbb{Z}$.

ZADANIE 2.I4 Udowodnić, że jeżeli $(x, y; m, n)$ jest czwórką Catalan'a (zobacz rozwiązanie Z2.D8), w której y jest liczbą pierwszą, to $(x, y; m, n) = (3, 2; 2, 3)$.

2.6.2 Wskazówki i rozwiązania

Pokazujemy rozwiązania/wskazówki wszystkich zadań.

Z2.A0 (IMO'59) Zobacz równość $3(14n + 3) - 2(21n + 4) = 1$.

Z2.A1 Niech $L := 3\,000\,003$ i $A(x, y) := 10^4 x + 10^2 y$. Zadanie polega na wyznaczeniu wszystkich par (x, y) liczb naturalnych z przedziału $[0; 9]$, dla których $13 | L + A(x, y)$. Dzielimy więc z resztą przez 13. Mamy: $L = 13 \cdot 230\,769 + 6$, $10^4 = 13 \cdot 769 + 3$ i $10^2 = 13 \cdot 7 + 9$. To daje równość $L + A(x, y) = 13(230\,769 + 769x + 7y) + 6 + 3x + 9y$, z której widzimy, że $13 | L + A(x, y)$ wtedy i tylko wtedy, gdy $13 | 3(2 + x + 3y)$. To z kolei, na mocy ZTA, zachodzi wtedy i tylko wtedy, gdy $13 | 2 + x + 3y$. Ponieważ $0 \leqslant x, y \leqslant 9$, więc ostatnia podzielność może mieć miejsce tylko gdy $2 + x + 3y = 13$ lub $2 + x + 3y = 26$. Musimy więc rozwiązać równania $x + 3y = 11$ i $x + 3y = 24$. Wobec "małości" występujących liczb nie musimy przywoływać twierdzenia T2.12. Znajdujemy rozwiązania: $(x, y) = (0, 8)$, $(2, 3)$, $(3, 7)$, $(5, 2)$, $(6, 6)$, $(8, 1)$ i $(9, 5)$.

Z2.A2 (1) Równość $13(3x+4y) = 2x+15y+37(x+y)$, Zasada Podstawowa i ZTA pozwalają natychmiast uzasadnić żądaną równoważność. **(2)** Patrz na równość: $(x^3+y^3+z^3)-(x+y+z) = x(x-1)(x+1)+y(y-1)(y+1)+z(z-1)(z+1)$ i zauważ, że liczba $u(u-1)(u+1)$, jako iloczyn trzech k o l e j n y c h liczb całkowitych, jest podzielna przez 2 i 3, więc, zobacz C2.17, też przez 6.

Z2.A3 Mamy równość $k^2(100l^2-1)^2-l^2(100k^2-1)^2 = (l^2-k^2)(100kl-1)(100kl+1)$. Stosujemy Zasadę Podstawową i, po zauważeniu względnej pierwszości $k^2 \perp 100kl-1$, korzystamy z ZTA.

Z2.A4 Jeżeli $11 \nmid x$, to istnieją takie liczby całkowite u, v, że $xu+11v = 1$, zobacz C2.32 i T2.6. Wobec tego równość $x^2+y^2 = 11a$ daje $(xu)^2+(yu)^2 = 11au^2$, czyli $(1-11v)^2+(yu)^2 = 11au^2$, więc $11|1+(yu)^2$. Teraz trzeba zobaczyć jakie reszty z dzielenia przez 11 dają kwadraty. Robimy to tak: każda liczba całkowita jest jednej z postaci $11s$, $11s\pm1$, $11s\pm2$, $11s\pm3$, $11s\pm4$ lub $11s\pm5$. Ich kwadraty są równe odpowiednio: $11S$, $11S+1$, $11S+4$, $11S+9$, $11S+5$ lub $11S+3$. Wobec tego $1+(yu)^2$ daje jedną z reszt 1, 2, 5, 10, 6 lub 4 przy dzieleniu przez 11. Nie jest więc podzielna przez 11. Znaleziona sprzeczność kończy rozwiązanie. U w a g a. Udowodniona teza jest przypadkiem szczególnym tezy ogólniejszej: *Jeżeli p jest liczbą pierwszą postaci $4k+3$ i $p|x^2+y^2$ dla pewnych liczb całkowitych x, y, to $p|x$ i $p|y$.* Po zapoznaniu się z elementami teorii reszt kwadratowych modulo p (zob. rozdział 5) Czytelnik z łatwością udowodni tę tezę, jak również będzie rozumiał wagę założenia $p = 4k+3$ (przecież, na przykład, $5|7^2+4^2$ ale $5 \nmid 7$ i $5 \nmid 4$).

Z2.A5 Rozstrzygającą jest tu uwaga, że jeżeli liczba całkowita x nie jest podzielna przez 5, to jej kwadrat x^2 daje resztę 1 lub 4 przy dzieleniu przez 5. Gdyby więc, żadna z liczb a, b, c nie była podzielna przez 5, to co najmniej dwie z liczb a^2, b^2, c^2 dawałyby przy dzieleniu przez 5 tę samą resztę (1 lub 4). Ich suma dawałaby wtedy resztę 2 lub 3, nie mogłaby więc być kwadratem. Czytelnik mógłby zechcieć podobnie uzasadnić, że w badanej sytuacji *co najmniej jedna z liczb a, b, c jest podzielna przez* 11.

Z2.A6 Korzystamy z C2.41. Niech $v_p(a) = s$, $v_p(b) = t$, $v_p(c) = u$ i $v_p(m) = r$ dla danej (dowolnej) liczby pierwszej p. Załóżmy (b.s.o.), że $s \leqslant t \leqslant u$. Teza zadania jest więc równoważna nierówności $r \leqslant s$. Zakładamy, nie wprost, że $s < r$. Założenie $m^3|abc$ daje nierówność $3r \leqslant s+t+u$, skąd $r \leqslant u$. Mamy więc $s < r \leqslant u$. Wówczas, zobacz C2.43.2, $r \leqslant v_p(a+c) = \min\{s, u\} = s < r$ (pierwsza nierówność wynika z założenia $m|a+c$). Otrzymana sprzeczność kończy rozwiązanie.

Z2.A7 (1) Zapisz $n^5+5 = n^5+5^5-5^5+5$. Wykorzystaj tożsamość *nieśmiertelną* (1.8) dla dowodu, że $n+5|n^5+5^5$. Powołaj się na Zasadę Podstawową. **(2)** Oznacz $a_n = 5^n+7^n$. Wtedy $a_n = (5^{n-1}+7^{n-1})(5+7)-5\cdot7^{n-1}-7\cdot5^{n-1}$, czyli $a_n = 12a_{n-1}-35a_{n-2}$ dla wszystkich $n \geqslant 2$. Podzielność $a_{n-1}|a_n$ daje więc podzielność $a_{n-1}|35a_{n-2}$. Ale $a_{n-1} \perp 35$ (sprawdź!), więc, na mocy ZTA, $a_{n-1}|a_{n-2}$. Nonsens, bo $a_{n-1} > a_{n-2}$. Pozostaje więc tylko $n = 1$.

Z2.A8 Rozważymy osobno przypadki: (1) $n = 2a$, (2) $n = 2a+1$. W przypadku (1) liczba $1+\cdots+n$ jest równa $a(2a+1)$. Ponieważ liczby a i $2a+1$ są względnie pierwsze, więc, wobec C2.17, wystarczy uzasadnić podzielności $a|1^k+\cdots+(2a)^k$ i $(2a+1)|1^k+\cdots+(2a)^k$. To łatwo uzasadnić wykorzystując "nieparzystą" wersję tożsamości nieśmiertelnej i odpowiednie pogrupowanie składników. Mianowicie, równość $x^k+y^k = (x+y)(x^{k-1}-x^{k-2}y+\cdots-xy^{k-2}+y^{k-2})$ zachodząca dla dowolnych liczb (w rzeczywistości, elementów dowolnego pierścienia przemiennego) x, y i n i e p a r z y s t e g o k pokazuje podzielność $(x+y)|x^k+y^k$. Stąd, grupując składniki sumy $\sum_{s=1}^{2a} s^k$, pierwszy z ostatnim, drugi z przedostatnim, itd., dostajemy podzielność tej sumy przez $2a+1$, zaś grupując pierwszy z przedostatnim, drugi z przedprzedostatnim, itd., znajdujemy $a-1$ sumek podzielnych przez $2a$ oraz dwa wyrazy a^k i $(2a)^k$ podzielne przez a i, ostatecznie, podzielność sumy $\sum_{s=1}^{2a} s^k$ przez a. W przypadku (2) postępujemy podobnie.

Z2.A9 Sprawdź najpierw, że liczby a, b, c są p a r a m i względnie pierwsze. Zauważ następnie, że liczba $N := ab+bc+ca+1$ jest podzielna przez każdą z liczb a, b, c. Wywnioskuj z C2.17, że

$abc|N$, i z C2.2, że $abc \leqslant N$. Teraz już musisz porzucić arytmetykę (teorię podzielności) na rzecz analizy (w tym przypadku – nierówności): widać bowiem, że liczba abc jest rzędu wielkości b^3, a liczba N rzędu wielkości $3b^2$, więc już przy $b \geqslant 4$ możesz się spodziewać sprzeczności. Rzeczywiście, gdy $b \geqslant 4$, to $c \geqslant 5$ i, wobec tego,

$$N = ab + bc + ca + 1 = \frac{abc}{c} + \frac{abc}{a} + \frac{abc}{b} + 1 \leqslant \frac{abc}{5} + \frac{abc}{2} + \frac{abc}{4} + 1 < abc.$$

Pozostaje Ci sprawdzić przypadek, gdy $b = 3$ i $a = 2$.

Z2.A10 Załóż, nie wprost, że $a^n + b^n = q(a^n - b^n)$ dla pewnego $q \in \mathbb{Z}$. Dostaniesz równość $(q+1)b^n = (q-1)a^n$. Nie tracąc ogólności rozważań, załóż też, że $a \perp b$ (gdyby tak nie było, podziel wszystko przez d^n, gdzie $d = \mathrm{NWD}\,(a, b)$, i zastosuj C2.12). Wykorzystaj ZTA. Otrzymasz równości $q+1 = a^n k$, $q-1 = b^n k$ dla pewnego $k \in \mathbb{Z}$. Odejmij stronami. Dostaniesz $2 = (a^n - b^n)k$. Wywnioskuj stąd, że $|a^n - b^n| \leqslant 2$. Teraz przyglądnij się dobrze ciągowi (1, 4, 9, 16, ...) kwadratów, ciągowi (1, 8, 27, 64, ...) **sześcianów**, ciągowi (1, 16, 81, 256, ...) **bikwadratów**, itd.

Z2.A11 (IMO'98) $b(a^2b+a+b) - a(ab^2+b+7) = b^2 - 7a$, więc podzielność $(ab^2+b+7)|(a^2b+a+b)$ implikuje podzielność $(ab^2+b+7)|(b^2-7a)$. Rozważamy osobno trzy przypadki: (1) $b^2 - 7a < 0$, (2) $b^2 - 7a > 0$, (3) $b^2 - 7a = 0$. W przypadku (1) mamy $ab^2 + b + 7 \leqslant |b^2 - 7a| = 7a - b^2$ (zobacz C2.2). Taka nierówność, wobec dodatniości a, b, jest możliwa tylko, gdy $b^2 < 7$, czyli gdy zachodzi jeden z podprzypadków: (i) $b = 1$ lub (ii) $b = 2$. W podprzypadku (i) badamy podzielność $(a+8)|(a^2+a+1)$, czyli podzielność $(a+8)|(a(a+8) - 7(a+8) + 57)$, więc podzielność $(a+8)|57$. Ponieważ $57 = 3 \cdot 19$, więc to może zachodzić tylko dla $a = 11$ i $a = 49$. Sprawdzamy, że pary $(a, b) = (11, 1), (49, 1)$ są dobre. W podprzypadku (ii) badamy podzielność $(4a+9)|(4-7a)$, czyli podzielność $(4a+9)|(4-7a+2(4a+9))$, więc $(4a+9)|(a+22)$. Taka podzielność implikowałaby nierówność $4a + 9 \leqslant a + 22$, która (dla $a \in \mathbb{N}$) jest możliwa tylko gdy $a = 1, 2, 3, 4$. Jednakże dla żadnej z tych wartości a nie zachodzi podzielność. W przypadku (2), znowu na mocy C2.2, dostajemy nieprawdziwą (dla liczb naturalnych!) nierówność $ab^2 + b + 7 \leqslant b^2 - 7a$. Pozostał do rozważenia przypadek (3). Wówczas $b^2 = 7a$, skąd $7|b$, czyli $b = 7c$, więc $a = 7c^2$. Łatwo widzieć, że pary $(a, b) = (7c^2, 7c)$, przy dowolnym $c \in \mathbb{N}$, spełniają warunki.

Z2.A12 (1) Sprowadź tezę do nierówności $\lfloor 2x \rfloor + \lfloor 2y \rfloor - \lfloor x + y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \geqslant 0$ dla dowolnych $x, y \in \mathbb{Q}_{\geqslant 0}$ (zob. C2.48, 47 i T2.17). W przypadku trudności, zob. ustęp 12.1.1; **(2)** Podobnie jak przed chwilą sprowadź tezę do nierówności $\lfloor 2x \rfloor + \lfloor 3y \rfloor - 2\lfloor x \rfloor - 3\lfloor y \rfloor \geqslant 0$; **(3)** Podobnie jak przed chwilą sprowadź tezę do nierówności $\lfloor (n-1)! \cdot n/p^s \rfloor - (n-1)!\lfloor n/p^s \rfloor \geqslant 0$; **(4)** Najprostsze rozwiązanie wynika z równości $\frac{1}{n+1}\binom{2n}{n} = 2\binom{2n}{n} - \binom{2n+1}{n+1}$. Eleganckie (kombinatoryczne) rozwiązanie znaleźć można w $\mathbb{KOM}$. Arytmetyczne (za pomocą C2.48) rozwiązanie jest też możliwe!

Z2.A13 Wystarczy udowodnić nierówność $(*)$ $v_p(B_1B_2 \cdot \ldots \cdot B_s) \leqslant v_p(A_1A_2 \cdot \ldots \cdot A_s)$ dla dowolnej liczby pierwszej p, zob. C2.41. Ustalmy więc liczbę $p \in \mathbb{P}$ i zapiszmy $A_t = p^{k_t}A'_t$, $B_t = p^{l_t}B'_t$ dla $t = 1, 2, \ldots, s$, gdzie A'_t i B'_t są względnie pierwsze z p. Przestawiając ewentualnie czynniki możemy uznać, że $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_s$ i $l_1 \geqslant l_2 \geqslant \ldots \geqslant l_s$. Przyjmując kolejno $m = p^{l_1}, p^{l_2}, \ldots, p^{l_s}$, sprawdzamy, dzięki założeniu (2.31), że $k_1 \geqslant l_1$, $k_2 \geqslant l_2$, ..., $k_s \geqslant l_s$. Stąd $k_1 + k_2 + \ldots + k_s \geqslant l_1 + l_2 + \ldots + l_s$, co, na mocy C2.43.1, dowodzi nierówności $(*)$ i kończy rozwiązanie.

Z2.A14 Sposób 1. Korzystamy z Z2.A13. Iloczyn (2.32) ma $s := \binom{n}{2} = \frac{n(n-1)}{2}$ czynników. Niech $A_1, A_2, \ldots, A_s$ oznaczają (dowolnie ustawione w ciąg) liczniki $a_l - a_k$ czynników tego iloczynu, zaś $B_1, B_2, \ldots, B_s$ oznaczają odpowiednie mianowniki $l - k$. Ustalmy teraz dowolną liczbę naturalną m. Twierdzimy, że liczby całkowite A_t i B_t spełniają nierówności (2.31). Aby to udowodnić oznaczmy przez n_r moc zbioru tych indeksów i, dla których wyraz a_i przy dzieleniu przez m daje resztę r. Tu r przebiega zbiór możliwych reszt, czyli $r \in \{0, 1, \ldots, m-1\}$. Jasne, że $m|a_l - a_k$ wtedy i tylko wtedy, gdy a_l i a_k dają tę samą resztę z dzielenia przez m. Stąd wynika, że ilość par (k, l), dla

których $m|a_l - a_k$, czyli liczba stojąca po prawej stronie (2.31), równa jest

$$\binom{n_0}{2} + \binom{n_1}{2} + \ldots + \binom{n_{m-1}}{2} = \frac{n_0^2 + n_1^2 + \ldots + n_{m-1}^2 - n}{2}, \tag{2.34}$$

bo $n_0 + n_1 + \ldots + n_{m-1} = n$. Aby wyznaczyć liczbę stojącą z lewej strony nierówności (2.31), zapiszmy $n = qm + r$, gdzie $0 \leqslant r < m$ i rozważmy następujące podzbiory zbioru $\{1, 2, \ldots, n\}$:

$$\begin{gathered}
\mathcal{X}_1 = \{1, m+1, 2m+1, \ldots, qm+1\}, \\
\ldots \quad \ldots \quad \ldots \\
\mathcal{X}_r = \{r, m+r, 2m+r, \ldots, qm+r\}, \\
\mathcal{X}_{r+1} = \{r+1, m+r+1, 2m+r+1, \ldots, (q-1)m+r+1\}, \\
\ldots \quad \ldots \quad \ldots \\
\mathcal{X}_m = \{m, 2m, \ldots, qm\}.
\end{gathered}$$

Każdy ze zbiorów $\mathcal{X}_1, \ldots, \mathcal{X}_r$ ma $q+1$ elementów dających stałą (w każdym zbiorze) resztę z dzielenia przez m. Każdy z pozostałych zbiorów $\mathcal{X}_{r+1}, \ldots, \mathcal{X}_m$ ma q elementów dających stałą (w każdym zbiorze) resztę z dzielenia przez m. Stąd widzimy, że liczba stojąca z lewej strony nierówności (2.28) jest równa $r\binom{q+1}{2} + (m-r)\binom{q}{2}$, czyli $rq + m\binom{q}{2}$. Aby zakończyć rozwiązanie wystarczy więc, dzięki Z2.A13 i równości (2.34), udowodnić, że

$$rq + m\binom{q}{2} \leqslant \frac{n_0^2 + n_1^2 + \ldots + n_{m-1}^2 - n}{2}.$$

Nierówność ta jest r ó w n o w a ż n a następującej nierówności: $\sum_{i=0}^{m-1}(n_i - q) \leqslant \sum_{i=0}^{m-1}(n_i - q)^2$, co wynika z równości $\sum_{i=0}^{m-1} n_i = n$ i $r = n - mq$ (sprawdzenie pozostawiamy Czytelnikowi). Ponieważ dla liczb całkowitych zachodzi oczywista nierówność $c \leqslant c^2$, więc wszystko jasne.

S p o s ó b 2. Skorzystamy teraz z elementarnej wiedzy dotyczącej wyznaczników, w szczególności tak zwanego **wyznacznika Vandermonde'a**. Czytelnik, który zna ten (skądinąd bardzo w a ż n y) wyznacznik, zauważył, że licznik, danej w (2.32), liczby L, jest równy wyznacznikowi (Vandermonde'a) $V(a_1, a_2, \ldots, a_n)$. Rzeczywiście:

$$V(x_1, x_2, \ldots, x_n) := \det[x_i^{j-1}]_{1 \leqslant i,\, j \leqslant n} = \prod_{1 \leqslant l < k \leqslant n} (x_k - x_l).$$

[Dowód (drugiej, bo pierwsza jest definicją!) równości jest prostym i sympatycznym zastosowaniem elementarnych własności wyznaczników (wystarczy to co można znaleźć w $\mathbb{KOM}$ 4.7.2) i indukcji matematycznej.] Wobec tego licznik liczby wymiernej L jest równy $V(a_1, a_2, \ldots, a_n)$, czyli

$$\det \begin{bmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ .. & .. & .. & \ldots & .. \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{bmatrix} \tag{2.35}$$

Z tej postaci, oczywiście, jeszcze nie widać, że ta liczba całkowita jest podzielna przez mianownik równy, jak łatwo widzieć, $1! \cdot 2! \cdot \ldots \cdot (n-1)!$. Korzystając z elementarnych (nie zmieniających wartości wyznacznika) operacji na kolumnach, znajdziemy postać wyznacznika (2.35), z której wszystko będzie jasne. W $\mathbb{KOM}$ znajdujemy (wygodne w kombinatoryce) oznaczenie tak zwanych **potęg malejących**: $X^{\underline{k}} := X(X-1) \cdot \ldots \cdot (X-k+1)$. Wymnażając dostaniemy równość

$$X^{\underline{k}} = s_0(k) + s_1(k)X + \ldots + s_k(k)X^k.$$

(W $\mathbb{KOM}$ 4.4.4 są nieco inne oznaczenia.) Mając to, mnożymy j-tą kolumnę wyznacznika (2.35), dla $j = 1, \ldots, (n-2)$, przez $s_{j-1}(n-1)$ i dodając do ostatniej (n-tej) kolumny, otrzymamy (równy(!) liczbowo) wyznacznik, który różni się od (2.35) tym, że w jego ostatniej kolumnie zamiast zwykłych potęg a_i^{n-1} stoją potęgi malejące $a_i^{\underline{n-1}}$. Podobnie postępujemy z kolumną $(n-1)$-szą, $(n-2)$-gą, itd. W wyniku dostaniemy wygodniejszą dla naszych celów postać wyznacznika (2.35):

$$\det \begin{bmatrix} 1 & a_1 & a_1^{\underline{2}} & \ldots & a_1^{\underline{n-1}} \\ 1 & a_2 & a_2^{\underline{2}} & \ldots & a_2^{\underline{n-1}} \\ .. & .. & .. & \ldots & .. \\ 1 & a_n & a_n^{\underline{2}} & \ldots & a_n^{\underline{n-1}} \end{bmatrix}$$

Bardzo łatwo bowiem podzielić ten wyznacznik przez mianownik $0!\cdot 1!\cdot\ldots\cdot(n-1)!$ liczby L, dzieląc wyrazy j-tej kolumny przez $(j-1)!$. Dostaniemy w ten sposób równość

$$L = \det \begin{bmatrix} \binom{a_1}{0} & \binom{a_1}{1} & \binom{a_1}{2} & \ldots & \binom{a_1}{n-1} \\ \binom{a_2}{0} & \binom{a_2}{1} & \binom{a_2}{2} & \ldots & \binom{a_2}{n-1} \\ .. & .. & .. & \ldots & .. \\ \binom{a_n}{0} & \binom{a_n}{1} & \binom{a_n}{2} & \ldots & \binom{a_n}{n-1} \end{bmatrix},$$

bowiem, porównaj $\mathbb{KOM}$, liczbę $\frac{1}{k!}x^{\underline{k}}$ wygodnie jest oznaczać symbolem $\binom{x}{k}$ dla dowolnej liczby x (a nie tylko dla liczb naturalnych x). Oczywiście, dla zakończenia rozwiązania trzeba wykazać jeszcze, że liczba $\binom{x}{k}$ jest liczbą całkowitą dla d o w o l n e j całkowitej liczby x. Zostawiamy to jako ćwiczenie dla Czytelnika (zob. również Z3.C1(1) oraz C12.43). Liczba L została w ten sposób zinterpretowana jako wyznacznik macierzy kwadratowej o wyrazach całkowitych. Więc $L \in \mathbb{Z}$.

Z2.B1 Oznacz $d = \mathrm{NWD}\,(a, b)$. Niech $a = da'$, $b = db'$. Ponieważ $a \neq b$, więc $a' \neq b'$. Zatem $a'+b' \geqslant 3$ (bo 3 jest najmniejszą sumą dwóch różnych liczb naturalnych). Stąd $a+b = d(a'+b') \geqslant 3d$. U w a g a. Tak samo można udowodnić uogólnienie: *Jeżeli liczby naturalne $a_1, \ldots, a_n$ są parami różne, to zachodzi nierówność* $\mathrm{NWD}\,(a_1, \ldots, a_n) \leqslant \frac{2}{n(n+1)}(a_1 + \cdots + a_n)$.

Z2.B2 Oznacz $d = \mathrm{NWD}\,(a, b)$ i połóż $a = da'$, $b = db'$. Masz więc wykazać, że zachodzi równość $\mathrm{NWD}\,(d(a'+b'), da'b') = d$ (zobacz T2.9), czyli $\mathrm{NWD}\,(a'+b', a'b') = 1$. Robisz to tak: jeżeli $k \in D(a'+b', a'b')$ i $k > 1$, to istnieje liczba pierwsza $p|k$ (zobacz T2.14). Wówczas $p|a'b'$, więc (b.s.o.) $p|a'$, oraz $p|a'+b'$, więc $p|b'$ (na mocy Zasady Podstawowej). Stąd dostaniesz: $p \in D(a', b')$. Ale to jest sprzeczne z względną pierwszością $a' \perp b'$, zobacz C2.12.

Z2.B3 Zapisz $|a| = \prod_i p_i^{\alpha_i}$, $|b| = \prod_i p_i^{\beta_i}$, $|c| = \prod_i p_i^{\gamma_i}$, zob. (RK) w 2.4.1. Dzięki C2.42, C2.47.1 sprowadź dowodzoną równość do równości $\max\{2\alpha_i, 2\beta_i, 2\gamma_i\} + \min\{\alpha_i, \beta_i\} + \min\{\beta_i, \gamma_i\} + \min\{\gamma_i, \alpha_i\} = \min\{2\alpha_i, 2\beta_i, 2\gamma_i\} + \max\{\alpha_i, \beta_i\} + \max\{\beta_i, \gamma_i\} + \max\{\gamma_i, \alpha_i\}$.

Z2.B4 Z równości $a_n + b_n\sqrt{2} = (1+\sqrt{2})^n = (1+\sqrt{2})(1+\sqrt{2})^{n-1} = (1+\sqrt{2})(a_{n-1} + b_{n-1}\sqrt{2})$ wywiedź równości $a_n = a_{n-1} + 2b_{n-1}$ i $b_n = a_{n-1} + b_{n-1}$ (m u s i s z wykorzystać niewymierność $\sqrt{2}$, zob. 1.1.1 P). Stąd dostaniesz natychmiast $a_n - 2b_n = -a_{n-1}$ i $a_n - b_n = b_{n-1}$. Załóż teraz, że $d \in D(a_n, b_n)$ (d jest wspólnym dzielnikiem). Dzięki udowodnionym związkom zobaczysz, że $d \in D(a_{n-1}, b_{n-1})$. Oczywista **indukcja wsteczna** pokazuje więc, że $d \in D(a_1, b_1)$. Ale $D(a_1, b_1) = \{1, -1\}$. I ostatecznie, $\mathrm{NWD}\,(a_n, b_n) = 1$ dla każdego $n \in \mathbb{N}$.

Z2.B5 Przedstaw $\mathrm{NWD}\,(m, n)$ w postaci kombinacji liniowej (o współczynnikach całkowitych) liczb m i n, zobacz (2.5). Możliwe jest też rozwiązanie za pomocą wzoru Legendre'a z T2.17 (!).

Z2.B6 Oznaczmy $k(X) = a + X$ i $l(X) = a^{p-1} - a^{p-2}X + a^{p-3}X^2 - \cdots + X^{p-1}$. Badamy więc największy wspólny dzielnik $d := \mathrm{NWD}\,(k(b), l(b))$. Rozważmy w tym celu wielomian $f(X) =$

$k(X)^{p-1} - l(X) + (-1)^s pa^s X^s$ zmiennej X o współczynnikach całkowitych, gdzie (dla uproszczenia) oznaczyliśmy $s = (p-1)/2$. Sprawdzenie, że $f(-a) = 0$, jest natychmiastowe. Wobec tego (tu korzystamy z twierdzenia Bézout'a, zobacz T3.2) istnieje taki wielomian $g(X)$ o współczynnikach całkowitych, że zachodzi równość $f(X) = (X+a)g(X)$. Kładąc tu $X = b$ dostajemy więc równość $k(b)^{p-1} - l(b) + (-1)^s pa^s b^s = k(b)g(b)$. Z tej równości, na mocy Zasady Podstawowej, widzimy, że $d|pa^s b^s$. Ale $d \perp a$ i $d \perp b$ (dlaczego?). Więc, na mocy ZTA, mamy tezę.

Z2.B7 Zauważ, że $v_p(\mathrm{NWW}\,(1, 2, \ldots, \lfloor n/k \rfloor)) = s$ iff $\lfloor n/p^{s+1} \rfloor < k \leqslant \lfloor n/p^s \rfloor$.

Z2.B8 Przetestuj liczby $m = a$, $n = a^2 - a + 1$, dla $a \in \mathbb{N}$. Możesz też "pobawić" się z (9.8).

Z2.B9 O ciągu $(a_n)_{n\in\mathbb{N}} = (a_1, a_2, \ldots)$ o wyrazach całkowitych mówimy, że

- ▷ ma **własność podzielności**, gdy $a_m | a_n$ dla wszystkich $m|n$;
- ▷ jest NWD**-ciągiem**, gdy $\mathrm{NWD}\,(a_m, a_n) = \pm a_{\mathrm{NWD}\,(m,n)}$ dla wszystkich m, n.

Mamy więc dowieść, że ciąg $(a^n - 1)_{n\in\mathbb{N}}$ jest NWD-ciągiem. Udowodnimy ogólniejsze:

T w i e r d z e n i e 1. *Jeżeli $a, b \in \mathbb{Z}$ i $a \perp b$, to ciąg $(u_n) = (a^n - b^n)$ jest* NWD*-ciągiem.*

D o w ó d. Pokazujemy najpierw, że: *ciąg $(u_n) = (a^n - b^n)$ ma własność podzielności.* To wynika z (1.8): jeżeli $n = qm$, to $u_n = (a^{m(q-1)} + a^{m(q-2)}b^m + \cdots + a^m b^{m(q-2)} + b^{m(q-1)})(a^m - b^m) =: cu_m$. Niech teraz $n = qm + r$, $0 \leqslant r < m$, będzie dzieleniem z resztą. Wtedy

$$u_n = a^n - b^n = b^r(a^{qm} - b^{qm}) + a^{qm}(a^r - b^r) = b^r u_{qm} + a^{qm} u_r = b^r c u_m + a^{qm} u_r.$$

Z tej równości natychmiast wynika zawieranie $D(u_m, u_r) \subseteq D(u_n, u_m)$ zbiorów wspólnych dzielników. Jest też odwrotnie: $D(u_n, u_m) \subseteq D(u_m, u_r)$. Rzeczywiście, jeżeli $d \in D(u_n, u_m)$, to $d | a^{qm} u_r$, więc, dzięki $d \perp a$ (uzasadnić!) i ZTA, $d|u_r$. Zatem $D(u_n, u_m) = D(u_m, u_r)$. Kontynuując algorytm Euklidesa dla pary n, m, dostajemy kolejno: $D(u_n, u_m) = D(u_m, u_r) = \cdots = D(u_d, 0) = D(u_d)$, gdzie $d = \mathrm{NWD}\,(n, m)$. Q.e.d.

U w a g a 1. *Każdy* NWD*-ciąg ma własność podzielności.* Rzeczywiście, $a|b$ wtedy i tylko wtedy, gdy $\mathrm{NWD}\,(a, b) = \pm a$. Jeżeli więc $m|n$, to $a_m = a_{\mathrm{NWD}\,(m,n)} = \pm\mathrm{NWD}\,(a_m, a_n)$, czyli $a_m | a_n$.

U w a g a 2. Zastanowimy się nad przypadkiem "plusowym", czyli nad ciągiem $(v_n) = (a^n + b^n)$. Taki ciąg na ogół n i e jest NWD-ciągiem, a nawet nie ma własności podzielności (Czytelnik zechce to przetestować na przykładzie ciągu $(V_n) = (2^n + 1)$). Możemy jednak udowodnić, że ma on następującą **własność nieparzystej podzielności**: *Jeżeli $m|n$ i n/m jest liczbą nieparzystą, to $v_m | v_n$.* To wynika z "plusowej" wersji tożsamości nieśmiertelnej, zob. 2.4.2 U: skoro $n = km$ i $2 \nmid k$, to $a^n + b^n = (a^m)^k + (b^m)^k = (a^m + b^m)Q_k(a^m, -b^m)$. Czasem korzystamy również z poniższego twierdzenia:

T w i e r d z e n i e 2. *Jeżeli $a, b \in \mathbb{Z}$, gdzie $a \perp b$, to dla n i e p a r z y s t y c h $m, n \in \mathbb{N}$ zachodzi równość* $\mathrm{NWD}\,(v_m, v_n) = \pm v_{\mathrm{NWD}\,(m,n)}$. *D o w ó d.* Niech $b_1 = -b$. Wówczas $a^k + b^k = a^k - b_1^k$, gdy $2 \nmid k$. Zatem, dla nieparzystych m, n: $D(a^n + b^n, a^m + b^m) = D(a^n - b_1^n, a^m - b_1^m) = D(a^d - b_1^d) = D(a^d + b^d)$, gdzie $d = \mathrm{NWD}\,(m, n)$. Druga równość wynika z Twierdzenia 1 (bo $a \perp b$ iff $a \perp b_1$), a trzecia z nieparzystości d (dzielnik liczby nieparzystej jest nieparzysty!). Q.e.d.

Z2.B10 Równości $\mathrm{NWD}\,(a_n, a_{ln}) = \mathrm{NWD}\,(n, ln) = n$ pokazują, że $n|a_n$ dla każdego $n \in \mathbb{N}$. Wywnioskuj stąd ogólnie równość zbiorów dzielników $D(a_n) = D(n)$ dla każdego $n \in \mathbb{N}$.

Z2.B11 Oznacz $M = \mathrm{NWW}\,(k_1, k_2, \ldots, k_n)$. Zauważ, że $M/k_n < M/k_{n-1} < \cdots < M/k_1$. Udowodnij przez i n d u k c j ę, że jeżeli $\mathcal{A} \subset \mathbb{N}$ i $\mathrm{card}(\mathcal{A}) = n$, to $\max(\mathcal{A}) \geqslant n$.

Z2.B12 Uzasadniamy, przez indukcję względem q, że dla dowolnych x, y, $q \in \mathbb{N}$ zachodzi równość $f(x, y + qx) = f(x, y)$. Bazą tej indukcji jest po prostu założona równość (3). Oto krok indukcyjny: $f(x, y + (q+1)x) = f(x, (y + x) + qx) = f(x, y + x) = f(x, y)$. Załóżmy teraz, że $n > m$ i że $n = qm + r$ jest dzieleniem z resztą d o d a t n i ą. Wówczas $f(m, r) = f(m, r + qm) = f(m, n)$. Jasne, że analogicznie dostajemy $f(r, r_1) = f(m, r)$, jeżeli $m = q_1 r + r_1$ jest drugą linijką algorytmu

Euklidesa i reszta r_1 jest dodatnia. Itd. W ten sposób możemy "dojść" do ostatniej niezerowej reszty w algorytmie, czyli dzielenia $r_{s-1} = q_{s+1}r_s + r_{s+1}$ i otrzymać równości $f(m, n) = f(r, m) = \cdots = f(r_{s+1}, r_s)$. Wiemy, że $r_s = q_{s+2}r_{s+1}$ oraz $r_{s+1} = \mathrm{NWD}\,(m, n)$. Dla zakończenia rozwiązania wystarczy więc udowodnić (przez prostą indukcję względem k), że $f(x, kx) = x$ dla $x, k \in \mathbb{N}$.

Z2.B13 Teza wynika natychmiast z tożsamości kombinatorycznej (zobacz Z3.C4).

$$\binom{k}{0}\binom{n}{k} - \binom{k}{1}\binom{n+1}{k} + \ldots + (-1)^k\binom{k}{k}\binom{n+k}{k} = (-1)^k. \tag{2.36}$$

Z2.B14 Oznaczmy $\mathcal{A}_i = (a_i) \cap [1951]$. Zbiór $\mathcal{A}_i$ jest więc podzbiorem (wszystkich) dodatnich wielokrotności liczby a_i niewiększych niż 1951 (zawartych w zbiorze $[1951] := \{1, 2, \ldots, 1951\}$). Moc zbioru $\mathcal{A}_i$ jest równa $\lfloor 1951/a_i \rfloor$. Założenie $\mathrm{NWW}\,(a_i, a_j) > 1951$ implikuje r o z ł ą c z n o ś ć zbiorów $\mathcal{A}_i$, $\mathcal{A}_j$. Wobec tego

$$1951 \geqslant |\mathcal{A}_1| + |\mathcal{A}_2| + \cdots + |\mathcal{A}_n| = \sum_{i=1}^{n} \left\lfloor \tfrac{1951}{a_i} \right\rfloor > \sum_{i=1}^{n} \left(\tfrac{1951}{a_i} - 1 \right) = 1951 \sum_{i=1}^{n} \tfrac{1}{a_i} - n,$$

bo $\lfloor x \rfloor > x - 1$ dla każdej liczby rzeczywistej x. Jednocześnie $n \leqslant 1951$. Stąd teza.

Z2.C0 Wystarczy zauważyć, że $p + q = 2 \cdot \frac{p+q}{2}$, a liczba $\frac{p+q}{2}$ nie jest liczbą pierwszą (bo leży między k o l e j n y m i liczbami pierwszymi).

Z2.C1 Liczba $a^2 + b^2 + c^2 + d^2$ jest(!) różnicą kwadratów $(a+d)^2 - (b+c)^2$, więc jest iloczynem $(a + d + b + c)(a + d - b - c)$. Jasne, że $1 < a + d + b + c \leqslant a^2 + d^2 + b^2 + c^2$, przy czym druga nierówność jest nieostra t y l k o gdy $a = b = c = d = 1$ (ale wtedy $ad \neq b^2 + bc + c^2$).

Z2.C2 (1) Zobacz tożsamość Sophie Germain. **(2)** Wykorzystaj tożsamość (1.8) i tożsamość $x^4+x^3+x^2+x+1 = (x^2+3x+1)^2-5x(x+1)^2$. **(3)** Rozłóż $f(x) := x^{3k+2}+x^{3l+1}+1$ na iloczyn: Odejmij i dodaj x^2+x+1. Otrzymasz $x^{3k+2}+x^{3l+1}+1 = x^2((x^3)^k-1)+x((x^3)^l-1)+x^2+x+1$. Tożsamość (1.8) pozwala napisać równość postaci $x^{3k+2}+x^{3l+1}+1 = (x^2+x+1)g(x)$. U w a g a. Warto też przeczytać ustęp 3.4.5, gdzie można się dowiedzieć, że istnienie rozkładu $f(x) = (x^2+x+1)g(x)$ jest równoważne dwóm równościom $f(\omega_3) = f(\omega_3^2) = 0$. **(4)** Indukcja względem n: Bazą jest $T_1 = 28 = 2 \cdot 2 \cdot 7$. Dzięki tożsamości $x^3 + 1 = (x+1)(x^2 - x + 1)$ dostaniesz równość $T_{n+1} = T_n \cdot (3^{2 \cdot 3^n} - 3^{3^n} + 1)$. Drugi czynnik jest różnicą kwadratów $(3^{3^n} + 1)^2 - (3^{(3^n+1)/2})^2$. To wystarcza.

Z2.C3 Załóżmy, nie wprost, że $a < b$ są dzielnikami danej liczby naturalnej n leżącymi w przedziale $[\sqrt{n}; \sqrt{n} + \sqrt[4]{n}]$. Niech $d = \mathrm{NWD}\,(a, b)$, i $a = dk$, $b = dl$ dla $k < l$, $k \perp l$. Zapisać $n = d_0dkl$. Z założenia $\sqrt{d_0dkl} \leqslant dk$ wywieść nierówność $d_0 < d$. Stąd $\sqrt{d_0d} \leqslant \sqrt{(d-1)d} < d - \frac{1}{2}$ (druga z tych nierówności jest nierównością AG). Podobnie $\sqrt{kl} \leqslant \sqrt{(l-1)l} < l - \frac{1}{2}$. Stąd $dl = b \leqslant \sqrt{d_0d}\sqrt{kl} + \sqrt[4]{d_0d}\sqrt[4]{kl} < \left(d - \frac{1}{2}\right)\left(l - \frac{1}{2}\right) + \sqrt{\left(d - \frac{1}{2}\right)\left(l - \frac{1}{2}\right)} < dl - \frac{d+l}{2} + \frac{1}{4} + \frac{d+l-1}{2}$, gdzie ostatnia nierówność znowu wynika z AG. Sprzeczność.

Z2.C4 Będziemy (tu i w innych miejscach) korzystać z wygodnego oznaczenia. Jeżeli $a \in \mathbb{Z}$, to oznaczamy $\mathrm{Supp}(a) = \{p \in \mathbb{P} : p|a\}$. Zbiór $\mathrm{Supp}(a)$ jest więc zbiorem wszystkich dzielników pierwszych liczby $a \in \mathbb{Z}$. Nazywamy go **nośnikiem** (ang. *support*) liczby a. Należy przekonać się o prawdziwości poniższych tez:

T e z a 0. $\mathrm{Supp}(0) = \mathbb{P}$;
T e z a 1. $\mathrm{Supp}(a) = \varnothing \iff a = \pm 1$;
T e z a 2. $a|b \implies \mathrm{Supp}(a) \subseteq \mathrm{Supp}(b)$;
T e z a 3. $\mathrm{Supp}(\mathrm{NWD}\,(a, b)) = \mathrm{Supp}(a) \cap \mathrm{Supp}(b)$;
T e z a 4. $a \perp b \iff \mathrm{Supp}(a) \cap \mathrm{Supp}(b) = \varnothing$;
T e z a 5. $\mathrm{Supp}(\mathrm{NWW}\,(a, b)) = \mathrm{Supp}(ab) = \mathrm{Supp}(a) \cup \mathrm{Supp}(b)$.

Jeżeli wszystkie dzielniki pierwsze liczby $a^{2d}-1$ są jednocześnie dzielnikami pierwszymi liczby a^d-1, czyli jeżeli $\mathrm{Supp}(a^{2d}-1)\subseteq\mathrm{Supp}(a^d-1)$, to zachodzi równość zbiorów $\mathrm{Supp}(a^{2d}-1)=\mathrm{Supp}(a^d-1)$ (zawieranie przeciwne $\mathrm{Supp}(a^d-1)\subseteq\mathrm{Supp}(a^{2d}-1)$ wynika bowiem z podzielności $a^d-1|a^{2d}-1$). Przeto $\mathrm{Supp}(a^d+1)\subseteq\mathrm{Supp}(a^{2d}-1)=\mathrm{Supp}(a^d-1)$. Jeżeli więc $p\in\mathrm{Supp}(a^d+1)$, to $p\in\mathrm{Supp}(a^d-1)$, i wówczas p dzieli różnicę $(a^d+1)-(a^d-1)=2$. Stąd $p=2$. Wobec tego $a^d+1=2^r$ przy pewnym $r\in\mathbb{N}$. Czyli $M_r=a^d$. Ale, zobacz Z2.D9, to jest możliwe tylko, gdy $d=1$, czyli gdy $a=M_r$.

Z2.C5 Zauważmy, że $m|n^k\iff\mathrm{Supp}(m)\subseteq\mathrm{Supp}(n)$. Mamy wykazać, że dla dowolnego $p\in\mathrm{Supp}(m)$ zachodzi $v_p(m^{m^m})\leqslant v_p(n^{n^n})$, zob. C2.41, czyli $m^m v_p(m)\leqslant n^n v_p(n)$, zob. C2.43.1. Ta nierówność jest oczywista, gdy $m=n$. Gdy zaś $m<n$, czyli, zob. Zasada Skwantowania, $m+1\leqslant n$, to $m^m v_p(m)\leqslant m^{m+1}\leqslant m^n<n^n\leqslant n^n v_p(n)$, bo $v_p(m)\leqslant m$ i $1\leqslant v_p(n)$. Dowód nierówności $v_p(m)\leqslant m$: Niech $e=v_p(m)$. Wtedy $e<2^e\leqslant p^e\leqslant m$ (pierwszej nierówności dowodzimy przez indukcję). U w a g a. Przy założeniach z zadania, na ogół $m^m\nmid n^n$. Przykład $4^4\nmid 6^6$.

Z2.C6 Używamy skrótu $A_r:=a^r-1$. Mamy $\mathrm{Supp}(A_k)=\mathrm{Supp}(A_1)$. Dowodzimy, że wówczas:

F a k t 1. *Jeżeli* $l|k$, *to* $\mathrm{Supp}(A_l)=\mathrm{Supp}(A_k)=\mathrm{Supp}(A_1)$.

D o w ó d. Mamy $\mathrm{Supp}(A_1)\subseteq\mathrm{Supp}(A_l)\subseteq\mathrm{Supp}(A_k)=\mathrm{Supp}(A_1)$. Q.e.d.

F a k t 2. *Jeżeli* $l|k$, *to* $\mathrm{Supp}(A_l/A_1)\subseteq\mathrm{Supp}(l)$.

D o w ó d. Niech $p\in\mathrm{Supp}(A_l/A_1)$. Wtedy $p\in\mathrm{Supp}(A_l)=\mathrm{Supp}(A_1)$, czyli $a=pu+1$. Stąd

$$A_l/A_1=\sum_{j=0}^{l-1}a^j=(pu+1)^{l-1}+(pu+1)^{l-2}+\cdots+(pu+1)+1=pU+l.$$

Skoro więc $p|(A_l/A_1)$, to (Zasada Podstawowa!) $p|l$, czyli $p\in\mathrm{Supp}(l)$. Q.e.d.

Mając to, dowodzimy, że $\mathrm{Supp}(k)\subseteq\{2\}$. Załóżmy, nie wprost, że $v_p(k)=\alpha\geqslant 1$ dla pewnej liczby pierwszej $p>2$. Niech $l=p^\alpha$. Wtedy $\mathrm{Supp}(l)=\{p\}$, więc, na mocy Faktu 2, $\mathrm{Supp}(A_l/A_1)=\{p\}$. To znaczy, że $A_l/A_1=p^\beta$ przy pewnym $\beta\geqslant 1$. Mamy wówczas

$$\beta=v_p(p^\beta)=v_p\left(\frac{A_l}{A_1}\right)=v_p(A_l)-v_p(A_1)=v_p(l)=\alpha.$$

Trzecia równość wynika z LZW (który można zastosować, bo $p>2$ i $v_p(A_1)\geqslant 1$, co wynika z $\{p\}=\mathrm{Supp}(A_l/A_1)\subseteq\mathrm{Supp}(A_l)=\mathrm{Supp}(A_1)$, zob. Fakt 1). Widzimy porażającą s p r z e c z n o ś ć:

$$l=p^\alpha=p^\beta=\frac{A_l}{A_1}=a^{l-1}+a^{l-2}+\cdots+a+1.$$

Wobec tego k może się dzielić tylko przez parzyste liczby pierwsze, czyli $k=2^m$. Pokazujemy teraz, że $m=1$. Gdyby $m\geqslant 2$, to mielibyśmy $4|k$, skąd $\mathrm{Supp}(a-1)\subseteq\mathrm{Supp}(a^2-1)\subseteq\mathrm{Supp}(a^4-1)\subseteq\mathrm{Supp}(a^k-1)$, więc $\mathrm{Supp}(a^4-1)=\mathrm{Supp}(a^2-1)$. Ale taka równość, na mocy Z2.C4, może zachodzić wyłącznie dla $a=1$. W ten sposób udowodniliśmy równość $k=2$.

Mamy więc równość $\mathrm{Supp}(a^2-1)=\mathrm{Supp}(a-1)$, skąd $\mathrm{Supp}(a+1)\subseteq\mathrm{Supp}(a^2-1)=\mathrm{Supp}(a-1)$. Jeżeli więc $q\in\mathrm{Supp}(a+1)$, to $q\in\mathrm{Supp}(a-1)$, skąd $q|(a+1)-(a-1)$, czyli $q|2$. Zatem $a+1=2^r$.

U w a g a 1. Teza daje się uogólnić. Zachodzi mianowicie (IMO'97 Shortlisted Problem 14):

T w i e r d z e n i e. Jeżeli $\mathrm{Supp}(b^m-1)=\mathrm{Supp}(b^n-1)$ *dla* $b\in\mathbb{N}_{\geqslant 2}$ *i pewnych liczb naturalnych* $1\leqslant m<n$, *to* $m=1$, $n=2$ *oraz* $b+1=2^r$ *dla pewnego* $r\in\mathbb{N}$.

D o w ó d. Niech $d=\mathrm{NWD}\,(m,n)$, $n=dk$, i połóżmy $a=b^d$. Wówczas

$$\mathrm{Supp}(a-1)=\mathrm{Supp}(b^m-1)\cap\mathrm{Supp}(b^n-1)=\mathrm{Supp}(b^n-1)=\mathrm{Supp}(a^k-1),$$

gdzie pierwsza równość wynika z równości $a-1=\mathrm{NWD}\,(b^m-1,\,b^n-1)=b^d-1$, zobacz Z2.B9, i Tezy 3 z rozw. Z2.C4. Mamy albo $k=1$ albo $k\geqslant 2$. W pierwszym przypadku, $n=d\leqslant m$, co jest nieprawdą (bo $m<n$). W drugim przypadku, na mocy naszego zadania, $k=2$. Wtedy $m=d$, $n=2d$, więc, zobacz Z2.C5, $d=1$. Ostatecznie, $b+1=a+1=M_r+1=2^r$.

Z2.C7(1) Niech $n|2^n+1$, czyli $2^n+1=nk$. Jasne, że k jest nieparzysta. Mamy wykazać, że $N|2^N+1$, gdzie $N=2^n+1=nk$. Wobec nieparzystości k mamy

$$2^N+1=2^{nk}+1=(2^n)^k+1=(2^n+1)((2^n)^{k-1}-(2^n)^{k-2}+\cdots-2^n+1)=Na$$

na mocy "plusowego" wariantu tożsamości nieśmiertelnej (zob. 2.3.4 U). U w a g a. Ponieważ 1 jest liczbą Nováka, więc 3, 9, 513, ... są liczbami Nováka. Wobec tego, istnieje n i e s k o ń c z e n i e wiele liczb Nováka. Łatwo też (przez indukcję) dowieść, że wszystkie liczby $n=3^k$ są liczbami Nováka. Korzystając z LZW, mamy nawet więcej: $v_3(2^{3^k}+1)=v_3(2+1)+v_3(3^k)=1+k$.

Z2.C7(2) Zauważmy, że liczby Nováka, jako dzielniki liczb nieparzystych $V_n:=2^n+1$, są n i e p a r z y s t e. Wiemy, że $\mathrm{NWD}\,(V_k,\,V_k)=V_{\mathrm{NWD}\,(k,l)}$ dla nieparzystych $k,\,l$ (zobacz Tw 2 w rozwiązaniu Z2.B9). Zatem: jeżeli $k,\,l$ są liczbami Nováka, a $d=\mathrm{NWD}\,(k,\,l)$, to $k|V_k$, $l|V_l$, więc $d|V_k$, $d|V_l$, skąd $d|\mathrm{NWD}\,(V_k,\,V_l)$ (zob. D2.4(2)), czyli $d|V_d$. Przeto d jest liczbą Nováka. Załóżmy teraz, że $m=\mathrm{NWW}\,(k,\,l)$ dla liczb Nováka $k,\,l$. Wówczas $V_k|V_m$, $V_l|V_m$, bowiem $k|m$, $l|m$, a ciąg (V_n), jak każdy ciąg (a^n+b^n), ma "nieparzystą" własność podzielności, zob. U2 w rozwiązaniu Z2.B9. Zatem $k|V_m$ i $l|V_m$. Więc $m|V_m$.

Z2.C7(3) Podkreślmy, że $p>2$ (liczba 2^n+1 nie ma dzielników parzystych). Wobec tego $V_n|V_{np}$. Więc $p|V_n|V_{np}$ i $n|V_n|V_{np}$. To niestety nie wystarcza dla dowodu, że $np|V_{np}$ (bo nie mamy założenia $n\perp p$). Ale, oznaczając $v_p(n)=\alpha$ i pisząc $n=p^\alpha k$, gdzie $p\nmid k$, mamy

$$v_p(V_{np})=v_p((2^n)^p+1)=v_p(2^n+1)+1\geqslant v_p(n)+1=\alpha+1,$$

na mocy (2.24) (nierówność wynika z podzielności $n|2^n+1$). Stąd $p^{\alpha+1}|V_{np}$. Jednocześnie $k|n|V_n|V_{np}$, więc, zobacz C2.17, $p^{\alpha+1}k|V_{np}$, czyli $np|V_{np}$.

Z2.C7(4) Oczywista iteracja rozumowania z Z2.C7(3) pokazuje, że prawdziwy jest

F a k t. Jeżeli $p_1,\ldots,p_s$ są dzielnikami pierwszymi liczby V_n, a przy tym n jest liczbą Nováka, to iloczyn $n\cdot p_1^{e_1}\cdot\ldots\cdot p_s^{e_s}$ jest liczbą Nováka dla dowolnych wykładników $e_1,\ldots,e_s\in\mathbb{N}$.

Mając to, weźmy dwie liczby Nováka m i n. Niech $d:=\mathrm{NWD}\,(m,\,n)=\prod_{p\in\mathbb{P}}p^{v_p(d)}$ i niech $m=dm'$, $n=dn'$. Wówczas, zob. Z2.C7(2), $N=dm'n'$ jest liczbą Nováka i $p|N|V_N$ dla wszystkich p, dla których $v_p(d)>0$. Na mocy faktu, $Nd=mn$ jest więc liczbą Nováka.

Z2.C7(5) *L e m a t. Jeżeli n jest liczbą Nováka, przy czym $n=3^\alpha k$, gdzie $3\nmid k$ i $\alpha\geqslant 1$, to istnieje taka liczba pierwsza p, że $p|V_{3n}$ i $p\nmid k$.*

D o w ó d. Mamy $V_{3n}=(2^n+1)(2^{2n}-2^n+1)$. Twierdzimy, że każdy różny od 3 dzielnik pierwszy liczby $2^{2n}-2^n+1$ jest dobry. Wykazujemy najpierw, że liczba $2^{2n}-2^n+1$ m a dzielnik pierwszy różny od 3. To wynika z równości (zob. LZW)

$$v_3(V_{3n})=v_3(2^{3n}+1)=v_3((2^3)^{3^\alpha k}+1)=v_3(2^3+1)+v_3(3^\alpha k)=2+\alpha,$$
$$v_3(V_n)=v_3(2^n+1)=v_3((2^3)^{3^{\alpha-1}k}+1)=v_3(2^3+1)+v_3(3^{\alpha-1}k)=2+\alpha-1.$$

Stąd $v_3(2^{2n}-2^n+1)=v_3(V_{3n})-v_3(V_n)=1$. Wobec tego $2^{2n}-2^n+1=3m$, gdzie $3\nmid m$ i $m>1$. Weźmy dowolny dzielnik pierwszy $p|m$. Wykazujemy teraz, że $p\nmid V_n$. To wynika z równości

$$\mathrm{NWD}\,(a^2-a+1,\,a+1)=\mathrm{NWD}\,(3,\,a+1)$$

prawdziwej dla dowolnej liczby naturalnej $a > 2$ (równość ta jest natychmiastowym wnioskiem następującego dzielenia z resztą $a^2 - a + 1 = (a-2)(a+1) + 3$). Z równości tej wnioskujemy (kładąc $a = 2^n$), że jedynym wspólnym dzielnikiem pierwszym liczb $2^{2n} - 2^n + 1$ i V_n może być tylko 3. Zatem, ponieważ $p|2^{2n} - 2^n + 1$ i $p \neq 3$, więc $p \nmid V_n$ i, tym bardziej, $p \nmid k$ (bo $k|n|V_n$). Q.e.d.

Jasne jest teraz jak, startując od liczby Nováka $n_1 = 3$, udowodnić przez indukcję, że *dla dowolnej liczby* $s \in \mathbb{N}$ *istnieje podzielna przez* 3 *liczba Nováka* n_s *mająca dokładnie* s *różnych dzielników pierwszych.* Rzeczywiście, jeżeli znamy już liczbę n_s, to, wobec lematu, wystarczy położyć $n_{s+1} = 3n_s p$ (i, korzystając najpierw z Z2.C7(4), uzasadnić, że $3n_s$ jest liczbą Nováka, a następnie, korzystając z Z2.C7(3), że $3n_s p$ również jest liczbą Nováka).

Z2.D0 Jeżeli $x = 2n+1$, to $x^2 = 4n^2 + 4n + 1 = 4N + 1$. Jeżeli zaś $x = 2m$, to $x^2 = 4M$. Tak natrafiamy na jeden z najważniejszych pomysłów w teorii liczb: *Kwadrat daje resztę* 0 *lub* 1 *przy dzieleniu przez* 4. Stąd wyciągamy wniosek: *Suma dwóch (trzech) kwadratów nieparzystych daje resztę* 2 *(resztę* 3*) przy dzieleniu przez* 4. Dla rozwiązania trzeciej części zadania rozważmy równanie $1^2 + 3^2 + 5^2 + w^2 = t^2$, czyli $35 = t^2 - w^2 = (t-w)(t+w)$. Rozwiązując układ równań $t - w = 1$, $t + w = 35$ znajdujemy równość $1^2 + 3^2 + 5^2 + 17^2 = 18^2$. Możemy ją teraz pomnożyć stronami przez kwadrat dowolnej liczby nieparzystej.

Z2.D1 Dowiedź kolejno tez: (1) *Liczba jest podzielna przez* 10 *wtedy i tylko wtedy, gdy jej ostatnią cyfrą jest* 0; (2) *Kwadrat podzielny przez* 10 *jest podzielny przez* 100; (3) *Kwadrat ma parzystą liczbę cyfr* 0 *na końcu*; (4) *Jeżeli* $a, n \in \mathbb{N}$ *i* $a^2|n$, *to* n *jest kwadratem wtedy i tylko wtedy, gdy iloraz* $\frac{n}{a^2}$ *jest kwadratem*; (5) $2|n$ *i* $4 \nmid n$.

Z2.D2 Niech $K := 10^3 a + 10^2 a + 10b + b$. Wtedy $K = 11(99a + (a+b))$. Jeżeli więc K jest kwadratem, to $11^2|K$, skąd $11|a+b$. Musimy więc sprawdzić osiem(!) przypadków: $a = 2, \ldots, 9$, $b = 11 - a$. Dobry jest tylko przypadek $a = 7$, $b = 4$.

Z2.D3 Ponieważ $\mathrm{NWD}\,(a, a+1) = 1$ (zob. C2.10), więc $\mathrm{NWD}\,(3a, a+1) = 1$ lub 3. Założona równość $3a(a+1) = (3b)^2$ w pierwszym przypadku daje tezę (zobacz *trik* T2.19). W drugim przypadku mamy $a + 1 = 3c$ i $ac = b^2$, więc (*trik*!) $a = d^2$, zatem $d^2 + 1 = 3c$. To jest niemożliwe, bo dla $d = 3t$ mamy $d^2 + 1 = 3T + 1 \neq 3c$, a dla $d = 3t \pm 1$ mamy $d^2 + 1 = (9t^2 \pm 6t + 1) + 1 = 3T + 2 \neq 3c$.

Z2.D4 (1) Jeżeli $4^n - 3^n = x^2$, to $(2^n - x)(2^n + x) = 3^n$. Stąd (na mocy jednoznaczności rozkładu na czynniki pierwsze) $2^n - x = 3^s$ i $2^n + x = 3^t$ dla $s, t \in \mathbb{Z}_{\geqslant 0}$ spełniających $s + t = n$. Dodając te równości stronami dostajemy $2^{n+1} = 3^s + 3^t$. To jest możliwe tylko, gdy $s = 0$, $t = n$. Więc $2^{n+1} = 1 + 3^n$. Ta równość zachodzi tylko dla $n = 1$ (bo $2^{n+1} < 1 + 3^n$ dla wszystkich $n \geqslant 2$). **(2)** Gdy $n = 2k+1$, to $5^n - 3^n = (4+1)^{2k+1} - (4-1)^{2k+1} = (4a+1) - (4b-1) = 4A + 2$, więc $5^n - 3^n$ nie jest kwadratem (zobacz rozwiązanie Z2.D1). Jeżeli zaś $n = 2k$ i $5^n - 3^n = x^2$, to mamy $(5^k - x)(5^k + x) = 3^n$, czyli $5^k - x = 3^s$ i $5^k + x = 3^t$ dla $s, t \in \mathbb{Z}_{\geqslant 0}$, $s + t = n$. Dodając stronami mamy $2 \cdot 5^k = 3^s + 3^t$, co jest możliwe tylko, gdy $s = 0$, $t = n$. Więc $2 \cdot 5^k = 1 + 3^{2k}$. Ta równość zachodzi tylko dla $k = 1$ (bo $2 \cdot 5^k < 1 + 3^{2k}$ dla wszystkich $k \geqslant 2$).

Z2.D5 Mamy $T_1 = \mathbf{1}$, $T_2 = 3$, $T_3 = 6$, $T_4 = 10$, $T_5 = 15$, $T_6 = 21$, $T_7 = 28$, $T_8 = \mathbf{36}$. Istnieją więc liczby trójkątne będące kwadratami. Załóżmy, że $T_k = a^2$ jest kwadratem. Wówczas

$$T_{4k^2+4k} = \frac{(4k^2+4k)(4k^2+4k+1)}{2} = 4 \cdot \frac{k(k+1)}{2} \cdot (2k+1)^2 = (2a(2k+1))^2.$$

Mamy więc metodę znajdowania coraz większych liczb trójkątnych będących kwadratami. Stąd teza. Uwaga. Opisana metoda nie daje wszystkich rozwiązań równania $T_x = y^2$. Na przykład $T_{49} = 35^2$. Później (zob. *równanie indyjskie*) nauczymy się znajdować wszystkie rozwiązania tego równania.

Z2.D6 (A) Gdyby $n(n+1) = x^2$, to, zobacz C2.10 i T2.19, $n = a^2$ i $n+1 = b^2$. Przyglądając się kwadratom (0, 1, 4, 9, ...) widzimy, że mogą się one różnić o 1 tylko gdy mniejszy jest równy 0. W

naszym przypadku to odpada. (B) Liczby całkowite kolejne są względnie pierwsze. Zatem $n \perp n+1$ i $n+2 \perp n+1$. Więc $n(n+2) \perp n+1$ dla dowolnej liczby $n \in \mathbb{N}$. Gdyby $n(n+1)(n+2) = x^2$, to, wobec powiedzianego i triku T2.19, byłoby $n(n+2) = a^2$ (i $n+1 = b^2$). Wtedy $a^2 = n(n+2) = n^2+2n = (n+1)^2 - 1$ i, znowu, kwadraty $(n+1)^2$ i a^2 leżałyby zbyt blisko siebie. (C) Mnożąc w iloczynie $x(x+1)(x+2)(x+3)$ osobno pierwszy czynnik przez czwarty i osobno drugi przez trzeci, dostajemy iloczyn $(x^2+3x)(x^2+3x+2)$. Iloczyn postaci $A(A+2)$ jest różnicą kwadratów $(A+1)^2 - 1^2$. Zatem $x(x+1)(x+2)(x+3) = (x^2+3x+1)^2 - 1^2$. Z tożsamości tej wnioskujemy, że iloczyn czterech kolejnych liczb naturalnych leży zbyt blisko kwadratu, by sam mógł być kwadratem.

Z2.D7 Zauważmy, że $(n+1)^3 - n^3 = m^2 \iff 3(2n+1)^2 = (2m-1)(2m+1)$. Łatwo widzieć, że $2m-1 \perp 2m+1$ (NWD tych liczb dzieli ich różnicę równą 2, ale jest $\neq 2$, bo $3(2n+1)^2$ jest liczbą nieparzystą). Zatem 3 dzieli jedną (i tylko jedną) z liczb $2m-1$, $2m+1$. Pokazujemy, że $3 \nmid 2m-1$: Gdyby $2m-1 = 3k$, to dostalibyśmy równość $(2n+1)^2 = \frac{2m-1}{3}(2m+1) = k(3k+2)$ i, na mocy *triku* z T2.19, $3k+2 = y^2$, co jest niemożliwe (kwadrat przy dzieleniu przez 3 nie daje reszty 2). Musi być więc $2m+1 = 3l$ dla pewnego $l \in \mathbb{N}$. Wtedy na mocy równości $(2n+1)^2 = (3l-2)l$ i *triku* mamy $3l-2 = x^2 = (2u+1)^2$ (bo x, jako dzielnik liczby nieparzystej $(2n+1)^2$, jest postaci $2u+1$). Stąd $2m = 3l-1 = x^2+1 = (2u+1)^2+1 = 2((u+1)^2+u^2)$, czyli $m = (u+1)^2+u^2$.

Z2.D8 Załóżmy, że $V_n = x^m$. Gdy $m = 2k$, to, oznaczając $x^k = 2c+1$ (co jest możliwe, bo x jest nieparzyste!), dostajemy równość $2^n = x^{2k} - 1 = (x^k-1)(x^k+1) = 4c(c+1)$, z której wynika, że $c = 1$ (z liczb c i $c+1$ jedna jest bowiem nieparzysta!), czyli $2^n = 8$, więc $n = 3$. Załóżmy teraz, że m jest nieparzysta. Wtedy, na mocy tożsamości nieśmiertelnej, $2^n = (x-1)(x^{m-1} + \cdots + x + 1)$. Drugi czynnik z prawej strony strony tej równości jest sumą nieparzystej (równej m) liczby składników nieparzystych, więc jest liczbą nieparzystą. Skąd $m = 1$.

U w a g a. Czwórkę $(x, y; m, n)$ liczb naturalnych nazwiemy **czwórką Catalan'a**, gdy $m, n \geqslant 2$ i zachodzi równość $x^m - y^n = 1$. Czwórki Catalan'a dostarczają więc właściwych potęg $y^n < x^m$ (liczb naturalnych) będących liczbami kolejnymi (tzn., różniącymi się o 1). Eugène Catalan (Belgia) postawił (1842) hipotezę, że *j e d y n ą czwórką Catalan'*a *jest czwórka* (3, 2; 2, 3). Ta hipoteza, tzw. ***problem Catalan'*a**, została ostatecznie udowodniona (2002) przez P. Mihăilescu (Rumunia). Pokazane rozwiązanie jest więc dowodem przypadku szczególnego hipotezy: *Jedyną czwórką Catalan'*a*, w której* $y = 2$*, jest czwórka* (3, 2; 2, 3). Inny przypadek szczególny mamy poniżej. Zobacz też Z2.I4.

Z2.D9 Niech $M_m = y^n$. Sprawdzamy, że $2 \nmid n$: Gdyby $n = 2k$, to równość $2^m - 1 = y^n$ dałaby się zapisać tak: $2 \cdot (2^{m-1} - 1) = (y^k - 1)(y^k + 1)$. Taka równość jest niemożliwa, bo prawa strona jest iloczynem dwóch czynników parzystych (y jest liczbą nieparzystą!), więc jest podzielna przez 2^2, a lewa strona jest podzielna tylko przez 2^1. Niech więc $n \geqslant 3$ będzie liczbą nieparzystą. Korzystamy z "plusowego" wariantu tożsamości nieśmiertelnej dla wykładnika nieparzystego, zobacz 2.4.2 U. Równość $M_m = y^n$ zapisujemy tak: $2^m = (y+1)(y^{n-1} - y^{n-2} + \ldots - y + 1)$. Z jednoznaczności rozkładu (liczb naturalnych) na czynniki pierwsze wnosimy stąd, że $y+1 = 2^l$ dla pewnego $1 \leqslant l < m$ (nie może być $l = m$, bo wtedy $n = 1$). Czyli $v_2(y+1) \geqslant 1$. Możemy teraz skorzystać z "plusowego" wariantu LZW dla $p = 2$, zobacz C2.52. Dostajemy $m = v_2(2^m) = v_2(y^n+1) = v_2(y+1) + v_2(n) = l + 0 = l$. Sprzeczność. Widzimy więc, że *Nie istnieje czwórka Catalan'*a*, w której* $x = 2$.

Z2.D10 Zbadamy najpierw czy może być $x = y$. Ponieważ $x^2 + 5x < (x+3)^2$, więc liczba x^2+5x, jako większa od x^2, może być co najwyżej jednym z dwóch kwadratów: $(x+1)^2$, $(x+2)^2$. Pierwsza z równości $x^2+5x = (x+1)^2$, $x^2+5x = (x+2)^2$ (jako równoważna równości $3x = 1$) jest niemożliwa, a druga daje $x = 4$. Mamy więc parę $(x, y) = (4, 4)$. Załóżmy teraz, że $x < y$. Wówczas $y^2+5x < y^2+5y < (y+3)^2$. Mamy zatem: (1) $y^2+5x = (y+1)^2$ lub (2) $y^2+5x = (y+2)^2$.

Z2.D11 Zapiszmy $xy = a^2c$ i $(p-x)(p-y) = b^2d$, gdzie c, d są bezkwadratowe (zob. C2.36). Wnioskujemy stąd, że $c = d$: Ponieważ $xy(p-x)(p-y) = (ab)^2cd$ jest kwadratem, więc cd jest kwadratem, skąd, wobec bezkwadratowości c i d, $c = d$. Zatem $p(p-x-y) = (p-x)(p-y) - xy =$

$c(b-a)(b+a)$. Jednocześnie $a \leqslant \sqrt{a^2c} = \sqrt{xy} \leqslant (x+y)/2 \leqslant (p-1)/2$ i $b \leqslant \sqrt{b^2c} = \sqrt{(p-x)(p-y)} \leqslant (2p-x-y)/2 < p$ (na mocy nierówności AG). Stąd wynika, że $b-a<p$, oraz $b+a<2p$. Ponieważ $p \nmid c$ (gdyby $p|c$ mielibyśmy $p|xy$, czyli $p|x$ lub $p|y$, co jest niemożliwe ze względów "wielkościowych"). Przeto $b+a=p$. Zakładając teraz, że $x \neq y$, mamy sprzeczność:

$$p = b+a < \frac{2p-x-y}{2} + \frac{x+y}{2} = p.$$

Z2.D12 Nie. Gdyby bowiem $x+2y=a^2$, $5x+13y=b^2$ i $7x+11y=c^2$, mielibyśmy równość $b^2+c^2=3(2a)^2$ i punkt wymierny $(\frac{b}{2a}, \frac{c}{2a})$ na okręgu o równaniu $u^2+w^2=3$, zobacz C2.66.

Z2.E1 (1) Spróbuj rozwiązać układ równań $14x+y=2^u$, $x+14y=2^w$. **(2)** Zauważ, że NWD $(y-2, y+2)=1$ i zastosuj trik z T2.19.

Z2.E2 Załóżmy (b.s.o.), że $a \leqslant b$. Jasne, że $c>b$. Więc (Zasada Skwantowania) $c \geqslant b+1$ skąd $c^n \geqslant (b+1)^n$. I $a^n+b^n=c^n \geqslant (b+1)^n = b^n + \binom{n}{1}b^{n-1} + \cdots + \binom{n}{n-1}b + 1 \geqslant b^n + nb^{n-1}$, więc $a^n \geqslant nb^{n-1} \geqslant na^{n-1}$. I ostatecznie, $\min\{a, b\} = a \geqslant n$.

Z2.E3 Niech $x=2^{4k}$, $y=2^{3k}$. Wówczas $x^3+y^4=2^{12k+1}$. Ponieważ $12k+1=5(12t+5)$ dla $k=5t+2$, więc mamy nieskończenie wiele rozwiązań $(x, y, z) = (2^{20t+8}, 2^{15t+6}, 2^{12t+5})$. U w a g a. Nie należy sądzić, że to są wszystkie rozwiązania. Na przykład trójka $(7^7 8^5 15^8, 7^5 8^4 15^6, 7^4 8^3 15^5)$ jest również rozwiązaniem (bo $7+8=15$).

Z2.E4 Oznacz $\alpha = \sqrt{2}-1$, $\beta = \sqrt{2}+1$ i sprawdź przez indukcję, że liczba

$$m = m(n) = \left(\frac{\alpha^n + \beta^n}{2}\right)^2$$

jest liczbą naturalną dla każdego $n \in \mathbb{N}$. Zobacz też Z2.B4.

Z2.F1 (1) Jeżeli $p \neq 3$, to $p=3t+1$ lub $p=3s-1$. Wówczas $2p+1=6t+3=3T$, odpowiednio $4p+1=12s+3=3S$. **(2)** Jeżeli $p \neq 5$, to $p=5t\pm 1$ lub $p=5s\pm 2$. Wówczas $4p^2+1=5T$, odpowiednio $6p^2+1=5S$. **(3)** Kwadrat nieparzystej i niepodzielnej przez 3 liczby całkowitej daje resztę 1 przy dzieleniu przez 3 (sprawdzić!). Wobec tego suma $p^2+q^2+r^2$ kwadratów liczb pierwszych >3 jest podzielna przez 3. Nie jest więc liczbą pierwszą. **(4)** Z 2.3.3 P3 wiemy, że 2^n-1 może być liczbą pierwszą tylko, gdy $n \in \mathbb{P}$, a z C2.39 wiemy, że 2^n+1 może być liczbą pierwszą tylko, gdy $n=2^k$. Jedyną liczbą pierwszą postaci 2^k jest liczba 2.

Z2.F2 Jeżeli m jest parzysta, to $\gamma(m)=\gamma(2m)$. Można więc wziąć $k=2m$ i $l=m$. Jeżeli zaś m jest liczbą nieparzystą, to niech p oznacza najmniejszą nieparzystą liczbę pierwszą, która n i e dzieli m. Wówczas $\gamma(pm)=\gamma(m)+1=\gamma(pm-m)$. Wystarczy więc położyć $k=pm$ i $l=(p-1)m$.

Z2.F3 Zauważmy przede wszystkim, że $q \geqslant n$ (gdyby $q<n$, to liczba złożona $q+qr=q(1+r)$ byłaby wyrazem badanego ciągu). Niech $p<n$ będzie liczbą pierwszą. Niech $\varrho_0, \varrho_1, \ldots, \varrho_{p-1}$ oznaczają reszty z dzielenia przez p początkowych p wyrazów naszego ciągu. Ponieważ $0<\varrho_j<p$ dla każdego $j=0, \ldots, p-1$ (bo reszta 0 nie występuje!), więc, zgodnie z zasadą szufladkową, istnieją liczby k, l takie, że $0 \leqslant k < l < p$ i $\varrho_k = \varrho_l$. To oznacza, że $(q+lr)-(q+kr)=(l-k)r$ jest liczbą naturalną podzielną przez p. Zatem, na mocy C2.32 i ZTA, $p|r$. Teraz trzeba zastosować C2.17.

Z2.F4 Równość Legendre'a daje $v_p(n!) = \sum_{k=1}^{\infty} \lfloor n/p^k \rfloor < n \sum_{k=1}^{\infty} 1/p^k = n/(p-1)$ dla dowolnej liczby pierwszej $p \leqslant n$ (korzystaliśmy tu z oczywistych nierówności $\lfloor x \rfloor \leqslant x$ i wzoru na sumę szeregu geometrycznego). Stąd $n! = \prod_{p \in \mathbb{P}} p^{v_p(n!)} = \prod_{p \leqslant n} p^{v_p(n!)} \leqslant \prod_{p \leqslant n} p^{n/(p-1)}$.

Z2.F5 Oznaczmy $A(n) = p_1 p_2 \cdot \ldots \cdot p_n = \prod_{j \leqslant n} p_j$. Dowodzimy najpierw nierówności słabszej: *Dla $n \geqslant 2$ zachodzi nierówność $A(n) > p_{n+1}$.* Rozważmy w tym celu liczbę $A(n)-1$. Liczba ta jest $\geqslant 2$, więc (zobacz T2.14) ma dzielnik pierwszy p. Wówczas $p \leqslant A(n)-1$ (zobacz C2.2). Z drugiej

strony, p jest różna od liczb $p_1, \ldots, p_n$, więc $p > p_n$. Czyli $p \geqslant p_{n+1}$. Stąd $p_{n+1} < A(n)$. Następnie sprawdzamy "na piechotę" nierówność (2.33) dla $4 \leqslant n \leqslant 10$. Teraz ustalmy $n > 10$ i rozważmy ciąg $\boldsymbol{a} = (A(n-1)-p_n,\ 2A(n-1)-p_n,\ \ldots,\ (p_n-1)A(n-1)-p_n)$. Wszystkie jego wyrazy są (różnymi) liczbami naturalnymi. Ponadto, jeżeli p jest dzielnikiem pierwszym wyrazu $kA(n-1)-p_n$ tego ciągu, to $p > p_n$. Nie może być bowiem $p = p_n$ (bo wtedy $p_n|k$, co jest niemożliwe wobec $k < p_n$), ani $p < p_n$ (bo wtedy $p = p_i$ dla $1 \leqslant i \leqslant n-1$, więc $p_i|p_n$, nonsens!). Dzięki temu sprawdzamy, że wyrazy ciągu $\boldsymbol{a}$ są parami w z g l ę d n i e p i e r w s z e. Rzeczywiście, gdyby liczba pierwsza $p > p_n$ dzieliła $kA(n-1)-p_n$ i $lA(n-1)-p_n$ dla pewnych $1 \leqslant k < l < p_n$, to dzieliłaby też $(l-k)A(n-1)$, co jest niemożliwe. Oznaczmy przez q_k dowolny dzielnik pierwszy liczby $kA(n-1)-p_n$. W ten sposób znajdziemy liczby pierwsze $q_2, q_3, \ldots, q_{p_n-1}$ (nie wpisaliśmy na tę listę q_1, bo nie udowodniliśmy, że $A(n-1)-p_n \neq 1$). Oznaczmy $p_n - 2 = t$. (Pierwsza uwaga na marginesie: $t > 2n$ dla wszystkich $n \geqslant 7$. W rzeczy samej, $p_7 = 17 > 2\cdot 7+2$, a ciąg $(2n+2)$ n i e rośnie szybciej niż ciąg (p_n)). Mamy t liczb pierwszych większych niż p_n i parami różnych (pamiętamy o względnej pierwszości wyrazów ciągu $\boldsymbol{a}$). Są to więc liczby $p_{n+n_1}, p_{n+n_2}, \ldots, p_{n+n_t}$, gdzie $1 \leqslant n_1 < n_2 < \ldots < n_t$ (druga uwaga na marginesie: $n_t \geqslant t$). Każda z nich jest dzielnikiem któregoś (każda swojego) wyrazu ciągu $\boldsymbol{a}$, każda więc jest $\leqslant$ od największego wyrazu $(p_n-1)A(n-1)-p_n = A(n)-A(n-1)-p_n$ tego ciągu. Stąd $A(n) > A(n)-A(n-1)-p_n \geqslant p_{n+n_t} \geqslant p_{n+t} > p_{3n}$ (trzecia nierówność wynika z drugiej uwagi na marginesie, a czwarta, z pierwszej). Otrzymana nierówność $A(n) > p_{3n}$ dla każdego $n \geqslant 7$, jest m o c n i e j s z a od nierówności Bonse. Rzeczywiście, Czytelnik łatwo właściwie zinterpretuje i uzasadni, że $A(n) > A(n/2)^2 > p_{3n/2}^2 > p_{n+1}^2$.

Z2.F6 (68 OM, III stopień) Niech $\{p_1, p_2, \ldots, p_m\} = \mathrm{Supp}(a_1\cdot\ldots\cdot a_n)$ będzie zbiorem wszystkich dzielników pierwszych iloczynu $a_1\cdot\ldots\cdot a_n$. Niech $a_i = p_1^{e_1(i)}p_2^{e_2(i)}\cdot\ldots\cdot p_m^{e_m(i)}$, zob. 2.4.1 (RK). Mamy:

$$a_i^{m-1} = \frac{a_i^m}{a_i} = \frac{a_i}{p_1^{e_1(i)}}\cdot\frac{a_i}{p_2^{e_2(i)}}\cdot\ldots\cdot\frac{a_i}{p_m^{e_m(i)}}.$$

Po wypisaniu takich równości jedna pod drugą dla $i = 1, \ldots, n$, dowodzimy, że w każdej kolumnie stoi n r ó ż n y c h liczb naturalnych: Gdyby dla $i < j$ zachodziła równość $a_i p_k^{-e_k(i)} = a_j p_k^{-e_k(j)}$, to mielibyśmy $a_j/a_i = p_k^{e_k(j)-e_k(i)}$. Ale $a_i < a_j < 2a_1$, skąd $1 < \frac{a_j}{a_i} < \frac{2a_1}{a_i} < \frac{2a_1}{a_1} = 2$, co dałoby niemożliwe dla żadnej liczby pierwszej (p_k) i dla żadnego wykładnika całkowitego α nierówności $1 < p_k^\alpha < 2$. Wystarczy teraz zauważyć, że iloczyn n różnych liczb naturalnych jest $\geqslant n!$.

Z2.F7 (68 OM, III stopień) Przedstaw liczbę naturalną n w postaci $2^a\cdot 3^b\cdot 5^c\cdot n'$, gdzie $n' \perp 30$, i zdefiniuj funkcję $f : \mathbb{N} \longrightarrow \mathbb{Z}$ wzorem $f(n) = a+3b-c$. Sprawdź równość $f(m\cdot n) = f(m)+f(n)$ dla dowolnych $m, n \in \mathbb{N}$. Do i-tego zbioru zalicz te i tylko te liczby n, dla których resztą z dzielenia liczby $f(n)$ przez 5 jest i. Zauważ, że $f(1) = 0$, $f(2) = 1$, $f(3) = 3$, $f(4) = 2$, $f(5) = 4$. Zatem, dla dowolnego $n \in \mathbb{N}$, liczby $f(n)$, $f(2n)$, $f(3n)$, $f(4n)$ i $f(5n)$ dają r ó ż n e reszty z dzielenia przez 5.

Z2.F8 (62 OM, I stopień) Tożsamość nieśmiertelna (1.8) daje rozkłady

$$M_{rs} = (2^r-1)\left((2^r)^{s-1}+(2^r)^{s-2}+\ \ldots\ +2^r+1\right) = M_rA, \tag{2.37}$$

$$M_{rs} = (2^s-1)\left((2^s)^{r-1}+(2^s)^{r-2}+\ \ldots\ +2^s+1\right) = M_sB, \tag{2.38}$$

Z Z2.B9 wiemy, że liczby M_r i M_s są względnie pierwsze. Z tej względnej pierwszości i równości $M_rA = M_sB$, na mocy ZTA, mamy $M_r|B$, czyli równość $B = M_rC$ dla pewnego $C \in \mathbb{N}$. Zapisujemy więc $M_{rs} = M_rM_sC$. W tym rozkładzie, czynniki M_r i M_s są większe od 1 i względnie pierwsze. Wobec tego jedyna możliwość, kiedy liczba M_{rs} n i e m a trzech różnych dzielników pierwszych, to taka, kiedy $M_r = p^k$, $M_s = q^l$, $C = p^aq^b$, gdzie p, q są różnymi liczbami pierwszymi. Wówczas, zobacz Z2.D9, $k = l = 1$. Wobec tego nasze założenie nie wprost może być zapisane tak: $M_{rs} = M_rM_sC = pq\cdot p^aq^b = p^{a+1}q^{b+1}$.

Pokazujemy, że w takiej sytuacji $b = 0$: Gdyby $b > 0$, to $q|C$, więc, tym bardziej, $q|M_rC$. Czyli $q|(2^s)^{r-1}+(2^s)^{r-2}+\ldots+2^s+1$. Ale, na mocy określenia, $2^s = q+1$. Stąd $(2^s)^t = (q+1)^t = q\cdot\text{coś}+1$ dla dowolnego $t \in \mathbb{Z}_{\geqslant 0}$ ("coś" $\in \mathbb{Z}$). Zatem $(2^s)^{r-1} + (2^s)^{r-2} + \ldots + 2^s + 1 = q \cdot \text{COŚ} + r$. Stąd, na mocy Zasady Podstawowej, $q|r$. Sprzeczność, bo $q = 2^s - 1 > 2^r - 1 > r$. Przeto $b = 0$.

Jednocześnie $a \geqslant 1$. Gdyby bowiem $a = 0$, równość $M_{rs} = p^{a+1}q$ nie mogłaby zachodzić ze względów "wielkościowych": liczba $M_{rs} = 2^{rs} - 1$ jest bowiem znacznie większa od liczby $2^{r+s} + 1$, która jest większa od $M_rM_s = pq$. Widzimy stąd, że założenie nie wprost wygląda tak: $M_{rs} = p^{a+1}q$, gdzie $a \geqslant 1$. Pokażemy teraz, że w takim razie $M_r = s$. Z równości (2.37) mamy bowiem

$$A = \frac{M_{rs}}{p} = (2^r)^{s-1} + (2^r)^{s-2} + \ldots + 2^r + 1 = p^a q.$$

Skąd wnosimy, że $p|A$. Ale, z określenia, $2^r = p + 1$, więc, podobnie jak wyżej, $(2^r)^t = p \cdot \text{coś} + 1$ i powyższa równość daje $A = p \cdot \text{COŚ} + s$. Stąd $p|s$. Wobec pierwszości liczb p, s widzimy, że $p = s$ czyli $2^r - 1 = s$.

Równość $M_{rs} = p^{a+1}q$ pisze się więc następująco: $s^{a+1}q = 2^{rs} - 1 = (2^r)^s - 1 = (s+1)^s - 1$. Ale

$$(s+1)^s - 1 = s^s + \binom{s}{1}s^{s-1} + \ldots + \binom{s}{s-2}s^2 + \binom{s}{s-1}s + 1 - 1 = s^3 \cdot \text{coś} + s^2,$$

bo $s|\binom{s}{s-2}$, zobacz C2.50. Zatem $s^{a+1}q = s^3 \cdot \text{coś} + s^2$, a stąd, w oczywisty sposób, $a+1 = 2$. Mamy więc $M_{rs} = p^2q$. I dostajemy rozstrzygającą sprzeczność:

$$M_{rs} = p^2q = (2^r - 1)^2(2^s - 1) < (2^r)^2 \cdot 2^s = 2^{2r+s} < 2^{rs} - 1 = M_{rs}.$$

Ta sprzeczność kończy rozwiązanie.

Z2.G1 Zauważmy najpierw, że (dokładnie) jedna z kolejnych czterech liczb naturalnych jest podzielna przez $4 = 2^2$, nie jest więc bezkwadratowa. Zatem, trójki kolejnych liczb bezkwadratowych (jeżeli istnieją) są postaci $(4k-3,\, 4k-2,\, 4k-1)$, dla $k \in \mathbb{N}$. Załóżmy nie wprost, że takich trójek jest skończenie wiele i że największą z nich jest $(4A-3,\, 4A-2,\, 4A-1)$. Wówczas wśród czterech liczb $4k-3, 4k-2, 4k-1, 4k$, dla dowolnego $k > A$, występują co najwyżej dwie liczby bezkwadratowe. Jeżeli więc oznaczymy przez $Q(n)$ liczbę liczb naturalnych bezkwadratowych $\leqslant n$, to mamy $Q(4n) \leqslant 3A + 2(n - A)$ dla wszystkich $n > A$. To i teza poniższego lematu, dają nierówność $(2 + 2\varepsilon)n < 2n + A$, czyli $\varepsilon < A/(2n)$ dla wszystkich $n > A$. Nonsens.

Lemat. Istnieje taka liczba $\varepsilon > 0$, że dla każdego $n \in \mathbb{N}$ zachodzi nierówność $Q(n) > (\frac{1}{2} + \varepsilon)n$.

Dowód. Ustalmy $n \in \mathbb{N}$. Dla danej liczby pierwszej p oznaczmy: $\mathcal{A}_p = \{k \in \mathbb{N} : k \leqslant n,\, p^2|k\}$. Jasne, że każda liczba naturalna $\leqslant n$ nie będąca liczbą bezkwadratową jest podzielna przez kwadrat jakiejś liczby pierwszej, należy więc do pewnego (co najmniej jednego) zbioru $\mathcal{A}_p$. Wobec tego zbiór $[\,n\,] \setminus (\mathcal{A}_2 \cup \mathcal{A}_3 \cup \cdots \cup \mathcal{A}_q)$ (suma po wszystkich liczbach pierwszych, których kwadrat jest $\leqslant n$), jest zbiorem wszystkich liczb bezkwadratowych $\leqslant n$. Jasne, że $\text{card}(\mathcal{A}_p) = \lfloor n/p^2 \rfloor$. Zatem

$$Q(n) = n - \text{card}(\mathcal{A}_2 \cup \mathcal{A}_3 \cup \cdots \cup \mathcal{A}_q) \geqslant n - \sum_{p \in \mathbb{P},\, p^2 \leqslant n} \left\lfloor \frac{n}{p^2} \right\rfloor \geqslant n - n\left(\frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{q^2}\right).$$

Dla zakończenia dowodu wystarczy więc uzasadnić, że $1 - (1/2^2 + 1/3^2 + \cdots + 1/q^2) > 1/2 + \varepsilon$ dla pewnej dodatniej liczby ε, czyli że $1/2^2 + 1/3^2 + \cdots + 1/q^2 < 1/2 - \varepsilon$ lub, równoważnie, że istnieje taka liczba dodatnia ε, że nierówność $S_q := 1/3^2 + 1/5^2 + \cdots + 1/q^2 < 1/4 - \varepsilon$ zachodzi dla dowolnie wielu składników (będących odwrotnościami kwadratów nieparzystych liczb pierwszych) sumy z lewej strony. W C1.4 widzieliśmy, że ta suma jest $< 3/4$, ale to jest za słabe. Mamy jednak

$$S_q = \frac{1}{3^2} + \frac{1}{5^2} + \cdots + \frac{1}{q^2} < \frac{1}{9} + \frac{1}{25} + \frac{1}{49} + \sum_{k=5}^{n} \frac{1}{(2k+1)^2} < \frac{1891}{11\,025} + \sum_{k=5}^{n} \frac{1}{(2k-1)(2k+1)}.$$

Ostatnia suma, dzięki $\frac{1}{(2k-1)(2k+1)} = \frac{1}{2}\left(\frac{1}{2k-1} - \frac{1}{2k+1}\right)$, "teleskopuje" się do $\frac{1}{18} - \frac{1}{2(2n+1)}$. Zatem $S_q < \frac{1891}{11\,025} + \frac{1}{18} < 0,23$. Więc można przyjąć $\varepsilon = 0,02$. Q.e.d.

Z2.G2 Niech $b_1 < b_2 < \cdots < b_s$ będą wszystkimi liczbami naturalnymi bezkwadratowymi z przedziału $[\,1;\, n\,]$. Rozpatrujemy dwa przypadki: (1) $n > b_s$, (2) $n = b_s$. W przypadku (1) zbadajmy przekrój $\{b_1, \ldots, b_s\} \cap \{n - b_1, \ldots, n - b_s\}$. Ponieważ, zobacz lemat z poprzedniego rozwiązania, $s > n/2$, więc ten przekrój jest niepusty. Zatem dla pewnego j, $b_j \in \{n - b_1, \ldots, n - b_s\}$, czyli $b_j = n - b_i$. W przypadku (2) mamy $s - 1 = Q(n-1) > (n-1)/2$. Więc, znowu na mocy Zasady Łat na Kapocie, zob. $\mathbb{KOM}$, zbiory $\{b_1, \ldots, b_{s-1}\} \cap \{n - b_1, \ldots, n - b_{s-1}\}$ mają niepusty przekrój.

Z2.H1 Jeżeli $m = u^2 + w^2$, to $2m = (u+w)^2 + (u-w)^2$. Jeżeli zaś $2m = x^2 + y^2$, to x, y są tej samej parzystości(!), więc $m = ((x+y)/2)^2 + ((x-y)/2)^2$ jest sumą kwadratów liczb całkowitych.

Z2.H2 Jeżeli $n = a^2 + b^2 + c^2$ i $a \geqslant b \geqslant c$, to $n^2 = (a^2 + b^2 - c^2)^2 + (2ac)^2 + (2bc)^2$. Trzeba jeszcze zauważyć, że $a^2 + b^2 - c^2 \in \mathbb{N}$.

Z2.H3 Gdy $k + (k+1) + \cdots + (k+r-1) = 2^n$, czyli $(2k+r-1)r = 2^{n+1}$, to mamy sprzeczność. Bowiem liczby $2k + r - 1$ i r są różnej parzystości. Niech teraz $n = 2^s(2m+1)$, gdzie $m \geqslant 1$. Szukamy takich $k \in \mathbb{N}$ i $r \in \mathbb{N}_{\geqslant 2}$, że zachodzi równość $k + (k+1) + \cdots + (k+r-1) = n$, czyli $(2k + r - 1)r = 2^{s+1}(2m+1)$. Równość ta jest spełniona w każdym z dwóch przypadków: $(k,\, r) = (2^s - m,\, 2m+1)$, $(k,\, r) = (m + 1 - 2^s,\, 2^{s+1})$. Natomiast w jednym (i tylko jednym) z tych przypadków zachodzą żądane nierówności $k \geqslant 1$ i $r \geqslant 2$. U w a g a. Można wykazać, że jeżeli $2m+1$ jest liczbą pierwszą, to uzyskane przedstawienie liczby $2^s(2m+1)$ w postaci sumy dwóch lub więcej kolejnych liczb naturalnych jest jedyne. I tylko wtedy! Zróbcie to.

Z2.H4 Liczbę a nazwijmy *dobrą*, gdy istnieje taka liczba $m \in \mathbb{N}$ i taki wybór znaków $\pm$, że $a = \pm 1^2 \pm 2^2 \pm \cdots \pm m^2$. Liczbę $a \in \mathbb{Z}$ nazwijmy *superdobrą*, gdy istnieje nieskończenie wiele odpowiednich liczb m (i odpowiednich wyborów znaków). Równości $0 = 1^2 + 2^2 - 3^2 + 4^2 - 5^2 - 6^2 + 7^2$, $1 = 1^2$, $2 = -1^2 - 2^2 - 3^2 + 4^2$ i $3 = -1^2 + 2^2$ pokazują, że liczby 0, 1, 2 i 3 są *dobre*. Oczywiste jest, że liczba a jest (*super*)*dobra* wtedy i tylko wtedy, gdy $-a$ jest (*super*)*dobra*. Prawdziwa dla wszystkich m równość $E_m := (m+1)^2 - (m+2)^2 - (m+3)^2 + (m+4)^2 = 4$ pozwala z łatwością uzasadnić, że jeżeli a jest liczbą *dobrą*, to również liczba $a + 4$ jest *dobra*. Stąd, dzięki pokazanej *dobroci* liczb 0, 1, 2, 3 i oczywistej indukcji, widzimy, że wszystkie liczby całkowite są *dobre*. Aby wykazać *superdobroć* wszystkich liczb całkowitych wystarczy wykorzystać tożsamość

$$(m+1)^2 - (m+2)^2 - (m+3)^2 + (m+4)^2 - (m+5)^2 + (m+6)^2 + (m+7)^2 - (m+8)^2 = 0,$$

która jest tylko inaczej zapisaną równością $E_m - E_{m+4} = 4 - 4 = 0$.

Z2.H5 Tezę można wywnioskować z tożsamości $6x = (x+1)^3 + (x-1)^3 + (-x)^3 + (-x)^3$. Dzięki niej, biorąc dowolną liczbę $a \in \mathbb{Z}$, przedstawiając ją w postaci $6b + r$ i wiedząc, że $(6b+r) - (6c+r)^3 = 6x$ (zob. Z2.A2(2)), możemy (na nieskończenie wiele sposobów) przedstawić a w postaci sumy pięciu sześcianów.

Z2.H6 Indukcja względem n. Baza jest oczywista. Niech $a < (n+1)!$. Dzielimy z resztą: $a = q(n+1) + r$, gdzie $0 \leqslant r < n+1$, czyli $0 \leqslant r \leqslant n$. Jeżeli $q = 0$, to $a = r$ jest żądaną "sumą" (jednoskładnikową) dzielników liczby $n!$. Jeżeli zaś $q \geqslant 1$, to $q < n!$, więc, na mocy założenia indukcji, $q = d_1 + \cdots + d_s$, gdzie $d_1 < \cdots < d_s$ są dzielnikami liczby $n!$ i $s \leqslant n$. Wówczas $a = r + d_1(n+1) + d_2(n+1) + \cdots + d_s(n+1)$ jest żądaną sumą różnych dzielników liczby $(n+1)!$.

Z2.I1 Dla $p = 2$ rzecz jest oczywista. Załóżmy więc, że p jest nieparzysta. Wówczas, dzięki 2.4.2 U, mamy $5|a$. Wtedy z C2.52 mamy

$$n \leqslant n v_5(a) = v_5(a^n) = v_5(2^p + 3^p) = v_5(2+3) + v_5(p) = 1 + v_5(p).$$

Gdyby więc $n \geqslant 2$, to musiałoby też być $v_5(p) \geqslant 1$, czyli $p = 5$. Ale $2^5 + 3^5 = 275 = 5^2 \cdot 11$.

Z2.I2 Zapisz sumę $1^n + 2^n + \cdots + 8^n$ w postaci $(1^n + 8^n) + (2^n + 7^n) + (3^n + 6^n) + (4^n + 5^n)$ i stosownie zwiększaj wykładniki 3-adyczne. U w a g a. Łatwo zastąpić liczbę 8 przez 9. Wówczas sumę $1^n + \cdots + 9^n$ zapisujemy w postaci $(1^n + 9^n) + \cdots + (4^n + 6^n) + 5^n$ i zwiększamy wykładniki 5-adyczne. Do sumy $1^n + \cdots + 10^n$ możemy podobnie zastosować liczbę $p = 11$ dla zwiększania wykładnika p-adycznego. Można też wykorzystać nieparzysty dzielnik pierwszy $p \in \mathrm{Supp}(A + 1)$ dla uogólnienia zadania na przypadek sumy $1^n + \cdots + A^n$. Co można zrobić, gdy $A + 1 = 2^r$?

Z2.I3 Łatwo zobaczyć, że $x,\, y \in \mathbb{Q}$. Rzeczywiście, skoro $x-y,\, x^2-y^2 \in \mathbb{Z}$, to $x+y = \frac{x^2-y^2}{x-y} \in \mathbb{Q}$. Zatem $2x = (x - y) + (x + y) \in \mathbb{Q}$, więc $x \in \mathbb{Q}$ i, podobnie, $y \in \mathbb{Q}$. Wobec tego możemy zapisać $x = \frac{a}{m}$, $y = \frac{b}{m}$, gdzie $a,\, b \in \mathbb{Z}$, a $m \in \mathbb{N}$ jest n a j m n i e j s z y m wspólnym mianownikiem. Wówczas, oznaczając $x^k - y^k = c_k$, gdzie $c_k \in \mathbb{Z}$, dostajemy równości $a^k - b^k = c_k m^k$ dla wszystkich $k \in \mathbb{N}$. Czyli $m^k | a^k - b^k$ dla wszystkich $k \in \mathbb{N}$. Chcemy udowodnić (bo to jest równoważne(!) z tezą zadania), że $m = 1$. Załóżmy, nie wprost, że $m > 1$ i że $p|m$, gdzie $p \in \mathbb{P}$, zob. T2.14. Jeżeli $p > 2$, to wybierając $k = p^n$, dostajemy, na mocy LZW (uzasadnić prawomocność stosowania tegoż!),

$$p^n = k \leqslant k v_p(m) = v_p(m^k) \leqslant v_p(a^k - b^k) = v_p(a - b) + v_p(k) = v_p(a - b) + n,$$

dla wszystkich $n \in \mathbb{N}$. Zauważyć tu sprzeczność. Znaleźć podobną sprzeczność, gdy $m = 2^\alpha$.

Z2.I4 Załóżmy, że w danej czwórce Catalan'*a* $(x,\, y;\, m,\, n)$ mamy $y = p \in \mathbb{P}$. Przypadek $p = 2$ został zbadany w Z2.D8. Znaleziona tam została czwórka Catalan'*a* $(3,\, \mathbf{2};\, 2,\, 3)$. Załóżmy więc teraz, że $p > 2$ i że $(x,\, p;\, m,\, n)$ jest czwórką Catalan'*a*. Wówczas $p^n = x^m - 1$. Taka równość nie może zajść (przy $n \geqslant 2$), gdy $x = 2$, zobacz Z2.D9. Załóżmy więc dodatkowo, że $x \geqslant 3$. Tożsamość "nieśmiertelna" (2.22) daje $p^n = (x - 1)Q_m(x,\, 1)$. Stąd (i z jednoznaczności rozkładu) mamy równości $x - 1 = p^\alpha$, $Q_m(x,\, 1) = p^\beta$ dla pewnych wykładników $\alpha,\, \beta$ spełniających warunki $\alpha \geqslant 1$ (bo $x - 1 \geqslant 2$!) i $\alpha + \beta = n$. Możemy(!) teraz zastosować lemat LZW, zob. T2.18. Dostajemy

$$v_p(m) = v_p(x^m - 1) - v_p(x - 1) = v_p(p^n) - \alpha = n - \alpha = \beta.$$

Stąd $m = p^\beta c$ dla pewnej liczby naturalnej c. I mamy "piękną" sprzeczność:

$$p^\beta = Q_m(x,\, 1) = \sum_{j=0}^{m-1} x^j > m = p^\beta c.$$

Rozdział 3

Wielomiany

Gauß nous apparaît, après 150 ans,
comme le flambeau qui a montré la route
à de nombreuses générations de mathématiciens,
et illuminé l'avenir comme nul autre l'a jamais fait.
(Jean Dieudonné)

Rozważać będziemy teraz zbiór $\mathcal{R}[X]$ wszystkich wielomianów o współczynnikach należących do pierścienia $\mathcal{R}$. Okaże się, i to jest g ł ó w n y m m o r a ł e m płynącym z tego rozdziału, że w przypadku, gdy pierścień $\mathcal{R}$ jest c i a ł e m (zobacz D1.10), w zbiorze $\mathcal{R}[X]$ (podobnie jak w zbiorze $\mathbb{Z}$) zachodzi twierdzenie o i s t n i e n i u i j e d n o z n a c z n o ś c i r o z k ł a d u na czynniki nierozkładalne.

3.1 Pierścień wielomianów

W matematyce szkolnej wielomian jest pewną, szczególnie prosto zdefiniowaną f u n k c j ą rzeczywistą, zob. 3.2.3 U2. W rzeczywistości wielomian jest czymś jeszcze prostszym.

Definicja 3.1 Niech $\mathcal{R}$ będzie pierścieniem przemiennym z jedynką. Wyrażenie postaci

$$f(X) = a_0 + a_1X + a_2X^2 + \ \ldots\ + a_nX^n = \sum_{k=0}^{n} a_kX^k, \tag{3.1}$$

gdzie $a_k \in \mathcal{R}$, nazywamy **wielomianem zmiennej** X **o współczynnikach z pierścienia** $\mathcal{R}$. Elementy a_k nazywamy **współczynnikami** wielomianu $f(X)$, współczynnik a_0 nazywa się **wyrazem wolnym**. Zbiór wszystkich wielomianów zmiennej X o współczynnikach z pierścienia $\mathcal{R}$ oznaczamy symbolem $\mathcal{R}[X]$. Wielomian, którego wszystkie współczynniki są równe 0 (zero pierścienia $\mathcal{R}$) nazywamy **wielomianem zerowym** i oznaczamy 0. Wielomian postaci $f(X) = a_0$ nazywamy **wielomianem stałym**.

Wielomiany **dodajemy** i **mnożymy** tak j a k w s z k o l e.

Ćwiczenie 3.1 Uzasadnić, że $\mathcal{R}[X]$ z "wprowadzonymi" działaniami dodawania i mnożenia jest pierścieniem przemiennym z jedynką. Tak zbudowany pierścień nazywamy **pierścieniem wielomianów jednej zmiennej** o **współczynnikach** z pierścienia $\mathcal{R}$.

Czasami używamy skróconego zapisu

$$f(X) = \sum_{k\geqslant 0} a_k X^k,$$

rozumiejąc przy tym, że prawie wszystkie (to znaczy wszystkie z wyjątkiem skończenie wielu) współczynniki a_k są równe 0. Przy takim sposobie pisania mamy

$$\sum_{k\geqslant 0} a_k X^k + \sum_{k\geqslant 0} b_k X^k = \sum_{k\geqslant 0} (a_k + b_k) X^k$$

oraz

$$\sum_{k\geqslant 0} a_k X^k \cdot \sum_{l\geqslant 0} b_l X^l = \sum_{r\geqslant 0} c_r X^r,$$

gdzie $c_r = \sum_{j=0}^{r} a_j b_{r-j}$.

Przykład 1. Klasyczny przykład wykorzystania mnożenia w pierścieniu wielomianów zobaczyć można w dowodzie ***tożsamości Cauchy'*ego-*Vandermonde'*a**:

$$\sum_{j=0}^{r} \binom{m}{j}\binom{n}{r-j} = \binom{m+n}{r}.$$

Robi się to tak: Rozważmy r-ty współczynnik wielomianu $f(X) = (1+X)^{m+n}$. Jest on równy, zobacz (1.7), $\binom{m+n}{r}$. Z drugiej strony wielomian $f(X)$ jest równy iloczynowi

$$(1+X)^m \cdot (1+X)^n = \sum_{k=0}^{m} \binom{m}{k} X^k \cdot \sum_{l=0}^{n} \binom{n}{l} X^l$$

dwóch wielomianów i, wobec tego, jego r-ty współczynnik jest równy

$$c_r = \sum_{j=0}^{r} a_j b_{r-j} = \sum_{j=0}^{r} \binom{m}{j}\binom{n}{r-j}.$$

Podobne przykłady znaleźć można w $\mathbb{KOM}$. ◊

Ćwiczenie 3.2 Mnożymy wielomian $\sum_{k=0}^{100} X^k$ przez wielomian $\sum_{k=0}^{100} (-1)^k X^k$. Wykazać, że w otrzymanym wielomianie wszystkie współczynniki c_{2s-1} są równe zero.

Definicja 3.2 Gdy $f(X) = \sum_{k\geqslant 0} a_k X^k \in \mathcal{R}[X]$ i n jest największym indeksem, dla którego $a_n \neq 0$, to a_n nazywamy **współczynnikiem wiodącym**, a liczbę n nazywamy **stopniem** wielomianu $f(X)$. Stopień wielomianu $f(X)$ oznaczamy $\deg f(X)$ lub po prostu $\deg f$. Umawiamy się, że wielomian zerowy ma stopień równy $-\infty$.

Ćwiczenie 3.3 Udowodnić, że stopień wielomianu spełnia warunki:

(1) $\deg\left(f(X) + g(X)\right) \leqslant \max\{\deg f(X), \deg g(X)\}$,

(2) $\deg f(X)g(X) \leqslant \deg f(X) + \deg g(X)$.

Definicja 3.3 Element $f(\lambda) := a_0 + a_1\lambda + a_2\lambda^2 + \ldots + a_n\lambda^n \in \mathcal{R}$, gdzie $f(X)$ jest wielomianem (3.1), a $\lambda \in \mathcal{R}$, nazywamy **wartością wielomianu** $f(X)$ dla argumentu λ. Element $\lambda \in \mathcal{R}$ nazywa się **pierwiastkiem wielomianu** $f(X)$, gdy $f(\lambda) = 0$. Pierwiastek wielomianu nazywa się również **miejscem zerowym** wielomianu lub **zerem** wielomianu.

Ostatnią z czterech definicji ogólnych jest definicja złożenia:

Definicja 3.4 Jeżeli $f(X) \in \mathcal{R}[X]$ jest wielomianem danym w (3.1), a $g(X) \in \mathcal{R}[X]$ jest dowolnym wielomianem, to wielomian $(f \circ g)(X)$ dany przez

$$(f \circ g)(X) := f(g(X)) = a_0 + a_1 g(X) + a_2 (g(X))^2 + \ldots + a_n (g(X))^n,$$

nazywa się **złożeniem** (lub **superpozycją**) wielomianów $g(X)$ i $f(X)$ (w tej kolejności).

P r z y k ł a d 2. Niech $f(X) = X^2 + X + 2$, $g(X) = X + 1$. Wtedy $g(f(X)) = X^2 + X + 3$, a $f(g(X)) = (X+1)^2 + (X+1) + 2 = X^2 + 3X + 4$. Widzimy, że składanie wielomianów n i e j e s t przemienne, tzn., $f \circ g$ jest na ogół r ó ż n e od $g \circ f$. $\Diamond$

3.2 Siedem idei podstawowych

W tym paragrafie przypomnimy i nieco usystematyzujemy szkolną wiedzę na temat wielomianów. Czytelnik, który boi się ogólnego pojęcia *pierścienia*, może chwilowo myśleć, że pierścień to taki zbiór liczb, w którym można bez ograniczeń dodawać, odejmować i mnożyć, a *ciało*, to taki pierścień, w którym można dodatkowo dzielić (nie przez 0, oczywiście). Znamy więc jeden pierścień n i e b ę d ą c y c i a ł e m, jest to $\mathbb{Z}$, i trzy ciała, są to $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$. W rzeczy samej znamy już nieskończenie wiele pierścieni: Jeżeli $\mathcal{R}$ jest dowolnym pierścieniem, to, jak wiemy z C3.1, zbiór $\mathcal{R}[X]$ wielomianów o współczynnikach w $\mathcal{R}$ jest również pierścieniem. Później poznamy jeszcze różne inne pierścienie, z których niektóre będą ciałami.

3.2.1 Pierwsza idea: twierdzenie Bézout'a

Pierwsza idea polega na "wyciąganiu przed nawias" czynnika dwumiennego postaci $X - \alpha$. Udowodnimy w tym celu w a ż n ą równość, którą nazwiemy ***równością Bézout'a***:

TWIERDZENIE 3.1 *Jeżeli $f(X) \in \mathcal{R}[X]$ jest wielomianem stopnia n i $\alpha \in \mathcal{R}$, to istnieje taki wielomian $g(X) \in \mathcal{R}[X]$, że zachodzi równość*

$$\boxed{\boxed{f(X) = (X - \alpha)g(X) + f(\alpha).}} \tag{3.2}$$

Ponadto, $\deg g(X) = n-1$, *a wielomiany $g(X)$ i $f(X)$ mają t e n s a m współczynnik wiodący.*

D O W Ó D. Niech $f(X) = a_0 + a_1 X + \ldots + a_n X^n$, gdzie $a_n \neq 0$. Wówczas

$$f(X) - f(\alpha) = \sum_{k=0}^{n} a_k X^k - \sum_{k=0}^{n} a_k \alpha^k = \sum_{k=1}^{n} a_k (X^k - \alpha^k).$$

Tożsamość (1.8) pozwala zapisać każdą różnicę $X^k - \alpha^k$ w postaci iloczynu

$$X^k - \alpha^k = (X - \alpha)(X^{k-1} + \alpha X^{k-2} + \ldots + \alpha^{k-2}X + \alpha^{k-1}) = (X - \alpha)g_{k-1}(X),$$

gdzie, jak widać, wielomian $g_{k-1}(X)$ ma współczynniki w pierścieniu $\mathcal{R}$ i stopnień równy $k-1$. Oznaczając przez $g(X)$ sumę $a_1g_0(X) + a_2g_1(X) + \ldots + a_ng_{n-1}(X)$ dostajemy więc równość $f(X) - f(\alpha) = (X - \alpha)g(X)$ równoważną równości (3.2). Ponadto, łatwo widzieć, że $g(X) = a_nX^{n-1} + \ldots$. Zatem $g(X)$ ma ten sam współczynnik wiodący co $f(X)$, oraz $\deg g(X) = n - 1$. □

U w a g a 1. Bardzo ważną okolicznością jest tu fakt, że współczynniki wielomianu $g(X)$ z równości (3.2) należą do tego samego pierścienia, do którego należą współczynniki wielomianu $f(X)$ i element α. W szczególności: *Jeżeli $f(X) \in \mathbb{Z}[X]$ i $\alpha \in \mathbb{Z}$, to również $g(X) \in \mathbb{Z}[X]$.* Często używany wniosek z powyższego formułujemy w postaci ćwiczenia:

Ćwiczenie 3.4 Uzasadnić, że dla dowolnego wielomianu $f(X) \in \mathbb{Z}[X]$ i liczb całkowitych a, b zachodzi relacja podzielności:

$$\boxed{\boxed{a - b | f(a) - f(b).}} \tag{3.3}$$

ZADANIE 3.1 Dane są liczby całkowite $a < b < c$. Dowieść, że n i e istnieje wielomian $f(X)$ o współczynnikach całkowitych, dla którego $f(c) = a$ i $f(a) = b$.

R o z w i ą z a n i e. Gdyby taki wielomian istniał, to, na mocy (3.3), $c - a | f(c) - f(a)$, czyli $c - a | a - b$, co jest niemożliwe, bo $|c - a| > |a - b|$. ◊

Okazuje się, że czynnik $X - \alpha$ można "wyciągnąć przed wielomian" $f(X)$ wtedy i tylko wtedy, gdy α jest pierwiastkiem wielomianu $f(X)$. Mówi o tym:

TWIERDZENIE 3.2 (***Bézout***) *Element $\alpha \in \mathcal{R}$ jest pierwiastkiem niezerowego wielomianu $f(X) \in \mathcal{R}[X]$ wtedy i tylko wtedy, gdy istnieje taki wielomian $g(X) \in \mathcal{R}[X]$, że*

$$f(X) = (X - \alpha)g(X). \tag{3.4}$$

Przy tym $\deg g(X) = \deg f(X) - 1$.

D O W Ó D. Wynika natychmiast z T3.1 i faktu, że $0 \cdot g(\alpha) = 0$, por. Z1.6.(1). □

WNIOSEK. *Dany jest pierścień $\mathcal{R}$ b e z d z i e l n i k ó w z e r a i niezerowy wielomian $f(X) \in \mathcal{R}[X]$. Jeżeli r ó ż n e elementy $\alpha_i \in \mathcal{R}$, dla $1 \leqslant i \leqslant s$, są pierwiastkami wielomianu $f(X)$, to zachodzi równość*

$$f(X) = (X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_s)h(X), \tag{3.5}$$

gdzie $h(X) \in \mathcal{R}[X]$, $\deg h(X) = \deg f(X) - s$ oraz $h(X)$ i $f(X)$ mają ten sam współczynnik wiodący.

D O W Ó D. Dla $s = 1$ mamy równość $f(X) = (X - \alpha_1)g(X)$. Załóżmy więc, że $s > 1$. Mamy $0 = f(\alpha_2) = (\alpha_2 - \alpha_1)g(\alpha_2)$. Ponieważ $\alpha_1 \neq \alpha_2$, czyli $\alpha_2 - \alpha_1 \neq 0$, a w $\mathcal{R}$ nie ma dzielników zera (co teraz zakładamy), więc α_2 jest[1] pierwiastkiem wielomianu $g(X)$. Zatem mamy równość typu (3.4): $g(X) = (X - \alpha_2)h(X)$. Skąd $f(X) = (X - \alpha_1)(X - \alpha_2)h(X)$. Tę sztuczkę można kontynuować. □

[1]Bez założenia, że $\mathcal{R}$ jest dziedziną całkowitości, nie moglibyśmy tego twierdzić!

ZADANIE 3.2 Udowodnić, że jeżeli wielomian o współczynnikach całkowitych przyjmuje dla trzech różnych argumentów całkowitych wartość 1, to wielomian ten nie ma pierwiastków całkowitych (czyli, żadna liczba całkowita nie jest jego pierwiastkiem).

Rozwiązanie. Załóżmy, że $f(X) \in \mathbb{Z}[X]$ jest tym wielomianem. Niech $f(a) = f(b) = f(c) = 1$. Wówczas wielomian $g(X) = f(X) - 1$ ma również współczynniki całkowite i trzy różne pierwiastki a, b, c. Zatem, rozkład (3.5) ma postać:

$$g(X) = (X-a)(X-b)(X-c)h(X), \tag{3.6}$$

dla pewnego $h(X) \in \mathbb{Z}[X]$. Załóżmy, nie wprost, że $f(X)$ ma pierwiastek całkowity i że d jest tym pierwiastkiem, $f(d) = 0$. Wtedy $-1 = f(d) - 1 = g(d) = (d-a)(d-b)(d-c)h(d)$, na mocy (3.6). Sprzeczność!, bo liczby -1 nie da się rozłożyć na iloczyn czterech czynników całkowitych, z których trzy są różne. ♢

Ćwiczenie 3.5 Dany jest wielomian $f(X) \in \mathbb{Z}[X]$. Udowodnić, że jeżeli dla czterech różnych argumentów całkowitych wartością tego wielomianu jest liczba 5, to $f(x) \neq 8$ dla każdej liczby całkowitej x.

3.2.2 Druga idea: algorytm dzielenia z resztą

Pamiętamy jak duże usługi oddała nam możliwość dzielenia z resztą w pierścieniu $\mathbb{Z}$. Jest więc bardzo obiecującym fakt, że w pierścieniu $\mathbb{K}[X]$ wielomianów jednej zmiennej o współczynnikach w cele możliwe jest dzielenie z resztą. Tę obietnicę zrealizujemy w 3.3.

Ćwiczenie 3.6 Udowodnić, że jeżeli $\mathcal{R}$ jest dziedziną całkowitości, i $f(X)$, $g(X) \in \mathcal{R}[X]$, to zachodzi równość $\deg f(X)g(X) = \deg f(X) + \deg g(X)$. Porównać C3.3(2).

TWIERDZENIE 3.3 (***Dzielenie z resztą***) *Jeżeli $a(X)$, $b(X) \in \mathbb{K}[X]$ i $b(X) \neq 0$, to istnieją takie, jednoznacznie wyznaczone wielomiany $q(X)$, $r(X) \in \mathbb{K}[X]$, że*

$$\boxed{\boxed{a(X) = q(X)b(X) + r(X) \quad i \quad \deg r(X) < \deg b(X).}} \tag{3.7}$$

DOWÓD. Dowód poprowadzimy przez indukcję względem stopnia wielomianu $a(X)$. Niech $a(X) = a_nX^n + \ldots + a_1X + a_0$, $b(X) = b_mX^m + \ldots + b_1X + b_0$, gdzie $\deg a(X) = n$, $\deg b(X) = m \geqslant 0$. Jeżeli $n < m$, to mamy równość $a(X) = 0 \cdot b(X) + a(X)$ i wystarczy położyć $q(X) = 0$, $r(X) = a(X)$. Jeżeli zaś $n \geqslant m$, to rozważmy wielomian

$$\widetilde{a}(X) = a(X) - \frac{a_n}{b_m}X^{n-m}b(X). \tag{3.8}$$

Ponieważ wielomian ten ma stopień mniejszy niż n (sprawdzić!), więc, na mocy założenia indukcyjnego, istnieją takie wielomiany $\widetilde{q}(X)$ i $r(X)$, że

$$\widetilde{a}(X) = \widetilde{q}(X)b(X) + r(X) \quad \text{i} \quad \deg r(X) < \deg b(X).$$

Stąd mamy $a(X) = q(X)b(X) + r(X)$, gdzie $q(X) = \frac{a_n}{b_m}X^{n-m} + \widetilde{q}(X)$. Dla dowodu jednoznaczności załóżmy, że zachodzą równości $a(X) = q_1(X)b(X) + r_1(X) = q_2(X)b(X) + r_2(X)$,

gdzie stopnie $\deg r_1$, $\deg r_2$ są mniejsze niż $\deg b$. Wtedy $(q_1-q_2)b = r_2 - r_1$. Stąd, ponieważ, na mocy C3.6 (patrz też C1.19), $\deg(q_1-q_2)b = \deg(q_1-q_2) + \deg b$, więc

$$\deg(q_1-q_2) + \deg b = \deg(r_2-r_1) \leqslant \max\{\deg r_2, \deg r_1\} < \deg b.$$

Zatem $\deg(q_1-q_2) < 0$, czyli $q_1(X) - q_2(X) = 0$ i, w końcu, $r_1(X) - r_2(X) = 0$. □

W opisanej sytuacji wielomian $q(X)$ nazywamy (niepełnym) **ilorazem**, a wielomian $r(X)$ **resztą** z dzielenia $a(X)$ przez $b(X)$. Gdy $r(X) = 0$, piszemy $b(X)|a(X)$ i mówimy, że wielomian $b(X)$ **dzieli** wielomian $a(X)$.

U w a g a 1. Czytelnik powinien tak długo wpatrywać się w (3.8), aż rozpozna k r o k nauczanego w szkole ***algorytmu dzielenia wielomianów***. Algorytm ten wykonuje się szczególnie łatwo, gdy $b_m = 1$. Wielomiany spełniające taki warunek warto nazwać:

Definicja 3.5 Wielomian $\sum_{k=0}^{m} b_k X^k \in \mathcal{R}[X]$ nazywa się wielomianem **unormowanym**, gdy jego współczynnik wiodący b_m jest równy 1 (jedynka pierścienia $\mathcal{R}$).

U w a g a 2. Zauważmy, że dowód i s t n i e n i a równości (3.7) przechodzi bez żadnych zmian dla wielomianów o współczynnikach w pierścieniu: trzeba jedynie żądać, by współczynnik b_m był elementem o d w r a c a l n y m. W szczególności, zawsze można wykonać dzielenie (z resztą!) przez wielomian u n o r m o w a n y. Gorzej jest z jednoznacznością! Dlaczego?

U w a g a 3. Należy też zauważyć, że równość Bézout'a (3.2) jest szczególnym przypadkiem równości (3.7). Mamy tam do czynienia z dzieleniem przez dwumian $b(X) = X - \alpha$. Resztą z tego dzielenia jest wielomian stopnia < 1, mianowicie element $f(\alpha)$ pierścienia $\mathcal{R}$.

W poniższych przykładach używamy oznaczeń:

$$\begin{aligned} A_n(X) &= X^n - 1, \\ B_n(X) &= X^n + 1, \\ C_n(X) &= X^n + X^{n-1} + \cdots + 1, \\ D_n(X) &= X^n + X^{n-2} + X^{n-4} + \ldots . \end{aligned}$$

Wyraz wolny wielomianu $D_n(X)$ jest równy 1, gdy n jest liczbą parzystą, a jest równy 0, gdy n jest liczbą nieparzystą.

P r z y k ł a d 2. Z faktu, że $A_1(X)|A_n(X)$ dla każdego $n \in \mathbb{N}$ korzystaliśmy już wyżej. Zobacz też tożsamość nieśmiertelną (1.8), z której wynika, że

$$A_n(X) = C_{n-1}(X) \cdot A_1(X) \tag{P2}$$

jest odpowiednim dzieleniem z resztą (zerową). ◊

P r z y k ł a d 3. Podzielimy teraz (z resztą) wielomian $B_n(X)$ przez $B_1(X)$. Dostajemy równość $X^n + 1 = q(X) \cdot (X+1) + r_n$, gdzie $r_n = B_n(-1) = (-1)^n + 1$. Konkretnie:

$$B_n(X) = (-1)^{n-1} C_{n-1}(-X) \cdot B_1(X) + [1 + (-1)^n]. \tag{P3}$$

Widzimy stąd, że $X+1|X^n+1$ wtedy i tylko wtedy, gdy $(-1)^n+1 = 0$. Więc z całą pewnością, gdy n jest n i e p a r z y s t e. A także wtedy, gdy $2 := 1+1 = 0$. ◊

P r z y k ł a d 4. Chcemy teraz podzielić wielomian $D_{4k}(X)$ przez wielomian $C_{2k}(X)$. Mnożąc $D_{4k}(X)$ przez X^2-1, czyli $C_{2k}(X^2)$ przez $A_1(X^2)$, dostajemy, wobec (P2), równość $(X^2-1)D_{4k}(X) = A_1(X^2)C_{2k}(X^2) = A_{2k+1}(X^2) = X^{4k+2}-1 = (X^{2k+1}-1)(X^{2k+1}+1)$. Czyli, wobec (P2) i (P3), $(X^2-1)D_{4k}(X) = (X-1)C_{2k}(X)\cdot(X+1)C_{2k}(-X)$. Zapiszmy to w posaci $(X^2-1)D_{4k}(X) = (X^2-1)C_{2k}(-X)C_{2k}(X)$. Stąd łatwo (jak?) wywnioskować równość:

$$D_{4k}(X) = C_{2k}(-X)\cdot C_{2k}(X). \quad \Diamond \tag{P4}$$

P r z y k ł a d 5. Podzielimy wreszcie, z resztą(!), wielomian $D_{4k+2}(X)$ przez $C_{2k+1}(X)$. Mamy $D_{4k+2}(X) = X^2D_{4k}(X)+1 = X^2C_{2k}(-X)C_{2k}(X) = [XC_{2k}(-X)]\cdot[XC_{2k}(X)]+1$. Stąd, ponieważ $XC_{2k}(X) = C_{2k+1}(X)-1$, $D_{4k+2}(X) = [XC_{2k}(-X)]\cdot C_{2k+1}(X)+1-XC_{2k}(-X)$. Ale $1-XC_{2k}(-X) = C_{2k+1}(-X)$, więc, dodając i odejmując $C_{2k+1}(X)$, dostajemy $D_{4k+2}(X) = [XC_{2k}(-X)-1]C_{2k+1}(X) + C_{2k+1}(X) + C_{2k+1}(-X)$. I ostatecznie

$$D_{4k+2}(X) = [-C_{2k+1}(-X)]\cdot C_{2k+1}(X) + 2D_{2k}(X). \quad \Diamond \tag{P5}$$

Ćwiczenie 3.7 (1) Wyznaczyć resztę z dzielenia $X^{100}-2X^{51}+1 \in \mathbb{Q}[X]$ przez X^2-1. **(2)** Wielomian $f(X) \in \mathbb{R}[X]$ daje przy dzieleniu przez $X+2$ resztę 3, a przy dzieleniu przez $X-3$ resztę -2. Jaką resztę daje wielomian $f(X)$ przy dzieleniu przez X^2-X-6?

Ćwiczenie 3.8 Dzielimy z resztą wielomian $X^{21}-1$ przez wielomian $X^4+X^3+2X^2+X+1$. Wyznaczyć współczynnik stojący przy X^{14} w (niepełnym) ilorazie.

3.2.3 Trzecia idea: twierdzenie Lagrange'*a* i o jednoznaczności

Twierdzenie Bézout'*a* zachodzi dla wielomianów o współczynnikach w d o w o l n y m pierścieniu. Wniosek WT3.2 zachodzi tylko dla dziedzin całkowitości. Również poniższe twierdzenie zachodzi w tym przypadku[2].

TWIERDZENIE 3.4 (***Twierdzenie Lagrange'a***[3]) *Jeżeli $\mathbb{K}$ jest ciałem, to wielomian stopnia $n \geqslant 1$ o współczynnikach w $\mathbb{K}$ ma c o n a j w y ż e j n pierwiastków w $\mathbb{K}$.*

D O W Ó D. Załóżmy, nie wprost, że wielomian $f(X)$ stopnia n ma $n+1$ (lub więcej) pierwiastków. Niech to będą $\alpha_1, \alpha_2, \ldots, \alpha_n$ i λ. Wówczas, na mocy wniosku WT3.2, możemy napisać $f(X) = (X-\alpha_1)(X-\alpha_2)\cdot\ldots\cdot(X-\alpha_n)\cdot a$, gdzie a oznacza wielomian stopnia 0, czyli n i e z e r o w y element ciała $\mathbb{K}$. Obliczając wartość wielomianu $f(X)$ dla argumentu λ mamy więc $0 = f(\lambda) = (\lambda-\alpha_1)(\lambda-\alpha_2)\cdot\ldots\cdot(\lambda-\alpha_n)\cdot a$. To jednakże jest niemożliwe, bo w ciele n i e m a dzielników zera, zobacz C1.19. □

U w a g a 1. Wielomian stopnia n może mieć m n i e j niż n pierwiastków (w ciele współczynników). Na przykład wielomian X^2+2X+1 ma tylko jeden pierwiastek $\alpha = -1$ (również w ciele liczb zespolonych!). A wielomian $X^3+X \in \mathbb{R}[X]$ ma również tylko jeden pierwiastek $\alpha = 0$ w zbiorze (ciele) liczb rzeczywistych $\mathbb{R}$. Sprawdźcie! Jednakże, gdy potraktujemy go jako wielomian o współczynnikach zespolonych, to ma on dokładnie trzy pierwiastki: $\alpha = 0, \beta = i, \gamma = -i$. Odpowiedni rozkład (3.5) ma w tym przypadku postać $X^3+X = (X-0)(X-i)(X-(-i))\cdot 1$, czyli $X^3+X = X(X-i)(X+i)$.

[2] W algebrze dowodzi się, że każda dziedzina całkowitości jest podpierścieniem pewnego ciała, tak zwanego **ciała ułamków**, tak jak pierścień $\mathbb{Z}$ liczb całkowitych jest podpierścieniem ciała $\mathbb{Q}$ liczb wymiernych.

[3] Lagrange udowodnił prawdziwość tego twierdzenia w przypadku, gdy $\mathbb{K} = \mathbb{F}_p$, zob. ustęp 5.4.3.

Oczywistym (wystarczy rozważyć wielomian $g(X) = f(X) - d$) wnioskiem z T3.4 jest:

WNIOSEK 1. *Jeżeli $f(X) \in \mathbb{K}[X]$ ma stopień $\leqslant n$ i dla $n+1$ różnych argumentów z ciała $\mathbb{K}$ przyjmuje daną wartość $d \in \mathbb{K}$, to $f(X) = d$.* □

Pokażemy ładny przykład zastosowania tego wniosku:

ZADANIE 3.3 Danych jest $2n$ liczb rzeczywistych $a_1, a_2, \ldots, a_n$ i $c_1, c_2, \ldots, c_n$. W (i, j)-te pole (czyli pole w przecięciu i-tego wiersza z j-tą kolumną) kwadratowej tablicy o wymiarach $n \times n$ wpisano liczbę $a_i + c_j$. Udowodnić, że jeżeli iloczyn liczb w wierszu nie zależy od wyboru wiersza, to iloczyn liczb w kolumnie nie zależy od wyboru kolumny.

R o z w i ą z a n i e. Rozważmy dwa wielomiany stopnia n:

$$f(X) = (X + a_1)(X + a_2) \cdot \ldots \cdot (X + a_n), \quad g(X) = (X - c_1)(X - c_2) \cdot \ldots \cdot (X - c_n).$$

Niech $r(X) = g(X) - f(X)$. Wielomian $r(X)$ ma stopień $\leqslant n-1$ i, zgodnie z założeniem, dla n różnych wartości argumentu, przyjmuje tę samą wartość (oznaczmy ją d):

$$r(-a_1) = r(-a_2) = \ldots = r(-a_n) = d.$$

Zatem, na mocy wniosku, wielomian $r(X)$ jest wielomianem stałym: $r(X) = d$. Stąd widzimy, że iloczyn liczb stojących w j-tej kolumnie, czyli $f(c_j)$, wynosi $f(c_j) = -(g(c_j) - f(c_j)) = -r(c_j) = -d$, i nie zależy od wyboru j. ◊

ZADANIE 3.4 Wyznaczyć wszystkie wielomiany $f(X) \in \mathbb{R}[X]$, spełniające warunek $xf(x-1) = (x+1)f(x)$ dla każdego $x \in \mathbb{R}$.

R o z w i ą z a n i e. Niech $f(X)$ będzie takim wielomianem. Kładąc $x = 0$ widzimy, że $0 = 1 \cdot f(0)$. Czyli $f(0) = 0$. Tę równość wykorzystamy jako b a z ę rozumowania indukcyjnego dowodzącego, że $f(n) = 0$ dla każdego $n \in \mathbb{N}$. Oto k r o k i n d u k c y j n y: jeżeli $f(k) = 0$, to $0 = (k+1)f(k) = (k+2)f(k+1)$, więc $f(k+1) = 0$. Wielomian $f(X)$ ma więc nieskończenie wiele pierwiastków. M u s i więc być wielomianem zerowym. ◊

Kolejnym wnioskiem z T3.4 jest poniższe twierdzenie o jednoznaczności:

WNIOSEK 2. (***Twierdzenie o jednoznaczności***) *Jeżeli $f(X) = \sum_k^n a_k X^k$ i $g(X) = \sum_k^n b_k X^k$ są dwoma wielomianami o współczynnikach w ciele $\mathbb{K}$, oraz $f(\alpha) = g(\alpha)$ dla każdego $\alpha \in A$, gdzie $A \subseteq \mathbb{K}$ jest podzbiorem mającym w i ę c e j niż n elementów, to $a_k = b_k$ dla każdego $k = 0, 1, 2, \ldots$, czyli $f(X) = g(X)$.*

D O W Ó D. Wynika bezpośrednio z poprzedniego wniosku zastosowanego do wielomianu $r(X)$ równego różnicy $f(X) - g(X)$. Wielomian ten ma bowiem stopień $\leqslant n$ i co najmniej $n+1$ razy przyjmuje wartość $d = 0$. Jest więc wielomianem zerowym. □

Oto przykładowe zastosowanie twierdzenia o jednoznaczności:

P r z y k ł a d. Dane są trzy (parami) różne liczby a, b, c. Chcemy udowodnić, że

$$L := \frac{(d-b)(d-c)}{(a-b)(a-c)} + \frac{(d-c)(d-a)}{(b-c)(b-a)} + \frac{(d-a)(d-b)}{(c-a)(c-b)} = 1$$

dla każdej liczby d. Myślimy o tym tak: Rozważamy wielomian

$$f(X) = \frac{(X-b)(X-c)}{(a-b)(a-c)} + \frac{(X-c)(X-a)}{(b-c)(b-a)} + \frac{(X-a)(X-b)}{(c-a)(c-b)}.$$

Jest on wielomianem stopnia $\leqslant 2$. Wystarczy więc znaleźć t r z y różne argumenty α, dla których $f(\alpha) = 1$, by stwierdzić, że $f(X) = 1$, w szczególności $L = f(d) = 1$. Sprawdzenie, że $\alpha = a, b, c$ są dobre, jest natychmiastowe. $\Diamond$

U w a g a 2. W matematyce szkolnej wielomian f j e s t f u n k c j ą określoną na zbiorze liczb rzeczywistych i zadaną wzorem $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, gdzie a_k są ustalonymi liczbami rzeczywistymi. W matematyce zaś, wielomian w y z n a c z a f u n k c j ę, zwaną **funkcją wielomianową**. To rozróżnienie jest w matematyce szkolnej (w świetle powyższego wniosku) b e z w i ę k s z e g o z n a c z e n i a, bowiem zbiór liczb rzeczywistych jest c i a ł e m i jest n i e s k o ń c z o n y. Wobec tego istnieje wzajemnie jednoznaczna odpowiedniość między wielomianami o współczynnikach rzeczywistych a funkcjami wielomianowymi określonymi na zbiorze liczb rzeczywistych. W ogólności tak dobrze n i e j e s t. W rozdziale 5 przekonamy się, że istnieją pierścienie (i ciała) mające tylko skończenie wiele elementów. Jeżeli $\mathcal{R} = \{\alpha_1, \alpha_2, \ldots, \alpha_s\}$ jest skończonym pierścieniem, w którym $1 \neq 0$, to wielomian

$$f(X) = (X-\alpha_1)(X-\alpha_2)\cdot \ldots \cdot (X-\alpha_s) \in \mathcal{R}[X]$$

jest n i e z e r o w y m wielomianem, ale wyznaczona przez niego funkcja $\lambda \longmapsto f(\lambda)$ przyjmuje wyłącznie wartości równe 0 (pierścienia $\mathcal{R}$). Przy okazji zauważmy, że pierścień, w którym $1 = 0$ składa się w y ł ą c z n i e z elementu 0, zobacz D1.7(4) i Z1.6(1).

3.2.4 Czwarta idea: pierwiastki wymierne

Czwarta podstawowa idea z dziedziny wielomianów dotyczy pierwiastków wymiernych wielomianów o współczynnikach c a ł k o w i t y c h. Odpowiednie twierdzenie to było przez nas sformułowane i udowodnione w ustępie 2.1.4, zobacz zadanie Z2.4.

Ćwiczenie 3.9 Udowodnić, że jeżeli $f(X) \in \mathbb{Z}[X]$ jest unormowany i liczba $k \in \mathbb{N}$ nie dzieli żadnej z liczb $f(a+j)$ dla pewnego $a \in \mathbb{Z}$ i wszystkich $1 \leqslant j \leqslant k$, to wielomian $f(X)$ nie ma pierwiastków wymiernych.

Ćwiczenie 3.10 Udowodnić, że jeżeli nieskracalny ułamek h/k jest pierwiastkiem wielomianu $f(X) = a_0 + a_1 X + \ldots + a_n X^n \in \mathbb{Z}[X]$, to $h - kt | f(t)$ dla każdej liczby całkowitej t. *Wskazówka.* Dla danej liczby całkowitej t rozważyć wielomian $g_t(X) = f(X+t)$.

N a j w a ż n i e j s z y m, z teoretycznego punktu widzenia, wnioskiem z zadania Z2.4, jest poniższe twierdzenie. Byłoby bardzo dobrze, gdyby Czytelnik udowodnił je szczegółowo, wszystko zrozumiał i na zawsze zachował w pamięci "operacyjnej".

TWIERDZENIE 3.5 *Jeżeli $\alpha \in \mathbb{Q}$ jest pierwiastkiem u n o r m o w a n e g o wielomianu o współczynnikach całkowitych (stopnia $\geqslant 1$), to $\alpha \in \mathbb{Z}$.* $\square$

3.2.5 Piąta idea: postać kanoniczna trójmianu kwadratowego

Piąta podstawowa idea z dziedziny wielomianów dotyczy **trójmianów kwadratowych**, czyli wielomianów drugiego stopnia, zapisywanych tradycyjnie w postaci

$$aX^2 + bX + c, \quad \text{gdzie} \quad a \neq 0. \tag{3.9}$$

Tym razem musimy ograniczyć się do przypadku, gdy $\mathbb{K}$ jest takim ciałem, w którym możliwe jest dzielenie przez 2, czyli ciałem, w którym $1 + 1 \neq 0$. Oczywiście, ciała $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ spełniają ten (dziwnie – dla początkującego matematyka – wyglądający) warunek.

Badając trójmian (3.9) sprowadzamy go do **postaci kanonicznej**. Robi się to za pomocą standardowej procedury **uzupełniania do (pełnego) kwadratu**:

$$aX^2 + bX + c = a\left(X^2 + 2 \cdot \tfrac{b}{2a}X + \left(\tfrac{b}{2a}\right)^2 - \left(\tfrac{b}{2a}\right)^2\right) + c = \boxed{\boxed{a\left(X + \tfrac{b}{2a}\right)^2 - \tfrac{\Delta}{4a},}} \tag{PK}$$

gdzie $\Delta = b^2 - 4ac$ jest tak zwanym **wyróżnikiem** trójmianu (3.9). Podkreślmy już w tym miejscu, że *wszystko czego dowiadujemy się w szkole (i poza szkołą) o trójmianie kwadratowym daje się odczytać z postaci kanonicznej.*

Pierwiastki trójmianu kwadratowego

Zaczniemy od problemu istnienia i (jeżeli istnieją) wyznaczania pierwiastków trójmianu (3.9). Z postaci kanonicznej łatwo widać, że prawdziwe jest:

TWIERDZENIE 3.6 *Jeżeli w ciele $\mathbb{K}$ istnieje taki element d, że $d^2 = \Delta$, to*

$$\boxed{\boxed{\alpha_1 = \frac{-b-d}{2a}, \qquad \alpha_2 = \frac{-b+d}{2a}}} \tag{3.10}$$

są pierwiastkami trójmianu (3.9)*, przy czym $\alpha_1 = \alpha_2 \Leftrightarrow \Delta = 0$. Jeżeli dla żadnego $d \in \mathbb{K}$ nie zachodzi równość $d^2 = \Delta$, to trójmian* (3.9) *nie ma pierwiastków w ciele $\mathbb{K}$.* □

Uwaga 1. Jeżeli trójmian (3.9) ma pierwiastki α_1, α_2, to równość (3.5) ma postać

$$aX^2 + bX + c = a(X - \alpha_1)(X - \alpha_2) \tag{3.11}$$

W przypadku $\alpha_1 = \alpha_2 = \alpha$ mówimy, że α jest **pierwiastkiem podwójnym**.

Uwaga 2. Element d spełniający warunek $d^2 = \Delta$ jest, oczywiście, pierwiastkiem wielomianu $f(X) = X^2 - \Delta$. Wobec tego w ciele mogą istnieć co najwyżej dwa takie elementy i, co więcej, jeżeli d jest takim pierwiastkiem, to drugim może być tylko $-d$. Takie d oznacza się zazwyczaj $\sqrt{\Delta}$ i nazywa się **pierwiastkiem kwadratowym** z Δ.

Uwaga 3. (1) W przypadku $\mathbb{K} = \mathbb{R}$ (typowy przypadek szkolny), warunkiem koniecznym i wystarczającym istnienia $\sqrt{\Delta}$ jest nieujemność: $\Delta \geqslant 0$. W przypadku $\mathbb{K} = \mathbb{C}$, każda liczba Δ ma pierwiastek kwadratowy. Wobec tego każdy trójmian kwadratowy o współczynnikach zespolonych ma pierwiastki w ciele liczb zespolonych. (3) W przypadku $\mathbb{K} = \mathbb{Q}$ warunek

$\Delta \geqslant 0$ jest wprawdzie warunkiem koniecznym istnienia pierwiastka kwadratowego $\sqrt{\Delta} \in \mathbb{Q}$, ale zdecydowanie nie jest warunkiem wystarczającym.

P r z y k ł a d 1. Niech $f_1(X) = X^2-7X+10$, $f_2(X) = X^2-7X+9$ i $f_3(X) = X^2-7X+13$. Mamy $\Delta_1 = 7^2 - 4 \cdot 10 = 3^2$, $\Delta_2 = 49 - 36 = 13 = (\sqrt{13})^2$ i $\Delta_3 = 49 - 52 = -3 = (\sqrt{3}i)^2$. Zatem $f_1(X)$ ma w ciele $\mathbb{Q}$ liczb wymiernych dwa pierwiastki: $\alpha_1 = \frac{7+3}{2} = 5$, $\alpha_2 = \frac{7-3}{2} = 2$, $f_2(X)$ nie ma pierwiastków wymiernych, ale ma w ciele $\mathbb{R}$ liczb rzeczywistych dwa pierwiastki: $\alpha_1 = \frac{7+\sqrt{13}}{2}$, $\alpha_2 = \frac{7-\sqrt{13}}{2}$, zaś trójmian $f_3(X)$ nie ma pierwiastków rzeczywistych, ale ma dwa pierwiastki zespolone $\alpha_1 = \frac{7+i\sqrt{3}}{2}$, $\alpha_2 = \frac{7-i\sqrt{3}}{2}$. $\Diamond$

P r z y k ł a d 2. Wyznaczymy wszystkie takie liczby całkowite x, że $|4x^2 + 12x - 27|$ jest liczbą pierwszą. Oto rozkład (3.11): $4X^2 + 12X - 27 = 4(X - 9/2)(X + 3/2)$. Stąd, dla każdego $x \in \mathbb{Z}$, $|4x^2 + 12x - 27| = |2x - 9| \cdot |2x + 3|$. Szansę na pierwszość mamy więc tylko, gdy $|2x - 9| = 1$ lub $|2x + 3| = 1$. $\Diamond$

Ćwiczenie 3.11 Dowieść, że trójmiany $f_1(X) = aX^2 + bX + c$, $f_2(X) = bX^2 + cX + a$ i $f_3(X) = cX^2 + aX + b$ mają w s p ó l n y pierwiastek wtedy i tylko wtedy, gdy $a + b + c = 0$.

Ćwiczenie 3.12 Załóżmy, że każdy z trójmianów $X^2 + 2aX + b^2$, $X^2 + 2bX + c^2 \in \mathbb{R}[X]$ ma dwa (różne) pierwiastki rzeczywiste. Uzasadnić, że wielomian $X^4 + 2(a^2 - 2c^2)X^2 + a^4$ nie ma pierwiastków rzeczywistych.

ZADANIE 3.5 Udowodnić, że z odcinków o długościach a, b, $c \in \mathbb{R}_{>0}$ można zbudować trójkąt wtedy i tylko wtedy, gdy zachodzi nierówność $2a^2b^2 + 2b^2c^2 + 2c^2a^2 > a^4 + b^4 + c^4$.

R o z w i ą z a n i e. Zapiszmy badaną nierówność tak: $a^4 - 2(b^2 + c^2)a^2 + (b^2 - c^2)^2 < 0$. To jest równoważne z faktem, że trójmian kwadratowy $f(X) = X^2 - 2(b^2 + c^2)X + (b^2 - c^2)^2$ przyjmuje wartość ujemną dla argumentu a^2. Napiszmy rozkład (3.11) dla tego trójmianu. Mamy $\Delta = 4(b^2 + c^2)^2 - 4(b^2 - c^2)^2 = 16b^2c^2$, więc $\sqrt{\Delta} = 4bc$. Stąd, na mocy wzorów (3.10), $\alpha_1 = (b - c)^2$, $\alpha_2 = (b + c)^2$. Wobec tego $f(X) = (X - (b - c)^2)(X - (b + c)^2)$. Przeto:

$$f(a^2) = (a^2 - (b - c)^2)((a^2 - (b + c)^2) = (a - b + c)(a + b - c)(a - b - c)(a + b + c).$$

Łatwo stąd wywnioskować, że $f(a^2) < 0$ wtedy i tylko wtedy, gdy $a + b > c$, $b + c > a$ i $c + a > b$. Pozostawiamy to Czytelnikowi. $\Diamond$

W finale 61 OM zadano takie zadanie:

ZADANIE 3.6 Dodatnie liczby wymierne a i b spełniają równość $a^3 + 4a^2b = 4a^2 + b^4$. Udowodnić, że liczba $\sqrt{a} - 1$ jest kwadratem liczby wymiernej.

R o z w i ą z a n i e. Równość $a^3 + 4a^2b = 4a^2 + b^4$ jest (jak łatwo sprawdzić) równoważna równości $a = \frac{(2a+b^2)^2}{(a+2b)^2}$. Widzimy stąd, że a jest kwadratem liczby wymiernej $d = \frac{2a+b^2}{a+2b}$. Równość $d = \frac{2a+b^2}{a+2b}$ interpretujemy tak: liczba b jest (wymiernym) pierwiastkiem trójmianu $f(X) = X^2 - 2dX + a(2 - d) \in \mathbb{Q}[X]$. Zatem, zobacz C3.13, wyróżnik $\Delta = 4d^2 - 4a(2 - d) = 4a(d - 1)$ tego trójmianu jest kwadratem liczby wymiernej. Zatem $d - 1 = \Delta/(2d)^2$ też jest kwadratem liczby wymiernej. $\Diamond$

Ćwiczenie 3.13 Udowodnić, że jeżeli $f(X) = aX^2+bX+c$ jest trójmianem kwadratowym o współczynnikach wymiernych i nieujemnym wyróżniku, to jego pierwiastki są w y m i e r n e wtedy i tylko wtedy, gdy wyróżnik $\Delta = b^2 - 4ac$ jest kwadratem liczby wymiernej.

3.2.6 Szósta idea: Wielomian jako funkcja rzeczywista

W szkole uczymy się przypadku r z e c z y w i s t e g o, to znaczy, że pierścieniem współczynników jest ciało $\mathbb{R}$ liczb rzeczywistych. O wielomianie (3.1) myślimy wtedy jak o (oznaczanej, dla uproszczenia, tym samym znaczkiem) f u n k c j i $f : \mathbb{R} \longrightarrow \mathbb{R}$ danej wzorem

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n, \tag{3.12}$$

porównaj 3.2.3 U2. Taki sposób myślenia jest charakterystyczny dla **analizy matematycznej** i w zasadzie wolimy rozwijać go w $\mathbb{RIN}$*'ie*, jednak kilka najprostszych własności trójmianów kwadratowych (i ogólniej, wielomianów) o współczynnikach rzeczywistych, traktowanych jako funkcje rzeczywiste, przyda się nam już teraz.

Twierdzenie 3.7 *Niech* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *będzie* ***funkcją kwadratową*** *daną za pomocą przepisu* $f(x) = ax^2 + bx + c$. *Załóżmy też, że* $a > 0$. *Wówczas:*

(1) *funkcja* f *jest malejąca w* $(-\infty; -b/2a]$ *i rosnąca w* $[-b/2a; \infty)$,

(2) *najmniejszą wartością funkcji* f *jest* $-\Delta/4a = f(-b/2a)$,

(3) *jeżeli* $f(x_1) < y_0 < f(x_2)$, *to między* x_1 *i* x_2 *istnieje taka liczba* x_0, *że* $f(x_0) = y_0$.

D O W Ó D. (1) Niech $x_1 < x_2 \leqslant -b/2a$. Wówczas $x_1 + b/2a < x_2 + b/2a \leqslant 0$. Zatem

$$f(x_1) = a\left(x_1 + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a} > a\left(x_2 + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a} = f(x_2).$$

Więc funkcja f jest malejąca w $(-\infty; -b/2a]$. Podobnie sprawdzamy drugą tezę.

(2) Ponieważ $z^2 \geqslant 0$ dla każdej liczby rzeczywistej z, więc dla każdego $x \in \mathbb{R}$

$$f(x) = a\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a} \geqslant -\frac{\Delta}{4a}$$

i równość zachodzi tylko dla $x = -b/2a$.

(3) Udowodnimy najpierw przypadek s z c z e g ó l n y, gdy $y_0 = 0$. Zakładamy więc, że $f(x_1) < 0$, $f(x_2) > 0$ i, b.s.o., $x_1 < x_2$. Mamy uzasadnić, że w przedziale $(x_1; x_2)$ istnieje pierwiastek (= miejsce zerowe) funkcji f. Przede wszystkim uzasadniamy, że pierwiastek w ogóle istnieje. Ponieważ $-\Delta/4a \leqslant f(x_1) < 0$ (bo $-\Delta/4a$ jest najmniejszą wartością), więc $\Delta > 0$. Biorąc pierwiastek arytmetyczny $d = \sqrt{\Delta}$, widzimy w (3.10) d w a pierwiastki $\alpha_1 < \alpha_2$. Z punktu (1) wiemy, że funkcja f maleje od wartości $0 = f(\alpha_1)$ do wartości najmniejszej $-\Delta/4a = f(-b/2a)$ w przedziale $[\alpha_1; -b/2a]$ i rośnie od wartości najmniejszej $-\Delta/4a$ do wartości $0 = f(\alpha_2)$ w przedziale $[-b/2a; \alpha_2]$. W całym przedziale $(\alpha_1; \alpha_2)$ przyjmuje więc wyłącznie wartości ujemne. I tylko tam(!). Z tego wynika, że $x_1 \in (\alpha_1; \alpha_2)$, a $x_2 \notin [\alpha_1; \alpha_2]$. Zatem: albo α_1 albo α_2 leży między x_1 i x_2. Dla dowodu w przypadku ogólnym patrzymy na funkcję $g : \mathbb{R} \longrightarrow \mathbb{R}$ daną wzorem $g(x) = f(x) - y_0$. To jest funkcja wielomianowa wyznaczona przez trójmian kwadratowy $g(X) = aX^2 + bX + c - y_0$. □

U w a g a 1. Czytelnik z pewnością potrafi zmienić to co zmienić należy, gdy $a < 0$.

U w a g a 2. Własność wyrażona w T3.7(3) nazywa się **własnością przyjmowania wartości pośrednich** lub **własnością Darboux**. Przysługuje ona wszystkim (zdefiniowanym na

przedziale) rzeczywistym **funkcjom ciągłym**, w szczególności wszystkim funkcjom wielomianowym (3.12). Dowód podamy w $\mathbb{RIN}$. Tam też dowiemy się, że każda funkcja wielomianowa (3.12) stopnia n i e p a r z y s t e g o dla wszystkich, dostatecznie dużych, $n \in \mathbb{N}$ spełnia warunek $f(-n)f(n) < 0$, więc że prawdziwe jest poniższe twierdzenie:

TWIERDZENIE 3.8 *Wielomian $f(X) \in \mathbb{R}[X]$ stopnia n i e p a r z y s t e g o ma co najmniej jeden pierwiastek rzeczywisty.* □

Pokażemy parę przykładów zastosowań T3.7.

P r z y k ł a d 1. Dane są liczby rzeczywiste $c_1, c_2, \ldots, c_n$. Wyznaczamy taką liczbę rzeczywistą, że suma kwadratów jej odległości od liczb c_i jest najmniejsza możliwa. Czyli znajdujemy argument, dla którego funkcja kwadratowa

$$f(x) = (x - c_1)^2 + (x - c_2)^2 + \ldots + (x - c_n)^2$$

przyjmuje najmniejszą wartość. Z T3.7(2) widzimy, że $x_{\min} = \dfrac{1}{n}(c_1 + c_2 + \cdots + c_n)$. ◊

P r z y k ł a d 2. Załóżmy, że $(4u - 2v + w)(u + v + w) + w(4u + 2v + w) = -1$ dla liczb $u, v, w \in \mathbb{R}$. Udowodnimy, że $v^2 > 4uw$. Rzeczywiście, warunek oznacza, że $f(-2)f(1) + f(0)f(2) = -1$, gdzie $f(x) = ux^2 + vx + w$. Stąd wnosimy, że co najmniej jeden z iloczynów $f(-2)f(1)$, $f(0)f(2)$ jest ujemny. Zatem, zobacz T3.7(3), trójmian f m a p i e r w i a s t e k (gdzieś w przedziale $(-2; 2)$). Wobec tego jego wyróżnik jest dodatni. ◊

P r z y k ł a d 3. Szlachetnym zastosowaniem jest dowód ***nierówności Schwarza***:

$$(a_1b_1 + a_2b_2 + \cdots + a_nb_n)^2 \leqslant (a_1^2 + a_2^2 + \cdots + a_n^2)(b_1^2 + b_2^2 + \cdots + b_n^2), \tag{3.13}$$

dla dowolnych układów $a_1, a_2, \ldots, a_n$ i $b_1, b_2, \ldots, b_n$ liczb rzeczywistych. Dla dowodu rozważmy trójmian kwadratowy $f(x) = Ax^2 + 2Sx + B$, gdzie $A = a_1^2 + \cdots + a_n^2$, $B = b_1^2 + \cdots + b_n^2$ i $S = a_1b_1 + \cdots + a_nb_n$. Zauważamy, że nierówność (3.13) jest równoważna nierówności $\Delta \leqslant 0$. A to wynika z oczywistego faktu, że funkcja kwadratowa wyznaczona przez trójmian $f(X)$ dana jest wzorem

$$f(x) = (a_1x - b_1)^2 + (a_2x - b_2)^2 + \ldots + (a_nx - b_n)^2,$$

z którego widać, że przyjmuje ona w y ł ą c z n i e wartości nieujemne. Może mieć więc co najwyżej jedno miejsce zerowe. Czyli rzeczywiście $\Delta \leqslant 0$. Co więcej, równość $\Delta = 0$ zachodzi tylko w przypadku, gdy istnieje taka liczba λ (pierwiastek trójmianu $f(X)$), że $\lambda a_i = b_i$ dla każdego $i = 1, \ldots, n$. Mówimy wtedy, że układy $a_1, a_2, \ldots, a_n$ i $b_1, b_2, \ldots, b_n$ są proporcjonalne. ◊

ZADANIE 3.7 Dany jest trójmian kwadratowy $f(X) = X^2 + aX + b \in \mathbb{R}[X]$. Udowodnić, że istnieje taka liczba $x \in [-1; 1]$, że $|f(x)| \geqslant \frac{1}{2}$.

R o z w i ą z a n i e. Załóżmy, nie wprost, że $|f(x)| < \frac{1}{2}$ dla wszystkich $x \in [-1; 1]$ i porównajmy $f(x)$ z funkcją kwadratową $g(x) = x^2 - 1/2$. Z założeń mamy $f(-1) - g(-1) < 0$, $f(0) - g(0) > 0$ i $f(1) - g(1) < 0$. Dzięki własności Darboux wnosimy stąd, że funkcja wielomianowa $f - g$ ma miejsce zerowe w przedziale $(-1; 0)$ i miejsce zerowe w przedziale $(0; 1)$. To daje sprzeczność, bowiem $f(x) - g(x) = ax + b - \frac{1}{2}$ jest funkcją wielomianową stopnia $\leqslant 1$, a taka może mieć dwa miejsca zerowe tylko gdy jest tożsamościowo równa 0, co tu nie ma miejsca, bo $f(0) - g(0) > 0$. ◊

3.2.7 Siódma idea: wzory Viète'*a*

Siódma podstawowa idea z dziedziny wielomianów dotyczy sumy i iloczynu pierwiastków trójmianu (3.9). Również tym razem zakładamy, że $1+1 \neq 0$. Ciała, w których $1+1=0$ nazywają się **ciałami charakterystyki** 2.

TWIERDZENIE 3.9 (***wzory Viète'a***) *Jeżeli* α_1, α_2 *są pierwiastkami trójmianu* (3.9), *to zachodzą równości*

$$\begin{cases} \alpha_1+\alpha_2 &= -\dfrac{b}{a}, \\ \alpha_1\alpha_2 &= \dfrac{c}{a}. \end{cases} \tag{3.14}$$

I odwrotnie, przy zadanych elementach a, b, $c \in \mathbb{K}$, *przy czym* $a \neq 0$, *rozwiązaniem układu równań* (3.14) *jest, z dokładnością do permutacji, para pierwiastków trójmianu* (3.9).

D O W Ó D. Wystarczy policzyć korzystając ze wzorów (3.10) i równości $\Delta^2 = b^2-4ac$. Odwrotnie, załóżmy, że para (α_1, α_2) jest rozwiązaniem układu (3.14). Wówczas, wstawiając, wyliczone z pierwszej równości, $\alpha_2 = -b/a - \alpha_1$, do drugiej równości, otrzymujemy równość $\alpha_1(-b/a-\alpha_1) = c/a$ równoważną równości $a\alpha_1^2 + b\alpha_1 + c = 0$. To pokazuje, że α_1 jest pierwiastkiem wielomianu (3.9). Jasne, że tak samo sprawdzamy, że α_2 jest pierwiastkiem tego wielomianu. □

Pokażemy kilka zadań na zastosowanie wzorów Viète'*a*.

ZADANIE 3.8 Dowieść, że jeżeli trójmian kwadratowy $f(X) = aX^2+bX+c \in \mathbb{Z}[X]$ ma pierwiastek wymierny, to co najmniej jedna z liczb a, b, c jest parzysta.

R o z w i ą z a n i e. Niech α będzie wymiernym pierwiastkiem wielomianu $f(X)$. Wówczas $0 = af(\alpha) = (a\alpha)^2 + b(a\alpha) + ac$. Stąd widzimy, że liczba w y m i e r n a $u_1 = a\alpha$ jest pierwiastkiem u n o r m o w a n e g o wielomianu $g(X) = X^2+bX+ac$ o współczynnikach całkowitych. Zatem, $u_1 \in \mathbb{Z}$, zobacz T3.5. Drugi pierwiastek u_2 wielomianu $g(X)$ jest, na mocy wzoru Viète'*a*, równy $-b-u_1$. Jest więc również liczbą całkowitą. Jednocześnie $u_1u_2 = ac$. Stąd $abc = -u_1u_2(u_1+u_2)$. Ponieważ trzy liczby całkowite u_1, u_2, u_1+u_2 n i e mogą być jednocześnie nieparzyste, więc mamy tezę. ◊

ZADANIE 3.9 Trójmian $f_1(X) = X^2+a_1X+b_1$ ma pierwiastki φ_1, ψ_1, a inny trójmian $f_2(X) = X^2+a_2X+b_2$ ma pierwiastki φ_2, ψ_2. Wyrazić za pomocą współczynników a_1, b_1, a_2, b_2 iloczyn $R(f_1, f_2) := (\varphi_1-\varphi_2)(\psi_1-\varphi_2)(\varphi_1-\psi_2)(\psi_1-\psi_2)$.

R o z w i ą z a n i e. Iloczyn pierwszych dwóch czynników, czyli $\varphi_1\psi_1 - (\varphi_1+\psi_1)\varphi_2 + \varphi_2^2$, jest, na mocy wzorów Viète'*a*, równy $b_1 + a_1\varphi_2 + \varphi_2^2 = f_1(\varphi_2)$. Podobnie, iloczyn trzeciego i czwartego czynnika jest równy $f_1(\psi_2)$. Wobec tego, $R(f_1, f_2) = (b_1+a_1\varphi_2+\varphi_2^2)(b_1+a_1\psi_2+\psi_2^2)$. Stąd, korzystając z równości Viète'*a* $\varphi_2+\psi_2 = -a_2$ i $\varphi_2\psi_2 = b_2$, łatwo dostajemy:

$$R(f_1, f_2) = (b_1-b_2)^2 + (a_1-a_2)(a_1b_2-a_2b_1). \quad \Diamond \tag{3.15}$$

ZADANIE 3.10 Załóżmy, że r jest nieparzystą liczbą całkowitą. Oznaczmy przez α, β pierwiastki trójmianu kwadratowego X^2-rX-1 i niech $a_n=\alpha^n+\beta^n$ dla $n\in\mathbb{Z}$. Udowodnić, że liczby a_{-2017} i a_{2016} są całkowite i względnie pierwsze.

Rozwiązanie. Zauważmy, że $a_{n+1}=(\alpha+\beta)(\alpha^n+\beta^n)-\alpha\beta(\alpha^{n-1}+\beta^{n-1})=ra_n+a_{n-1}$ dla dowolnego $n\in\mathbb{Z}$. Mamy więc związek rekurencyjny pozwalający wyznaczać liczby a_n z (dwóch) poprzednich, ale również z (dwóch) następnych. Dla znajomości całego ciągu $(a_n)_{n\in\mathbb{Z}}$ wystarczy więc znać dwa kolejne wyrazy. Ponieważ $a_0=2$, $a_1=r$, więc jesteśmy już prawie w domu: ponieważ zarówno rekurencja "w przód" $a_{n+1}=ra_n+a_{n-1}$, jak i rekurencja "w tył" $a_{n-1}=-ra_n+a_{n+1}$ zwraca liczby całkowite, więc dowód całkowitości liczb a_{-2017} i a_{2016} mamy załatwiony. Dzięki równości $\alpha\beta=-1$ widzimy, że $a_{-n}=\alpha^{-n}+\beta^{-n}=\frac{\alpha^n+\beta^n}{(\alpha\beta)^n}=(-1)^na_n$. Zatem $a_{-2017}=-a_{2017}$. Przypomnijmy sobie teraz twierdzenie T2.10. Dzięki niemu mamy równości $\mathrm{NWD}\,(a_{n+1},\,a_n)=\mathrm{NWD}\,(a_n,\,a_{n-1})$. Stąd, przez oczywistą indukcję, $\mathrm{NWD}\,(a_{n+1},\,a_n)=\mathrm{NWD}\,(a_1,\,a_0)=\mathrm{NWD}\,(r,\,2)=1$ (pamiętamy o nieparzystości r). $\Diamond$

U w a g a 1. Wzory Viète'*a* pozwalają wyznaczyć, za pomocą współczynników a, b, c, różne **funkcje symetryczne** pierwiastków α_1, α_2 trójmianu (3.9). Na przykład

$$\alpha_1^2+\alpha_2^2=(\alpha_1+\alpha_2)^2-2\alpha_1\alpha_2=\left(-\frac{b}{a}\right)^2-2\cdot\frac{c}{a}=\frac{b^2-2ac}{a^2},$$

$$\alpha_1^3+\alpha_2^3=(\alpha_1+\alpha_2)^3-3\alpha_1\alpha_2(\alpha_1+\alpha_2)=\frac{-b^3+3abc}{a^3}.\ \Diamond$$

Ćwiczenie 3.14 Dane są liczby a, b, c, gdzie $ac\neq bc$ i α_1, α_2, α_3. Ponadto, α_1, α_2 są pierwiastkami trójmianu $X^2+aX+bc$, a α_2, α_3 są pierwiastkami trójmianu $X^2+bX+ac$. Udowodnić, że wówczas α_1, α_3 są pierwiastkami trójmianu $X^2+cX+ab$.

Ćwiczenie 3.15 Niech u, v będą pierwiastkami trójmianu $X^2+pX-1/(2p^2)\in\mathbb{R}[X]$. Udowodnić, że zachodzi nierówność $u^4+v^4\geqslant 2+\sqrt{2}$.

W powyższych zadaniach dostrzegamy taką i d e ę: *Istnieje ścisły związek między parą liczb* $(\alpha,\,\beta)$ *a wielomianem* $(X-\alpha)(X-\beta)$, *którego te liczby są pierwiastkami.* Wykorzystywanie tej idei nazwijmy (na nasz użytek) **filozofią Viète'a**. Oto prosta teza tej filozofii: *Jeżeli znamy sumę* $\alpha+\beta$ *i iloczyn* $\alpha\beta$ *liczb* α, β, *to znamy te liczby (z dokładnością do przestawienia).* Rzeczywiście, jeżeli $\alpha+\beta=p$, $\alpha\beta=q$, to liczby α, β są pierwiastkami równania kwadratowego $x^2-px+q=0$, a te pierwiastki umiemy wyznaczyć[4] (czyli znamy).

P r z y k ł a d 1. Załóżmy, że chcemy rozwiązać układ równań

$$\begin{cases} u+uv+v=19,\\ u^2+v^2=10. \end{cases}$$

Zgodnie z filozofią Viète'*a* badamy wielomian $(X-u)(X-v)=X^2-pX+q$. Widzimy, że $p+q=19$ i $p^2-2q=10$. Mnożąc pierwszą z tych równości przez 2 i dodając do drugiej,

[4]Ta teza jest całkowicie prawdziwa w ś w i e c i e z e s p o l o n y m. Gdy poruszamy się tylko w świecie liczb rzeczywistych, musimy przedtem z b a d a ć w y r ó ż n i k, czyli liczbę $p^2-4q=(\alpha+\beta)^2-4\alpha\beta=(\alpha-\beta)^2$. Widzimy, że jeżeli liczby α, β mają być rzeczywiste, to musi zachodzić nierówność $p^2-4q\geqslant 0$.

otrzymamy $p^2+2p=48$, czyli $(p+1)^2=49$. Stąd $p=6$ lub $p=-8$. I, odpowiednio $q=13$ lub $q=27$. Mamy więc $\Delta=p^2-4q=-16$ lub $\Delta=-44$. Co oznacza, że badany układ równań n i e ma rozwiązań rzeczywistych. Na marginesie: pary $(3-2i,\ 3+2i)$ i $(-4-\sqrt{-11},\ -4+\sqrt{-11})$, a także $(3+2i,\ 3-2i)$ i $(-4+\sqrt{-11},\ -4-\sqrt{-11})$, są rozwiązaniami badanego układu w dziedzinie zespolonej. ◊

Pięknym i bardzo ważnym przykładem myślenia w duchu filozofii Viète'a jest poniższe:

ZADANIE 3.11 Udowodnić, że jeżeli co najmniej jedna z liczb a, b jest wymierna, a suma $a+b$ i iloczyn ab są całkowite, to a i b są liczbami całkowitymi.

R o z w i ą z a n i e. Załóżmy, że $a\in\mathbb{Q}$ oraz $a+b,\ ab\in\mathbb{Z}$. Wówczas wielomian unormowany $(X-a)(X-b)=X^2-(a+b)X+ab$ jest wielomianem o współczynnikach całkowitych. Zatem, zobacz T3.5, jego wymierny pierwiastek a j e s t liczbą całkowitą. Wobec tego również $b=(a+b)-a$ jest liczbą całkowitą. U w a g a. Założenie wymierności co najmniej jednej z liczb a, b, jest ważne. Kontrprzykład: $a=3+2\sqrt{2}$, $b=3-2\sqrt{2}$. ◊

P r z y k ł a d 2. *Jeżeli m, n są takimi niezerowymi liczbami całkowitymi, że $\frac{m}{n}+\frac{n}{m}$ jest liczbą całkowitą, to $|m|=|n|$.* Rzeczywiście, ponieważ $\frac{m}{n}\cdot\frac{n}{m}=1\in\mathbb{Z}$, więc, na mocy Z3.11, $n|m$ i $m|n$. Stąd, zobacz C2.2, $|n|\leqslant|m|$ i $|m|\leqslant|n|$. ◊

P r z y k ł a d 3. *Jeżeli $x^2y^2|x^5+y^5$ dla pewnych $x,\ y\in\mathbb{N}$, to $x^2|y^3$.* Rzeczywiście, liczby wymierne $a=x^3/y^2$ i $b=y^3/x^2$ spełniają założenia zadania Z3.11. ◊

Skoki Viète'a

Jednym z przykładów myślenia w duchu filozofii Viète'a jest **technika skoków Viète'a** (*Vieta's jumpings*). Technika ta staje się coraz bardziej popularna w OM. Jej istotę zobaczyć można w rozwiązaniu poniższego zadania.

ZADANIE 3.12 Liczby naturalne a, b spełniają warunek $ab|a^2+b^2+2$. Udowodnić, że zachodzi równość $(a^2+b^2+2)/ab=4$.

R o z w i ą z a n i e. Dla danej liczby naturalnej k oznaczmy przez $\mathcal{A}(k)$ zbiór wszystkich takich par uporządkowanych $(a,\ b)$ liczb naturalnych, że $a^2+b^2+2=kab$. Teza zadania mówi więc, że *jeżeli zbiór $\mathcal{A}(k)$ jest niepusty, to $k=4$*. Łatwo widzieć niepustość zbioru $\mathcal{A}(4)$: na przykład pary $(1,\ 1)$ i $(3,\ 1)$ należą do $\mathcal{A}(4)$.

Weźmy więc liczbę naturalną $k\neq4$, załóżmy, nie wprost, że $\mathcal{A}(k)\neq\varnothing$ i że $(a,\ b)\in\mathcal{A}(k)$. Zauważamy najpierw, że wówczas $a\neq b$. Rzeczywiście, gdyby $a=b$, to podzielność $a^2|2a^2+2$ dałaby (Zasada Podstawowa!) podzielność $a^2|2$. Wtedy $a=1$. Zatem $a=b=1$, więc $(a,\ b)\notin\mathcal{A}(k)$, bo $k\neq4$. Załóżmy więc, że $a>b$. Równość $a^2+b^2+2=kab$ interpretujemy następująco: liczba a jest pierwiastkiem trójmianu kwadratowego

$$f(X)=X^2-kbX+b^2+2\in\mathbb{Z}[X]. \tag{3.16}$$

Niech $\widetilde{a}$ będzie d r u g i m pierwiastkiem tego trójmianu. Z zadania Z3.11 wiemy, że $\widetilde{a}$ jest liczbą całkowitą. Co więcej, druga równość Viète'a $a\widetilde{a}=b^2+2$ dowodzi, że $\widetilde{a}>0$. Więc $\widetilde{a}$ jest liczbą naturalną i para $(b,\ \widetilde{a})$ również jest elementem zbioru $\mathcal{A}(k)$. Wykażemy teraz, że zachodzi nierówność $b\geqslant\widetilde{a}$. Gdyby było odwrotnie, czyli gdyby $b<\widetilde{a}$, to (Zasada Skwantowania!) $b+1\leqslant\widetilde{a}$, co, łącznie z założoną nierównością $b+1\leqslant a$ i drugą równością Viète'a,

dałoby nierówność nieprawdziwą: $(b+1)^2 \leqslant a\widetilde{a} = b^2+2$. Ponieważ, jak wiemy, w zbiorze $\mathcal{A}(k)$ nie ma par postaci (c, c), więc w rzeczywistości zachodzi nierówność $b > \widetilde{a}$. Możemy więc znowu wykonać **skok Viète'a**: rozważyć trójmian $f_1(X) = X^2 - k\widetilde{a}X + \widetilde{a}^2 + 2$ i jego pierwiastki b i $\widetilde{b}$. W ten sposób znajdziemy kolejną parę $(\widetilde{a}, \widetilde{b})$ należącą do zbioru $\mathcal{A}(k)$, przy czym $a > b > \widetilde{a} > \widetilde{b} > 0$. Jasne, że czegoś takiego n i e da się kontynuować w nieskończoność. Uzyskana sprzeczność kończy rozwiązanie. ◊

U w a g a 2. Przedstawione rozumowanie jest charakterystyczne dla tak zwanej **metody desantu nieskończonego**. Nieskończone schodzenie $a > b > \widetilde{a} > \widetilde{b} > \ldots$ można "przeciąć" już w pierwszym kroku, dokładając na początku rozumowania założenie, że para (a, b) jest takim elementem zbioru $\mathcal{A}(k)$, dla którego wartość sumy $a+b$ jest n a j m n i e j s z a. (Jeżeli zbiór $\mathcal{A}(k)$ jest niepusty, i składa się z par liczb naturalnych, to, na mocy Zasady Minimum, para z najmniejszą sumą i s t n i e j e.) Wówczas sprzeczność znajdujemy już w pierwszym kroku.

U w a g a 3. Przejście od pary $(a, b) \in \mathcal{A}(k)$ do pary $(b, \widetilde{a}) \in \mathcal{A}(k)$ nazwaliśmy **skokiem Viète'a**. W rozwiązaniu wykorzystaliśmy "skok w dół". Można też wykorzystać "skok wzwyż":

P r z y k ł a d 4. Udowodnimy, że zbiór $\mathcal{A}(4)$ z zadania Z3.12 jest zbiorem nieskończonym. Startujemy od pary $(a_1, b_1) := (1, 1)$ należącej do zbioru $\mathcal{A}(4)$. To znaczy, że liczba 1 jest pierwiastkiem trójmianu $X^2 - 4X + 3$. Drugim pierwiastkiem tego trójmianu jest 3. W ten sposób z pary $(1, 1)$ wykonaliśmy skok Viète'a do pary $(a_2, b_2) := (1, 3)$. Ta para prowadzi do trójmianu $X^2 - 12X + 11$, którego mniejszym pierwiastkiem jest 1. Drugim pierwiastkiem tego trójmianu jest liczba 11. W ten sposób z pary $(1, 3)$ wykonaliśmy skok Viète'a do pary $(a_3, b_3) := (3, 11)$. Itd. Jeżeli, dla danego $n \geqslant 3$, mamy parę (a_n, b_n), gdzie $a_n < b_n$, to $\widetilde{a_n}$, drugi (obok a_n) pierwiastek równania $x^2 - 4b_n x + b_n^2 + 2 = 0$, jest w i ę k s z y niż b_n. W ten sposób powstaje para $(a_{n+1}, b_{n+1}) := (b_n, \widetilde{a_n})$. Z pierwszej równości Viète'a mamy $b_{n+1} = 4b_n - a_n$. Widzimy piękny skok Viète'a

$$(a_n, b_n) \curvearrowright (a_{n+1}, b_{n+1}) := (b_n, 4b_n - a_n).$$

Ten skok jest "skokiem wzwyż", bowiem $a_{n+1} + b_{n+1} = 5b_n - a_n > a_n + b_n$. Łatwo sprawdzić, że ciąg (a_n) spełnia równanie rekurencyjne $a_{n+2} = 4a_{n+1} - a_n$ dla każdego $n \in \mathbb{N}$. W rozdziale 9 nauczymy się teoryjki, dzięki której będziemy mogli uzasadnić, że zachodzi następująca równość:

$$a_n = \frac{(\sqrt{3}-1)(2+\sqrt{3})^{n-1} + (\sqrt{3}+1)(2-\sqrt{3})^{n-1}}{2\sqrt{3}}. \quad \Diamond$$

Ćwiczenie 3.16 Czy w opisany powyżej sposób znajdujemy w s z y s t k i e pary (a, b) ze zbioru $\mathcal{A}(4)$?

Ćwiczenie 3.17 Udowodnić, że jeżeli liczby naturalne c, d są takie, że $k = \frac{c^2+d^2+1}{cd}$ jest liczbą naturalną, to $k = 3$. Udowodnić, że równanie $x^2 + y^2 + 1 = 3xy$ ma rozwiązanie w liczbach naturalnych większych niż 20162017.

Ćwiczenie 3.18 Udowodnić, że istnieją takie $x, y, u, v \in \mathbb{N}_{\geqslant 2016}$, że zachodzi równość

$$\frac{x}{yuv} + \frac{y}{uvx} + \frac{u}{vxy} + \frac{v}{xyu} = \frac{1}{x} + \frac{1}{y} + \frac{1}{u} + \frac{1}{v}.$$

W OM (na poziomie IMO) technika skoków Viète'a pojawiła się w Australii w roku 1988, kiedy to tylko kilku uczestników poradziło sobie z takim zadaniem:

ZADANIE 3.13 Dane są takie liczby naturalne a, b, że iloraz $\dfrac{a^2+b^2}{1+ab}$ jest też liczbą naturalną. Udowodnić, że ten iloraz jest kwadratem liczby naturalnej.

Rozwiązanie. Zorganizujmy rozwiązanie podobnie jak rozwiązanie Z3.12: dla danej liczby naturalnej k oznaczmy przez $\mathcal{B}(k)$ zbiór wszystkich takich par (a, b) liczb naturalnych, że $a^2+b^2 = k(1+ab)$. Teza zadania brzmi więc tak: *jeżeli $\mathcal{B}(k)$ jest zbiorem niepustym, to k jest kwadratem.*

Weźmy więc liczbę $k \in \mathbb{N}$ nie będącą kwadratem, załóżmy, nie wprost, że $\mathcal{B}(k) \neq \varnothing$ i że $(a, b) \in \mathcal{B}(k)$. Zauważmy najpierw, że wówczas $a \neq b$. Rzeczywiście, gdyby $a = b$, to byłoby $k = (a^2+b^2)/(1+ab) = 2a^2/(1+a^2) < 2$, czyli $k = 1$, a to jest kwadrat. Bez straty ogólności załóżmy więc, że $a > b$. Równość $a^2+b^2 = k(1+ab)$ interpretujemy następująco: liczba a jest pierwiastkiem trójmianu

$$f(X) = X^2 - kbX + b^2 - k \in \mathbb{Z}[X]. \tag{3.17}$$

Niech $\widetilde{a}$ będzie drugim pierwiastkiem tego trójmianu. Z zadania Z3.11 wiemy, że $\widetilde{a}$ jest liczbą całkowitą. Sprawdzamy, że $\widetilde{a} > 0$: gdyby $\widetilde{a} = 0$, to $0 = f(\widetilde{a}) = b^2 - k$ i $k = b^2$ wbrew założeniu; gdyby zaś $\widetilde{a} < 0$, to z równości $0 = f(\widetilde{a}) = \widetilde{a}^2 - kb\widetilde{a} + b^2 - k$ dostalibyśmy równość niemożliwą $\widetilde{a}^2 + b^2 = k(1+\widetilde{a}b)$ (po jej lewej stronie jest liczba dodatnia, a po prawej stronie liczba niedodatnia). Dostajemy teraz rozstrzygającą nierówność:

$$\widetilde{a} = \frac{b^2-k}{a} < \frac{a^2-k}{a} < a.$$

(Równość jest, inaczej zapisaną, równością Viète'a $a\widetilde{a} = b^2 - k$.) Znajdujemy się w ten sposób w sytuacji niemożliwego desantu nieskończonego: jeżeli $(a, b) \in \mathcal{B}(k)$, gdzie $k \in \mathbb{N}$ nie jest kwadratem, to w zbiorze $\mathcal{B}(k)$ znajdzie się para $(\widetilde{a}, b)$ z mniejszą sumą. $\Diamond$

Uwaga 4. W związku z powyższym zadaniem powstaje naturalne pytanie, czy dla danej liczby $n \in \mathbb{N}$ zbiór $\mathcal{B}(n^2)$ jest niepusty. Łatwo sprawdzić, że $\mathcal{B}(1) = \{(1, 1)\}$. Ponieważ $(2, 8) \in \mathcal{B}(4)$, więc, podobnie jak w powyższym P4, można, "skacząc wzwyż", wyznaczyć wszystkie elementy zbioru $\mathcal{B}(4)$. Po zapoznaniu się z dalszymi fragmentami skryptu Czytelnik będzie w stanie wykazać, że najmniejszym elementem w $\mathcal{B}(9)$ jest para $(2133, 18\,957)$. Itp.

3.3 Jednoznaczność rozkładu w pierścieniu wielomianów

Ten paragraf ma charakter teoretyczny. Chcemy w nim udowodnić twierdzenie o istnieniu i jednoznaczności rozkładu wielomianu o współczynnikach z danego ciała na iloczyn wielomianów nierozkładalnych (będących analogonami liczb pierwszych). Wykład prowadzimy według wzorca z rozdziału 2. Również oznaczenia wybraliśmy analogiczne.

W dalszym ciągu $\mathbb{K}$ oznacza ustalone ciało. Pierścień który badamy, jest pierścieniem $\mathbb{K}[X]$ wielomianów jednej zmiennej X o współczynnikach z ciała $\mathbb{K}$. Przede wszystkim musimy wyznaczyć **grupę jedności** w pierścieniu $\mathbb{K}[X]$, a następnie musimy się przekonać, że w tym pierścieniu nie ma dzielników zera:

Ćwiczenie 3.19 Uzasadnić, że $\mathbb{K}[X]^*$ (zobacz D1.8) składa się ze wszystkich wielomianów stopnia zero. Możemy (i będziemy) więc utożsamiać: $\mathbb{K}[X]^* = \mathbb{K}^* = \mathbb{K} \setminus \{0\}$. *Wskazówka.* Wykorzystać C3.6.

Ćwiczenie 3.20 Udowodnić, że w pierścieniu $\mathbb{K}[X]$ n i e m a dzielników zera. To znaczy, że jeżeli $a(X)b(X) = 0$, to $a(X) = 0$ lub $b(X) = 0$. *Wskazówka.* Patrz C3.6.

3.3.1 Podzielność w pierścieniu wielomianów

Definicja podzielności w pierścieniu $\mathbb{K}[X]$ naśladuje definicję podzielności w pierścieniu $\mathbb{Z}$.

Definicja 3.6 Mówimy, że wielomian $b(X) \in \mathbb{K}[X]$ **dzieli** wielomian $a(X) \in \mathbb{K}[X]$, gdy istnieje taki wielomian $q(X) \in \mathbb{K}[X]$, że

$$a(X) = b(X) \cdot q(X).$$

Zapisujemy to tak: $b(X)|a(X)$ lub, po prostu, $b|a$. Mówimy też w takiej sytuacji, że wielomian $b(X)$ jest **dzielnikiem** wielomianu $a(X)$ lub, że wielomian $a(X)$ jest **wielokrotnością** wielomianu $b(X)$. Zbiór wszystkich wielokrotności wielomianu $b = b(X)$ oznaczamy symbolem $(b) = (b(X))$ i nazywamy **ideałem głównym generowanym** przez $b(X)$.

Ćwiczenie 3.21 Udowodnić, że jeżeli $b(X) \neq 0$, to $b|a$ wtedy i tylko wtedy, gdy reszta z dzielenia wielomianu $a(X)$ przez wielomian $b(X)$ jest wielomianem zerowym.

Ćwiczenie 3.22 Udowodnić, że $b(X)|a(X)$ wtedy i tylko wtedy, gdy $(a) \subseteq (b)$.

Ćwiczenie 3.23 Jeżeli $b|a$, to $\deg b \leqslant \deg a$.

ZADANIE 3.14 Udowodnić analogony tez (1), (2), (3), (4) twierdzenia T2.1.

R o z w i ą z a n i e. Jedynie teza (3) jest nowa i mówi, że jeżeli $a|b$ i $b|a$, to istnieje taki niezerowy element $u \in \mathbb{K}$, że $a(X) = ub(X)$. To wynika z porównania stopni: jeżeli $a(X) = u(X)b(X)$ dla pewnego wielomianu $u(X) \in \mathbb{K}[X]$, to $\deg a = \deg u + \deg b$, zobacz C3.6. Ale $\deg a \leqslant \deg b$, bo $a|b$. Stąd $\deg u = 0$, czyli $u(X)$ jest niezerową stałą $u \in \mathbb{K}$. $\Diamond$

Definicja 3.7 Jeżeli $a(X), b(X) \in \mathbb{K}[X]$ i istnieje taki niezerowy element $u \in \mathbb{K}$, że $a(X) = ub(X)$, to mówimy, że wielomiany $a(X)$ i $b(X)$ są **stowarzyszone** i oznaczamy to tak: $a(X) \sim b(X)$.

Ćwiczenie 3.24 Dane są niezerowe wielomiany $a(Y), b(Y) \in \mathbb{K}[Y]$. Dowieść, że $a(Y) \sim b(Y)$ wtedy i tylko wtedy, gdy $a(Y)|b(Y)$ i $b(Y)|a(Y)$.

Ćwiczenie 3.25 Wykazać, że równość $(a(X)) = (b(X))$ zachodzi wtedy i tylko wtedy, gdy $a(X) \sim b(X)$.

3.3.2 Ideał. Największy wspólny dzielnik

W zbiorze (pierścieniu) liczb całkowitych $\mathbb{Z}$ duże usługi oddało nam pojęcie ideału, a zwłaszcza fakt, że każdy ideał w $\mathbb{Z}$ jest ideałem głównym. Okazuje się, że podobny fakt ma miejsce w pierścieniu $\mathbb{K}[X]$ wielomianów jednej zmiennej o współczynnikach z ciała $\mathbb{K}$.

Definicja 3.8 Podzbiór $I \subseteq \mathbb{K}[X]$ nazywamy **ideałem**, gdy zawiera wielomian zerowy 0 oraz spełnia następujące warunki:

(1) jeżeli $a(X) \in I$ i $b(X) \in I$, to $a(X) + b(X) \in I$,

(2) jeżeli $k(X) \in \mathbb{Z}[X]$ i $a(X) \in I$, to $k(X)a(X) \in I$.

Ćwiczenie 3.26 Udowodnić, że iloczyn teoriomnogościowy (czyli część wspólna) dowolnej rodziny ideałów pierścienia $\mathbb{K}[X]$ jest ideałem.

Ćwiczenie 3.27 Udowodnić, że jeżeli $a(X)$, $b(X)$ są wielomianami w $\mathbb{K}[X]$, to zbiór

$$(a,\, b) := \{a(X)s(X) + b(X)t(X) : s(X),\, t(X) \in \mathbb{K}[X]\} \tag{3.18}$$

jest ideałem w $\mathbb{K}[X]$. Jest to **ideał generowany przez wielomiany** $a(X)$, $b(X)$.

Arcyważnym twierdzeniem jest analogon twierdzenia T2.3.

TWIERDZENIE 3.10 *Każdy ideał w pierścieniu $\mathbb{K}[X]$ jest ideałem głównym.*

D O W Ó D. Dowód tego twierdzenia przebiega według takiego samego schematu jak dowód twierdzenia T2.3. Jeżeli ideał $I \subseteq \mathbb{K}[X]$ zawiera tylko jeden element, to $I = (0)$. Jeżeli zawiera elementy niezerowe, to niech $d(X)$ będzie niezerowym wielomianem n a j n i ż s z e g o s t o p n i a należącym do I. Wówczas dowolny wielomian $a(X)$ należący do I jest wielokrotnością $d(X)$. Rzeczywiście, dzieląc z resztą, mamy

$$a(X) = q(X)d(X) + r(X), \quad \text{gdzie} \quad \deg r(X) < \deg d(X).$$

Stąd, ponieważ $r(X) = a(X) - q(X)d(X) \in I$, mamy $r(X) = 0$. Czyli $d|a$. Widzimy więc, że $I \subseteq (d)$. Ponieważ zawieranie przeciwne jest oczywiste, więc mamy ostatecznie $I = (d)$. To kończy dowód. □

Mówimy, że pierścień $\mathbb{K}[X]$ jest **dziedziną ideałów głównych**.

Podamy teraz definicję największego wspólnego dzielnika dwóch wielomianów. Czytelnik zechce porównać tę definicję z definicją D2.4.

Definicja 3.9 Niech dane będą dwa, nie równe oba zero, wielomiany $a(X)$, $b(X) \in \mathbb{K}[X]$. Wielomian $d(X) \in \mathbb{K}[X]$ nazywa się **największym wspólnym dzielnikiem** wielomianów $a(X)$ i $b(X)$, gdy

(1) $d(X)|a(X)$ i $d(X)|b(X)$ ($d(X)$ jest wspólnym dzielnikiem),

(2) jeżeli $e(X)|a(X)$ i $e(X)|b(X)$, to $e(X)|d(X)$, ($d(X)$ jest podzielny przez każdy wspólny dzielnik).

Nie wiemy jeszcze, czy taki wielomian $d(X)$ istnieje! Jeżeli tak jest, to oznaczamy go symbolem $\mathrm{NWD}\,(a(X),\, b(X))$ lub $\mathrm{NWD}\,(a,\, b)$. Istnienie największego wspólnego dzielnika dwóch wielomianów w y n i k a z faktu, że każdy ideał jest ideałem głównym:

TWIERDZENIE 3.11 (***Gauss***) *Jeżeli wielomiany $a(X)$, $b(X)$ nie są oba równe zero, to i s t n i e j e największy wspólny dzielnik tych wielomianów. Jest on wyznaczony jednoznacznie z dokładnością do mnożenia przez element niezerowy, czyli z dokładnością do relacji stowarzyszenia. Ponadto istnieją takie wielomiany $s(X)$, $t(X) \in \mathbb{K}[X]$, że*

$$\mathrm{NWD}\,(a(X),\, b(X)) = a(X)s(X) + b(X)t(X).$$

D O W Ó D. Rozważmy ideał $(a,\, b)$, zob. (3.18). Wiemy, że jest on główny. Niech więc:

$$(d(X)) = (a(X),\, b(X)) = \{a(X)s(X) + b(X)t(X) : s(X),\, t(X) \in \mathbb{K}[X]\}.$$

Twierdzimy, że $d(X) = \mathrm{NWD}\,(a(X),\, b(X))$. Dowód przebiega tak samo (*mutatis mutandis*) jak dowód T2.4. □

Ćwiczenie 3.28 Udowodnić, że jeżeli dla wielomianów a, b, przy czym $b \neq 0$, i wielomianów q, r zachodzi równość $a(X) = q(X)b(X) + r(X)$, to $\mathrm{NWD}\,(a,\, b) = \mathrm{NWD}\,(b,\, r)$.

Ćwiczenie 3.29 Sformułować i udowodnić poprawność ***algorytmu Euklidesa w*** pierścieniu $\mathbb{K}[X]$ wielomianów jednej zmiennej o współczynnikach w c i e l e.

Ćwiczenie 3.30 Dla jakiej wartości $k \in \mathbb{Q}$ wielomiany $X^4 + kX^2 + 1$ i $X^3 + kX + 1$ mają wspólny pierwiastek? *Wskazówka.* Wykorzystać algorytm Euklidesa.

3.3.3 Zasadnicze twierdzenie arytmetyki wielomianów

Dokładnie tak samo (*mutatis mutandis*) jak w pierścieniu liczb całkowitych dochodzimy do zasadniczego twierdzenia arytmetyki w pierścieniu wielomianów o współczynnikach w ciele.

Definicja 3.10 Wielomiany $a(X)$, $b(X) \in \mathbb{K}[X]$ takie, że $\mathrm{NWD}\,(a(X),\, b(X)) \sim 1$ nazywamy wielomianami **względnie pierwszymi**.

Ćwiczenie 3.31 Udowodnić, że wielomiany $a(X)$, $b(X)$ są względnie pierwsze wtedy i tylko wtedy, gdy istnieją takie wielomiany $s(X)$, $t(X)$, że $a(X)s(X) + b(X)t(X) = 1$.

Sformułujemy teraz analogon zasadniczego twierdzenia arytmetyki:

TWIERDZENIE 3.12 (***Zasadnicze Twierdzenie Arytmetyki w*** $\mathbb{K}[X]$) *Dla dowolnych wielomianów $a(X)$, $b(X)$ i $c(X)$ z pierścienia $\mathbb{K}[X]$ zachodzi*

$$\boxed{\boxed{\textit{jeżeli } a(X)|b(X)c(X) \textit{ i } \mathrm{NWD}\,(a(X),\, b(X)) \sim 1,\ \textit{to } a(X)|c(X)}}.$$

D O W Ó D. Dowód różni się tylko tym czym musi od dowodu twierdzenia T2.7. □

Ćwiczenie 3.32 Sformułować i rozwiązać analogony następujących zadań: C2.12, Z2.3, C2.13, C2.14, C2.15, C2.18 i C2.19.

3.3.4 Wielomiany nierozkładalne

Analogonami liczb pierwszych w pierścieniach wielomianów są wielomiany nierozkładalne. W szkole uczymy się, że liczba pierwsza to taka, która ma mało dzielników. Równoważnie, taka, której się w żaden istotny sposób nie da rozłożyć na iloczyn dwóch czynników: zawsze któryś z nich okaże się być równym ± 1. Definicja wielomianu nierozkładalnego jest (prawie) automatycznym przetłumaczeniem, na przypadek pierścienia $\mathbb{K}[X]$, szkolnej definicji liczby pierwszej w $\mathbb{N}$:

Definicja 3.11 Wielomian $p(X) \in \mathbb{K}[X]$ nazywa się **wielomianem nierozkładalnym**, gdy $\deg p(X) \geqslant 1$ i ma następującą własność: jeżeli $p(X) = a(X)b(X)$ dla pewnych wielomianów $a(X), b(X) \in \mathbb{K}[X]$, to $\deg a = 0$ lub $\deg b = 0$.

Ćwiczenie 3.33 Każdy wielomian stopnia pierwszego jest nierozkładalny. Udowodnić, że wielomian $aX^2 + bX + c \in \mathbb{K}[X]$ stopnia drugiego jest nierozkładalny wtedy i tylko wtedy, gdy wyróżnik $\Delta = b^2 - 4ac$ nie jest kwadratem żadnego elementu z ciała $\mathbb{K}$.

Ćwiczenie 3.34 Udowodnić, że wielomian trzeciego stopnia jest nierozkładalny w $\mathbb{K}[X]$ wtedy i tylko wtedy, gdy nie ma pierwiastków w $\mathbb{K}$.

Ćwiczenie 3.35 Jeżeli $p(X)$ jest wielomianem nierozkładalnym, to dla danego wielomianu $a(X) \in \mathbb{K}[X]$, albo $p(X)|a(X)$, albo $\mathrm{NWD}\,(p, a) \sim 1$.

Udowodnimy teraz bardzo ważną charakteryzację wielomianów nierozkładalnych. Jest ona analogiczna do charakteryzacji liczb pierwszych podanej w T2.15.

Twierdzenie 3.13 *Wielomian $p(X)$ jest wielomianem nierozkładalnym wtedy i tylko wtedy, gdy dla dowolnych wielomianów $a(X), b(X) \in \mathbb{K}[X]$ zachodzi implikacja:*

$$p(X)|a(X)b(X) \quad \Longrightarrow \quad p(X)|a(X) \quad \textit{lub} \quad p(X)|b(X). \tag{3.19}$$

Dowód. ($\Longrightarrow$) Niech $p(X)$ będzie wielomianem nierozkładalnym, niech $p(X)|a(X)b(X)$ i niech $p(X) \nmid a(X)$. Wówczas, na mocy C3.35, $\mathrm{NWD}\,(a, p) \sim 1$, więc, na mocy ZTA w pierścieniu $\mathbb{K}[X]$, zobacz T3.12, $p(X)|b(X)$.

($\Longleftarrow$) Jeżeli $p(X)$ nie jest nierozkładalny, to istnieją takie wielomiany $a(X), b(X)$, że $p(X) = a(X)b(X)$ i $\deg a(X), \deg b(X) < \deg p(X)$. Wtedy $p(X)|a(X)b(X)$, ale $p(X) \nmid a(X)$ i $p(X) \nmid b(X)$, bo wielomiany a i b mają za małe stopnie. Zatem $p(X)$ nie spełnia (3.19). □

Ćwiczenie 3.36 Uzasadnić przez indukcję, że jeżeli wielomian nierozkładalny jest dzielnikiem iloczynu n wielomianów, to jest dzielnikiem co najmniej jednego czynnika tego iloczynu.

3.3.5 Jednoznaczność rozkładu

Zrealizujemy teraz ważny cel tego rozdziału: udowodnimy, że w pierścieniu wielomianów jednej zmiennej o współczynnikach z ciała zachodzi twierdzenie o jednoznaczności rozkładu na iloczyn wielomianów nierozkładalnych.

TWIERDZENIE 3.14 (***O jednoznaczności rozkładu w*** $\mathbb{K}[X]$) *Dowolny wielomian* $f(X) \in \mathbb{K}[X]$ *stopnia* > 0 *daje się zapisać w postaci iloczynu wielomianów nierozkładalnych:*

$$\boxed{\boxed{f(X) = p_1(X)p_2(X) \cdot \ldots \cdot p_s(X).}}$$

Przedstawienie takie jest jednoznaczne w takim sensie: Jeżeli $f(X) = q_1(X)q_2(X) \cdot \ldots \cdot q_t(X)$ *jest również przedstawieniem wielomianu* $f(X)$ *w postaci iloczynu wielomianów nierozkładalnych, to* $s = t$ *i, po ewentualnym przenumerowaniu,*

$$p_1(X) \sim q_1(X), \quad p_2(X) \sim q_2(X), \quad \ldots, \quad p_s(X) \sim q_s(X).$$

D O W Ó D. Dowód jest teraz (po zrobionych przygotowaniach) prosty i naśladuje dowód T2.16. Najpierw dowodzimy analogonu T2.14, czyli że każdy wielomian stopnia $\geqslant 1$ dzieli się przez wielomian nierozkładalny. Gdyby tak nie było, to niech $f(X)$ będzie wielomianem najniższego stopnia, który nie dzieli się przez żaden wielomian nierozkładalny. Wówczas wielomian $f(X)$ n i e jest nierozkładalny (bo dzieli się przez siebie), więc istnieją takie wielomiany $b(X), c(X) \in \mathbb{K}[X]$ stopnia $\geqslant 1$, że $f(X) = b(X)c(X)$. Ale wówczas $b(X)$ dzieli się przez jakiś wielomian nierozkładalny, nazwijmy go $p(X)$, bo ma stopień $< \deg f$. Zatem i $f(X)$ dzieli się przez $p(X)$. Sprzeczność.

Dowód jednoznaczności przeprowadzamy tak samo (*mutatis mutandis*) jak dowód T2.16, wykorzystując C3.36 zamiast C2.39. □

3.4 Dalsze twierdzenia o wielomianach

W tym paragrafie nauczymy się paru nowych rzeczy o wielomianach. Zaczynamy od ważnego przypadku pieścienia $\mathbb{Z}[X]$ wielomianów jednej zmiennej o współczynnikach całkowitych. Okazuje się, że, mimo że $\mathbb{Z}$ n i e jest ciałem i w pierścieniu $\mathbb{Z}[X]$ n i e istnieje algorytm dzielenia z resztą, w $\mathbb{Z}[X]$ prawdziwy jest analogon twierdzenia T3.14 o jednoznaczności rozkładu. Poznamy kilka metod badania nierozkładalności wielomianów w pierścieniu $\mathbb{Q}[X]$, w szczególności za pomocą kryterium Eisensteina. W pierścieniu $\mathbb{C}[X]$ wielomianów jednej zmiennej o współczynnikach zespolonych nierozkładalne są jedynie wielomiany stopnia pierwszego. Ta teza jest tylko innym sformułowaniem tak zwanego Zasadniczego Twierdzenia Algebry. Po omówieniu tego twierdzenia przechodzimy do rozkładu tak zwanych wielomianów podziału koła $X^n - 1$ na iloczyn wielomianów cyklotomicznych, do rozwiązywania równań trzeciego stopnia, wzorów Viète'*a*, wielomianów palindromicznych, wielomianu interpolacyjnego Lagrange'*a* i rozkładu funkcji wymiernych na ułamki proste.

3.4.1 Zawartość wielomianu

Wielomiany o współczynnikach całkowitych można d o d a w a ć i m n o ż y ć (i w wyniku otrzymuje się wielomiany o współczynnikach całkowitych). To oznacza, że zbiór $\mathbb{Z}[X]$ wszystkich takich wielomianów j e s t p i e r ś c i e n i e m. Jasne jest, co oznacza, że jeden taki wielomian d z i e l i drugi taki, patrz definicja D3.6. Ponieważ w pierścieniu $\mathbb{Z}$ liczb całkowitych nie ma dzielników zera, więc równość z ćwiczenia C3.6 jest prawdziwa. Zobaczymy najpierw które elementy w $\mathbb{Z}[X]$ są odwracalne (zobacz D1.8):

Ćwiczenie 3.37 $\mathbb{Z}[X]^* = \mathbb{Z}^* = \{-1, +1\}$. Udowodnić te równości.

Jeżeli $f(X) = f_0 + f_1X + \ldots + f_nX^n$ jest dowolnym wielomianem o współczynnikach całkowitych, $C = \mathrm{NWD}\,(f_0, f_1, \ldots, f_n)$ jest największym wspólnym dzielnikiem jego współczynników, to możemy zapisać

$$f(X) = C(a_0 + a_1X + \ldots + a_nX^n), \tag{3.20}$$

gdzie $f_k = C \cdot a_k$. Wiemy, porównaj C2.12, że wówczas największy wspólny dzielnik współczynników wielomianu $a_0+a_1X+\ldots+a_nX^n$ jest równy 1. Wielomiany mające taką własność nazywamy wielomianami pierwotnymi:

Definicja 3.12 Wielomian $a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$ nazywa się **wielomianem pierwotnym**, gdy $\mathrm{NWD}\,(a_0, a_1, \ldots, a_n) = 1$.

Pierwsze twierdzenie w tym paragrafie jest kolejnym lematem Gaussa:

LEMAT 3.1 (***Lemat Gaussa***) *Jeżeli $f(X), g(X) \in \mathbb{Z}[X]$ są dwoma wielomianami pierwotnymi, to ich iloczyn $f(X)g(X)$ jest wielomianem pierwotnym.*

D O W Ó D. Niech $f(X) = a_0+a_1X+\ldots+a_kX^k$, $g(X) = b_0+b_1X+\ldots+b_lX^l$. Wówczas $f(X)g(X) = c_0 + c_1X + \ldots + c_nX^n$ gdzie

$$c_t = \sum_{i=0}^{t} a_{t-i}b_i.$$

Załóżmy nie wprost, że $\mathrm{NWD}\,(c_0, c_1, \ldots, c_n) \neq 1$ i niech p będzie taką liczbą pierwszą, że $p|c_0, p|c_1, \ldots, p|c_n$. Ponieważ $\mathrm{NWD}\,(a_0, a_1, \ldots, a_k) = \mathrm{NWD}\,(b_0, b_1, \ldots, b_l) = 1$, więc p nie może dzielić ani wszystkich a_i, ani wszystkich b_j. Niech $p|a_0, p|a_1, \ldots, p|a_s$ i $p \nmid a_{s+1}$ oraz $p|b_0, p|b_1, \ldots, p|b_t$ i $p \nmid b_{t+1}$. Rozważmy współczynnik

$$c_{s+t+2} = a_0b_{s+t+2} + \ldots + a_{s+1}b_{t+1} + \ldots + a_{s+t+2}b_0.$$

Ponieważ wszystkie, z wyjątkiem $a_{s+1}b_{t+1}$, iloczyny po prawej stronie są podzielne przez p, więc mamy sprzeczność, bo $p|c_{s+t+2}$, zobacz Zasadę Podstawową. □

Lemat Gaussa L3.1 dostarcza podstawowego narzędzia w dowodzie twierdzenia Gaussa, które mówi, że rozkład w pierścieniu $\mathbb{Q}[X]$ wielomianu o współczynnikach całkowitych jest w istocie tym samym, co rozkład tego wielomianu w pierścieniu $\mathbb{Z}[X]$.

Wielomiany o współczynnikach wymiernych mają tak zwaną zawartość:

Definicja 3.13 Jeżeli $f(X) = f_0 + f_1X + \ldots + f_nX^n \in \mathbb{Q}[X]$ jest niezerowym wielomianem o współczynnikach wymiernych, to **zawartością** tego wielomianu nazywamy taką liczbę wymierną $C = C(f) > 0$, dla której zachodzi równość

$$f(X) = C(f)(a_0 + a_1X + \ldots + a_nX^n) = C(f)a(X),$$

gdzie $a(X) = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$ jest wielomianem pierwotnym.

ZADANIE 3.15 Udowodnić, że niezerowy wielomian o współczynnikach wymiernych ma dokładnie jedną zawartość.

Rozwiązanie. Jeżeli $f(X) = \sum a_k X^k \in \mathbb{Q}[X]$ i $m > 0$ jest wspólnym mianownikiem wszystkich liczb wymiernych $a_k = \frac{b_k}{m}$, a $d = \mathrm{NWD}\,(b_0, b_1, \ldots, b_n)$, to $f(X) = \frac{d}{m}(b'_0 + b'_1 X + \ldots + b'_n X^n)$, gdzie $b_k = db'_k$. Kładąc $C(f) = \frac{d}{m}$ widzimy, że istnieje takie $C = C(f) \in \mathbb{Q}_{>0}$, że $f(X) = C(f)a(X)$, gdzie $a(X) \in \mathbb{Z}[X]$ jest wielomianem pierwotnym.

Załóżmy teraz, że $f(X) = C \cdot a(X) = \widetilde{C} \cdot \widetilde{a}(X)$, gdzie $a(X), \widetilde{a}(X) \in \mathbb{Z}[X]$ są pierwotne, a $C, \widetilde{C} \in \mathbb{Q}_{>0}$. Wówczas, oznaczając $\frac{C}{\widetilde{C}} = \frac{a}{b}$, gdzie $\mathrm{NWD}\,(a, b) = 1$, mamy

$$ah_k = b\widetilde{h}_k \quad \text{dla każdego} \quad k \leqslant \deg f.$$

Tu, przez h_k (odpowiednio $\widetilde{h}_k$) oznaczyliśmy współczynnik wielomianu $a(X)$ (odpowiednio $\widetilde{a}(X)$) stojący przy X^k. Dzięki ZTA mamy $a|\widetilde{h}_k$, $b|h_k$ dla każdego k. Z pierwotności wielomianów a, $\widetilde{a}$ mamy więc $a = \pm 1$, $b = \pm 1$, co kończy dowód jednoznaczności. ◊

ZADANIE 3.16 Udowodnić, że dla dowolnych dwóch niezerowych wielomianów $f(X)$, $g(X) \in \mathbb{Q}[X]$ zachodzi równość $C(fg) = C(f) \cdot C(g)$.

Rozwiązanie. Teza jest natychmiastowym wnioskiem z Z3.15 i L3.1. ◊

Twierdzenie 3.15 (***Gauss***) *Jeżeli $f(X) \in \mathbb{Z}[X]$ i $f(X) = g(X)h(X)$ jest rozkładem na iloczyn wielomianów o współczynnikach wymiernych, to istnieją takie wielomiany $\overline{g}(X)$, $\overline{h}(X)$ o współczynnikach całkowitych, że*

$$f(X) = \overline{g}(X)\overline{h}(X) \quad \textit{oraz} \quad \overline{g}(X) \sim g(X), \quad \overline{h}(X) \sim h(X).$$

DOWÓD. Niech $g(X) = C(g)a(X)$, $h(X) = C(h)b(X)$ będą rozkładami wielomianów $g(X)$, $h(X)$ na iloczyn zawartości i części pierwotnych $a, b \in \mathbb{Z}[X]$. Wówczas $C(g) \cdot C(h) = C(gh) = C(f) \in \mathbb{Z}$. Wystarczy położyć $\overline{G}(X) = C(f)a(X)$, $\overline{H}(X) = b(X)$. □

Widzimy, że nierozkładalność wielomianu o współczynnikach całkowitych w pierścieniu $\mathbb{Z}[X]$ pociąga za sobą jego nierozkładalność w pierścieniu $\mathbb{Q}[X]$. Wnioskiem z T3.14 i powyższego jest:

Twierdzenie 3.16 (***Twierdzenie o jednoznaczności rozkładu w*** $\mathbb{Z}[X]$) *Każdy wielomian $f(X) \in \mathbb{Z}[X]$ stopnia większego niż zero da się zapisać w postaci iloczynu wielomianów nierozkładalnych w $\mathbb{Z}[X]$:*

$$f(X) = p_1(X)p_2(X) \cdot \ldots \cdot p_s(X).$$

Ponadto przedstawienie takie jest jednoznaczne w następującym sensie: Jeżeli

$$f(X) = q_1(X)q_2(X) \cdot \ldots \cdot q_t(X)$$

jest również przedstawieniem wielomianu $f(X)$ w postaci iloczynu wielomianów nierozkładalnych, to $s = t$ i, po ewentualnym przenumerowaniu,

$$p_1(X) \sim q_1(X), \quad p_2(X) \sim q_2(X), \quad \ldots, \quad p_s(X) \sim q_s(X).$$

□

3.4.2 Wielomiany nierozkładalne w $\mathbb{Q}[X]$

Wiemy, że wielomiany nierozkładalne w pierścieniu wielomianów o współczynnikach w danym ciele grają rolę elementarnych cegiełek, z których zbudowane są inne wielomiany tego pierścienia, zobacz T3.14. Warto więc wiedzieć, k t ó r e wielomiany są nierozkładalne w danym pierścieniu $\mathbb{K}[X]$. Zajmiemy się teraz tym problemem w przypadku $\mathbb{K} = \mathbb{Q}$ i pokażemy parę przykładów rozumowań pokazujących nierozkładalność wybranych wielomianów o współczynnikach wymiernych (równoważnie, jak wiemy z twierdzenia Gaussa, całkowitych).

Oto pierwszy przykład:

P r z y k ł a d 1. Załóżmy, że wielomian $f(X) \in \mathbb{Z}[X]$ ma stopień n i spełnia warunki: $|f(x_j)| \in \mathbb{P}$ dla pewnych (różnych) liczb całkowitych $x_1, x_2, \ldots, x_{2n+1}$. Chcemy udowodnić nierozkładalność $f(X)$. Zakładamy (nie wprost), że $f(X) = g(X)h(X)$ jest rozkładem w $\mathbb{Z}[X]$ na iloczyn dwóch wielomianów stopni mniejszych niż n (korzystamy tu oczywiście z twierdzenia Gaussa T3.15). Oznaczmy $k = \deg g(X)$, $l = \deg h(X)$. Wówczas mamy $2n+1$ równości $|g(x_j)| \cdot |h(x_j)| = p_j$, gdzie p_j są liczbami pierwszymi (niekoniecznie różnymi). Stąd, dla każdego j, albo $g(x_j) = \pm 1$, albo $h(x_j) = \pm 1$. Oznaczmy przez $\mathcal{G}_+ = \{j : g(x_j) = 1\}$, $\mathcal{G}_- = \{j : g(x_j) = -1\}$, $\mathcal{H}_+ = \{j : h(x_j) = 1\}$ i $\mathcal{H}_- = \{j : h(x_j) = -1\}$. Zbiory te są parami rozłączne(!), a ich sumą jest zbiór $\{1, 2, \ldots, 2n+1\}$. Ponadto, na mocy W1T3.4 $\operatorname{card}(\mathcal{G}_+) \leqslant k$, $\operatorname{card}(\mathcal{G}_-) \leqslant k$ i $\operatorname{card}(\mathcal{H}_+) \leqslant l$, $\operatorname{card}(\mathcal{H}_-) \leqslant l$. Stąd mamy sprzeczność: $2n+1 = k+k+l+l = 2n$. $\Diamond$

Ćwiczenie 3.38 Niech $|f(0)| = |f(1)| = |f(2)| = |f(3)| = |f(4)| = 1$ dla wielomianu $f(X) \in \mathbb{Z}[X]$ stopnia 5. Udowodnić, że wielomian $f(X)$ jest nierozkładalny w $\mathbb{Q}[X]$.

ZADANIE 3.17 Liczby $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ są parami różne. Udowodnić, że wielomian $(X-a_1)(X-a_2)\cdot \ldots \cdot (X-a_n) - 1$ jest nierozkładalny w $\mathbb{Q}[X]$.

R o z w i ą z a n i e. Załóżmy nie wprost, że

$$(X-a_1)(X-a_2)\cdot \ldots \cdot (X-a_n) - 1 = f(X)g(X), \tag{3.21}$$

gdzie $f(X), g(X) \in \mathbb{Z}[X]$ są unormowane i

$$\deg f(X), \deg g(X) \leqslant n-1. \tag{3.22}$$

Obliczamy wartości obu stron równości (3.21) dla argumentów $a_1, a_2, \ldots, a_n$. Znajdujemy $f(a_k)g(a_k) = -1$ dla każdego $1 \leqslant k \leqslant n$. To, wobec całkowitości, może zajść tylko, gdy $f(a_k) = 1$, $g(a_k) = -1$ lub $f(a_k) = -1$, $g(a_k) = 1$. Zatem, wielomian $f(X) + g(X)$, który (na mocy (3.22)) ma stopień $\leqslant n-1$, przyjmuje wartość 0 dla n różnych argumentów $a_1, \ldots, a_n$. Więc, zobacz W1T3.4, $f(X) + g(X) = 0$. Stąd wynika, że równość (3.21) ma postać $(X-a_1)(X-a_2)\cdot \ldots \cdot (X-a_n) - 1 = -f(X)^2$. Ale taka równość jest niemożliwa, bo wielomian z lewej strony jest wielomianem unormowanym, a współczynnik przy najwyższej potędze X ze strony prawej jest równy -1. $\Diamond$

Jedno ogólne twierdzenie o nierozkładalności wielomianów o współczynnikach całkowitych obowiązuje każdego olimpijczyka:

TWIERDZENIE 3.17 (***Kryterium Eisensteina***) *Jeśli* $a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$ *i istnieje taka liczba pierwsza* p*, że*

$$p|a_0, \quad p|a_1, \quad \ldots, \quad p|a_{n-1}, \quad p \nmid a_n \qquad \text{oraz} \qquad p^2 \nmid a_0,$$

to wielomian $a_0 + a_1X + \ldots + a_nX^n$ *jest nierozkładalny w* $\mathbb{Q}[X]$.

D O W Ó D. Załóżmy nie wprost, że

$$a_0 + a_1X + \ldots + a_nX^n = (b_0 + b_1X + \ldots + b_kX^k)(c_0 + c_1X + \ldots + c_lX^l)$$

jest rozkładem naszego wielomianu na iloczyn dwóch czynników stopnia co najmniej pierwszego o współczynnikach całkowitych. Wówczas $p|b_0c_0$, więc, nie zmniejszając ogólności rozważań, możemy uznać, że $p|b_0$. Ale wtedy $p \nmid c_0$, bo $p^2 \nmid a_0$. Jednocześnie $p|b_0c_1 + b_1c_0$, zatem $p|b_1c_0$, więc $p|b_1$. Podobnie, ponieważ $p|b_0c_2 + b_1c_1 + b_2c_0$, więc $p|b_2$. Postępując tak dalej widzimy, że $p|b_0$, $p|b_1$, $\ldots$, $p|b_k$. To jest niemożliwe, bo $b_kc_l = a_n$, a $p \nmid a_n$. Sprzeczność. □

Kryterium Eisensteina rzadko udaje się zastosować bezpośrednio. Jeden przykład takiego bezpośredniego zastosowania pokazujemy w poniższym ćwiczeniu:

Ćwiczenie 3.39 Udowodnić, że jeżeli dla liczby całkowitej a i liczby pierwszej p, zachodzi równość $v_p(a) = 1$, gdzie $v_p(a)$ oznacza wykładnik p-adyczny liczby a, to wielomian $X^n + a$ jest nierozkładalny w $\mathbb{Q}[X]$.

Kryterium Eisensteina czasem daje się zastosować po stosownej zamianie zmiennej. Klasyczny przykład widzimy w poniższym zadaniu:

ZADANIE 3.18 Jeżeli p jest liczbą pierwszą, to wielomian (tzw. wielomian cyklotomiczny, zob. 3.4.6) $\Phi_p(X) = 1 + X + X^2 + \ldots + X^{p-1}$ jest nierozkładalny w $\mathbb{Q}[X]$.

R o z w i ą z a n i e. Korzystając z rozkładu (zobacz też tożsamość "nieśmiertelną" (1.8)) $X^p - 1 = (X-1)(1 + X + \ldots + X^{p-2} + X^{p-1})$ i dokonując podstawienia $X - 1 = Y$ widzimy, że nasz wielomian (względem nowej zmiennej Y) ma postać

$$\frac{(Y+1)^p - 1}{Y} = Y^{p-1} + \binom{p}{1}Y^{p-2} + \ldots + \binom{p}{p-2}Y + \binom{p}{p-1},$$

do której bezpośrednio stosuje się kryterium Eisensteina, zobacz C2.50. ◊

Ćwiczenie 3.40 Do wielomianu $14 + 3X - 3X^2 + 2X^3$ nie można bezpośrednio zastosować kryterium Eisensteina. Znaleźć taką liczbę całkowitą a, by zamiana zmiennej $X = Y + a$ pozwalała stwierdzić nierozkładalność tego wielomianu.

W poniższym przykładzie zobaczymy jeszcze jedną modyfikację rozumowania zastosowanego w trakcie dowodu kryterium Eisensteina. Należy ją dobrze przemyśleć, a następnie udowodnić sformułowane w ćwiczeniu C3.41, uogólnione kryterium Eisensteina.

P r z y k ł a d 2. Udowodnimy, że wielomian $X^{11} + 11X^{10} + 7$ jest nierozkładalny w $\mathbb{Q}[X]$. Załóżmy w tym celu, że mamy rozkład w $\mathbb{Z}[X]$

$$7 + 11X^{10} + X^{11} = (b_0 + b_1X + \ldots + X^k)(c_0 + c_1X + \ldots + X^l) \tag{3.23}$$

na dwa czynniki unormowane. Bez straty ogólności możemy założyć, że $b_0 = \pm 7$ i $c_0 = \pm 1$. Wówczas $0 = b_0c_1 + b_1c_0$. Stąd, dzięki Zasadzie Podstawowej, $7|b_1$. Dalej, równość $0 = b_0c_2 + b_1c_1 + b_2c_0$, tak samo jak przed chwilą, daje $7|b_2$. I tak dalej, aż do: $7|b_9$. (Zauważmy nawiasem, że, zgodnie z umową z paragrafu 3.1, wielomian m a wszystkie współczynniki, choć od pewnego miejsca są one równe zero.) Ponieważ $b_k = 1$, więc $k > 9$. Czyli $k = 10$, a $l = 1$. Zatem, drugi czynnik w równości (3.23) ma postać $X \pm 1$. To by jednakże oznaczało, że badany wielomian ma pierwiastek 1 lub -1. Sprzeczność, bo nie ma! $\Diamond$

Ćwiczenie 3.41 Udowodnić ***uogólnione kryterium Eisensteina***: *Niech*

$$a(X) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + X^n \in \mathbb{Z}[X].$$

Załóżmy, że istnieje liczba pierwsza p i taki indeks $k \in \{0, 1, \ldots, n-1\}$, że spełnione są warunki: $p|a_s$ dla $0 \leqslant s \leqslant k$, ale $p^2 \nmid a_0$. Wówczas, wielomian $a(X)$ m a nierozkładalny dzielnik stopnia co najmniej $k+1$.

Ćwiczenie 3.42 Dana jest liczba pierwsza p. Uzasadnić, że istnieje wielomian $F(X) \in \mathbb{Z}[X]$, którego wartość dla dowolnego argumentu całkowitego $x \neq \pm 1$ wynosi

$$\frac{x^{p^3} - 1}{x^{p^2} - 1}.$$

Udowodnić, że ten wielomian jest nierozkładalny w $\mathbb{Q}[X]$. Uogólnić.

W rozwiązaniu kolejnego zadania korzystamy z tak zwanego Małego Twierdzenia Fermat'a, zobacz 5.2.3. Nie będziemy się też wzdragać przed używaniem notacji kongruencyjnej.

ZADANIE 3.19 Udowodnić, że jeżeli $5 \nmid a$, to wielomian $X^5 - X + a \in \mathbb{Z}[X]$ jest nierozkładalny w pierścieniu $\mathbb{Q}[X]$ wielomianów o współczynnikach wymiernych.

R o z w i ą z a n i e. Na mocy twierdzenia Gaussa T3.15, wystarczy udowodnić, że wielomian $h_a(X) = X^5 - X + a$ nie da się nietrywialnie rozłożyć na iloczyn w pierścieniu $\mathbb{Z}[X]$. Każdy ewentualny rozkład jest jednej z dwóch postaci:

$$X^5 - X + a = (X - b)(X^4 + cX^3 + dX^2 + eX + f), \tag{3.24}$$

$$X^5 - X + a = (X^2 + bX + c)(X^3 + dX^2 + eX + f). \tag{3.25}$$

Czytelnik powinien przekonać się samodzielnie, dlaczego można (bez straty ogólności) uznać, że oba czynniki w rozkładzie na iloczyn w $\mathbb{Z}[X]$ wielomianu unormowanego w $\mathbb{Z}[X]$, są wielomianami unormowanymi. Pokażemy najpierw, że przypadek (3.24) zajść nie może. Gdyby zachodził, to byłoby $h_a(b) = 0$. Ale $b^5 - b \equiv 0 \,(\mathrm{mod}\, 5)$ (zobacz (5.12)), więc

$$0 = h_a(b) = b^5 - b + a \equiv a \,(\mathrm{mod}\, 5),$$

co jest sprzeczne z założeniem $5 \nmid a$. Załóżmy więc, że zachodzi równość (3.25), czyli:

$$X^5 - X + a = X^5 + (b + d)X^4 + (c + bd + e)X^3 + (f + be + cd)X^2 + (ce + bf)X + cf.$$

Porównujemy współczynniki:

$$b+d=0, \qquad c+bd+e=0, \qquad f+be+cd=0, \tag{3.26}$$

$$ce+bf=-1, \qquad cf=a. \tag{3.27}$$

Z równości (3.26) wyrażamy d, e i f za pomocą b i c: $d=-b$ $e=b^2-c$ i $f=2bc-b^3$. Wobec tego, równości (3.27) dają:

$$3b^2c-c^2=b^4-1, \tag{3.28}$$

$$bc(2c-b^2)=a. \tag{3.29}$$

Założenie, że $a \not\equiv 0 \,(\mathrm{mod}\, 5)$ i równość (3.29) dowodzą, że $b \not\equiv 0 \,(\mathrm{mod}\, 5)$ i $c \not\equiv 0 \,(\mathrm{mod}\, 5)$. Zatem b i c są odwracalne modulo 5. Przeto, prawa strona równości (3.28) jest podzielna przez 5, patrz MTF, więc $c(3b^2-c) \equiv 0 \,(\mathrm{mod}\, 5)$. Stąd, wobec odwracalności $c \,(\mathrm{mod}\, 5)$, $3b^2 \equiv c \,(\mathrm{mod}\, 5)$. Mnożąc przez 2, dostajemy $b^2 \equiv 2c \,(\mathrm{mod}\, 5)$, co, dzięki (3.29) daje $a=bc(2c-b^2) \equiv 0 \,(\mathrm{mod}\, 5)$. Sprzeczność. $\Diamond$

3.4.3 Zasadnicze Twierdzenie Algebry

Liczby zespolone już znamy, zobacz paragraf 1.5. Zbiór tych liczb jest ciałem względem dodawania (1.9) i mnożenia (1.10). Ciało liczb zespolonych jest szczególnie sympatyczne jeśli chodzi o istnienie w nim pierwiastków równań wielomianowych.

Definicja 3.14 Jeżeli każdy wielomian $f(X) \in \mathbb{K}[X]$ stopnia dodatniego ma w ciele $\mathbb{K}$ pierwiastek, to ciało $\mathbb{K}$ nazywa się **ciałem algebraicznie domkniętym**.

Ważnym twierdzeniem, po raz pierwszy w historii matematyki udowodnionym (bez luk) przez Gaussa w końcu XVIII wieku (zobacz motto do tego rozdziału), jest:

TWIERDZENIE 3.18 (***Zasadnicze Twierdzenie Algebry***) *Ciało $\mathbb{C}$ liczb zespolonych jest algebraicznie domknięte. Równoważnie, jeżeli $f(X)=a_0+a_1X+\ldots+a_nX^n \in \mathbb{C}[X]$ jest wielomianem stopnia n, to zachodzi równość*

$$f(X)=a_n\,(X-\alpha_1)(X-\alpha_2)\cdot\ldots\cdot(X-\alpha_n), \tag{3.30}$$

dla pewnych, niekoniecznie różnych, liczb zespolonych α_i.

DOWÓD. Równoważność dwóch sformułowań wynika z WT3.2. Istnieje wiele dowodów tego twierdzenia. Opowiemy (bez szczegółów) o jednym z dowodów topologicznych. Przypomnijmy, że liczby zespolone utożsamiamy z punktami płaszczyzny. *Liczba zespolona* oznacza więc to samo co *punkt* (płaszczyzny).

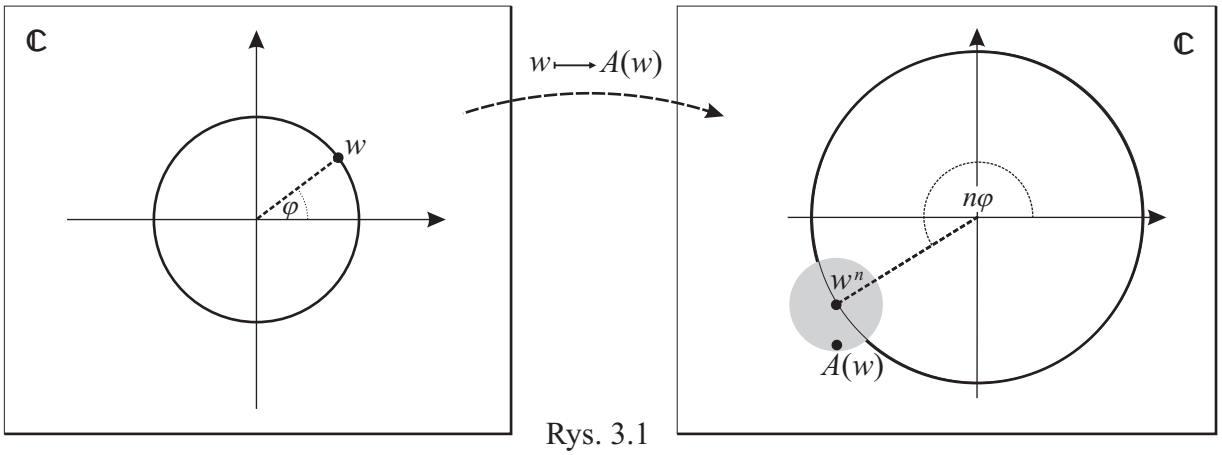
Niech $f(X)=a_0+a_1X+\ldots+X^n$ będzie wielomianem unormowanym stopnia n o współczynnikach zespolonych. Rozważmy okrąg $\mathcal{C}(r)=\{z \in \mathbb{C} : |z|=r\}$ o środku w punkcie 0 i promieniu $r>0$. Jeżeli zmienna liczba zespolona w przebiega okrąg $\mathcal{C}(r)$, to jej obraz (wartość wielomianu) $f(w)$ przebiega pewną krzywą $\mathcal{W}(r)$. Przyjrzyjmy się bliżej krzywym $\mathcal{W}(r)$. W tym celu zapiszmy wartość $f(w)/w^n$ w postaci

$$\frac{f(w)}{w^n}=1+\frac{a_{n-1}}{w}+\ldots+\frac{a_1}{w^{n-1}}+\frac{a_0}{w^n}=1+k(w).$$

Możemy dzielić przez w, bo $|w| = r > 0$. Wyznaczona przez tę równość liczba zespolona $k(w)$ jest, przy dostatecznie dużych r, bardzo m a ł a. Konkretnie, jeżeli przez M oznaczymy $\max(|a_0|, |a_1|, \ldots, |a_{n-1}|)$, to, korzystając z nierówności trójkąta (zobacz C1.23), faktu, że moduł ilorazu równy jest ilorazowi modułów (zobacz C1.25) i tożsamości fundamentalnej (1.8), znajdujemy:

$$|k(w)| = \left|\frac{a_{n-1}}{w} + \ldots + \frac{a_1}{w^{n-1}} + \frac{a_0}{w^n}\right| \leqslant \left|\frac{a_{n-1}}{w}\right| + \ldots + \left|\frac{a_1}{w^{n-1}}\right| + \left|\frac{a_0}{w^n}\right| \leqslant$$
$$\leqslant \frac{M}{r} + \ldots + \frac{M}{r^{n-1}} + \frac{M}{r^n} = \frac{M}{r} \cdot \frac{1 - \frac{1}{r^n}}{1 - \frac{1}{r}} < \frac{M}{r-1}.$$

Niech $R = 5M + 1$. Widzimy, że dla każdego $r \geqslant R$ zachodzi nierówność $|k(w)| < 1/5$. Jeżeli więc $r \geqslant R$, to wartość $f(w) = w^n + k(w)w^n$ jest równa w^n z błędem względnym mniejszym niż $0,2$. Czyli, punkt $f(w)$ znajduje się "w pobliżu" punktu w^n, zobacz rys. 3.1.



Rys. 3.1

Zobaczmy jeszcze gdzie znajduje się punkt w^n. Jeżeli $w \in \mathcal{C}(r)$ ma argument φ, to $w = r(\cos\varphi + i\sin\varphi)$, więc, na mocy wzoru de Moivre'a (1.14), $w^n = r^n(\cos n\varphi + i\sin n\varphi)$. Widzimy stąd, że jeżeli punkt w porusza się ze stałą prędkością kątową po okręgu $\mathcal{C}(r)$, to punkt w^n porusza po (dużo) większym okręgu $\mathcal{C}(r^n)$ z n razy większą prędkością kątową. Gdy więc argument φ liczby w zmienia się od $\varphi = 0$ do $\varphi = 2\pi$, to punkt w^n n-krotnie okrąża 0. To samo więc robi bliski mu punkt $f(w)$.

Obserwacja ruchu punktu $f(w)$, gdy punkt w porusza się ze stałą prędkością kątową po okręgu $\mathcal{C}(r)$, jest podobna do ptolemejskiej obserwacji ruchu planety. Widzimy jednostajny ruch po okręgu $\mathcal{C}(r^n)$ opisywany przez składnik w^n i skomplikowany układ "epicykli" opisywany przez składnik $k(w)w^n$. Jakby to nie było, jedno jest pewne: jeżeli $r \geqslant R$, to krzywa $\mathcal{W}(r)$ n-krotnie okrąża punkt 0 startując od punktu $f(r)$ i kończąc w tym samym punkcie.

Załóżmy teraz, n i e w p r o s t, że wielomian f n i e m a pierwiastków. Wtedy $a_0 \neq 0$ (gdy $a_0 = 0$, to $w = 0$ jest pierwiastkiem wielomianu f). Ponadto, ż a d n a z k r z y w y c h $\mathcal{W}(r)$ n i e przechodzi przez punkt 0. Jest więc zawarta w "płaszczyźnie z dziurką" $\mathbb{C} \setminus \{0\}$. Jeżeli teraz będziemy stopniowo (w sposób ciągły) zmniejszali promień r, zaczynając od $r = R$, to krzywa $\mathcal{W}(r)$ będzie się stopniowo (w sposób ciągły) deformowała cały czas pozostając w $\mathbb{C} \setminus \{0\}$. I w "końcu", przy bardzo małym r będzie leżała w pewnym małym kole wokół punktu $f(0) = a_0$. Czytelnik z pewnością widzi w tym p o r a ż a j ą c ą s p r z e c z n o ś ć. Sprzeczność ta kończy dowód. □

3.4.4 Rozkłady w pierścieniu $\mathbb{C}[X]$ i $\mathbb{R}[X]$

Będziemy teraz rozkładać na czynniki nierozkładalne wielomiany w pierścieniach $\mathbb{C}[X]$ i $\mathbb{R}[X]$.

Ćwiczenie 3.43 Ciało $\mathbb{K}$ jest algebraicznie domknięte wtedy i tylko wtedy, gdy jedynymi wielomianami nierozkładalnymi w pierścieniu $\mathbb{K}[X]$ są wielomiany stopnia pierwszego.

Ponieważ, dzięki Gaussowi, wiemy na pewno, że ciało $\mathbb{C}$ liczb zespolonych jest algebraicznie domknięte, więc widzimy, że j e d y n y m i wielomianami nierozkładalnymi w pierścieniu $\mathbb{C}[X]$ są wielomiany stopnia pierwszego. Natomiast w pierścieniu $\mathbb{R}[X]$ wielomianów o współczynnikach rzeczywistych, poza wielomianami stopnia pierwszego, tylko jeszcze niektóre trójmiany kwadratowe są nierozkładalne (por. C3.33). Przed dowodem stosownego twierdzenia, udowodnimy lemat:

LEMAT 3.2 *Jeżeli liczba zespolona w jest pierwiastkiem wielomianu $f(X) \in \mathbb{R}[X]$, to liczba sprzężona $\overline{w}$ również jest pierwiastkiem tego wielomianu.*

D O W Ó D. Niech $f(X) = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{R}[X]$ (i $f(w) = 0$). Wówczas

$$0 = \overline{0} = \overline{a_0 + a_1 \cdot w + \ldots + a_n \cdot w^n} = \overline{a_0} + \overline{a_1} \cdot \overline{w} + \ldots + \overline{a_n} \cdot \overline{w}^n =$$
$$= a_0 + a_1 \cdot \overline{w} + \ldots + a_n \cdot \overline{w}^n = f(\overline{w}).$$

Napisane równości wynikają z faktu, że sprzężenie sumy równe jest sumie sprzężeń, zobacz C1.22(1), sprzężenie iloczynu równe jest iloczynowi sprzężeń, zobacz C1.22(2), i z faktu, że sprzężenie liczby rzeczywistej równe jest tej liczbie. □

Możemy teraz udowodnić zapowiedziane:

TWIERDZENIE 3.19 *W pierścieniu $\mathbb{R}[X]$, nierozkładalnymi są tylko wielomiany stopnia pierwszego i trójmiany kwadratowe $aX^2 + bX + c$, dla których $\Delta < 0$.*

D O W Ó D. Załóżmy, że $p(X) \in \mathbb{R}[X]$ jest nierozkładalny. Wtedy $\deg p(X) \geqslant 1$, więc, na mocy T3.18, istnieje liczba $\alpha \in \mathbb{C}$ będąca pierwiastkiem wielomianu $p(X)$. Dzięki twierdzeniu Bézout'*a* T3.2, możemy napisać

$$p(X) = (X - \alpha)s(X), \tag{3.31}$$

gdzie $s(X) \in \mathbb{C}[X]$. Zachodzi jedna z możliwości: albo $\alpha \in \mathbb{R}$, albo $\alpha \notin \mathbb{R}$.

Jeżeli $\alpha \in \mathbb{R}$, to, jak wiemy (zobacz 3.2.1 U1), wielomian $s(X)$ ma współczynniki rzeczywiste, a, wobec nierozkładalności wielomianu $p(X)$, wielomian $s(X)$ jest stopnia zero. W takiej więc sytuacji, wielomian $p(X)$ jest wielomianem stopnia 1.

Jeżeli zaś $\alpha \notin \mathbb{R}$, to $\alpha \neq \overline{\alpha}$ oraz

$$0 = p(\overline{\alpha}) = (\overline{\alpha} - \alpha)s(\overline{\alpha}),$$

gdzie pierwsza równość wynika z L3.2, a druga z (3.31). Stąd $s(\overline{\alpha}) = 0$, więc, znów na mocy twierdzenia Bézout'*a*, $s(X) = (X - \overline{\alpha})t(X)$. Zatem

$$p(X) = (X - \alpha)(X - \overline{\alpha})t(X) = (X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha})t(X). \tag{3.32}$$

Wielomian $X^2-(\alpha+\overline{\alpha})X+\alpha\overline{\alpha}$ jest wielomianem o współczynnikach rzeczywistych (zobacz C1.21 i C1.22), zatem i wielomian $t(X)$ jest wielomianem o współczynnikach rzeczywistych. Nierozkładalność wielomianu $p(X)$ i równość (3.32) dowodzą, że $t(X)$ jest wielomianem stopnia zero, $t(X)=c$, a $p(X)$ jest trójmianem kwadratowym $cX^2-c(\alpha+\overline{\alpha})X+c\alpha\overline{\alpha}$ o współczynnikach rzeczywistych i wyróżniku $\Delta=c^2(\alpha+\overline{\alpha})^2-4c^2\alpha\overline{\alpha}=c^2(\alpha-\overline{\alpha})^2=4c^2i^2(\operatorname{Im}\alpha)^2$, jak widać, ujemnym (zobacz jeszcze raz C1.21). □

U w a g a. W ustępie 3.4.2 widzieliśmy, że w pierścieniu $\mathbb{Q}[X]$ istnieją wielomiany nierozkładalne dowolnych stopni $\geqslant 1$. Na przykład X^n+7 jest nierozkładalny w $\mathbb{Q}[X]$ przy dowolnym $n\in\mathbb{N}$, zobacz C3.39.

Dzięki zdobytej wiedzy na temat wielomianów nierozkładalnych w $\mathbb{C}[X]$ i $\mathbb{R}[X]$ możemy uszczegółowić twierdzenie T3.14 w tych przypadkach. Sformułujemy to w postaci wniosków:

WNIOSEK 1. *Jeżeli $f(X)\in\mathbb{C}[X]$ jest wielomianem stopnia n, to istnieją takie, jednoznacznie wyznaczone, liczby zespolone $\lambda_1, \lambda_2, \ldots, \lambda_t$ i takie, jednoznacznie wyznaczone, liczby naturalne $e_1, e_2, \ldots, e_t$, że zachodzi równość*

$$f(X)=C(X-\lambda_1)^{e_1}(X-\lambda_2)^{e_2}\cdot\ldots\cdot(X-\lambda_t)^{e_t}, \tag{3.33}$$

gdzie C jest współczynnikiem przy X^n w wielomianie $f(X)$, oraz $e_1+\cdots+e_t=n$. □

Zauważmy bijące w oczy podobieństwo równości (3.33) i 2.4.1 (RK).

WNIOSEK 2. *Jeżeli $f(X)\in\mathbb{R}[X]$ jest wielomianem stopnia n, to istnieją takie, jednoznacznie wyznaczone, liczby rzeczywiste $a_1, a_2, \ldots, a_r$ oraz liczby zespolone nierzeczywiste $b_1+ic_1, b_2+ic_2, \ldots, b_s+ic_s$ i takie, jednoznacznie wyznaczone, liczby naturalne $e_1, e_2, \ldots, e_r$ oraz $d_1, d_2, \ldots, d_s$, że zachodzi równość*

$$f(X)=C(X-a_1)^{e_1}\cdot\ldots\cdot(X-a_r)^{e_r}\cdot((X-b_1)^2+c_1^2)^{d_1}\cdot\ldots\cdot((X-b_s)^2+c_s^2)^{d_s}, \tag{3.34}$$

gdzie C jest współczynnikiem przy X^n w $f(X)$, oraz $e_1+\cdots+e_r+2d_1+\cdots+2d_s=n$. □

Dzięki istnieniu rozkładu (3.34) możemy rozwiązać interesujące:

Ćwiczenie 3.44 Udowodnić, że jeżeli wielomian $f(X)\in\mathbb{R}[X]$ przyjmuje dla każdego argumentu rzeczywistego wartość n i e u j e m n ą, to istnieją wielomiany $a(X), b(X)\in\mathbb{R}[X]$, dla których zachodzi równość $f(X)=a(X)^2+b(X)^2$. *Wskazówka.* Wykorzystać, prawdziwą w każdym pierścieniu(!), tożsamość $(\alpha^2+\beta^2)(\gamma^2+\delta^2)=(\alpha\gamma-\beta\delta)^2+(\alpha\delta+\beta\gamma)^2$, por. (8.1).

3.4.5 Pierwiastki wielomianu X^n-1

Zobaczymy teraz jak wyglądają pierwiastki wielomianów X^n-1, przy $n\in\mathbb{N}$. Sytuacja jest, oczywiście, różna w zależności od wyboru ciała, w którym szukamy tych pierwiastków.

Ćwiczenie 3.45 Udowodnić, że wielomian X^n-1 nie ma różnych od ±1 pierwiastków rzeczywistych. Przy czym 1 jest pierwiastkiem każdego z tych wielomianów, $n\geqslant 1$, a -1 jest dodatkowo pierwiastkiem X^n-1 dla n parzystych (i większych od 0).

Przejdźmy do liczb zespolonych i przywołajmy ćwiczenie C1.36. Ustalmy n. Niech

$$\omega = \omega_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \tag{3.35}$$

będzie pierwiastkiem n-tego stopnia z jedynki o najmniejszym d o d a t n i m argumencie. Jest oczywiste, że liczby $\omega,\ \omega^2,\ \ldots,\ \omega^{n-1}$ i $\omega^0 = 1$ są pierwiastkami wielomianu $X^n - 1$. Liczby te są są parami różne (tworzą wierzchołki n-kąta foremnego wpisanego w okrąg jednostkowy, zobacz przypadek $n = 9$ na rysunku 1.5b), więc równość (3.33) ma tu postać:

$$X^n - 1 = (X-1)(X-\omega)(X-\omega^2)\cdot\ \ldots\ \cdot(X-\omega^{n-1}). \tag{3.36}$$

Rozkład (3.36) wielomianu $X^n - 1$ na **czynniki liniowe** (to znaczy stopnia 1) w pierścieniu $\mathbb{C}[X]$ pozwala łatwo napisać rozkład tego wielomianu na **czynniki kwadratowe** (to znaczy stopnia 2) w pierścieniu $\mathbb{R}[X]$. Zauważmy w tym celu, że dla każdego k zachodzi równość

$$\omega^{n-k} = \overline{\omega^k}. \tag{3.37}$$

Grupując i wymnażając w iloczynie (3.36) czynniki $X - \omega^k$ i $X - \omega^{n-k}$, dostaniemy

$$(X-\omega^k)(X-\omega^{n-k}) = (X-\omega^k)(X-\overline{\omega^k}) = X^2 - 2\mathrm{Re}\,(\omega^k)X + 1,$$

bo, patrz (1.12), $\omega^k\cdot\overline{\omega^k} = 1$. Ale $\mathrm{Re}\,(\omega^k) = \cos\frac{2k\pi}{n}$, więc, w zależności od parzystości wykładnika n, dostajemy rozkłady wielomianu $X^n - 1$ na czynniki w pierścieniu $\mathbb{R}[X]$:

$$X^{2m+1} - 1 = (X-1)\cdot\prod_{k=1}^{m}\left(X^2 - \left(2\cos\tfrac{2k\pi}{2m+1}\right)X + 1\right), \tag{3.38}$$

$$X^{2m} - 1 = (X-1)(X+1)\prod_{k=1}^{m-1}\left(X^2 - \left(2\cos\tfrac{2k\pi}{2m}\right)X + 1\right). \tag{3.39}$$

Ćwiczenie 3.46 Udowodnić, że dla dowolnych liczb (zespolonych, rzeczywistych, wymiernych, całkowitych) a, b i dowolnego wykładnika $n \geqslant 1$ zachodzą równości

$$a^n - b^n = (a-b)\cdot(a-\omega b)\cdot\ \ldots\ \cdot(a-\omega^{n-1}b), \tag{3.40}$$

$$a^n + b^n = (a-\eta b)\cdot(a-\eta^3 b)\cdot\ \ldots\ \cdot(a-\eta^{2n-1}b), \tag{3.41}$$

gdzie $\omega = \omega_n$, $\eta = \omega_{2n}$, patrz (3.35).

TWIERDZENIE 3.20 (***Twierdzenie o strażakach***) *Niech $n \geqslant 2$. Suma wszystkich pierwiastków n-tego stopnia z jedynki jest równa zero.*

D O W Ó D. Po rozwiązaniu ćwiczenia C1.36, rzecz jest jasna:

$$1 + \omega + \omega^2 + \ \ldots\ + \omega^{n-1} = \frac{1-\omega^n}{1-\omega} = \frac{1-1}{1-\omega} = 0,$$

zobacz tożsamość nieśmiertelną (1.8). □

U w a g a. Zauważmy, że, wobec równości (3.36), twierdzenie o strażakach jest równoważne z faktem, że $(n-1)$-szy współczynnik wielomianu $X^n - 1$ jest równy 0. Podobnie widzimy, że zerowy współczynnik jest równy $(-1)^n \cdot 1 \cdot \omega \cdot \omega^2 \cdot \ldots \cdot \omega^{n-1} = -1$, skąd:

$$1 \cdot \omega \cdot \omega^2 \cdot \ldots \cdot \omega^{n-1} = (-1)^{n-1}. \tag{3.42}$$

Zobacz też wzory Viète'a w ustępie 3.4.8.

ZADANIE 3.20 Wyznaczyć wszystkie takie układy (a, b, c) liczb naturalnych, że wielomian $f(X) := X^a + X^b + X^c$ dzieli się w pierścieniu $\mathbb{Q}[X]$ przez wielomian $X^2 + X + 1$.

R o z w i ą z a n i e. Załóżmy, że liczby a, b, c dają r ó ż n e reszty z dzielenia przez 3. Niech na przykład $a = 3k + 2$, $b = 3l + 1$, $c = 3m$. Wówczas

$$f(X) = X^2[(X^3)^k - 1] + X[(X^3)^l - 1] + [(X^3)^m - 1] + X^2 + X + 1.$$

Stąd, stosując tożsamość nieśmiertelną (1.8) do każdego z wyrażeń w nawiasach kwadratowych, widzimy, że $f(X) = (X^3 - 1)q(X) + X^2 + X + 1$. Ale, znów dzięki (1.8), wiemy, że wielomian $X^3 - 1$ dzieli się przez $X^2 + X + 1$. Zatem $X^2 + X + 1 | X^a + X^b + X^c$ w tym przypadku.

Odwrotnie, załóżmy, że zachodzi równość

$$X^a + X^b + X^c = q(X) \cdot (X^2 + X + 1). \tag{3.43}$$

Zauważmy, że zarówno $\omega = \omega_3$ jak i $\omega^2 = \omega_3^2$ s ą pierwiastkami wielomianu $X^2 + X + 1$. Wobec tego, jeżeli zachodzi równość (3.43), to zachodzą równości $f(\omega) = f(\omega^2) = 0$. Ale

$$f(\omega) = \omega^a + \omega^b + \omega^c = \omega^{r_1} + \omega^{r_2} + \omega^{r_3},$$

gdzie r_1, r_2, r_3 oznaczają reszty z dzielenia a, b, c przez 3. Łatwo sprawdzić, że ta suma jest równa 0 wtedy i tylko wtedy, gdy te reszty są różne. Wtedy też, i tylko wtedy, $f(\omega^2) = 0$. Wobec tego $X^2 + X + 1 | X^a + X^b + X^c$ wtedy i tylko wtedy, gdy wykładniki a, b, c dają różne reszty z dzielenia przez 3. $\Diamond$

Ćwiczenie 3.47 Wyznaczyć wszystkie takie liczby naturalne n, dla których liczba naturalna $1\underbrace{00\ldots0}_{n}1\underbrace{00\ldots0}_{n}1$ jest podzielna przez 37.

Ćwiczenie 3.48 Załóżmy, że liczby $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}_{\geqslant 0}$ dają różne reszty z dzielenia przez 5. Udowodnić, że wielomian $\Phi_5(X) := 1 + X + X^2 + X^3 + X^4$ jest w pierścieniu $\mathbb{Z}[X]$ dzielnikiem wielomianu $X^{a_0} + X^{a_1} + X^{a_2} + X^{a_3} + X^{a_4}$.

3.4.6 Wielomiany cyklotomiczne

Wielomiany $1 + X + X^2$ oraz $1 + X + X^2 + X^3 + X^4$ są przykładami tak zwanych wielomianów cyklotomicznych.

Definicja 3.15 Niech n będzie dowolną liczbą naturalną i niech $\omega = \omega_n$ będzie zadana przez (3.35). Wielomian

$$\Phi_n(X) = \prod_{k \perp n} (X - \omega^k), \tag{3.44}$$

gdzie iloczyn rozciąga się na wszystkie takie k, że $1 \leqslant k \leqslant n$ i $\mathrm{NWD}\,(k,\, n) = 1$, nazywa się n-tym **wielomianem cyklotomicznym**.

P r z y k ł a d. Jasne, że $\Phi_1(X) = X - 1$. Policzmy jeszcze (korzystając z (3.37):

$$\begin{aligned}
&\Phi_2(X) = X - \omega_2 = X + 1,\\
&\Phi_3(X) = (X - \omega_3)(X - \omega_3^2) = X^2 + X + 1,\\
&\Phi_4(X) = (X - \omega_4)(X - \omega_4^3) = (X - i)(X + i) = X^2 + 1,\\
&\Phi_5(X) = (X - \omega_5)(X - \omega_5^2)(X - \omega_5^3)(X - \omega_5^4) = X^4 + X^3 + X^2 + X + 1,\\
&\Phi_6(X) = (X - \omega_6)(X - \omega_6^5) = X^2 - X + 1. \ \Diamond
\end{aligned}$$

Ćwiczenie 3.49 Udowodnić, że wszystkie wielomiany cyklotomiczne mają współczynniki rzeczywiste. Porównaj też C4.22.

Ćwiczenie 3.50 Uzasadnić, że jeżeli p jest liczbą pierwszą, to

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \ \ldots\ + X + 1. \tag{3.45}$$

Ćwiczenie 3.51 Udowodnić, że dla dowolnej liczby naturalnej n zachodzi równość:

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{3.46}$$

W Z3.18 wykazaliśmy, że wielomiany cyklotomiczne $\Phi_p(X)$ (dla $p \in \mathbb{P}$) są nierozkładalne w pierścieniu $\mathbb{Q}[X]$. Poniższe twierdzenie jest w a ż n e. Wynika z niego, między innymi, że rozkład (3.46) jest rozkładem na czynniki n i e r o z k ł a d a l n e. Dowód będziemy w stanie podać dopiero w rozdziale 6.

Twierdzenie 3.21 *Niech $n \in \mathbb{N}$. Wielomian cyklotomiczny $\Phi_n(X)$ ma współczynniki całkowite i jest nierozkładalny w pierścieniu $\mathbb{Q}[X]$.* □

3.4.7 Rozwiązywanie równań stopnia 3 i 4

Powiemy tu parę słów na temat wyznaczania pierwiastków wielomianów stopnia 3, czyli rozwiązywania równań postaci

$$u^3 + au^2 + bu + c = 0, \tag{3.47}$$

gdzie a, b, c są liczbami (zespolonymi).

Chcąc wyznaczyć pierwiastki równania (3.47), najpierw redukujemy takie równanie do postaci bez wyrazu kwadratowego. Uzyskuje się to przez podstawienie $u = x + k$ ze stosownie dobranym k. Mamy

$$(x+k)^3 + a(x+k)^2 + b(x+k) + c = x^3 + (3k+a)x^2 + \cdots = 0,$$

gdzie kropkami oznaczamy wyrazy niższego stopnia. Widzimy stąd, że przyjmując $k = -a/3$ dostaniemy równanie bez wyrazu kwadratowego (tzw. **postać zredukowaną**):

$$x^3 + Ax + B = 0, \tag{3.48}$$

gdzie $A = -\frac{1}{3}a^2 + b$, $B = \frac{2}{27}a^3 - \frac{1}{3}ab + c$. Rozwiązanie równania (3.48) w przypadku, gdy $B = 0$, jest oczywiste: jednym pierwiastkiem jest wówczas $\alpha_1 = 0$, pozostałe dwa są pierwiastkami równania $x^2 + A = 0$. Również w przypadku, gdy $A = 0$ nie mamy żadnych kłopotów ze znalezieniem pierwiastków: jeżeli α_1 jest taką liczbą (zespoloną), że $\alpha_1^3 = -B$, to $\alpha_2 = \omega\alpha_1$ i $\alpha_3 = \omega^2\alpha_1$ są pozostałymi pierwiastkami równania $x^3 + B = 0$. Tu (i dalej w tym ustępie) ω oznacza ω_3, zobacz (3.35). W dalszym ciągu zakładamy więc, że $A \neq 0$ i $B \neq 0$.

Niccolò Fontana Tartaglia był prawdopodobnie pierwszym, który zauważył, że pierwiastki równania (3.48) można wyrazić za pomocą pierwiastków równania **trzykwadratowego**:

$$z^6 + Bz^3 - \frac{A^3}{27} = 0 \tag{3.49}$$

zwanego **równaniem rozwiązującym**. Wyróżnik trójmianu kwadratowego $X^2 + BX - A^3/27$, czyli liczbę

$$\boxed{\boxed{\Delta = 4\left(\frac{B^2}{4} + \frac{A^3}{27}\right)}} \tag{3.50}$$

nazywamy **wyróżnikiem** równania sześciennego (3.48).

TWIERDZENIE 3.22 *Jeżeli $\lambda \neq 0$ jest pierwiastkiem równania* (3.49)*, to $\mu = -A/3\lambda$ jest również pierwiastkiem równania* (3.49)*. Ponadto liczby*

$$\alpha_1 := \lambda + \mu, \quad \alpha_2 := \omega\lambda + \omega^2\mu, \quad \alpha_3 := \omega^2\lambda + \omega\mu \tag{3.51}$$

są pierwiastkami równania (3.48)*.*

D O W Ó D. Niech $f(X) = X^6 + BX^3 - A^3/27$. Załóżmy, że $f(\lambda) = 0$. Wtedy, jak łatwo widzieć, $f(-A/3\lambda) = -A^3/(27\lambda^6)f(\lambda) = 0$. Więc $f(\mu) = 0$. Sprawdzenie, że liczby (3.51) są pierwiastkami równania (3.48), jest prostym rachunkiem. Na przykład:

$$\begin{aligned}
\alpha_2^3 + A\alpha_2 + B &= (\omega\lambda + \omega^2\mu)^3 + A(\omega\lambda + \omega^2\mu) + B \\
&= \omega^3\lambda^3 + \omega^6\mu^3 + 3\omega\lambda\omega^2\mu(\omega\lambda + \omega^2\mu) + A(\omega\lambda + \omega^2\mu) + B \\
&= \lambda^3 + \mu^3 + (3\lambda\mu + A)(\omega\lambda + \omega^2\mu) + B = \lambda^3 + \mu^3 + B \\
&= \lambda^{-3}\left(\lambda^6 + B\lambda^3 - \frac{A^3}{27}\right) = \lambda^{-3}f(\lambda) = 0.
\end{aligned}$$

Podobnie sprawdzamy, że $\alpha_1^3 + A\alpha_1 + B = \alpha_3^3 + A\alpha_3 + B = 0$. □

U w a g a 1. Wyjaśnimy jeszcze jak Tartaglia mógł wpaść na pomysł rozważania równania rozwiązującego. Szukał on mianowicie rozwiązania x równania (3.48) w postaci sumy dwóch nowych n i e w i a d o m y c h u, v. Podstawiając $x = u + v$ otrzymujemy:

$$(u+v)^3 + A(u+v) + B = u^3 + v^3 + (3uv + A)(u+v) + B = 0.$$

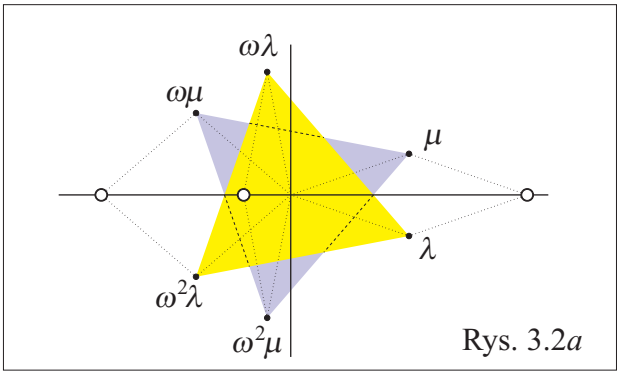
Narzucając dodatkowy warunek $3uv + A = 0$ widzimy, że liczby u^3 i v^3 spełniają układ równań typu Viète'*a*, zobacz (3.14):

$$\begin{cases} u^3 + v^3 = -B, \\ u^3 v^3 = -\dfrac{A^3}{27}. \end{cases} \tag{3.52}$$

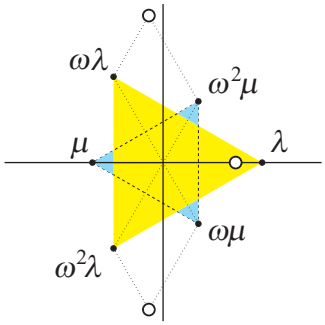
To, zgodnie z twierdzeniem T3.9, oznacza, że liczby u^3 i v^3 są pierwiastkami równania kwadratowego $u^2 + Bu - A^3/27 = 0$ o wyróżniku Δ. Jasne jest wobec tego, że dowolny pierwiastek 3-go stopnia z u czy z v jest pierwiastkiem równania rozwiązującego (3.49). I odwrotnie, 3-cia potęga dowolnego pierwiastka równania (3.49) jest jedną z liczb u^3, v^3.

Ćwiczenie 3.52 Udowodnić, że pewne dwie z liczb (3.51) są równe wtedy i tylko wtedy, gdy $\Delta = 0$.

Jeżeli $\Delta \neq 0$, to równanie rozwiązujące ma sześć pierwiastków, które tworzą wierzchołki dwóch trójkątów: $\{\lambda, \omega\lambda, \omega^2\lambda\}$ oraz $\{\mu, \omega\mu, \omega^2\mu\}$. Nazwijmy je **trójkątami Tartaglia'*i***. Na rysunku 3.2*a* pokazujemy trójkąty Tartaglia'*i* w przypadku, gdy współczynniki A, B są rzeczywiste i $\Delta < 0$. Na rysunku 3.2*b* pokazujemy przypadek rzeczywistych A, B i dodatniego wyróżnika Δ. Kółkami zaznaczyliśmy pierwiastki odpowiedniego równania (3.48).



Rys. 3.2*a*



Rys. 3.2*b*

Ćwiczenie 3.53 Znaleźć rozwiązania (pierwiastki) równania $x^3 - \frac{3}{2}x^2 - 3x + \frac{5}{4} = 0$. Narysować odpowiednie trójkąty Tartaglia'*i*.

Ćwiczenie 3.54 Udowodnić tożsamość

$$\boxed{x^3 + y^3 + z^3 - 3xyz = (x+y+z)(x+\omega y+\omega^2 z)(x+\omega^2 y+\omega z).}$$

Podstawiając tu $x = X$, $y = -\lambda$ oraz $z = -\mu$, wywnioskować, że pierwiastkami wielomianu $X^3 - 3\lambda\mu X - \lambda^3 - \mu^3$ są liczby $\alpha_1 = \lambda + \mu$, $\alpha_2 = \omega\lambda + \omega^2\mu$ i $\alpha_3 = \omega^2\lambda + \omega\mu$.

Uwaga o równaniach stopnia 4

Równania (wielomianowe) stopnia 2 (równania kwadratowe) umieli rozwiązywać starożytni Babilończycy. Domyślili się bowiem, że wzory (3.10) z łatwością można wyprowadzić z postaci kanonicznej (PK) z ustępu 3.2.5. Niedługo po tym jak Cardano wyłudził od Tartaglia'*i* opisaną powyżej metodę rozwiązywania równań stopnia 3, jego uczeń Ludovico Ferrari pokazał analogiczną metodę postępowania z równaniami stopnia 4. Jej szkic jest następujący:

(0) Mamy (do rozwiązania) równanie: $u^4 + au^3 + bu^2 + cu + d = 0$.

(1) Kładąc $u = x - a/4$ sprowadzamy je do postaci zredukowanej (bez wyrazu z trzecią potęgą niewiadomej): $x^4 + Ax^2 + Bx + C = 0$. Jeżeli okaże się, że $B = 0$, to rozwiązujemy otrzymane równanie dwukwadratowe.

(2) Jeżeli zaś $B \neq 0$, to, wprowadzając niewiadomą y (do wyznaczenia!), nasze równanie zapisujemy w postaci: $(x^2 + y)^2 - [(2y - A)x^2 - Bx + (y^2 - C)] = 0$.

(3) Staramy się teraz tak dobrać y, by wyrażenie w nawiasie kwadratowym było kwadratem. Robimy to za pomocą standardowej babilońskiej metody uzupełniania do pełnego kwadratu (zob. wyprowadzenie (PK) w ustępie 3.2.5). To prowadzi do równania sześciennego!

(4) Wiemy już teraz co zrobić z otrzymaną różnicą kwadratów.

U w a g a 2. Na tej drodze to już k r e s możliwości: za pomocą sztuczek polegających na tworzeniu kombinacji algebraicznych (dodawania, odejmowania, mnożenia i dzielenia) współczynników, n i e u d a j e się sprowadzić problemu znajdowania pierwiastków równania wielomianowego stopnia wyższego niż 4 do problemu wyciągania pierwiastków. Nie chodzi tu o to, że nie potrafimy tego zrobić. Chodzi o to, że tego się zrobić n i e d a. Udowodnili to Ruffini (1799) i Abel (1824). Jest to jedno z pierwszych ważnych twierdzeń n e g a t y w n y c h matematyki. Niestety nie możemy tu opowiedzieć o jego dowodzie.

3.4.8 Wzory Viète'*a*

Prawdopodobnie najczęściej stosowanym w zadaniach olimpijskich narzędziem dotyczącym wielomianów i ich pierwiastków są tak zwane wzory Viète'*a*, których przypadek szczególny, dla wielomianów stopnia drugiego, przypomnieliśmy w (3.14).

WZORY VIÈTE'*a* *Liczby (zespolone)* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *są wszystkimi (z uwzględnieniem krotności) pierwiastkami wielomianu unormowanego* $a_0 + a_1X + \ldots + X^n \in \mathbb{C}[X]$ *wtedy i tylko wtedy, gdy dla każdego* $1 \leqslant s \leqslant n$ *zachodzi równość*:

$$\sum_{1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant n} \alpha_{i_1}\alpha_{i_2} \cdot \ldots \cdot \alpha_{i_s} = (-1)^s a_{n-s}. \tag{3.53}$$

D O W Ó D. Zwrot *z uwzględnieniem krotności* oznacza, że w ciągu $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ występują wszystkie pierwiastki wielomianu, i każdy z nich tyle razy ile wynosi jego krotność. Zobacz (3.33), gdzie e_j oznacza krotność pierwiastka λ_j. Dowód równości (3.53) polega na wymnożeniu i porównaniu współczynników w równości

$$a_0 + a_1X + a_2X^2 + \ldots + X^n = (X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_n).$$

Należy się przy tym powołać na twierdzenie o jednoznaczności W2T3.4. □

W OM istnieje mnóstwo przykładów zastosowania wzorów Viète'*a*.

P r z y k ł a d 1. Rozpatrując przypadki, łatwo sprawdzić, że jeżeli suma $p=\alpha+\beta$ i iloczyn $q=\alpha\beta$ dwóch liczb rzeczywistych są dodatnie, to α i β są dodatnie. Dużo prościej jest rozważyć wielomian $f(X)=(X-\alpha)(X-\beta)$ i zauważyć, że, ponieważ $f(x)=x^2-px+q>0$ dla wszystkich $x\leqslant 0$, więc jego pierwiastki nie są $\leqslant 0$. Oto analogiczna sztuczka dla trzech liczb: *Jeżeli* $\alpha,\ \beta,\ \gamma\in\mathbb{R}$ *i* $p:=\alpha+\beta+\gamma\geqslant 0$, $q:=\alpha\beta+\beta\gamma+\gamma\alpha\geqslant 0$ *oraz* $r:=\alpha\beta\gamma\geqslant 0$, *to* $\alpha\geqslant 0$, $\beta\geqslant 0$ *i* $\gamma\geqslant 0$. Rzeczywiście, rozważmy wielomian $f(X)=(X-\alpha)(X-\beta)(X-\gamma)=X^3-pX^2+qX-r$. Jeżeli $x<0$, to $x=-y$, gdzie $y>0$ i wówczas $f(x)=f(-y)=-(y^3+py^2+qy+r)<0$. Widzimy, że żaden pierwiastek wielomianu $f(X)$ n i e jest ujemny, tzn. $\alpha,\ \beta,\ \gamma\geqslant 0$. Czytelnik z łatwością uogólni tę sztuczkę na przypadek n liczb rzeczywistych. $\Diamond$

P r z y k ł a d 2. Niech $\alpha,\ \beta,\ \gamma$ będą pierwiastkami wielomianu X^3-X-1. Wyznaczmy

$$L=\frac{\alpha-1}{\alpha+1}+\frac{\beta-1}{\beta+1}+\frac{\gamma-1}{\gamma+1}.$$

Po odjęciu 1 od każdego składnika tej sumy i podzieleniu przez -2, otrzymujemy równość $\frac{3-L}{2}=\frac{1}{\alpha+1}+\frac{1}{\beta+1}+\frac{1}{\gamma+1}=\frac{\beta\gamma+\beta+\gamma+1+\alpha\gamma+\alpha+\gamma+1+\alpha\beta+\alpha+\beta+1}{\alpha\beta\gamma+\alpha\beta+\beta\gamma+\gamma\alpha+\alpha+\beta+\gamma+1}$. Korzystając teraz z równości Viète'*a* $\alpha+\beta+\gamma=0$, $\alpha\beta+\beta\gamma+\gamma\alpha=-1$ i $\alpha\beta\gamma=1$ dostajemy $\frac{3-L}{2}=2$. Skąd $L=-1$. Można też wyznaczyć wielomian, którego pierwiastkami są składniki sumy L: zauważmy w tym celu, że $x=\frac{\alpha-1}{\alpha+1}$ wtedy i tylko wtedy, gdy $\alpha=\frac{1+x}{1-x}$. Stąd, wobec założonej równości $\alpha^3=\alpha+1$, mamy $\left(\frac{1+x}{1-x}\right)^3=\frac{2}{1-x}$, czyli $(1+x)^3=2(1-x)^2$. Widzimy więc, że składniki sumy L są pierwiastkami wielomianu X^3+X^2+7X-1. Znowu (na mocy równości Viète'*a*) dostajemy nie tylko równość $L=-1$, ale również równości

$$\frac{(\alpha-1)(\beta-1)}{(\alpha+1)(\beta+1)}+\frac{(\beta-1)(\gamma-1)}{(\beta+1)(\gamma+1)}+\frac{(\gamma-1)(\alpha-1)}{(\gamma+1)(\alpha+1)}=7,\quad \frac{(\alpha-1)(\beta-1)(\gamma-1)}{(\alpha+1)(\beta+1)(\gamma+1)}=1.\quad\Diamond$$

Pokazane sztuczki są przykładami myślenia w duchu nazwanym w ustępie 3.2.7 *filozofią Viète'*a. Oto jej myśl przewodnia: *Jeżeli badamy liczby* $\alpha_1,\ \ldots,\ \alpha_n$, *to dobrze jest zbadać wielomian* $(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$, *którego te liczby są pierwiastkami.* To może być szczególnie użyteczne, gdy w problemie występują funkcje s y m e t r y c z n e zmiennych α_i, zob. 6.2.

Ćwiczenie 3.55 Uogólnić tezę zadania Z3.11. Tzn., udowodnić, że *Jeżeli* $a,\ b,\ c\in\mathbb{Q}$ *są takie, że liczby* $a+b+c$, $ab+bc+ca$ *i* abc *są liczbami całkowitymi, to* $a,\ b,\ c\in\mathbb{Z}$. Uogólniać dalej. Na przykład, *Jeżeli* $a,\ b,\ c,\ d$ *są liczbami wymiernymi, dla których liczby* $a+b+c+d$, $ab+ac+ad+bc+bd+cd$, $abc+abd+acd+bcd$ *i* $abcd$ *są całkowite, to* $a,\ b,\ c,\ d\in\mathbb{Z}$. Itd.

ZADANIE 3.21 Udowodnić, że jeżeli $a+b+c=0$, to

$$\frac{a^5+b^5+c^5}{5}=\frac{a^2+b^2+c^2}{2}\cdot\frac{a^3+b^3+c^3}{3}. \tag{3.54}$$

R o z w i ą z a n i e. Rozważmy wielomian $f(X)=(X-a)(X-b)(X-c)=X^3+qX+r$, którego liczby $a,\ b,\ c$ są pierwiastkami. Współczynnik przy X^2 jest, na mocy założenia, równy 0. Ponieważ $f(a)=f(b)=f(c)=0$, więc mamy

$$\begin{cases} a^3=-qa-r,\\ b^3=-qb-r,\\ c^3=-qc-r. \end{cases} \tag{3.55}$$

Dodając stronami, po uwzględnieniu założenia $a+b+c=0$, dostajemy

$$\frac{a^3+b^3+c^3}{3} = -r. \tag{3.56}$$

Z drugiej strony, $0=(a+b+c)^2 = a^2+b^2+c^2+2(ab+bc+ca) = a^2+b^2+c^2+2q$, więc

$$\frac{a^2+b^2+c^2}{2} = -q. \tag{3.57}$$

Pomnóżmy teraz pierwszą z równości (3.55) przez a^2, drugą przez b^2, trzecią przez c^2 i dodajmy stronami. Dostaniemy:

$$a^5+b^5+c^5 = -q(a^3+b^3+c^3) - r(a^2+b^2+c^2).$$

Wstawiając tu w miejsce $-q$ i $-r$ wartości z równości (3.56) i (3.57), po prostych przekształceniach, otrzymamy (3.54). ◊

ZADANIE 3.22 Rozwiązać układ równań

$$\begin{cases} x+y+z=3, \\ x^2+y^2+z^2=5, \\ x^3+y^3+z^3=9. \end{cases} \tag{3.58}$$

Rozwiązanie. Załóżmy, że trójka (a, b, c) jest rozwiązaniem i, w zgodzie z filozofią Viète'a, rozważmy wielomian $f(X) = (X-a)(X-b)(X-c) = X^3+\sigma_1X^2+\sigma_2X+\sigma_3$. Oznaczamy tu (i w dalszym ciągu – zobacz też ustęp 6.2.1):

$$\sigma_1 = a+b+c, \qquad \sigma_2 = ab+bc+ca, \qquad \sigma_3 = abc. \tag{3.59}$$

Wygodnie też będzie specjalnie oznaczyć sumy potęg badanych liczb, na przykład tak:

$$s_1 = a+b+c, \quad s_2 = a^2+b^2+c^2, \quad s_3 = a^3+b^3+c^3. \tag{3.60}$$

Przy tych oznaczeniach założenie, że (a, b, c) jest rozwiązaniem układu (3.58), zapisujemy tak: $s_1=3$, $s_2=5$, $s_3=9$. Druga część rozwiązania zasadza się na obserwacji, że dla dowolnych a, b, c, istnieją zależności pozwalające wyrazić s_1, s_2, s_3 za pomocą $\sigma_1, \sigma_2, \sigma_3$ i odwrotnie, zobacz C3.56. Wobec tego równości (3.62) dają: $\sigma_1=3$, $\sigma_2=2$, $\sigma_3=0$. Zatem $f(X) = X^3-3X^2+2X$. Pierwiastkami tego wielomianu są liczby 0, 1, 2. Stąd odpowiedź: Układ (3.58) ma sześć rozwiązań. Są to: trójka (0, 1, 2) i jej permutacje. ◊

Ćwiczenie 3.56 Przy oznaczeniach wprowadzonych w (3.59) i (3.60), zachodzą równości:

$$s_1 = \sigma_1, \qquad s_2 = \sigma_1^2 - 2\sigma_2, \qquad s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3, \tag{3.61}$$

$$\sigma_1 = s_1, \qquad \sigma_2 = \tfrac{1}{2}(s_1^2 - s_2), \qquad \sigma_3 = \tfrac{1}{6}(s_1^3 - 3s_1s_2 + 2s_3). \tag{3.62}$$

Ucząc się o wielomianach symetrycznych, powiemy nieco więcej o równościach takiego typu.

Ćwiczenie 3.57 Udowodnić, że jeżeli $a+b+c=0$, to

$$2a^4+2b^4+2c^4=(a^2+b^2+c^2)^2.$$

Ćwiczenie 3.58 Udowodnić, że jeżeli $a+b+c=0$, to

$$\frac{a^7+b^7+c^7}{7}=\frac{a^2+b^2+c^2}{2}\cdot\frac{a^5+b^5+c^5}{5}.$$

Ćwiczenie 3.59 Wyznaczyć wszystkie rzeczywiste rozwiązania równania

$$\sqrt[4]{337-x}+\sqrt[4]{x}=7.$$

Ćwiczenie 3.60 Udowodnić, że jeżeli u, v, $w\neq 0$ i zachodzą równości $u+v+w=a$ oraz $1/u+1/v+1/w=1/a$, to co najmniej jedna z liczb u, v, w jest równa a.

3.4.9 Wielomiany palindromiczne

Ostatnim rozważanym teraz tematem związanym z pierwiastkami wielomianów jest temat tak zwanych wielomianów palindromicznych.

Definicja 3.16 Wielomian $q(X)=a_0+a_1X+\ldots+a_nX^n$ nazwiemy **wielomianem palindromicznym**, gdy $a_0\neq 0$ i $a_s=a_{n-s}$ dla każdego s.

Poniższe ćwiczenia pokazują, że rozwiązywanie równań wielomianowych $q(x)=0$, z wielomianem palindromicznym $q(X)$, może być uproszczone.

Ćwiczenie 3.61 Wielomian $q(X)$ stopnia n jest wielomianem palindromicznym wtedy i tylko wtedy, gdy zachodzi równość $X^n q\left(\frac{1}{X}\right)=q(X)$.

Ćwiczenie 3.62 Jeżeli α jest pierwiastkiem wielomianu palindromicznego, to $\alpha\neq 0$ i α^{-1} jest również pierwiastkiem.

Ćwiczenie 3.63 Jeżeli wielomian $q(X)$ jest wielomianem palindromicznym nieparzystego stopnia, to -1 jest jego pierwiastkiem i w rozkładzie $q(X)=(X+1)\cdot r(X)$ wielomian $r(X)$ jest wielomianem palindromicznym stopnia parzystego.

Ćwiczenie 3.64 Jeżeli $q(X)$ jest wielomianem palindromicznym stopnia parzystego $2m$, to można go zapisać w postaci $q(X)=X^m\cdot s(Z)$, gdzie $s(Z)$ jest wielomianem stopnia m zmiennej $Z=X+X^{-1}$.

P r z y k ł a d. Chcemy rozwiązać równanie $q(x)=0$ przy

$$q(X)=2+3X+4X^2+4X^3+3X^4+2X^5.$$

Wiemy z C3.63, że $(X+1)|q(X)$. To daje rozwiązanie $\alpha_1=-1$. Dzieląc otrzymamy:

$$q(X)=(X+1)(2X^4+X^3+3X^2+X+2)=(X+1)\cdot r(X).$$

Podstawienie z ćwiczenia C3.64 daje

$$r(x) = x^2\left[2\left(x^2+\frac{1}{x^2}\right)+\left(x+\frac{1}{x}\right)+3\right] = x^2(2(z^2-2)+z+3) = x^2(2z^2+z-1).$$

Rozwiązując równanie kwadratowe $2z^2+z-1$ otrzymujemy dwa rozwiązania: $z_1=-1$ i $z_2=1/2$. Wracając do niewiadomej x, otrzymujemy dwa równania kwadratowe:

$$x+\frac{1}{x}=-1, \quad \text{oraz} \quad x+\frac{1}{x}=1/2,$$

a te już potrafimy rozwiązać. ◊

U w a g a. O tym, że d a się wyrazić X^n+X^{-n} jako wielomian zmiennej $Z=X+X^{-1}$, i jak to zrobić dla dużych n, powiemy w ustępie poświęconym wielomianom Czebyszewa.

3.4.10 Wielomian interpolacyjny Lagrange'*a*

Udowodnimy teraz proste (i przydatne) ***twierdzenie interpolacyjne Lagrange'*a**.

TWIERDZENIE 3.23 *Niech $\alpha_0, \alpha_1, \ldots, \alpha_n$ będą (parami) różnymi elementami ciała $\mathbb{K}$, a $\beta_0, \beta_1, \ldots, \beta_n$, dowolnymi elementami tego ciała. Wówczas istnieje dokładnie jeden taki wielomian $f(X)\in\mathbb{K}[X]$, że $\deg f(X)\leqslant n$ oraz $f(\alpha_j)=\beta_j$ dla każdego $j=0,1,\ldots,n$.*

D O W Ó D. Dla każdego $0\leqslant k\leqslant n$ zdefiniujmy wielomian stopnia n

$$g_k(X)=\prod_{j=0,\,j\neq k}^{n}(\alpha_k-\alpha_j)^{-1}(X-\alpha_j). \tag{3.63}$$

Jasne, że $g_k(\alpha_l)=0$ dla $k\neq l$, oraz $g_k(\alpha_k)=1$. Widzimy stąd natychmiast, że wielomian $f(X)=\sum_{k=0}^{n}\beta_k g_k(X)$ spełnia żądane warunki. Jeżeli $h(X)$ również spełnia te warunki, to wielonian $f(X)-h(X)$ ma stopień mniejszy bądź równy n i $n+1$ różnych pierwiastków $\alpha_0, \alpha_1, \ldots, \alpha_n$, jest więc wielomianem zerowym, zobacz W2T3.4. □

Ćwiczenie 3.65 Niech $f(X)\in\mathbb{R}[X]$ będzie takim wielomianem stopnia n, że dla $k=0,1,\ldots,n$ zachodzi równość $f(k)=k/(k+1)$. Wyznaczyć $f(n+1)$.

Ćwiczenie 3.66 Udowodnić następujące równości:

$$\sum_{k=0}^{n}(-1)^k k^m\binom{n}{k}=\begin{cases}0, & \text{gdy } 0\leqslant m<n,\\ (-1)^n n!, & \text{gdy } m=n.\end{cases}$$

Wskazówka. Zbadać wielomian interpolacyjny Lagrange'*a*, który dla argumentów $\alpha_k=k$, $k=0,1,\ldots,n$, przyjmuje wartości k^m.

3.4.11 Funkcje wymierne. Ułamki proste

Ten ustęp poświęcimy na rozkładanie funkcji wymiernych na ułamki proste.

Definicja 3.17 Niech $\mathbb{K}$ będzie ciałem. Napis $\frac{a(X)}{b(X)}$, gdzie $a(X)$, $b(X) \in \mathbb{K}[X]$, przy czym $b(X) \neq 0$, nazywamy **funkcją wymierną zmiennej** X **nad ciałem** $\mathbb{K}$. Uważamy, że funkcja wymierna $\frac{a(X)}{b(X)}$ jest **równa** funkcji wymiernej $\frac{c(X)}{d(X)}$, co zapisujemy $\frac{a(X)}{b(X)} = \frac{c(X)}{d(X)}$, gdy zachodzi równość wielomianów $a(X)d(X) = b(X)c(X)$. Zbiór wszystkich funkcji wymiernych zmiennej X nad ciałem $\mathbb{K}$ oznaczamy symbolem $\mathbb{K}(X)$. Wielomian $a(X) \in \mathbb{K}[X]$ utożsamiamy z funkcją wymierną $\frac{a(X)}{1}$. W szczególności, gdy **mianownik** $b(X)$ funkcji wymiernej $\frac{a(X)}{b(X)}$ jest dzielnikiem **licznika** $a(X)$ i zachodzi równość $a(X) = b(X)cX)$ w pierścieniu $\mathbb{K}[X]$, to funkcja wymierna $\frac{a(X)}{b(X)}$ jest r ó w n a wielomianowi $c(X)$ w $\mathbb{K}(X)$.

P r z y k ł a d 1. Przepiszmy tożsamość (1.8) jako równość w ciele funkcji wymiernych:

$$\frac{a^n - X^n}{a - X} = a^{n-1} + a^{n-2}X + \cdots + aX^{n-2} + X^{n-1}. \quad \Diamond$$

Zbiór $\mathbb{K}(X)$ funkcji wymiernych nad $\mathbb{K}$ ma się tak do swojego podzbioru $\mathbb{K}[X]$ wielomianów nad $\mathbb{K}$, jak zbiór liczb wymiernych $\mathbb{Q}$ ma się do swojego podzbioru $\mathbb{Z}$ liczb całkowitych. Czytelnik zdaje sobie sprawę z pożytków płynących z rozszerzenia zbioru $\mathbb{Z}$ liczb całkowitych do zbioru $\mathbb{Q}$ liczb wymiernych (ułamków). Podobnie użyteczne jest rozszerzenie $\mathbb{K}[X] \subset \mathbb{K}(X)$. Aby to pełniej zobaczyć nauczymy się wykonywać działania dodawania i mnożenia, a także dzielenia w $\mathbb{K}(X)$. Funkcje wymierne dodajemy i mnożymy w sposób naturalny:

$$\frac{a(X)}{b(X)} + \frac{c(X)}{d(X)} := \frac{a(X)d(X) + b(X)c(X)}{b(X)d(X)},$$

$$\frac{a(X)}{b(X)} \cdot \frac{c(X)}{d(X)} := \frac{a(X)c(X)}{b(X)d(X)}.$$

Ćwiczenie 3.67 Załóżmy, że $\varphi_1(X)$, $\varphi_2(X)$, $\psi(X) \in \mathbb{K}(X)$ i $\varphi_1(X) = \varphi_2(X)$. Udowodnić, że wówczas $\varphi_1(X) + \psi(X) = \varphi_2(X) + \psi(X)$, oraz $\varphi_1(X) \cdot \psi(X) = \varphi_2(X) \cdot \psi(X)$.

Ćwiczenie 3.68 Udowodnić, że $\mathbb{K}(X)$ z określonymi wyżej działaniami jest ciałem.

Matematycy mówią, że $\mathbb{Q}$ jest **ciałem ułamków** pierścienia $\mathbb{Z}$, a $\mathbb{K}(X)$ jest ciałem ułamków pierścienia $\mathbb{K}[X]$.

P r z y k ł a d 2. Rozważmy wielomian $f(X) = \sum_{k=0}^{n} (k+1)X^k \in \mathbb{Q}[X]$. Zapiszemy go jako funkcję wymierną, czyli w postaci ułamka $\frac{a(X)}{b(X)}$. W tym celu liczymy iloczyn $(1 - X)f(X)$:

$$f(X) - Xf(X) = \sum_{k=0}^{n} (k+1)X^k - \sum_{k=0}^{n} (k+1)X^{k+1} = 1 + X + X^2 + \cdots + X^n - (n+1)X^{n+1}.$$

Pierwszy składnik sumy zapisujemy (tak jak w P1) w postaci $(1-X^{n+1})/(1-X)$. Po wykonaniu działań i podzieleniu przez $1 - X$ (to znaczy, po pomnożeniu w $\mathbb{Q}(X)$ przez $\frac{1}{1-X}$), dostajemy

$$\sum_{k=0}^{n} (k+1)X^k = \frac{1 - (n+2)X^{n+1} + (n+1)X^{n+2}}{(1-X)^2}. \quad \Diamond$$

Definicja 3.18 Funkcję wymierną postaci

$$\frac{a(X)}{p(X)^n},$$

gdzie wielomian $p(X)$ jest nierozkładalny (w $\mathbb{K}[X]$), oraz $\deg a(X) < \deg p(X)$, nazywamy **funkcją wymierną prostą** lub **ułamkiem prostym**.

Chcemy zapisywać funkcje wymierne w postaci sum ułamków prostych:

LEMAT 3.3 *Jeżeli mianownik funkcji wymiernej* $\varphi(X) = \frac{a(X)}{u(X)v(X)}$ *jest iloczynem dwóch wielomianów względnie pierwszych, to* $\varphi(X)$ *jest sumą postaci* $\frac{a_1(X)}{u(X)} + \frac{a_2(X)}{v(X)}$.

D O W Ó D. Założenie względnej pierwszości wielomianów $u(X)$, $v(X)$ pozwala napisać równość Gaussa $u(X)k(X) + v(X)l(X) = 1$ dla pewnych wielomianów $k(X)$, $l(X)$, zobacz T3.11. Mnożąc tę równość przez $a(X)$ dostajemy

$$\frac{a(X)}{u(X)v(X)} = \frac{u(X)k(X)a(X) + v(X)l(X)a(X)}{u(X)v(X)} = \frac{k(X)a(X)}{v(X)} + \frac{l(X)a(X)}{u(X)}.$$

Wystarczy więc położyć $a_1(X) = l(X)a(X)$ i $a_2(X) = k(X)a(X)$. □

TWIERDZENIE 3.24 *Każdą funkcję wymierną* $\varphi(X) \in \mathbb{K}(X)$ *można przedstawić w postaci sumy wielomianu i pewnej liczby funkcji wymiernych prostych.*

D O W Ó D. Jasnym być powinno jak za pomocą prostej indukcji uogólnić tezę lematu na przypadek, gdy w mianowniku funkcji wymiernej $\varphi(X)$ stoi iloczyn dowolnej liczby parami względnie pierwszych czynników. Przedstawmy więc mianownik $b(X)$ danej funkcji wymiernej $\frac{a(X)}{b(X)}$ w postaci

$$b(X) = Cp_1(X)^{e_1}p_2(X)^{e_2} \cdot \ldots \cdot p_s(X)^{e_s},$$

gdzie $p_j(X)$ są parami niestowarzyszonymi wielomianami nierozkładalnymi, a $C \in \mathbb{K}$. [Taki rozkład uzyskuje się z rozkładu opowiedzianego w T3.14 przez zgrupowanie w jedną potęgę czynników stowarzyszonych. To samo zrobiliśmy w 2.4.1 (RK) w przypadku pierścienia $\mathbb{Z}$.] "Wrzucając" czynnik C do licznika widzimy funkcję wymierną mającą s parami względnie pierwszych czynników $p_i(X)^{e_i}$ w mianowniku. Mamy więc rozkład

$$\varphi(X) = \frac{a_1(X)}{p_1(X)^{e_1}} + \frac{a_2(X)}{p_2(X)^{e_2}} + \ldots + \frac{a_s(X)}{p_s(X)^{e_s}}.$$

Składniki tej sumy nie muszą być ułamkami prostymi, bo $\deg a_i(X)$ może być za duży. Gdy tak jest, dzielimy licznik $a_i(X)$ przez $p_i(X)$ z resztą: $a_i(X) = q_i(X)p_i(X) + d_i(X)$. Otrzymamy:

$$\frac{a_i(X)}{p_i(X)^{e_i}} = \frac{q_i(X)}{p_i(X)^{e_i-1}} + \frac{d_i(X)}{p_i(X)^{e_i}}.$$

Drugi składnik w tej sumie jest już ułamkiem prostym. Czytelnik z pewnością wie co zrobić z pierwszym składnikiem dla zakończenia dowodu. □

P r z y k ł a d 3. Wiemy, że $X^2 + X + 1 = (X - \omega)(X - \overline{\omega})$, zobacz Z3.20. Stąd

$$\frac{2X+1}{X^2+X+1} = \frac{1}{X-\omega} + \frac{1}{X-\overline{\omega}}. \quad \Diamond$$

Ćwiczenie 3.69 Wymyślić co to jest rozkład liczby wymiernej na sumę ułamków prostych i udowodnić możliwość takiego rozkładu.

3.4.12 Funkcje wymierne jako funkcje

Funkcja wymierna jest n a p i s e m, zobacz D3.17. Podobnie jak wielomian!, zobacz D3.1. I, podobnie jak wielomian, w y z n a c z a pewną funkcję.

Definicja 3.19 Niech $\mathbb{K}$ będzie ciałem, a $\varphi(X) = \frac{a(X)}{b(X)} \in \mathbb{K}(X)$. Kładziemy

$$\varphi(\lambda) = \frac{a(\lambda)}{b(\lambda)} = a(\lambda)b(\lambda)^{-1}$$

dla wszystkich $\lambda \in \mathbb{K}$, dla których $b(\lambda) \neq 0$. (Zauważyć i udowodnić, że jeżeli $\varphi_1(X) = \varphi_2(X)$, to $\varphi_1(\lambda) = \varphi_2(\lambda)$ dla wszystkich $\lambda \in \mathbb{K}$, dla których to ma sens!) Tak określony element $\varphi(\lambda) \in \mathbb{K}$ nazywamy **wartością funkcji wymiernej** dla argumentu $\lambda \in D_\varphi$. Przy tym symbolem D_φ oznaczamy **dziedzinę określoności** funkcji wymiernej $\varphi(X)$, czyli zbiór $D_\varphi := \mathbb{K} \setminus \{\lambda_1, \ldots, \lambda_s\}$, gdzie $\{\lambda_1, \ldots, \lambda_s\}$ jest zbiorem wszystkich pierwiastków (miejsc zerowych) wielomianu $b(X)$. W ten sposób funkcja wymierna $\varphi(X) \in \mathbb{K}(X)$ określa funkcję $D_\varphi \ni \lambda \longmapsto \varphi(\lambda) \in \mathbb{K}$ określoną na dopełnieniu (w $\mathbb{K}$) zbioru zer mianownika.

Twierdzenie 3.25 (***Twierdzenie o jednoznaczności dla funkcji wymiernych***) *Jeżeli $\varphi(X), \psi(X) \in \mathbb{K}(X)$ są takimi funkcjami wymiernymi, że funkcje*

$$\lambda \longmapsto \varphi(\lambda) \quad i \quad \lambda \longmapsto \psi(\lambda)$$

pokrywają się na zbiorze $D_\varphi \cap D_\psi$, a ten zbiór jest nieskończony, to $\varphi(X) = \psi(X)$ w $\mathbb{K}(X)$.

D O W Ó D. Niech $\varphi(X) = \frac{a(X)}{b(X)}$ i $\psi(X) = \frac{c(X)}{d(X)}$. Jeżeli $a(\lambda)b(\lambda)^{-1} = c(\lambda)d(\lambda)^{-1}$ dla $\lambda \in D_\varphi \cap D_\psi$, to $a(\lambda)d(\lambda) = b(\lambda)c(\lambda)$ dla wszystkich takich λ. Te równości oznaczają, że wielomiany $a(X)d(X)$ i $b(X)c(X)$ przyjmują te same wartości na dużym (mającym nieskończenie wiele, w szczególności, więcej niż maksimum stopni tych wielomianów) zbiorze $D_\varphi \cap D_\psi$. Powołując się na twierdzenie o jednoznaczności dla wielomianów, zob. W2T3.4, otrzymujemy równość $a(X)d(X) = b(X)c(X)$ w pierścieniu $\mathbb{K}[X]$. Czyli, zgodnie z definicją równości funkcji wymiernych, równość $\varphi(X) = \psi(X)$. □

3.5 Wielomiany wielu zmiennych

Często zmiennych jest więcej niż jedna. Myślimy i mówimy wtedy o wielomianach wielu zmiennych. Postępowanie z takimi wielomianami jest prawie tak samo proste jak z wielomianami jednej zmiennej.

3.5.1 Definicje

Czytelnik z pewnością domyśla się, co to jest wielomian wielu zmiennych. Na przykład

$$A(X, Y) = a_0(X) + a_1(X)Y + a_2(X)Y^2 + \cdots + a_n(X)Y^n,$$

gdzie $a_i(X)$ są wielomianami zmiennej X o współczynnikach z ciała $\mathbb{K}$, jest **wielomianem dwóch zmiennych**.

Zbiór wielomianów dwóch zmiennych o współczynnikach w ciele $\mathbb{K}$ oznaczamy symbolem $\mathbb{K}[X, Y]$. Pierścień $\mathbb{K}[X, Y]$ może być uważany za pierścień wielomianów jednej zmiennej Y o współczynnikach z pierścienia $\mathbb{K}[X]$:

$$\mathbb{K}[X, Y] = \mathbb{K}[X][Y].$$

Ponieważ w pierścieniu współczynników $\mathbb{K}[X]$ istnieje, jak wiemy z 3.3.2, NWD dowolnego skończonego układu elementów, więc możemy wprowadzić pojęcie **zawartości** wielomianu dwóch zmiennych, udowodnić analogony lematu i twierdzenia Gaussa (zobacz L3.1 i T3.15), a następnie ***twierdzenia o jednoznaczności rozkładu*** na czynniki nierozkładalne. Byłoby dobrze gdyby Czytelnik zechciał się o tym przekonać.

Pojęcie wielomianu n zmiennych jest natychmiastowym uogólnieniem:

Definicja 3.20 Skończoną sumę postaci

$$A(X_1, X_2, \ldots, X_n) = \sum a_{k_1 k_2 \ldots k_n} X_1^{k_1} X_2^{k_2} \ldots X_n^{k_n}, \tag{3.64}$$

gdzie $a_{k_1 k_2 \ldots k_n} \in \mathbb{K}$, nazywamy **wielomianem n zmiennych** o współczynnikach z ciała $\mathbb{K}$. Zbiór wielomianów n zmiennych $X_1, X_2, \ldots, X_n$, oznaczany przez $\mathbb{K}[X_1, X_2, \ldots, X_n]$, może być uważny za zbiór wielomianów jednej zmiennej X_n o współczynnikach z pierścienia $\mathbb{K}[X_1, \ldots, X_{n-1}]$ wielomianów $(n-1)$ zmiennych:

$$\mathbb{K}[X_1, X_2, \ldots, X_n] = \mathbb{K}[X_1, \ \ldots, X_{n-1}][X_n].$$

Wielomiany dodajemy i mnożymy w sposób "naturalny". Przy tych działaniach zbiór $\mathbb{K}[X_1, X_2, \ldots, X_n]$ jest pierścieniem przemiennym z jedynką. Również w tym pierścieniu zachodzi twierdzenie o istnieniu i jednoznaczności rozkładu na czynniki nierozkładalne.

Definicja 3.21 Wielomian postaci $aX_1^{k_1} X_2^{k_2} \cdot \ldots \cdot X_n^{k_n}$, gdzie $a \in \mathbb{K}$, nazywamy **jednomianem**. Jeżeli przy tym jego współczynnik a jest różny od 0, to **stopniem** tego jednomianu nazywamy liczbę

$$k_1 + k_2 + \ \ldots \ + k_n.$$

Maksymalny ze stopni (niezerowych!) jednomianów występujących w danym wielomianie A nazywamy **stopniem wielomianu** A i oznaczamy symbolem $\deg A$.

Ćwiczenie 3.70 Udowodnić, że dla dowolnych wielomianów $A, B \in \mathbb{K}[X_1, \ldots, X_n]$,

(1) $\deg(A \cdot B) = \deg A + \deg B$,

(2) $\deg(A + B) \leqslant \max\{\deg A, \deg B\}$ (gdy $\deg A \neq \deg B$, to zachodzi równość).

Jednomiany występujące w sumie (3.64), wygodnie jest porządkować (rosnąco lub malejąco) według stopni. Piszemy więc

$$A(X_1, X_2, \ldots, X_n) = A_{(0)} + A_{(1)} + A_{(2)} + \ \ldots \ + A_{(d)}, \tag{3.65}$$

gdzie $A_{(k)}$ oznacza sumę wszystkich (niezerowych) jednomianów stopnia k występujących w (3.64), a d jest stopniem wielomianu A. Taki sposób ("malejąco") uporządkowania widzimy w (11.45) dla wielomianu dwóch zmiennych stopnia 2 i w (11.50) dla wielomianu dwóch zmiennych stopnia 3. Składnik $A_{(k)}$ nazywa się **składnikiem jednorodnym stopnia** k wielomianu A. Jasne, że spełnia on **warunek jednorodności stopnia** k:

$$A_{(k)}(\lambda x_1,\, \lambda x_2,\, \ldots,\, \lambda x_n) = \lambda^k \cdot A_{(k)}(x_1,\, x_2,\, \ldots,\, x_n)$$

dla dowolnych $\lambda,\, x_1,\, x_2,\, \ldots,\, x_n \in \mathbb{K}$.

3.5.2 Tożsamość Sophie Germain

Do wielomianów wielu zmiennych powrócimy jeszcze w rozdziale 6. Teraz wykorzystamy nadarzającą się okazję, by powiedzieć parę słów na temat pewnego wzoru skróconego mnożenia. U w a g a. Olimpijczycy mogą używać terminu *wzory skróconego mnożenia*, pod warunkiem, że wiedzą, że chodzi o **tożsamości algebraiczne**.

Sprawdzenie, że w pierścieniu $\mathbb{Q}[X,\, Y]$ zachodzi równość

$$4X^4 + Y^4 = (2X^2 + 2XY + Y^2)(2X^2 - 2XY + Y^2), \tag{3.66}$$

jest natychmiastowe. Zapisujemy to też w postaci tak zwanej ***tożsamości Sophie Germain***:

$$\boxed{\boxed{4x^4 + y^4 = (2x^2 + 2xy + y^2)(2x^2 - 2xy + y^2).}} \tag{3.67}$$

Znający wzór na różnicę kwadratów łatwo się domyślają skąd to się wzięło:

$$4x^4 + y^4 = 4(x^2)^2 + 4x^2y^2 + (y^2)^2 - (2xy)^2 = (2x^2 + y^2)^2 - (2xy)^2.$$

ZADANIE 3.23 Niech $A_n = 2^{2^n-2} + 1$. Dowieść, że A_n jest złożona dla $n \in \mathbb{N}_{\geqslant 3}$.

R o z w i ą z a n i e. Dzięki tożsamości (3.67) mamy:

$$A_n = \frac{1}{4}\left(4 \cdot 1^4 + 2^{2^n}\right) = \frac{1}{4}\left(2 + 2 \cdot 2^{2^{n-2}} + 2^{2^{n-1}}\right)\left(2 - 2 \cdot 2^{2^{n-2}} + 2^{2^{n-1}}\right) =$$
$$= \left(1 + 2^{2^{n-2}} + 2^{2^{n-1}-1}\right)\left(1 - 2^{2^{n-2}} + 2^{2^{n-1}-1}\right).$$

Wystarczy teraz sprawdzić, że drugi z tych czynników jest liczbą naturalną $\geqslant 2$. To jest jasne, bo $2^{n-2} < 2^{n-1} - 1$ dla $n \geqslant 3$. $\Diamond$

Ćwiczenie 3.71 Wyliczyć sumy $\sum_{k=1}^{100} \dfrac{4k}{4k^4+1}$ oraz $\sum_{k=1}^{64} \dfrac{4k^2-2}{4k^4+1}$.

Ćwiczenie 3.72 Udowodnić, że dla wszystkich n istnieje nieskończenie wiele liczb naturalnych a, dla których liczba $n^4 + a$ jest liczbą złożoną.

Ćwiczenie 3.73 Liczba $n^4 + 4^n$ jest liczbą pierwszą wtedy i tylko wtedy, gdy $n = 1$.

Ćwiczenie 3.74 Rozłożyć wielomian $X^4 + 324$ na iloczyn czynników najmniejszych możliwych stopni, najpierw w pierścieniu $\mathbb{Q}[X]$, potem w $\mathbb{R}[X]$, a następnie w $\mathbb{C}[X]$.

3.5.3 Jeszcze dwie faktoryzacje

Na zakończenie tego paragrafu powrócimy do tożsamości z ćwiczenia C3.54. Czytelnicy, którym nie udało się dotychczas rozwiązać tego ćwiczenia, powinni spróbować jeszcze raz:

Ćwiczenie 3.75 Udowodnić tożsamości:

$$x^3+y^3+z^3-3xyz=(x+y+z)(x+\omega y+\omega^2 z)(x+\omega^2 y+\omega z), \tag{3.68}$$

$$x^3+y^3+z^3-3xyz=(x+y+z)(x^2+y^2+z^2-xy-yz-zx), \tag{3.69}$$

$$x^3+y^3+z^3-3xyz=\frac{1}{2}(x+y+z)\left((x-y)^2+(y-z)^2+(z-x)^2\right). \tag{3.70}$$

Wskazówka. Dla dowodu (3.68) zobacz twierdzenie o strażakach T3.20.

Pokażemy kilka przykładów zastosowania tych tożsamości.

P r z y k ł a d. Niech a, b, $c\in\mathbb{R}$, $a\neq b$. Załóżmy, że zachodzi równość $c^3=a^3+b^3+3abc$. Udowodnimy, że $c=a+b$. Korzystając z tożsamości (3.68), możemy przepisać założenie w postaci $0=c^3+(-a)^3+(-b)^3-3(-a)(-b)c=(c-a-b)(c-\omega a-\omega^2 b)(c-\omega^2 a-\omega b)$. Stąd, ponieważ $c\neq\omega a+\omega^2 b$ (bo $\omega a+\omega^2 b\notin\mathbb{R}$) i $c\neq\omega^2 a+\omega b$ (bo również $\omega^2 a+\omega b\notin\mathbb{R}$), więc $c=a+b$. To, że $\omega a+\omega^2 b\notin\mathbb{R}$ sprawdzamy sprzęgając: $\overline{\omega a+\omega^2 b}=\omega^2 a+\omega b\neq\omega a+\omega^2 b$. $\Diamond$

Twierdzenie 3.26 *Jeżeli* $x+y+z=0$, *to* $x^3+y^3+z^3=3xyz$. $\square$

Ćwiczenie 3.76 Rozwiązać równanie $(x^2-x-2)^3+(x^2-5x+6)^3=(2x^2-6x+4)^3$. *Wskazówka.* Podstawmy $u=x^2-x-2$, $v=x^2-5x+6$ i $w=-2x^2+6x-4$. Widzimy, że $u+v+w=0$.

Ćwiczenie 3.77 Liczba $3^{3^n}\left(3^{3^n}+1\right)+3^{3^n+1}-1$ jest złożona dla każdego $n\in\mathbb{N}$. Dowieść.

ZADANIE 3.24 Oznaczmy $F(a,b,c)=a^3+b^3+c^3-3abc$. Udowodnić, że zbiór $\mathscr{S}$ liczb całkowitych dających się przedstawić w postaci $F(a,b,c)$ przy a, b, $c\in\mathbb{Z}$, jest **multyplikatywnym podzbiorem** zbioru $\mathbb{Z}$ (tzn., że $uv\in\mathscr{S}$ dla dowolnych u, $v\in\mathscr{S}$).

R o z w i ą z a n i e. Wykorzystamy (3.68). Z równości tej widzimy, że liczba u należy do zbioru $\mathscr{S}$ wtedy i tylko wtedy, gdy istnieje taki wielomian $f(X)=a+bX+cX^2\in\mathbb{Z}[X]$, że $u=f(1)f(\omega)f(\omega^2)$. Niech dodatkowo $v=g(1)g(\omega)g(\omega^2)$ będzie również elementem zbioru $\mathscr{S}$. Wówczas $u\cdot v=f(1)f(\omega)f(\omega^2)\cdot g(1)g(\omega)g(\omega^2)=h(1)h(\omega)h(\omega^2)$, gdzie $h(X)=f(X)g(X)$ jest wielomianem stopnia $\leqslant 4$ o współczynnikach całkowitych. Dzieląc (z resztą) wielomian $h(X)$ przez wielomian X^3-1 dostajemy $h(X)=q(X)(X^3-1)+r(X)$. Reszta $r(X)$ jest wielomianem stopnia $\leqslant 2$ o współczynnikach całkowitych(!). Oraz, oczywiście, $h(1)=r(1)$, $h(\omega)=r(\omega)$ i $h(\omega^2)=r(\omega^2)$. Zatem $uv=r(1)r(\omega)r(\omega^2)$, więc $uv\in\mathscr{S}$. $\Diamond$

Ćwiczenie 3.78 Udowodnić, że równanie $x^3+y^3+z^3-3xyz=3$ nie ma rozwiązań w liczbach całkowitych. *Wskazówka.* Wykorzystać równość (3.70)

Ćwiczenie 3.79 Udowodnić, że zbiór $\mathscr{S}$ z zadania Z3.24 jest równy $\{a\in\mathbb{Z}:\ v_3(a)\neq 1\}$, czyli że składa się ze wszystkich liczb całkowitych postaci $3k\pm 1$ lub $9k$.

Ćwiczenie 3.80 Udowodnić, że jeżeli dla liczb całkowitych a, b, c zachodzi równość

$$(a-b)^2+(b-c)^2+(c-a)^2=abc,$$

to liczba $a+b+c+6$ jest dzielnikiem liczby $a^3+b^3+c^3$.

Ćwiczenie 3.81 Udowodnić tożsamość:

$$\boxed{(x+y+z)^3-x^3-y^3-z^3=3(x+y)(y+z)(z+x).} \tag{3.71}$$

Wskazówka. Zobaczyć, że wielomian $(X+Y+Z)^2-X^3-Y^3-Z^3\in\mathbb{Q}[Y,Z]\,[X]$ jednej zmiennej X ma w pierścieniu współczynników $\mathbb{Q}[Y,Z]$ pierwiastek $-Y$. Więc dzieli się przez wielomian nierozkładalny $X-(-Y)$. Itd. Można też po prostu mnożyć.

Tożsamość (3.71) można wykorzystać w rozwiązaniu poniższego ćwiczenia:

Ćwiczenie 3.82 Udowodnić, że dla dowolnych liczb naturalnych k, l, m liczba

$$(k+l+m)^{2013}-k^{2013}-l^{2013}-m^{2013}$$

jest podzielna przez liczbę $(k+l+m)^3-k^3-l^3-m^3$. *Wskazówka.* Liczba $-a$ jest pierwiastkiem wielomianu $(X+a+b)^{2n+1}-X^{2n+1}-a^{2n+1}-b^{2n+1}$.

3.6 Zadania dodatkowe

Do rozwiązania poniższych zadań wystarczy w zasadzie teoria wyłożona w tym i poprzednim rozdziale. W paru wyjątkowych przypadkach dobrze jest mieć trochę więcej wiedzy z analizy matematycznej (nierówność między średnimi, proste granice). Coraz ważniejsza staje się też umiejętność posługiwania się liczbami zespolonymi (wystarcza teoria z rozdziału 1).

3.6.1 Treści zadań

Dla wygody poniższy zbiorek zadań podzieliliśmy na podzbiorki.

A. Współczynniki wielomianów.

ZADANIE 3.A1 Wielomian $(1-X+X^2)^5$ o współczynnikach całkowitych zapisujemy w postaci $\sum_{j\geqslant 0}a_jX^j$. Wyznaczyć: **(1)** sumę $a_0+a_1+\ldots+a_{10}$; **(2)** sumę naprzemienną $a_1-a_2+\cdots+a_9$.

ZADANIE 3.A2 Dane są wielomiany $f(X)=(1+X-X^2)^{77}$ i $h(X)=(1-X+X^2)^{77}$ o współczynnikach całkowitych. Która z liczb f_{20} czy h_{20} jest większa? (Współczynnik stojący przy X^j w danym wielomianie $a(X)$ wygodnie jest oznaczać symbolem a_j.)

ZADANIE 3.A3 Dane są liczby naturalne $k_1<k_2<\cdots<k_m$. Niech $N=2^{k_1}+2^{k_2}+\cdots+2^{k_m}$. Wyznaczyć liczbę nieparzystych współczynników wielomianu $f(X)=(1+X)^N$.

ZADANIE 3.A4 Liczby a, $b\in\mathbb{R}$ są różne. Wyznaczyć współczynnik f_{17} w wielomianie:
(1) $f(X)=\sum_{j=0}^{100}(a+X)^{100-j}(b+X)^j=(a+X)^{100}+(a+X)^{99}(b+X)+\ldots+(b+X)^{100}$;
(2) $f(X)=\sum_{k=1}^{N}k(1+X)^k=(1+X)+2(1+X)^2+\ldots+N(1+X)^N$.

ZADANIE 3.A5 Udowodnić tożsamość

$$(x+1)(x^2+1)(x^{2^2}+1)\cdot\ldots\cdot(x^{2^{n-1}}+1) = x^{2^n-1}+\ldots+x^2+x+1.$$

ZADANIE 3.A6 Wyznaczyć wielomian (tzn., jego współczynniki) dany przez

$$f(X) = (X^2-X+1)(X^4-X^2+1)(X^8-X^4+1)\cdot\ldots\cdot(X^{2^n}-X^{2^{n-1}}+1).$$

ZADANIE 3.A7 Niech $n\in\mathbb{N}$. Obliczyć sumę $S(n) = \binom{n}{0}^2 - \binom{n}{1}^2 + \binom{n}{2}^2 - \ldots + (-1)^n\binom{n}{n}^2$.

B. Zadania z arytmetyką liczb całkowitych w tle

ZADANIE 3.B1 Liczba trzycyfrowa $(abc)_{10}$ jest liczbą pierwszą. Udowodnić, że liczba b^2-4ac nie jest kwadratem (liczby całkowitej).

ZADANIE 3.B2 Udowodnić, że jeżeli wielomian $f(X)\in\mathbb{Z}[X]$ przyjmuje wartość 1 dla czterech argumentów całkowitych, to $f(x)\neq -1$ dla każdego $x\in\mathbb{Z}$.

ZADANIE 3.B3 Uzasadnić, że jeżeli $f(X)\in\mathbb{Z}[X]$ i $f(20)f(13) = 2013$, to $f(X)$ nie ma pierwiastków całkowitych.

ZADANIE 3.B4 Udowodnić, że jeżeli $f(X)\in\mathbb{Z}[X]$ i $|f(a)| = |f(b)| = |f(c)| = 1$ dla liczb całkowitych $a<b<c$, to $f(X)$ nie ma pierwiastków całkowitych.

ZADANIE 3.B5 Udowodnić, że jeżeli $f(X)\in\mathbb{Z}[X]$ i $f(c_i)$ jest liczbą podzielną przez daną liczbę naturalną m dla pewnych m kolejnych liczb całkowitych $c_1, c_2, \ldots, c_m$, to wartości $f(x)$, dla wszystkich $x\in\mathbb{Z}$, są podzielne przez m.

ZADANIE 3.B6 Dany jest niestały wielomian $f(X)\in\mathbb{Z}[X]$. Udowodnić, że istnieje co najmniej jedna liczba naturalna m, dla której wartość $f(m)$ nie jest potęgą liczby 2 o wykładniku całkowitym.

ZADANIE 3.B7 Dane są liczby całkowite a, b, c. Udowodnić, że istnieje taka liczba naturalna n, że liczba $f(n) := n^3+an^2+bn+c$ nie jest kwadratem liczby całkowitej.

ZADANIE 3.B8 Ciąg (a_k) o wyrazach całkowitych spełnia warunki: (1) $(k-l)|(a_k-a_l)$ dla dowolnych liczb naturalnych k, l, (2) istnieje taki wielomian $f(X)\in\mathbb{Z}[X]$, że $|a_k|\leqslant|f(k)|$ dla każdego $k\in\mathbb{N}$. Dowieść, że istnieje taki wielomian $g(X)\in\mathbb{R}[X]$, że $a_m = g(m)$ dla każdego $m\in\mathbb{N}$.

ZADANIE 3.B9 Wielomian $f(X)\in\mathbb{Z}[X]$ spełnia warunek $f(m)>m$ dla każdej liczby naturalnej m. Definiujemy ciąg (a_n) indukcyjnie: $a_1 = 1$ i $a_{n+1} = f(a_n)$ dla każdego $n\in\mathbb{N}$. Załóżmy, że dla każdej liczby $d\in\mathbb{N}$ istnieje taki indeks n, że $d|a_n$. Udowodnić, że $f(X) = 1+X$.

ZADANIE 3.B10 Wielomian $f(X) = X^2+aX+b\in\mathbb{Z}[X]$ spełnia warunek: dla każdej liczby pierwszej p istnieje taka liczba całkowita k, że $p|f(k)$ i $p|f(k+1)$. Udowodnić, że istnieje taka liczba $m\in\mathbb{Z}$, że $f(m) = f(m+1) = 0$.

C. Wielomiany przyjmujące na $\mathbb{Z}$ wartości całkowite

ZADANIE 3.C1 Wielomian n-tego stopnia $\binom{X}{n}\in\mathbb{Q}[X]$ zdefiniowany jest, dla $n\in\mathbb{N}$, wzorem

$$\binom{X}{n} := \frac{1}{n!}X(X-1)\cdot\ldots\cdot(X-n+1). \tag{3.72}$$

Ponadto kładziemy $\binom{X}{0} = 1$. Udowodnić, że:

(1) Wartość $\binom{x}{n}$ jest liczbą całkowitą dla każdego $x\in\mathbb{Z}$;

(2) W pierścieniu $\mathbb{Q}[X]$ zachodzi, dla każdego $n\in\mathbb{N}$, równość:

$$\binom{X+1}{n} = \binom{X}{n} + \binom{X}{n-1}; \tag{3.73}$$

(3) Jeżeli $f(X) \in \mathbb{K}[X]$ (gdzie $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ lub $\mathbb{C}$) jest wielomianem stopnia n, to istnieją takie jednoznacznie wyznaczone elementy $\alpha_0, \alpha_1, \ldots, \alpha_n \in \mathbb{K}$, że

$$f(X) = \alpha_0 + \alpha_1 \binom{X}{1} + \ldots + \alpha_n \binom{X}{n}. \tag{3.74}$$

ZADANIE 3.C2 Dany jest wielomian $f(X) \in \mathbb{C}[X]$. Udowodnić: **(1)** Jeżeli $f(a) \in \mathbb{Z}$ dla wszystkich $a \in \mathbb{Z}$, to (istniejące i jednoznacznie wyznaczone na mocy Z3.C1(3)) liczby $\alpha_0, \ldots, \alpha_n$ są liczbami całkowitymi; **(2)** Jeżeli $\deg f(X) = n$ i $f(a), f(a+1), \ldots, f(a+n)$ są liczbami całkowitymi dla pewnego $a \in \mathbb{Z}$, to $f(x) \in \mathbb{Z}$ dla każdego $x \in \mathbb{Z}$.

ZADANIE 3.C3 Udowodnić, że jeżeli $f(X) \in \mathbb{Z}[X]$ jest wielomianem pierwotnym stopnia n, to największy wspólny dzielnik wszystkich liczb $f(k)$, przy $k \in \mathbb{Z}$, jest dzielnikiem liczby $n!$.

ZADANIE 3.C4 Udowodnić tożsamość (2.36).

D. Wielomiany przyjmujące wartości danego typu

ZADANIE 3.D1 Trójmian kwadratowy $f(X) = X^2 + pX + q$ dla dwóch kolejnych liczb całkowitych przyjmuje wartości będące kwadratami kolejnych liczb całkowitych. Udowodnić, że $f(x)$ jest kwadratem (liczby całkowitej) dla każdego $x \in \mathbb{Z}$.

ZADANIE 3.D2 Dany jest trójmian kwadratowy $f(X) = aX^2 + bX + c$. Udowodnić, że jeżeli dla każdej liczby całkowitej x liczba $f(x)$ jest kwadratem liczby całkowitej, to istnieją takie liczby r, d, że dla każdego x zachodzi równość $f(x) = (rx + d)^2$.

ZADANIE 3.D3 Udowodnić, że jeżeli wielomian $f(X) = aX^2 + bX + c \in \mathbb{Z}[X]$ ma taką własność, że $f(x)$ jest czwartą potęgą liczby całkowitej dla każdej liczby całkowitej x, to $a = b = 0$.

ZADANIE 3.D4 Niech $f(X) \in \mathbb{R}[X]$. Udowodnić, że jeżeli zbiór $\mathcal{A}(f) := \{k \in \mathbb{Z} : f(k) \notin \mathbb{Z}\}$ jest niepusty, to jest zbiorem nieskończonym.

ZADANIE 3.D5 Dowieść, że jeżeli dla wielomianu $f(X) \in \mathbb{R}[X]$ stopnia n, liczby $f(k^2)$ są całkowite dla $k = 0, 1, \ldots, n$, to $f(x^2) \in \mathbb{Z}$ dla każdego $x \in \mathbb{Z}$. Ale może się zdarzyć, że $f(y) \notin \mathbb{Z}$ dla pewnego $y \in \mathbb{Z}$.

ZADANIE 3.D6 Wyznaczyć wszystkie takie wielomiany $f(X) \in \mathbb{Z}[X]$, że każda liczba całkowita y jest wartością $f(x)$ dla pewnego $x \in \mathbb{Z}$.

E. Pierwiastki wielomianów

ZADANIE 3.E1 Jeżeli $f(X) = aX^3 + bX^2 + cX + d \in \mathbb{Z}[X]$, przy czym $bc \in 2\mathbb{Z}$ oraz $ad \notin 2\mathbb{Z}$, to nie wszystkie pierwiastki wielomianu $f(X)$ są liczbami wymiernymi.

ZADANIE 3.E2 Dowieść, że jeżeli $c, d \in \mathbb{Z}$ i $c \neq 0$, to równanie $x^3 - 3cx^2 - dx + c = 0$ ma nie więcej niż jeden pierwiastek wymierny.

ZADANIE 3.E3 Wyznaczyć wszystkie takie liczby wymierne c, dla których trójmian kwadratowy $cX^2 + (2c+1)X + 2c - 1$ ma oba pierwiastki będące liczbami całkowitymi.

ZADANIE 3.E4 Udowodnić, że wielomian $\sum_{j=0}^{n} a_j X^j \in \mathbb{R}[X]$, w którym $a_n = 1$, $a_{n-1} = a_{n-2} = 0$ i $a_0 \neq 0$, ma co najwyżej $n - 1$ pierwiastków rzeczywistych.

ZADANIE 3.E5 Udowodnić, że jeżeli wielomian $f(X) = X^3 + aX^2 + bX + c \in \mathbb{R}[X]$ ma trzy (parami) różne pierwiastki rzeczywiste, to wielomian $g(X) = 8X^3 + 8aX^2 + 2(a^2 + b)X + ab - c$ również ma trzy (parami) różne pierwiastki rzeczywiste.

ZADANIE 3.E6 Niech α, β będą (dwoma z czterech) pierwiastkami wielomianu $X^4 + X^3 - 1$. Udowodnić, że $\alpha\beta$ jest pierwiastkiem wielomianu $X^6 + X^4 + X^3 - X^2 - 1$.

ZADANIE 3.E7 Udowodnić, że jeżeli jeden z trzech pierwiastków wielomianu $aX^3 + bX + c \in \mathbb{Q}[X]$ jest iloczynem dwóch pozostałych pierwiastków, to jest on liczbą wymierną.

ZADANIE 3.E8 Wielomian $f(X) = X^n - X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_2X^2 - n^2X + 1 \in \mathbb{R}[X]$ ma n $(n \geqslant 4)$ dodatnich pierwiastków. Wykazać, że wszystkie one są równe.

ZADANIE 3.E9 Wskazać warunki konieczne i dostateczne, jakie powinien spełniać wielomian $X^3 + aX^2 + bX + c \in \mathbb{R}[X]$, by mieć trzy pierwiastki rzeczywiste tworzące ciąg arytmetyczny.

ZADANIE 3.E10 Wielomian postaci $c_0+c_1X+\cdots+c_nX^n$, gdzie każda z liczb $c_0, c_1, \ldots, c_n$ jest równa 1 lub -1, nazwiemy (±1)-*wielomianem*. Wyznaczyć wszystkie (±1)-wielomiany mające same pierwiastki rzeczywiste (tzn. takie, których wszystkie pierwiastki w $\mathbb{C}$ mają zerowe części urojone).

ZADANIE 3.E11 Uzasadnić, że istnieje taki nieskończony ciąg $(a_k)_{k\geqslant0}$ o wyrazach rzeczywistych, że dla każdego $n \geqslant 1$ wielomian $a_0+a_1X+\cdots+a_nX^n$ ma dokładnie n r ó ż n y c h pierwiastków rzeczywistych.

ZADANIE 3.E12 Dany jest taki wielomian unormowany $f(X) \in \mathbb{R}[X]$, że $|f(i)| < 1$ $(i = \sqrt{-1})$. Udowodnić, że istnieje taki pierwiastek zespolony $b + ci$ wielomianu $f(X)$, że zachodzi nierówność $(b^2 + c^2 + 1)^2 - 4b^2 < 1$.

ZADANIE 3.E13 Niech $r(X) = X^n - (r_{n-1}X^{n-1} + \cdots + r_1X + r_0) \in \mathbb{R}[X]$, gdzie $r_j \geqslant 0$ dla $j = 0, \ldots, n-1$. Udowodnić, że wielomian $r(X)$ ma dokładnie jeden pierwiastek nieujemny ϱ_0. Ponadto, gdy $r(X) \neq X^n$ (czyli gdy co najmniej jeden współczynnik $r_0, \ldots, r_{n-1}$ jest różny od 0), to $\varrho_0 > 0$ oraz $r(x) < 0$ dla $x \in (0; \varrho_0)$ i $r(x) > 0$ dla $x \in (\varrho_0; \infty)$.

ZADANIE 3.E14 Niech $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ będzie wielomianem unormowanym o współczynnikach zespolonych. Niech $r(X) = X^n - |a_{n-1}|X^{n-1} - \cdots - |a_1|X - |a_0|$ będzie tzw. **wielomianem Pólya'*i*** wielomianu $f(X)$. Udowodnić, że dla dowolnego pierwiastka λ wielomianu $f(X)$ zachodzi nierówność podwójna: $|\lambda| \leqslant \varrho_0 \leqslant 2\max\{\sqrt[k]{|a_{n-k}|} : k = 1, \ldots, n\}$, gdzie ϱ_0 oznacza (jedyny) nieujemny pierwiastek wielomianu $r(X)$ (zobacz poprzednie zadanie).

ZADANIE 3.E15 Dla danego wielomianu $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}[X]$ stopnia n oznaczmy $M = \max\{|a_j|/|a_n| : j = 0, \ldots, n-1\}$. Niech $\lambda \in \mathbb{C}$ będzie dowolnym pierwiastkiem wielomianu $f(X)$. Udowodnić, że

(1) $|\lambda| \leqslant 1 + M$;

(2) jeżeli $a_j \geqslant 0$ dla wszystkich j oraz $\operatorname{Re}\lambda \geqslant 0$, to $|\lambda| \leqslant \dfrac{1+\sqrt{1+4M}}{2}$.

F. Pierwiastki wspólne

ZADANIE 3.F1 Udowodnić, że jeżeli trójmiany kwadratowe $f_i(X) = X^2 + a_iX + b_i \in \mathbb{Z}[X]$, dla $i = 1, 2$, mają wspólny pierwiastek nie będący liczbą całkowitą, to $a_1 = a_2$ i $b_1 = b_2$.

ZADANIE 3.F2 Dowieść, że $\alpha \in \mathbb{K}$ jest wspólnym pierwiastkiem wielomianów $f(X), g(X) \in \mathbb{K}[X]$ wtedy i tylko wtedy, gdy α jest pierwiastkiem wielomianu $\operatorname{NWD}(f, g)$.

ZADANIE 3.F3 Dla danych dwóch unormowanych trójmianów kwadratowych o współczynnikach rzeczywistych $f_1(X) = X^2 + a_1X + b_1$ i $f_2(X) = X^2 + a_2X + b_2$ oznaczmy

$$R(f_1, f_2) := (b_2 - b_1)^2 + (a_1 - a_2)(a_1b_2 - a_2b_1). \tag{3.75}$$

Udowodnić, że **(1)** Trójmiany f_1, f_2 mają wspólny pierwiastek (być może zespolony) wtedy i tylko wtedy, gdy $R(f_1, f_2) = 0$; **(2)** Jeżeli $R(f_1, f_2) < 0$, to oba trójmiany mają pierwiastki rzeczywiste i to takie, że między dwoma pierwiastkami jednego z nich leży pierwiastek drugiego).

ZADANIE 3.F4 Liczba $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ jest wspólnym pierwiastkiem wielomianów trzeciego stopnia $f(X), g(X) \in \mathbb{Q}[X]$. Dowieść, że wielomiany $f(X), g(X)$ mają wspólny pierwiastek $\beta \neq \alpha$.

ZADANIE 3.F5 Dana jest liczba całkowita c. Udowodnić, że $\sqrt[3]{c}$ jest pierwiastkiem trójmianu kwadratowego o współczynnikach całkowitych wtedy i tylko wtedy, gdy $c = k^3$ dla pewnego $k \in \mathbb{Z}$.

G. Zastosowanie wzorów Viète'a

ZADANIE 3.G0 Jeżeli $X^3+aX^2+bX+c\in\mathbb{R}[X]$ ma trzy pierwiastki rzeczywiste, to $a^2\geqslant 3b$.

ZADANIE 3.G1 Dowieść, że jeżeli wielomian $f(X)=aX^3-aX^2+bX+b\in\mathbb{R}[X]$ ma dokładnie trzy różne pierwiastki α, β, γ, to zachodzi równość $\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}+\frac{1}{\alpha+\beta+\gamma}=0$.

ZADANIE 3.G2 Dana jest liczba $m\in\mathbb{N}$. Udowodnić, że jeżeli liczby całkowite a, b, c, d spełniają warunki $m|a+b+c+d$ i $m|a^2+b^2+c^2+d^2$, to $m|a^4+b^4+c^4+d^4+4abcd$.

ZADANIE 3.G3 Jeżeli α, β, $\gamma\in\mathbb{R}_{\geqslant 0}$ i $\alpha+\beta+\gamma=1$, to $0\leqslant\alpha\beta+\beta\gamma+\gamma\alpha-2\alpha\beta\gamma\leqslant\frac{7}{27}$.

ZADANIE 3.G4 Wyznaczyć wszystkie takie pary liczb naturalnych (a,b), że $a|b^2+1$ i $b|a^2+1$.

ZADANIE 3.G5 Niezerowe liczby całkowite a, b, c są takie, że $\frac{a}{b}+\frac{b}{c}+\frac{c}{a}$ oraz $\frac{a}{c}+\frac{c}{b}+\frac{b}{a}$ są liczbami całkowitymi. Udowodnić, że $|a|=|b|=|c|$.

ZADANIE 3.G6 Liczby α, β, $\gamma\in\mathbb{R}_{\neq 0}$ spełniają warunki $\alpha+\beta+\gamma\neq 0$ i $\frac{1}{\alpha+\beta+\gamma}=\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}$. Udowodnić, że $(\alpha^{2017}+\beta^{2017}+\gamma^{2017})^{-1}=\alpha^{-2017}+\beta^{-2017}+\gamma^{-2017}$.

ZADANIE 3.G7 Rozwiązać układ równań

$$\begin{cases} x_1+x_2+\ldots+x_n=n,\\ x_1^2+x_2^2+\ldots+x_n^2=n,\\ \qquad\ldots\ldots\ldots\\ x_1^n+x_2^n+\ldots+x_n^n=n. \end{cases}$$

ZADANIE 3.G8 Udowodnić, że jeżeli liczby n a t u r a l n e a, b są takie, że $(ab-1)|(a^2+b^2)$, to iloraz $(a^2+b^2)/(ab-1)$ jest równy 5.

H. Wielkość wielomianów

ZADANIE 3.H1 Wielomian $f(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_1X+1$ o nieujemnych współczynnikach ma n pierwiastków rzeczywistych. Udowodnić, że $f(2)\geqslant 3^n$.

ZADANIE 3.H2 Niech $f(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0\in\mathbb{R}[X]$ i niech $s_0<s_1<\cdots<s_n$ będą liczbami całkowitymi. Dowieść, że $|f(s_k)|\geqslant n!/2^n$ dla pewnego $0\leqslant k\leqslant n$.

ZADANIE 3.H3 Wielomian $f(X)\in\mathbb{R}[X]$ ma stopień $2n$. Ponadto $|f(a)|\leqslant 1$ dla każdej liczby całkowitej $a\in[-n;\,n]$. Udowodnić, że dla każdego $x\in[-n;\,n]$ zachodzi nierówność $|f(x)|\leqslant 2^{2n}$.

ZADANIE 3.H4 Liczby a, b, $c\in\mathbb{R}$ są takie, że $|ax^2+bx+c|\leqslant 1$ dla wszystkich $|x|\leqslant 1$. Udowodnić, że wówczas $|cx^2+bx+a|\leqslant 2$ dla wszystkich $|x|\leqslant 1$.

ZADANIE 3.H5 Dowieść, że istnieje taki wielomian $f(X)\in\mathbb{Z}[X]$ (o współczynnikach całkowitych!), że dla każdego $x\in[1/10;\,9/10]$ zachodzi nierówność $|f(x)-\frac{1}{2}|<10^{-3}$.

I. Podzielność wielomianów

ZADANIE 3.I1 Dowieść, że $X^2+X+1|(X+1)^{2n+1}+X^{n+2}$ dla każdej $n\in\mathbb{N}$.

ZADANIE 3.I2 Udowodnić, że wielomian $X^2-2(\cos\varphi)X+1$ jest w pierścieniu $\mathbb{R}[X]$ dzielnikiem wielomianu $(\sin\varphi)X^n-(\sin n\varphi)X+\sin(n-1)\varphi$ przy dowolnych $\varphi\notin\mathbb{Z}\pi$ i $n\geqslant 2$.

ZADANIE 3.I3 Udowodnić, że dla dowolnych n, $k\in\mathbb{N}$ wielomian $(X-1)(X^2-1)\cdot\ldots\cdot(X^k-1)$ jest dzielnikiem wielomianu $(X^{n+1}-1)(X^{n+2}-1)\cdot\ldots\cdot(X^{n+k}-1)$ w pierścieniu $\mathbb{Q}[X]$.

ZADANIE 3.I4 Dla jakich k, $n\in\mathbb{N}$ zachodzi $1+X+X^2+\cdots+X^k|1+X^n+X^{2n}+\cdots+X^{kn}$?

ZADANIE 3.I5 Wyznaczyć wszystkie wielomiany stopnia 2 należące do $\mathbb{Z}[X]$ i będące dzielnikami (w $\mathbb{Z}[X]$) (± 1)-wielomianów (zobacz Z3.E10).

J. Wielomiany nierozkładalne

ZADANIE 3.J1 Niech $f(X) = (X-a_1)^2(X-a_2)^2\cdot\ldots\cdot(X-a_n)^2+1 \in \mathbb{Z}[X]$ dla parami różnych liczb całkowitych $a_1, \ldots, a_n$. Udowodnić, że wielomian $f(X)$ jest nierozkładalny w $\mathbb{Q}[X]$.

ZADANIE 3.J2 (1) Niech $f(X) = (X-a_1)(X-a_2)\cdot\ldots\cdot(X-a_n)+1 \in \mathbb{Z}[X]$ dla parami różnych liczb całkowitych $a_1, \ldots, a_n$. Udowodnić, że jeżeli $n \neq 2, 4$, to $f(X)$ jest nierozkładalny w $\mathbb{Q}[X]$; **(2)** Dla jakich $a, b \in \mathbb{Z}$ wielomian $(X-a)(X-b)+1$ jest rozkładalny w $\mathbb{Q}[X]$?; **(3)** Wyznaczyć takie $a, b, c, d \in \mathbb{Z}$, że $(X-a)(X-b)(X-c)(X-d)+1$ jest rozkładalny w $\mathbb{Q}[X]$.

ZADANIE 3.J3 Niech $f(X) \in \mathbb{Z}[X]$, $\deg f(X) = 2n+1$. Załóżmy, że $|f(c_j)| \in \{1\} \cup \mathbb{P}$ dla pewnych liczb całkowitych $c_1 < c_2 < \cdots < c_{2n+1}$. Dowieść, że $f(X)$ jest nierozkładalny w $\mathbb{Q}[X]$.

ZADANIE 3.J4 Niech $f(X) \in \mathbb{Z}[X]$ będzie wielomianem unormowanym stopnia $n \geqslant 5$. Udowodnić, że jeżeli $|f(c_j)| = 1$ dla pewnych liczb całkowitych $c_1 < c_2 < \cdots < c_n$, to $f(X)$ jest nierozkładalny w $\mathbb{Q}[X]$.

ZADANIE 3.J5 Niech $n \in \mathbb{N}$. Udowodnić, że wielomian $X^{2^n}+1$ jest nierozkładalny w $\mathbb{Q}[X]$.

ZADANIE 3.J6 Niech $p \in \mathbb{P}_{>2}$. Udowodnić, że $X^p+pX^{p-1}+p+1$ jest nierozkładalny w $\mathbb{Q}[X]$.

ZADANIE 3.J7 Udowodnić nierozkładalność wielomianu $X^4+2X^3+3X^2+4X+5$ w $\mathbb{Q}[X]$.

ZADANIE 3.J8 Udowodnić, że wielomin X^n+4 jest nierozkładalny w $\mathbb{Q}[X]$ (równoważnie, w $\mathbb{Z}[X]$) wtedy i tylko wtedy, gdy wykładnik n nie jest podzielny przez 4.

ZADANIE 3.J9 Niech $p(X) \in \mathbb{Z}[X]$ będzie takim unormowanym wielomianem nierozkładalnym w $\mathbb{Q}[X]$, że $|p(0)|$ nie jest kwadratem. Udowodnić, że złożenie (superpozycja) $f(X) = p(X^2)$ również jest wielomianem nierozkładalnym w $\mathbb{Q}[X]$.

ZADANIE 3.J10 Udowodnić, że wielomian $5X^5+2X^4+4X^3+2X^2+8X+7$ jest nierozkładalny w $\mathbb{Q}[X]$. U w a g a. Liczba 524 287 jest liczbą pierwszą[5].

ZADANIE 3.J11 Dane są liczby całkowite $k_1 < k_2 < \cdots < k_{2n}$. Dowieść, że istnieje nieskończenie wiele takich liczb pierwszych p, że wielomian $f(X) = (X-k_1)(X-k_2)\cdot\ldots\cdot(X-k_{2n})+p$ jest nierozkładalny w pierścieniu $\mathbb{Z}[X]$.

ZADANIE 3.J12 Dowieść, że wielomianu X^7Y^7+1 nie da się przedstawić w postaci $f(X)g(Y)$.

ZADANIE 3.J13 Zbadać rozkładalność wielomianu $X_1^2+X_2^2+\cdots+X_n^2 \in \mathbb{K}[X_1, X_2, \ldots, X_n]$.

K. Rozkładanie na czynniki

ZADANIE 3.K1 Rozłożyć wielomian X^8+X^4+1 na iloczyn czynników nierozkładalnych w pierścieniach $\mathbb{Q}[X]$, $\mathbb{R}[X]$ i $\mathbb{C}[X]$.

ZADANIE 3.K2 Rozłożyć podobnie jak wyżej wielomian X^5+X+1.

ZADANIE 3.K3 Rozłożyć wielomian $f(X) = X^{2n}+X^{2n-2}+\cdots+X^2+1$ na iloczyn czynników nierozkładalnych w pierścieniach $\mathbb{R}[X]$ i $\mathbb{C}[X]$.

ZADANIE 3.K4 Rozłożyć podobnie jak wyżej wielomian $f(X) = X^{2n}+X^n+1$.

ZADANIE 3.K5 Rozłożyć na czynniki nierozkładalne w pierścieniu $\mathbb{Z}[X, Y]$:

(1) $(X+Y)^3-X^3-Y^3$;
(2) $(X+Y)^5-X^5-Y^5$;
(3) $(X+Y)^7-X^7-Y^7$.

ZADANIE 3.K6 Liczby całkowite a, b, c są parami różne, a $n \in \mathbb{N}$. Udowodnić, że

$$\frac{a^n}{(a-b)(a-c)}+\frac{b^n}{(b-a)(b-c)}+\frac{c^n}{(c-a)(c-b)} \in \mathbb{Z}.$$

[5]jest to liczba M_{19}, której pierwszość została udowodniona przez Cataldi'*ego* w 1588 roku

L. Superpozycje

ZADANIE 3.L1 Załóżmy, że trójmian kwadratowy $f(X) \in \mathbb{R}[X]$ jest taki, że $f(x) \neq x$ dla każdego $x \in \mathbb{R}$. Udowodnić, że wtedy również $f(f(x)) \neq x$ dla każdego $x \in \mathbb{R}$.

ZADANIE 3.L2 Dla danego wielomianu $f(X) \in \mathcal{R}[X]$ i liczby $n \in \mathbb{Z}_{\geqslant 0}$ definiujemy (indukcyjnie) **iteracje** $f^{[n]}(X)$ wielomianu $f(X)$. Mianowicie: $f^{[n+1]}(X) = f(f^{[n]}(X))$ oraz $f^{[0]}(X) = X$. Udowodnić, że $f(X) - X | f^{[n]}(X) - X$ dla dowolnego wielomianu $f(X) \in \mathcal{R}[X]$ i dowolnej $n \in \mathbb{N}$.

ZADANIE 3.L3 Dla danego wielomianu $f(X) \in \mathbb{Z}[X]$ i liczby całkowitej a zachodzi równość $f^{[k]}(a) = a$ przy pewnym $k \in \mathbb{N}$. Udowodnić, że wówczas $f^{[2]}(a) = a$.

ZADANIE 3.L4 Wielomian $f(X) \in \mathbb{Z}[X]$ ma stopień $n \geqslant 2$. Udowodnić, że dla danego $k \in \mathbb{N}$ istnieje co najwyżej n liczb całkowitych a, dla których zachodzi równość $f^{[k]}(a) = a$.

ZADANIE 3.L5 Dane są takie wielomiany u n o r m o w a n e $f(X), g(X) \in \mathbb{K}[X]$, że zachodzi równość $f^{[2]}(X) = g^{[2]}(X)$. Udowodnić, że $f(X) = g(X)$.

ZADANIE 3.L6 Wielomian $f(X) \in \mathbb{R}[X]$ jest taki, że $f(\sin x) = f(\cos x)$ dla każdej liczby rzeczywistej x. Udowodnić, że $f(X) = l(X^4 - X^2)$ dla pewnego wielomianu $l(X) \in \mathbb{R}[X]$.

ZADANIE 3.L7 Dany jest wielomian: $f(X) = X^2 - 2 \in \mathbb{R}[X]$. Udowodnić, że dla każdego n wszystkie pierwiastki wielomianu $f^{[n]}(X)$ są rzeczywiste i różne.

ZADANIE 3.L8 Udowodnić, że n i e da się znaleźć takich trzech trójmianów kwadratowych $f(X)$, $g(X)$, $h(X) \in \mathbb{R}[X]$, żeby wielomian $f(g(h(X)))$ miał osiem pierwiastków $1, 2, \ldots, 8$.

M. Wielomiany jako funkcje rzeczywiste

ZADANIE 3.M1 Udowodnić, że każda funkcja wielomianowa $\mathbb{R} \ni x \longmapsto f(x) \in \mathbb{R}$ jest różnicą dwóch funkcji wielomianowych rosnących.

ZADANIE 3.M2 Niech $f(X) \in \mathbb{R}[X]$. Załóżmy, że dla wszystkich $x \in \mathbb{R}_{\geqslant 0}$ zachodzi nierówność $f(x) \geqslant 0$. Dowieść, że $f(X) = a(X)^2 + Xb(X)^2$ dla pewnych wielomianów $a(X), b(X) \in \mathbb{R}[X]$.

ZADANIE 3.M3 Czy istnieje taki wielomian $f(X, Y) \in \mathbb{R}[X, Y]$, że **zbiór wartości**:

$$f(\mathbb{R} \times \mathbb{R}) := \{f(x, y) : (x, y) \in \mathbb{R} \times \mathbb{R}\}$$

jest równy przedziałowi (nieskończonemu) $(0; \infty)$?

N. Wielomiany jako funkcje tworzące

ZADANIE 3.N1 Niech $(k_1, k_2, \ldots, k_n)$ i $(l_1, l_2, \ldots, l_n)$ będą dwoma r ó ż n y m i ciągami o wyrazach ze zbioru $\mathbb{N}$. Oznaczmy przez $\mathcal{A}$ zbiór $\{(i, j) : 1 \leqslant i < j \leqslant n\}$ i zdefiniujmy dwie funkcje $\varphi, \psi : [n] \times [n] \longrightarrow \mathbb{N}$ przez $\varphi(i, j) = k_i + k_j$, $\psi(i, j) = l_i + l_j$. Załóżmy, że istnieje taka bijekcja $b : \mathcal{A} \longrightarrow \mathcal{A}$, że zachodzi równość $\varphi = \psi \circ b$. Udowodnić, że n jest potęgą 2^s dla pewnego $s \in \mathbb{N}$.

3.6.2 Wskazówki/rozwiązania

Stopień szczegółowości poniższych wskazówek/rozwiązań jest dość różny. Niektóre są bardzo szczegółowe (dwa sposoby rozumowania, dodatkowe uwagi, uogólnienia, itp.). Inne są bardziej lakoniczne. Czasami wskazówki brak. To może, ale nie musi oznaczać, że zadanie jest łatwe.

Z3.A1 (1) Wystarczy, oczywiście obliczyć: $f(1) = (1 - 1 + 1^2)^5 = 1$. **(2)** Ponieważ $a_0 = f(0)$ (jak zawsze), więc w naszym przypadku $a_0 = 1$. Również łatwo widzieć, że $a_{10} = 1$. Oraz $3^5 = f(-1) = a_0 - a_1 + a_2 - \ldots - a_9 + a_{10}$. Stąd $a_1 - a_2 + \cdots + a_9 = 2 - 3^5$.

Z3.A2 Rozważ jeszcze dwa wielomiany: $\widetilde{f}(X) = f(-X)$ i $\widetilde{h}(X) = g(-X)$. Ponieważ $(-X)^{2k} = X^{2k}$ więc jest jasne, że zachodzą równości $f_{20} = \widetilde{f}_{20}$ i $h_{20} = \widetilde{h}_{20}$. Łatwo porównać liczby $\widetilde{f}_{20}$ i $\widetilde{h}_{20}$.

Z3.A3 Wiemy z C2.50, że wszystkie, z wyjątkiem wiodącego i zerowego, współczynniki wielomianu $(1+X)^{2^k}$ są parzyste. Zatem w wielomianie $(1+X)^N = (1+X)^{k_1}(1+X)^{k_2}\cdot\ldots\cdot(1+X)^{k_m}$ nieparzyste mogą być tylko współczynniki przy iloczynie jedynek i przy iloczynach postaci $X^{2^{k_{s_1}}}\cdot\ldots\cdot X^{2^{k_{s_j}}}$. Takich iloczynów jest tyle ile podzbiorów ma zbiór $\{k_1, k_2, \ldots, k_m\}$, czyli 2^m. Trzeba jeszcze sprawdzić, że jednomiany $X^{2^{k_{s_1}}}\cdot\ldots\cdot X^{2^{k_{s_j}}}$ są parami różne, co jest równoważne faktowi jednoznaczności zapisu liczb naturalnych w systemie dwójkowym (systemie pozycyjnym o podstawie 2).

Z3.A4 (1) Patrz ogólnie: $f(X) = \sum_{j=0}^{N}(a+X)^{N-j}(b+X)^j$. Pomnóż ten wielomian przez $(X+a)-(X+b)$ i skorzystaj z tożsamości nieśmiertelnej (1.8). Dostaniesz równość $(a-b)f(X) = (X+a)^{N+1} - (X+b)^{N+1}$. Stąd równość $f_k = (a-b)^{-1}\binom{N+1}{k}(a^{N+1-k} - b^{N+1-k})$. **(2)** Zobacz 3.4.11 P2.

Z3.A5 S p o s ó b 1. Oczywista indukcja względem n. Oznaczmy przez $\mathcal{A}_n$ zbiór wszystkich liczb całkowitych z przedziału $[\,0;\,2^n\,]$. Potrzebny w dowodzie tożsamości krok indukcyjny jest dokładnie równoważny równości: $\mathcal{A}_n \sqcup (\mathcal{A}_n + 2^{n+1}) = \mathcal{A}_{n+1}$, a ta równość jest w gruncie rzeczy tylko innym sposobem powiedzenia, że liczby całkowite nieujemne mają dokładnie jedno przedstawienie w systemie dwójkowym. U w a g a. Oznaczenie $\mathcal{A}+x$ wprowadziliśmy w rozwiązaniu zadania Z1.4.

S p o s ó b 2. Pomnóż wielomian $f(X) = (X+1)(X^2+1)(X^{2^2}+1)\cdot\ldots\cdot(X^{2^{n-1}}+1)$ przez wielomian $X-1$. Dzięki oczywistej indukcji dostaniesz równość $(X-1)f(X) = X^{2^n}-1$. Porównaj tę równość z tożsamością nieśmiertelną $(X-1)(X^{2^n-1}+X^{2^n-2}+\cdots+X+1) = X^{2^n}-1$. I wykorzystaj istnienie i j e d n o z n a c z n o ś ć ilorazu, zobacz T3.3.

Z3.A6 Sztuka polega tu na tym, że łatwo wyznaczyć iloczyn $(X^2+X+1)f(X)$. Mamy bowiem $(X^{2k}+X^k+1)(X^{2k}-X^k+1) = X^{4k}+X^{2k}+1$ dla każdego $k\in\mathbb{N}$. Przez oczywistą indukcję dostajemy stąd równość $(X^2+X+1)f(X) = X^{2^{n+1}}+X^{2^n}+1$. Dla wyznaczenia wielomianu $f(X)$ trzeba więc podzielić $X^{2^{n+1}}+X^{2^n}+1$ przez X^2+X+1. Wykładniki 2^{n+1} i 2^n dają reszty 1 i 2 (lub 2 i 1) przy dzieleniu przez 3. Dokładniej, reszty 1 i 2, gdy n jest nieparzysta, a reszty 2 i 1, gdy n jest parzysta (sprawdźcie!). Działamy więc o g ó l n i e j: dzielimy X^a+X^b+1, przy wykładnikach a i b dających reszty 1 i 2 (lub 2 i 1) przy dzieleniu przez 3. Twierdzenie o strażakach daje równość $X^a+X^b+1 = (X^a-\omega^a)+(X^b-\omega^b)$. Korzystając więc z tożsamości nieśmiertelnej, mamy

$$\frac{X^a+X^b+1}{X-\omega} = \sum_{j=0}^{a-1}\omega^{a-1-j}X^j + \sum_{j=0}^{b-1}\omega^{b-1-j}X^j. \qquad (*)$$

Dokładnie tak samo, mamy $X^a+X^b+1 = (X^a-\overline{\omega}^a)+(X^b-\overline{\omega}^b)$, skąd dostaniemy sprzężoną wersję równości $(*)$: wszystko tak samo z zamianą ω na $\overline{\omega}$. Mnożąc oczywistą równość (w $\mathbb{C}(X)$)

$$\frac{1}{X^2+X+1} = \frac{1}{(X-\omega)(X-\overline{\omega})} = \frac{1}{\omega-\overline{\omega}}\cdot\left(\frac{1}{X-\omega}-\frac{1}{X-\overline{\omega}}\right)$$

przez X^a+X^b+1 i korzystając z równości $(*)$, $(\overline{*})$, dostajemy

$$\frac{X^a+X^b+1}{X^2+X+1} = \sum_{j=0}^{a-1}\frac{\omega^{a-1-j}-\overline{\omega}^{a-1-j}}{\omega-\overline{\omega}}X^j + \sum_{j=0}^{b-1}\frac{\omega^{b-1-j}-\overline{\omega}^{b-1-j}}{\omega-\overline{\omega}}X^j.$$

Czytelnik może zechcieć dalej upraszczać: zapisać uzyskany wielomian w postaci jednolitej $\sum_{j\geqslant 0}c_jX^j$, podstawić $a=2^{n+1}$, $b=2^n$, itd.

Z3.A7 Rozważyć wielomian $(1+X)^n(1-X)^n$. Por. P1 z paragrafu 3.1.

Z3.B1 Mamy $(abc)_{10} = 10^2a + 10b + c = f(10)$, gdzie $f(X) = aX^2 + bX + c \in \mathbb{Z}[X]$. Załóżmy, nie wprost, że $\Delta = b^2 - 4ac = k^2$ dla pewnego $k \in \mathbb{Z}_{\geqslant 0}$. Wówczas liczby $\alpha_1 = (-b + k)/2a$, $\alpha_2 = (-b - k)/2a$ są (wymiernymi!) pierwiastkami trójmianu $f(X)$. Zapiszmy rozkład (3.11) dla $X = 10$ w postaci $4a(10^2a + 10b + c) = 4af(10) = 4a^2(10 - \alpha_1)(10 - \alpha_2) = (20a + b - k)(20a + b + k)$. Wobec tego, liczba pierwsza $10^2a + 10b + c$ dzieli co najmniej jeden z czynników z prawej strony. Jest więc niewiększa od większego z nich, zobacz C2.2: $100a + 10b + c \leqslant 20a + b + k$. Czyli $80a + 9b + c \leqslant k = \sqrt{b^2 - aac} \leqslant \sqrt{81} = 9$ (bo $0 \leqslant a, b, c \leqslant 9$). To jest sprzeczne z założeniem $a \geqslant 1$.

Z3.B2 Zobacz rozwiązanie Z3.2. Zauważ, że liczby $2 = 1 - (-1)$ nie da się przedstawić w postaci iloczynu pięciu czynników całkowitych, z których cztery byłyby (parami) różne.

Z3.B3 Ponieważ 2013 jest liczbą nieparzystą, więc jej dzielniki $f(20)$, $f(13)$ są nieparzyste. Jeżeli teraz $a \in 2\mathbb{Z}$, to, ponieważ $20 - a | f(20) - f(a)$, zobacz (3.3), więc $f(a)$ jest liczbą tej samej parzystości co $f(20)$, czyli jest liczbą nieparzystą. Jeżeli zaś $a \in 2\mathbb{Z} + 1$ (jest nieparzysta), to, podzielność $13 - a | f(13) - f(a)$, podobnie jak przed chwilą, pokazuje, że $f(a)$ jest liczbą nieparzystą. Widzimy więc, że wartość $f(a)$, dla wszystkich $a \in \mathbb{Z}$, jest liczbą nieparzystą. Ostatecznie, $f(a) \neq 0$ dla wszystkich $a \in \mathbb{Z}$. Uwaga. Podobnie dowodzimy: *Jeżeli* $f(2)f(0)f(1)f(3) = 2013$, *to* $f(x) \neq 2014$ *dla* $x \in \mathbb{Z}$.

Z3.B4 Załóżmy, nie wprost, że $f(n) = 0$ dla pewnego $n \in \mathbb{Z}$. Wówczas $a - n | f(a) - f(n)$ (zob. C3.4), czyli $a - n | \pm 1$, więc $a - n = \pm 1$. Podobnie, $b - n = \pm 1$ i $c - n = \pm 1$. Przeto $a, b, c \in \{n - 1, n + 1\}$. Ostatecznie $\{a, b, c\} \subseteq \{n - 1, n + 1\}$. Nonsens!

Z3.B5 Dla danej (dowolnej) liczby całkowitej x istnieje (dokładnie jeden) indeks i, dla którego $m | x - c_i$. Jednocześnie $x - c_i | f(x) - f(c_i)$, na mocy (3.3). Więc $m | f(x) - f(c_i)$. Stąd, na mocy Zasady Podstawowej, $m | f(x)$.

Z3.B6 Niech $f(X) = a_0 + a_1X + \cdots + a_nX^n$. Załóżmy, że wszystkie wartości $f(m)$, przy $m \in \mathbb{N}$, są postaci 2^s, gdzie $s \in \mathbb{Z}_{\geqslant 0}$. Pokażemy – na dwa sposoby – że to prowadzi do sprzeczności. Pierwszy sposób będzie arytmetyczny (wykorzystujący głównie podzielność w zbiorze $\mathbb{Z}$), a drugi "wielkościowy" (wykorzystujący głównie relację $\leqslant$ w $\mathbb{Z}$).

Sposób 1. Załóżmy, że $a_0 \neq 0$ i zapiszmy $a_0 = 2^k a_0'$, gdzie $k = v_2(a_0)$, $2 \nmid a_0'$, i rozważmy liczby $f(2^t)$ dla $t > k$. Mamy $f(2^t) = a_0 + a_1 \cdot 2^t + \cdots + a_n \cdot 2^{tn} = 2^k(a_0' + 2^{t-k} \cdot A(t))$. Liczba tej postaci może być potęgą dwójki tylko, gdy $a_0' + 2^{t-k} \cdot A(t) = 1$. To, z kolei, może mieć miejsce tylko, gdy $A(t) = a_1 + a_2 \cdot 2^t + \cdots + a_n \cdot 2^{t(n-1)} = 0$ dla wszystkich $t > k$. Co może zajść tylko, gdy $a_1 + a_2X + \cdots + a_nX^{n-1} = 0$. Więc tylko, gdy $f(X) = a_0$. Ale wielomian $f(X)$ miał być niestały! To dowodzi, że $a_0 = 0$. Wtedy jednakże liczba $f(3)$, jako podzielna przez 3, nie może być potęgą dwójki. Uzyskana sprzeczność kończy rozwiązanie.

Sposób 2. Intuicja leżąca u podstaw tego sposobu rozwiązania jest natury wielkościowej. Chodzi o to, że (niestały) wielomian traktowany jako funkcja rzeczywista wprawdzie rośnie do nieskończoności ale "robi" to zdecydowanie wolniej niż funkcja wykładnicza (*wzrost wielomianowy jest wolniejszy niż wzrost wykładniczy*). Tę obserwację wykorzystujemy tak: Dla danej liczby $t \in \mathbb{N}$ rozważmy ciąg

$$f(1), f(2), \ldots, f(tn + 1). \qquad (*)$$

Każdy wyraz tego ciągu jest (wobec założenia nie wprost) potęgą 2^s. Przy tym liczba 2 występuje w nim co najwyżej n razy, liczba 2^2 występuje co najwyżej n razy, liczba 2^3 występuje co najwyżej n razy, itd., aż do liczby 2^t. Wobec tego w ciągu $(*)$ występuje liczba 2^{t+k} dla pewnego $k \in \mathbb{N}$. Stąd wynika nierówność $f(tn+1) > 2^t$ dla każdej liczby naturalnej $t \geqslant t_0$. Liczbę t_0 wybieramy tak, żeby mieć pewność, że $x \longmapsto f(x)$ jest funkcją rosnącą dla $x \geqslant t_0/n$. Stąd łatwo wywieść nierówność $f(x) \geqslant a^x$ prawdziwą dla wszystkich dostatecznie dużych x przy pewnej liczbie $a > 1$ (na przykład $a = \sqrt[n]{2}$). To jest właśnie oczekiwana sprzeczność, zobacz $\mathbb{RIN}$.

Z3.B7 Mamy prosty

L e m a t. Jeżeli różnica kwadratów (liczb całkowitych) jest liczbą parzystą, to jest liczbą podzielną przez 4. *D o w ó d.* Różnica (kwadratów) liczb całkowitych jest parzysta tylko, gdy te liczby są tej samej parzystości. Mamy więc dwa przypadki: $(2k)^2-(2l)^2=4(k^2-l^2)$ lub $(2k+1)^2-(2l+1)^2=4(k^2-l^2+k-l)$. Q.e.d.

Załóżmy teraz, nie wprost, że wszystkie liczby $f(n)$, $n\in\mathbb{N}$, są kwadratami (liczb całkowitych). W szczególności, liczby $f(1)$, $f(3)$, $f(2)$ i $f(4)$ są kwadratami. Symbolicznie: $1+a+b+c=\square$, $27+9a+3b+c=\square$, $8+4a+2b+c=\square$ i $64+16a+4b+c=\square$. Stąd otrzymujemy $f(3)-f(1)=26+8a+2b=\square-\square$. Widać, że $f(3)-f(1)$ jest parzystą różnicą kwadratów. Zatem, na mocy lematu, jest podzielna przez 4. Stąd, na mocy Zasady Podstawowej, $4|2+2b$. Jednocześnie $f(4)-f(2)=56+12a+2b=\square-\square$. Stąd, podobnie jak wyżej, $4|2b$. Uzyskane podzielności $4|2+2b$ i $4|2b$ pokazują oczywistą s p r z e c z n o ś ć: $4|2$.

Z3.B8 Udowodnimy najpierw trzy lemaciki.

L e m a t 1. *Jeżeli $f(X)\in\mathbb{R}[X]$, $\deg f(X)=n$, to istnieje taka stała $C>0$, że dla wszystkich $x\in\mathbb{N}$ zachodzi nierówność $|f(x)|\leqslant Cx^n$. Ponadto, nierówność $|f(x)|\leqslant Cx^{n-1}$, przy dowolnej stałej $C>0$ zachodzi tylko dla s k o ń c z e n i e wielu $x\in\mathbb{N}$. D o w ó d.* Niech $f(X)=a_0+a_1X+\cdots+a_nX^n$. Niech $M=\max\{|a_i|:0\leqslant i\leqslant n\}$. Wówczas $|f(x)|\leqslant|a_0|+|a_1|x+\cdots+|a_n|x^n\leqslant M(1+x+\cdots+x^n)$ (na mocy nierówności trójkąta) dla dowolnego $x\in\mathbb{N}$. Wystarczy więc przyjąć $C=M(n+1)$. Z drugiej strony, gdyby $|f(x)|\leqslant Cx^{n-1}$ dla nieskończenie wielu $x\in\mathbb{N}$, to, zapisując $f(x)=a(x)+a_nx^n$ i korzystając z udowodnionej nierówności $|-a(x)|\leqslant C'x^{n-1}$, otrzymalibyśmy nierówność $|a_nx^n|=|f(x)-a(x)|\leqslant|f(x)|+|-a(x)|\leqslant(C+C')x^{n-1}$. Stąd, po podzieleniu przez x, mamy s p r z e c z n o ś ć: $|a_n|x\leqslant C+C'$ dla nieskończenie wielu $x\in\mathbb{N}$. Q.e.d.

L e m a t 2. *Jeżeli $r_1,\ldots,r_s\in\mathbb{N}$ są dzielnikami liczby $m\in\mathbb{N}$, to* $\mathrm{NWW}(r_1,\ldots,r_s)|m$. *D o w ó d.* Najmniejsza wspólna wielokrotność jest dzielnikiem każdej wspólnej wielokrotności, por. D2.6. Teza jest równoważna implikacji $\forall_i k_i\leqslant l\Longrightarrow\max\{k_1,\ldots,k_s\}\leqslant l$, zob. C2.41 i C2.42. Q.e.d.

L e m a t 3. *Dla dowolnych liczb naturalnych $r_1,\ldots,r_s$ zachodzi nierówność* $r_1\cdot r_2\cdot\ldots\cdot r_s\leqslant\mathrm{NWW}(r_1,\ldots,r_s)\cdot\prod_{1\leqslant i<j\leqslant s}\mathrm{NWD}(r_i,r_j)$. *D o w ó d.* Żądaną nierówność wnioskujemy (na mocy C2.2) z podzielności $r_1\cdot\ldots\cdot r_s|\mathrm{NWW}(r_1,\ldots,r_s)\cdot\prod_{1\leqslant i<j\leqslant s}\mathrm{NWD}(r_i,r_j)$. Ta podzielność wyniknie, na mocy C2.41 i C2.42, z nierówności $k_1+\cdots+k_s\leqslant\max\{k_1,\ldots,k_s\}+\sum_{1\leqslant i<j\leqslant s}\min\{k_i,k_j\}$, gdzie $p\in\mathbb{P}$ i $k_i=v_p(r_i)$. Łatwy dowód pozostawiamy Czytelnikowi. Q.e.d.

Przechodzimy do rozwiązania zadania. Oznaczmy $n=\deg f(X)$. Niech $g(X)$ będzie (jedynym) takim wielomianem stopnia $\leqslant n$, że $g(k)=a_k$ dla wszystkich $k=1,2,\ldots,n+1$ (zobacz T3.23 w ustępie 3.4.10, gdzie widzimy, że wielomian $g(X)$ ma współczynniki w y m i e r n e). Pokażemy, że $g(X)$ jest właściwym wyborem (tzn., że $g(k)=a_k$ dla k a ż d e g o $k\in\mathbb{N}$). Ponieważ $g(X)\in\mathbb{Q}[X]$, więc istnieje taka liczba naturalna d, że wielomian $h(X):=dg(X)$ ma współczynniki całkowite (tzn., d jest wspólną wielokrotnością mianowników wszystkich współczynników wielomianu $g(X)$). Rozważmy teraz dowolną liczbę naturalną $m>n+1$. Zapiszmy równość

$$d(a_m-g(m))=d(a_m-a_k)+(h(k)-h(m)).\qquad(*)$$

Drugi składnik z prawej strony jest, na mocy (3.3), podzielny przez różnicę $m-k$. Ponieważ pierwszy składnik, na mocy założenia (1), jest też podzielny przez tę różnicę, więc mamy $m-k|d(a_m-g(m))$ dla każdego $1\leqslant k\leqslant n+1$. Oznaczmy $d_m:=\mathrm{NWW}(m-1,m-2,\ldots,m-n-1)$. Wykazane podzielności, na mocy lematu 2, dają podzielność $d_m|d(a_m-g(m))$. Przypomnijmy, że dążymy do wykazania równości $a_m-g(m)=0$ dla każdego m. Załóżmy więc, nie wprost, że $a_m-g(m)\neq0$ dla pewnego $m>n+1$. Wówczas, zobacz C2.2, $d_m\leqslant|d(a_m-g(m))|$. Ponieważ, jednocześnie, $|d(a_m-g(m))|\leqslant|da_m|+|dg(m)|\leqslant d|f(m)|+d|g(m)|\leqslant dC'm^n+dC''m^r\leqslant Cm^n$ (na mocy założenia (2) i pierwszej części lematu 1; tu $r=\deg g(X)\leqslant n$), więc $d_m\leqslant Cm^n$. Chcemy teraz zastosować lemat 3. Rozważmy w tym celu wielomian $t(X)=(X-1)(X-2)\cdot\ldots\cdot(X-n-1)$. Jest to wielomian

stopnia $n+1$. Jego wartość dla $X=m$, na mocy lematu 3, możemy oszacować

$$t(m) \leqslant d_m \cdot \prod_{1\leqslant i<j\leqslant n+1} \mathrm{NWD}\,(m-i,\, m-j) \leqslant CDm^n, \qquad (**)$$

gdzie przez D oznaczyliśmy iloczyn $\prod_{i<j}(j-i)$ (korzystamy tu z nierówności $\mathrm{NWD}\,(a,\,b)\leqslant |a-b|$ dla różnych liczb całkowitych a, b; *każdy wspólny dzielnik różnych liczb całkowitych jest dzielnikiem różnicy tych liczb*). Otrzymana nierówność $(**)$ jest, na mocy drugiej części lematu 1, fałszywa dla dostatecznie dużych m. Wnioskujemy stąd, że dla wszystkich $m>m_0$ (przy pewnym $m_0\in\mathbb{N}$) zachodzi równość $a_m=g(m)$. Dla zakończenia rozwiązania musimy jeszcze udowodnić równość $a_m=g(m)$ dla wszystkich $m=n+2,\,n+3,\ldots,\,m_0$. Dla każdego takiego m, dzięki równości $(*)$, widzimy, że liczba $d(a_m-g(m))$ jest podzielna przez $m-k$ dla wszystkich $k>m_0$. To, oczywiście, jest możliwe tylko, gdy $a_m-g(m)=0$.

Z3.B9 Będziemy korzystać z następującej własności ciągu (a_n):

$$a_k-a_l \mid a_{k+r}-a_{l+r} \qquad (*)$$

dla wszystkich $k,\,l\in\mathbb{N}$. Wynika ona z (3.3). Rzeczywiście, mamy $a_k-a_l \mid f(a_k)-f(a_l)$, czyli $a_k-a_l\mid a_{k+1}-a_{l+1}$. Ponieważ, dokładnie tak samo, $a_{k+1}-a_{l+1}\mid a_{k+2}-a_{l+2}$, więc (dzielnik dzielnika jest dzielnikiem!) $a_k-a_l\mid a_{k+2}-a_{l+2}$. Itd., oczywista indukcja daje więc $(*)$.

Udowodnimy przez indukcję, że $f(m)=m+1$ dla każdego $m\in\mathbb{N}$. Zacznijmy (baza indukcji!) od dowodu równości $f(1)=2$. Załóżmy, nie wprost, że $f(1)\neq 2$. Wówczas, wobec założenia $f(m)>m$, mamy $f(1)\geqslant 3$. Niech $d=f(1)-1$. Wtedy $d\geqslant 2$. Popatrzmy na reszty z dzielenia liczb a_m przez d. Liczba $a_1=1$ daje resztę 1 z dzielenia przez d. Liczba $a_2=f(1)=d+1$ też daje resztę 1 z dzielenia przez d. Ponieważ, na mocy $(*)$ $a_2-1\mid a_m-a_{m-1}$, dla każdego $m\geqslant 3$, czyli $d\mid a_m-a_{m-1}$, więc (trywialna indukcja!) wszystkie liczby a_m dają tę samą resztę 1 z dzielenia przez d. To, wobec założenia o podzielności któregoś wyrazu ciągu (a_n) przez d, jest niemożliwe. Zatem $a_2=f(1)=2$. Krok indukcyjny wykonujemy analogicznie: jeżeli $f(1)=2$, $f(2)=3$, …, $f(m-1)=m$, czyli $a_1=1$ i $a_2=2$, …, $a_m=m$, ale $a_{m+1}=f(a_m)=f(m)\neq m+1$, to $d:=f(m)-1\geqslant m+1$. Wówczas żadna z liczb $a_1,\,a_2,\ldots,\,a_m$ nie jest podzielna przez d (bo są mniejsze niż d i dodatnie). Jednocześnie liczba $a_{m+1}=f(m)=d+1$, więc daje z dzielenia przez d resztę 1, i ogólnie, dla każdego $r\in\mathbb{N}$ liczba $a_{m+r}-a_r$ jest podzielna przez $d=a_{m+1}-a_1$, więc liczby a_{m+r} i a_r dają tę samą resztę przy dzieleniu przez d. Dostajemy sprzeczność z założeniem $d\mid a_n$ dla pewnego n. Ta sprzeczność dowodzi równości $f(m)=m+1$ dla każdego $m\in\mathbb{N}$. Stąd, zob. W2T3.4, $f(X)=X+1$.

Z3.B10 (1) Stosując warunek dla $p=2$ sprawdzamy, że a jest nieparzysta. Kładziemy więc $a=-1-2m$. (2) Dla dowolnej $p\in\mathbb{P}_{>2}$ znajdujemy $k\in\mathbb{Z}$, że p dzieli $f(k+1)-f(k)=2(k-m)$, czyli $p\mid k-m$. (3) Stąd, zobacz (3.3), $p\mid f(k)-f(m)$, skąd $p\mid f(m)$, więc $p\mid m^2+am+b$, czyli $p\mid -m^2-m+b$. Skoro więc liczba $b-m^2-m$ jest podzielna przez wszystkie $p\in\mathbb{P}_{>2}$, to $b-m^2-m=0$. (4) Mamy więc $(X-m)(X-m-1)=X^2-(-1-2m)X+m^2+m=X^2+aX+b=f(X)$, co dowodzi, że $f(m)=f(m+1)=0$.

Z3.C1 (1) Całkowitość liczby $\binom{x}{n}$ dla wszystkich $x\in\mathbb{N}$ wynika natychmiast z jej interpretacji kombinatorycznej (zobacz $\mathbb{KOM}$, gdzie przekonujemy się, że $\binom{N}{n}$ jest równa liczbie (całkowitej, nieujemnej) n-elementowych podzbiorów zbioru N-elementowego). Możemy to również zobaczyć sposobem arytmetycznym, zob. C2.49. Jeżeli $x\in\mathbb{Z}_{<0}$, to $-x\in\mathbb{N}$ i zachodzi oczywista równość

$$\binom{x}{n}=\frac{1}{n!}x(x-1)\cdot\ldots\cdot(x-n+1)=\frac{(-1)^n}{n!}(-x+n-1)\cdot\ldots\cdot(-x)=(-1)^n\binom{-x+n-1}{n}.$$

Stąd $\binom{x}{n}\in\mathbb{Z}$. **(2)** Z definicji (3.72) mamy natychmiast **równość pochłaniania** $\binom{X+1}{n}=\frac{X+1}{n}\binom{X}{n-1}$. Wyprowadzenie stąd równości (3.73) jest równie natychmiastowe. **(3)** Rozumujemy indukcyjnie wzglę-

dem stopnia n. Baza indukcji jest jasna: wielomian stopnia 0 jest stałą α_0. Rozważmy więc wielomian $f(X) = a_0 + a_1X + \cdots + a_nX^n$ stopnia $n \geqslant 1$. Wówczas różnica $f(X) - a_n n!\binom{X}{n}$ ma stopień $\leqslant n-1$ i współczynniki w (tym samym co wielomian $f(X)$) ciele $\mathbb{K}$. Istnieją więc (dzięki założeniu indukcyjnemu) takie jednoznacznie wyznaczone elementy $\alpha_0, \ldots, \alpha_{n-1} \in \mathbb{K}$, że

$$f(X) - a_n n!\binom{X}{n} = \alpha_0 + \alpha_1\binom{X}{1} + \ \ldots\ + \alpha_{n-1}\binom{X}{n-1}.$$

Widzimy stąd zachodzenie równości (3.74) (przy $\alpha_n = a_n n!$). Zobaczmy jak ma się rzecz z jednoznacznością: Gdyby, oprócz (3.74), zachodziła też równość $f(X) = \beta_0 + \beta_1\binom{X}{1} + \cdots + \beta_n\binom{X}{n}$, to kładąc $X = 0$ (tzn., wyznaczając wartość dla argumentu 0) znajdujemy równość $\beta_0 = \alpha_0$. Stąd, po odjęciu α_0, dostajemy równość wielomianów $\alpha_1\binom{X}{1} + \cdots + \alpha_n\binom{X}{n} = \beta_1\binom{X}{n} + \cdots + \beta_n\binom{X}{n}$. Tu kładziemy $X = 1$ i znajdujemy równość $\beta_1 = \alpha_1$. Postępując tak dalej, kończymy rozwiązanie. U w a g a. (Dla znających język algebry liniowej.) Układ $\{X^0, X^1, X^2, \ldots\}$ jest **bazą** przestrzeni wektorowej $\mathbb{K}[X]$ (to jest tylko inny sposób definicji zbioru $\mathbb{K}[X]$), zaś inną bazą tej samej przestrzeni jest układ $\left\{\binom{X}{0}, \binom{X}{1}, \binom{X}{2}, \ldots\right\}$. Co więcej, jeżeli przez $\mathbb{K}_n[X]$ oznaczymy podprzestrzeń wielomianów stopni $\leqslant n$, to jej bazą jest zarówno układ $\{X^0, X^1, \ldots, X^n\}$ jak i układ $\left\{\binom{X}{0}, \binom{X}{1}, \ldots, \binom{X}{n}\right\}$.

Z3.C2 (1) Zapisujemy (jednoznacznie!) nasz wielomian w postaci (3.74) i kładziemy kolejno $X = 0$ (to daje $\alpha_0 \in \mathbb{Z}$), $X = 1$ (to daje $\alpha_0+\alpha_1 \in \mathbb{Z}$, więc $\alpha_1 \in \mathbb{Z}$), $X = 2$ (to daje $\alpha_0+2\alpha_1+\alpha_2 \in \mathbb{Z}$, więc $\alpha_2 \in \mathbb{Z}$), i tak dalej. Oczywista indukcja! **(2)** Wielomian $g(X) := f(X+a)$ również ma stopień n (i współczynniki zespolone), oraz przyjmuje wartości całkowite dla $n+1$ argumentów $0, 1, \ldots, n$. To, jak widać z rozwiązania poprzedniego zadania, wystarcza do stwierdzenia całkowitości współczynników α_j w jego zapisie w postaci (3.74). To, z kolei, dowodzi, że $g(x) \in \mathbb{Z}$ dla wszystkich $x \in \mathbb{Z}$. Zatem i $f(X)$ ma tę własność.

Z3.C3 Mamy lemacik: *L e m a t. Załóżmy, że* $a_i \in \mathbb{Z}$, $\mathrm{NWD}\,(a_0, a_1, \ldots, a_n) = 1$ *i, dla pewnej liczby wymiernej* $q \neq 0$, *liczby* $qa_0, qa_1, \ldots, qa_n$ *są całkowite. Wówczas* $q \in \mathbb{Z}$. *D o w ó d.* Zapiszmy $q = h/k$ w postaci nieskracalnej. I niech $qa_i = c_i \in \mathbb{Z}$. Czyli $ha_i = kc_i$. Stąd, na mocy ZTA, $k|a_i$ dla każdego $i = 0, \ldots, n$. Względna pierwszość liczb a_i pokazuje, że $k = \pm 1$. Q.e.d.

Niech $f(X) = a_0+a_1X+\cdots+a_nX^n$, $a_j \in \mathbb{Z}$, i załóżmy, że liczba naturalna $d \in \mathbb{N}$ dzieli wszystkie elementy zbioru $\{f(k) : k \in \mathbb{N}\}$. Wówczas wielomian $\frac{1}{d}f(X)$ ma współczynniki w y m i e r n e i przyjmuje dla argumentów całkowitych wartości całkowite. Zapiszmy go, zob. Z3.C2(1), w postaci

$$\frac{1}{d}f(X) = \frac{a_0}{d} + \frac{a_1}{d}X + \ \ldots\ + \frac{a_n}{d}X^n = b_0 + b_1\binom{X}{1} + \cdots + b_n\binom{X}{n},$$

gdzie $b_i \in \mathbb{Z}$. Mnożąc tę równość przez $n!$, dostajemy równość

$$\frac{n!}{d}a_0 + \frac{n!}{d}a_1X + \ \ldots\ + \frac{n!}{d}a_nX^n = c_0 + c_1X + c_2X(X-1) + \cdots + c_nX(X-1)\cdot\ldots\cdot(X-n+1),$$

gdzie $c_i = b_i n! \in \mathbb{Z}$. Widać, że współczynniki stojące przy potęgach X^k zmiennej X w wielomianie z prawej strony są liczbami całkowitymi. Zatem wszystkie liczby $\frac{n!}{d}a_i$ są liczbami całkowitymi. Wystarczy teraz zastosować lemacik dla $q = n!/d$.

Z3.C4 Rozważmy wielomian $f_k(X) := \sum_{j=0}^{k}(-1)^j\binom{k}{j}\binom{X+j}{k} \in \mathbb{Q}[X]$. Pokażemy, że jest on wielomianem stałym (to znaczy stopnia $\leqslant 0$). Badamy w tym celu różnicę $f_k(X+1) - f_k(X)$. Mamy

$$f_k(X+1) - f_k(X) = \sum_{j=0}^{k}(-1)^j\binom{k}{j}\left[\binom{X+1+j}{k} - \binom{X+j}{k}\right] = \sum_{j=0}^{k}(-1)^j\binom{k}{j}\binom{X+j}{k-1}.$$

Druga równość wynika z (3.73). Korzystając teraz z równości $\binom{k}{j} = \binom{k-1}{j} + \binom{k-1}{j-1}$ konstytuujących trójkąt Pascala (zob. $\mathbb{KOM}$), które, nawiasem mówiąc, są równoważne równościom (3.73), mamy

$$f_k(X+1) - f_k(X) = \sum_{j=0}^{k} (-1)^j \binom{k-1}{j}\binom{X+j}{k-1} + \sum_{j=0}^{k} (-1)^j \binom{k-1}{j-1}\binom{X+j}{k-1}.$$

Pierwszy składnik otrzymanej sumy jest równy $f_{k-1}(X)$. Drugi jest równy $-\sum_{i=0}^{k-1}(-1)^i\binom{k-1}{i}\binom{X+1+i}{k-1}$, czyli $f_{k-1}(X+1)$. Mamy więc

$$f_k(X+1) - f_k(X) = (-1)(f_{k-1}(X+1) - f_{k-1}(X)) = \ldots = (-1)^k(f_0(X+1) - f_0(X)) = 0.$$

Udowodniona równość $f_k(X+1) - f_k(X) = 0$ (po podstawieniu kolejno $X = 0, 1, \ldots, k$) daje równości $f_k(0) = f_k(1) = \cdots = f_k(k)$, z których, dzięki W1T3.4, wnioskujemy, że $\deg f_k(X) = 0$. Wielomian $f_k(X)$ jest więc wielomianem stałym. Dla zakończenia rozwiązania wystarczy wyznaczyć wartość $f_k(0)$. A ta jest równa $(-1)^k$.

Z3.D1 Niech $f(k) = m^2$ i $f(k+1) = (m+1)^2$. Wówczas $2m+1 = f(k+1) - f(k) = 2k+1+p$. Stąd $p = 2(m-k)$. Stąd $m^2 = f(k) = k^2 + 2(m-k)k + q$, więc $q = (m-k)^2$. Zatem $f(x) = x^2 + 2(m-k)x + (m-k)^2 = (x+m-k)^2$.

Z3.D2 Teza zadania jest wprawdzie czysto teorioliczbowo-algebraiczna, rozwiązanie jednak wymaga pewnej wiedzy analitycznej. Ponieważ $f(n)$ jest kwadratem dla każdego $n \in \mathbb{N}$, więc $f(n) \geqslant 0$ dla każdego $n \in \mathbb{N}$. Zatem możemy określić funkcję $g : \mathbb{N} \longrightarrow \mathbb{Z}_{\geqslant 0}$ wzorem $g(n) = \sqrt{an^2+bn+c}$ (pierwiastek arytmetyczny, tzn. nieujemny). Liczymy granicę $\lim_{n\to\infty}[g(n+1) - g(n)]$. To się robi za pomocą metody standardowej: Zapisujemy

$$g(n+1) - g(n) = \frac{f(n+1) - f(n)}{g(n+1) + g(n)} = \frac{2an + a + b}{g(n+1) + g(n)}.$$

Dzieląc licznik i mianownik przez $n\sqrt{a}$ (uzasadniwszy przedtem, że $a > 0$) dostajemy równość

$$g(n+1) - g(n) = \frac{2\sqrt{a} + \frac{a+b}{n\sqrt{a}}}{\sqrt{1 + \frac{2a+b}{an} + \frac{a+b+c}{an^2}} + \sqrt{1 + \frac{b}{an} + \frac{c}{an^2}}},$$

z której widać, że $\lim_{x\to\infty} g(n+1) - g(n) = \sqrt{a}$. Ale ciąg liczb całkowitych jest zbieżny tylko, gdy jest stały od pewnego miejsca. Mamy więc liczbę naturalną $r := \sqrt{a} \in \mathbb{N}$, dla której zachodzi równość $g(n+1) - g(n) = r$ dla wszystkich $n \geqslant n_0$. To oznacza, że ciąg $g(n_0)$, $g(n_0+1)$, $g(n_0+2), \ldots$ jest ciągiem arytmetycznym o różnicy r. Zatem $g(n_0+k) = g(n_0)+kr$ dla każdego $k \in \mathbb{Z}_{\geqslant 0}$. Połóżmy $x = n_0 + k$. Wówczas $ax^2 + bx + c = f(n_0+k) = g(n_0+k)^2 = (g(n_0) + kr)^2 = (rx - rn_0 + g(n_0))^2$ dla wszystkich całkowitych $x \geqslant n_0$. Widzimy więc dwa wielomiany:

$$f(X) = aX^2 + bX + c \quad \text{i} \quad \widetilde{f}(X) = r^2X + 2(g(n_0) - rn_0)rX + (g(n_0) - rn_0)^2,$$

które przyjmują tę samą wartość dla nieskończenie wielu argumentów. Zatem, zobacz W2T3.4, $f(X) = \widetilde{f}(X)$, więc też $f(x) = (rx+d)^2$ dla każdego x (gdzie $d = g(n_0) - rn_0$).

Z3.D3 Jasne jest, że $a \geqslant 0$ (w przeciwnym przypadku $f(x)$ byłaby liczbą ujemną dla pewnych $x \in \mathbb{Z}$, a bikwadrat nigdy nie jest ujemny). Równie jasne jest, że $c \geqslant 0$ (bo $c = f(0)$). Załóżmy, nie wprost, że co najmniej jedna z liczb a, b jest różna od zera. Rozważmy (dużą) liczbę naturalną n i zbiór $\mathcal{A}_n = \{f(0), f(1), \ldots, f(n)\}$. Ten zbiór ma co najmniej $n/2$ elementów (dana wartość $f(k)$ może być przyjęta dla jeszcze co najwyżej jednego argumentu, zobacz W1T3.4) i jest podzbiorem zbioru $\mathcal{B}_n = \{0, 1, \ldots, an^2 + |b|n + c\}$. Ponadto każdy jego element jest bikwadratem.

Ponieważ bikwadratów w zbiorze $\mathcal{B}_n$ jest co najwyżej $\sqrt[4]{an^2+|b|n+c}+1$, więc mamy nierówność $\sqrt[4]{an^2+|b|n+c}+1 \geqslant n/2$. Ta nierówność, równoważna nierówności $an^2+|b|n+c \geqslant (n/2-1)^4$, jest niemożliwa dla dostatecznie dużych n. Uzyskana sprzeczność kończy rozwiązanie.

Z3.D4 Załóżmy, nie wprost, że $\mathcal{A}(f)$ jest niepusty i skończony. Niech k_0 oznacza najmniejszy, a k_1 największy element zbioru $\mathcal{A}(f)$. Rozważmy wielomian $g(X) = f(X+1) - f(X)$. Wówczas $g(k_1)$, jako różnica $f(k_1+1) - f(k_1)$ liczby całkowitej i niecałkowitej, jest liczbą niecałkowitą. Zatem $k_1 \in \mathcal{A}(g)$. Jeżeli $k > k_1$, to $g(k) = f(k+1) - f(k)$, jako różnica liczb całkowitych, jest liczbą całkowitą, więc $k \notin \mathcal{A}(g)$. Podobnie, jeżeli $k < k_0 - 1$, to $k \notin \mathcal{A}(g)$. Podsumowując, mamy taki w n i o s e k: *jeżeli $\mathcal{A}(f)$ jest niepusty i skończony, to $\mathcal{A}(g)$ też jest niepusty i skończony*. Ale $\deg(g) = \deg(f)-1 < \deg(f)$. W ten sposób, po skończonej liczbie kroków, dojdziemy do wielomianu h stopnia 0, dla którego zbiór $\mathcal{A}(h)$ jest niepusty i skończony. Nonsens! U w a g a. Pokazane rozumowanie ma charakter z s t ę p o w a n i a, czyli **desantu** (**nieskończonego**). Można je zastąpić (jednocześnie uzasadniając(!) jego poprawność) przez rozumowanie oparte na Zasadzie Minimum. W aktualnym przypadku robimy to tak: skoro (założenie nie wprost) i s t n i e j ą *brzydkie* wielomiany (takie, dla których zbiór $\mathcal{A}(f)$ jest skończony i niepusty), to istnieje też *brzydki* wielomian f_0 n a j n i ż s z e g o stopnia. Wówczas wielomian $f_0(X+1) - f_0(X)$ jest jednocześnie *brzydki* i *ładny*.

Z3.D5 Rozważ wielomian $g(X) = f(X^2)$. Wielomian ten ma stopień $2n$ i dla $2n+1$ (kolejnych) argumentów całkowitych $x = -n, -n+1, \ldots, n-1, n$ przyjmuje wartość całkowitą. Zatem, zobacz Z3.C2(2), $f(x^2) = g(x) \in \mathbb{Z}$ dla wszystkich $x \in \mathbb{Z}$. Kontrprzykładów jest dużo, na przykład $f(X) = X(X-1)/12$.

Z3.D6 Załóżmy, że obraz $f(\mathbb{Z}) := \{f(x) : x \in \mathbb{Z}\}$ jest, dla danego wielomianu $f(X) \in \mathbb{Z}[X]$, całym zbiorem $\mathbb{Z}$. Niech, w szczególności, $f(a) = 0$ i $f(b) = 1$ dla danych $a, b \in \mathbb{Z}$. Wówczas, zob. C3.4, $b-a|f(b)-f(a)$, czyli $b-a|1$, więc $|b-a| = 1$. Jeżeli $b = a+1$, to dowodzimy przez indukcję, że $f(a+k) = k$ dla każdego $k \in \mathbb{N}$. Wtedy, na mocy W2T3.4, $f(a+X) = X$, więc $f(X) = X - a$. Jeżeli $b = a-1$, to podobnie dowodzimy, że $f(X) = -X + a$.

Z3.E1 Zauważcie, że jeżeli u jest pierwiastkiem wielomianu $f(X)$, to au jest pierwiastkiem wielomianu unormowanego $g(X) = X^3 + bX^2 + acX + a^2d$ (wystarczy w tym celu pomnożyć równość $au^3 + bu^2 + cu + d = 0$ przez a^2 por. rozwiązanie Z3.8). Jeżeli więc wielomian $f(X)$ ma trzy pierwiastki wymierne u_1, u_2, u_3, to wielomian $g(X)$ ma trzy pierwiastki wymierne au_1, au_2, au_3, które w dodatku, zobacz T3.5, są liczbami całkowitymi. Oznaczmy je k_1, k_2, k_3. Wtedy $k_1k_2k_3 = -a^2d$. Więc nieparzysta(!) liczba $-a^2d$ jest iloczynem trzech czynników k_1, k_2, k_3. Zatem czynniki te są liczbami nieparzystymi. Przeto $k_1+k_2+k_3 = -b$ jest liczbą nieparzystą i $k_1k_2+k_2k_3+k_3k_1 = ac$ jest liczbą nieparzystą. Więc i bac jest liczbą nieparzystą. To jest sprzeczne z założeniem $bc \in 2\mathbb{Z}$.

Z3.E2 S p o s ó b 1. Jeżeli α_1, α_2, α_3 są pierwiastkami wielomianu $f(X) = X^3 - 3X^2 - dX + c$ i dwa z nich są liczbami wymiernymi, to i trzeci jest liczbą wymierną (bo $\alpha_1 + \alpha_2 + \alpha_3 = 3c \in \mathbb{Q}$), w dodatku są one wszystkie liczbami całkowitymi, zob. T3.5. Z tego wynika, że możemy przyjąć następujące założenie nie wprost: układ równań $x + y + z = 3c$, $xy + yz + zx = -d$, $xyz = -c$, gdzie $c \neq 0$, ma rozwiązania w liczbach całkowitych, i szukać sprzeczności. Ponieważ druga z tych równości mówi tylko, że suma iloczynów liczb całkowitych jest liczbą całkowitą, więc sprzeczności musimy szukać w założeniach $x, y, z \in \mathbb{Z}$, $x + y + z = 3c$, $xyz = -c$ i $c \neq 0$. Mamy

$$3|c| = |x+y+z| \leqslant |x| + |y| + |z| \leqslant |xyz| + |xyz| + |xyz| = 3|xyz| = 3|c|.$$

Pierwsza nierówność jest nierównością trójkąta, a druga wynika z faktu, że $|yz|, |xz|, |xy| \geqslant 1$ (bowiem, na mocy $xyz = -c \neq 0$, $x, y, z \neq 0$). Stąd wynika, że obie nierówności są w rzeczywistości równościami. Pierwsza jest równością tylko w przypadku, gdy x, y, z są tego samego znaku (sprawdzić!), zaś druga jest równością tylko w przypadku, gdy $|yz| = |xz| = |xy| = 1$, czyli gdy $|x| = |y| = |z| = 1$. Może więc być tylko, albo $x = y = z = -1$, albo $x = y = z = 1$.

Obie możliwości prowadzą do sprzeczności $\mp 1 = c = \pm 1$. Sposób 2. Z Z2.4 wiemy, że wymierne pierwiastki (jeżeli istnieją) są w rzeczywistości liczbami całkowitymi będącymi dzielnikami liczby c. Załóżmy (nie wprost), że liczby całkowite $m \neq n$ są pierwiastkami. Wówczas $w(X) := X^3 - 3cX^2 - dX + c = (X - m)(X - n)(aX + b)$ (zobacz (3.5)). Stąd wynika, że $a = 1$, oraz że $-b$ jest (całkowitym) pierwiastkiem wielomianu $w(X)$. Ponadto $-b|c$ (bo każdy całkowity pierwiastek tak czyni). Równość Viète'a $m + n - b = 3c$ i, wynikające z podzielności, nierówności $|m| \leqslant |c|$, $|n| \leqslant |c|$, $|-b| \leqslant |c|$, dowodzą, że $m = n = -b = c$. To jest sprzeczne z równością $mn(-b) = -c$ (trzecią równością Viète'a), bo $c^3 \neq -c$ dla całkowitego, niezerowego c.

Z3.E3 Wyróżnik $(2c+1)^2 - 4c(2c-1) = 4c^2 + 4c + 1 - 8c^2 + 4c = -4c^2 + 8c + 1$ jest nieujemny wtedy i tylko wtedy, gdy $(2 - \sqrt{5})/2 \leqslant c \leqslant (2 + \sqrt{5})/2$. Jeżeli c spełnia powyższe nierówności i $c \neq 0$ (co oznacza ten warunek?), to pierwiastki x_1, x_2 są liczbami rzeczywistymi. Ze wzorów Viète'a mamy wówczas: $x_1 + x_2 = -(2c+1)/c$, $x_1 \cdot x_2 = (2c-1)/c$. Stąd

$$(x_1 - 1)(x_2 - 1) = x_1x_2 - x_1 - x_2 + 1 = \frac{2c-1}{c} + \frac{2c+1}{c} + 1 = 5.$$

Szukamy całkowitych x_1, x_2. Jednoznaczność rozkładu (liczb całkowitych na iloczyn liczb pierwszych, zobacz T2.16) i powyższa równość dają więc jedną z możliwości:

$$\begin{cases} x_1 - 1 = 1, \\ x_2 - 1 = 5, \end{cases} \quad \begin{cases} x_1 - 1 = 5, \\ x_2 - 1 = 1, \end{cases} \quad \begin{cases} x_1 - 1 = -1, \\ x_2 - 1 = -5, \end{cases} \quad \begin{cases} x_1 - 1 = -5, \\ x_2 - 1 = -1. \end{cases}$$

Przeto, $(x_1, x_2) = (2, 6), (6, 2), (0, -4)$ lub $(-4, 0)$. Pierwsze dwie możliwości dają $c = -1/10$, a kolejne dwie, $c = 1/2$. Sprawdzenie, że te wartości c są dobre, opuszczamy.

Z3.E4 Załóżmy, nie wprost, że $\alpha_1, \alpha_2, \ldots, \alpha_n$ są pierwiastkami (rzeczywistymi). Założenia $a_{n-1} = a_{n-2} = 0$, czyli (zobacz wzory Viète'a) dają

$$\alpha_1^2 + \alpha_2^2 + \cdots + \alpha_n^2 = \left(\sum_{j=1}^{n} \alpha_j\right)^2 - 2\sum_{i<j} a_ia_j = (-a_{n-1})^2 - 2a_{n-2} = 0.$$

Zatem (pamiętamy o założeniu rzeczywistości liczb α_j), wszystkie α_j są równe 0. Stąd $a_0 = \pm\alpha_1 \cdot \ldots \cdot \alpha_n$. Sprzeczność.

Z3.E5 Sztuczka polega na zauważeniu, że jeżeli $\alpha_1 < \alpha_2 < \alpha_3$ są pierwiastkami wielomianu $X^3 + aX^2 + bX + c$, to średnie arytmetyczne $\beta_1 = (\alpha_1 + \alpha_2)/2$, $\beta_2 = (\alpha_1 + \alpha_3)/2$ i $\beta_3 = (\alpha_2 + \alpha_3)/2$ są pierwiastkami wielomianu $8X^3 + 8aX^2 + 2(a^2 + b)X + ab - c$. Ponadto, oczywiście, $\beta_1, \beta_2, \beta_3 \in \mathbb{R}$ i $\beta_1 < \beta_2 < \beta_3$.

Z3.E6 Niech $f(X) = X^4 + X^3 - 1 = (X - \alpha)(X - \beta)(X - \gamma)(X - \delta)$. Równości $f(\alpha) = f(\beta) = 0$ dają $\alpha^3 = 1/(\alpha + 1)$ i $\beta^3 = 1/(\beta + 1)$. Stąd $(\alpha\beta)^3 = 1/(\alpha + 1)(\beta + 1) = (\gamma + 1)(\delta + 1)/f(-1) = -(\gamma+1)(\delta+1)$. Analogicznie $(\gamma\delta)^3 = -(\alpha+1)(\beta+1)$. Wobec tego suma $(\alpha\beta)^3 + (\gamma\delta)^3 + \alpha\beta + \gamma\delta + 1$ jest równa $-(\gamma+1)(\delta+1) - (\alpha+1)(\beta+1) + \alpha\beta + \gamma\delta + 1 = -1 - \alpha - \beta - \gamma - \delta = 0$, ponieważ, zgodnie ze wzorem Viète'a, $\alpha + \beta + \gamma + \delta = -1$. Stąd

$$(\alpha\beta)^6 + (\alpha\beta)^4 + (\alpha\beta)^3 - (\alpha\beta)^2 - 1 = (\alpha\beta)^3 \cdot \left((\alpha\beta)^3 - \left(\frac{1}{\alpha\beta}\right)^3 + \alpha\beta - \frac{1}{\alpha\beta} + 1\right) = 0,$$

ponieważ (toujour ce François Viète!) $\alpha\beta\gamma\delta = -1$.

Z3.E7 Załóżmy, że α, β i $\alpha\beta$ są pierwiastkami. Dzięki wzorom Viète'a, mamy $\alpha+\beta+\alpha\beta = 0$ oraz $\alpha\beta+\alpha^2\beta+\alpha\beta^2 = b/a$ i $\alpha^2\beta^2 = -c/a$. Suma drugiej i trzeciej z tych równości dają $\alpha\beta(1+\alpha)(1+\beta) = (b-c)/a$. Zaś pierwsza daje $(1 + \alpha)(1 + \beta) = 1$. Stąd $\alpha\beta = (b - c)/a \in \mathbb{Q}$.

Z3.E8 Niech $\alpha_1, \ldots, \alpha_n$ będą pierwiastkami. Na mocy wzorów Viète'a, $\alpha_1 + \cdots + \alpha_n = 1$ oraz

$$\frac{1}{\alpha_1} + \cdots + \frac{1}{\alpha_n} = \frac{\sum_{1 \leqslant i_1 < \cdots < i_{n-1} \leqslant n} \alpha_{i_1} \cdot \ldots \cdot \alpha_{i_{n-1}}}{\alpha_1 \alpha_1 \cdot \ldots \cdot \alpha_n} = \frac{(-1)^{n-1}(-n^2)}{(-1)^n} = n^2.$$

Dwukrotne zastosowanie nierówności AGH daje więc

$$n^2 = 1 \cdot n^2 = (\alpha_1 + \cdots + \alpha_n)\left(\frac{1}{\alpha_1} + \cdots + \frac{1}{\alpha_n}\right) \geqslant n \sqrt[n]{\alpha_1 \cdot \ldots \cdot \alpha_n} \cdot n \sqrt[n]{\frac{1}{\alpha_1} \cdot \ldots \cdot \frac{1}{\alpha_n}} = n^2.$$

W obu nierównościach AGH zachodzi więc r ó w n o ś ć. Stąd, jak wiadomo, mamy $\alpha_1 = \alpha_2 = \cdots = \alpha_n$.

Z3.E9 Pierwiastki $\alpha_1, \alpha_2, \alpha_3$ tworzą ciąg arytmetyczny wtedy i tylko wtedy, gdy jeden z nich jest średnią arytmetyczną dwóch pozostałych. Np. $2\alpha_3 = \alpha_1 + \alpha_2$. Wówczas $3\alpha_3 = \alpha_1 + \alpha_2 + \alpha_3 = -a$ (zobacz wzory Viète'a). I odwrotnie. Widzimy więc, że pierwiastki wielomianu $f(X)$ tworzą ciąg arytmetyczny wtedy i tylko wtedy, gdy $f((-1/3)a) = 0$. Czyli wtedy i tylko wtedy, gdy zachodzi równość $(*)\, 2a^3 - 9ab + 27c = 0$. Musimy jeszcze dołożyć warunek gwarantujący rzeczywistość (należenie do $\mathbb{R}$) pierwiastków. Otóż równości Viète'a $\alpha_1+\alpha_2+\alpha_3 = a$ i $\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1 = b$, po podstawieniu $\alpha_3 = -a/3$ i uproszczeniu, dają równości $\alpha_1 + \alpha_2 = -2a/3$ i $\alpha_2\alpha_3 = b - 2a^2/9$, które pokazują, zob. T3.9, że α_1, α_2 są pierwiastkami trójmianu kwadratowego $X^2 + \frac{2a}{3}X + \left(b - \frac{2a^2}{9}\right)$. Ten trójmian ma wyróżnik $\Delta = 4a^2/9 - 4(b - 2a^2/9) = (4/3)(a^2 - 3b)$. Drugim poszukiwanym warunkiem jest więc nierówność $(**)\, a^2 \geqslant 3b$.

Z3.E10 Załóżmy, że $X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ jest unormowanym (± 1)-wielomianem i że $\alpha_1, \ldots, \alpha_n$ są jego pierwiastkami rzeczywistymi. Wówczas, przy $n \geqslant 2$,

$$1 - 2c_{n-2} = c_{n-1}^2 - 2c_{n-2} = \alpha_1^2 + \cdots + \alpha_n^2 \geqslant n \sqrt[n]{\alpha_1^2 \cdot \ldots \cdot \alpha_n^2} = nc_0^{2/n} = n.$$

Druga i trzecia równość wynikają ze wzorów Viète'a, nierówność jest nierównością AG, a pierwsza i czwarta równość wynika z założenia $c_i = \pm 1$. Otrzymana nierówność $1 - 2c_{n-2} \geqslant n$ implikuje równość $c_{n-2} = -1$ i nierówność $n \leqslant 3$. Wystarczy teraz sprawdzić, że wielomiany $X - 1$, $X + 1$, $X^2 - X - 1$, $X^2 + X - 1$ oraz $X^3 - X^2 - X + 1$ i $X^3 + X^2 - X - 1$ są dobre. Dalszych sześć dobrych wielomianów dostaniemy biorąc wielomiany przeciwne do wypisanych.

Z3.E11 Żądany ciąg budujemy i n d u k c y j n i e. Niech $a_0 = -1$, $a_1 = 1$. Ponieważ wielomian $a_0 + a_1X = -1 + X$ ma pierwiastek rzeczywisty, więc początek (indukcji) jest zrobiony. Dla zrobienia kroku indukcyjnego załóżmy, że mamy wielomian $f_n(X) := a_0 + a_1X + \cdots + a_nX^n$ mający n różnych pierwiastków rzeczywistych $\lambda_1 < \lambda_2 < \cdots < \lambda_n$ i spełniający (dodatkowo) warunek $(-1)^{n-1}a_n > 0$. Ustalamy takie liczby $c_0, c_1, \ldots, c_n$, że $c_0 < \lambda_1 < c_1 < \lambda_2 < \cdots < c_{n-1} < \lambda_n < c_n$. Wówczas, oczywiście, $f_n(c_0) < 0$, $f_n(c_1) > 0$, $f_n(c_2) < 0$, itd (ciąg oscylujący wokół zera). Oznaczmy

$$M = \max\{|f_n(c_0)|, |f_n(c_1)|, \ldots, |f_n(c_n)|\}.$$

Dobieramy taką liczbę a_{n+1}, by: (1) $a_na_{n+1} < 0$, (2) $|a_{n+1}| < M/(2|c_k^{n+1}|)$ dla każdego $k = 0, 1, \ldots, n$. To jest możliwe! Wówczas wielomian $f_{n+1}(X) := f_n(X) + a_{n+1}X^{n+1}$ dla argumentów c_k przyjmuje wartości tych samych znaków co wielomian $f_n(X)$ (ma więc pierwiastki w każdym przedziale $(c_k; c_{k+1})$, zob. 3.2.6 U2). Łatwo też uzasadnić istnienie jeszcze jednego pierwiastka na prawo od c_n.

Z3.E12 Piszemy rozkład (3.34) (pamiętamy, że $C = 1$). Kładziemy $X = i$ i liczymy moduł:

$$1 > |f(i)| = |i - a_1|^{e_1} \cdot \ldots \cdot |i - a_r|^{e_r} \cdot |(i - b_1)^2 + c_1^2|^{d_1} \cdot \ldots \cdot |(i - b_s)^2 + c_s^2|^{d_s}.$$

Ponieważ czynniki $|i-a_k|^{e_k}$ są $\geqslant 1$ (moduł $|i-a_k|$ jest odległością liczby r z e c z y w i s t e j a_k od liczby $i=\sqrt{-1}$), więc co najmniej jeden z czynników $|(i-b_l)^2+c_l^2|$ musi być <1. Liczba zespolona $b+ic=b_l+ic_l$ jest pierwiastkiem czynnika $(X-b_l)^2+c_l^2$ wielomianu $f(X)$, więc jest też, oczywiście, pierwiastkiem tego wielomianu. Mamy więc $1>|(i-b)^2+c^2|^2=[(i-b)^2+c^2]\cdot[(-i-b)^2+c^2]=[c^2+b^2+1-2bi]\cdot[c^2+b^2+1+2bi]$, co jest dowodzoną nierównością.

Z3.E13 Z założeń wynika istnienie takiego $1\leqslant k<n$, że $r_{n-k}>0$. Wówczas

$$\frac{x^n-r(x)}{x^n}=\frac{r_{n-1}}{x}+\frac{r_{n-2}}{x^2}+\cdots+\frac{r_1}{x^{n-1}}+\frac{r_0}{x^n}\geqslant\frac{r_{n-k}}{x^k}>1$$

dla dowolnego $0<x<\sqrt[k]{r_{n-k}}$. Stąd wynika, że $r(x)<0$ dla wszystkich tych x. Z drugiej strony, dla $x>\max\{nr_{n-1},\sqrt[2]{nr_{n-2}},\dots,\sqrt[n-1]{nr_1},\sqrt[n]{nr_0}\}$ mamy $x^n=x^k\,x^{n-k}>nr_{n-k}x^{n-k}$ przy każdym $k=1,\dots,n$, skąd, po zsumowaniu, $nx^n>n\sum_{k=1}^n r_{n-k}x^{n-k}$. Więc $r(x)>0$ dla tych x. Przysługująca wielomianom rzeczywistym własność Darboux pokazuje więc istnienie pierwiastka dodatniego ϱ. Ponadto, jeżeli $x>\varrho$, to

$$\frac{r(x)}{x^n}=\frac{r(x)}{x^n}-\frac{r(\varrho)}{\varrho^n}=[1-\sum_{k=1}^n r_{n-k}x^{-k}]-[1-\sum_{k=1}^n r_{n-k}\,\varrho^{-k}]=\sum_{k=1}^n r_{n-k}\left(\frac{1}{\varrho^k}-\frac{1}{x^k}\right)>0,$$

czyli $r(x)>0$ dla wszystkich takich x. Jasne, że to kończy rozwiązanie.

Z3.E14 (*Nierówność lewa*) Równość $f(\lambda)=0$ zapisujemy tak: $-\lambda^n=a_{n-1}\lambda^{n-1}+\cdots+a_1\lambda+a_0$. Stąd, na mocy C1.23,

$$|\lambda|^n=|-\lambda^n|=|a_{n-1}\lambda^{n-1}+\cdots+a_1\lambda+a_0|\leqslant|a_{n-1}|\cdot|\lambda|^{n-1}+\cdots+|a_1|\cdot|\lambda|+|a_0|.$$

Otrzymaną nierówność zapiszmy w postaci $r(x)=x^n-(r_{n-1}x^{n-1}+\cdots+r_1x+r_0)\leqslant 0$, gdzie położyliśmy $x=|\lambda|$ i $r_s=|a_s|$ dla $s=0,\dots,n-1$. Dowodzona nierówność jest oczywista, gdy $\lambda=0$. Załóżmy więc, że $\lambda\neq 0$, czyli $f(X)\neq X^n$. Wówczas, jak wiemy z Z3.E13, nierówność $r(x)\leqslant 0$ może zachodzić tylko, gdy $x\leqslant\varrho_0$. Mamy więc nierówność $|\lambda|\leqslant\varrho_0$ dla każdego niezerowego pierwiastka wielomianu $f(X)$. (*Nierówność prawa*) Niech $b=2\max\{\sqrt[k]{|a_{n-k}|}:k=1,\dots,n\}$. Wówczas $b\geqslant 2\sqrt[k]{|a_{n-k}|}$ dla każdego $k=1,\dots,n$, czyli $|a_{n-k}|\leqslant b^k/2^k$. Stąd

$$r(b)=b^n-|a_{n-1}|b^{n-1}-\cdots-|a_1|b-|a_0|\geqslant b^n\left(1-\frac{1}{2}-\frac{1}{2^2}-\cdots-\frac{1}{2^n}\right)=\frac{b^n}{2^n}.$$

Więc $r(b)>0$, gdy $b>0$ (zauważmy, że równość $b=0$ może zachodzić tylko, gdy $f(X)=X^n$, a wtedy wszystko jest oczywiste). Wobec tezy Z3.E13, oznacza to, że $b>\varrho_0$.

Z3.E15 Niech $A_k:=\frac{a_k}{a_n}$ dla $0\leqslant k<n$. Wielomian $g(X)=A_0+A_1X+\cdots+A_{n-1}X^{n-1}+X^n$ ma oczywiście te same pierwiastki co $f(X)$. Poza tym $M=\max\{|A_0|,\dots,|A_{n-1}|\}$.

(1) Jeżeli $|\lambda|\leqslant 1$, to teza jest prawdziwa. Załóżmy więc, że dla pewnego pierwiastka λ wielomianu $f(X)$ zachodzi $|\lambda|>1$. Równość $-\lambda^n=A_0+A_1\lambda+\cdots+A_{n-1}\lambda^{n-1}$ jest inaczej zapisaną równością $g(\lambda)=0$. Stąd, na mocy C1.23 i tożsamości nieśmiertelnej,

$$|\lambda|^n=\left|A_0+\cdots+A_{n-1}\lambda^{n-1}\right|\leqslant M(1+|\lambda|+\cdots+|\lambda|^{n-1})=M\,\frac{|\lambda|^n-1}{|\lambda|-1}<M\,\frac{|\lambda|^n}{|\lambda|-1}.$$

Przeto $|\lambda|-1<M$.

(2) Niech $\lambda\neq 0$ będzie pierwiastkiem $g(X)$. Równość $g(\lambda)=0$ zapisujemy tak:

$$1+\frac{A_{n-1}}{\lambda}=\frac{-A_{n-2}}{\lambda^2}+\frac{-A_{n-3}}{\lambda^3}+\ \dots\ +\frac{-A_0}{\lambda^n}.$$

Stąd, na mocy nierówności trójkąta z C1.23 i nierówności $|-A_k| \leqslant M$,

$$\left|1+\frac{A_{n-1}}{\lambda}\right| \leqslant \frac{|-A_0|}{|\lambda^n|}+\frac{|-A_1|}{|\lambda^{n-1}|}+\ldots+\frac{|-A_{n-2}|}{|\lambda^2|} \leqslant \frac{M}{|\lambda|^2}\left(\frac{1}{|\lambda|^{n-2}}+\frac{1}{|\lambda|^{n-3}}+\ldots+1\right).$$

Załóżmy teraz, że $|\lambda|>1$. Wówczas suma w nawiasie z prawej strony jest (ściśle) mniejsza niż suma $1/(1-q)$ zbieżnego szeregu geometrycznego $\sum_{k\geqslant 0} q^k$ o ilorazie $q=1/|\lambda|<1$. Mamy więc nierówność $|1+A_{n-1}/\lambda| < M/(|\lambda|^2-|\lambda|)$. Z drugiej strony mamy (geometrycznie) oczywistą nierówność $\operatorname{Re} z \leqslant |z|$ dla każdej liczby zespolonej (algebraicznie jest ona oczywistą nierównością $a \leqslant \sqrt{a^2+b^2}$). To daje

$$1+\operatorname{Re}\frac{A_{n-1}}{\lambda} = \operatorname{Re}\left(1+\frac{A_{n-1}}{\lambda}\right) \leqslant \left|1+\frac{A_{n-1}}{\lambda}\right| < \frac{M}{|\lambda|^2-|\lambda|}.$$

Teraz wykorzystamy założenie $\operatorname{Re}\lambda \geqslant 0$. Wówczas $\operatorname{Re}(A_{n-1}/\lambda) \geqslant 0$ (bo $A_{n-1} \geqslant 0$). Dostajemy więc nierówność $1 < M/(|\lambda|^2-|\lambda|)$, czyli nierówność $|\lambda|^2-|\lambda|-M<0$, która oznacza, że liczba $|\lambda|$ leży między pierwiastkami $\frac{1-\sqrt{1+4M}}{2}$ i $\frac{1+\sqrt{1+4M}}{2}$ trójmianu kwadratowego x^2-x-M.

Z3.F1 Jeżeli $\alpha \notin \mathbb{Z}$ i $f_i(\alpha)=0$, to $\alpha \notin \mathbb{Q}$, zob. T3.5. Równość $\alpha^2+a_1\alpha+b_1 = \alpha^2+a_2\alpha+b_2\,(=0)$ daje $(a_1-a_2)\alpha = b_2-b_1$. Stąd, w przypadku $a_1-a_2\neq 0$, dostalibyśmy równość $\alpha=(b_2-b_1)/(a_1-a_2)$. Ale ona jest niemożliwa, bo $\alpha\notin\mathbb{Q}$. Więc $a_1=a_2$. Stąd też $b_1=b_2$.

Z3.F2 Niech $f(\alpha)=g(\alpha)=0$ i niech $d(X)=\operatorname{NWD}(f(X),g(X))$. Wtedy, zobacz T3.11, $d(X)=f(X)s(X)+g(X)t(X)$. Zatem $d(\alpha)=f(\alpha)s(\alpha)+g(\alpha)t(\alpha)=0$, zob. Z1.6. Odwrotnie, jeżeli $d(\alpha)=0$, to, ponieważ $d(X)|f(X)$, czyli $f(X)=d(X)k(X)$, więc $f(\alpha)=d(\alpha)k(\alpha)=0$. I, podobnie, $g(\alpha)=0$.

Z3.F3 (1) W rozwiązaniu zadania Z3.9 widzieliśmy, że $R(f_1,f_2)=f_1(\varphi_2)f_1(\psi_2)$, gdzie φ_2,ψ_2 oznaczają pierwiastki trójmianu $f_2(X)$. Tak samo sprawdzamy, że $R(f_1,f_2)=f_2(\varphi_1)f_2(\psi_1)$. To kończy dowód tezy (1). Przechodzimy do tezy **(2)**. Warunek $R(f_1,f_2)<0$ oznacza, w szczególności, że $a_1\neq a_2$. Liczymy wartości $f_1(\xi)$, $f_2(\xi)$ przy $\xi=(b_2-b_1)/(a_1-a_2)$:

$$f_1(\xi)=\left(\frac{b_2-b_1}{a_1-a_2}\right)^2+a_1\frac{b_2-b_1}{a_1-a_2}+b_1=\frac{R(f_1,f_2)}{(a_1-a_2)^2}=\left(\frac{b_2-b_1}{a_1-a_2}\right)^2+a_2\frac{b_2-b_1}{a_1-a_2}+b_2=f_2(\xi).$$

Zatem $f_1(\xi)=R(f_1,f_2)/(a_1-a_2)^2<0$. To dowodzi, że $f_(X)$ ma d w a pierwiastki rzeczywiste (leżące po różnych stronach ξ). Również $f_2(X)$ ma dwa różne pierwiastki. Ponadto, nierówność $f_1(\varphi_2)f_1(\psi_2)<0$ dowodzi, na mocy T3.7(3), że jeden pierwiastek trójmianu $f_1(X)$ leży gdzieś między φ_2 a ψ_2. I wzajemnie.

Z3.F4 Niech $d(X)\in\mathbb{Q}[X]$ oznacza największy wspólny dzielnik wielomianów $f(X)$ i $g(X)$. Wówczas, zobacz Z3.F2, $d(\alpha)=0$. Podkreślamy wyraźnie i mocno, że $d(X)$ ma współczynniki wymierne! Wielomian stopnia $\leqslant 1$ o współczynnikach wymiernych n i e ma pierwiastków niewymiernych! Zatem $\deg d(X)\geqslant 2$. Jeżeli $\deg d(X)=2$, to drugi pierwiastek β wielomianu $d(X)$ jest wspólnym pierwiastkiem wielomianów $f(X)$, $g(X)$. Ponadto, $\beta\neq\alpha$ (gdyby $\beta=\alpha$, to, ponieważ $\alpha+\beta$ jest, na mocy wzoru Viète'*a*, liczbą wymierną, więc i α byłaby liczbą wymierną, wbrew założeniu). Pozostał nam do rozważenia przypadek, gdy $\deg d(X)=3$. Wówczas $f(X)\sim g(X)\sim d(X)$, więc k a ż d y pierwiastek wielomianu $f(X)$ jest też pierwiastkiem wielomianu $g(X)$. Mamy więc rozkłady $f(X)=a(X-\alpha)(X-\beta)(X-\gamma)$ i $g(X)=b(X-\alpha)(X-\beta)(X-\gamma)$ dla pewnych liczb wymiernych a,b i pewnych liczb z e s p o l o n y c h β,γ. Gdyby $\beta=\alpha=\gamma$, to, na mocy wzoru Viète'*a*, byłoby $3\alpha=\alpha+\beta+\gamma\in\mathbb{Q}$, więc i $\alpha\in\mathbb{Q}$, co nie ma miejsca. Musi być więc $\beta\neq\alpha$ lub $\gamma\neq\alpha$. To p r a w i e kończy rozwiązanie zadania.

Z3.F5 Jeżeli $c=k^3$, to $f(k)=0$ dla $f(X)=X(X-k)=X^2-kX$. Dla dowodu wynikania odwrotnego, załóżmy, że $f(\sqrt[3]{c})=0$, gdzie $f(X)\in\mathbb{Z}[X]$ i $\deg f(X)=2$. Wówczas $\sqrt[3]{c}$ jest

wspólnym pierwiastkiem wielomianu $f(X)$ i wielomianu X^3-c. Dzieląc (z resztą) X^3-c przez $f(X)$, dostajemy równość $X^3-c=q(X)f(X)+r(X)$, gdzie $r(X)$ jest wielomianem stopnia $\leqslant 1$ o współczynnikach wymiernych. Obliczając wartość wielomianów z obu stron tej równości dla argumentu $\sqrt[3]{c}$, dostajemy równość $r(\sqrt[3]{c})=0$. Czyli, ponieważ $r(X)=aX+b\in\mathbb{Q}[X]$, $\sqrt[3]{c}=-b/a\in\mathbb{Q}$. Wystarczy się teraz powołać na C2.19.

Z3.G0 $(-\alpha-\beta-\gamma)^2\geqslant 3(\alpha\beta+\beta\gamma+\gamma\alpha)\iff \frac{1}{2}(\alpha-\beta)^2+\frac{1}{2}(\beta-\gamma)^2+\frac{1}{2}(\gamma-\alpha)^2\geqslant 0.$

Z3.G1 Zauważmy najpierw, że $a\neq 0$ (gdy $a=0$, to wielomian $f(X)=bX+b$ ma trzy pierwiastki tylko, gdy jest wielomianem zerowym ($b=0$), ale wówczas ma więcej niż trzy pierwiastki). Zauważmy teraz, że żaden z pierwiastków α, β, γ nie jest równy 0. W przeciwnym razie, na mocy wzoru Viète'a $b=-a\alpha\beta\gamma=0$ i wtedy $f(X)=aX^3-aX^2$ wprawdzie ma trzy pierwiastki, ale n i e są one różne (pierwiastek 0 jest podwójny). Reszta rozwiązania jest natychmiastowa: Ze wzorów Viète'a wiemy, że $\alpha+\beta+\gamma=1$, $\alpha\beta+\beta\gamma+\gamma\alpha=\frac{b}{a}$ i $\alpha\beta\gamma=-\frac{b}{a}$. Stąd: $\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}=\frac{\beta\gamma+\gamma\alpha+\alpha\beta}{\alpha\beta\gamma}=-1$.

Z3.G2 Niech, jak zwykle, $f(X)=(X-a)(X-b)(X-c)(X-d)=X^4-\sigma_1X^3+\sigma_2X^2-\sigma_3X+\sigma_4$. Równość $f(a)=0$ zapisujemy tak: $a^4=\sigma_1a^3-\sigma_2a^2+\sigma_3a-\sigma_4$. Podobnie zapisujemy równości $f(b)=0$, $f(c)=0$ i $f(d)=0$. Dodając otrzymane cztery równości stronami dostajemy:

$$a^4+b^4+c^4+d^4=\sigma_1(a^3+b^3+c^3+d^3)-\sigma_2(a^2+b^2+c^2+d^2)+\sigma_3(a+b+c+d)-4\sigma_4.$$

Stąd, i z założeń $m|\sigma_1$, $m|a^2+b^2+c^2+d^2$, natychmiast mamy tezę. U w a g a. Podobnie dowodzimy, że jeżeli liczba naturalna m dzieli sumę pięciu liczb całkowitych i sumę ich kwadratów, to suma piątych potęg tych liczb daje tę samą resztę co pięciokrotność ich iloczynu przy dzieleniu przez m.

Z3.G3 Nierówność lewa jest oczywista: $2\alpha\beta\gamma\leqslant 3\alpha\beta\gamma\leqslant\alpha\beta\gamma+\alpha\beta\gamma+\alpha\beta\gamma\leqslant\alpha\beta+\beta\gamma+\gamma\alpha$. Dla dowodu prawej badamy wielomian $f(X)=(X-\alpha)(X-\beta)(X-\gamma)=X^3-X^2+qX+r$. Mamy udowodnić, że $q+2r\leqslant\frac{7}{27}$, lub, co jest równoważne, że $(\frac{1}{2}-\alpha)(\frac{1}{2}-\beta)(\frac{1}{2}-\gamma)=f(\frac{1}{2})\leqslant\frac{1}{216}$. Otóż, gdy któryś (co najwyżej jeden(!)) z pierwiastków jest $\geqslant\frac{1}{2}$, mamy $f(\frac{1}{2})\leqslant 0\leqslant\frac{1}{216}$, gdy zaś wszystkie są $<1/2$, to, stosując nierówność AG, mamy $\sqrt[3]{f(1/2)}\leqslant\frac{1}{3}\left((\frac{1}{2}-\alpha)+(\frac{1}{2}-\beta)+(\frac{1}{2}-\gamma)\right)=\frac{1}{6}$.

Z3.G4 Założenia $a|b^2+1$ i $b|a^2+1$ dają podzielność $ab|(a^2+1)(b^2+1)$ czyli $ab|a^2b^2+a^2+b^2+1$, więc (zob. Zasada Podstawowa) $ab|a^2+b^2+1$. Teraz patrz C3.17.

Z3.G5 Niech $\alpha=\frac{a}{b}$, $\beta=\frac{b}{c}$ i $\gamma=\frac{c}{a}$. Wówczas $\alpha+\beta+\gamma\in\mathbb{Z}$, $\alpha\beta\gamma=1\in\mathbb{Z}$. A także $\alpha\beta+\beta\gamma+\gamma\alpha=\frac{a}{c}+\frac{b}{a}+\frac{c}{b}$ jest liczbą całkowitą. Zatem wielomian $(X-\alpha)(X-\beta)(X-\gamma)$ ma współczynniki całkowite, jest unormowany i ma pierwiastki wymierne α, β, γ. Zatem, zobacz T3.5, α, β, γ są liczbami całkowitymi. Czyli $b|a$, $c|b$ i $a|c$. Więc $|b|\leqslant|a|\leqslant|c|\leqslant|b|$. Stąd teza.

Z3.G6 Udowodnimy twierdzenie ogólniejsze: *Jeżeli $m,n\in\mathbb{N}$ są liczbami nieparzystymi, a α, β, γ są takimi liczbami, że wszystkie napisane ułamki mają sens (tzn., mianowniki są różne 0), to*

$$\frac{1}{\alpha^m+\beta^m+\gamma^m}=\frac{1}{\alpha^m}+\frac{1}{\beta^m}+\frac{1}{\gamma^m}\iff\frac{1}{\alpha^n+\beta^n+\gamma^n}=\frac{1}{\alpha^n}+\frac{1}{\beta^n}+\frac{1}{\gamma^n}.\qquad(*)$$

Niech $f(X)=(X-\alpha^m)(X-\beta^m)(X-\gamma^m)=X^3-pX^2+qX-r$ będzie wielomianem, którego pierwiastkami są α^m, β^m, γ^m. Załóżmy, że zachodzi równość $\frac{1}{\alpha^m+\beta^m+\gamma^m}=\frac{1}{\alpha^m}+\frac{1}{\beta^m}+\frac{1}{\gamma^m}$. Zapisujemy ją w postaci $\frac{1}{-p}=\frac{q}{-r}$, czyli $r=pq$. Stąd $f(X)=X^3-pX^2+qX-pq=X^2(X-p)+q(X-p)=(X-p)(X^2+q)$. Widać, że $p=\alpha^m+\beta^m+\gamma^m$ jest pierwiastkiem wielomianu $f(X)$. Ale jedynymi pierwiastkami wielomianu $f(X)$ są α^m, β^m, γ^m, więc suma $\alpha^m+\beta^m+\gamma^m$ jest równa jednej z liczb α^m, β^m, γ^m. Zatem suma pewnych dwóch z liczb α^m, β^m, γ^m jest równa 0, na przykład $\alpha^m+\beta^m=0$. Więc (tu korzystamy z założenia nieparzystości m) $\alpha=-\beta$. Wówczas, oczywiście, zachodzi równość z lewej strony $(*)$.

Z3.G7 Znowu *filozofia Viète'*a! Niech $(x_1, \ldots, x_n)$ będzie rozwiązaniem i niech $f(X)$ będzie odpowiednim wielomianem: $f(X) = (X - x_1) \cdot \ldots \cdot (X - x_1) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Mnożąc k-tą równość przez a_{k-1} (pamiętamy, że $a_n = 1$) i dodając, dostajemy równość

$$0 = f(x_1) + f(x_2) + \cdots + f(x_n) = na_0 + na_1 + \cdots + na_{n-1} + n = nf(1).$$

Stąd widzimy, że liczba 1 jest pierwiastkiem wielomianu $f(X)$. Czyli: k t ó r e ś x_j jest równe 1. Oczywista indukcja pokazuje więc, że $(x_1, \ldots, x_n) = (1, \ldots, 1)$.

Z3.G8 Niech $\mathcal{B}(k) := \{(x, y) \in \mathbb{N} \times \mathbb{N} : x^2 + y^2 = k(xy - 1)\}$. (1) Pokaż, że $\mathcal{B}(1) = \mathcal{B}(2) = \varnothing$. Załóż więc, że $k \geqslant 3$ i że $\mathcal{B}(k) \neq \varnothing$. (2) Ze wszystkich par (x, y) należących do $\mathcal{B}(k)$ wybierz (Zasada Minimum!) parę o najmniejszym y. Niech (a, b_0) będzie taką parą. (3) Wykaż, że $a \neq b_0$, więc $a > b_0$. (4) Rozważ trójmian $f(X) = X^2 - kb_0X + b_0^2 + k$ i wykonaj *skok Viète'*a $a \mapsto \widetilde{a}$. (5) Wykaż, że $\widetilde{a} \neq a$ (wyróżnik trójmianu $f(X)$ jest niezerowy!). Załóż (b.s.o.), że $b_0 < a < \widetilde{a}$. (6) Z równości Viète'*a* $(a + \widetilde{a} = kb_0,\ a\widetilde{a} = b_0^2 + k)$ wywnioskuj, że $b_0^2 + k - kb_0 = (a - 1)(\widetilde{a} - 1) - 1 \geqslant b_0(b_0 + 1) - 1$. Dostaniesz stąd nierówność $(b_0 - 1)(k + 1) \leqslant 0$, z której łatwo zobaczyć, że $b_0 = 1$. (7) Więc $a + \widetilde{a} = k$, $a\widetilde{a} = k + 1$, skąd natychmiast dostaniesz $a = 2$, $\widetilde{a} = 3$, $k = 5$. U w a g a. $(321, 67) \in \mathcal{B}(5)$.

Z3.H1 Nieujemność współczynników implikuje ujemność (ścisłą, bo $a_0 = 1$) pierwiastków. Niech $-\alpha_i$, przy $i = 1, \ldots, n$, będą tymi pierwiastkami. Wówczas $f(x) = (x+\alpha_1)\cdot\ldots\cdot(x+\alpha_n)$ dla każdego $x \in \mathbb{R}$. Zatem $f(2) = (2 + \alpha_1) \cdot \ldots \cdot (2 + \alpha_n)$. Ale $2 + \alpha_i = 1 + 1 + \alpha_i \geqslant 3\sqrt[3]{1 \cdot 1 \cdot \alpha_i}$ (nierówność AG). To, po wymnożeniu i wykorzystaniu równości Viète'*a* $\alpha_1 \cdot \ldots \cdot \alpha_n = 1$, daje tezę.

Z3.H2 Napiszmy wielomian interpolacyjny dla argumentów $\alpha_k = s_k$ i wartości $\beta_k = f(s_k)$, zob. T3.23. Wówczas

$$g_k(X) = \frac{(X - s_0)(X - s_1) \cdot \ldots \cdot (X - s_n)}{(s_k - s_0)(s_k - s_1) \cdot \ldots \cdot (s_k - s_n)} =: \prod_{j \neq k} \frac{X - s_j}{s_k - s_j},$$

gdzie w liczniku jest opuszczony czynnik $(X - s_k)$, a w mianowniku czynnik $(s_k - s_k)$. Widać stąd, że wielomian (n-tego stopnia) $g_k(X)$ ma współczynnik $(g_k)_n$ przy X^n równy $\prod_{j \neq k} (s_k - s_j)^{-1}$. Oszacujemy wartość tego współczynnika. Łatwo widać, że założenia $s_0 < s_1 < \cdots < s_n$ i $s_k \in \mathbb{Z}$, implikują nierówności $|s_k - s_j| \geqslant |k - j|$. Stąd

$$|(g_k)_n| = \prod_{j \neq k} \frac{1}{|s_k - s_j|} = \prod_{j<k} \frac{1}{|s_k - s_j|} \cdot \prod_{j>k} \frac{1}{|s_k - s_j|} \leqslant \prod_{j<k} \frac{1}{|k - j|} \cdot \prod_{j>k} \frac{1}{|k - j|} = \frac{1}{k!(n - k)!}.$$

Jak zwykle, iloczyn pusty (bez czynników) uznajemy za równy 1 (por. równość $0! = 1$). Załóżmy teraz, nie wprost, że dla każdego $k = 0, \ldots, n$ zachodzi nierówność $|f(s_k)| < n!/2^n$. Wówczas, ponieważ zachodzi równość $f(X) = \sum_{k=0}^n f(s_k)g_k(X)$, zobacz tezę o jednoznaczności w T3.23, z której wynika równość $1 = \sum_{k=0}^n f(s_k)(g_k)_n$ (bo $f(X)$ jest unormowany), mamy

$$1 = |\sum_{k=0}^n f(s_k)(g_k)_n| \leqslant \sum_{k=0}^n |f(s_k)| \cdot |(g_k)_n| < \sum_{k=0}^n \frac{n!}{2^n} \cdot \frac{1}{k!(n - k)!} = \frac{1}{2^n} \cdot \sum_{k=0}^n \binom{n}{k} = \frac{2^n}{2^n} = 1.$$

Uzyskana sprzeczność kończy rozwiązanie.

Z3.H3 Wykorzystamy twierdzenie T3.23. Dzięki niemu (wybierając $\alpha_k = k - n$, $\beta_k = f(k)$, przy $0 \leqslant k \leqslant 2n$) zapisujemy wielomian $f(X)$ w postaci $f(X) = \sum_{k=-n}^n f(k)g_k(X)$, gdzie

$$g_k(X) = \prod_{j \neq k} \frac{X - j}{k - j} = \frac{\prod_{j=-n}^{k-1} (X - j) \cdot \prod_{j=k+1}^n (X - j)}{\prod_{j=-n}^{k-1} (k - j) \cdot \prod_{j=k+1}^n (k - j)} = \frac{\prod_{j=-n}^{k-1} (X - j) \cdot \prod_{j=k+1}^n (X - j)}{(n + k)! \cdot (-1)^{n-k}(n - k)!}.$$

Weźmy teraz dowolną liczbę $x \in [-n; n]$ i oszacujmy licznik ułamka $g_k(x)$. Jego wartość bezwzględna jest równa iloczynowi $2n$ czynników $\prod_{j=-n}^{k-1} |x-j| \cdot \prod_{j=k+1}^{n} |x-j|$, które można ustawić według "wzrostu". W ten sposób łatwo widzieć, że jest on $\leqslant (2n)!$. Podsumowując otrzymamy:

$$|f(x)| \leqslant \sum_{k=-n}^{n} |f(k)| \cdot |g_k(x)| \leqslant \sum_{k=-n}^{n} \frac{(2n)!}{(n+k)!(n-k)!} = \sum_{l=0}^{2n} \binom{2n}{l} = (1+1)^{2n} = 2^{2n}.$$

Z3.H4 B.s.o. zakładamy, że $a \geqslant 0$ (gdy $a < 0$ możemy zamiast wielomianu $f(X) := aX^2+bX+c$ patrzeć na wielomian $-f(X)$). Również możemy założyć, że $b \geqslant 0$ (gdy $b < 0$ możemy patrzeć na wielomian $f(-X)$). Mamy $|f(-1)| \leqslant 1$, $|f(0)| \leqslant 1$ i $|f(1)| \leqslant 1$, czyli $|a-b+c| \leqslant 1$, $|c| \leqslant 1$ i $|a+b+c| \leqslant 1$. Stąd wyprowadzamy dwie nierówności: (i) $|a+b| \leqslant 2$, (ii) $|a-b| \leqslant 2$. Rzeczywiście: $|a+b| = |a+b+c-c| \leqslant |a+b+c| + |-c| \leqslant 2$ i $|a-b| = |a-b+c-c| \leqslant |a-b+c| + |-c| \leqslant 2$. Załóżmy teraz, że $c \geqslant 0$. Wówczas $0 \leqslant cx^2 \leqslant c$ dla $|x| \leqslant 1$. I mamy:

$$-2 \leqslant a-b = 0-b+c \leqslant cx^2+bx+a \leqslant c+b+a = f(1) \leqslant 1 \leqslant 2,$$

gdzie pierwsza nierówność wynika z (ii), a druga z oczywistej (przy $|x| \leqslant 1$) nierówności $-b \leqslant bx \leqslant b$. Podobnie działamy w przypadku $c \leqslant 0$ (wtedy $c \leqslant cx^2 \leqslant 0$):

$$-2 \leqslant -1 \leqslant f(-1) = a-b+c \leqslant a+bx+cx^2 \leqslant a+b+0 \leqslant 2.$$

Koniec! U w a g a. Nierówności $|cX^2+bx+a| \leqslant 2$ nie da się polepszyć. Przykład: $f(X) = 2X^2-1$.

Z3.H5 Wielomian $f(X) = \frac{1}{2}[(2X-1)^n+1]$ przy dostatecznie dużych n, j e s t dobry.

Z3.I1 Oznaczmy $f_n(X) = (X+1)^{2n+1} + X^{n+2}$ i $\Phi_3(X) = X^2+X+1$. S p o s ó b 1. Indukcja względem n. Wygodnie ją zacząć od $n = 0$. Wtedy baza indukcji jest oczywista. Załóżmy więc, że $\Phi_3(X) | f_n(X)$ i zapiszmy $f_n(X) = g(X)\Phi_3(X)$. Wówczas

$$f_{n+1}(X) = (X+1)^2[f_n(X) - X^{n+2}] + X^{n+3} = (X+1)^2 g(X)\Phi_3(X) + X^{n+2}[X-(X+1)^2].$$

Ponieważ $X-(X+1)^2 = -\Phi_3(X)$, więc koniec. S p o s ó b 2. Sprawdzamy, że $\omega = \omega_3$ jest pierwiastkiem wielomianu $f_n(X)$. Korzystamy z twierdzenia o strażakach. Mamy więc $\omega+1 = -\omega^2$. Stąd $f_n(\omega) = (\omega+1)^{2n+1} + \omega^{n+2} = (-\omega^2)^{2n+1} + \omega^{n+2} = -\omega^{4n+2} + \omega^{n+2} = -\omega^{3n}\omega^{n+2} + \omega^{n+2} = -\omega^{n+2} + \omega^{n+2} = 0$. Równie łatwo widać, że $f_n(\omega^2) = 0$. Zatem $(X-\omega)(X-\omega^2) = \Phi_3(X)$ dzieli $f_n(X)$. Zobacz też Z3.20.

Z3.I2 Rozkładamy wielomian $d(X) = X^2 - 2(\cos\varphi)X + 1$ na czynniki nierozkładalne. Ponieważ $\Delta = 4\cos^2\varphi - 4 = -4\sin^2\varphi$, więc $\sqrt{\Delta} = 2i\sin\varphi$. Wobec tego pierwiastkiem wielomianu $d(X)$ jest liczba $\alpha = \cos\varphi + i\sin\varphi$ i, zobacz też 3.4.4 L3.2, liczba sprzężona $\overline{\alpha} = \cos\varphi - i\sin\varphi$. Mamy więc $d(X) = (X-\alpha)(X-\overline{\alpha})$. Ponieważ $\alpha \neq \overline{\alpha}$ (bo, przy narzuconych założeniach, α nie jest liczbą rzeczywistą), więc wielomiany $X-\alpha$ i $X-\overline{\alpha}$ są względnie pierwsze. Dla wykazania podzielności $d(X) | f(X)$, gdzie $f(X) = (\sin\varphi)X^n - (\sin n\varphi)X + \sin(n-1)\varphi$, wystarczy więc sprawdzić, że zarówno $X-\alpha | f(X)$ jak i $X-\overline{\alpha} | f(X)$. Czyli, że zarówno $f(\alpha) = 0$ jak i $f(\overline{\alpha}) = 0$, zobacz T3.2. Ponieważ, zobacz 3.4.4 L3.2, druga równość jest wnioskiem z pierwszej, więc sprawdzamy tylko tę pierwszą. Korzystamy przy tym ze wzoru de Moivre'a, zobacz (1.14). Mamy

$$f(\alpha) = \sin\varphi(\cos n\varphi + i\sin n\varphi) - \sin n\varphi(\cos\varphi + i\sin\varphi) + \sin(n-1)\varphi = 0,$$

co jest równoważne równości $\sin(n-1)\varphi = \sin n\varphi\cos\varphi - \sin\varphi\cos n\varphi$.

Z3.I3 Rozkładamy, zgodnie z C3.50, wszystkie występujące wielomiany X^a-1 na czynniki cyklotomiczne. Wówczas dostaniemy

$$I(a;\, k) := (X^{a+1}-1)(X^{a+2}-1)\cdot\ldots\cdot(X^{a+k}-1) = \prod_{j=1}^{k} \prod_{d | a+j} \Phi_d(X)$$

dla dowolnej liczby naturalnej a. Zastanawiamy się ile razy dany wielomian $\Phi_d(X)$ występuje jako czynnik w iloczynie z prawej strony tej równości. Odpowiedź jest jasna: tyle razy ile jest wyrazów podzielnych przez d w ciągu $(a+1,\, a+2,\, \ldots,\, a+k)$. Ponieważ wyrazów podzielnych przez d w ciągu $(1,\, 2,\, \ldots,\, a+k)$ jest, oczywiście, dokładnie $\lfloor (a+k)/d \rfloor$, a wyrazów podzielnych przez d w ciągu $(1,\, 2,\, \ldots,\, a)$ jest $\lfloor a/d \rfloor$, więc w ciągu $(a+1,\, a+2,\, \ldots,\, a+k)$ występuje dokładnie $\lfloor (a+k)/d \rfloor - \lfloor a/d \rfloor$ wyrazów podzielnych przez d. Dla dowodu naszej tezy, czyli podzielności $I(0;\, k) | I(n;\, k)$, wystarczy zatem udowodnić, że dla każdej liczby naturalnej d zachodzi nierówność

$$\lfloor (n+k)/d \rfloor - \lfloor n/d \rfloor \geqslant \lfloor k/d \rfloor - \lfloor 0/d \rfloor .$$

Ta nierówność jest przypadkiem szczególnym nierówności $\lfloor x+y \rfloor \geqslant \lfloor x \rfloor + \lfloor y \rfloor$ prawdziwej dla dowolnych liczb rzeczywistych x, y, zobacz też C12.1.5.

Z3.I4 Dzielna jest równa $\frac{X^{(k+1)n}-1}{X^n-1}$, a dzielnik $\frac{X^{k+1}-1}{X-1}$. Chcemy wyznaczyć takie liczby naturalne k, n, dla których funkcja wymierna (zobacz C3.51)

$$\frac{(X-1)(X^{(k+1)n}-1)}{(X^n-1)(X^{k+1}-1)} = \frac{\Phi_1(X) \cdot \prod_{d|(k+1)n} \Phi_d(X)}{\prod_{d|n} \Phi_d(X) \cdot \prod_{d|k+1} \Phi_d(X)}$$

jest w istocie równa wielomianowi. To z pewnością będzie miało miejsce, gdy każdemu wystąpieniu czynnika $\Phi_d(X)$ w mianowniku towarzyszy wystąpienie tego czynnika w liczniku. Twierdzimy, że tak jest na pewno, gdy $\mathrm{NWD}\,(k+1,\, n) = 1$ (to jest jasne, bo wtedy dany czynnik $\Phi_d(X)$, dla $d \neq 1$, z mianownika występuje dokładnie raz: albo w pierwszym, albo w drugim z napisanych tam iloczynów). I tak na pewno n i e jest, gdy istnieje wspólny (różny od 1) dzielnik liczb n i $k+1$ (niech bowiem $p \in \mathbb{P}$ będzie takim wspólnym dzielnikiem, wtedy n i e r o z k ł a d a l n y czynnik $\Phi_p(X)$ występuje dwukrotnie w mianowniku i tylko jednokrotnie w liczniku).

Z3.I5 Załóżmy, że $f(X) = c + bX + X^2 \in \mathbb{Z}$ jest dzielnikiem (± 1)-wielomianu, czyli że zachodzi równość $(c + bX + X^2)h(X) = c_0 + c_1 X + \ldots + c_n X^n$ dla pewnego wielomianu $h(X) \in \mathbb{Z}[X]$. Z równości tej wynika, oczywiście, równość $c = \pm 1$. Korzystamy teraz z tezy Z3.E14(1). Dzięki niej wiemy, że wszystkie pierwiastki u (zespolone, w szczególności rzeczywiste!) (± 1)-wielomianu spełniają warunek $|u| < 2$. Wobec tego również jego dzielnik $f(X)$ może mieć tylko pierwiastki spełniające ten warunek. Stąd widzimy, że $f(-2) > 0$, $f(2) > 0$ (w przeciwnym wypadku w przedziale $[\,-2;\, 2\,]$ znalazłby się pierwiastek, zob. T3.7). Wyznaczamy więc pary $(b,\, c)$ liczb całkowitych, dla których $c = \pm 1$ i zachodzą nierówności $4 - 2b + c > 0$ oraz $4 + 2b + c > 0$. Takich par jest osiem. Równości $(1-2X+X^2)(1+X) = 1-X-X^2+X^3$, $(1+2X+X^2)(-1+X) = -1-X+X^2+X^3$, $(1+X^2)(1+X) = 1+X+X^2+X^3$, $(-1+X^2)(1+X) = -1-X+X^2+X^3$ pokazują cztery unormowane trójmiany kwadratowe-dzielniki (± 1)-wielomianów. Ponadto (± 1)-trójmiany kwadratowe $1+X+X^2$, $-1+X+X^2$, $-1-X+X^2$ i $1-X+X^2$ są własnymi dzielnikami. Mamy więc osiem u n o r m o w a n y c h trójmianów $f(X)$ dzielników (± 1)-wielomianów. Do listy należy oczywiście dołączyć jeszcze osiem trójmianów $-f(X)$.

Z3.J1 Załóżmy, że $f(X) = g(X)h(X)$. Tu $g(X)$, $h(X) \in \mathbb{Z}[X]$ są unormowane, oraz $\deg g(X) = n-k$, $\deg h(X) = n+k$, gdzie $0 \leqslant k < n$. Licząc wartości dla argumentów a_j, dostajemy n równości $g(a_j)h(a_j) = 1$. To znaczy (jesteśmy w świecie liczb całkowitych!), że $g(a_j) = h(a_j) = \pm 1$ dla wszystkich a_j. Zauważmy teraz, że ani $g(X)$ ani $h(X)$ nie mają pierwiastków rzeczywistych. Więc, ponieważ oba są unormowane, przyjmują wyłącznie wartości d o d a t n i e. To wynika z własności Darboux (wielomian rzeczywisty przyjmujący wartości dodatnie i ujemne, przyjmuje też wartość 0). Zatem $g(a_j) = h(a_j) = 1$ dla każdego j. Gdyby $k \neq 0$, to wielomian $g(X)$ (stopnia $< n$) przyjmujący n razy wartość 1, byłby s t a ł ą. Jedyną więc możliwość rozkładalności wielomianu $f(X)$ daje przypadek $k = 0$. Wtedy oba wielomiany $g(X)$, $h(X)$ są stopnia n i na zbiorze $\{a_1,\, \ldots,\, a_n\}$ przyjmują oba wartość 1. Wówczas ich różnica $g(X) - h(X)$ jest wielomianem stopnia $< n$ (bo

oba są unormowane) i ma n miejsc zerowych. Jest więc $g(X) - h(X) = 0$. Założona równość $f(X) = g(X)h(X)$ ma zatem postać $(X - a_1)^2 \cdot \ldots \cdot (X - a_n)^2 + 1 = g(X)^2$. Jednakowoż ta równość również nie może mieć miejsca (przy $n \in \mathbb{N}$). Dawałaby bowiem równość $u^2 + 1 = w^2$ dla nieskończenie wielu liczb całkowitych u, w.

Z3.J2 (1) Załóżmy, że $f(X) = g(X)h(X)$, gdzie $g(X)$, $h(X) \in \mathbb{Z}[X]$ są wielomianami unormowanymi stopni $\leqslant n-1$. Kładąc tu $X = a_j$ widzimy, że $g(a_j)h(a_j) = 1$ dla każdego $j = 1, \ldots, n$. Czyli $g(a_j) = h(a_j)(= \pm 1)$. Zatem $g(x) - h(x) = 0$ dla n różnych argumentów, więc, zobacz W1T3.4, $g(X) - h(X) = 0$, czyli $g(X) = h(X)$. Równość $f(X) = g(X)h(X)$ może więc być przepisana tak: $(X - a_1)(X - a_2) \cdot \ldots \cdot (X - a_{2k}) = (g(X) - 1)(g(X) + 1)$, gdzie $n = 2k$ i, oczywiście, $k = \deg g(X)$. Widzimy już teraz, że gdy n jest liczbą nieparzystą, to $f(X)$ jest nierozkładalny. Gdy zaś $n = 2k$, to, dzięki jednoznaczności rozkładu (zobacz T3.14), możemy uznać, że $h_1(X) := (X-a_1)\cdot\ldots\cdot(X-a_k) = g(X)-1$ i $h_2(X) := (X-a_{k+1})\cdot\ldots\cdot(X-a_{2k}) = g(X)+1$. Stąd mamy równość $h_1(X) - h_2(X) = 2$. Kładąc w tej równości $X = a_{2k}$ znajdujemy rozkład $(a_{2k} - a_1)(a_{2k} - a_2) \cdot \ldots \cdot (a_{2k} - a_k) = 2$ liczby (pierwszej!) 2 na iloczyn k różnych czynników całkowitych. To jest możliwe tylko, gdy $k = 1$ lub $k = 2$. Przechodzimy więc do części **(2)**. Z powyższej analizy wynika, że wielomian $(X-a)(X-b)+1$ może być rozkładalny tylko, gdy $|b-a| = 2$. Wtedy mamy rozkład postaci $(X-c-1)(X-c+1)+1 = (X-c)^2$. **(3)**. W tym przypadku mamy $(X - a - 2)(X - a - 1)(X - a)(X - a + 1) + 1 = [X^2 - (2a - 1)X + a^2 + a - 1]^2$, zob. rozw. Z2.D6.

Z3.J3 (Zobacz też C3.38.) Załóżmy nie wprost, że $f(X) = g(X)h(X)$ jest rozkładem w $\mathbb{Z}[X]$. Niech $\deg g(X) = k$, $\deg h(X) = l$. Zbiór $\{c \in \mathbb{Z} : |g(c)| = 1\} = \{c \in \mathbb{Z} : g(c)^2 = 1\}$ jest zbiorem pierwiastków wielomianu $g(X)^2 - 1$ i, jako taki, ma co najwyżej $2k$ elementów (zob. T3.4 i C3.6). Z tych samych powodów zbiór $\{c \in \mathbb{Z} : |h(c)| = 1\}$ ma co najwyżej $2l$ elementów. Ponieważ $|f(c_j)| = |g(c_j)| \cdot |h(c_j)| \in \mathbb{P} \cup \{1\}$ dla każdego $j = 1, \ldots, 2n + 1$, więc każda z liczb c_j należy do $\{c \in \mathbb{Z} : |g(c)| = 1\}$ lub do $\{c \in \mathbb{Z} : |h(c)| = 1\}$. Stąd mamy sprzeczność:

$$2n + 1 = \operatorname{card}\{c_1, \ldots, c_{2n+1}\} \leqslant \operatorname{card}(\{c \in \mathcal{Z} : |g(c)| = 1\} \cup \{c \in \mathbb{Z} : |h(c)| = 1\}) \leqslant 2(k + l) = 2n.$$

Z3.J4 Udowodnimy *Lemat. Jeżeli $f(X) \in \mathbb{Z}[X]$ i $|f(c_j)| = 1$ dla pięciu różnych liczb całkowitych $c_1, c_2, \ldots, c_5$, to $f(c_1) = f(c_2) = \cdots = f(c_5)$. Dowód.* Pokazujemy najpierw, że nie może być $f(c_1) = f(c_2) = f(c_3) = f(c_4) = 1$ i $f(c_5) = -1$. Rzeczywiście, wówczas mielibyśmy rozkład $f(X) - 1 = (X - c_1)(X - c_2)(X - c_3)(X - c_4)g(X)$, gdzie $g(X) \in \mathbb{Z}[X]$, zob. WT3.2. Wtedy $-2 = f(c_5) - 1 = (c_5 - c_1)(c_5 - c_2)(c_5 - c_3)(c_5 - c_4)g(c_5)$, co, wobec różności czterech czynników $c_5 - c_j$, jest niemożliwe. Zamieniając ewentualnie $f(X)$ na $-f(X)$, widzimy, że jeżeli cztery z pięciu liczb $f(c_j)$ są równe, to wszystkie są równe. Pokazujemy teraz, że niemożliwy jest przypadek $f(c_1) = f(c_2) = f(c_3) = 1$ i $f(c_4) = f(c_5) = -1$. Mamy wtedy bowiem $f(X)-1 = (X-c_1)(X-c_2)(X-c_3)h(X)$. Kładąc w tej równości $X = c_4$ i $X = c_5$ dostajemy dwa różne rozkłady liczby -2 na iloczyn liczb całkowitych:

$$-2 = (c_4 - c_1)(c_4 - c_2)(c_4 - c_3)h(c_4) = (c_5 - c_1)(c_5 - c_2)(c_5 - c_3)h(c_5).$$

Aby zobaczyć, że takie równości nie mogą zachodzić, załóżmy (b.s.o), że $c_1 < c_2 < c_3$ i $c_4 < c_5$. Wówczas te dwa rozkłady są wyznaczone jednoznacznie: $-2 = 1 \cdot (-1) \cdot (-2) \cdot (-1) = 2 \cdot 1 \cdot (-1) \cdot 1$. Stąd $(c_5 - c_1) - (c_4 - c_1) = 2 - 1 = 1$ i $(c_5 - c_2) - (c_4 - c_2) = 1 - (-1) = 2$. Sprzeczność! Q.e.d.

Przechodzimy do rozwiązania zadania: Ponieważ $n \geqslant 5$, więc, na mocy lematu, możemy (b.s.o.) założyć, że $f(c_j) = 1$ dla wszystkich j. Mamy więc rozkład $f(X)-1 = a(X-c_1)(X-c_2)\cdot\ldots\cdot(X-c_n)$ dla pewnej liczby całkowitej a. Założenie unormowania daje równość $a = 1$. Teraz powołujemy się na Z3.17.

Z3.J5 Połóżmy $Y = X - 1$. Wtedy $F_n(X) = F_n(Y + 1) = Y^{2^n} + \cdots + 2$. Wystarczy teraz zastosować kryterium Eisensteina. Dla sprawdzenia zachodzenia warunków tego kryterium, czyli po-

dzielności $2|\binom{2^n}{k}$ dla każdego $1 \leqslant k \leqslant 2^n - 1$, można skorzystać z formuły Legendre'*a* T2.17, zobacz też Z12.11.

Z3.J6 Podobnie jak przed chwilą położymy $X = Y - 1$.

Z3.J7 Oznaczmy, ogólniej $f(X) = \sum_{j=0}^{p-1}(p-j)X^j$ (przy $p \in \mathbb{P}$). Jeżeli $\alpha \in \mathbb{C}$ jest pierwiastkiem (zespolonym) wielomianu $f(X)$, to mamy $0 = (\alpha-1)f(\alpha) = \alpha^p+\alpha^{p-1}+\ldots+\alpha-p$. Stąd wnosimy, że $|\alpha| > 1$. Gdyby bowiem było $|\alpha| \leqslant 1$, to, na podstawie nierówności trójkąta, $p = |\alpha^p+\alpha^{p-1}+\cdots+\alpha| \leqslant |\alpha|^p + |\alpha|^{p-1} + \cdots + |\alpha| \leqslant 1+1+\cdots+1 = p$. To jest możliwe tylko, gdy $|\alpha| = 1$. Co więcej, równość $|\beta_1 + \beta_2 + \cdots + \beta_n| = n$, dla liczb zespolonych β_j o modułach równych 1, jest możliwa t y l k o, gdy $\beta_1 = \beta_2 = \cdots = \beta_n$ (gdy, na przykład $\beta_1 \neq \beta_2$, to (nierówność trójkąta!) $|\beta_1 + \beta_2| < 2$, więc $|\beta_1 + \beta_2 + \cdots + \beta_n| \leqslant |\beta_1 + \beta_2| + |\beta_3| + \cdots + |\beta_n| < 2 + (n-2) = n$). Zatem $\alpha = \alpha^2$, co dowodzi, że $\alpha = 1$. Ale $f(1) \neq 0$, więc $\alpha = 1$ nie jest pierwiastkiem $f(X)$. Widzimy, że wszystkie pierwiastki wielomianu $f(X)$ mają moduł ściśle większy niż 1. Załóżmy teraz, że $f(X) = g(X)h(X)$ jest (nietrywialnym) rozkładem na czynniki w $\mathbb{Z}[X]$. Wówczas $g_0h_0 = p$, więc $|g_0| = 1$ lub $|h_0| = 1$, niech, b.s.o., $|g_0| = 1$. To jest niemożliwe, bo g_0 jest, na mocy wzoru Viète'*a*, równy iloczynowi niektórych p i e r w i a s t k ó w wielomianu $f(X)$, a one wszystkie mają moduły > 1.

Z3.J8 Rozkład wielomianu $X^{4k}+4$ w $\mathbb{Z}[X]$ otrzymujemy natychmiast z tożsamości Sophie Germain (3.66): $X^{4k} + 4 = (X^{2k} + 2X^k + 2)(X^{2k} - 2X^k + 2)$. Załóżmy więc, nie wprost, że $4 \nmid n$ i $X^n + 4 = f(X)g(X)$, gdzie $f(X), g(X) \in \mathbb{Z}[X]$. Niech $1 \leqslant k := \deg f(X) < n$. Zauważmy, że każdy pierwiastek (rzeczywisty czy zespolony) wielomianu $X^n + 4$ ma moduł (wartość bezwzględną) równy $2^{2/n}$ (równość $\alpha^n + 4 = 0$ implikuje równość $|\alpha|^n = 2^2$, skąd $|\alpha| = 2^{2/n}$). Ponieważ k a ż d y pierwiastek wielomianu $f(X)$ jest jednocześnie pierwiastkiem wielomianu $X^n + 4$, więc (wzory Viète'*a*!) wyraz wolny $f(0)$ wielomianu $f(X)$ jest iloczynem k liczb zespolonych o module $2^{2/n}$. Zatem $|f(0)| = 2^{2k/n}$. Ale $f(0) \in \mathbb{Z}$. Wnioskujemy stąd, $n = 2k$. Gdyby k było liczbą nieparzystą, to wielomian $f(X)$ miałby pierwiastek rzeczywisty (zobacz T3.8) i wtedy również wielomian $X^n + 4$ miałby pierwiastek rzeczywisty. Sprzeczność, bo $\lambda^{2k} + 4 > 0$ dla każdej liczby $\lambda \in \mathbb{R}$.

Z3.J9 Oto przydatne lematy dotyczące wielomianów o współczynnikach wymiernych:

L e m a t 1. *Jeżeli $a(X) = b(X)c(X)$, to $a(f(X)) = b(f(X))c(f(X))$ dla dowolnego wielomianu $f(X)$. Odwrotnie, jeżeli dla pewnego n i e s t a ł e g o (tzn., stopnia $\geqslant 1$) wielomianu $f(X)$ zachodzi równość $a(f(X)) = b(f(X))c(f(X))$, to $a(X) = b(X)c(X)$. D o w ó d.* Wynikanie $\Rightarrow$ jest (dość?) jasne. Wynikanie $\Leftarrow$ sprowadza się do implikacji $a(f(X)) = b(f(X)) \implies a(X) = b(X)$. Dla jej dowodu powołujemy się na twierdzenie o jednoznaczności (zob. W2T3.4): ponieważ $a(f(x)) = b(f(x))$, więc wystarczy zauważyć, że elementów postaci $f(x)$ jest dowolnie d u ż o (więcej niż maksimum stopni wielomianów $a(X), b(X)$), a to wynika z założenia niestałości wielomianu $f(X)$ i n i e s k o ń c z o n o ś c i ciała liczb wymiernych. Q.e.d.

L e m a t 2. *Dla wielomianu $a(X) \in \mathbb{Q}[X]$ zachodzi równość $a(-X) = a(X)$ wtedy i tylko wtedy, gdy wszystkie nieparzyste współczynniki a_{2l+1} są równe 0, i wtedy i tylko wtedy, gdy istnieje taki wielomian $b(X)$, że zachodzi równość $a(X) = b(X^2)$. D o w ó d* pozostawiamy Czytelnikowi.

L e m a t 3. *Dla wielomianu $a(X) \in \mathbb{Q}[X]$ zachodzi równość $a(-X) = -a(X)$ wtedy i tylko wtedy, gdy wszystkie parzyste współczynniki a_{2l} są równe 0, i wtedy i tylko wtedy, gdy istnieje taki wielomian $b(X)$, że zachodzi równość $a(X) = Xb(X^2)$. D o w ó d* pozostawiamy Czytelnikowi.

Przechodzimy do rozwiązania zadania. Niech $n = \deg p(X)$. Wówczas $\deg f(X) = 2n$. Załóżmy, nie wprost, że istnieje rozkład $f(X) = q(X)h(X)$ w $\mathbb{Z}[X]$. Możemy przy tym założyć, że czynniki $q(X), h(X)$ są unormowanymi wielomianami o współczynnikach całkowitych, $q(X)$ jest n i e r o z k ł a d a l n y, a $0 < \deg h(X) < 2n$. Ponieważ $f(X) = p(X^2)$, więc, dzięki lematom 2, 1, mamy $q(-X)h(-X) = f(-X) = f(X) = q(X)h(X)$ (potrzebna tu część dowodu lematu 2 wygląda tak: $f(-X) = p((-X)^2) = p(X^2) = f(X)$). Korzystając z lematu 1 łatwo wywnioskować, że wielomian $q(-X)$ również (tak jak $q(X)$) jest nierozkładalny. Rozważmy więc dwa przypadki (jedyne

możliwe!): (1) $q(X) \sim q(-X)$, (2) $q(X) \perp q(-X)$.

Przypadek (1) zajść nie może. Rzeczywiście, w takim razie $q(-X) = \pm q(X)$. Mamy dwa podprzypadki: (1a) $q(-X) = q(X)$, (1b) $q(-X) = -q(X)$. W podprzypadku (1a) mamy $q(X) = t(X^2)$ (zob. lemat 2), więc $t(X^2)|p(X^2)$, więc $t(X)|p(X)$ (zob. lemat 1), więc $t(X) = \pm 1$ (bo $\deg t(X) < \deg p(X)$, a $p(X)$ jest nierozkładalny), więc $q(X) = \pm 1$, co jest niemożliwe, bo wielomian nierozkładalny ma stopień > 0. W podprzypadku (1b) mamy $q(X) = Xs(X^2)$ (zob. lemat 3), więc $q(X) = \pm X$ (bo $q(X)$ jest nierozkładalny), więc $f(X) = \pm Xh(X)$, więc wyraz wolny $f_0 = p_0 = 0$, co jest kwadratem. Sprzeczność. Również przypadek (2) prowadzi do sprzeczności. Rzeczywiście, wówczas równość $q(X)h(X) = q(-X)h(-X)$ i ZTA w $\mathbb{K}[X]$, zob. T3.12, daje równość $h(X) = q(-X)l(X)$ i, wynikającą z niej (na mocy lematu 1), równość $h(-X) = q(X)l(-X)$. Stąd $q(X)q(-X)l(X) = q(-X)q(X)l(-X)$, czyli $l(X) = l(-X)$, więc (lemat 1!) $l(X) = k(X^2)$. Ale $l(X)|f(X)$, czyli $k(X^2)|p(X^2)$, więc (zob. część $\Leftarrow$ lematu 1 przy $t(X) = X^2$) $k(X)|p(X)$, co, wobec nierozkładalności $p(X)$, daje $k(X) = \pm 1$, więc i $l(X) = \pm 1$. Dostajemy wtedy równość $f(X) = q(X)q(-X)l(X) = \pm q(X)q(-X)$, z której wynika równość $p(0) = p_0 = f_0 = \pm q_0^2$. To jest sprzeczne z założeniem niekwadratowości $|p(0)|$. U w a g a. Założenie, że $|p(0)|$ nie jest kwadratem, jest istotne. Na przykład $p(X) = X^2 + X + 1$ jest nierozkładalny (w $\mathbb{Q}[X]$), ale $p(X^2) = X^4 + X^2 + 1 = (X^2 + 1)^2 - X^2 = (X^2 - X + 1)(X^2 + X + 1)$. Ogólniej: patrzmy na wielomian $p(X) = X^2 + X + (2c^2 + 2c + 1)^2$ przy dowolnym $c \in \mathbb{Z}$.

Z3.J10 Domyślamy się, że prawdziwa jest teza ogólniejsza: *Jeżeli* $a_n 10^n + \cdots + a_1 10 + a_0$ *jest zapisem liczby pierwszej* p *w systemie o podstawie* 10, *to wielomian* $f(X) = a_n X^n + \cdots + a_1 X + a_0$ *jest nierozkładalny w* $\mathbb{Q}[X]$. *D o w ó d.* Załóżmy, nie wprost, że istnieje rozkład $f(X) = g(X)h(X)$ w pierścieniu $\mathbb{Z}[X]$ (równoważnie, zobacz T3.15, w pierścieniu $\mathbb{Q}[X]$). Wówczas $p = f(10) = g(10)h(10)$. Więc, ponieważ $g(10), h(10) \in \mathbb{Z}$, możemy (b.s.o) założyć, że $|g(10)| = 1$. Napiszmy rozkład (3.30) dla wielomianu $g(X)$: $g(X) = C(X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_k)$. Ponieważ każdy pierwiastek α_j wielomianu $g(X)$ jest też pierwiastkiem wielomianu $f(X)$, więc (zobacz Z3.E14(2)) $|\alpha_j| < 4$ lub $\operatorname{Re}\alpha_j < 0$ (liczba M w naszym przypadku jest bowiem $\leqslant 9$). Stąd, oczywiście, $|10 - \alpha_j| > 6$ dla każdego j. I ostatecznie, $1 = |g(10)| = |C| \cdot |10 - \alpha_1| \cdot \ldots \cdot |10 - \alpha_k| > 6^k$. Sprzeczność.

Z3.J11 Zauważmy najpierw, że jeżeli p jest d o s t a t e c z n i e duża, to $f(x) > 0$ dla wszystkich $x \in \mathbb{Z}$. To jest oczywiście prawda przy $x < k_1$ lub $x > k_{2n}$ (dla dowolnej liczby pierwszej p). Dla pozostałych x wystarczy wybrać p spełniające warunek $p > (k_{2n} - k_1)^{2n}$. Wówczas $|x - k_j| < \sqrt[2n]{p}$ dla każdego j, więc $|f(x) - p| = |x - k_1| \cdot \ldots \cdot |x - k_{2n}| < p$, skąd $-p < f(x) - p < p$, czyli $0 < f(x)$. Załóżmy teraz, że istnieje rozkład $f(X) = g(X)h(X)$ na iloczyn unormowanych wielomianów (w $\mathbb{Z}[X]$) stopni $< 2n$. Wówczas $g(x) > 0$ i $h(x) > 0$ dla wszystkich $x \in \mathbb{Z}$, oraz $g(k_j)h(k_j) = p$ dla każdego j. Czyli $g(k_j) = p$ i $h(k_j) = 1$ lub $g(k_j) = 1$ i $h(k_j) = p$ dla każdego $j = 1, 2, \ldots, 2n$. Zatem wielomian $s(X) = g(X) + h(X)$ stopnia $< 2n$ (zob. C3.3(1)) dla wszystkich argumentów k_j przyjmuje wartość $p + 1$. Więc, zobacz W1T3.4, $g(x) + h(x) - p - 1 = 0$ dla każdego $x \in \mathbb{Z}$. To jest jednak n i e m o ż l i w e dla wielomianów niestałych i przyjmujących wartości dodatnie. Rozwiązanie kończy uwaga, że opisanych liczb pierwszych jest nieskończenie wiele.

Z3.J12 Równość $X^7Y^7 + 1 = f(X)g(Y)$, po podstawieniu $X = 0$ daje $1 = f(0)g(Y)$, co oznacza, że $g(Y)$ jest wielomianem stałym (stopnia 0). Podobnie, $f(X)$ jest wielomianem stopnia 0. Jasne, że iloczyn takich dwóch n i e jest równy $X^7Y^7 + 1$. U w a g a. Wielomian $X^7Y^7 + 1$ jest r o z k ł a d a l n y w pierścieniu $\mathbb{Q}[X, Y]$: $X^7Y^7 + 1 = (XY + 1)(X^6Y^6 - X^5Y^5 + \cdots - XY + 1)$. Podobnie można rozłożyć wielomian $X^aY^b + 1$ w przypadku, gdy istnieje nieparzysty i > 1 wspólny dzielnik wykładników a, b.

Z3.J13 Odpowiedź zależy od n. Dla $n = 1$ rzecz jest oczywista: mamy rozkład $X_1^2 = X_1 \cdot X_1$.

Dla $n = 2$ znamy (bardzo ważny i/bo często używany) rozkład

$$\boxed{\boxed{X_1^2 + X_2^2 = (X_1 + iX_2)(X_1 - iX_2)}} \tag{3.76}$$

w pierścieniu $\mathbb{C}[X_1, X_2]$. Aliści $X_1^2 + X_2^2$ jest nierozkładalny w pierścieniu $\mathbb{R}[X_1, X_2]$ (tym bardziej więc w pierścieniu $\mathbb{Q}[X_1, X_2]$). Rzeczywiście, gdyby $X_1^2 + X_2^2 = f(X_1, X_2)g(X_1, X_2)$, to kładąc $X_2 = 1$ dostalibyśmy rozkład $X_1^2 + 1 = \widetilde{f}(X_1)\widetilde{g}(X_1)$ w pierścieniu $\mathbb{R}[X_1]$. Taki rozkład nie jest możliwy gdy $\deg \widetilde{f}(X_1) = \deg \widetilde{g}(X_1) = 1$ (bo wyróżnik dwumianu kwadratowego $X_1^2 + 1$ jest ujemny). B.s.o. załóżmy więc, że $\deg \widetilde{f}(X_1) = 2$ i $\deg \widetilde{g}(X_1) = 0$. To znaczy, że wielomian $g(X_1, X_2)$ nie zależy od X_1. Kładąc teraz $X_2 = 1$ w równości $X_1^2 + X_2^2 = f(X_1, X_2)g(X_1, X_2)$ i rozumując podobnie, widzimy, że (tym razem) wielomian $f(X_1, X_2)$ nie zależy od X_2 (gdyby to wielomian $g(X_1, X_2)$ nie zależał od X_2, to byłby stałą, czyli wielomianem stopnia 0, i rozkład $X_1^2 + X_2^2 = f(X_1, X_2)g(X_1, X_2)$ nie byłby "prawdziwym" rozkładem!). Widzimy więc, że jedyną szansę na istnienie "prawdziwego" rozkładu daje równość $X_1^2 + X_2^2 = k(X_1)l(X_2)$ dla wielomianów $k(X_1) \in \mathbb{R}[X_1]$, $l(X_2) \in \mathbb{R}[X_2]$. Kładąc w tej równości $X_2 = 0$ dostajemy równość $X_1^2 = c \cdot k(X_1)$ gdzie $c = l(0) \in \mathbb{R}_{\neq 0}$. Podobnie $X_2^2 = d \cdot l(X_2)$. Stąd dostajemy sprzeczność $(cd)^{-1}X_1^2X_2^2 = X_1^2 + X_2^2$. Przechodzimy do przypadku $n \geqslant 3$. Załóżmy, że

$$X_1^2 + X_2^2 + \ldots + X_n^2 = f(X_1, X_2, \ldots, X_n)g(X_1, X_2, \ldots, X_n) \tag{$*$}$$

jest rozkładem w pierścieniu $\mathbb{C}[X_1, X_2, \ldots, X_n]$. A priori możliwe są dwa przypadki: (1) istnieje taki indeks $j = 1, \ldots, n$, że $\deg_{X_j} f = \deg_{X_j} g = 1$ (przez $\deg_{X_j} h$ oznaczamy oczywiście stopień wielomianu h względem zmiennej X_j), (2) dla każdego j wielomian f ma względem zmiennej X_j stopień 1 ± 1, a wielomian g ma względem tej zmiennej stopień 1 ∓ 1. Zaczniemy od zbadania przypadku (2). W tym przypadku możemy (b.s.o.) uważać, że iloczyn z prawej strony równości $(*)$ ma postać $k(X_1, \ldots, X_s)l(X_{s+1}, \ldots, X_n)$, gdzie wielomian $k(X_1, \ldots, X_s)$ jest postaci $cX_1^2 + \ldots$, a wielomian $l(X_{s+1}, \ldots, X_n)$ jest postaci $dX_{s+1}^2 + \ldots$, przy czym $cd \neq 0$ (kropkami oznaczamy pozostałe wyrazy). Jasne, że wówczas równość $(*)$ nie może zachodzić, bo po jej prawej stronie występuje wyraz $cdX_1^2X_{s+1}^2$, którego nie ma po stronie lewej. W przypadku (1) załóżmy (b.s.o.), że $\deg_{X_1} f = \deg_{X_1} g = 1$. Wówczas rozkład $(*)$ ma postać

$$X_1^2 + X_2^2 + \ldots + X_n^2 = (cX_1 + k(X_2, \ldots, X_n))(dX_1 + l(X_2, \ldots, X_n)),$$

z której wnioskujemy, że $cd = 1$. "Przerzucając" w razie potrzeby stałą c z pierwszego nawiasu do drugiego, możemy od razu założyć, że $c = d = 1$. Wymnażając dostajemy wówczas

$$X_1^2 + X_2^2 + \cdots + X_n^2 = X_1^2 + (k + l)X_1 + k \cdot l.$$

Stąd otrzymamy równość $k(X_2, \ldots, X_n) = -l(X_2, \ldots, X_n)$ i rozkład

$$X_2^2 + \cdots + X_n^2 = k(X_2, \ldots, X_n)l(X_2, \ldots, X_n)$$

w pierścieniu $\mathbb{C}[X_2, \ldots, X_n]$. Ponieważ czynniki z prawej strony tego rozkładu różnią się tylko znakiem, więc oba muszą być stopnia 1 względem każdej swojej zmiennej. Mamy więc równość

$$X_2^2 + \cdots + X_n^2 = -(a_1 + a_2X_2 + \cdots + a_nX_n)(a_1 + a_2X_2 + \cdots + a_nX_n).$$

Stąd dostajemy $a_2^2 = a_3^2 = \cdots = a_n^2 = -1$ oraz $2a_ia_j = 0$ dla wszystkich $2 \leqslant i < j \leqslant n$. Jasne, że (przy $n \geqslant 3$) takie równości nie mogą zachodzić! Mamy zatem *odpowiedź*: wielomian $\sum_{j=1}^n X_j^2$ jest nierozkładalny w $\mathbb{C}[X_1, \ldots, X_n]$ przy $n \geqslant 3$ i jest rozkładalny przy $n = 2$ (zobacz rozkład (3.76)).

Z3.K1 Wielomian $X^{4k}+X^{2k}+1$, dla $k\in\mathbb{Z}_{\geqslant 0}$, łatwo przedstawić w postaci różnicy kwadratów: $X^{4k}+X^{2k}+1=X^{4k}+2X^{2k}+1-X^{2k}=(X^{2k}+1)^2-(X^k)^2$. Stosując tę sztuczkę dla $k=2$, a potem dla $k=1$, znajdujemy rozkład w $\mathbb{Q}[X]$:

$$X^8+X^4+1=(X^4-X^2+1)(X^2-X+1)(X^2+X+1). \qquad (\mathbb{Q})$$

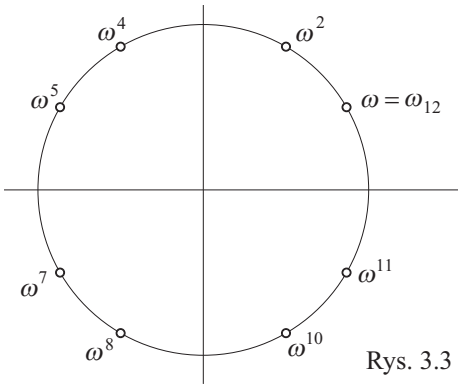
Pokazujemy, że występujące tu trzy czynniki są nierozkładalne w $\mathbb{Q}[X]$. Drugi i trzeci czynnik są nierozkładalne nawet w $\mathbb{R}[X]$ (bo $\Delta=-3<0$). Nierozkładalność w $\mathbb{Q}[X]$ (równoważnie, w $\mathbb{Z}[X]$) czynnika X^4-X^2+1 pokazujemy "na piechotę" (tak jak w rozwiązaniu zadania Z3.19, tylko łatwiej). Rozkład $(\mathbb{Q})$ jest więc rozkładem wielomianu X^8+X^4+1 na czynniki nierozkładalne w $\mathbb{Q}[X]$. [Przy okazji zauważmy, że nasz dobry druh X^2+X+1 jest wielomianem cyklotomicznym $\Phi_3(X)$, a jego kompan $X^2-X+1=\Phi_3(-X)$ jest wielomianem cyklotomicznym $\Phi_6(X)$, zobacz 3.4.6 P.]

Czynnik X^4-X^2+1 rozkładu $(\mathbb{Q})$ jest różnicą kwadratów $(X^2+1)^2-(\sqrt{3}X)^2$ w pierścieniu $\mathbb{R}[X]$. W tym pierścieniu mamy więc rozkład:

$$X^8+X^4+1=(X^2-\sqrt{3}X+1)(X^2+\sqrt{3}X+1)(X^2-X+1)(X^2+X+1) \qquad (\mathbb{R})$$

na iloczyn czynników nierozkładalnych w $\mathbb{R}[X]$ (wszystkie cztery wyróżniki są ujemne!).

Przechodzimy do pierścienia $\mathbb{C}[X]$. Tu, jak wiemy z T3.18, wszystkie czynniki w rozkładzie wielomianu $f(X)$ na iloczyn czynników nierozkładalnych, są postaci $X-\alpha$, gdzie α jest pierwiastkiem $f(X)$. Pierwiastki trzeciego i czwartego czynnika z rozkładu $(\mathbb{R})$ znamy dobrze, zobacz Z3.20. Są to ω_3 i ω_3^2 dla wielomianu X^2+X+1 i $-\omega_3$ i $-\omega_3^2$ dla wielomianu X^2-X+1. Na rysunku 3.3 widzimy wszystkie osiem pierwiastków wielomianu X^8+X^4+1. Wszystkie są pierwiastkami 12-ego stopnia z 1 i, jako takie, są potęgami liczby $\omega=\omega_{12}=\cos\pi/6+i\sin\pi/6$, por. C1.36. Przy tym: $\omega^4=\omega_3$, $\omega^8=\omega_3^2$ są pierwiastkami czynnika X^2+X+1, $\omega^2=-\omega_3^2$, $\omega^{10}=-\omega_3$ są pierwiastkami czynika X^2-X+1, ω^5, ω^7 są pierwiastkami czynnika $X^2-\sqrt{3}X+1$, a ω, ω^{11} są pierwiastkami czynnika $X^2+\sqrt{3}X+1$. Mamy więc rozkład wielomianu X^8+X^4+1 na czynniki nierozkładalne w $\mathbb{C}[X]$:



Rys. 3.3

$$X^8+X^4+1=(X-\omega^5)(X-\omega^7)(X-\omega)(X-\omega^{11})(X-\omega^2)(X-\omega^{10})(X-\omega^4)(X-\omega^8) \qquad (\mathbb{C})$$

Z3.K2 Z zadania Z3.20 wiemy, że $f(X):=X^5+X+1$ dzieli się przez $\Phi_3(X)=X^2+X+1$. Rzeczywiście, $X^5+X+1=X^2(X^3-1)+X^2+X+1=X^2(X-1)(X^2+X+1)+X^2+X+1$, skąd

$$X^5+X+1=(X^3-X^2+1)(X^2+X+1). \qquad (\mathbb{Q})$$

To jest rozkład na czynniki nierozkładalne w $\mathbb{Q}[X]$ (wielomian X^3-X^2+1 jest nierozkładalny w $\mathbb{Q}[X]$, bo nie ma pierwiastka wymiernego, zobacz C3.34 i Z2.4). Czynnik X^2+X+1 jest nierozkładalny w $\mathbb{R}[X]$. Natomiast czynnik X^3-X^2+1 ma pierwiastek rzeczywisty. Znajdujemy go za pomocą metody opisanej w ustępie 3.4.7. Najpierw, za pomocą podstawienia $X=Y+\frac{1}{3}$, pozbywamy się wyrazu kwadratowego. Dostaniemy równość $X^3-X^2+1=Y^3-\frac{1}{3}Y+\frac{25}{27}=\frac{1}{27}(Z^3-3Z+25)$, gdzie, dla ułatwienia, położyliśmy dodatkowo $Z=3Y$. Zgodnie z 3.4.7 U1, szukamy pierwiastków równania $z^3-3z+25=0$ w postaci $z=\lambda+\mu$. W aktualnym przypadku układ (3.52) wygląda tak: $\lambda^3+\mu^3=-25$, $\lambda^3\mu^3=1$. Wybieramy r z e c z y w i s t e

$$\lambda=\sqrt[3]{\frac{-25-3\sqrt{69}}{2}},\quad \mu=\sqrt[3]{\frac{-25+3\sqrt{69}}{2}}.$$

Dostajemy rozkład badanego wielomianu w $\mathbb{R}[X]$:

$$f(X) = \left(X - \frac{\lambda+\mu+1}{3}\right)\left(X^2 + \frac{\lambda+\mu-2}{3}\,X + \frac{\lambda^2+\mu^2-\lambda-\mu}{9}\right)(X^2+X+1), \qquad (\mathbb{R})$$

gdzie drugi i trzeci czynnik są nierozkładalne (w pierścieniu $\mathbb{R}[X]$). Ich rozkłady na czynniki liniowe w pierścieniu $\mathbb{C}[X]$ pozostawiamy Czytelnikowi.

Z3.K3 Z tożsamości nieśmiertelnej (1.8) widzimy, że $(X^2-1)f(X) = X^{2n+2}-1$. Wystarczy teraz zastosować (3.39) przy $m = n+1$ i skorzystać z jednoznaczności rozkładu w $\mathbb{R}[X]$. Dostaniemy rozkład w $\mathbb{R}[X]$:

$$f(X) = \prod_{k=1}^{n} \left(X^2 - (2\cos\tfrac{2k\pi}{2n+2})X + 1\right).$$

Trzeba jeszcze, zobacz T3.19, zauważyć ujemność wyróżników: $\Delta = 4\cos^2\frac{2k\pi}{2n+2} - 4 < 0$.

Z3.K4 Rozważmy $g(X) = X^2+X+1 = (X-\omega)(X-\overline{\omega})$, gdzie $\omega = \omega_3$, zob. (3.35), jest pierwiastkiem stopnia 3 z jedynki o argumencie $2\pi/3$. Badany wielomian $f(X)$ jest superpozycją $g(X^n) = (X^n-\omega)(X^n-\overline{\omega})$. Aby znaleźć jego rozkład na czynniki liniowe (tzn., stopnia pierwszego) w $\mathbb{C}[X]$ wystarczy znaleźć pierwiastki wielomianu $X^n-\omega$ i wielomianu $X^n-\overline{\omega}$.

Z3.K5 Sprawdzenie równości

$$(X+Y)^3 - X^3 - Y^3 = 3XY(X+Y), \qquad (3.77)$$

$$(X+Y)^5 - X^5 - Y^5 = 5XY(X+Y)(X^2+XY+Y^2), \qquad (3.78)$$

$$(X+Y)^7 - X^7 - Y^7 = 7XY(X+Y)(X^2+XY+Y^2)^2 \qquad (3.79)$$

jest prostym rachunkiem. Nierozkładalność występujących tu czynników jest jasna dla 3, 5, 7, X, Y i $X+Y$. Gdyby wielomian $F(X,Y) = X^2+XY+Y^2$ dał się rozłożyć na iloczyn $G(X,Y)H(X,Y)$ w pierścieniu $\mathbb{Z}[X,Y]$, to mielibyśmy rozkład $X^2+X+1 = F(X,1) = G(X,1)H(X,1)$ w $\mathbb{Z}[X]$.

Z3.K6 Rozważmy wielomian $f(X,Y,Z) = X^n(Y-Z)+Y^n(Z-X)+Z^n(X-Y) \in \mathbb{Z}[X,Y,Z]$. Gdy popatrzymy na niego jak na wielomian zmiennej X o współczynnikach w pierścieniu $\mathbb{Z}[Y,Z]$, to widzimy, że $Y \in \mathbb{Z}[Y,Z]$ jest jego pierwiastkiem. Z T3.2 wynika więc równość $f(X,Y,Z) = (X-Y)g_1(X,Y,Z)$ dla pewnego wielomianu $g_1 \in \mathbb{Z}[X,Y,Z]$ (na marginesie dodajmy, że stopniem wielomianu g_1 względem zmiennej X jest $n-1$). Podobnie sprawdzamy, że zachodzą równości $f(X,Y,Z) = (Y-Z)g_2(X,Y,Z)$ i $f(X,Y,Z) = (Z-X)g_3(X,Y,Z)$. Elementy $X-Y$, $Y-Z$ i $Z-X$ pierścienia $\mathbb{Z}[X,Y,Z]$ są nierozkładalne i niestowarzyszone (sprawdzić!) i każdy z nich jest dzielnikiem wielomianu f. Zatem i ich iloczyn jest dzielnikiem tego wielomianu. Istnieje więc równość

$$X^n(Y-Z)+Y^n(Z-X)+Z^n(X-Y) = (X-Y)(Y-Z)(Z-X)g(X,Y,Z)$$

dla pewnego wielomianu $g(X,Y,Z) \in \mathbb{Z}[X,Y,Z]$.

Z3.L1 Niech $f(X) = aX^2+bX+c$. Fakt nieistnienia rozwiązań równania $ax^2+bx+c = x$ oznacza (jest równoważny), że trójmian kwadratowy $aX^2+(b-1)X+c$ n i e ma pierwiastków rzeczywistych. W szczególności, funkcja wielomianowa $\mathbb{R} \ni x \longmapsto ax^2+(b-1)x+c$ przyjmuje wyłącznie wartości j e d n e g o z n a k u (tego samego co znak a). Załóżmy (na przykład), że $a<0$. Wówczas $ax^2+(b-1)x+c<0$, czyli $f(x)<x$ dla każdego $x \in \mathbb{R}$. Zakładamy teraz, nie wprost, że $\alpha \in \mathbb{R}$ jest pierwiastkiem superpozycji $f(f(X))$, tzn. że $f(f(\alpha)) = 0$. Ponieważ $f(f(\alpha)) < f(\alpha)$, więc otrzymujemy sprzeczność $0 < f(\alpha) < 0$. Podobnie badamy przypadek, gdy $a>0$.

Z3.L2 Oto zadanie ogólniejsze: Wielomiany $f(X)$, $g(X) \in \mathbb{R}[X]$ są różne, ale **komutujące** w tym sensie, że superpozycje $f(g(X))$ i $g(f(X))$ są równe. Udowodnić, że dla dowolnej liczby naturalnej n wielomian $f^{[n]}(X) - g^{[n]}(X)$ jest podzielny przez wielomian $f(X) - g(X)$.

L e m a t 1. *Jeżeli wielomiany $a(X)$, $b(X)$ są różne, to dla dowolnego wielomianu $h(X)$ wielomian $h(a(X)) - h(b(X))$ jest podzielny przez wielomian $a(X) - b(X)$.* *D o w ó d* jest natychmiastowy. Rzeczywiście, jeżeli $h(X) = \sum_{k\geqslant 0} h_k X^k$, to

$$h(a(X)) - h(b(X)) = \sum_{k\geqslant 1} h_k(a(X)^k - b(X)^k) = \sum_{k\geqslant 1} h_k(a(X) - b(X))(a(X)^{k-1} + \cdots + b(X)^{k-1}),$$

na mocy tożsamości nieśmiertelnej (prawdziwej w k a ż d y m pierścieniu przemiennym). Q.e.d.

L e m a t 2. *Jeżeli wielomiany $a(X)$, $b(X)$ komutują, to dla dowolnego $n \in \mathbb{Z}_{\geqslant 0}$ zachodzi równość superpozycji $a^{[n]}(b(X)) = b(a^{[n]}(X))$.* D o w ó d jest natychmiastowym (rzetelnie patrząc, indukcyjnym!) uogólnieniem równości $a(a(b(X))) = a(b(a(X))) = b(a(a(X)))$. Q.e.d.

Zadanie rozwiązujemy przez indukcję względem n. Baza indukcji (przypadek $n = 1$) jest oczywista. Załóżmy prawdziwość tezy dla danego $n \in \mathbb{N}$. Piszemy (dzięki lematowi 2) równość:

$$\begin{aligned} f^{[n+1]}(X) - g^{[n+1]}(X) &= [f^{[n]}(f(X)) - f^{[n]}(g(X))] + [f^{[n]}(g(X)) - g^{[n]}(g(X))] \\ &= [f^{[n]}(f(X)) - f^{[n]}(g(X))] + [g(f^{[n]}(X)) - g(g^{[n]}(X))]. \end{aligned}$$

Wielomian z pierwszego nawiasu kwadratowego jest podzielny przez $f(X) - g(X)$ (na mocy lematu 1), a wielomian z drugiego nawiasu kwadratowego jest podzielny przez $f^{[n]}(X) - g^{[n]}(X)$, więc też, na mocy założenia indukcyjnego, przez $f(X) - g(X)$. Jasne jest, że zadanie wyjściowe sprowadza się do ogólniejszego w przypadku, gdy $g(X) = X$.

Z3.L3 Teza jest oczywista, gdy $k = 1$. Załóżmy więc, że $k \geqslant 2$. Definiujemy indukcyjnie ciąg (a_n): $a_0 = a$ i $a_{n+1} = f(a_n)$ dla $n \in \mathbb{Z}_{\geqslant 0}$. Oznaczmy też $r_n = a_{n+1} - a_n$ dla $n = 0, 1, \ldots$. Wówczas dla każdego $n \in \mathbb{Z}_{\geqslant 0}$ zachodzi warunek $r_n | r_{n+1}$, zobacz C3.4. Założenie $f^{[k]}(a) = a$, czyli $a_k = a_0$ implikuje równość $r_k = r_0$. Ta równość i podzielności $r_0 | r_1 | \ldots | r_{k-1} | r_k$, na mocy C2.2, dają s t a ł o ś ć ciągu $(|r_n|)$: $|r_n| = r$ dla każdego $n \geqslant 0$. Załóżmy teraz, że $r_0 = r$ (rozumujemy podobnie, z zamianą maksimum na minimum, gdy $r_0 = -r$) i niech $a_s = \max\{a_0, a_1, \ldots, a_{k-1}\}$. Wówczas $a_{s-1} = a_s - r = a_{s+1}$. Stąd $a_{s+2} = f(a_{s+1}) = f(a_{s-1}) = a_s$, $a_{s+3} = f(a_{s+2}) = f(a_s) = a_{s+1}$, itd., przez oczywistą indukcję, $a_{s+2j} = a_s$ oraz $a_{s+2j-1} = a_{s+1}$ dla każdego $j \in \mathbb{N}$. Jedyną więc szansę na zachodzenie równości $a_k = a_0$ daje przypadek $s = 1$.

Z3.L4 Oznaczmy $\mathrm{Fix}(f^{[k]}) := \{x \in \mathbb{Z} : f^{[k]}(x) = x\}$. Mamy wykazać, że $\mathrm{card}\,(\mathrm{Fix}(f^{[k]})) \leqslant n$. Dla $k = 1$ rzecz jest oczywista: zbiór $\mathrm{Fix}(f) = \{x \in \mathbb{Z} : f(x) = x\}$ jest zbiorem pierwiastków wielomianu $f(X) - X$ (stopnia n), zobacz T3.4. Gdy zaś $k \geqslant 2$, to, jak wiemy z poprzedniego zadania, zachodzi inkluzja $\mathrm{Fix}(f^{[k]}) \subseteq \{x \in \mathbb{Z} : f^{[2]}(x) = x\}$. Wystarczy więc wykazać, że zbiór $\mathrm{Fix}(f^{[2]})$ ma co najwyżej n elementów. Zbiór $\mathrm{Fix}(f^{[2]})$ jest sumą (teoriomnogościową) co najwyżej n-elementowego zbioru $\mathrm{Fix}(f) := \{x \in \mathbb{Z} : f(x) = x\}$ i reszty. Jeżeli ta reszta jest zbiorem pustym, to koniec. Załóżmy więc, że $a \in \mathrm{Fix}(f^{[2]}) \setminus \mathrm{Fix}(f)$. Wówczas $f(a) = b \neq a$ i $f(b) = a$. Zamieniając ewentualnie a z b, możemy założyć, że $a < b$. Jeżeli $\{a, b\} = \mathrm{Fix}(f^{[2]})$, to koniec (bo $2 \leqslant n$). Niech więc $x \in \mathrm{Fix}(f^{[2]}) \setminus \{a, b\}$. Oznaczmy $y = f(x)$ i załóżmy (po ewentualnej zamianie miejscami jest to możliwe), że $x \leqslant y$. Wówczas $a - x | f(a) - f(x)$, czyli $a - x | b - y$, oraz $b - y | f(b) - f(y)$, więc $b - y | a - x$. Zatem $|a - x| = |b - y|$. Podobnie, $|a - y| = |b - x|$. Łatwo stąd wywnioskować, że środek przedziału $[a; b]$ pokrywa się ze środkiem przedziału $[x; y]$. Czyli $a + b = x + y$, więc $r := a + b = x + f(x)$. To oznacza, że k a ż d a liczba $x \in \mathrm{Fix}(f^{[2]})$ jest pierwiastkiem wielomianu $f(X) + X - r$ i kończy rozwiązanie.

Z3.L5 Łatwo widzieć, że $\deg a(b(X)) = \deg a(X) \deg b(X)$ dla dowolnych niezerowych wielomianów w pierścieniu $\mathbb{K}[X]$ wielomianów o współczynnikach w c i e l e. W szczególności, $\deg a^{[2]}(X) = n^2$

jeżeli $\deg a(X) = n$. Równość $f^{[2]}(X) = g^{[2]}(X)$ implikuje więc równość $\deg g(X) = \deg f(X)$. Załóżmy, nie wprost, że $f(X) \neq g(X)$ i oznaczmy $r(X) = f(X) - g(X)$. Wówczas

$$f^{[2]}(X) - g^{[2]}(X) = [g(f(X)) - g(g(X))] + r(f(X)).$$

Różnicę $g(f(X)) - g(g(X))$, tak samo jak w dowodzie T3.1, przedstawiamy w postaci iloczynu

$$(f(X) - g(X))h(X) = r(X)h(X)$$

i znajdujemy sprzeczność z założeniem, że $k := \deg r(X)$ jest $\neq -\infty$. Osobno rozważamy przypadek $k = 0$ i $1 \leqslant k < n$ (!). U w a g a. Unormowanie jest ważne. Przykład: $g(X) = f(-X) \neq f(X)$.

Z3.L6 Mamy $f(-\sin x) = f(\sin(-x)) = f(\cos(-x)) = f(\cos x) = f(\sin x)$ dla każdego $x \in \mathbb{R}$. Stąd widzimy, że $f(-u) = f(u)$ dla nieskończenie wielu $u \in \mathbb{R}$ (mianowicie dla wszystkich $u \in [\,-1;\,1\,]$). Więc, zobacz W2T3.4, $f(-X) = f(X)$. Łatwo uzasadnić (zob. Lemat 2 w rozwiązaniu Z3.J9), że wówczas $f(X) = g(X^2)$ dla pewnego wielomianu $g(X) \in \mathbb{R}[X]$. Mamy wtedy $g(\sin^2 x) = f(\sin x) = f(\cos x) = g(\cos^2 x) = g(1 - \sin^2 x)$. Więc $g(u) = g(1-u)$ dla nieskończenie wielu $u \in \mathbb{R}$. Więc, podobnie jak przed chwilą, $g(X) = g(1-X)$. Rozważmy wielomian $h(X) = g(X+\frac{1}{2})$. Wówczas $h(-X) = g(-X + \frac{1}{2}) = g(1 - (-X + \frac{1}{2})) = g(X + \frac{1}{2}) = h(X)$. Zatem $h(X) = k(X^2)$ dla pewnego wielomianu $k(X) \in \mathbb{R}[X]$. Ostatecznie $f(X) = g(X^2) = h(X^2 - \frac{1}{2}) = k(X^4 - X^2 + \frac{1}{4}) = l(X^4 - X^2)$.

Z3.L7 Wielomian $f(X)$ ma stopień 2 i d w a pierwiastki: $\sqrt{2} = 2\cos\frac{\pi}{4}$ i $-\sqrt{2} = 2\cos\frac{3\pi}{4}$. To nasuwa myśl podstawienia $X = 2\cos u$. Sprawdzamy (indukcyjnie), że

$$f^{[n]}(2\cos u) = 2\cos 2^n u.$$

Wobec tego $f^{[n]}(x) = 0$ (dla $x \in [\,-2;\,2\,]$) zachodzi, gdy $2\cos 2^n u = 0$ (dla $u \in [\,0;\,\pi\,]$). Łatwo wskazać 2^n różnych wartości $u \in [\,0;\,\pi\,]$, dla których zachodzi równość $\cos 2^n u = 0$. U w a g a. Podobnie można wskazać 2^n pierwiastków rzeczywistych wielomianu $f^{[n]}(X) - X$.

Z3.L8 Załóżmy, nie wprost, że istnieją trójmiany kwadratowe $f(X)$, $g(X)$, $h(X)$. Wówczas liczby $h(1), h(2), \ldots, h(8)$ są pierwiastkami wielomianu stopnia czwartego $f(g(X))$. Ponieważ $h(a) = h(b)$ przy $a \neq b$ wtedy i tylko wtedy, gdy liczby a, b leżą symetrycznie względem odciętej wierzchołka paraboli $y = h(x)$, więc musi być $h(1) = h(8)$, $h(2) = h(7)$, $h(3) = h(6)$ i $h(4) = h(5)$, a wierzchołek paraboli $y = h(x)$ ma odciętą równą $9/2$. Ponadto, $h(1) < h(2) < h(3) < h(4)$ lub $h(1) > h(2) > h(3) > h(4)$. Wobec tego liczby $g(h(1))$, $g(h(2))$, $g(h(3))$, $g(h(4))$ są pierwiastkami trójmianu kwadratowego $f(X)$. Zatem $g(h(1)) = g(h(4))$ i $g(h(2)) = g(h(3))$. Więc liczby $h(2)$ i $h(3)$ leżą izotomicznie w przedziale $[\,h(1);\,h(4)\,]$ (są równo odległe od środka tego przedziału), skąd $h(1) + h(4) = h(2) + h(3)$. Kładąc $h(X) = pX^2 + qX + r$ dostajemy równość $17p + 5q + 2r = 13p + 5q + 2r$. Mamy więc sprzeczność, bo $p \neq 0$.

Z3.M1 Oznaczymy przez $\mathcal{M}$ zbiór wszystkich wielomianów $f(X) \in \mathbb{R}[X]$ postaci $g(X) - h(X)$, gdzie $g(X)$, $h(X) \in \mathbb{R}[X]$ są takie, że funkcje $x \longmapsto g(x)$, $x \longmapsto h(x)$ są (ściśle) rosnące. Pokażemy, że $\mathcal{M} = \mathbb{R}[X]$. Rozumujemy przez indukcję względem stopnia. Równość $a = (a + X) - X$ pokazuje, że każdy wielomian stały (tzn., stopnia $\leqslant 0$) należy do $\mathcal{M}$. Załóżmy więc teraz, że wszystkie wielomiany stopnia $\leqslant n$ należą do $\mathcal{M}$ i rozważmy wielomian $f(X)$ stopnia $n+1$. Jest on równy sumie $aX^{n+1} + f_1(X)$, gdzie $\deg f_1(X) \leqslant n$. Rozpatrzymy dwa przypadki: (1) $n = 2k$ i (2) $n = 2k-1$. W przypadku (1) wybieramy dowolną taką liczbę $b > 0$, że $a + b > 0$ i takie wielomiany $g(X)$, $h(X)$, że $f_1(X) = g(X) - h(X)$, a funkcje $x \longmapsto g(x)$ i $x \longmapsto h(x)$ są rosnące. Wówczas równość $f(X) = [(a+b)X^{2k+1} + g(X)] - [bX^{2k+1} + h(X)]$ pokazuje, że $f(X) \in \mathcal{M}$. W przypadku (2) napiszmy najpierw równość $\frac{1}{2k+1}[(X+a)^{2k+1} - X^{2k+1}] = aX^{n+1} + k(X)$ (zob. wzór dwumienny), gdzie $\deg k(X) \leqslant n$. Wtedy $f(X) = \frac{1}{2k+1}[(X+a)^{2k+1} - X^{2k+1}] - k(X) + f_1(X)$. Wielomian $f_1(X) - k(X)$

ma stopień $\leqslant n$ (zob. C3.3(1)), więc należy do $\mathcal{M}$. Pisząc go w odpowiedniej postaci $g(X)-h(X)$ mamy równość $f(X)=[\frac{1}{2k+1}(X+a)^{2k+1}+g(X)]-[\frac{1}{2k+1}X^{2k+1}+h(X)]$ pokazującą, że $f(X)\in\mathcal{M}$.

Z3.M2 Rozwiążemy najpierw C3.44. Po pierwsze łatwo widzieć, że współczynnik C w rozkładzie (3.34) jest $\geqslant 0$. Rzeczywiście, gdy $C<0$ i istnieją pierwiastki rzeczywiste a_j, to dla $x>\max\{a_1,\ldots,a_r\}$ mamy $f(x)<0$. Gdy zaś $C<0$ i nie ma pierwiastków rzeczywistych, to $f(x)<0$ dla wszystkich $x\in\mathbb{R}$. Po drugie łatwo widzieć, że wszystkie wykładniki e_i są parzyste. Załóżmy bowiem (b.s.o.), że $a_1<a_2<\cdots<a_r$ i $e_j=2k+1$. Wówczas dla $a_{j-1}<x_1<a_j<x_2<a_{j+1}$ mamy $f(x_1)f(x_2)<0$, co jest niemożliwe. Wobec tego pierwszą część iloczynu (3.34) zapisujemy w postaci $c(X)^2$, gdzie $c(X)=\sqrt{C}(X-a_1)^{e_1/2}\cdot\ldots\cdot(X-a_r)^{e_r/2}$. Ponieważ wszystkie pozostałe czynniki w rozkładzie (3.34) są postaci $g(X)^2+h(X)^2$, więc, korzystając wielokrotnie z tożsamości podanej we wskazówce, możemy ich iloczyn zapisać w postaci sumy $a_1(X)^2+b_1(X)^2$. Kładąc wreszcie $a(X)=a_1(X)c(X)$ i $b(X)=b_1(X)c(X)$ mamy tezę. Przechodzimy do rozwiązania zadania. Nierówność $f(x)\geqslant 0$ dla $x\geqslant 0$, jak widać z powyższej analizy, oznacza parzystość wykładników e_i dla tych i, dla których $a_i\geqslant 0$. Wykorzystujemy taką wersję tożsamości (8.1):

$$(\alpha^2+X\beta^2)(\gamma^2+X\delta^2)=(\alpha\gamma+X\beta\delta)^2+X(\alpha\delta-\beta\gamma)^2.$$

Czynnik postaci $(X-b)^2+c^2$ łatwo zapisać w postaci $g(X)^2+Xh(X)^2$: Niech $d=\sqrt{b^2+c^2}>|b|$. Wtedy $(X-b)^2+c^2=(X-d)^2+X(\sqrt{2d-2b})^2$. Dalej wszystko powinno być jasne.

Z3.M3 *Odpowiedź*: tak. Oto przykład: $f(X,Y)=X^2Y^4+X^2Y^2+2XY^2+X^2+X+1$. Zapiszmy bowiem $f(x,y)=a(y)x^2+b(y)x+c(y)=(y^4+y^2+1)x^2+(2y^2+1)x+1$. Przy każdym ustalonym $y=y_0\in\mathbb{R}$ widzimy tu trójmian kwadratowy o współczynniku $a=a(y_0)>0$ i ujemnym wyróżniku $\Delta=\Delta(y_0)=b(y_0)^2-4a(y_0)c(y_0)=(2y_0^2+1)^2-4(y_0^4+y_0^2+1)=-3$. Dzięki T3.7 widzimy, że zbiór $\{f(x,y_0):x\in\mathbb{R}\}$ jest równy zbiorowi

$$\mathcal{A}(y_0)=\Big[\,\tfrac{3}{4y_0^4+4y_0^2+4};\,\infty\Big)\,.$$

Ponieważ $\bigcup_{y\in\mathbb{R}}\mathcal{A}(y)=(\,0;\,\infty\,)$, więc mamy tezę.

Z3.N1 Rozważmy dwa (różne!) wielomiany $f(X)=\sum_{j=1}^n X^{k_j}$ i $g(X)=\sum_{j=1}^n X^{l_j}$. Wówczas

$$f(X)^2=\sum_{j=1}^n X^{2k_j}+2\sum_{(i,j)\in\mathcal{A}}X^{k_i+k_j}=f(X^2)+2\sum_{(i,j)\in\mathcal{A}}X^{k_i+k_j}.$$

Podobna równość dla wielomianu $g(X)^2$ pokazuje, że

$$f(X)^2-f(X^2)=2\sum_{(i,j)\in\mathcal{A}}X^{\varphi(i,j)}=2\sum_{(i,j)\in\mathcal{A}}X^{b(\psi(i,j))}=g(X)^2-g(X^2).$$

Mamy więc równość $f(X)^2-g(X)^2=f(X^2)-g(X^2)$. Jednocześnie, ponieważ $f(1)=g(1)=n$, więc wielomian $f(X)-g(X)$ ma pierwiastek $\alpha=1$. Zatem $f(X)-g(X)=(X-1)^k\,h(X)$ dla pewnego $k\in\mathbb{N}$ i pewnego wielomianu $h(X)$, przy czym $h(1)\neq 0$. Stąd

$$f(X)+g(X)=\frac{f(X)^2-g(X)^2}{f(X)-g(X)}=\frac{f(X^2)-g(X^2)}{f(X)-g(X)}=\frac{(X^2-1)^k\,h(X^2)}{(X-1)^k\,h(X)}=(X+1)^k\frac{h(X^2)}{h(X)}.$$

Kładąc tu $X=1$ dostajemy równość $2n=2^k$.

Rozdział 4

Funkcje arytmetyczne

Lisez Euler, c'est notre maître à tous.
(Pierre Simon de Laplace)

W tym krótkim rozdziale zdefiniujemy kilka prostych ale użytecznych funkcji arytmetycznych. Najważniejszą z nich jest funkcja Eulera φ. Przypomnijmy, że (dla nas) zbiór liczb naturalnych to $\mathbb{N} = \{x \in \mathbb{Z} : x \geqslant 1\}$.

Definicja 4.1 Dowolną funkcję $f : \mathbb{N} \longrightarrow \mathbb{C}$ nazywamy **funkcją arytmetyczną**.

Funkcje arytmetyczne rozważane w dalszym ciągu, przyjmują zazwyczaj wartości całkowite (w $\mathbb{Z}$). Szczególnie ważne są funkcje arytmetyczne multyplikatywne.

Definicja 4.2 Funkcję arytmetyczną f nazywamy **multyplikatywną**, gdy nie jest równa tożsamościowo 0 i dla dowolnych względnie pierwszych $m, n \in \mathbb{N}$ zachodzi równość

$$f(mn) = f(m)f(n). \tag{4.1}$$

Ćwiczenie 4.1 Jeżeli f jest multyplikatywną funkcją arytmetyczną, to $f(1) = 1$.

4.1 Sumy potęg dzielników

W tym paragrafie pokażemy parę ćwiczeń na temat ilości, sumy i, ogólniej, sumy potęg dzielników dodatnich danej liczby naturalnej.

Definicja 4.3 Niech $\alpha \in \mathbb{R}$. Dla danej liczby naturalnej n oznaczamy

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha.$$

Sumowanie rozciąga się na wszystkie dodatnie dzielniki liczby n.

Ćwiczenie 4.2 Udowodnić, że funkcja σ_α, dla dowolnego $\alpha \in \mathbb{R}$, jest funkcją multyplikatywną. *Wskazówka.* Jeżeli $m \perp n$, to $d|mn$ wtedy i tylko wtedy, gdy istnieje dokładnie jedna taka para dzielników (dodatnich) $d_1|m$, $d_2|n$, że $d = d_1 d_2$.

Uwaga. Jasne, że funkcja multyplikatywna jest jednoznacznie wyznaczona przez swoje wartości na potęgach liczb pierwszych.

4.1.1 Funkcja τ

Liczbę $\sigma_0(n)$ wyrażającą, zgodnie ze wzorem (4.1), liczbę (dodatnich) dzielników liczby naturalnej n oznacza się prościej $\tau(n)$.

Ćwiczenie 4.3 Udowodnić, że jeżeli $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ jest kanonicznym rozkładem liczby naturalnej n na czynniki pierwsze, to

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdot \ldots \cdot (e_s + 1). \tag{4.2}$$

Ćwiczenie 4.4 Udowodnić, że $\tau(n)$ jest liczbą nieparzystą wtedy i tylko wtedy, gdy n jest kwadratem (liczby naturalnej).

U w a g a. Teza tego ćwiczenia wynika natychmiast z równości (4.2). Warto jednak przeprowadzić niezależne rozumowanie następująco: Jeżeli $d < \sqrt{n}$ jest dzielnikiem n, to n/d jest dzielnikiem n spełniającym (oczywiście) nierówność $n/d > \sqrt{n}$. Dla danej liczby n zachodzi więc jedna z dwóch możliwości:

(1) $\sqrt{n} \notin \mathbb{N}$ i wtedy dzielniki n występują w parach $\{d, \frac{n}{d}\}$, więc $2|\tau(n)$, albo

(2) $\sqrt{n} \in \mathbb{N}$ i wtedy $\sqrt{n}$ jest jedynym dzielnikiem bez pary. W tym przypadku $2 \nmid \tau(n)$.

Ćwiczenie 4.5 Udowodnić nierówność $\tau(n) \leqslant 2\sqrt{n}$.

Ćwiczenie 4.6 Rozwiązać ***zadanie o znudzonych uczniach***: W pewnej szkole każdy z 456 uczniów ma swój kod będący jedną z liczb 1, 2, ..., 456 i swoją szafkę oznaczoną tym kodem. W dniu wagarowicza (tego dnia nie było nieobecnych) bawili się oni następująco: uczeń mający kod n, przyszedłszy do szkoły przechodził wzdłuż korytarza z szafkami i zmieniał stan (zamknięte otwierał, a otwarte zamykał) wszystkich szafek, których numer był podzielny przez n. Przed rozpoczęciem zabawy wszystkie szafki były zamknięte. Udowodnić, że po zakończeniu zabawy pan woźny znalazł dokładnie 21 otwartych szafek. Rozwiązać też ***zadanie o woźnym matematyku***: Ponieważ otwieranie i zamykanie szafek bardzo się im spodobało, uczniowie tej szkoły postanowili bawić się w to co ranka. Pan woźny twierdzi, że potrafi – tylko na podstawie stanu szafek – wskazać kody uczniów nieobecnych danego dnia w szkole. Udowodnić, że pan woźny ma podstawy do takiego twierdzenia.

Ćwiczenie 4.7 Udowodnić równość $\prod_{d|n} d = n^{\tau(n)/2}$.

Ćwiczenie 4.8 Oznaczamy $T(n) := \tau(1) + \tau(2) + \ldots + \tau(n)$. Udowodnić, że dla dowolnego $n \in \mathbb{N}$ zachodzi równość

$$T(n) = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \ldots + \left\lfloor \frac{n}{n} \right\rfloor.$$

Ćwiczenie 4.9 Udowodnić, że dla dowolnej liczby naturalnej n zachodzi równość

$$\sum_{d|n} \tau(d)^3 = \Big(\sum_{d|n} \tau(d)\Big)^2. \tag{4.3}$$

4.1.2 Funkcja σ

Liczbę $\sigma_1(n)$ oznacza się prościej $\sigma(n)$.

Ćwiczenie 4.10 Udowodnić, że jeżeli $n = p_1^{e_1}p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ jest kanonicznym rozkładem liczby naturalnej n na czynniki pierwsze, to

$$\sigma(n) = \frac{p_1^{e_1+1}-1}{p_1-1} \cdot \frac{p_2^{e_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_s^{e_s+1}-1}{p_s-1}.$$

ZADANIE 4.1 Udowodnić, że dla dowolnej liczby naturalnej n zachodzą nierówności

$$\frac{1}{2}n(n-1) \leqslant \sigma(1) + \sigma(2) + \ldots + \sigma(n) \leqslant n^2. \tag{4.4}$$

R o z w i ą z a n i e. Liczba $d \leqslant n$ występuje jako składnik sumy $\sum_{k\leqslant n}\sigma(k)$ dokładnie $\lfloor n/d \rfloor$ razy. Zatem $\sum_{k=1}^{n}\sigma(k) = \lfloor \frac{n}{1} \rfloor \cdot 1 + \lfloor \frac{n}{2} \rfloor \cdot 2 + \ldots + \lfloor \frac{n}{n} \rfloor \cdot n$. Stąd (wobec $x - 1 < \lfloor x \rfloor \leqslant x$)

$$n^2 - \frac{n(n+1)}{2} = \sum_{k=1}^{n}\left(\frac{n}{k} - 1\right) \cdot k < \sum_{k=1}^{n}\sigma(k) \leqslant \sum_{k=1}^{n}\frac{n}{k} \cdot k = n^2. \quad \Diamond$$

Ćwiczenie 4.11 Udowodnić, że dla dowolnej liczby naturalnej n zachodzi nierówność

$$\frac{\sigma(1)}{1} + \frac{\sigma(2)}{2} + \ldots + \frac{\sigma(n)}{n} \leqslant 2n.$$

Ćwiczenie 4.12 Udowodnić, że $\sigma(n)$ jest liczbą nieparzystą wtedy i tylko wtedy, gdy n jest kwadratem lub podwojonym kwadratem.

Liczbę naturalną n nazywamy **liczbą doskonałą**, gdy równa jest sumie swoich właściwych (tzn., różnych od n) dzielników naturalnych. Czyli, gdy $\sigma(n) = 2n$.

ZADANIE 4.2 Udowodnić dwa twierdzenia o liczbach doskonałych:

(1) (***Twierdzenie Euklidesa***) *Jeżeli M_p jest liczbą pierwszą Mersenne'*a, *to liczba $2^{p-1}M_p$ jest liczbą doskonałą*;

(2) (***Twierdzenie Eulera***) *Jeżeli n jest p a r z y s t ą liczbą doskonałą, to istnieje taka liczba pierwsza Mersenne'*a M_p, *że $n = 2^{p-1}M_p$.*

R o z w i ą z a n i e. (1) Na mocy C4.10 mamy $\sigma(2^{p-1}M_p) = (2^p - 1) \cdot (M_p^2 - 1)/(M_p - 1) = M_p(M_p + 1) = 2^pM_p = 2n$.

(2) Niech $n = 2^{e-1}m$, gdzie $e > 1$ i $m \equiv 1 \pmod 2$. Zatem, zobacz C4.2, $2^em = 2n = \sigma(2^{e-1}m) = \sigma(2^{e-1})\sigma(m) = (2^e - 1)\sigma(m)$. Stąd, ponieważ $2^e \perp 2^e - 1$, na mocy ZTA, $\sigma(m) = 2^e \cdot a$ i jednocześnie $m = (2^e - 1)a$ przy pewnym $a \in \mathbb{N}$. Ostatnią równość zapisujemy w postaci $m = 2^e \cdot a - a$. Stąd $m + a = 2^e \cdot a = \sigma(m)$. Ponieważ $m|m$ i $a|m$, więc m i a są j e d y n y m i dzielnikami liczby m. Zatem m jest liczbą pierwszą, a $a = 1$. Czyli $m = M_e$ i $e = p$ jest też liczbą pierwszą (zobacz 2.3.3 P3). $\Diamond$

U w a g a. Liczby $6 = 2^{2-1}(2^2 - 1)$, $28 = 2^{3-1}(2^3 - 1)$, $496 = 2^{5-1}(2^5 - 1)$ są pierwszymi trzema liczbami doskonałymi. Dotychczas nie znaleziono żadnej nieparzystej liczby doskonałej.

4.2 Funkcja φ Eulera

Najczęściej spotykaną w teorii liczb funkcją arytmetyczną jest **funkcja φ Eulera**.

Definicja 4.4 Symbolem $\varphi(n)$ oznaczmy moc zbioru liczb naturalnych mniejszych lub równych n i względnie pierwszych z n. Tzn., $\varphi(n) = \operatorname{card}\{k \in \mathbb{N} : k \leqslant n,\ k \perp n\}$.

TWIERDZENIE 4.1 *Funkcja φ Eulera jest funkcją multyplikatywną.*

D O W Ó D. Niech $\operatorname{NWD}(m, n) = 1$. Chcemy wskazać te spośród liczb $1, 2, \ldots, mn$, które są względnie pierwsze z mn. W tym celu ustawmy te liczby w tablicę:

$$\begin{array}{cccccc} 1 & 2 & \ldots & k & \ldots & m \\ m+1 & m+2 & \ldots & m+k & \ldots & m+m \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+k & \ldots & (n-1)m+m \end{array}$$

W tablicy tej występują dwa typy kolumn: kolumnę nazwiemy *dobrą*, gdy jej nagłówek k jest względnie pierwszy z m, pozostałe kolumny nazwiemy *złymi*. Prawdziwe są tezy:

(1) Kolumn dobrych jest $\varphi(m)$.

(2) Każdy wyraz złej kolumny ma wspólny, większy od 1, dzielnik z m, więc tym bardziej z mn. Liczby względnie pierwsze z mn występują więc w y ł ą c z n i e w kolumnach dobrych.

(3) Każda kolumna ma n wyrazów, z których każdy daje i n n ą resztę z dzielenia przez n. Wobec tego dokładnie $\varphi(n)$ z nich jest względnie pierwszych z n.

Dowód dwóch pierwszych tez pozostawiamy Czytelnikowi. Trzecią uzasadniamy tak: Załóżmy, że wyrazy $k + sm$, $k + tm$ $(0 \leqslant s \leqslant t < n)$ k-tej kolumny dają przy dzieleniu przez n tę samą resztę r. Czyli że $k + sm = qn + r$ i $k + tm = q'n + r$. Odejmując dostajemy $(t - s)m = (q' - q)n$. Wówczas, na mocy ZTA, $n|(t - s)$, co pokazuje, że $t - s = 0$, bo $0 \leqslant t - s < n$. Wobec tego (przestawiając) możemy zapisać wyrazy danej kolumny: $q_0 n$, $q_1 n + 1$, $\ldots$, $q_{n-1} n + n - 1$. Jasne, że wśród nich jest $\varphi(n)$ względnie pierwszych z n.

Ponieważ dana liczba naturalna jest względnie pierwsza z mn wtedy i tylko wtedy, gdy jest względnie pierwsza zarówno z m jak i z n, więc znaleźliśmy $\varphi(m)\varphi(n)$ liczb względnie pierwszych z mn w naszej tablicy. To kończy dowód. □

Z kolejnej własności funkcji φ Eulera będziemy korzystać w rozdziale 5:

TWIERDZENIE 4.2 (***Gauss***) *Dla każdej liczby naturalnej n zachodzi równość*

$$n = \sum_{d|n} \varphi(d). \tag{4.5}$$

D O W Ó D. Wypiszmy kolejno wszystkie ułamki (właściwe) o mianowniku n:

$$\tfrac{1}{n},\quad \tfrac{2}{n},\quad \tfrac{3}{n},\quad \ldots\quad ,\quad \tfrac{n}{n}$$

i sprowadźmy je do postaci nieskracalnej:

$$\tfrac{1}{n},\quad \ldots\quad ,\ \tfrac{k}{d},\quad \ldots\quad ,\ \tfrac{1}{1}.$$

Typowy ułamek z tego (n-wyrazowego) ciągu ma postać $\frac{k}{d}$, gdzie d jest dzielnikiem n, a k jest jedną z $\varphi(d)$ liczb naturalnych $\leqslant d$ i względnie pierwszych z d. To kończy dowód. □

TWIERDZENIE 4.3 *Jeżeli* $n > 1$ *jest liczbą naturalną oraz* $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ *jest kanonicznym rozkładem* n *na czynniki pierwsze, to*

$$\boxed{\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right).} \tag{4.6}$$

D O W Ó D. Jasna(?!) równość $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$ i multyplikatywność funkcji φ kończą dowód. Dobrze jednak przeprowadzić rozumowanie niezależne (dowodzące zresztą, że φ jest multyplikatywna). Korzystamy przy tym z Zasady Włączeń-Wyłączeń, zob. $\mathbb{KOM}$.

Dla każdego dzielnika pierwszego $p_i|n$ oznaczmy przez A_i zbiór takich wszystkich liczb naturalnych k, że $k \leqslant n$ i $p_i|k$. Jasne, że $|A_i| = \frac{n}{p_i}$, i, ogólnie

$$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_t}| = \frac{n}{p_{i_1} p_{i_2} \cdot \ldots \cdot p_{i_t}}$$

dla różnych $1 \leqslant i_1 < i_2 < \ldots < i_t \leqslant s$. Ponadto, suma $A_1 \cup A_2 \cup \ldots \cup A_s$ składa sie z tych wszystkich liczb $k \in [\,n\,]$, dla których $\mathrm{NWD}\,(k,\, n) \neq 1$. Zatem $\varphi(n) = n - |A_1 \cup A_2 \cup \ldots \cup A_s|$. To, po wykorzystaniu równości włączeń-wyłączeń, łatwo daje (4.6). □

P r z y k ł a d. Korzystając z multyplikatywności funkcji φ możemy (za Eulerem) pokazać nasz P I Ą T Y D O W Ó D TE: Zakładając, że $p_1 = 2, \ldots, p_r$ są liczbami pierwszymi, wybieramy liczbę $1 < m < p_1 \cdot \ldots \cdot p_r$ względnie pierwszą z $p_1 \cdot \ldots \cdot p_r$ (taka liczba m istnieje, bo $\varphi(p_1 \cdot \ldots \cdot p_r) = \varphi(p_1) \cdot \ldots \cdot \varphi(p_r) = (p_1 - 1) \cdot \ldots \cdot (p_r - 1) \geqslant 2$). Wybierając dowolny pierwszy dzielnik $p|m$, zob. T2.14, znajdujemy n o w ą, tzn. różną od $p_1, \ldots, p_r$, liczbę pierwszą. ◊

Ćwiczenie 4.13 Udowodnić, że $\varphi(n)$ jest liczbą parzystą dla każdego $n \geqslant 3$.

Ćwiczenie 4.14 Udowodnić, że jeżeli $m|n$, to $\varphi(m)|\varphi(n)$.

Ćwiczenie 4.15 Udowodnić, że $\varphi(d)\varphi(mn) = d\varphi(m)\varphi(n)$, gdzie $d = \mathrm{NWD}\,(m,\, n)$.

4.3 Splot Dirichlet'*a* i odwracanie Möbiusa

Niech $\mathcal{A}$ oznacza zbiór wszystkich funkcji arytmetycznych. W zbiorze tym, poza oczywistym działaniem $+$ dodawania funkcji, można wprowadzić pewne działanie mnożenia. Mnożenie to nazywa się splotem Dirichlet'*a* i oznacza $*$. Układ $(\mathcal{A},\, +,\, *)$ okaże się być pierścieniem przemiennym z jedynką, zobacz D1.7.

4.3.1 Splot Dirichlet'*a*

Mnożenie splotowe ma wiele zastosowań w teorii liczb.

Definicja 4.5 Niech dane będą dwie funkcje arytmetyczne f i g. **Splotem Dirichlet'*a*** tych funkcji nazywamy funkcję arytmetyczną $f * g$ daną wzorem

$$(f * g)(n) = \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right).$$

Ćwiczenie 4.16 Udowodnić, że splot jest działaniem łącznym i przemiennym.

Ćwiczenie 4.17 Splot funkcji multyplikatywnych jest funkcją multyplikatywną.

Ćwiczenie 4.18 Uzasadnić, że funkcja arytmetyczna ε dana przez

$$\varepsilon(n) = \begin{cases} 1, & \text{gdy} \quad n = 1, \\ 0, & \text{gdy} \quad n > 1, \end{cases} \tag{4.7}$$

jest elementem neutralnym względem splotu.

4.3.2 Twierdzenie Möbiusa o odwracaniu

Dziwnie wyglądająca (na pierwszy rzut oka) funkcja μ Möbiusa jest niezwykle przydatna.

Definicja 4.6 (**Funkcja μ Möbiusa**) Jeżeli $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ jest kanonicznym rozkładem liczby naturalnej n na czynniki pierwsze, to kładziemy

$$\mu(n) = \begin{cases} 1, & \text{gdy } n = 1, \\ (-1)^s, & \text{gdy wszystkie } e_i \text{ są równe } 1, \\ 0, & \text{gdy przynajmniej jeden z wykładników } e_i \text{ jest } \geqslant 2. \end{cases} \tag{4.8}$$

TWIERDZENIE 4.4 *Funkcja μ Möbiusa jest funkcją multyplikatywną.*

D O W Ó D. Dowód jest natychmiastowy: jeżeli $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$, $m = q_1^{f_1} q_2^{f_2} \cdot \ldots \cdot q_t^{f_t}$ są względnie pierwsze, to żadne p_i nie jest równe żadnemu q_j. Przypadek, gdy któreś e_i lub któreś f_j jest $\geqslant 2$, jest oczywisty. Przypadek, gdy wszystkie $e_i = 1$ i wszystkie $f_j = 1$, jest równie oczywisty i sprowadza się do równości $(-1)^{s+t} = (-1)^s \cdot (-1)^t$. □

Określimy teraz jeszcze jedną arcyprostą funkcję arytmetyczną wzorem

$$\mathbf{1}(n) = 1 \quad \text{dla każdego } n \in \mathbb{N}. \tag{4.9}$$

P r z y k ł a d 1. Mamy $(\mathbf{1} * \mathbf{1})(n) = \sum_{d|n} \mathbf{1}(d) \cdot \mathbf{1}\left(\frac{n}{d}\right) = \sum_{d|n} 1 = \tau(n)$. ◊

ZADANIE 4.3 Udowodnić, że funkcje μ i $\mathbf{1}$ są wzajemnie swoimi odwrotnościami względem splotu. Czyli, że $\mu * \mathbf{1} = \varepsilon$

R o z w i ą z a n i e. Ponieważ μ i $\mathbf{1}$ są funkcjami multyplikatywnymi więc ich splot też jest multyplikatywny. Zatem, zobacz 4.1 U, wystarczy sprawdzić, że $(\mu * \mathbf{1})(p^k) = 0$ dla każdego $p \in \mathbb{P}$ i każdego $k \in \mathbb{N}$. A to jest jasne. ◊

P r z y k ł a d 2. Dla każdej liczby naturalnej n zachodzi równość

$$\sum_{d|n} \tau(d)\mu\left(\tfrac{n}{d}\right) = 1. \tag{4.10}$$

Rzeczywiście, wobec P1, $\tau * \mu = (\mathbf{1} * \mathbf{1}) * \mu = \mathbf{1} * (\mathbf{1} * \mu) = \mathbf{1} * \varepsilon = \mathbf{1}$ (zobacz C4.18). ◊

P r z y k ł a d 3. Niech $\iota(n) = n$ dla każdego n. Równość (4.5) może być zapisana tak: $\varphi * \mathbf{1} = \iota$. Wobec tego, dla każdego $n \in \mathbb{N}$,

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}, \tag{4.11}$$

co jest tylko innym zapisem równości $\varphi = \varphi * (\mathbf{1} * \mu) = (\varphi * \mathbf{1}) * \mu = \iota * \mu$. ◊

TWIERDZENIE 4.5 (***Twierdzenie Möbiusa o odwracaniu***) *Jeżeli dana jest funkcja arytmetyczna f, a funkcja arytmetyczna g zadana jest wzorem*

$$g(n) = \sum_{d|n} f(d), \tag{4.12}$$

to dla każdego $n \in \mathbb{N}$

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right). \tag{4.12'}$$

D O W Ó D. Zauważmy, że równość (4.12) może być zapisana jako $g = \mathbf{1} * f$. Reszta, tak jak w P2 i P3, wynika z łączności splotu i ze wzajemnej odwrotności funkcji μ i $\mathbf{1}$. □

Ćwiczenie 4.19 Udowodnić, że obie równości (4.12) i (4.12') są równoważne równości

$$\sum_{k=1}^{n} g(k) = \sum_{d=1}^{n} \left\lfloor \frac{n}{d} \right\rfloor f(d). \tag{4.12"}$$

Multyplikatywna (dotycząca mnożenia) wersja wynikania (4.12) ⇒ (4.12') opisana jest w C4.20. Przez $\mathbb{C}^*$ oznaczamy zbiór niezerowych liczb zespolonych.

Ćwiczenie 4.20 Dana jest funkcja arytmetyczna $f : \mathbb{N} \longrightarrow \mathbb{C}^*$. Oznaczymy przez h funkcję arytmetyczną daną wzorem $h(n) = \prod_{d|n} f(d)$ dla każdego n. Udowodnić, że wówczas

$$f(n) = \prod_{d|n} h\left(\tfrac{n}{d}\right)^{\mu(d)}.$$

Wskazówka. $\prod_{d|n} h(\frac{n}{d})^{\mu(d)} = \prod_{d|n} \prod_{e|\frac{n}{d}} f(e)^{\mu(d)} = \prod_{ed|n} f(e)^{\mu(d)} = \prod_{e|n} f(e)^{\sum_{d|\frac{n}{e}} \mu(d)} = f(n)$.

Zastosujemy powyższe do wzbogacenia wiedzy o wielomianach cyklotomicznych, zob. 3.4.6.

Ćwiczenie 4.21 Udowodnić, że n-ty wielomian cyklotomiczny wyraża się formułą

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu\left(\frac{n}{d}\right)}. \tag{4.13}$$

Ćwiczenie 4.22 Udowodnić, że wielomian cyklotomiczny $\Phi_n(X)$ ma współczynniki całkowite. *Wskazówka.* Wielomiany stojące w liczniku i mianowniku ilorazu z prawej strony równości (4.13) są unormowane i należą do $\mathbb{Z}[X]$. Zobacz też dowód T3.3.

Ćwiczenie 4.23 Uzasadnić, że $\deg \Phi_n(X) = \varphi(n)$. Uzasadnić też, że wyraz wolny $\Phi_n(0)$ jest równy ± 1. *Wskazówka.* Zobacz (3.46).

4.4 Piętnaście zadań dodatkowych

Warto rozwiązać jeszcze kilka zadań.

4.4.1 Treści zadań

Do rozwiązania poniższych zadań wystarczy teoria wyłożona w poprzednich rozdziałach. W jednym miejscu korzystamy z tak zwanego Postulatu Bertrand'*a*, zob. T12.11.

A. Zadania o funkcjach τ, σ i φ

ZADANIE 4.A1 Uzasadnić, że zbiór $\{n \in \mathbb{N} : \tau(n)|n\}$ jest nieskończony.

ZADANIE 4.A2 Dowieść, że jeżeli $\varphi(n)|n$, to n jest postaci $2^a 3^b$.

ZADANIE 4.A3 Udowodnić: **(1)** $\sigma(n) > \tau(n)\sqrt{n}$ dla dowolnego $n \in \mathbb{N}_{\neq 1}$; **(2)** $\varphi(n) \geqslant \sqrt{n}$ dla wszystkich $n \neq 2, 6$; **(3)** $\varphi(n) \leqslant n - \sqrt{n}$ dla złożonych $n \in \mathbb{N}$.

ZADANIE 4.A4 Obliczyć w ciągu 10 minut sumę $\sum_{k=1}^{100} \tau(k)$.

ZADANIE 4.A5 Rozwiązać w liczbach naturalnych równanie $\tau(n) + \varphi(n) = n$.

ZADANIE 4.A6 Udowodnić, że istnieje nieskończenie wiele takich liczb naturalnych $n \geqslant 2$, dla których spełniona jest nierówność $\frac{\sigma(n)}{n} > \max\{\frac{\sigma(1)}{1}, \frac{\sigma(2)}{2}, \ldots, \frac{\sigma(n-1)}{n-1}\}$.

ZADANIE 4.A7 Udowodnić, że jeżeli $\sigma(n)$ jest potęgą (o wykładniku naturalnym) liczby 2, to również $\tau(n)$ jest potęgą (o wykładniku naturalnym) liczby 2.

ZADANIE 4.A8 Udowodnić, że dla każdej liczby $n \in \mathbb{N}$ zachodzi równość

$$\left\lfloor \frac{n}{1} \right\rfloor \varphi(1) + \left\lfloor \frac{n}{2} \right\rfloor \varphi(2) + \ldots + \left\lfloor \frac{n}{n} \right\rfloor \varphi(n) = \frac{n(n+1)}{2}. \tag{4.14}$$

B. Inne funkcje arytmetyczne

ZADANIE 4.B1 Dla $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s} \in \mathbb{N}$ kładziemy $\lambda(n) = (-1)^{e_1+e_2+\cdots+e_s}$, w szczególności $\lambda(1) = 1$. Udowodnić, że $\lambda * \mathbf{1}$ jest funkcją charakterystyczną podzbioru kwadratów w $\mathbb{N}$.

ZADANIE 4.B2 Przez $\sigma_+(n)$ oznaczamy sumę tych naturalnych dzielników k liczby n, dla których $\lambda(k) = +1$ (zob. Z4.B1), przez $\sigma_-(n)$ oznaczamy sumę pozostałych dzielników naturalnych liczby n. Udowodnić, że $n \longmapsto \sigma_+(n) - \sigma_-(n)$ jest funkcją arytmetyczną multyplikatywną.

ZADANIE 4.B3 Przez $i(n)$ oznaczmy iloczyn wszystkich (naturalnych) dzielników liczby naturalnej n. Rozstrzygnąć, czy istnieją różne liczby m, n, dla których $i(m) = i(n)$.

C. Funkcja arytmetyczna π

ZADANIE 4.C1 Przez $\pi(n)$ oznaczamy moc zbioru $\mathbb{P} \cap \{1, 2, \ldots, n\}$, czyli liczbę liczb pierwszych $\leqslant n$. Udowodnić ***Twierdzenie Eulera***: $\lim_{n\to\infty} \frac{\pi(n)}{n} = 0$.

ZADANIE 4.C2 Udowodnić, że zbiór $\{n \in \mathbb{N} : \pi(n)|n\}$ jest nieskończony.

D. Drugie twierdzenie Möbiusa o odwracaniu

ZADANIE 4.D1 Niech $f : (0; \infty) \longrightarrow \mathbb{C}$ będzie dowolną funkcją spełniającą warunek $f(x) = 0$ dla wszystkich $x \in (0; 1)$. Oznaczmy przez F funkcję $F(x) = \sum_{k\in\mathbb{N}} f(\frac{x}{k})$ (suma pusta jest z definicji równa 0). Udowodnić, że wówczas $f(x) = \sum_{k\in\mathbb{N}} \mu(k) F(\frac{x}{k})$ dla każdego $x > 0$.

ZADANIE 4.D2 Udowodnić równość

$$\varphi(1) + \varphi(2) + \cdots + \varphi(n) = \frac{1}{2} + \frac{1}{2} \sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2. \tag{4.15}$$

4.4.2 Rozwiązania wybranych ćwiczeń i zadań dodatkowych

Pokazujemy też rozwiązania wybranych ćwiczeń z tego rozdziału.

C4.6 (ZZU) Zauważmy, że (po zakończonej zabawie) szafka o numerze k będzie otwarta iff zmieniano jej stan nieparzystą liczbę razy. Ponieważ jej stan zmieniali ci (i tylko ci) uczniowie, których kod jest dzielnikiem numeru k, więc szafka o numerze k będzie otwarta iff $\tau(k)$ jest liczbą nieparzystą, czyli, zob. C4.4, iff k jest kwadratem. Kwadratów $\leqslant 456$ jest dokładnie 21.

(ZWM) *Absencją* (danego dnia) nazwiemy podzbiór zbioru $[\,n\,]=\{1,\,2,\ldots,\,n\}$ składający się z numerów uczniów nieobecnych (tego dnia) w szkole. Zbiór $\mathcal{A}$ wszystkich *absencji* utożsamiamy więc ze zbiorem potęgowym $\mathcal{P}([\,n\,])$, zob. $\mathbb{KOM}$. Zbiór $\mathcal{S}$ możliwych stanów szafek (utożsamialny ze zbiorem ciągów binarnych długości n, zob. $\mathbb{KOM}$) równie łatwo utożsamiamy ze zbiorem potęgowym $\mathcal{P}([\,n\,])$. Wymyślona przez uczniów zabawa wyznacza f u n k c j ę $Z:\mathcal{A}\longrightarrow\mathcal{S}$. Pan woźny twierdzi, że Z jest b i j e k c j ą. Dla uzasadnienia jego tezy wystarczy udowodnić, że Z jest i n j e k c j ą (zobacz $\mathbb{KOM}$ C1.12). Niech więc A_1 będzie *absencją* pewnego dnia (powiedzmy we wtorek), A_2 absencją innego dnia (powiedzmy w środę) i załóżmy, że $A_1\neq A_2$. Wówczas co najmniej jeden ze zbiorów $A_1\smallsetminus A_2$, $A_2\smallsetminus A_1$ jest niepusty ($A_1\smallsetminus A_2=A_2\smallsetminus A_1=\varnothing$ iff $A_1=A_2$). Załóżmy (b.s.o.), że $A_1\smallsetminus A_2\neq\varnothing$ i że k jest najmniejszą liczbą zbioru $A_1\smallsetminus A_2$. To znaczy, że uczeń o kodzie k był nieobecny we wtorek i obecny w środę, a każdy uczeń o kodzie mniejszym niż k albo był obecny we wtorek i w środę, albo był nieobecny i we wtorek i w środę. Jasnym być powinno, że pan woźny zobaczy inny stan szafki o numerze k we wtorek a inny w środę. Zatem $Z(A_1)\neq Z(A_2)$.

C4.8 Wyobraźmy sobie tablicę kwadratową (szachownicę) wymiaru $n\times n$. W pole $(k,\,l)$ (czyli l-te pole k-tego wiersza) wpisujemy *krzyżyk* wtedy i tylko wtedy, gdy $l|k$. Należy teraz zauważyć, że obie strony dowodzonej równości wyrażają liczbę wszystkich *krzyżyków*: lewa strona "zlicza" *krzyżyki* wierszami, a prawa "zlicza" *krzyżyki* kolumnami. (Zasada podwójnego zliczania!)

C4.9 Korzystamy z (łatwej do udowodnienia przez indukcję) równości

$$\sum_{k=1}^{N}k^3=(\sum_{k=1}^{N}k)^2. \tag{4.16}$$

Dzięki niej widzimy, że równość (4.3) jest prawdziwa, gdy n jest potęgą p^e liczby pierwszej. Przypadek dowolnego n najprościej jest sprawdzić dowodząc, że funkcje $n\longmapsto\sum_{d|n}\tau(d)^3$ i $n\longmapsto(\,\sum_{d|n}\tau(d)\,)^2$ są funkcjami arytmetycznymi multyplikatywnymi. Zobacz 4.1 U i C4.17.

C4.11 Oznaczmy $\Sigma(n)=\sigma(1)+\sigma(2)+\,\ldots\,+\sigma(n)$ dla $n\in\mathbb{N}$. Z Z4.1 mamy $\Sigma(n)\leqslant n^2$. Stosujmy metodę sumowania przez części (transformację Abela):

$$\begin{aligned}\sum_{k=1}^{n}\frac{\sigma(k)}{k}&=\frac{\Sigma(1)}{1}+\frac{\Sigma(2)-\Sigma(1)}{2}+\cdots+\frac{\Sigma(n)-\Sigma(n-1)}{n}=\\&=\left(1-\tfrac12\right)\Sigma(1)+\left(\tfrac12-\tfrac13\right)\Sigma(2)+\left(\tfrac13-\tfrac14\right)\Sigma(3)+\cdots+\left(\tfrac{1}{n-1}-\tfrac1n\right)\Sigma(n-1)+\tfrac1n\Sigma(n)\leqslant\\&\leqslant\left(1-\tfrac12\right)\cdot1^2+\left(\tfrac12-\tfrac13\right)\cdot2^2+\left(\tfrac13-\tfrac14\right)\cdot3^2+\cdots+\left(\tfrac{1}{n-1}-\tfrac1n\right)\cdot(n-1)^2+\tfrac1n\cdot n^2=\\&=\sum_{k=1}^{n-1}\tfrac{1}{k(k+1)}\cdot k^2+n=\sum_{k=1}^{n-1}\tfrac{k}{k+1}+n.\end{aligned}$$

Sprawdzenie, że $\sum_{k=1}^{n-1}\frac{k}{k+1}\leqslant n$, jest natychmiastowe.

Z4.A1 Do tego zbioru należą wszystkie liczby $n=p^{p-1}$ dla $p\in\mathbb{P}$.

Z4.A2 Korzystając z (4.6), łatwo uzasadnić, że jeżeli liczba n ma (co najmniej) dwa różne nieparzyste dzielniki pierwsze, to $\varphi(n) \nmid n$. Rzeczywiście, pisząc $n = 2^a p^b q^c m$, gdzie $2 < p < q$ są liczbami pierwszymi, $2 \perp m$, $p \perp m$, $q \perp m$, oraz $b, c \geqslant 1$, mamy $\varphi(n) = 2^{a-1}p^{b-1}(p-1)q^{c-1}(q-1)\varphi(m)$, gdy $a \geqslant 1$, oraz $\varphi(n) = p^{b-1}(p-1)q^{c-1}(q-1)\varphi(m)$, gdy $a = 0$. W każdym z tych dwóch przypadków $v_2(\varphi(n)) > v_2(n)$, patrz teraz C2.41. Zbadanie liczb postaci $2^a p^b$ pozostawiamy Czytelnikowi.

Z4.A3(1) Niech $D_+(n) = \{d_1, \ldots, d_s\}$ $(s = \tau(n))$. Korzystając z nierówności AG mamy

$$\frac{\sigma(n)}{\tau(n)} = \frac{d_1 + \cdots + d_s}{s} > \sqrt[s]{d_1 \cdot \ldots \cdot d_s}.$$

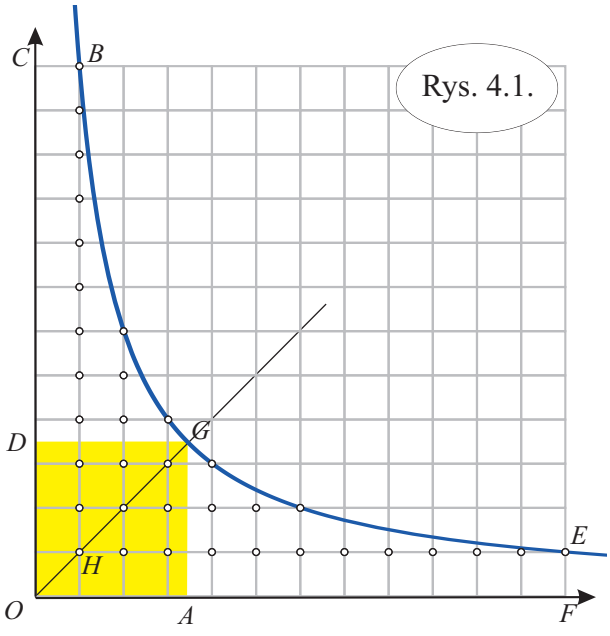
Nierówność jest ostra, bo d_i są różne. Wystarczy więc uzasadnić, że $\sqrt[s]{d_1 \cdot \ldots \cdot d_s} = \sqrt{n}$. A to jest natychmiastowym wnioskiem z 4.1.1 U. **(2)** Gdy $n = 2^k$, to $\varphi(n) = 2^{k-1}$, co, przy $k \geqslant 2$, jest $\geqslant 2^{k/2} = \sqrt{n}$. Gdy $n = p^k$, gdzie $p \in \mathbb{P} \setminus \{2\}$, to $\varphi(n) = p^{k-1}(p-1) \geqslant \sqrt{p^k} = \sqrt{n}$, itd. **(3)** Niech p_1 będzie najmniejszym dzielnikiem pierwszym liczby złożonej $n \in \mathbb{N}$. Wówczas, zob. C2.35, $p_1 \leqslant \sqrt{n}$, skąd, zob. (4.6),

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right) \leqslant n\left(1 - \frac{1}{p_1}\right) \leqslant n\left(1 - \frac{1}{\sqrt{n}}\right) = n - \sqrt{n}.$$

Z4.A4 W ciągu pierwszej minuty przypominamy sobie C4.8 i przekonujemy się, że łatwiej jest obliczyć sumę $\sum_{k=1}^{100} \lfloor \frac{100}{k} \rfloor$. Ale to również jest nieco deprymujące. Warto więc poświęcić osiem minut na dowód następującego ***wzoru Dirichlet'a***:

$$T(n) = 2\left(\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{\lfloor \sqrt{n} \rfloor} \right\rfloor\right) - \lfloor \sqrt{n} \rfloor^2. \tag{4.17}$$

Liczba $\tau(k)$ przedstawia, oczywiście, liczbę rozwiązań w $\mathbb{N}$ równania $xy = k$ (każdy dzielnik naturalny d liczby k daje parę $(x, y) = (d, \frac{k}{d})$ i odwrotnie). Wobec tego liczba $T(n) = \sum_{k=1}^{n} \tau(k)$ przedstawia liczbę rozwiązań w liczbach naturalnych nierówności $xy \leqslant n$. Warto popatrzeć na to g e o m e t r y c z n i e.



Rys. 4.1.

Wszystko zobaczyć można na rysunku obok przedstawiającym przypadek $n = 12$. Liczba $T(n)$ jest liczbą punktów kratowych $(x, y) \in \mathbb{N} \times \mathbb{N}$ leżących pod wykresem funkcji $f(x) = \frac{n}{x}$ i na samym wykresie. Tzn., wewnątrz i na brzegu "trójkąta" HEB. Mamy $B = (1, n)$, $E = (n, 1)$, $G = (\sqrt{n}, \sqrt{n})$. Całość jest symetryczna względem prostej OG (dwusiecznej pierwszej ćwiartki układu współrzędnych). Łatwo dzięki temu właściwie zinterpretować wyrażenie z prawej strony równości (4.17): składnik $\lfloor \frac{n}{k} \rfloor$ sumy $\sum_{k=1}^{\lfloor \sqrt{n} \rfloor} \lfloor \frac{n}{k} \rfloor$ wyraża liczbę badanych punktów kratowych na prostej $x = k$, więc ta suma jest równa liczbie badanych punktów kratowych w "pięciokącie" $OAGBC$. Ta liczba jest równa liczbie badanych punktów kratowych w (symetrycznym) "pięciokącie" $ODGEF$. Dwukrotność tej sumy jest więc liczbą badanych punktów kratowych w "pięciokącie" $OFEBC$, przy czym punkty kratowe leżące w kwadracie $OAGD$ liczymy dwukrotnie. Dlatego trzeba odjąć $\lfloor \sqrt{n} \rfloor^2$.

Ostatnia minuta powinna wystarczyć do wyliczenia

$$\left\lfloor \tfrac{100}{1} \right\rfloor + \left\lfloor \tfrac{100}{2} \right\rfloor + \left\lfloor \tfrac{100}{3} \right\rfloor + \left\lfloor \tfrac{100}{4} \right\rfloor + \left\lfloor \tfrac{100}{5} \right\rfloor + \left\lfloor \tfrac{100}{6} \right\rfloor + \left\lfloor \tfrac{100}{7} \right\rfloor + \left\lfloor \tfrac{100}{8} \right\rfloor + \left\lfloor \tfrac{100}{9} \right\rfloor + \left\lfloor \tfrac{100}{10} \right\rfloor .$$

Dostajemy 291. Ostatecznie $T(100) = 2 \cdot 291 - 100 = 482$.

Z4.A5 W zbiorze $[\,n\,] = \{1, \ldots, n\}$ mamy dwa podzbiory: $\Phi_n = \{k \in [\,n\,] : \mathrm{NWD}\,(k,\, n) = 1\}$ i $D_+(n) = \{k \in [\,n\,] : k|n\} = \{k \in [\,n\,] : \mathrm{NWD}\,(k,\, n) = k\}$. Jasne, że $\Phi_n \cap D_+(n) = \{1\}$. Oznaczmy

$$R_n = [\,n\,] \setminus (\Phi_n \cup D_+(n)).$$

R_n składa się z tych liczb $k \in [\,n\,]$, które nie są dzielnikami n i nie są względnie pierwsze z n. Czyli $R_n = \{k \in [\,n\,] : 1 < \mathrm{NWD}\,(k,\, n) < k\}$. Mamy więc rozbicie $[\,n\,] = (\Phi_n \setminus \{1\}) \sqcup D_+(n) \sqcup R_n$. Skąd

$$n = |\Phi_n \setminus \{1\}| + |D_+(n)| + |R_n| = \varphi(n) - 1 + \tau(n) + |R_n|.$$

W ten sposób uzasadniliśmy kryterium:

L e m a t. Równość $\varphi(n) + \tau(n) = n$ zachodzi wtedy i tylko wtedy, gdy $|R_n| = 1$. □

(1) Pokażemy, że *jeżeli* $|\mathrm{Supp}(n)| \geqslant 3$, *to* $\varphi(n) + \tau(n) \neq n$. Rzeczywiście, załóżmy, że $n = cpqr$, gdzie $c \in \mathbb{N}$, a $p < q < r$ są liczbami pierwszymi, przy czym r jest n a j w i ę k s z y m dzielnikiem pierwszym liczby n. Wybierzmy liczbę pierwszą l spełniającą nierówności $r < l < 2r$. Taka liczba istnieje na mocy Postulatu Bertrand'*a*, zob. T12.11. Wówczas $pl,\, ql \in R_n$. Rzeczywiście, $pl < ql < 2qr \leqslant n$ oraz $\mathrm{NWD}\,(pl,\, n) = \mathrm{NWD}\,(ql,\, n) = l < pl < ql$. Zatem $|R_n| \geqslant 2$, więc, na mocy kryterium, $\varphi(n) + \tau(n) \neq n$.

(2) Załóżmy teraz, że $n = cpq$, gdzie $p < q$ są liczbami pierwszymi, oraz $c \in \mathbb{N}$ i $c \geqslant 4$. Wybierzmy wówczas liczby pierwsze $l_1,\, l_2$ spełniające nierówności $q < l_1 < 2q < l_2 < 4q$. Wtedy $l_1 p,\, l_2 p \in R_n$. Więc $|R_n| \geqslant 2$, skąd $\varphi(n) + \tau(n) \neq n$ dla takich n.

Pozostały nam do rozpatrzenia następujące przypadki:

(3) $n = 3pq,\ p < q$. Wówczas, jeżeli $p \neq 3$ i $q \neq 3$, to $|\mathrm{Supp}(n)| \geqslant 3$, więc jesteśmy w przypadku (1). Jeżeli zaś $p = 3$, to $n = 9q$ i wtedy $\tau(n) + \varphi(n) = 3 \cdot 2 + 6(q-1) = 6q \neq n$. Jeżeli wreszcie $q = 3$, to $n = 18$ i wtedy $\tau(n) + \varphi(n) = 6 + 6 = 12 \neq n$.

(4) $n = 2pq,\ p < q$. Wówczas, jeżeli $2 < p$, to $|\mathrm{Supp}(n)| \geqslant 3$. Jeżeli zaś $p = 2$, to $n = 4q$ i wtedy $\tau(n) + \varphi(n) = 3 \cdot 2 + 2(q-1) = 4 + 2q$ co, dla $q > 2$, jest $\neq n$.

(5) $n = pq,\ p < q$. W tej sytuacji $\tau(n) + \varphi(n) = 4 + (p-1)(q-1)$, więc równość $\tau(n) + \varphi(n) = n$ zachodzi tylko, gdy $p + q = 5$. Stąd $p = 2$, $q = 3$, więc $\boxed{n = 6.}$

(6) $n = p^e,\ e \geqslant 1$. Wtedy $\tau(n) + \varphi(n) = e + 1 + p^e - p^{e-1}$ i równość $\tau(n) + \varphi(n) = n$ zachodzi tylko, gdy $e + 1 = p^{e-1}$. Taka równość może zajść co najwyżej dla $e = 1, 2, 3$. Rzeczywiście, $p^{e-1} \geqslant 2^{e-1}$, a $e + 1 < 2^{e-1}$ dla wszystkich $e \geqslant 4$ (łatwe sprawdzenie przez indukcję pozostawiamy Czytelnikowi). W podprzypadku $e = 1$ mamy $\tau(n) + \varphi(n) = 2 + p - 1 \neq n$. W podprzypadku $e = 2$ mamy $\tau(n) + \varphi(n) = 3 + p^2 - p$, co jest równe n tylko dla $p = 3$. Stąd dostajemy rozwiązanie $\boxed{n = 9.}$ W podprzypadku $e = 3$ mamy $\tau(n) + \varphi(n) = 4 + p^3 - p^2$, co jest równe n tylko dla $p = 2$. Stąd dostajemy rozwiązanie $\boxed{n = 8.}$

(7) Ten przypadek dotyczy tylko liczby $n = 1$, dla której $\tau(n) + \varphi(n) \neq n$.

Z4.A6 Wyraz a_n ciągu o wyrazach rzeczywistych (a_n), który jest ściśle większy od wszystkich wyrazów poprzednich (tzn., $a_n > a_k$ dla wszystkich $k = 1, \ldots, n-1$), nazwijmy wyrazem *górującym* ciągu. Udowodnimy lemat:

L e m a t. Jeżeli ciąg (a_n) ma skończenie wiele wyrazów górujących, to jest ciągiem ograniczonym z góry. D o w ó d. Niech N będzie największym indeksem, dla którego a_N jest wyrazem górującym. Twierdzimy, że wówczas $a_N \geqslant a_n$ dla wszystkich n. Nierówność ta jest prawdziwa dla $n \leqslant N$ (bo a_N jest górujący). Gdyby zaś istniały takie $j \in \mathbb{N}$, że $a_{N+j} > a_N$, to wybierając $j = j_0$, najmniejsze takie j (Zasada Minimum!), dostaniemy "nowy" wyraz górujący a_{N+j_0}. Sprzeczność. Q.e.d.

Mając ten lemat można rozwiązać zadanie dowodząc, że ciąg $\left(\frac{\sigma(n)}{n}\right)$ nie jest ciągiem ograniczonym. Na przykład tak: ponieważ każda z liczb $\frac{n!}{1}, \frac{n!}{2}, \ldots, \frac{n!}{n}$ jest dzielnikiem liczby $N = n!$, więc liczba $\frac{\sigma(N)}{N} = \frac{\sigma(n!)}{n!}$ jest większa niż $1 + \frac{1}{2} + \cdots + \frac{1}{n}$, czyli, zobacz T12.5, dowolnie duża.

Ci którzy nie znają jeszcze szeregu harmonicznego mogą rozumować następująco. Zauważyć najpierw, że pokazany dowód lematu dowodzi więcej niż tylko ograniczoność ciągu (a_n). Pokazuje mianowicie, że (a_n) jest ograniczony z góry przez najstarszy (tzn., o największym indeksie) wyraz górujący. Gdyby więc $\frac{\sigma(N)}{N}$ był najstarszym wyrazem górującym ciągu $\left(\frac{\sigma(n)}{n}\right)$, to wybierając dowolną liczbę pierwszą $p \nmid N$ znaleźlibyśmy sprzeczność: $\frac{\sigma(pN)}{pN} = \frac{\sigma(p)}{p} \cdot \frac{\sigma(N)}{N} = \frac{p+1}{p} \cdot \frac{\sigma(N)}{N} > \frac{\sigma(N)}{N}$.

Z4.A7 Korzystając z równości (4.2) i (4.3) sprowadzamy rozwiązanie do następującego lematu:

Lemat. Jeżeli $p \in \mathbb{P}$ i $e \in \mathbb{N}$, a liczba $(p^{e+1} - 1)/(p - 1)$ jest potęgą dwójki, to również liczba $e + 1$ jest potęgą dwójki. Dowód lematu i jego wykorzystanie pozostawiamy Czytelnikowi.

Z4.A8 Możemy to zrobić przez indukcję względem n. Mamy mianowicie

$$\sum_{k=1}^{n+1} \lfloor \tfrac{n+1}{k} \rfloor \varphi(k) = \sum_{k=1}^{n+1} \left(\lfloor \tfrac{n+1}{k} \rfloor - \lfloor \tfrac{n}{k} \rfloor \right) \varphi(k) + \sum_{k=1}^{n+1} \lfloor \tfrac{n}{k} \rfloor \varphi(k).$$

Łatwo uzasadnić, że $\lfloor \frac{n+1}{k} \rfloor - \lfloor \frac{n}{k} \rfloor = \begin{cases} 1, & \text{gdy } k | n+1, \\ 0, & \text{gdy } k \nmid n. \end{cases}$ dla $k, n \in \mathbb{N}$. Wobec tego

$$\sum_{k=1}^{n+1} \lfloor \tfrac{n+1}{k} \rfloor \varphi(k) = \sum_{k | n+1} \varphi(k) + \sum_{k=1}^{n} \lfloor \tfrac{n}{k} \rfloor \varphi(k) = n + 1 + \frac{n(n+1)}{2},$$

na mocy T4.2 i założenia indukcyjnego.

Z4.B1 Funkcja λ jest oczywiście funkcją multyplikatywną (nawet **silnie multyplikatywną**, to znaczy że równość (4.1) zachodzi dla wszystkich, a nie tylko dla względnie pierwszych, liczb naturalnych m, n). Zatem, zobacz C4.17, funkcja $n \longmapsto \sum_{d|n} \lambda(d)$, czyli funkcja $\mathbf{1} * \lambda$, jest również funkcją multyplikatywną. Wobec tego wystarczy uzasadnić, że dla dowolnej liczby pierwszej p, suma $\sum_{k \leqslant e} \lambda(p^k)$ jest równa 1 iff $2|e$ i jest równa 0 iff $2 \nmid e$. A to jest jasne.

Z4.B2 Wykazujemy, że dla dowolnych względnie pierwszych m, $n \in \mathbb{N}$:

$$\sigma_+(mn) = \sigma_+(m) \cdot \sigma_+(n) + \sigma_-(m) \cdot \sigma_-(n),$$
$$\sigma_-(mn) = \sigma_+(m) \cdot \sigma_-(n) + \sigma_-(m) \cdot \sigma_+(n).$$

Stąd natychmiast widzimy multyplikatywność funkcji $n \longmapsto \sigma_+(n) - \sigma_-(n)$.

Z4.B3 Z C4.7 wiemy, że $i(n) = n^{\tau(n)/2}$. Załóżmy, że dla pewnych m, $n \in \mathbb{N}$ zachodzi równość $i(m) = i(n)$, czyli równość $m^{\tau(m)} = n^{\tau(n)}$. Wówczas, oczywiście, $\mathrm{Supp}(m) = \mathrm{Supp}(n)$. Zapiszmy więc $m = p_1^{d_1} p_2^{d_2} \cdot \ldots \cdot p_r^{d_r}$ i $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$. Równość $i(m) = i(n)$ i jednoznaczność rozkładu dają więc równości $d_1\tau(m) = e_1\tau(n)$, $d_2\tau(m) = e_2\tau(n)$, $\ldots$, $d_r\tau(m) = e_r\tau(n)$, czyli, $e_i = d_i x$ dla $i \in [r]$, gdzie $x = \tau(m)/\tau(n)$. Korzystając teraz z (4.2) możemy więc napisać

$$x = \frac{\tau(m)}{\tau(n)} = \frac{(d_1 + 1) \cdot \ldots \cdot (d_r + 1)}{(d_1 x + 1) \cdot \ldots \cdot (d_r x + 1)}.$$

Stąd wnioskujemy, że $x = 1$ (gdy $x > 1$, to prawa strona jest < 1 i odwrotnie). Zatem $m = n$.

Z4.C1 W trzech krokach udowodnimy więcej.

F a k t 1. *Dla dowolnej liczby naturalnej* $k \geqslant 2$ *zachodzi nierówność*

$$\pi(2k) - \pi(k) \leqslant \frac{2k \log 2}{\log k}. \tag{4.18}$$

D o w ó d. Pomysł polega na przyjrzeniu się współczynnikowi dwumiennemu $\binom{2k}{k}$: Każda liczba pierwsza $p \in (k; 2k]$ dzieli licznik ułamka $\frac{2k(2k-1)\cdot\ldots\cdot(k+1)}{n!} = \binom{2k}{k}$ i, oczywiście, n i e dzieli mianownika tego ułamka. Zatem $p|\binom{2k}{k}$. Jeżeli więc $p_1, \ldots, p_s$ są wszystkimi liczbami pierwszymi z przedziału $(k; 2k]$, to ich iloczyn $p_1 \cdot \ldots \cdot p_s$ jest dzielnikiem $\binom{2k}{k}$, zobacz C2.17. W szczególności, zobacz C2.2, $p_1 \cdot \ldots \cdot p_s \leqslant \binom{2k}{k}$. Wobec tego

$$k^{\pi(2k)-\pi(k)} = k^s \leqslant p_1 p_2 \cdot \ldots \cdot p_s \leqslant \binom{2k}{k} \leqslant (1+1)^{2k} = 2^{2k}.$$

Lewa nierówność wynika z nierówności $k \leqslant p_1 < \cdots < p_s$. Prawa nierówność jest jasna, bo $\binom{2k}{k}$ jest tylko jednym (środkowym!) wyrazem sumy $\sum_{j=0}^{2k}\binom{2k}{j} = 2^{2k}$, zob. (1.7). Po zlogarytmowaniu dostajemy (4.18). Q.e.d.

F a k t 2. *Dla dowolnej liczby naturalnej* $m \geqslant 1$ *zachodzi nierówność* $\pi(2^{2m}) \leqslant 3 \cdot \frac{2^{2m}}{2m}$.

D o w ó d. Kładąc w (4.18) kolejno $k = 2^{2m-1}, 2^{2m-2}, \ldots, 2^m$ i dodając stronami dostajemy

$$\pi(2^{2m}) - \pi(2^m) \leqslant \frac{2^{2m}}{2m-1} + \frac{2^{2m-1}}{2m-2} + \cdots + \frac{2^{m+1}}{m}.$$

Stąd $\pi(2^{2m}) - \pi(2^m) \leqslant \frac{2^{m+1}}{m}(1+2+\cdots+2^{m-1}) < \frac{2^{2m}}{m}$. To, wraz z nierównością oczywistą $\pi(2^m) \leqslant 2^m$ i nierównością łatwą $2^m \leqslant \frac{2^{2m}}{2m}$, daje żądaną nierówność. Q.e.d.

F a k t 3. *Dla dowolnej liczby naturalnej* n *zachodzi nierówność*:

$$\pi(n) < 6 \log 2 \cdot \frac{n}{\log n}. \tag{4.19}$$

D o w ó d. Weźmy taką (oczywiście jedyną) liczbę $m \in \mathbb{N}$, że $2^{2m-1} \leqslant n < 2^{2m}$. Wówczas

$$\pi(n) \leqslant \pi(2^{2m}) \leqslant 3 \cdot \frac{2^{2m}}{2m} \leqslant \frac{6n}{2m} < 6 \log 2 \cdot \frac{n}{\log n},$$

bo $2^{2m} \leqslant 2n$ i $\log n < 2m \log 2$. Q.e.d.

Nierówność (4.19) daje więcej niż chcieliśmy: widzimy z niej, że ciąg $\frac{\pi(n)}{n}$ zbiega do 0 co najmniej tak szybko jak odwrotność logarytmu (pomnożona przez pewną stałą).

Z4.C2 Ustalmy liczbę naturalną $m \geqslant 2$ i rozważmy zbiór $A = \{k \in \mathbb{N} : \pi(km) \geqslant k\}$. Zbiór ten jest niepusty (bo $1 \in A$) i skończony (bo, jak wiemy z poprzedniego zadania, $\frac{\pi(km)}{km} < \frac{1}{m}$ dla wszystkich dostatecznie dużych k). Niech więc k_0 będzie największym elementem tego zbioru. Twierdzimy, że wówczas $\pi(k_0 m) = k_0$. Gdyby bowiem $\pi(k_0 m) > k_0$, to mielibyśmy $\pi((k_0+1)m) \geqslant \pi(k_0 m) \geqslant k_0 + 1$ (pierwsza nierówność wynika z niemalejącości ciągu $(\pi(n))$, a druga z Zasady Skwantowania), co jest sprzeczne z maksymalnością k_0. Mamy więc równość $m\pi(k_0 m) = k_0 m$. Liczba $n = k_0 m$ jest zatem takim argumentem, dla którego zachodzi podzielność $\pi(n)|n$. Co więcej, iloraz $n/\pi(n)$ jest równy m. Uzasadniliśmy w ten sposób, że dla każdej liczby naturalnej m istnieje taka liczba naturalna n_m, że $\pi(n_m)|n_m$. Liczby n_m są różne (gdy $n_i = n_j$, to $i = n_i/\pi(n_i) = n_j/\pi(n_j) = j$). Przeto zbiór $\{n \in \mathbb{N} : \pi(n)|n\}$ jest zbiorem nieskończonym.

U w a g a. Okazuje się, że to jest zadanie z analizy! Udowodniliśmy(?!) przecież następujący:

L e m a t. *Jeżeli ciąg* (a_n) *liczb naturalnych jest ciągiem niemalejącym i rośnie do* ∞, *a jednocześnie* $\lim_{n\to\infty} \frac{a_n}{n} = 0$, *to k a ż d y ułamek egipski* $\frac{1}{m}$ *jest wartością ciągu* $(\frac{a_n}{n})$.

Z4.D1 Ustalmy liczbę rzeczywistą $x > 0$ i liczbę naturalną n. Zastanówmy się ile razy i z jakim znakiem występuje w sumie $\sum_{k\in\mathbb{N}} \mu(k)F(\frac{x}{k})$ wyraz $f(\frac{x}{n})$. Otóż, występuje on (ze znakiem $\mu(k)$) w tych (i tylko tych) składnikach $\mu(k)F(\frac{x}{k})$, dla których $k|n$. Wobec tego

$$\sum_{k\in\mathbb{N}} \mu(k)F(\tfrac{x}{k}) = \sum_{n\in\mathbb{N}} (\sum_{k|n} \mu(k)) f(\tfrac{x}{n}) = f(x),$$

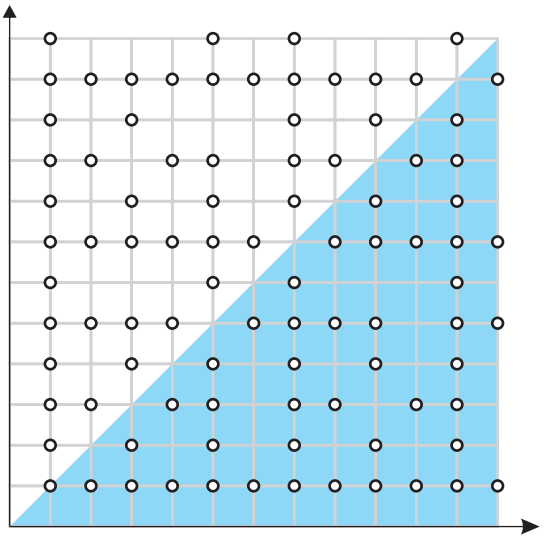
bo $\sum_{k|n} \mu(k) = 0$ dla wszystkich $n > 1$, zobacz Z4.3.

Z4.D2 Oznaczmy, dla danego $d \leqslant n$, $\mathcal{I}_d(n) = \{(k, l) \in \mathbb{N} \times \mathbb{N} : 1 \leqslant k, l \leqslant n, \mathrm{NWD}\,(k, l) = d\}$.

Zauważmy, że zbiór $\mathcal{I}_1(n)$ składa się z tych i tylko tych punktów kratowych o współrzędnych naturalnych $\leqslant n$, które widać z punktu $(0, 0)$. To znaczy tych, których nie "zasłania" inny punkt kratowy. Na rysunku 4.2 pokazujemy przypadek $n = 12$. Łatwo widzieć, że:

(1) odbicie $(x, y) \longmapsto (y, x)$ (czyli odbicie w dwusiecznej I ćwiartki układu współrzędnych) daje bijekcję zbioru $\mathcal{T}$ tych punktów $(x, y) \in \mathcal{I}_1(n)$, dla których $0 < y \leqslant x \leqslant n$ na zbiór tych punktów zbioru $\mathcal{I}_1(n)$, dla których $0 < x \leqslant y \leqslant n$,

(2) $\mathrm{card}\,(\mathcal{I}_1(n) \cap \mathcal{T}) = \varphi(1) + \varphi(2) + \cdots + \varphi(n)$. Rzeczywiście, punkty zbioru $\mathcal{I}_1(n)$ leżące w trójkącie $\mathcal{T}$ na prostej $x = k$ to dokładnie te punkty (k, l), dla których $1 \leqslant l \leqslant k$ i $\mathrm{NWD}\,(k, l) = 1$.



Rys. 4.2

Wobec tego mamy równość:

$$\varphi(1) + \varphi(2) + \varphi(3) + \cdots + \varphi(n) = \frac{1 + \mathrm{card}\ \mathcal{I}_1(n)}{2}.$$

Dla zakończenia rozwiązania wystarczy więc udowodnić równość

$$\mathrm{card}\ \mathcal{I}_1(n) = \sum_{k\in\mathbb{N}} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2. \tag{4.20}$$

Równość tę wyprowadzamy z Z4.D1 i dwóch obserwacji:

(A) funkcja $(k, l) \longmapsto (\frac{k}{d}, \frac{l}{d})$ jest bijekcją zbioru $\mathcal{I}_d(n)$ na zbiór $\mathcal{I}_1(\lfloor \frac{n}{d} \rfloor)$. Zob. C2.12.

(B) zbiory $\mathcal{I}_d(n)$ dla $d \leqslant n$ są parami rozłączne. Ich sumą jest zbiór $[\,n\,] \times [\,n\,]$, skąd

$$n^2 = \mathrm{card}\,\{(k, l) : 1 \leqslant k, l \leqslant n\} = \mathrm{card}\ \mathcal{I}_1(n) + \mathrm{card}\ \mathcal{I}_2(n) + \ldots \mathrm{card}\ \mathcal{I}_n(n).$$

Jeżeli więc oznaczymy $f(x) = \mathrm{card}\ \mathcal{I}_1(\lfloor x \rfloor)$ dla dowolnego $x > 0$, to $F(x) := \sum_{k\in\mathbb{N}} f(\frac{x}{k}) = \lfloor x \rfloor^2$. Stąd i z Z4.D1 dostajemy równość (4.20).

U w a g a. Korzystając z równości $\sum_{k\in\mathbb{N}} \frac{\mu(k)}{k^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$, zob. T12.7, i równości (4.20), można wykazać, że zachodzi następująca równość

$$\mathrm{card}\ \mathcal{I}_1(n) = \tfrac{6n^2}{\pi^2} + C(n)n \log n \tag{4.21}$$

dla pewnej funkcji o g r a n i c z o n e j C. Można z niej wywnioskować, że losowo wybrany ułamek $\frac{k}{l}$, dla $1 \leqslant k, l \leqslant n$, jest nieskracalny z prawdopodobieństwem bliskim $\frac{6}{\pi^2} \approx 0,6079$.

Rozdział 5

Arytmetyka modularna

Man weiß, das alle Bemühungen der größten Mathematiker vor Gauß
an dieser steilen Klippe gescheitert sind, bis es endlich diesem Einzigen gelang,
den verborgenen Pfad zu entdecken und bis zum Ziele vorzudringen.

(Gotthold Eisenstein)

Arytmetyka modularna jest sztuką wykonywania operacji algebraicznych d o d a w a n i a, m n o ż e n i a i, gdy się uda, d z i e l e n i a, a nawet r o z w i ą z y w a n i a r ó w n a ń algebraicznych, nie na liczbach, ale na r e s z t a c h z dzielenia liczb całkowitych przez ustaloną liczbę naturalną $m > 1$ zwaną **modułem** (łac. *modulus* – miara). Startując od wstępnych definicji, poprzez twierdzenia Eulera, Fermat'a i Wilsona dochodzimy do twierdzenia chińskiego o resztach. Następnie uczymy się pojęć rzędu elementu grupy, pierwiastków pierwotnych i reszt kwadratowych. Kulminacyjnym twierdzeniem rozdziału jest prawo wzajemności dla reszt kwadratowych. O tym właśnie twierdzeniu mówi przytoczone wyżej zdanie Eisensteina.

5.1 Wstęp do teorii kongruencji

Wprowadzimy pojęcie kongruencji. Pokażemy podstawowe motywacje uzasadniające przydatność i potrzebę takiego wprowadzenia. I zaczniemy się uczyć rozwiązywania równań wielomianowych w **arytmetyce modularnej**.

5.1.1 Definicja i cechy podzielności

Poznajemy teraz (pochodzącą od Gaussa) notację. Nauczymy się elementarnych reguł manipulacji z kongruencjami i zastosujemy je w dowodzie (najprostszych) cech podzielności.

Definicja 5.1 Niech $m > 1$ będzie ustaloną liczbą naturalną. Mówimy, że liczba całkowita a **przystaje** do liczby całkowitej b modulo m, gdy $m|a-b$. Zapisujemy to tak:

$$\boxed{a \equiv b \,(\mathrm{mod}\, m).}$$

Relację $\cdot \equiv \cdot \,(\mathrm{mod}\, m)$ nazywamy **kongruencją modulo** m (lub **według modułu** m).

Jasnym jest (być powinno!), że relacja $a \equiv b \,(\mathrm{mod}\, m)$ zachodzi wtedy i tylko wtedy, gdy liczby a i b dają tę samą resztę z dzielenia przez m.

TWIERDZENIE 5.1 *Ustalmy liczbę naturalną* $m > 1$. *Wówczas dla dowolnych liczb całkowitych* a, b, c, d *zachodzą związki:*

(1) $a \equiv a \,(\mathrm{mod}\, m)$,

(2) jeżeli $a \equiv b \,(\mathrm{mod}\, m)$, to $b \equiv a \,(\mathrm{mod}\, m)$,

(3) jeżeli $a \equiv b \,(\mathrm{mod}\, m)$ i $b \equiv c \,(\mathrm{mod}\, m)$, to $a \equiv c \,(\mathrm{mod}\, m)$,

(4) jeżeli $a \equiv b \,(\mathrm{mod}\, m)$ i $c \equiv d \,(\mathrm{mod}\, m)$, to $a \pm c \equiv b \pm d \,(\mathrm{mod}\, m)$,

(5) jeżeli $a \equiv b \,(\mathrm{mod}\, m)$ i $c \equiv d \,(\mathrm{mod}\, m)$, to $ac \equiv bd \,(\mathrm{mod}\, m)$.

D O W Ó D. Uzasadnimy jedynie punkt (5). Czytelnik zechce się przekonać, że pozostałe są dla niego oczywiste. Niech $c - d = ms$ i $a - b = mt$. Wówczas

$$ac - bd = ac - ad + ad - bd = a(c - d) + (a - b)d = ams + mtd = m(as + td),$$

co pokazuje, że $m|ac - bd$, i kończy dowód. □

Tezy (1), (2) i (3) mówią, że relacja kongruencji modulo m jest relacją równoważności, zob. $\mathbb{KOM}$. Tezy (4) i (5) mówią, że relacja ta jest **zgodna z dodawaniem** (**odejmowaniem**) i **mnożeniem**. To oznacza, że kongruencje wolno d o d a w a ć, (o d e j m o w a ć) i m n o ż y ć stronami. Również p o t ę g o w a ć. Oto kilka przykładów wykorzystania tych własności:

P r z y k ł a d 1. *Dwiema ostatnimi cyframi (dziesiętnymi) liczby Fermat'*a F_{10} *są* 1, 7. Rzeczywiście: $2^{12} = 4096$, czyli $2^{12} \equiv -4 \,(\mathrm{mod}\, 100)$. Wobec tego $2^{72} \equiv (2^{12})^6 \equiv (-4)^6 \equiv 2^{12} \equiv -4 \,(\mathrm{mod}\, 100)$. Stąd $2^{432} \equiv (2^{72})^6 \equiv (-4)^6 \equiv -4 \,(\mathrm{mod}\, 100)$. Zatem

$$2^{1024} = (2^{432})^2 \cdot (2^{72})^2 \cdot 2^{12} \cdot 2^4 \equiv (-4)^2 \cdot (-4)^2 \cdot (-4) \cdot 2^4 \equiv -2^{14} \equiv -(-4) \cdot 2^2 \equiv 16 \,(\mathrm{mod}\, 100).$$

Wobec tego $F_{10} \equiv 17 \,(\mathrm{mod}\, 100)$. Q.e.d. Podobne (nieco żmudniejsze) rachunki pokazują, że trzema ostatnimi cyframi dziesiętnymi liczby F_{10} są 2, 1, 7. Q.e.d. ◊

P r z y k ł a d 2. *Liczba* $L_n = 2^{n+2} + 3^{2n+1}$ *jest, dla każdego* $n \in \mathbb{N}$, *podzielna przez* 7. Rzeczywiście: $2^{n+2} \equiv 4 \cdot 2^n \,(\mathrm{mod}\, 7)$ oraz $3^{2n+1} \equiv 3 \cdot (3^2)^n \equiv 3 \cdot 2^n \,(\mathrm{mod}\, 7)$. Stąd, po dodaniu stronami, $L_n \equiv 7 \cdot 2^n \equiv 0 \,(\mathrm{mod}\, 7)$. Q.e.d. ◊

P r z y k ł a d 3. *Liczba* $L_n = 3^n + 4^n$ *nie jest, dla żadnego* $n \in \mathbb{N}$, *podzielna przez* 11. Rzeczywiście: $(3, 3^2, 3^3, 3^4, 3^5) \equiv (3, 9, 5, 4, 1) \,(\mathrm{mod}\, 11)$ (taki zapis oznacza, oczywiście, że kolejne wyrazy ciągu z lewej strony przystają modulo 11 do odpowiednich wyrazów ze strony prawej) oraz $(4, 4^2, 4^3, 4^4, 4^5) \equiv (4, 5, 9, 3, 1) \,(\mathrm{mod}\, 11)$. Wobec tego

$$(L_{5k+1}, L_{5k+2}, L_{5k+3}, L_{5k+4}, L_{5k+5}) \equiv (7, 4, 4, 7, 2) \,(\mathrm{mod}\, 11)$$

dla każdego $k \in \mathbb{N}$, co oznacza, że żadna liczba L_n nie przystaje do 0 modulo 11. Q.e.d. ◊

Prostym ale bardzo ważnym wnioskiem[1] z T5.1 jest:

TWIERDZENIE 5.2 *Niech* $f(X) \in \mathbb{Z}[X]$ *będzie wielomianem o współczynnikach całkowitych. Wówczas dla dowolnych liczb całkowitych* a, b:

$$\boxed{a \equiv b \,(\mathrm{mod}\, m) \quad \Longrightarrow \quad f(a) \equiv f(b) \,(\mathrm{mod}\, m).}$$

[1] Jest to również wniosek z podzielności (3.3), z której korzystaliśmy już wielokrotnie.

D O W Ó D. Niech $f(X) = c_0+c_1X+c_2X^2+\ldots+c_nX^n$. Wiemy, że kongruencje można dodawać, odejmować i mnożyć stronami. W szczególności, jeżeli $a \equiv b \,(\mathrm{mod}\, m)$, to dla dowolnego $k \geqslant 0$, $a^k \equiv b^k \,(\mathrm{mod}\, m)$. Mnożąc stronami tę kongruencję przez kongruencję $c_k \equiv c_k \,(\mathrm{mod}\, m)$, dostajemy $c_k a^k \equiv c_k b^k \,(\mathrm{mod}\, m)$ dla każdego k. Wystarczy teraz dodać te kongruencje. □

U w a g a. Kongruencji n i e w o l n o dzielić stronami nawet jeżeli (co zdarza się rzadko) dzielenie jest wykonalne w zbiorze liczb całkowitych. Na przykład, mimo że $96 \equiv 36 \,(\mathrm{mod}\, 20)$ i $24 \equiv 4 \,(\mathrm{mod}\, 20)$, to $\frac{96}{24} \not\equiv \frac{36}{4} \,(\mathrm{mod}\, 20)$. Wszelako prawdziwe jest (należy zauważyć, że jest to tylko inna postać ZTA!) następujące:

PRAWO SKRACANIA *Jeżeli* $\mathrm{NWD}\,(c,\, m) = 1$ *i* $ac \equiv bc \,(\mathrm{mod}\, m)$, *to* $a \equiv b \,(\mathrm{mod}\, m)$.

Oto kilka przykładowych zastosowań twierdzenia T5.2:

ZADANIE 5.1 Wielomian $f(X) = X^3 - 4X^2 + X + 13$ nie ma pierwiastków całkowitych.

R o z w i ą z a n i e. Jeżeli $a \equiv 0 \,(\mathrm{mod}\, 3)$, to $f(a) \equiv f(0) \equiv 13 \equiv 1 \,(\mathrm{mod}\, 3)$. Jeżeli $a \equiv 1 \,(\mathrm{mod}\, 3)$, to $f(a) \equiv f(1) \equiv 11 \equiv 2 \,(\mathrm{mod}\, 3)$. Jeżeli zaś $a \equiv -1 \,(\mathrm{mod}\, 3)$, to $f(a) \equiv -13 \equiv 1 \,(\mathrm{mod}\, 3)$. Te trzy proste fakty pokazują, że wartość wielomianu $f(X)$ dla argumentu całkowitego n i g d y nie jest liczbą podzielną przez 3, w szczególności, nigdy nie jest równa 0. Wielomian $f(X)$ n i e m a więc pierwiastków całkowitych. ◊

Ćwiczenie 5.1 Dany jest wielomian $f(X) \in \mathbb{Z}[X]$. Udowodnić, że jeżeli $f(2)$ jest liczbą podzielną przez 5, a $f(5)$ jest liczbą podzielną przez 2, to $10|f(7)$.

Proste zastosowanie twierdzenia T5.2 zobaczyć można w dowodach ***cech podzielności***:

ZADANIE 5.2 Niech $A = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_n 10^n$ będzie zapisem liczby naturalnej w systemie dziesiętnym. Wówczas

(1) $A \equiv a_0 + a_1 + \ldots + a_n \,(\mathrm{mod}\, 3)$,

(2) $A \equiv a_0 + a_1 + \ldots + a_n \,(\mathrm{mod}\, 9)$,

(3) $A \equiv a_0 - a_1 + a_2 - \ldots + (-1)^n a_n \,(\mathrm{mod}\, 11)$.

R o z w i ą z a n i e. Niech $f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$. Wtedy $A = f(10)$. Ponieważ $10 \equiv 1 \,(\mathrm{mod}\, 9)$, więc, na mocy T5.2, $A \equiv f(1) \,(\mathrm{mod}\, 9)$. Podobnie sprawdzamy pozostałe przystawania. Zauważmy, że dostaliśmy więcej niż w szkole. Mianowicie: *liczba naturalna i suma jej cyfr dziesiętnych dają tę samą resztę z dzielenia przez* 9 *(i przez* 3*). Liczba naturalna i naprzemienna suma jej cyfr dają tę samą resztę z dzielenia przez* 11. ◊

Ćwiczenie 5.2 Nie wykonując mnożenia uzasadnić, że $1234 \cdot 2345 \neq 2881730$. *Wskazówka.* Wymyślić, uzasadnić i zastosować ***dziewiątkowy test poprawności mnożenia***. Jaką odpowiedź dałby tu test trójkowy? A test jedenastkowy?

ZADANIE 5.3 Udowodnić, że jeżeli $f(X) \in \mathbb{Z}[X]$ jest wielomianem stopnia $n \geqslant 1$, to istnieje taka liczba naturalna x, że $|f(x)|$ jest liczbą złożoną.

R o z w i ą z a n i e. Wybierzmy taką liczbę naturalną c, że $|f(c)| > 1$. (Czytelnik powinien sam uzasadnić, że taka liczba c istnieje.) Jeżeli $|f(c)|$ jest liczbą złożoną, to $x = c$ jest dobra. Jeżeli zaś $|f(c)| = p$ jest liczbą pierwszą, to rozważmy liczby naturalne $c_k = c + kp$,

dla $k = 0, 1, \ldots, s$, gdzie $s = 3n$ ($n = \deg f(X)$). Wówczas, ponieważ $c_k \equiv c \pmod p$ dla wszystkich k, więc $f(c_k) \equiv f(c) \equiv 0 \pmod p$. Czyli $p|f(c_k)$ dla wszystkich k. Gdyby żadna z liczb $|f(c_k)|$ nie była liczbą złożoną, to liczby $f(c_k)$ (jako podzielne przez p) byłyby równe 0, p lub $-p$. Ale równość $f(c_k) = 0$ może zachodzić dla co najwyżej n liczb c_k, zobacz twierdzenie T3.4. Podobnie, równość $f(c_k) = p$ może zachodzić dla co najwyżej n liczb c_k (aby to zobaczyć wystarczy zastosować T3.4 do wielomianu $f(X) - p$) i, podobnie, równość $f(c_k) = -p$ może zachodzić dla co najwyżej n liczb c_k. Ponieważ mamy $3n+1$ liczb c_k, więc widzimy, że co najmniej jedna z liczb $|f(c_k)|$ j e s t l i c z b ą z ł o ż o n ą. ◊

Ćwiczenie 5.3 Uzasadnić, że, w sytuacji z powyższego zadania, istnieje n i e s k o ń c z e n i e wiele takich $x \in \mathbb{N}$, że $|f(x)|$ ma więcej niż 2017 dzielników będących liczbami pierwszymi.

5.1.2 Motywacja: równania diofantyczne

Ważnym tematem teorii liczb są **równania diofantyczne**, czyli równania postaci

$$f(x_1, x_2, \ldots, x_n) = 0 \tag{5.1}$$

gdzie $f(X_1, X_2, \ldots, X_n)$ jest wielomianem n zmiennych o współczynnikach c a ł k o w i t y c h. Chodzi o rozstrzygnięcie, czy równanie takie ma rozwiązania całkowite i, jeżeli tak, to o wyznaczenie takowych. Chwilowo o wielomianach n zmiennych wystarczy wiedzieć tylko tyle, że są to wyrażenia zbudowane z liczb całkowitych i zmiennych $X_1, X_2, \ldots, X_n$ za pomocą działań dodawania, odejmowania i mnożenia, na przykład $15X_1^2 - 7X_2^2 - 9$ czy $5X_1^2 + 11X_2^2 + 13X_3^2$. Zobacz też ustęp 6.5.1. Zaczniemy od przykładowych zadań.

ZADANIE 5.4 Udowodnić, że równanie $15x^2 - 7y^2 - 9 = 0$ nie ma rozwiązań w $\mathbb{Z}$.

R o z w i ą z a n i e. Załóżmy, nie wprost, że para $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ jest rozwiązaniem naszego równania i weźmy moduł $m = 5$. Wówczas $3y^2 \equiv 4 \pmod 5$, bo $15 \equiv 0 \pmod 5$, $-7 \equiv 3 \pmod 5$ i $9 \equiv 4 \pmod 5$. Mnożąc kongruencję $3y^2 \equiv 4 \pmod 5$ stronami przez 2 (mnożenie obustronne przez a to to samo, co mnożenie stronami przez kongruencję $a \equiv a \pmod m$) otrzymamy $y^2 \equiv 3 \pmod 5$. Ale to jest niemożliwe, bowiem: $0^2 \equiv 0 \pmod 5$, $1^2 \equiv (-1)^2 \equiv 4^2 \equiv 1 \pmod 5$ i $2^2 \equiv (-2)^2 \equiv 3^2 \equiv 4 \pmod 5$. To znaczy, że kwadrat (liczby całkowitej) daje resztę 0, 1 lub 4 z dzielenia przez 5. Więc nie daje reszty 3. Sprzeczność. ◊

ZADANIE 5.5 Udowodnić, że równanie $5x^3 + 11y^3 + 13z^3 = 0$ nie ma innych rozwiązań w liczbach całkowitych oprócz $x = 0$, $y = 0$, $z = 0$.

R o z w i ą z a n i e. Załóżmy, że trójka (x, y, z) jest rozwiązaniem i weźmy moduł $m = 13$. Wówczas, z jasnych powodów, $5x^3 - 2y^3 \equiv 0 \pmod{13}$, czyli $5x^3 \equiv 2y^3 \pmod{13}$, lub, po pomnożeniu przez 7, $9x^3 \equiv y^3 \pmod{13}$. Zobaczmy teraz jak wyglądają sześciany modulo 13, lub, równoważnie, jakie reszty z dzielenia przez 13 dają sześciany liczb całkowitych. Łatwo sprawdzamy, że modulo 13: 1^3, 3^3, $9^3 \equiv 1$, 2^3, 5^3, $6^3 \equiv 8$, 4^3, 10^3, $12^3 \equiv 12$, 7^3, 8^3, $11^3 \equiv 5$ i, oczywiście, $0^3 \equiv 0$. Stąd, $9x^3 \equiv 9, 7, 4, 6, 0 \pmod{13}$. Widzimy, że jedyną szansę na zachodzenie kongruencji $9x^3 \equiv y^3 \pmod{13}$ daje $x \equiv y \equiv 0 \pmod{13}$. Teraz przechodzimy do ofensywy: wykorzystamy **desant nieskończony**. Niech $x = 13u$, $y = 13v$. Wstawiając to do badanego równania widzimy, że $13|z$. Niech więc $z = 13w$. Wstawiając raz jeszcze i upraszczając przez 13^3 otrzymujemy $5u^3 + 11v^3 + 13w^3 = 0$. Widzimy więc, że trójka

(u, v, w) jest r ó w n i e ż r o z w i ą z a n i e m naszego równania. Badając tę trójkę dokładnie tak samo jak przed chwilą badaliśmy trójkę (x, y, z), znajdujemy, że $13|u$, $13|v$, $13|w$. Więc $13^2|x$, $13^2|y$, $13^2|z$. Postępując tak dalej widzimy, że $x \equiv y \equiv z \equiv 0 \,(\mathrm{mod}\, 13^n)$ dla każdego $n \in \mathbb{N}$. To dowodzi, że $x = y = z = 0$ i kończy rozwiązanie zadania. $\Diamond$

Ćwiczenie 5.4 Rozwiąż w liczbach naturalnych k, n równanie $1! + 2! + \ldots + n! = k^3$. *Wskazówka.* Zredukować modulo 7. Zauważmy, że to równanie (w świetle wyżej przyjętej definicji) nie jest równaniem diofantycznym – lewa strona n i e j e s t wielomianem zmiennej n.

Ćwiczenie 5.5 Udowodnić uogólnienie twierdzenia T5.2: *Jeżeli* $f(X_1, X_2, \ldots, X_n)$ *jest wielomianem o współczynnikach całkowitych, oraz* $a_k \equiv b_k \,(\mathrm{mod}\, m)$ *dla* $k = 1, 2, \ldots, n$, *to* $f(a_1, a_2, \ldots, a_n) \equiv f(b_1, b_2, \ldots, b_n) \,(\mathrm{mod}\, m)$.

Definicja 5.2 Niech $f(X_1, X_2, \ldots, X_n)$ będzie wielomianem o współczynnikach całkowitych. **Rozwiązaniem kongruencji (wielomianowej)**

$$f(x_1, x_2, \ldots, x_n) \equiv 0 \,(\mathrm{mod}\, m) \tag{5.2}$$

nazywamy taką n-kę $(c_1, c_2, \ldots, c_n)$ liczb całkowitych, że $f(c_1, c_2, \ldots, c_n) \equiv 0 \,(\mathrm{mod}\, m)$. Mówimy, że rozwiązania $(c_1, c_2, \ldots, c_n)$ i $(c'_1, c'_2, \ldots, c'_n)$ są **równoważne** (**modulo** m), gdy dla każdego $k = 1, 2, \ldots, n$ zachodzi przystawanie $c_k \equiv c'_k \,(\mathrm{mod}\, m)$. **Liczbą rozwiązań kongruencji** (5.2) nazywamy liczbę rozwiązań n i e r ó w n o w a ż n y c h. Zbiór wszystkich nierównoważnych rozwiązań kongruencji (5.2) oznaczamy symbolem $\mathcal{N}(f; m)$. Liczbę elementów tego zbioru oznaczamy symbolem $N(f; m)$.

P r z y k ł a d. Niech $f(X, Y) = X^2 + Y^2$. Tezę Z2.A3 zapisujemy tak: $N(f; 11) = 1$, a mianowicie: $\mathcal{N}(f; 11) = \{(0, 0)\}$ (zbiór jednoelementowy, którego jedynym elementem jest para uporządkowana $(0, 0)$). $\Diamond$

Oczywistym jest, że jeżeli n-ka $(c_1, c_2, \ldots, c_n)$ jest rozwiązaniem równania (5.1) w liczbach całkowitych, to jest ona rozwiązaniem kongruencji (5.2) dla d o w o l n e g o modułu m. W n i o s k u j e m y stąd, że jeżeli dla choćby jednego modułu m kongruencja (5.2) nie ma rozwiązań, to i równanie (5.1) nie ma rozwiązań całkowitych. Inaczej mówiąc, istnienie rozwiązań kongruencji (5.2) jest w a r u n k i e m k o n i e c z n y m istnienia rozwiązań równania (5.1) w liczbach całkowitych. Podkreślić tu trzeba, że ten warunek (nawet spełniony dla wszystkich modułów m) n i e j e s t w y s t a r c z a j ą c y. Istnieją takie wielomiany $f(X)$, że zbiory $\mathcal{N}(f; m)$ są niepuste przy dowolnym module m, ale równanie $f(x) = 0$ nie ma rozwiązań w zbiorze liczb całkowitych. Stosowne przykłady zobaczymy w dalszym ciągu, na przykład w ustępie 5.8.3.

5.1.3 Twierdzenie Schura

Pokażemy teraz, że jeżeli wielomian f (o współczynnikach całkowitych jednej lub wielu zmiennych) o współczynnikach całkowitych nie jest wielomianem stałym (tzn., jeżeli $\deg(f) \geqslant 1$), to istnieje nieskończenie wiele modułów m, dla których zbiór $\mathcal{N}(f; m)$ jest n i e p u s t y.

Definicja 5.3 Dany jest wielomian f o współczynnikach całkowitych. Liczbę naturalną m nazwiemy f-**wyróżnioną**, gdy kongruencja $f(x) \equiv 0 \,(\mathrm{mod}\, m)$ ma rozwiązania, czyli gdy zbiór $\mathcal{N}(f; m)$ jest niepusty. Innymi słowy, liczba f-wyróżniona jest dzielnikiem liczby $f(k_1, \ldots, k_n)$ dla pewnych całkowitych (równoważnie(!): naturalnych) $k_1, \ldots, k_n$.

TWIERDZENIE 5.3 (***Twierdzenie Schura***) *Dla dowolnego wielomianu* $f(X) \in \mathbb{Z}[X]$ *stopnia* $\geqslant 1$ *istnieje nieskończenie wiele liczb pierwszych* f*-wyróżnionych.*

D O W Ó D. Niech $f(X) = a_0 + a_1X + \cdots + a_nX^n$. Jasne, że każdy dzielnik pierwszy liczby a_0 jest f-wyróżniony. Wobec tego, w przypadku, gdy $a_0 = 0$, k a ż d a liczba pierwsza jest f-wyróżniona. Załóżmy więc teraz, że $a_0 \neq 0$. Naśladując Euklidesa (zobacz pierwszy dowód TE), załóżmy, że $\{p_1, \ldots, p_r\}$ jest skończonym zbiorem liczb pierwszych f-wyróżnionych i rozważmy wielomian $g(X)$ dany przez

$$g(X) = \frac{1}{a_0} f(p_1 \cdot \ldots \cdot p_r a_0 X) = 1 + p_1 \cdot \ldots \cdot p_r a_1 X + \cdots + (p_1 \cdot \ldots \cdot p_r)^n a_0^{n-1} a_n X^n.$$

Jasne, że $\deg(g) = \deg(f)$. Jasne też, że $g(X) \in \mathbb{Z}[X]$. Na mocy Z5.3 istnieje taka liczba naturalna c, że $|g(c)|$ jest liczbą złożoną. Niech p będzie d o w o l n y m dzielnikiem pierwszym liczby $g(c)$. Wówczas $f(p_1 \cdot \ldots \cdot p_r a_0 c) = a_0 g(c) \equiv 0 \,(\mathrm{mod}\, p)$. Mamy więc rozwiązanie $x_0 = p_1 \cdot \ldots \cdot p_r a_0 c$ kongruencji $f(x) \equiv 0 \,(\mathrm{mod}\, p)$, więc p jest liczbą pierwszą f-wyróżnioną. Jednocześnie, jak widać z postaci wielomianu $g(X)$, zachodzi kongruencja $g(c) \equiv 1 \,(\mathrm{mod}\, p_i)$ dla każdego $i = 1, \ldots, r$. To dowodzi, że $p \neq p_i$ dla każdego i. W ten sposób znajdujemy n o w ą liczbę pierwszą f-wyróżnioną. To, oczywiście, kończy dowód. □

Ćwiczenie 5.6 Uogólnić powyższy dowód na przypadek wielomianu wielu zmiennych.

U w a g a. Inny dowód twierdzenia Schura (w duchu tak zwanej **analitycznej teorii liczb**) pokazujemy w ustępie 12.3.2.

5.1.4 Kongruencje liniowe

Zaczynamy nasze badania zbiorów $\mathcal{N}(f; m)$ rozwiązań kongruencji wielomianowych postaci (5.2) od n a j p r o s t s z e g o przypadku, gdy wielomian f jest wielomianem jednej zmiennej stopnia 1. Czyli, zajmiemy się rozwiązywaniem kongruencji postaci $ax \equiv b \,(\mathrm{mod}\, m)$. Nazywamy je **kongruencjami stopnia pierwszego** lub **kongruencjami liniowymi**.

TWIERDZENIE 5.4 (***O kongruencji liniowej***) *Niech* a, b *i* $m \geqslant 1$ *będą danymi liczbami całkowitymi i niech* $d = \mathrm{NWD}\,(a, m)$. *Wówczas kongruencja liniowa*

$$ax + b \equiv 0 \,(\mathrm{mod}\, m) \tag{5.3}$$

ma rozwiązania wtedy i tylko wtedy, gdy $d|b$. *Gdy ten warunek jest spełniony, to kongruencja* (5.3) *ma dokładnie* d *(nierównoważnych!) rozwiązań. Ponadto, gdy* c *jest rozwiązaniem, a* $m' = m/d$, *to w s z y s t k i e (parami nierównoważne) rozwiązania zadane są przez:*

$$c, \quad c + m', \quad c + 2m', \quad \ldots, \quad c + (d-1)m'. \tag{5.4}$$

D O W Ó D. To twierdzenie jest w istocie jedynie innym sformułowaniem twierdzenia T2.12. Rzeczywiście, kongruencja (5.3) jest tylko innym zapisem faktu, że $m|ax + b$ co z kolei jest tym samym co równość $ax - my = -b$ dla pewnego $y \in \mathbb{Z}$. Czytelnik zechce z pewnością uzupełnić wszystkie szczegóły. □

U w a g a. Ani wzorów (5.4) ani (równoważnych im) wzorów (2.11) nie musimy zapamiętywać. Obowiązkowe jest natomiast z r o z u m i e n i e opisanej powyżej (i w dowodzie twierdzenia T2.12) metody badania równania $ax - my = -b$ i, równoważnej mu, kongruencji $ax + b \equiv 0 \,(\mathrm{mod}\, m)$. Rzecz jest prosta, co widać w poniższym przykładzie:

P r z y k ł a d. Mamy ciąg równoważności:

$$6x \equiv 15 \,(\mathrm{mod}\, 21) \;\Leftrightarrow\; 21|6x - 15 \;\Leftrightarrow\; 7|2x - 5 \;\Leftrightarrow\; 2x - 5 = 7y \;\Leftrightarrow\; 2x - 7y = 5.$$

Widzimy więc, że kongruencja $6x \equiv 15 \,(\mathrm{mod}\, 21)$ jest równoważna kolejno:

$$2x - 7y = 2 \cdot 20 - 7 \cdot 5 \;\Leftrightarrow\; 2(x - 20) = 7(y - 5) \;\Leftrightarrow\; x \equiv 20 \equiv 6 \,(\mathrm{mod}\, 7).$$

Kongruencja $6x \equiv 15 \,(\mathrm{mod}\, 21)$ ma więc t r z y rozwiązania: 6, 13 i 20. ◊

Twierdzenie T5.4 formułujemy też następująco:

TWIERDZENIE 5.4bis *Jeżeli $f(X) = aX + b \in \mathbb{Z}[X]$ jest dwumianem o współczynnikach całkowitych ($a \neq 0$), oraz* $\mathrm{NWD}\,(a, m) = d$, *to*:

$$N(f;\, m) = \begin{cases} d, & \text{gdy} \quad d|b, \\ 0, & \text{gdy} \quad d \nmid b. \end{cases} \tag{5.5}$$

Ponadto, jeżeli $c \in \mathcal{N}(f;\, m)$, a $m' = m/d$, to $\mathcal{N}(f;\, m) = \{c,\, c + m',\, \ldots,\, c + (d-1)m'\}$.

5.1.5 Odwracanie modulo m

Kongruencje umiemy dodawać (odejmować) i mnożyć stronami. Teraz zajmiemy się przez chwilę możliwością obustronnego dzielenia przez daną liczbę całkowitą.

Ponieważ d z i e l e n i e j e s t m n o ż e n i e m p r z e z o d w r o t n o ś ć, więc wystarczy się zastanowić nad problemem istnienia odwrotności. Przyjmiemy następującą definicję:

Definicja 5.4 Mówimy, że liczba całkowita a jest **odwracalna modulo** m, gdy istnieje taka liczba całkowita x, że zachodzi kongruencja $ax \equiv 1 \,(\mathrm{mod}\, m)$. W takiej sytuacji mówimy, że (liczba) x jest **odwrotnością (liczby)** a **modulo** m.

P r z y k ł a d. Ponieważ $4 \cdot 11 \equiv 1 \,(\mathrm{mod}\, 43)$, więc odwrotnością liczby 4 modulo 43 jest każda liczba postaci $11 + 43a$. Łatwo sprawdzić, że kongruencja $4x \equiv 1 \,(\mathrm{mod}\, 54)$ n i e m a rozwiązań. Zatem, liczba 4 n i e m a odwrotności modulo 54. ◊

Prostego kryterium odwracalności modulo m dostarcza twierdzenie:

TWIERDZENIE 5.5 *Liczba a ma odwrotność modulo m wtedy i tylko wtedy, gdy liczby a i m są względnie pierwsze. Co więcej, jeżeli x_1 i x_2 są odwrotnościami liczby a modulo m, to $x_1 \equiv x_2 \,(\mathrm{mod}\, m)$.*

D O W Ó D. Jest natychmiastowym wnioskiem z twierdzenia T5.4. W rzeczy samej, odwrotność liczby a modulo m jest po prostu rozwiązaniem kongruencji $ax \equiv 1 \,(\mathrm{mod}\, m)$, która ma dokładnie jedno $(\mathrm{mod}\, m)$ rozwiązanie wtedy i tylko wtedy, gdy $\mathrm{NWD}\,(a, m)|1$. □

U w a g a 1. Odwrotność a modulo m oznaczamy $a^{-1} \pmod m$ lub (gdy wiemy o jaki moduł chodzi) po prostu a^{-1}. Może być ona e f e k t y w n i e w y z n a c z o n a za pomocą algorytmu Euklidesa: istotnie, algorytm Euklidesa pozwala na efektywne wyznaczenie liczb całkowitych x, y, spełniających równość $1 = \mathrm{NWD}\,(a, m) = ax + my$. Wówczas $x \equiv a^{-1} \pmod m$.

U w a g a 2. Zauważmy również, że jeżeli liczba a jest odwracalna modulo m, to kongruencja $ax \equiv b \pmod m$ jest r ó w n o w a ż n a kongruencji $x \equiv ba^{-1} \pmod m$.

Ćwiczenie 5.7 Udowodnić, że iloczyn liczb odwracalnych modulo m jest liczbą odwracalną modulo m. Ponadto, iloczyn odwrotności jest odwrotnością iloczynu, czyli:

$$(a \cdot b)^{-1} \equiv a^{-1} \cdot b^{-1} \pmod m.$$

5.2 Twierdzenie Eulera, Fermat'*a* i Wilsona

Nazwane w tytule twierdzenia należą do absolutnie niezbędnego minimum teorioliczbowego "uzbrojenia" każdego olimpijczyka.

5.2.1 Zupełne i zredukowane układy reszt

Przyjrzyjmy się przez chwilę układom reszt modulo $m \in \mathbb{N}$.

Definicja 5.5 **(1)** Zbiór $\{0, 1, \ldots, m-1\}$ nazywamy **standardowym zupełnym układem reszt** modulo m. **(2)** Zbiór $\{b_1, b_2, \ldots, b_m\}$, gdzie każda z liczb b_k daje i n n ą resztę z dzielenia przez m, nazywamy **zupełnym układem reszt modulo** m. **(3)** Zbiór

$$\Phi(m) = \{k \in \mathbb{N} : 1 \leqslant k \leqslant m, \mathrm{NWD}\,(k, m) = 1\} \tag{5.6}$$

nazywamy **standardowym zredukowanym układem reszt** modulo m. **(4)** Zbiór liczb całkowitych $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$, z których każda daje i n n ą resztę z dzielenia przez m i każda jest w z g l ę d n i e p i e r w s z a z m, nazywamy **zredukowanym układem reszt** modulo m. [Pamiętamy, zobacz D4.4, że przez $\varphi(m)$ oznaczyliśmy moc zbioru $\Phi(m)$.]

P r z y k ł a d. Niech $m = 10$. Wówczas zbiór $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ jest standardowym zupełnym układem reszt, zbiór $\{20, -9, 22, -27, 44, -45, 66, -63, 88, -81\}$ jest zupełnym układem reszt, $\Phi(10) = \{1, 3, 7, 9\}$, a zbiór $\{-9, 13, -13, 39\}$ jest zredukowanym układem reszt modulo 10. $\Diamond$

Ćwiczenie 5.8 Udowodnić, że zbiór $\{c + ta : 0 \leqslant t < m\}$ jest zupełnym układem reszt modulo m wtedy i tylko wtedy, gdy $\mathrm{NWD}\,(a, m) = 1$. Gdy $c = 0$, $a = 1$, dostaniemy standardowy zupełny układ reszt modulo m.

Ćwiczenie 5.9 Załóżmy, że $\{b_1, b_2, \ldots, b_m\}$ jest zupełnym układem reszt modulo m. Udowodnić, że jeżeli $a, c \in \mathbb{N}$ oraz $\mathrm{NWD}\,(a, m) = 1$, to zachodzi równość

$$\sum_{j=1}^{m} \left\{ \frac{ab_j + c}{m} \right\} = \frac{m-1}{2},$$

gdzie $\{x\}$ oznacza część ułamkową liczby rzeczywistej x, zobacz D12.1.

LEMAT 5.1 *Jeżeli* $\{r_1, r_2, \ldots, r_s\}$, *gdzie* $s = \varphi(m)$, *jest zredukowanym układem reszt modulo* m, *i* a *jest liczbą względnie pierwszą z* m, *to zbiór* $\{ar_1, ar_2, \ldots, ar_s\}$ *jest również zredukowanym układem reszt modulo* m.

D O W Ó D. Liczba ar_i jest względnie pierwsza z m. Ponadto, liczby ar_i są różne modulo m (to znaczy, że $ar_i \not\equiv ar_j \pmod m$ dla $i \neq j$. Sprawdźcie!). Jest ich $\varphi(m)$, więc stanowią one zredukowany układ reszt modulo m. □

5.2.2 Twierdzenie Eulera

Najważniejszym twierdzeniem dotyczącym kongruencji jest twierdzenie Eulera.

TWIERDZENIE 5.6 (***Twierdzenie Eulera*** **– 1763**) *Jeżeli* $\mathrm{NWD}\,(a, m) = 1$, *to*

$$\boxed{a^{\varphi(m)} \equiv 1 \pmod m.} \tag{5.7}$$

D O W Ó D. Oznaczmy $s = \varphi(m)$. Niech $\{r_1, r_2, \ldots, r_s\}$ będzie dowolnym zredukowanym układem reszt modulo m. Dzięki lematowi L5.1 wiemy, że $\{ar_1, ar_2, \ldots, ar_s\}$ jest również zredukowanym układem reszt modulo m. Stąd $r_1r_2 \cdot \ldots \cdot r_s \equiv (ar_1) \cdot (ar_2) \cdot \ldots \cdot (ar_s) \pmod m$. Oznaczając $c = r_1r_2 \cdot \ldots \cdot r_s$ otrzymujemy więc $c \equiv a^s c \pmod m$. Wystarczy teraz uprościć przez c, czyli pomnożyć obie strony tej kongruencji przez $c^{-1} \pmod m$. Ćwiczenie C5.7 poucza nas, że iloczyn elementów odwracalnych modulo m sam jest elementem odwracalnym modulo m. Więc odwrotność $c^{-1} \pmod m$ i s t n i e j e! □

P r z y k ł a d 1. W jednym z zadań OM'54 należało udowodnić, że liczba $53^{53} - 33^{33}$ jest podzielna przez 10. Należało więc sprawdzić, że $53^{53} \equiv 33^{33} \pmod{10}$. Robimy to tak: ponieważ $\varphi(10) = 4$ i $10 \perp 53$, więc, na mocy T5.6, $53^{53} = 53 \cdot (53^4)^{13} \equiv 3 \cdot 1^{13} \equiv 3 \pmod{10}$. Podobnie, $33^{33} \equiv 3 \pmod{10}$. Stąd teza. ◊

P r z y k ł a d 2. Załóżmy, że $a, b \in \mathbb{N}$ i $a \perp b$. Kładąc $x = \varphi(b)$ i $y = \varphi(a)$ znajdujemy rozwiązanie kongruencji $a^x + b^y \equiv 1 \pmod{ab}$. Rzeczywiście: $a^x \equiv 1 \pmod b$ i $b^y \equiv 0 \pmod b$, co, po dodaniu stronami, daje $a^x + b^y \equiv 1 \pmod b$. Podobnie, $a^x + b^y \equiv 1 \pmod a$. Wspomnijmy teraz raz jeszcze założenie $a \perp b$ i wykorzystajmy C2.17. ◊

ZADANIE 5.6 Udowodnić, że jeżeli $n \in \mathbb{N}_{\geqslant 2}$, to $n \nmid 2^n - 1$.

R o z w i ą z a n i e. Załóżmy nie wprost, że istnieją liczby naturalne $n > 1$, dla których $n|2^n - 1$ i niech $m > 1$ będzie n a j m n i e j s z ą taką liczbą. Wtedy

$$2^m \equiv 1 \pmod m. \tag{5.8}$$

Jasne, że m jest liczbą nieparzystą, więc, na mocy twierdzenia Eulera,

$$2^{\varphi(m)} \equiv 1 \pmod m. \tag{5.9}$$

Oznaczmy $d = \mathrm{NWD}\,(m, \varphi(m))$. Wówczas, na mocy T2.6, $ma + \varphi(m)b = d$ dla pewnych $a, b \in \mathbb{Z}$. Jasne, że dokładnie jedna z liczb a, b jest ujemna. Załóżmy, że $a < 0$ (przypadek, gdy $b < 0$, bada się podobnie). Wówczas, na mocy kongruencji (5.8) i (5.9), mamy

$$2^d \equiv 2^d \cdot (2^m)^{-a} = 2^{d-ma} \equiv 2^{\varphi(m)b} \equiv (2^{\varphi(m)})^b \equiv 1^b \equiv 1 \pmod m. \tag{5.10}$$

Czyli $m|2^d - 1$. Ale d jest dzielnikiem m, więc $d|2^d - 1$, co, wobec minimalności m i nierówności $d \leqslant \varphi(m) < m$, daje równość $d = 1$. To jednakże jest niemożliwe, bo wtedy, na mocy (5.10), byłoby $2 \equiv 1 \pmod m$, czyli $m = 1$. Ta sprzeczność kończy rozwiązanie. ◊

5.2.3 Małe twierdzenie Fermat'*a*

Prawdopodobnie najczęściej stosowanym w OM twierdzeniem teorioliczbowym jest tak zwane Małe Twierdzenie Fermat'*a*. Jest ono przypadkiem szczególnym twierdzenia Eulera.

WNIOSEK (***Małe Twierdzenie Fermat'*a, MTF**) *Jeżeli p jest liczbą pierwszą i p nie jest dzielnikiem liczby całkowitej a, to*

$$\boxed{\boxed{a^{p-1} \equiv 1 \,(\mathrm{mod}\, p).}} \tag{5.11}$$

DOWÓD. Sposób 1. Jeżeli m jest liczbą pierwszą, to $\varphi(m) = m - 1$. Wobec tego, kongruencja (5.11) jest natychmiastowym wnioskiem z twierdzenia Eulera.

Sposób 2. Udowodnimy (niezależnie od T5.6) często używaną, ogólniejszą kongruencję:

$$\boxed{\boxed{a^p \equiv a \,(\mathrm{mod}\, p)}} \tag{5.12}$$

dla dowolnej liczby całkowitej a. Gdy $p = 2$, rzecz jest oczywista(!). Załóżmy więc, że $p > 2$. Kongruencję $a^p \equiv a \,(\mathrm{mod}\, p)$ udowodnimy najpierw dla $a = n \in \mathbb{N}$ przez indukcję względem n. Dla $n = 1$ sprawa jest jasna. Założenie indukcyjne $p|n^p - n$, wzór dwumienny i wniosek z formuły Legendre'*a* (patrz C2.50) pozwalają napisać

$$(n+1)^p = n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \ \ldots\ + \binom{p}{p-1} n + 1 \equiv n^p + 1 \equiv n + 1 \,(\mathrm{mod}\, p)$$

i skończyć dowód dla liczb naturalnych n. Gdy a jest ujemną liczbą całkowitą, to, wobec nieparzystości p, mamy $a^p \equiv -(-a)^p \equiv -(-a) \equiv a \,(\mathrm{mod}\, p)$. Mając (5.12), czyli $p|a(a^{p-1}-1)$, po wykorzystaniu założenia $p \nmid a$ i ZTA, dostajemy podzielność $p|a^{p-1} - 1$, czyli (5.11). □

Uwaga. Jeszcze co najmniej dwa sposoby dowodu MTF znaleźć można w $\mathbb{KOM}$.

Pokażemy parę przykładów stosowania Małego Twierdzenia Fermat'*a*:

Przykład 1. *Dla liczb $a_1, \ldots, a_n \in \mathbb{Z}$ i liczby $p \in \mathbb{P}$ zachodzi równoważność*:

$$p|(a_1^p + a_2^p + \ \ldots\ + a_n^p) \quad \Longleftrightarrow \quad p|(a_1 + a_2 + \ \ldots\ + a_n).$$

Rzeczywiście, dodajmy stronami kongruencje $a_i^p \equiv a_i \,(\mathrm{mod}\, p)$, zob. (5.12). Widzimy wtedy, że liczby $\sum_{i=1}^n a_i^p$ i $\sum_{i=1}^n a_i$ dają tę samą resztę z dzielenia przez p. Q.e.d. ◊

Przykład 2. *Jeżeli $7|(a^6 + b^6 + c^6)$ dla pewnych liczb całkowitych a, b, c, to $343|abc$.* Rzeczywiście, gdy k spośród liczb a, b, c dzieli się przez 7 (pozostałe $3-k$ jest niepodzielnych przez 7), to $a^6 + b^6 + c^6 \equiv 3 - k \,(\mathrm{mod}\, 7)$. Podzielność $7|(a^6 + b^6 + c^6)$ zachodzi więc tylko w przypadku, gdy $k = 3$. Wtedy $7|a$, $7|b$, $7|c$. Q.e.d. ◊

Przykład 3. *Zachodzi podzielność* $547|2^{2^{2^4}} - 2^{2^{2^2}}$. Rzeczywiście, 547 jest liczbą pierwszą, a badana liczba jest równa $2^K(2^{N-K}-1)$, gdzie $K = 2^{2^2}$, a $N = 2^{2^4}$. Wystarczy zobaczyć, że $546|N - K$; wtedy bowiem $2^{N-K} - 1 = 2^{546a} - 1 = (2^{546})^a - 1 \equiv 1^a - 1 \equiv 0 \,(\mathrm{mod}\, 547)$ na mocy MTF. Ponieważ $546 = 2 \cdot 3 \cdot 7 \cdot 13$, a $N - K = 2^4(2^{12} - 1) = 2^4(4^6 - 1) = 2^4(64^2 - 1)$, więc potrzebne podzielności $13|N - K$, $7|N - K$ i $3|N - K$ wynikają z MTF. Q.e.d. ◊

P r z y k ł a d 4. *Jeżeli* $p \in \mathbb{P}$ *i* $q = 2p - 1 \in \mathbb{P}$, *to* $p|a^q - a$ *dla* $a \in \mathbb{Z}$. Rzeczywiście, mnożąc kongruencję $a^p \equiv a \,(\mathrm{mod}\, p)$ przez a^{p-1}, dostajemy $a^q \equiv a^p \equiv a \,(\mathrm{mod}\, p)$. Q.e.d. $\Diamond$

Należy koniecznie rozwiązać poniższe dwa ćwiczenia (z ich tez korzysta się bardzo często):

Ćwiczenie 5.10 Dana jest liczba pierwsza p i liczba całkowita a. Udowodnić, że jeżeli $a^2 \equiv 1 \,(\mathrm{mod}\, p)$, to $a \equiv 1 \,(\mathrm{mod}\, p)$ lub $a \equiv -1 \,(\mathrm{mod}\, p)$ (piszemy w skrócie $a \equiv \pm 1 \,(\mathrm{mod}\, p)$).

Ćwiczenie 5.11 Niech p będzie nieparzystą liczbą pierwszą i niech $s = \frac{p-1}{2}$. Udowodnić, że jeżeli $p \nmid a$, to $a^s \equiv \pm 1 \,(\mathrm{mod}\, p)$.

W rozwiązaniu poniższego zadania wykorzystamy tezy ćwiczeń C5.10 i C5.11:

ZADANIE 5.7 Dla danych liczb całkowitych b i $a_1, a_2, \ldots, a_{20}$ zachodzi równość

$$b^{11} = a_1^{11} + a_2^{11} + \ldots + a_{20}^{11}.$$

Udowodnić, że iloczyn $ba_1a_2 \cdot \ldots \cdot a_{20}$ jest liczbą podzielną przez 23.

R o z w i ą z a n i e. Jeżeli jedna z liczb a_i jest podzielna przez 23, to koniec. Załóżmy więc, że liczby $a_1, a_2, \ldots, a_{20}$ nie są podzielne przez 23. Wówczas dla każdego $1 \leqslant i \leqslant 20$, a_i^{11} jest liczbą całkowitą, której kwadrat a_i^{22} daje resztę 1 przy dzieleniu przez 23: $a_i^{22} \equiv 1 \,(\mathrm{mod}\, 23)$. Wobec tego $a_i^{11} \equiv \pm 1 \,(\mathrm{mod}\, 23)$ dla każdego $1 \leqslant i \leqslant 20$, patrz C5.10. Jeżeli k składników sumy $a_1^{11} + a_2^{11} + \ldots + a_{20}^{11}$ przystaje do 1 modulo 23, a $20 - k$ pozostałych przystaje do -1 modulo 23, to $b^{11} = a_1^{11} + a_2^{11} + \ldots + a_{20}^{11} \equiv k - (20 - k) \equiv 2k - 20 \,(\mathrm{mod}\, 23)$. Zatem $b^{11} \not\equiv \pm 1 \,(\mathrm{mod}\, 23)$ co, wobec C5.11, jest niemożliwe, gdy $23 \nmid b$. $\Diamond$

Ćwiczenie 5.12 Udowodnić, że $2^{16} - 2^4 | n^{16} - n^4$ dla każdej liczby naturalnej n.

Ćwiczenie 5.13 Niech $L_n = n^{n^{n^4}} - n^{n^{n^2}}$. Udowodnić, że $547 | L_n$ dla każdego $n \in \mathbb{N}$.

5.2.4 Twierdzenie Wilsona

Trzecim twierdzeniem z tej serii jest twierdzenie Wilsona.

TWIERDZENIE 5.7 (***Twierdzenie Wilsona***) *Dla każdej liczby pierwszej* p *zachodzi*

$$\boxed{(p-1)! \equiv -1 \,(\mathrm{mod}\, p).} \tag{5.13}$$

D O W Ó D. Dla $p = 2, 3$ rzecz jest oczywista. Załóżmy więc, że p jest liczbą pierwszą $\geqslant 5$ i rozważmy zbiór $T := \{2, 3, \ldots, p-2\}$. Elementy zbioru T można pogrupować w pary postaci $\{a, \widetilde{a}\}$, gdzie $\widetilde{a} \equiv a^{-1} \,(\mathrm{mod}\, p)$. Rzeczywiście, ponieważ wszystkie liczby $a \in T$ są względnie pierwsze z p, więc, na mocy T5.5, mają odwrotności modulo p. Ponadto, $\widetilde{a} \neq 1, \neq -1, \neq a$. Gdyby bowiem $\widetilde{a} = 1$, to $a \cdot 1 \equiv 1 \,(\mathrm{mod}\, p)$, co nie ma miejsca. Podobnie $\widetilde{a} \neq -1$. Wreszcie, gdyby $\widetilde{a} = a$, to $a \cdot a \equiv 1 \,(\mathrm{mod}\, p)$, co też nie może zajść, patrz C5.10. Zatem iloczyn $I = 2 \cdot 3 \cdot \ldots \cdot (p-2)$ jest równy iloczynowi iloczynów postaci $a \cdot \widetilde{a}$, z których każdy jest

$\equiv 1 \,(\mathrm{mod}\, p)$. Więc $I \equiv 1 \,(\mathrm{mod}\, p)$. Wystarczy teraz pomnożyć tę kongruencję stronami przez kongruencję $1 \cdot (p-1) \equiv -1 \,(\mathrm{mod}\, p)$. □

P r z y k ł a d 1. *Zachodzi kongruencja* $61! + 1 \equiv 0 \,(\mathrm{mod}\, 71)$. Rzeczywiście, z twierdzenia Wilsona mamy $-1 \equiv 70! \equiv 61! \cdot (-9)(-8) \cdot \ldots \cdot (-1) \,(\mathrm{mod}\, 71)$. Wystarczy teraz pomnożyć stronami kongruencje $(-9) \cdot (-8) \equiv 1 \,(\mathrm{mod}\, 71)$ i $-7! = -5040 \equiv 1 \,(\mathrm{mod}\, 71)$. Q.e.d. ◊

P r z y k ł a d 2. *Jeżeli dla* $n \in \mathbb{N}_{\geqslant 2}$ *zachodzi kongruencja* $(n-1)! \equiv -1 \,(\mathrm{mod}\, n)$ *to* $n \in \mathbb{P}$. Istotnie, jeżeli $a|n$, gdzie $1 < a < n$, to w iloczynie $1 \cdot 2 \cdot \ldots \cdot (n-1)$ występuje czynnik a, więc $a|(n-1)!$. Jednocześnie, przechodniość (zob. T2.1(2)) relacji podzielności daje $a|(n-1)! + 1$, więc też (zob. T2.1(4)), $a|1$, sprzeczność. Q.e.d. ◊

P r z y k ł a d 3. *Dla* $a \in \mathbb{Z}$ *i* $p \in \mathbb{P}$ *zachodzi* $a^p(p-1)! + a \equiv 0 \,(\mathrm{mod}\, p)$. Rzeczywiście, wystarczy pomnożyć stronami kongruencje $a^p \equiv a \,(\mathrm{mod}\, p)$ i $(p-1)! \equiv -1 \,(\mathrm{mod}\, p)$. Q.e.d. ◊

Ćwiczenie 5.14 Niech $p > 2$ będzie liczbą pierwszą. Udowodnić, że jeżeli

$$a_1,\, a_2,\, \ldots,\, a_p \quad \text{i} \quad b_1,\, b_2,\, \ldots,\, b_p$$

są permutacjami liczb $1,\, 2,\, \ldots,\, p$, to wśród iloczynów $a_1b_1,\, a_2b_2,\, \ldots,\, a_pb_p$ są dwa dające tę samą resztę z dzielenia przez p.

U w a g a. Twierdzenie Wilsona można sformułować też tak: *Jeżeli* $r_1,\, r_2,\, \ldots,\, r_{p-1}$ *jest dowolnym z r e d u k o w a n y m układem reszt modulo* p, *to*

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1} \equiv -1 \,(\mathrm{mod}\, p). \tag{5.14}$$

Twierdzenie Wilsona zostało przez Gaussa uogólnione następująco: *Jeżeli* $r_1,\, r_2,\, \ldots,\, r_{\varphi(m)}$ *jest dowolnym zredukowanym układem reszt modulo* $m > 1$, *to*

$$\boxed{r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \equiv \begin{cases} -1 \,(\mathrm{mod}\, m), & \text{gdy} \quad m = 2,\, 4,\, p^e,\, 2p^e, \\ 1 \,(\mathrm{mod}\, m), & \text{w pozostałych przypadkach.} \end{cases}} \tag{5.15}$$

Tu p oznacza dowolną nieparzystą liczbę pierwszą. Zobacz też ćwiczenie C5.62.

5.3 Układy kongruencji liniowych

Będziemy się teraz zajmowali problemem rozwiązalności i wyznaczenia struktury rozwiązań układów kongruencji liniowych postaci:

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, m_1) \\ x \equiv b_2 \,(\mathrm{mod}\, m_2) \\ \quad \ldots \\ x \equiv b_r \,(\mathrm{mod}\, m_r) \end{cases} \tag{5.16}$$

gdzie b_i są dowolnymi liczbami całkowitymi, a $m_i \geqslant 2$ są liczbami naturalnymi.

5.3.1 Twierdzenie chińskie o resztach

Prawdziwość poniższego twierdzenia została odkryta dawno temu w Chinach.

TWIERDZENIE 5.8 (***Twierdzenie chińskie o resztach***) *Jeżeli* $m_1, m_2, \ldots, m_r \geqslant 2$ *są parami względnie pierwszymi liczbami naturalnymi, zaś* $b_1, b_2, \ldots, b_r$ *są dowolnymi liczbami całkowitymi i* $M = m_1 \cdot \ldots \cdot m_r$, *to w zbiorze* $\{0, 1, \ldots, M-1\}$ *istnieje dokładnie jedno rozwiązanie układu* (5.16).

D O W Ó D. Niech $M_k = M/m_k$, dla $k = 1, 2, \ldots, r$. Jasne, że $\mathrm{NWD}\,(M_k, m_k) = 1$ dla każdego k. Wobec tego, zobacz T5.5 istnieją odwrotności M_k^{-1} liczb M_k modulo m_k dla każdego k. To znaczy, że zachodzą kongruencje:

$$M_k M_k^{-1} \equiv 1 \,(\mathrm{mod}\, m_k) \tag{5.17}$$

dla każdego k. Twierdzimy, że liczba

$$x_0 = b_1 M_1 M_1^{-1} + b_2 M_2 M_2^{-1} + \ldots + b_r M_r M_r^{-1}$$

jest rozwiązaniem układu (5.16). Istotnie, dla $l \neq k$ mamy $b_l M_l M_l^{-1} \equiv 0 \,(\mathrm{mod}\, m_k)$. Stąd $x_0 \equiv b_k M_k M_k^{-1} \,(\mathrm{mod}\, m_k)$, co, wobec (5.17), daje $x_0 \equiv b_k \,(\mathrm{mod}\, m_k)$ dla każdego k.

Załóżmy teraz, że x_1 również jest rozwiązaniem układu (5.16). Wówczas $x_1 \equiv b_k \equiv x_0 \,(\mathrm{mod}\, m_k)$ dla każdego k. Zatem, parami względnie pierwsze, liczby m_k dzielą liczbę $x_1 - x_0$. Więc ich iloczyn M również dzieli $x_1 - x_0$, zobacz C2.17. To oznacza, że $x_1 \equiv x_0 \,(\mathrm{mod}\, M)$. Sprawdzenie, że jest również odwrotnie, to znaczy, że

$$x \equiv x_0 \,(\mathrm{mod}\, M) \quad \Longrightarrow \quad x \text{ jest rozwiązaniem układu (5.16)},$$

nie przedstawia żadnych trudności. Jasne więc, że dokładnie jedno rozwiązanie spełnia nierówność $0 \leqslant x < M$. □

U w a g a 1. Twierdzenie chińskie o resztach mówi, że układ kongruencji (5.16), przy założeniu $m_i \perp m_j$ dla $i \neq j$, jest r ó w n o w a ż n y jednej kongruencji liniowej

$$x \equiv b_1 M_1 M_1^{-1} + b_2 M_2 M_2^{-1} + \ldots + b_r M_r M_r^{-1} \,(\mathrm{mod}\, m_1 m_2 \cdot \ldots \cdot m_r). \tag{5.18}$$

P r z y k ł a d 1. Wyznaczymy rozwiązania układu kongruencji

$$\begin{cases} 5x \equiv 13 \,(\mathrm{mod}\, 8) \\ 14x \equiv 21 \,(\mathrm{mod}\, 49) \\ 3x \equiv 4 \,(\mathrm{mod}\, 11) \end{cases}$$

Ponieważ 5 jest odwrotnością 5 modulo 8, więc mnożąc obustronnie pierwszą kongruencję przez 5, dostajemy kongruencję równoważną $x \equiv 1 \,(\mathrm{mod}\, 8)$. Podobnie, mnożąc trzecią kongruencję stronami przez 4, dostajemy kongruencję równoważną $x \equiv 5 \,(\mathrm{mod}\, 11)$. Druga kongruencja jest równoważna relacji $49 | 14x - 21$ czyli relacji $7 | 2x - 3$, więc kongruencji $2x \equiv 3 \,(\mathrm{mod}\, 7)$,

którą mnożymy obustronnie przez 4, bo 4 jest odwrotnością 2 modulo 7. Wobec tego badany układ kongruencji jest r ó w n o w a ż n y układowi typu (5.16):

$$\begin{cases} x \equiv 1 \,(\mathrm{mod}\, 8) \\ x \equiv 5 \,(\mathrm{mod}\, 7) \\ x \equiv 5 \,(\mathrm{mod}\, 11) \end{cases}$$

Teraz możemy zastosować wzór (5.18). Mamy: $m_1 = 8$, $m_2 = 7$, $m_3 = 11$ oraz $M_1 = 77$, $M_2 = 88$, $M_3 = 56$. Zatem $M_1^{-1} = 5$, $M_2^{-1} = 2$ i $M_3^{-1} = 1$. I ostatecznie:

$$x \equiv 1 \cdot 77 \cdot 5 + 5 \cdot 88 \cdot 2 + 5 \cdot 56 \cdot 1 \equiv 1545 \equiv 313 \,(\mathrm{mod}\, 616). \quad \Diamond$$

Legendarne "zastosowanie" twierdzenia chińskiego znaleźć można w ćwiczeniu:

Ćwiczenie 5.15 Aby wyznaczyć liczbę żołnierzy w swojej armii cesarz rozkazywał ustawiać się im w szyku dwójkowym, trójkowym, 5-kowym, 7-kowym, 11-kowym, 13-kowym i 17-kowym, za każdym razem polecając pisarzowi notować liczbę żołnierzy "zbywających". Udowodnić, że znając tylko te siedem liczb, cesarz mógł jednoznacznie wyznaczyć liczebność swojej armii, przy założeniu, że nie była ona większa niż pół miliona.

Typowe zastosowanie twierdzenia chińskiego możemy zobaczyć w poniższych zadaniach:

Ćwiczenie 5.16 Udowodnić, że: **(1)** istnieje ciąg kolejnych 2011 liczb naturalnych, z których każda dzieli się przez co najmniej 2011 różnych liczb pierwszych, **(2)** istnieją dowolnie długie ciągi arytmetyczne o takich wyrazach całkowitych, że każdy z nich jest podzielny przez sześcian innej liczby naturalnej.

ZADANIE 5.8 Udowodnić, że istnieje ciąg kolejnych 2011 liczb naturalnych, z których żadna nie jest potęgą liczby naturalnej o wykładniku $\geqslant 2$.

R o z w i ą z a n i e. Zauważmy, że jeżeli dla danej liczby pierwszej p zachodzi kongruencja $a \equiv p \,(\mathrm{mod}\, p^2)$, to $v_p(a) = 1$ co, oczywiście, oznacza, że a n i e j e s t potęgą liczby naturalnej o wykładniku $\geqslant 2$. Weźmy teraz $r = 2011$ różnych liczb pierwszych $p_1, p_2, \ldots, p_r$ i rozwiążmy układ kongruencji

$$\begin{cases} x \equiv p_1 - 1 \,(\mathrm{mod}\, p_1^2), \\ x \equiv p_2 - 2 \,(\mathrm{mod}\, p_2^2), \\ \qquad \vdots \\ x \equiv p_r - r \,(\mathrm{mod}\, p_r^2). \end{cases}$$

Dzięki twierdzeniu chińskiemu wiemy, że układ ten ma rozwiązanie $x \in \mathbb{N}$, a dzięki uwadze uczynionej na początku rozwiązania wiemy, że żadna z kolejnych 2011 liczb $x + 1$, $x + 2$, $\ldots$, $x + r$ nie jest potęgą liczby naturalnej o wykładniku $\geqslant 2$. $\Diamond$

ZADANIE 5.9 Udowodnić, że istnieje nieskończenie wiele takich liczb naturalnych a, dla których liczba $a^2 + 1$ ma co najmniej 2011 różnych dzielników pierwszych.

Rozwiązanie. Rozważmy wielomian $f(X) = X^2+1$. Z twierdzenia Schura T5.3 wiemy, że istnieje $r := 2011$ liczb pierwszych f-wyróżnionych $p_1, p_2, \ldots, p_r$. Dla każdej z nich istnieje liczba naturalna $n_k \in \mathcal{N}(f; p_k)$. Zachodzą więc kongruencje $f(n_k) \equiv 0 \,(\mathrm{mod}\, p_k)$ dla $k = 1, \ldots, r$. Dzięki twierdzeniu chińskiemu o resztach wiemy, że istnieje taka liczba naturalna a, dla której $a \equiv n_k \,(\mathrm{mod}\, p_k)$ dla wszystkich $k = 1, \ldots, r$. Wówczas $f(a) \equiv f(n_k) \equiv 0 \,(\mathrm{mod}\, p_k)$ dla każdego $k \leqslant r$, zobacz T5.2. Zatem liczba $f(a) = a^2 + 1$ ma r różnych dzielników pierwszych $p_1, p_2, \ldots, p_r$. Liczby $a_t = a + tp_1p_2 \cdot \ldots \cdot p_r$, dla $t \in \mathbb{N}$, również spełniają(!) kongruencje $a_t \equiv n_k \,(\mathrm{mod}\, p_k)$ dla każdego k, są więc też dla nas dobre. $\Diamond$

Oto jeszcze dwa ćwiczenia w podobnym duchu:

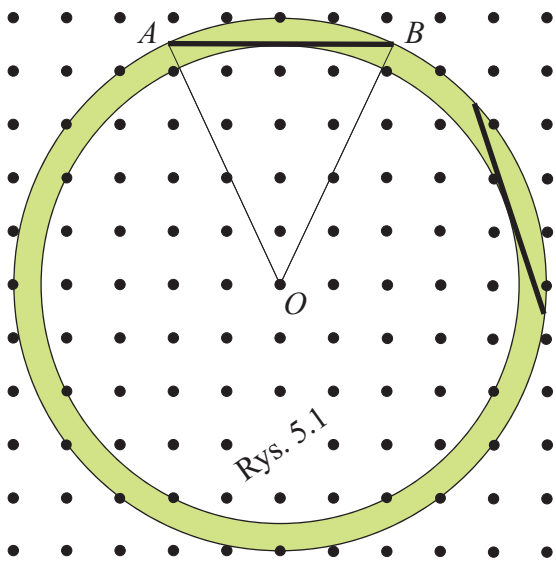
Ćwiczenie 5.17 Udowodnić, że dla każdej liczby naturalnej n istnieje taka liczba całkowita M, że $2^{2^n} - 1 | M^2 + 9$. *Wskazówka.* $2^{2^n} - 1 = F_{n-1} \cdot \ldots \cdot F_1 \cdot 3$. Zobacz Z2.2.

Ćwiczenie 5.18 Udowodnić, że istnieją takie różne i parami względnie pierwsze liczby $n_1, \ldots, n_{11} \in \mathbb{N}$, że liczba $n_1n_2 \cdot \ldots \cdot n_{11} - 1$ jest iloczynem dwóch kolejnych liczb naturalnych.

5.3.2 Zadanie o długiej igle

Pokażemy teraz jedno interesujące zadanie, w rozwiązaniu którego istotnym elementem jest chińskie twierdzenie o resztach. W trakcie rozwiązywania korzystać będziemy z paru faktów, które udowodnimy później.

ZADANIE 5.10 W każdym punkcie kratowym płaszczyzny wbita jest pionowo szpilka. Ponadto na płaszczyźnie tej leży igła o długości 2011 w położeniu pokrywającym się z odcinkiem $\overline{KL}$, gdzie $K = (0, \frac{1}{2})$, $L = (2011, \frac{1}{2})$. Udowodnić, że można tę igłę tak przesunąć bez zahaczania o szpilki, by zajęła ona położenie pokrywające się z odcinkiem $\overline{MN}$, gdzie $M = (0, \frac{3}{2})$, $N = (2011, \frac{3}{2})$.



Rys. 5.1

Rozwiązanie. Oto pomysł na przesuwanie igły: należy znaleźć takie dwa okręgi współśrodkowe o promieniach R_1 i R_2, i wspólnym środku w punkcie kratowym O, by w pierścieniu kołowym $\{X : R_1 < |OX| < R_2\}$, zobacz rysunek 5.1, nie było ani jednego punktu kratowego i by w tym pierścieniu dało się umieścić cięciwę większego okręgu o długości $2011 + \varepsilon$ leżącą całkowicie na zewnątrz okręgu mniejszego. Na rysunku 5.1 pokazujemy jak można (nie zahaczając o punkty kratowe) obrócić o dowolny kąt igłę o długości nieznacznie krótszej niż $2\sqrt{5}$. Dowcip polega na tym, że mniejszy okrąg ma promień $\sqrt{20}$, większy ma promień $\sqrt{25}$, a żadna z liczb 21, 22, 23, 24 nie jest sumą dwóch kwadratów (liczb całkowitych), więc w pierścieniu kołowym $\mathcal{P}(\sqrt{20}, \sqrt{25})$ nie ma ani jednego punktu kratowego. Można więc w nim przesuwać odcinek nieznacznie krótszy niż $2\sqrt{5}$.

LEMAT 5.2 *Dla dowolnej liczby naturalnej s istnieje ciąg kolejnych liczb naturalnych $c+1, c+2, \ldots, c+s$, z których żadna nie jest sumą dwóch kwadratów liczb całkowitych.*

D O W Ó D. Niech $p_1, p_2, \ldots, p_s$ będzie dowolnym układem różnych liczb pierwszych postaci $4x+3$. Nietrudno udowodnić istnienie takiego układu, zobacz 5.5.5 P2. Niech $k > 0$ będzie dowolnym rozwiązaniem układu

$$\begin{cases} x \equiv p_1 - 1 \,(\mathrm{mod}\, p_1^2) \\ x \equiv p_2 - 2 \,(\mathrm{mod}\, p_2^2) \\ \qquad \vdots \\ x \equiv p_s - s \,(\mathrm{mod}\, p_s^2) \end{cases}$$

Wówczas liczba $k+j$ dzieli się przez p_j ale nie dzieli się przez p_j^2, n i e j e s t więc sumą dwóch kwadratów, zobacz twierdzenie T8.2. Q.e.d.

Dzięki temu lematowi możemy rozważyć ciąg $k+1, k+2, \ldots, k+s$ kolejnych liczb naturalnych nie będących sumami dwóch kwadratów. I niech $R_1 = \sqrt{k+1/2}$, $R_2 = \sqrt{k+s+1/2}$. Twierdzimy, że w pierścieniu $\mathcal{P}(R_1, R_2)$ o środku $O = (0, 0)$ nie ma ani jednego punktu kratowego. Gdyby bowiem $\mathbb{Z} \times \mathbb{Z} \ni (a, b) \in \mathcal{P}(R_1, R_2)$, to

$$R_1 < \sqrt{a^2+b^2} < R_2 \quad \Longrightarrow \quad k + \tfrac{1}{2} < a^2 + b^2 < k + s + \tfrac{1}{2}.$$

Ale to jest niemożliwe, bo żadna liczba całkowita z przedziału $[\,k+1;\, k+s\,]$ n i e j e s t sumą dwóch kwadratów. Oszacujemy teraz długość cięciwy okręgu $K(O, R_2)$ leżącej na zewnątrz okręgu $K(O, R_1)$. Z twierdzenia Pitagorasa zastosowanego do trójkąta prostokątnego $\triangle OAM$, gdzie M jest środkiem boku $\overline{AB}$, patrz rysunek 5.1, mamy $|AB| = 2\sqrt{R_2^2 - R_1^2} = 2\sqrt{s}$. Zatem, aby zapewnić sobie możliwość bezkolizyjnego obrócenia igły o kąt prosty, wystarczy wybrać liczbę naturalną $s \geqslant 1006^2$. Resztę rozwiązania zadania opuszczamy. $\Diamond$

5.3.3 Uogólnione twierdzenie chińskie o resztach

W tym ustępie powiemy o uogólnionym twierdzeniu chińskim o resztach. Mówi ono o możliwości rozwiązania układu (5.16) bez założenia względnej pierwszości par m_i, m_j. Pokażemy również jedną interesującą interpretację takiego uogólnionego twierdzenia chińskiego.

LEMAT 5.3 *Niech $m_1 \neq m_2\ (\geqslant 2)$ będą dowolnymi modułami, niech $d = \mathrm{NWD}\,(m_1, m_2)$ oraz $m = \mathrm{NWW}\,(m_1, m_2)$. Wówczas układ kongruencji*

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, m_1) \\ x \equiv b_2 \,(\mathrm{mod}\, m_2) \end{cases} \tag{5.19}$$

ma rozwiązanie wtedy i tylko wtedy, gdy $d | b_1 - b_2$. Ponadto, jeżeli ten warunek jest spełniony, to istnieje taka liczba całkowita b, że układ ten jest r ó w n o w a ż n y jednej kongruencji

$$x \equiv b \,(\mathrm{mod}\, m). \tag{5.20}$$

D O W Ó D. Załóżmy, że x_0 jest rozwiązaniem układu (5.19). Wówczas $x_0 = b_1 + m_1 u_1$ dla pewnego $u_1 \in \mathbb{Z}$ i jednocześnie $x_0 = b_2 + m_2 u_2$ dla pewnego $u_2 \in \mathbb{Z}$. Zatem $m_1 u_1 - m_2 u_2 = b_2 - b_1$, co oznacza, że równanie

$$m_1 x - m_2 y = b_2 - b_1 \tag{5.21}$$

ma rozwiązanie (u_1, u_2) w liczbach całkowitych. Odwrotnie, jeżeli równanie (5.21) ma rozwiązanie (x, y) w liczbach całkowitych, to $x_0 = b_1 + m_1 x$ $(= b_2 + m_2 y)$ jest rozwiązaniem układu (5.19). Z twierdzenia Bachet'*a* T2.12 wiemy, że warunkiem koniecznym i wystarczającym rozwiązalności równania (5.21) w liczbach całkowitych jest zachodzenie podzielności $d|b_2 - b_1$. Wobec tego pierwsza część lematu jest udowodniona.

Załóżmy teraz, że spełniony jest warunek $d|b_1 - b_2$. Niech

$$d = m_1 u_0 + m_2 v_0. \tag{5.22}$$

Taka równość zachodzi dla pewnych $u_0, v_0 \in \mathbb{Z}$, zobacz twierdzenie Gaussa-Bézout'*a* T2.6. Twierdzimy, że wówczas

$$b = b_1 + \frac{m_1 u_0}{d}(b_2 - b_1) \tag{5.23}$$

jest szukaną liczbą. Aby się o tym przekonać musimy sprawdzić, że

$$x - b \in (m) \iff x - b_1 \in (m_1) \quad \text{i} \quad x - b_2 \in (m_2)$$

dla dowolnej liczby całkowitej x. (Przypomnijmy, że (a) oznacza zbiór (wszystkich) całkowitoliczbowych wielokrotności liczby $a \in \mathbb{Z}$ i że zachodzi równość: $m_1 m_2 = dm$, zobacz T2.9.) Ta równoważność łatwo wynika z równości (5.23) i z, wynikającej z niej (dzięki równości (5.22)), równości $b = b_2 + \frac{m_2 v_0}{d}(b_1 - b_2)$. Sprawdzenie pozostawiamy Czytelnikowi. □

Lemat L5.3 stanowi bazę rozumowania indukcyjnego, za pomocą którego udowodnimy uogólnione twierdzenie chińskie o resztach:

TWIERDZENIE 5.9 (***Uogólnione twierdzenie chińskie o resztach***) *Układ* (5.16) *ma rozwiązania wtedy i tylko wtedy, gdy dla wszystkich* $1 \leqslant i < j \leqslant r$ *zachodzi*

$$b_i \equiv b_j \,(\mathrm{mod}\, \mathrm{NWD}\,(m_i, m_j)). \tag{5.24}$$

Ponadto, gdy te warunki są spełnione, to istnieje taka liczba $B \in \mathbb{Z}$, *że układ* (5.16) *jest równoważny jednej kongruencji*

$$x \equiv B \,(\mathrm{mod}\, M), \tag{5.25}$$

gdzie $M = \mathrm{NWW}\,(m_1, m_2, \ldots, m_r)$.

D O W Ó D. Załóżmy, że $x_0 \in \mathbb{Z}$ jest rozwiązaniem układu (5.16). Wówczas $x_0 = b_i + m_i t$ i jednocześnie $x_0 = b_j + m_j s$ dla pewnych liczb całkowitych t, s. Stąd (odejmując) otrzymujemy równość $b_i - b_j = m_j s - m_i t$, z której na mocy T2.12, dostajemy: NWD $(m_i, m_j)|b_i - b_j$, czyli $b_i \equiv b_j \,(\mathrm{mod}\, \mathrm{NWD}\,(m_i, m_j))$. To dowodzi k o n i e c z n o ś c i zachodzenia warunków (5.24) dla rozwiązalności układu (5.16).

Pokażemy teraz, że zachodzenie kongruencji (5.24) jest w a r u n k i e m w y s t a r c z a j ą c y m istnienia rozwiązania układu (5.16). Zrobimy to za pomocą indukcji względem r. Załóżmy w tym celu, że warunki typu (5.24) implikują istnienie rozwiązań układów typu (5.16) mających $r-1$ kongruencji i rozważmy układ (5.16) spełniający (5.24). W szczególności, mamy $b_1 \equiv b_2 \,(\mathrm{mod}\,\mathrm{NWD}\,(m_1,\, m_2))$. Warunek ten, jak wiemy z lematu, implikuje, że układ (5.16) równoważny jest z układem $r-1$ kongruencji:

$$\begin{cases} x \equiv b \,(\mathrm{mod}\, m) \\ x \equiv b_3 \,(\mathrm{mod}\, m_3) \\ \quad \dots \\ x \equiv b_r \,(\mathrm{mod}\, m_r) \end{cases} \tag{5.26}$$

gdzie b zadane jest przez (5.23), a $m = \mathrm{NWW}\,(m_1,\, m_2)$. Jeżeli uda się nam sprawdzić, że

$$b \equiv b_k \,(\mathrm{mod}\,\mathrm{NWD}\,(m,\, m_k)) \tag{5.27}$$

dla każdego $k = 3, \dots, r$, to korzystając z założenia indukcyjnego, udowodnimy istnienie rozwiązania układu (5.26), czyli również (równoważnego mu) układu (5.16).

Niech p będzie dowolną liczbą pierwszą. Oznaczmy przez

$$\alpha = v_p(m_1), \quad \beta = v_p(m_2), \quad \gamma = v_p(m_k)$$

odpowiednie wykładniki p-adyczne. Czytelnik, który dotychczas nie rozwiązał ćwiczeń C2.41, C2.42 i C2.43 powinien teraz to zrobić. Kongruencja (5.27) jest, na mocy C2.41, równoważna nierównościom $v_p(\mathrm{NWD}\,(m,\, m_k)) \leqslant v_p(b-b_k)$ dla każdego p. Te nierówności są, wobec C2.42, równoważne nierównościom

$$\min\{\max\{v_p(m_1),\, v_p(m_2)\},\, v_p(m_k)\} \leqslant v_p(b-b_k),$$

czyli $\min\{\max\{\alpha,\, \beta\},\, \gamma\} \leqslant v_p(b-b_k)$. Ponieważ dla dowolnych liczb rzeczywistych α, β, γ zachodzi równość (dowód pozostawiamy Czytelnikowi w charakterze ćwiczenia)

$$\min\{\max\{\alpha,\, \beta\},\, \gamma\} = \max\{\min\{\alpha,\, \gamma\},\, \min\{\beta,\, \gamma\}\}, \tag{5.28}$$

więc ostatnią nierówność można przepisać do postaci:

$$\max\{\min\{\alpha,\, \gamma\},\, \min\{\beta,\, \gamma)\}\} \leqslant v_p(b-b_k).$$

Jasne, że nierówność ta wynika z dwóch nierówności:

$$\min\{\alpha,\, \gamma\} \leqslant v_p(b-b_k), \quad \min\{\beta,\, \gamma\} \leqslant v_p(b-b_k). \tag{5.29}$$

Aby wykazać pierwszą z tych nierówności zauważmy, że, na mocy (5.23), zachodzi równość

$$b - b_k = (b-b_1) + (b_1 - b_k) = m_1 u_0 \cdot \frac{b_2 - b_1}{d} + (b_1 - b_k).$$

Pierwszy składnik sumy stojącej po prawej stronie jest podzielny przez m_1 (bowiem $d|b_1 - b_2$) a drugi jest podzielny przez $p^{\min\{\alpha,\gamma\}}$. Ponieważ $p^{\alpha}|m_1$, więc oba składniki są podzielne przez $p^{\min\{\alpha,\gamma\}}$. Zatem pierwsza nierówność (5.29) jest prawdziwa. Analogicznie, korzystając

z równości $b = b_2 + m_2 v_0 \frac{b_1 - b_2}{d}$, dowodzimy drugiej nierówności (5.29). To kończy dowód kongruencji (5.27).

Załóżmy wreszcie, że x_0 jest dowolnym rozwiązaniem spełniającego warunki (5.24) układu (5.16). Niech B będzie resztą z dzielenia x_0 przez $M = \mathrm{NWW}\,(m_1, m_2, \ldots, m_r)$. Wówczas $x_0 \equiv B \,(\mathrm{mod}\, M)$. Twierdzimy, że k a ż d e rozwiązanie x układu (5.16) spełnia (5.25). Mamy bowiem

$$x \equiv b_k \equiv x_0 \,(\mathrm{mod}\, m_k),$$

czyli $m_k | x - x_0$ dla każdego $k = 1, 2, \ldots, r$. Stąd, wobec podstawowej własności najmniejszej wspólnej wielokrotności, $M | x - x_0$, czyli $x \equiv x_0 \equiv B \,(\mathrm{mod}\, M)$. Równie łatwo sprawdzić, że kongruencja $x \equiv B \,(\mathrm{mod}\, M)$ pociąga warunki $x \equiv b_k \,(\mathrm{mod}\, m_k)$ dla każdego k. To kończy dowód twierdzenia. □

W poniższym zadaniu możemy zobaczyć ładną interpretację uogólnionego twierdzenia chińskiego o resztach:

ZADANIE 5.11 Danych jest r ciągów arytmetycznych $(b_k + m_k t)_{t \in \mathbb{Z}}$ nieskończonych w obie strony. Załóżmy, że każde dwa z nich mają wspólny wyraz. Udowodnić, że wszystkie te ciągi arytmetyczne mają wspólny wyraz.

R o z w i ą z a n i e. Co to znaczy, że ciągi arytmetyczne $(b_i + m_i t)$ i $(b_j + m_j t)$ mają wspólny wyraz? Jeżeli $c = b_i + m_i t_1 = b_j + m_j t_2$ jest takim wspólnym wyrazem, to c jest rozwiązaniem układu kongruencji

$$\begin{cases} x \equiv b_i \,(\mathrm{mod}\, m_i) \\ x \equiv b_j \,(\mathrm{mod}\, m_j) \end{cases}$$

Z lematu L5.3 wiemy, że układ ten ma rozwiązania wtedy i tylko wtedy, gdy

$$\mathrm{NWD}\,(m_i, m_j) | b_i - b_j,$$

czyli, gdy $b_i \equiv b_j \,(\mathrm{mod}\, \mathrm{NWD}\,(m_i, m_j))$.

Jeżeli więc każda para $(b_i + m_i t)$, $(b_j + m_j t)$ z badanych ciągów ma wyraz wspólny, to dla wszystkich $1 \leqslant i < j \leqslant r$ zachodzą kongruencje (5.24), więc, na mocy T5.9, układ (5.16) ma rozwiązania i tworzą one c i ą g a r y t m e t y c z n y $(B + Mt)$, gdzie M oznacza najmniejszą wspólną wielokrotność liczb $m_1, m_2, \ldots, m_r$ a B jest pewną liczbą całkowitą. Wyrazami tego ciągu arytmetycznego są wyrazy wspólne wszystkich badanych ciągów. ◊

5.4 Pierścień klas reszt modulo m

Każdy zna i umie stosować **algebrę parzystości**, to znaczy wie, że suma i iloczyn liczb parzystych jest liczbą parzystą, że suma liczb nieparzystych jest liczbą parzystą, a iloczyn liczb nieparzystych jest liczbą nieparzystą itd. Jeżeli umówimy się oznaczać *parzysty* literą P, a *nieparzysty* literą N, to ta algebra jest wyznaczona przez tabelki:

$+$	P	N
P	P	N
N	N	P

$\cdot$	P	N
P	P	P
N	P	N

(5.30)

Parzysty od nieparzystego różni się resztą z dzielenia przez 2: parzysty to taki, który daje resztę 0, a nieparzysty to taki, który daje resztę 1. Możemy więc oznaczać $P = 0 \,(\mathrm{mod}\, 2)$ i $N = 1 \,(\mathrm{mod}\, 2)$.

5.4.1 Działania na warstwach modulo m

Nauczymy się teraz dodawać i mnożyć warstwy modulo m. Zbiór warstw modulo m wraz z tym dodawaniem i mnożeniem jest pierścieniem przemiennym z jedynką, zob. D1.7.

Definicja 5.6 Niech dana będzie ustalona liczba naturalna $m > 1$. Dla danej liczby całkowitej a oznaczamy

$$a \,(\mathrm{mod}\, m) := \{a + tm : t \in \mathbb{Z}\} = \{\ldots, a - 2m, a - m, a, a + m, a + 2m, \ldots\}.$$

Podzbiór $a \,(\mathrm{mod}\, m) \subseteq \mathbb{Z}$, który jest nieskończonym (w obie strony) ciągiem arytmetycznym o różnicy m, nazywamy **warstwą modulo** m lub **klasą reszt (liczb całkowitych) modulo** m wyznaczoną przez $a \in \mathbb{Z}$. Ponieważ oznaczenie $a \,(\mathrm{mod}\, m)$ jest (jakkolwiek jednoznaczne) dość "ciężkie", więc często stosujemy prostsze oznaczenia, takie jak $\overline{a}$ lub $[a]$. Oczywiście tylko w przypadku, gdy wiemy o jaki moduł m chodzi. Jasne jest, że $a \,(\mathrm{mod}\, m)$ składa się z wszystkich tych (i tylko tych) liczb całkowitych, które dają tę samą resztę z dzielenia przez m co liczba a. Zatem, $a \,(\mathrm{mod}\, m) = b \,(\mathrm{mod}\, m)$ wtedy i tylko wtedy, gdy $a \equiv b \,(\mathrm{mod}\, m)$.

Zbiór wszystkich warstw modulo m oznaczamy symbolem $\mathbb{Z}/m$:

$$\mathbb{Z}/m := \{a \,(\mathrm{mod}\, m) \,:\, a \in \mathbb{Z}\}. \tag{5.31}$$

Ćwiczenie 5.19 Uzasadnić, że $|\mathbb{Z}/m| = m$.

W zbiorze $\mathbb{Z}/m$ wprowadzamy działania **dodawania** i **mnożenia modulo** m:

$$a \,(\mathrm{mod}\, m) + b \,(\mathrm{mod}\, m) := (a + b) \,(\mathrm{mod}\, m), \tag{5.32}$$

$$a \,(\mathrm{mod}\, m) \cdot b \,(\mathrm{mod}\, m) := (a \cdot b) \,(\mathrm{mod}\, m). \tag{5.33}$$

Przykład 1. Napiszemy tabelki dodawania i mnożenia modulo 6. Dla uproszczenia piszemy $\boldsymbol{k} = k \,(\mathrm{mod}\, m)$. Zgodnie ze wzorami (5.32) (odp. (5.33)), $\boldsymbol{k} + \boldsymbol{l} = \boldsymbol{r}$ (odp. $\boldsymbol{k} \cdot \boldsymbol{l} = \boldsymbol{r}$), gdzie r jest resztą z dzielenia sumy $k + l$ (odp. iloczynu kl) przez m.

$+$	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**3**	**4**	**5**	**0**
2	**2**	**3**	**4**	**5**	**0**	**1**
3	**3**	**4**	**5**	**0**	**1**	**2**
4	**4**	**5**	**0**	**1**	**2**	**3**
5	**5**	**0**	**1**	**2**	**3**	**4**

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**
2	**0**	**2**	**4**	**0**	**2**	**4**
3	**0**	**3**	**0**	**3**	**0**	**3**
4	**0**	**4**	**2**	**0**	**4**	**2**
5	**0**	**5**	**4**	**3**	**2**	**1**

$\Diamond$

Przykład 2. Napiszemy jeszcze tabelki dodawania i mnożenia modulo 7. Należy zwrócić uwagę na istotną różnicę w tabelkach mnożenia: w "niezerowej" części tabelki mnożenia modulo

7 nie występuje **0**. Tymczasem w "niezerowej" części tabelki mnożenia modulo 6 warstwa **0** występuje. Czy już teraz potraficie wyjaśnić to zjawisko? W związku z tym należy zajrzeć do ćwiczenia C1.19. Rozwiązanie zagadki pokażemy w T5.11.

$+$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	**0**	**1**	**2**	**3**	**4**	**5**	**6**
1	**1**	**2**	**3**	**4**	**5**	**6**	**0**
2	**2**	**3**	**4**	**5**	**6**	**0**	**1**
3	**3**	**4**	**5**	**6**	**0**	**1**	**2**
4	**4**	**5**	**6**	**0**	**1**	**2**	**3**
5	**5**	**6**	**0**	**1**	**2**	**3**	**4**
6	**6**	**0**	**1**	**2**	**3**	**4**	**5**

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**	**6**
2	**0**	**2**	**4**	**6**	**1**	**3**	**5**
3	**0**	**3**	**6**	**2**	**5**	**1**	**4**
4	**0**	**4**	**1**	**5**	**2**	**6**	**3**
5	**0**	**5**	**3**	**1**	**6**	**4**	**2**
6	**0**	**6**	**5**	**4**	**3**	**2**	**1**

$\Diamond$

Dwa kolejne ćwiczenia są bardzo proste, bardzo nudne i bardzo ważne. Rzetelny Czytelnik powinien bezwzględnie je rozwiązać:

Ćwiczenie 5.20 Udowodnić, że określenia (5.32) i (5.33) są sensowne.

Ćwiczenie 5.21 Udowodnić, że zbiór $\mathbb{Z}/m$ wszystkich warstw modulo m, wraz ze zdefiniowanymi przez równości (5.32) i (5.33) działaniami, jest pierścieniem przemiennym z jedynką, zobacz D1.7. Zerem jest warstwa $\mathbf{0} = 0 \pmod m$, a jedynką jest warstwa $\mathbf{1} = 1 \pmod m$.

Definicja 5.7 Zbiór $\mathbb{Z}/m$ wraz z wyżej określonymi działaniami dodawania i mnożenia modulo m nazywa się **pierścieniem klas reszt (liczb całkowitych) modulo** m.

5.4.2 Grupa $(\mathbb{Z}/m)^*$ warstw odwracalnych

Jedną z pierwszych czynności jaką musimy wykonać, dostawszy do rąk pierścień $\mathcal{R}$, jest wyznaczenie zbioru (grupy) jego elementów odwracalnych $\mathcal{R}^*$, zobacz D1.8. Wiemy, że $\mathbb{Z}^* = \{1, -1\}$ oraz $\mathbb{K}[X]^* = \mathbb{K}^* = \mathbb{K} \setminus \{0\}$. Obecnie chcemy wyznaczyć grupę $(\mathbb{Z}/m)^*$ elementów odwracalnych pierścienia $\mathbb{Z}/m$.

Ćwiczenie 5.22 Udowodnić, że elementem odwrotnym do warstwy odwracalnej $a \pmod m$ w pierścieniu $\mathbb{Z}/m$ jest warstwa $a^{-1} \pmod m$, gdzie a^{-1} jest odwrotnością a modulo m. Wywnioskować stąd, że

$$(\mathbb{Z}/m)^* := \{a \pmod m \,:\, \mathrm{NWD}\,(a,\, m) = 1\}, \tag{5.34}$$

i że $|(\mathbb{Z}/m)^*| = \varphi(m)$, zobacz D4.4.

TWIERDZENIE 5.10 *$(\mathbb{Z}/m)^*$ z działaniem mnożenia modulo m jest grupą abelową.*

DOWÓD. Elementem neutralnym jest $1 \pmod m$. Elementem odwrotnym do danej warstwy $a \pmod m$ jest warstwa $a^{-1} \pmod m$. Pozostałe postulaty są oczywiste(!). $\square$

P r z y k ł a d. Oto tabelka mnożenia modulo 30 w grupie $(\mathbb{Z}/30)^*$:

·	**1**	**7**	**11**	**13**	**17**	**19**	**23**	**29**
1	**1**	**7**	**11**	**13**	**17**	**19**	**23**	**29**
7	**7**	**19**	**17**	**1**	**29**	**13**	**11**	**23**
11	**11**	**17**	**1**	**23**	**7**	**29**	**13**	**19**
13	**13**	**1**	**23**	**19**	**11**	**7**	**29**	**17**
17	**17**	**29**	**7**	**11**	**19**	**23**	**1**	**13**
19	**19**	**13**	**29**	**7**	**23**	**1**	**17**	**11**
23	**23**	**11**	**13**	**29**	**1**	**17**	**19**	**7**
29	**29**	**23**	**19**	**17**	**13**	**11**	**7**	**1**

Warto się przyglądać tej tabelce i jej podobnym. Zauważmy na przykład, że w każdym wierszu (i w każdej kolumnie) występuje permutacja nagłówków – dlaczego? Ostatni wiersz (odpowiednio: ostatnia kolumna) jest odwróceniem pierwszego wiersza (odpowiednio: pierwszej kolumny) – dlaczego? W grupie $(\mathbb{Z}/30)^*$ występują dwa kwadraty: **1** i **19**. Itd. ◊

Ćwiczenie 5.23 Napisać tabelki mnożenia grup $(\mathbb{Z}/6)^*$, $(\mathbb{Z}/5)^*$ i $(\mathbb{Z}/8)^*$. Warto porównać grupy $(\mathbb{Z}/5)^*$ i $(\mathbb{Z}/8)^*$: obie są czteroelementowe, ale istotnie różne!

5.4.3 Ciało $\mathbb{Z}/p$

Grupa $(\mathbb{Z}/m)^*$ jest grupą elementów odwracalnych (jedności) pierścienia $\mathbb{Z}/m$. Pamiętamy, że pierścień jest ciałem, gdy w s z y s t k i e jego niezerowe elementy są odwracalne, zob. D1.10. Dla jakiego modułu m, pierścień $\mathbb{Z}/m$ jest ciałem? Odpowiedź na to pytanie zawarta jest w następującym b a r d z o w a ż n y m twierdzeniu:

TWIERDZENIE 5.11 *Pierścień $\mathbb{Z}/m$ (z dodawaniem i mnożeniem modulo m) jest ciałem wtedy i tylko wtedy, gdy m jest liczbą pierwszą.*

D O W Ó D. Gdy m jest liczbą złożoną, na przykład $m = ab$, to $a \pmod m$ i $b \pmod m$ są dzielnikami zera: $a \pmod m \cdot b \pmod m = m \pmod m = 0 \pmod m$. Więc $\mathbb{Z}/m$ w takim przypadku n i e jest ciałem (zob. C1.19). Gdy m jest liczbą pierwszą, to wszystkie niezerowe warstwy modulo m są odwracalne. Mamy więc w tym przypadku do czynienia z ciałem. □

U w a g a. Jeżeli p jest liczbą pierwszą, to ciało $\mathbb{Z}/p$ oznaczamy również symbolem $\mathbb{F}_p$. W angielszczyźnie matematycznej *ciało* nazywa się *field*.

5.4.4 Pierwiastki kongruencji wielomianowych

Wygodnie będzie nieco inaczej spojrzeć na kongruencje wielomianowe (5.2) i na zbiory rozwiązań takich kongruencji. Opowiemy o tym w przypadku wielomianów jednej zmiennej, choć równie dobrze moglibyśmy to robić w przypadku ogólnym.

Zaczniemy od wprowadzenia wygodnego skrótu. Mianowicie, gdy $h(X) = \sum_{k\geqslant 0} a_k X^k$ i $g(X) = \sum_{k\geqslant 0} b_k X^k$ są dwoma wielomianami o współczynnikach całkowitych, to piszemy

$$h(X) \equiv g(X) \,(\mathrm{mod}\, m), \tag{5.35}$$

gdy $a_k \equiv b_k \,(\mathrm{mod}\, m)$ dla każdego k.

Ćwiczenie 5.24 Udowodnić, że relacja (5.35) jest relacją równoważności. Ponadto, udowodnić, że jest to **relacja zgodna z dodawaniem** i **mnożeniem** wielomianów, co oznacza, że jeżeli $h(X) \equiv g(X) \,(\mathrm{mod}\, m)$ i $k(X) \equiv l(X) \,(\mathrm{mod}\, m)$, to $h(X)+k(X) \equiv g(X)+l(X) \,(\mathrm{mod}\, m)$ i $h(X) \cdot k(X) \equiv g(X) \cdot l(X) \,(\mathrm{mod}\, m)$.

Jeżeli $h(X) = a_0 + a_1 X + \ldots + a_n X^n$ jest dowolnym wielomianem o współczynnikach całkowitych, a m jest dowolnym modułem, to wielomian

$$h(X) \,(\mathrm{mod}\, m) := [h](X) = [a_0] + [a_1]X + \ldots + [a_n]X^n, \tag{5.36}$$

gdzie $[a_k] = a_k \,(\mathrm{mod}\, m)$ jest warstwą modulo m wyznaczoną przez a_k, nazywamy **redukcją** wielomianu $h(X)$ modulo m. Wielomian $h(X) \,(\mathrm{mod}\, m)$ (oznaczany w skrócie $[h](X)$) jest wielomianem o współczynnikach w pierścieniu $\mathbb{Z}/m$.

Jasne, że $h(X) \equiv k(X) \,(\mathrm{mod}\, m)$ wtedy i tylko wtedy, gdy $[h](X) = [k](X)$.

Istnieje mała (i mało ważna) różnica między rozwiązaniem kongruencji $h(x) \equiv 0 \,(\mathrm{mod}\, m)$ a **pierwiastkiem** redukcji $h(X) \,(\mathrm{mod}\, m)$. Możemy powiedzieć, że rozwiązania kongruencji $h(x) \equiv 0 \,(\mathrm{mod}\, m)$ (jeśli istnieją) tworzą warstwy modulo m, a pierwiastki wielomianu $[h](X)$ są warstwami. Pierwiastek redukcji $[h](X) = h(X) \,(\mathrm{mod}\, m)$ wielomianu nazywa się też **pierwiastkiem kongruencji wielomianowej** $h(x) \equiv 0 \,(\mathrm{mod}\, m)$.

OZNACZENIE Dla danego wielomianu $h(X) \in \mathcal{R}[X]$ o współczynnikach w danym pierścieniu $\mathcal{R}$, symbolem $\mathcal{N}(h;\, \mathcal{R})$ oznaczamy zbiór należących do $\mathcal{R}$ pierwiastków wielomianu $h(X)$, czyli takich elementów α należących do $\mathcal{R}$, że $h(\alpha) = 0$, gdzie 0 oznacza zero pierścienia $\mathcal{R}$. Gdy $\mathcal{R}$ jest pierścieniem $\mathbb{Z}/m$ klas reszt liczb całkowitych (czyli warstw) modulo m, a $h(X)$ jest wielomianem o współczynnikach całkowitych, to, oczywiście, mamy utożsamienie

$$\mathcal{N}(h;\, m) = \mathcal{N}([h];\, \mathbb{Z}/m), \tag{5.37}$$

gdzie $[h] = h(X) \,(\mathrm{mod}\, m)$ jest redukcją modulo m. Zbiór $\mathcal{N}(h;\, m)$ jest więc zbiorem pierwiastków redukcji $h(X) \,(\mathrm{mod}\, m)$ wielomianu $h(X)$ modulo m. Czyli zbiorem nierównoważnych rozwiązań kongruencji $h(x) \equiv 0 \,(\mathrm{mod}\, m)$, zobacz D5.2.

Przykład 1. Niech $f(X) = X^2 - 1$, $g(X) = X^4 - 1$. Wówczas

$$\mathcal{N}(f;\, 8) = \mathcal{N}(g;\, 8) = \{1 \,(\mathrm{mod}\, 8),\, 3 \,(\mathrm{mod}\, 8),\, 5 \,(\mathrm{mod}\, 8),\, 7 \,(\mathrm{mod}\, 8)\}.$$

Podczas gdy $\mathcal{N}(f;\, 5) = \{1 \,(\mathrm{mod}\, 5),\, 4 \,(\mathrm{mod}\, 5)\}$, a $\mathcal{N}(g;\, 5) = (\mathbb{Z}/5)^*$. $\Diamond$

Ćwiczenie 5.25 Przekonać się, że małe twierdzenie Fermat'a może być zapisane następująco: *Jeżeli p jest liczbą pierwszą, a $h(X) = X^{p-1} - 1$, to $\mathcal{N}(h;\, p) = (\mathbb{Z}/p)^*$.* Lub, równoważnie: *Jeżeli p jest liczbą pierwszą, a $f(X) = X^p - X$, to $\mathcal{N}(f;\, p) = \mathbb{Z}/p$.*

Ćwiczenie 5.26 Rozważmy wielomian $h(X) = X^2 - 1$. Udowodnić, że dla dowolnej liczby pierwszej $p > 2$ i dowolnego wykładnika $e \in \mathbb{N}$ zachodzi równość $N(h;\, p^e) = 2$. Czyli, że warstwy $1 \,(\mathrm{mod}\, p^e)$ i $(-1) \,(\mathrm{mod}\, p^e)$ są jedynymi pierwiastkami kongruencji $x^2 \equiv 1 \,(\mathrm{mod}\, p^e)$.

Ćwiczenie 5.27 Rozważmy wielomian $h(X) = X^2 - 1$. Dowieść, że zachodzą równości $N(h;\, 2) = 1$, $N(h;\, 4) = 2$ oraz $N(h;\, 2^e) = 4$ dla dowolnego wykładnika $e \geqslant 3$.

Ćwiczenie 5.28 Niech $h(X) = X^8 - 1$. Uzasadnić, że $N(h;\, 15) = 8$. Uogólnić!

Zbiór $\mathcal{N}(h;\, m)$, jako podzbiór zbioru skończonego $\mathbb{Z}/m$, sam jest zbiorem skończonym (być może – pustym). Istnieje więc łatwa (tym łatwiejsza im mniejszy jest moduł m) procedura wyznaczania tego zbioru. W szczególności, istnieje procedura sprawdzania czy zbiór ten jest niepusty. Jasne jest też (była już o tym mowa w ustępie 5.1.2), że jeżeli dany jest wielomian $h(X)$ o współczynnikach całkowitych, to niepustość zbiorów $\mathcal{N}(h;\, m)$ dla każdego m jest warunkiem koniecznym istnienia pierwiastków całkowitych wielomianu $h(X)$:

$$a \in \mathcal{N}(h;\, \mathbb{Z}) \quad \Longrightarrow \quad a \,(\mathrm{mod}\, m) \in \mathcal{N}(h;\, m)$$

dla każdego m. Ten warunek konieczny na ogół nie jest warunkiem wystarczającym:

Przykład 2. Dany jest wielomian $h(X) = 6X^2 - X - 1$. Łatwo sprawdzić, że nie ma on pierwiastków całkowitych. Pokażemy, że $\mathcal{N}(h;\, m)$ jest zbiorem niepustym przy dowolnym module m. Przedstawmy bowiem dowolny moduł w postaci iloczynu $m = 2^k n$, gdzie $k = v_2(m)$. Wówczas $\mathrm{NWD}\,(n,\, 2^k) = 1$, więc, zobacz twierdzenie chińskie, układ

$$\begin{cases} 3x + 1 \equiv 0 \,(\mathrm{mod}\, 2^k), \\ 2x - 1 \equiv 0 \,(\mathrm{mod}\, n) \end{cases} \quad \Longleftrightarrow \quad \begin{cases} x \equiv (-1) \cdot 3^{-1} \,(\mathrm{mod}\, 2^k), \\ x \equiv 2^{-1} \,(\mathrm{mod}\, n) \end{cases}$$

ma rozwiązanie c. Wtedy $6c^2 - c - 1 = (3c + 1)(2c - 1) = 2^k a \cdot nb = mab \equiv 0 \,(\mathrm{mod}\, m)$, czyli $c \,(\mathrm{mod}\, m) \in \mathcal{Z}_h(m)$. Widzimy, że $\mathcal{N}(h;\, m) \neq \varnothing$ dla każdego m, ale $\mathcal{N}(h;\, \mathbb{Z}) = \varnothing$. $\Diamond$

Stosując twierdzenie Bézout'a T3.1 rozwiązujemy:

Ćwiczenie 5.29 Udowodnić, że jeżeli $h(X) \in \mathbb{Z}[X]$ i $a \in \mathbb{Z}$ jest rozwiązaniem kongruencji $h(x) \equiv 0 \,(\mathrm{mod}\, m)$, to istnieje taki wielomian $g(X) \in \mathbb{Z}[X]$, że

$$h(X) \equiv (X - a)g(X) \,(\mathrm{mod}\, m). \tag{5.38}$$

Relacja (5.38) może być równoważnie zapisana tak: $[h](X) = (X - [a])[g](X)$, gdzie $=$ jest równością wielomianów o współczynnikach w $\mathbb{Z}/m$, $[h]$ i $[g]$ oznaczają redukcje odpowiednich wielomianów modulo m, a $[a] = a \,(\mathrm{mod}\, m)$. Załóżmy, że $[a]$ jest pierwiastkiem kongruencji wielomianowej $h(x) \equiv 0 \,(\mathrm{mod}\, m)$. Wówczas, wobec powyższego, mamy $(x - a)g(x) \equiv 0 \,(\mathrm{mod}\, m)$. Należy wyraźnie podkreślić, że z tego nie wynika, że każde rozwiązanie kongruencji $h(x) \equiv 0 \,(\mathrm{mod}\, m)$ jest rozwiązaniem kongruencji $x - a \equiv 0 \,(\mathrm{mod}\, m)$ lub kongruencji $g(x) \equiv 0 \,(\mathrm{mod}\, m)$. Jest to związane z możliwością istnienia dzielników zera w pierścieniu $\mathbb{Z}/m$.

Przykład 3. Rozważmy jeszcze raz redukcję wielomianu $X^2 - 1$ modulo 8. Wiemy, że 1 jest rozwiązaniem kongruencji $x^2 - 1 \equiv 0 \,(\mathrm{mod}\, 8)$. Odpowiedni rozkład (5.38) wygląda tak: $X^2 - 1 \equiv (X - 1)(X + 1) \,(\mathrm{mod}\, 8)$. Ale 3 jest również rozwiązaniem, przeto otrzymujemy $X^2 - 1 \equiv (X - 3)(X + 3) \,(\mathrm{mod}\, 8)$. Zwróćmy uwagę na (gwałcącą nadzieje na jednoznaczność rozkładu!) równość $(X + [7])(X + [1]) = (X + [5])(X + [3])$ w $\mathbb{Z}/8[X]$. $\Diamond$

5.4.5 Kongruencje wielomianowe modulo p

Twierdzenie Lagrange'a[2] T3.4 ma jeden, bardzo ważny w teorii liczb, wniosek. Dla stałych odwołań formułujemy go w postaci osobnego twierdzenia:

TWIERDZENIE 5.12 *Jeżeli $h(X) \in \mathbb{Z}[X]$ jest wielomianem stopnia $n \geqslant 1$, a p jest liczbą pierwszą, to kongruencja $h(x) \equiv 0 \,(\mathrm{mod}\, p)$ ma co najwyżej n rozwiązań.*

D O W Ó D. Rozwiązania kongruencji $h(x) \equiv 0 \,(\mathrm{mod}\, p)$ utożsamiamy z pierwiastkami wielomianu $[h](X) \in \mathbb{Z}/p\,[X]$, a ten wielomian ma stopień[3] $\leqslant n$. Wobec "ciałowości" pierścienia współczynników $\mathbb{Z}/p$ mamy więc tezę na mocy T3.4. □

U w a g a. Podkreślmy mocno wagę założenia pierwszości modułu p. Na przykład wielomian $X^2 - [1] \in \mathbb{Z}/8\,[X]$ ma stopień 2 i c z t e r y pierwiastki w $\mathbb{Z}/8$, zob. 5.4.4 P3. Oczywiście jest to związane z faktem, że pierścień $\mathbb{Z}/8$ n i e jest ciałem.

Ćwiczenie 5.30 Udowodnić, że jeżeli p jest liczbą pierwszą, to wielomian $X^{p-1} - [1]$ o współczynnikach w ciele $\mathbb{F}_p$ rozkłada się na czynniki liniowe (= pierwszego stopnia)

$$X^{p-1} - [1] = (X - [1])(X - [2]) \cdot \ldots \cdot (X - [p-1])$$

w pierścieniu $\mathbb{F}_p[X]$. Ta równość jest równoważna z MTF. Dlaczego?

Ćwiczenie 5.31 Korzystając z C5.30 udowodnić raz jeszcze twierdzenie Wilsona.

Ćwiczenie 5.32 Dana jest liczba pierwsza p i wielomian $h(X) \in \mathbb{Z}[X]$. Udowodnić, że $p|h(c)$ dla każdego $c \in \mathbb{Z}$ wtedy i tylko wtedy, gdy istnieje taki wielomian $g(X) \in \mathbb{Z}[X]$, że $h(X) \equiv (X^p - X)g(X) \,(\mathrm{mod}\, p)$.

5.4.6 Ważne zastosowanie twierdzenia chińskiego

Najważniejszym zastosowaniem twierdzenia chińskiego są poniższe T5.13 i WT5.13. Mówią one, że problem i s t n i e n i a i wyznaczenia l i c z b y rozwiązań kongruencji $h(x) \equiv 0 \,(\mathrm{mod}\, m)$ dla dowolnego modułu m, jest sprowadzalny do problemów istnienia i wyznaczania liczby rozwiązań kongruencji $h(x) \equiv 0 \,(\mathrm{mod}\, p^{v_p(m)})$ dla dzielników pierwszych $p \in \mathrm{Supp}(m)$. Mówimy w takiej sytuacji o **lokalizacji problemu** w liczbie (dla liczby) pierwszej p.

TWIERDZENIE 5.13 *Niech $h(X) \in \mathbb{Z}[X]$ i niech $m = m_1 m_2 \cdot \ldots \cdot m_s$ będzie rozkładem na czynniki parami względnie pierwsze. Wówczas, istnieje bijekcja:*

$$\psi : \mathcal{N}(h;\, m_1) \times \mathcal{N}(h;\, m_2) \times \ \ldots \ \times \mathcal{N}(h;\, m_s) \longleftrightarrow \mathcal{N}(h;\, m).$$

[2] Z historycznego punktu widzenia ta nazwa jest pewnym nadużyciem: zazwyczaj, zobacz na przykład [**11**], to tylko twierdzenie T5.12 przypisuje się Lagrange'*owi*.

[3] Zauważmy, że ten stopień może być m n i e j s z y niż n. Na przykład redukcja wielomianu $3X^2 + X + 1$ modulo 3 jest wielomianem stopnia 1 w $\mathbb{Z}/3[X]$.

D O W Ó D. Zauważmy najpierw, że jeżeli $\mathcal{N}(h;\, m_i)$ jest zbiorem pustym dla pewnego $1 \leqslant i \leqslant s$, to i $\mathcal{N}(h;\, m)$ jest zbiorem pustym. Istotnie, jeżeli $c \,(\mathrm{mod}\, m) \in \mathcal{N}(h;\, m)$, czyli $m|h(c)$, to $m_i|h(c)$, więc $c \,(\mathrm{mod}\, m_i) \in \mathcal{N}(h;\, m_i)$. Załóżmy więc, że zbiory $\mathcal{N}(h;\, m_i)$ są niepuste dla wszystkich $1 \leqslant i \leqslant s$. Niech

$$(c_1 \,(\mathrm{mod}\, m_1),\, c_2 \,(\mathrm{mod}\, m_2),\, \ldots,\, c_s \,(\mathrm{mod}\, m_s)) \in \mathcal{N}(h;\, m_1) \times \mathcal{N}(h;\, m_2) \times \ldots \times \mathcal{N}(h;\, m_s)$$

i niech c będzie (istniejącym na mocy twierdzenia chińskiego) rozwiązaniem układu

$$\begin{cases} x \equiv c_1 \,(\mathrm{mod}\, m_1), \\ x \equiv c_2 \,(\mathrm{mod}\, m_2), \\ \qquad \ldots \\ x \equiv c_s \,(\mathrm{mod}\, m_s). \end{cases} \tag{5.39}$$

Kładziemy $\psi(c_1 \,(\mathrm{mod}\, m_1),\, c_2 \,(\mathrm{mod}\, m_2),\, \ldots,\, c_s \,(\mathrm{mod}\, m_s)) = c \,(\mathrm{mod}\, m)$. Sprawdzenie, że to jest p o p r a w n i e o k r e ś l o n a b i j e k c j a pozostawiamy Czytelnikowi. □

Z tego twierdzenia mamy natychmiastowy wniosek:

WNIOSEK *Niech $m = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ będzie kanonicznym rozkładem liczby naturalnej na czynniki pierwsze i niech $h(X)$ będzie wielomianem o współczynnikach całkowitych. Wówczas kongruencja $h(x) \equiv 0 \,(\mathrm{mod}\, m)$ ma rozwiązanie wtedy i tylko wtedy, gdy mają rozwiązania kongruencje $h(x) \equiv 0 \,(\mathrm{mod}\, p_k^{e_k})$ dla wszystkich k. Co więcej, zachodzi równość*

$$N(h;\, m) = N(h;\, p_1^{e_1}) \cdot N(h;\, p_2^{e_2}) \cdot \ldots \cdot N(h;\, p_s^{e_s}). \quad \square$$

P r z y k ł a d 1. Niech $f(X) = X^2 + 4X + 5 \in \mathbb{Z}[X]$. Wyznaczymy zbiór $\mathcal{N}(f;\, 65)$ pierwiastków kongruencji $f(x) \equiv 0 \,(\mathrm{mod}\, 65)$. Znajdziemy w tym celu zbiory $\mathcal{N}(f;\, 5)$ i $\mathcal{N}(f;\, 13)$. Kongruencje kwadratowe będziemy wprawdzie systemowo rozwiązywać dopiero w paragrafie 5.7, ale już teraz możemy łatwo sprawdzić, że kongruencja $f(x) \equiv 0 \,(\mathrm{mod}\, 5)$ ma dwa rozwiązania $0 \,(\mathrm{mod}\, 5)$ i $1 \,(\mathrm{mod}\, 5)$, a kongruencja $f(x) \equiv 0 \,(\mathrm{mod}\, 13)$ również ma dwa rozwiązania $3 \,(\mathrm{mod}\, 13)$ i $6 \,(\mathrm{mod}\, 13)$. Na mocy WT5.13 widzimy więc, że $\mathcal{N}(f;\, 65)$ jest zbiorem 4-elementowym. Dla wyznaczenia tego zbioru, czyli zbioru wszystkich pierwiastków kongruencji $x^2 + 4x + 5 \equiv 0 \,(\mathrm{mod}\, 65)$, musimy rozwiązać układy typu (5.39). W tym przypadku:

$$\begin{cases} x \equiv 0 \,(\mathrm{mod}\, 5), \\ x \equiv 3 \,(\mathrm{mod}\, 13), \end{cases} \quad \begin{cases} x \equiv 0 \,(\mathrm{mod}\, 5), \\ x \equiv 6 \,(\mathrm{mod}\, 13), \end{cases} \quad \begin{cases} x \equiv 1 \,(\mathrm{mod}\, 5), \\ x \equiv 3 \,(\mathrm{mod}\, 13), \end{cases} \quad \begin{cases} x \equiv 1 \,(\mathrm{mod}\, 5), \\ x \equiv 6 \,(\mathrm{mod}\, 13). \end{cases}$$

Oto rozwiązania: $x_1 \equiv 55 \,(\mathrm{mod}\, 65)$, $x_2 \equiv 45 \,(\mathrm{mod}\, 65)$, $x_3 \equiv 16 \,(\mathrm{mod}\, 65)$, $x_4 \equiv 6 \,(\mathrm{mod}\, 65)$. ◊

P r z y k ł a d 2. Niech $g(X) = X^2 + 3X + 16 \in \mathbb{Z}[X]$. Wyznaczymy zbiór $\mathcal{N}(g;\, 85)$ pierwiastków (= rozwiązań) kongruencji $g(x) \equiv 0 \,(\mathrm{mod}\, 85)$. Kongruencja $g(x) \equiv 0 \,(\mathrm{mod}\, 5)$ ma tylko jedno rozwiązanie $1 \,(\mathrm{mod}\, 5)$ (przekonanie się o tym przez sprawdzenie pięciu możliwości, jest natychmiastowe, a poza tym $g(x) \equiv (x-1)^2 \,(\mathrm{mod}\, 5)$). Jednocześnie, ponieważ

$$g(x) \equiv x^2 + 3x + 16 \equiv x^2 + 20x - 1 \equiv x^2 + 2 \cdot 10x + 100 - 100 - 1 \equiv (x+10)^2 + 1 \,(\mathrm{mod}\, 17),$$

więc kongruencja $g(x) \equiv 0 \,(\mathrm{mod}\, 17)$ ma dwa rozwiązania $x \equiv \pm 4 - 10$, czyli $3 \,(\mathrm{mod}\, 17)$ oraz $11 \,(\mathrm{mod}\, 17)$. Rozwiązując odpowiednie układy typu (5.39) znajdujemy wszystkie(!) dwa rozwiązania $x_1 \equiv 71 \,(\mathrm{mod}\, 85)$ i $x_2 \equiv 11 \,(\mathrm{mod}\, 85)$. ◊

P r z y k ł a d 3. Niech $h(X) = X^2 - 3X - 5 \in \mathbb{Z}[X]$. Zbiór $\mathcal{N}(h;\, 55)$ jest pusty, bo kongruencja $h(x) \equiv 0 \,(\mathrm{mod}\, 11)$ nie ma rozwiązań (sprawdźcie!). ◊

Ćwiczenie 5.33 Wyznaczyć $N(X^2-1;\,m)$ w zależności od modułu m. *Wskazówka.* Jeżeli kanonicznym rozkładem m na czynniki pierwsze jest $m = 2^e p_1^{e_1}\cdot\ldots\cdot p_s^{e_s}$, przy czym $e_1\cdot\ldots\cdot e_s \neq 0$, to powinniśmy dostać $N(X^2-1;\,m) = 2^{s+\varepsilon(e)}$, gdzie $\varepsilon(e)=0$, gdy $e\leqslant 1$, $\varepsilon(e)=1$, gdy $e=2$ i $\varepsilon(e)=2$, gdy $e\geqslant 2$.

Ćwiczenie 5.34 Wielomian $h(X)\in\mathbb{Z}[X]$ wyznacza funkcję $\mathbb{N}\ni m\longmapsto N(h;\,m)\in\mathbb{Z}$. Udowodnić, że ta funkcja jest funkcją arytmetyczną multyplikatywną, zobacz D4.2.

5.5 Rząd elementu grupy w teorii liczb

Grupy są najbardziej fundamentalnymi strukturami całej matematyki. Występują w różnych jej działach. Grają też bardzo ważną rolę w teorii liczb. Ten paragraf poświęcamy na wstępne wyjaśnienie tej roli. Pierwsze dwa ustępy mają charakter ogólny. Czytanie można zacząć od ustępu 5.5.4. Ostatnie dwa ustępy pokazują zastosowania nieco bardziej wysublimowane.

5.5.1 Podgrupy i twierdzenie Lagrange'*a*

Zdefiniujemy teraz pojęcie podgrupy i udowodnimy podstawowe twierdzenie Lagrange'*a*.

Niech $(\Gamma,*)$ będzie grupą z działaniem $*$ i elementem neutralnym ε. Jasne, że k-ta **potęga** α^k elementu $\alpha\in\Gamma$ oznacza k-krotny iloczyn $\alpha*\alpha*\ldots*\alpha$. Oczywistym jest, że prawidłowo należy to określić indukcyjnie: $\alpha^1=\alpha$ i $\alpha^{k+1}=\alpha^k*\alpha$ dla $k\in\mathbb{N}$. Będziemy również uważać, że $\alpha^0=\varepsilon$ oraz $\alpha^{-k}=(\alpha^{-1})^k$. Wtedy:

Ćwiczenie 5.35 Udowodnić, że dla dowolnego elementu α danej grupy z działaniem $*$ i dowolnych liczb całkowitych m, n mamy: $\alpha^{m+n}=\alpha^m*\alpha^n$ i $(\alpha^m)^n=(\alpha^n)^m=\alpha^{mn}$.

Uwaga. Jasne jest również, że w przypadku addytywnym (to znaczy, w przypadku działania dodawania zapisywanego za pomocą znaku $+$) k-tą potęgę elementu α nazywamy k-tą **wielokrotnością** i oznaczamy symbolem $k\alpha$ (czasem $k\cdot\alpha$). Przy czym $-\alpha=(-1)\cdot\alpha$ oznacza **element przeciwny** do α. Równości z ćwiczenia C5.35 mają w takim przypadku postać:

$$(m+n)\alpha = m\alpha+n\alpha,\quad n(m\alpha)=m(n\alpha)=(mn)\alpha.$$

Definicja 5.8 Niech $(\Gamma,*)$ będzie grupą. Niepusty podzbiór Λ zbioru Γ nazywamy **podgrupą** grupy Γ, gdy dla dowolnych dwóch elementów $\alpha,\beta\in\Lambda$ zarówno $\alpha*\beta$ jak i α^{-1} należą do zbioru Λ. (Mówimy, że Λ jest **zamknięty** względem działania $*$ i brania odwrotności.)

Przykłady. (1) Każdy ideał w pierścieniu $\mathbb{Z}$ jest podgrupą grupy $(\mathbb{Z},+)$. (2) Zbiór

$$T=\{z\in\mathbb{C}:\,|z|=1\} \tag{5.40}$$

liczb zespolonych o module równym 1 jest grupą względem mnożenia liczb zespolonych. (3) Dla dowolnej liczby naturalnej n podzbiór $\mu_n(\mathbb{C})$ pierwiastków n-tego stopnia z 1 jest podgrupą grupy T, zobacz C1.35 i C1.36. (4) Sama grupa T jest podgrupą grupy $(\mathbb{C}^*,\cdot)$ niezerowych liczb zespolonych z mnożeniem jako działaniem. (5) $\mathbb{Z}$ jest podgrupą w grupie $(\mathbb{Q},+)$ liczb wymiernych z dodawaniem. (6) Jeżeli $(\Gamma,*)$ jest dowolną grupą, α jest dowolnym jej elementem, to zbiór $(\alpha):=\{\alpha^k:\,k\in\mathbb{Z}\}$ wszystkich potęg elementu α jest podgrupą grupy Γ. Nazywamy ją **podgrupą generowaną przez** α. ◊

Ćwiczenie 5.36 Uzasadnić wszystkie tezy powiedziane w powyższych przykładach.

Udowodnimy teraz kolejne (nie ostatnie w tym skrypcie!) twierdzenie Lagrange'*a*:

LEMAT 5.4 (***Twierdzenie Lagrange'a***) *Załóżmy, że* Γ *jest grupą skończoną, a* Λ *jest jej podgrupą. Jeżeli* $\operatorname{card}(\Gamma) = n$ *i* $\operatorname{card}(\Lambda) = r$, *to* $r|n$.

D O W Ó D. Niech $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_r\}$. Dla dowolnego elementu $\alpha \in \Gamma$ oznaczmy:

$$\alpha\Lambda := \{\alpha * \lambda_1, \alpha * \lambda_2, \ldots, \alpha * \lambda_r\}.$$

Sprawdzamy najpierw, że zbiory postaci $\alpha\Lambda$ są albo r o z ł ą c z n e albo się p o k r y w a j ą. Rzeczywiście, jeżeli $\alpha\Lambda \cap \beta\Lambda \neq \varnothing$ i $\gamma \in \alpha\Lambda \cap \beta\Lambda$, to $\gamma = \alpha * \lambda_i = \beta * \lambda_j$ dla pewnych $1 \leqslant i, j \leqslant m$. Stąd: d o w o l n y element $\alpha * \lambda_k$ zbioru $\alpha\Lambda$ może być zapisany jako

$$\alpha * \lambda_k = (\gamma * \lambda_i^{-1}) * \lambda_k = \gamma * (\lambda_i^{-1} * \lambda_k) = (\beta * \lambda_j) * (\lambda_i^{-1} * \lambda_k) = \beta * [\lambda_j * (\lambda_i^{-1} * \lambda_k)].$$

Ponieważ Λ jest podgrupą, więc $\lambda_j * (\lambda_i^{-1} * \lambda_k) \in \Lambda$. Wobec tego $\alpha * \lambda_k \in \beta\Lambda$. W ten sposób wykazaliśmy, że $\alpha\Lambda \subseteq \beta\Lambda$. Tak samo sprawdzamy, że $\beta\Lambda \subseteq \alpha\Lambda$. Zatem $\alpha\Lambda = \beta\Lambda$.

Łatwo też sprawdzić, że każdy ze zbiorów $\alpha\Lambda$ ma dokładnie r elementów. Istotnie, jeżeli $\alpha * \lambda_i = \alpha * \lambda_j$, to mnożąc tę równość z lewej strony przez α^{-1} dostajemy równość $\lambda_i = \lambda_j$.

Z powyższego wynika, że zbiór Γ jest s u m ą r o z ł ą c z n ą pewnej liczby (oznaczmy ją k) zbiorów $\alpha\Lambda$, z których każdy ma r elementów. Stąd $n = r \cdot k$, czyli $r|n$. □

5.5.2 Podstawowe własności rzędu elementu

Każdemu elementowi grupy skończonej przyporządkowujemy tak zwany rząd, który jest najmniejszym $\geqslant 1$ wykładnikiem potęgi, do jakiej należy podnieść ten element, aby otrzymać element neutralny. Udowodnimy trzy podstawowe twierdzenia o rzędzie.

Definicja 5.9 Dana jest grupa Γ i jej element α. **Rzędem** elementu $\alpha \in \Gamma$ nazywamy n a j m n i e j s z ą taką liczbę naturalną r, że $\alpha^r = \varepsilon$. Rząd elementu α, jeżeli istnieje, oznaczamy symbolem $\operatorname{rz}(\alpha)$. Jeżeli $\alpha^k \neq \varepsilon$ dla każdego $k \in \mathbb{N}$, to mówimy, że α jest elementem **rzędu nieskończonego**.

P r z y k ł a d. Warstwa $4 \pmod{11}$ jako element grupy $\mathbb{Z}/11$ z dodawaniem $\pmod{11}$ ma rząd równy 11. Ta sama warstwa, jako element grupy $(\mathbb{Z}/11)^*$ z mnożeniem $\pmod{11}$, ma rząd równy 5. Liczba -1 jako element grupy $(\mathbb{Z}, +)$ jest elementem rzędu nieskończonego, a liczba 0 ma w tej samej grupie rząd 1. Czytelnik zechce samodzielnie to sprawdzić. ◊

Udowodnimy teraz trzy podstawowe twierdzenia o rzędzie elementów grup:

TWIERDZENIE 5.14 *Każdy element grupy skończonej ma rząd* (*skończony*!) *i rząd ten jest dzielnikiem liczby elementów grupy.*

D O W Ó D. Niech Γ będzie grupą skończoną, $\operatorname{card}(\Gamma) = n$. Niech $\alpha \in \Gamma$ będzie dowolnym jej elementem. Wypiszmy ciąg k o l e j n y c h p o t ę g elementu α:

$$\alpha^0, \alpha^1, \alpha^2, \alpha^3, \ldots \alpha^n, \ldots \tag{5.41}$$

i rozważmy $n+1$ początkowych wyrazów tego ciągu. Ponieważ tych wyrazów jest więcej niż elementów w grupie Γ, więc co najmniej dwa z tych wyrazów są równe. Niech $\alpha^k = \alpha^l$, dla pewnych $0 \leqslant k < l \leqslant n$. Mnożąc tę równość lewostronnie przez $\alpha^{-k} = (\alpha^k)^{-1}$ dostajemy:

$$\varepsilon = \alpha^0 = \alpha^{-k} * \alpha^k = \alpha^{-k} * \alpha^l = \alpha^{l-k}.$$

Kładąc $t = l - k$ mamy $\alpha^t = \varepsilon$. Widzimy więc, że istnieją d o d a t n i e wykładniki t, dla których $\alpha^t = \varepsilon$. Dzięki Zasadzie Minimum możemy wybrać n a j m n i e j s z y taki wykładnik. Oznaczmy go r. Uzasadniliśmy w ten sposób, że element α m a r z ą d. Zauważmy, że elementy $\alpha, \alpha^2, \ldots, \alpha^r = \varepsilon$ są p a r a m i r ó ż n e. (Gdyby $\alpha^k = \alpha^l$ dla $1 \leqslant k < l \leqslant d$, to, tak jak wyżej, dostalibyśmy równość $\alpha^{l-k} = \varepsilon$, co jest niemożliwe, bo $0 < l - k < r$.) Ponadto, jeżeli $m \in \mathbb{Z}$ jest dowolną liczbą całkowitą, $m = qr + s$, $0 \leqslant s < r$, jest wynikiem dzielenia z resztą m przez r, to $\alpha^m = \alpha^{qr+s} = (\alpha^r)^q * \alpha^s = \varepsilon^q * \alpha^s = \varepsilon * \alpha^s = \alpha^s$.

Widzimy stąd, że podgrupa (α) generowana przez α jest równa

$$\Lambda := \{\varepsilon, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}. \tag{5.42}$$

Dla zakończenia dowodu wystarczy się powołać na twierdzenie Lagrange'a L5.4. □

TWIERDZENIE 5.15 *Jeżeli dla elementu α pewnej grupy zachodzi równość $\alpha^s = \varepsilon$, gdzie $s \in \mathbb{N}$, to istnieje* $\mathrm{rz}\,(\alpha)$ *i zachodzi podzielność* $\mathrm{rz}\,(\alpha) | s$.

D O W Ó D. Z równości $\alpha^s = \varepsilon$ wynika, że $\mathrm{rz}\,(\alpha)$ i s t n i e j e. Oznaczając go r, dzielimy z resztą: $s = qr + t$, gdzie $0 \leqslant t < r$. Wówczas $\varepsilon = \alpha^s = \alpha^{qr+t} = (\alpha^r)^q * \alpha^t = \varepsilon^q * \alpha^t = \alpha^t$, co, wobec minimalności r, daje $t = 0$, czyli $r | s$. □

TWIERDZENIE 5.16 *Niech $\alpha, \beta \in \Gamma$ będą takimi elementami grupy* a b e l o w e j $(\Gamma, *)$, *że* $\mathrm{NWD}\,(\mathrm{rz}\,(\alpha), \mathrm{rz}\,(\beta)) = 1$. *Wówczas rząd iloczynu równy jest iloczynowi rzędów:*

$$\mathrm{rz}\,(\alpha * \beta) = \mathrm{rz}\,(\alpha) \cdot \mathrm{rz}\,(\beta). \tag{5.43}$$

D O W Ó D. Niech $\mathrm{rz}\,(\alpha) = a$, $\mathrm{rz}\,(\beta) = b$. Wówczas $(\alpha * \beta)^{ab} = (\alpha^a)^b * (\beta^b)^a = \varepsilon^b * \varepsilon^a = \varepsilon$. Stąd i z twierdzenia T5.15 wynika, że $\mathrm{rz}\,(\alpha * \beta)$ jest dzielnikiem iloczynu ab dwóch względnie pierwszych czynników. Możemy więc napisać

$$\mathrm{rz}\,(\alpha * \beta) = cd, \tag{5.44}$$

gdzie $c | a$ i $d | b$. (Opieramy się tu na prostym lemacie, na którym opieraliśmy się również rozwiązując ćwiczenie C4.2.) Piszemy więc $a = ck$, $b = dl$ dla pewnych liczb naturalnych k, l. Podnieśmy obie strony, wynikającej z (5.44), równości $\varepsilon = (\alpha * \beta)^{cd}$, do potęgi k. Dostaniemy

$$\varepsilon = \varepsilon^k = ((\alpha * \beta)^{cd})^k = (\alpha * \beta)^{ad} = (\alpha^a)^d * \beta^{ad} = \varepsilon^d * \beta^{ad} = \beta^{ad}.$$

Stąd, znów dzięki T5.15, $b | ad$. Założenie $a \perp b$ i ZTA (zob. T2.7) dają więc $b | d$. Ale $d | b$. Zatem $d = b$. Podobnie sprawdzamy, że $c = a$. To kończy dowód. □

U w a g a. W dowodzie twierdzenia T5.16 założenie abelowości (przemienności) grupy nie było wykorzystane *in extenso*. Jedynie ważnym jest to, że elementy α, β k o m u t u j ą, czyli że zachodzi równość $\alpha * \beta = \beta * \alpha$, zobacz poniższe ćwiczenie.

Ćwiczenie 5.37 Udowodnić, że jeżeli elementy α, β danej grupy komutują, to dla dowolnego wykładnika $k \in \mathbb{Z}$ zachodzi równość $(\alpha * \beta)^k = \alpha^k * \beta^k$.

Ćwiczenie 5.38 Niech $\alpha \in \Gamma$ będzie elementem grupy Γ. I niech $\mathrm{rz}\,(\alpha) = r$. Niech $k \in \mathbb{Z}$. Udowodnić, że $\mathrm{rz}\,(\alpha^k) = r$ wtedy i tylko wtedy, gdy $\mathrm{NWD}\,(k, r) = 1$. *Wskazówka.* Czy widzicie, że to jest wnioskiem z poniższego T5.17 ?

5.5.3 Rząd elementu w grupie $(\mathbb{Z}/m,\, +)$

W tym ustępie przyglądniemy się grupie $(\mathbb{Z}/m,\, +)$ klas reszt liczb całkowitych $(\mathrm{mod}\, m)$ z działaniem dodawania $(\mathrm{mod}\, m)$.

Mówimy więc teraz o przypadku a d d y t y w n y m, czyli o grupie $(\mathbb{Z}/m,\, +)$ klas reszt liczb całkowitych modulo m z dodawaniem modulo m określonym przez (5.32):

$$(\Gamma,\, *) = (\mathbb{Z}/m,\, +), \quad \varepsilon := \overline{0} = \mathbf{0} = 0\,(\mathrm{mod}\, m).$$

Łatwo wyrazić rząd elementu $k\,(\mathrm{mod}\, m)$ grupy $\mathbb{Z}/m$ (z dodawaniem modulo m) za pomocą najprostszych operacji teorioliczbowych.

P r z y k ł a d. Weźmy grupę $\mathbb{Z}/15$ z dodawaniem modulo 15. Wypiszmy ciąg (5.41) dla trzech wyborów elementu s:

$$\begin{aligned} s = \mathbf{6}: &\quad (\mathbf{6},\, \mathbf{12},\, \mathbf{3},\, \mathbf{9},\, \mathbf{0}),\, \mathbf{6},\, \mathbf{12},\, \mathbf{3},\, \mathbf{9},\, \ldots, \\ s = \mathbf{8}: &\quad (\mathbf{8},\, \mathbf{1},\, \mathbf{9},\, \mathbf{2},\, \mathbf{10},\, \mathbf{3},\, \mathbf{11},\, \mathbf{4},\, \mathbf{12},\, \mathbf{5},\, \mathbf{13},\, \mathbf{6},\, \mathbf{14},\, \mathbf{7},\, \mathbf{0}),\, \mathbf{8},\, \ldots, \\ s = \mathbf{10}: &\quad (\mathbf{10},\, \mathbf{5},\, \mathbf{0}),\, \mathbf{10},\, \mathbf{5},\, \ldots\,. \quad \lozenge \end{aligned}$$

Po takich i temu podobnych przykładach łatwo postawić hipotezę i następnie ją udowodnić:

Twierdzenie 5.17 *Rząd elementu* $k\,(\mathrm{mod}\, m) \in (\mathbb{Z}/m,\, +)$ *wynosi*

$$\mathrm{rz}\, k\,(\mathrm{mod}\, m) = \frac{m}{\mathrm{NWD}\,(k,\, m)}. \tag{5.45}$$

D O W Ó D. Wypisujmy ciąg (5.41) dla elementu $\alpha = k\,(\mathrm{mod}\, m)$ grupy $(\mathbb{Z}/m,\, +)$ aż do momentu pojawienia się elementu neutralnego, czyli $0\,(\mathrm{mod}\, m)$:

$$k\,(\mathrm{mod}\, m),\, 2k\,(\mathrm{mod}\, m),\, \ldots,\, rk\,(\mathrm{mod}\, m) = 0\,(\mathrm{mod}\, m).$$

Ostatnia równość jest równoważna z podzielnością

$$m|rk. \tag{5.46}$$

Szukamy więc najmniejszej dodatniej liczby całkowitej r, dla której zachodzi taka podzielność. Jeżeli oznaczymy $d = \mathrm{NWD}\,(k,\, m)$ i $k = dk',\, m = dm'$, to (5.46) daje podzielność $m'|rk'$. Względna pierwszość liczb m' i k' daje więc, na mocy ZTA, $m'|r$. Ponieważ $r = m'$ spełnia wymagania (bo $m'k = m'dk' = mk'$), więc $m' = \frac{m}{d}$ jest poszukiwanym rzędem. $\square$

5.5.4 Rząd elementu w grupie $((\mathbb{Z}/m)^*,\, \cdot)$

W tym ustępie wykorzystujemy rząd elementu w grupie $(\mathbb{Z}/m)^*$ elementów odwracalnych pierścienia $\mathbb{Z}/m$ klas reszt liczb całkowitych $(\mathrm{mod}\, m)$ z działaniem mnożenia $(\mathrm{mod}\, m)$.

Mówimy więc teraz o przypadku m u l t y p l i k a t y w n y m, czyli o grupie

$$(\Gamma,\, *) = ((\mathbb{Z}/m)^*,\, \cdot), \quad \varepsilon = \overline{1} = \mathbf{1} = 1\,(\mathrm{mod}\, m),$$

względnie pierwszych z m klas reszt liczb całkowitych $(\mathrm{mod}\, m)$. Działaniem jest tu oczywiście mnożenie modulo m, zobacz (5.33). Grupa $(\mathbb{Z}/m)^*$ jedności (elementów odwracalnych) pierścienia $\mathbb{Z}/m$ ma $\varphi(m)$ elementów, które utożsamiamy zazwyczaj z elementami zredukowanego układu reszt modulo m. Rząd elementu $a\,(\mathrm{mod}\, m)$ w grupie $(\mathbb{Z}/m)^*$ oznaczamy (dla odróżnienia od przypadku addytywnego) symbolem[4] $\mathrm{rz}_m(a)$.

Przypominamy, że $r = \mathrm{rz}_m(a)$, gdy (i tylko gdy) r jest najmniejszą liczbą naturalną, dla której $a^r \equiv 1\,(\mathrm{mod}\, m)$. Wiemy, że dla dowolnego $a \in \mathbb{Z}$, jeżeli $a \perp m$, to:

(R1) taka liczba r istnieje (zob. T5.14);

(R2) r jest dzielnikiem każdej liczby s, dla której $a^s \equiv 1\,(\mathrm{mod}\, m)$ (zob. T5.15);

(R3) $r|\varphi(m)$, w szczególności, $r|p-1$, gdy $m = p \in \mathbb{P}$ (zob. T5.5, w szczególności, MTF).

W przeciwieństwie do rozpatrzonego w poprzednim ustępie przypadku addytywnego, w przypadku multyplikatywnym nie istnieją żadne proste sposoby wyrażenia $\mathrm{rz}_m(a)$. W zasadzie dysponujemy tylko jedną metodą wyznaczania tej liczby: wypisujemy tak długo wyrazy ciągu typu (5.41), aż natrafimy na wyraz równy elementowi neutralnemu $1\,(\mathrm{mod}\, m)$.

Przykład. Weźmy $6\,(\mathrm{mod}\, 13) \in (\mathbb{Z}/13)^*$. Ciąg (5.41) dla tego elementu wygląda następująco: **6**, **10**, **8**, **9**, **2**, **12**, **7**, **3**, **5**, **4**, **11**, **1**, ... Widzimy stąd, że $\mathrm{rz}_{13}(6) = 12$. ◊

Pokażemy kilka typowych zadań, w których wykorzystuje się własności rzędu rz_m.

ZADANIE 5.12 Dowieść, że jeżeli $n > 1$ jest nieparzystą liczbą naturalną, to $n \nmid 3^n - 1$.

Rozwiązanie. Załóżmy (nie wprost), że $n|3^n - 1$ dla $n \equiv 1\,(\mathrm{mod}\, 2)$, $n > 1$. Niech p będzie najmniejszym dzielnikiem pierwszym liczby n, zobacz T2.14. Wówczas $p|3^n - 1$, czyli $3^n \equiv 1\,(\mathrm{mod}\, p)$. Stąd $p \neq 3$. Niech $r = \mathrm{rz}_p(3)$. Wtedy, na mocy (R2), $r|n$. Zauważmy, że $r \neq 1$ (gdy $r = 1$, to $3^1 \equiv 1\,(\mathrm{mod}\, p)$, co jest możliwe tylko dla $p = 2$, ale $2 \nmid n$). Więc $p \leqslant r$, bo p jest najmniejszym, różnym od 1, dzielnikiem n. Jednocześnie, na mocy (R3), $r|p-1$. Stąd $r \leqslant p - 1 < p$. Dostajemy niedorzeczność: $r < p \leqslant r$. ◊

ZADANIE 5.13 Dowieść, że jeżeli $n \geqslant 2$ jest liczbą naturalną i $n|11^n - 2^n$, to $3|n$.

Rozwiązanie. Załóżmy, że dla pewnego $n \geqslant 2$ zachodzi $n|11^n - 2^n$. Niech p będzie najmniejszą liczbą pierwszą dzielącą n. Wówczas $11^n \equiv 2^n\,(\mathrm{mod}\, p)$. Oraz $p \neq 2$ (dlaczego?). Niech b będzie odwrotnością 2 modulo p. Mamy więc $(11b)^n \equiv 1\,(\mathrm{mod}\, p)$. Oznaczmy $r = \mathrm{rz}_p(11b)$. Wtedy, na mocy (R2), $r|n$. Stąd $r = 1$ albo $r \geqslant p$, bo p jest najmniejszym, różnym od 1, dzielnikiem n. W przypadku $r = 1$ mamy $11b \equiv 1\,(\mathrm{mod}\, p)$, skąd $11 \equiv 2\,(\mathrm{mod}\, p)$, więc $p|9$, czyli $p = 3$. W przypadku zaś $r \geqslant p$ dostajemy sprzeczność, bo $r|p-1$. ◊

Przed rozwiązaniem następnego zadania udowodnimy użyteczny lemat:

LEMAT 5.5 *Dany jest moduł $m > 2$ i względnie pierwsza z nim liczba całkowita a. Załóżmy, że $s \geqslant 1$ jest najmniejszym takim wykładnikiem, że*

$$a^s \equiv -1\,(\mathrm{mod}\, m). \tag{5.47}$$

Wówczas $\mathrm{rz}_m(a) = 2s$. Ponadto: $a^t \equiv -1\,(\mathrm{mod}\, m) \iff t = (2k-1)s$, $k \in \mathbb{N}$.

[4] "Uczciwe" matematycznie oznaczenia $\mathrm{rz}_{(\mathbb{Z}/m)^*}(a)$, czy, proponowane w poprzednich wydaniach skryptu, $\mathrm{rz}\, a\,(\mathrm{mod}^* m)$, są zbyt "ciężkie". Uwaga. W literaturze olimpijskiej używa się symbolu $\mathrm{ord}_m(a)$. Nie zdecydowaliśmy się na jego wprowadzenie, ponieważ w literaturze matematycznej, zobacz na przykład **[2]**, symbol $\mathrm{ord}_p(a)$ oznacza wykładnik p-adyczny liczby $a \in \mathbb{Z}$, czyli nasze $v_p(a)$.

D O W Ó D. Niech $\alpha = a \,(\mathrm{mod}\, m) \in \mathbb{Z}/m$. Kongruencja (5.47) pokazuje, że $\alpha \in (\mathbb{Z}/m)^*$ (odwrotnością α jest warstwa $-\alpha^{s-1}$). Niech $r = \mathrm{rz}_m(a) = \mathrm{rz}\,(\alpha)$. Rozważmy ciąg

$$\alpha,\ \alpha^2,\ \ldots,\ \alpha^r.$$

Z dowodu T5.14 wiemy, że w tym ciągu występują wszystkie potęgi α^t elementu $\alpha \in (\mathbb{Z}/m)^*$. W szczególności element $(-1)\,(\mathrm{mod}\, m) = \alpha^s$. To, wobec minimalności s, oznacza, że $s \leqslant r$. Ponadto $s \neq r$. Gdyby bowiem $r = s$, to byłoby $-1 \equiv a^s \equiv a^r \equiv 1 \,(\mathrm{mod}\, m)$, czyli $m|2$, co, wobec założenia $m > 2$, jest niemożliwe. Zatem $s < r$.

Podnosząc kongruencję (5.47) obustronnie do kwadratu, dostaniemy $a^{2s} \equiv 1 \,(\mathrm{mod}\, m)$, skąd, na mocy (R2), $r|2s$. To, wobec nierówności $s < r$, jest możliwe tylko, gdy $r = 2s$.

Załóżmy teraz, że $a^t \equiv -1 \,(\mathrm{mod}\, m)$. Podnosząc do kwadratu mamy $a^{2t} \equiv 1 \,(\mathrm{mod}\, m)$, skąd $r|2t$. Czyli $2s|2t$, więc $s|t$. Sprawdzenie, że $t/s \equiv 1 \,(\mathrm{mod}\, 2)$, pozostawiamy Czytelnikowi. □

U w a g a 1. Wykładnik s spełniający (5.47) może n i e i s t n i e ć. Przykładów jest na to mnóstwo: $a = 2$, $m = 7$ lub $a = 3$, $m = 3^{2011} - 1$ itp. To oznacza, że w ciągu $[a]$, $[a]^2$, $[a]^3$, ... kolejnych potęg warstwy $a \,(\mathrm{mod}\, m)$, może nie występować warstwa $(-1)\,(\mathrm{mod}\, m)$. Lemat mówi, że jeżeli występuje, to "robi" to dokładnie w połowie "dystansu" między $[a]$ a $[a]^r$ (w szczególności r musi być parzyste) i potem na co r-tym miejscu.

ZADANIE 5.14 Udowodnić, że każda liczba Nováka jest podzielna przez 3.

R o z w i ą z a n i e. Załóżmy, że $n|2^n + 1$. Niech p będzie n a j m n i e j s z y m dzielnikiem pierwszym liczby n. Wtedy $2^n + 1 \equiv 0 \,(\mathrm{mod}\, p)$. Stąd $2^n \equiv -1 \,(\mathrm{mod}\, p)$. Niech s będzie najmniejszym wykładnikiem, dla którego $2^s \equiv -1 \,(\mathrm{mod}\, p)$. Wówczas na mocy lematu L5.5, $n = (2k-1)s$ dla pewnego $k \in \mathbb{N}$ i $2s = r$, gdzie $r := \mathrm{rz}_p(2)$. Ponieważ $r \leqslant p - 1 < p$, więc $s < 2s = r < p$. Stąd wynika, że $s = 1$; w przeciwnym razie s byłoby mniejszym niż p właściwym dzielnikiem n. Przeto $2^1 \equiv -1 \,(\mathrm{mod}\, p)$. Skąd: $p = 3$. ◊

ZADANIE 5.15 Dowieść, że jeżeli liczba pierwsza p dzieli liczbę Fermat'a $F_n = 2^{2^n} + 1$, to $p = 2^{n+1}a + 1$ dla pewnej liczby naturalnej a.

R o z w i ą z a n i e. Niech $r = \mathrm{rz}_p(2)$. Ponieważ $p|F_n$, więc $2^{2^n} \equiv -1 \,(\mathrm{mod}\, p)$. Z lematu L5.5 wiemy więc, że $2^n = (2k-1)s$, gdzie s oznacza najmniejszy taki dodatni wykładnik, że $2^s \equiv -1 \,(\mathrm{mod}\, p)$. Stąd $k = 1$ i, wobec tego, $s = 2^n$. Zatem $2^{n+1} = 2s = r$. Jednocześnie, na mocy (R3), $r|p-1$. Więc $p - 1 = ar$ dla pewnego naturalnego a. ◊

Ćwiczenie 5.39 Niech $a \in \mathbb{N}_{>1}$ i $q \in \mathbb{P}_{>2}$. Udowodnić, że każdy nieparzysty dzielnik pierwszy liczby $a^q - 1$ jest dzielnikiem liczby $a - 1$ lub jest postaci $2qx + 1$, gdzie $x \in \mathbb{N}$.

Ćwiczenie 5.40 Udowodnić, że jeżeli $n \in \mathbb{N}_{\geqslant 2}$ i $n|5^n + 8^n$, to $13|n$.

Ćwiczenie 5.41 Dowieść, że jeżeli $n, a \in \mathbb{N}$ i $n < a$, to $n|\varphi(a^n - 1)$.

Ćwiczenie 5.42 Załóżmy, że $2^n \equiv 1 \,(\mathrm{mod}\, p)$ i $2^n \not\equiv 1 \,(\mathrm{mod}\, p^2)$ dla pewnej liczby pierwszej $p > 2$ i pewnego $n \in \mathbb{N}$. Niech $r = \mathrm{rz}_p(2)$. Udowodnić, że $2^r \not\equiv 1 \,(\mathrm{mod}\, p^2)$.

Ćwiczenie 5.43 Wyznaczyć wszystkie liczby pierwsze p, q, dla których $pq|2^p + 2^q$.

Ćwiczenie 5.44 Jeżeli $p \in \mathbb{P}$, to liczba $p^p - 1$ ma dzielnik pierwszy postaci $px + 1$.

5.5.5 O liczbach pierwszych w ciągach arytmetycznych

W tym ustępie wykorzystamy własności funkcji rzędu $\mathrm{rz}_p : (\mathbb{Z}/p)^* \longrightarrow \mathbb{N}$ w dowodzie jednego przypadku szczególnego słynnego ***Twierdzenia Dirichlet'a o liczbach pierwszych w postępach arytmetycznych***:

TWIERDZENIE 5.18 (**Dirichlet – 1837**) *Jeżeli liczby naturalne r i a są względnie pierwsze, to nieskończony ciąg arytmetyczny $(rx+a)_{x\in\mathbb{N}}$ zawiera nieskończenie wiele wyrazów będących liczbami pierwszymi.* □

Dowód twierdzenia Dirichlet'a jest dla nas za trudny.[5] Dla niektórych konkretnych wartości r i a rzecz jest bardziej elementarna: już Euklides pokazał prawdziwość twierdzenia T5.18 dla $r = 2$ i $a = 1$, ogólniej, dla $r = 2$ i dowolnego(!) $a \equiv 1 \,(\mathrm{mod}\, 2)$. Niewielkie modyfikacje oryginalnego rozumowania Euklidesa z ustępu 2.3.1 pozwalają udowodnić niektóre inne przypadki szczególne[6] twierdzenia Dirichlet'a.

P r z y k ł a d 1. *Liczb pierwszych postaci $3x+2$, $x \in \mathbb{N}$, jest nieskończenie wiele.* Rzeczywiście, załóżmy nie wprost, że takich liczb jest tylko skończenie wiele i że $p_1 = 5$, $p_2 = 11$, $\ldots$, p_r są wszystkimi takimi liczbami. Niech $N = 3p_1p_2 \cdot \ldots \cdot p_r + 2$. Liczba N jest postaci $3x + 2$, ale, jak łatwo widzieć, nie dzieli się przez żadną z liczb p_1, p_2, $\ldots$, p_r. Więc w jej rozkładzie na czynniki pierwsze występują tylko czynniki postaci $3x + 1$ (bo ani czynnik 2 ani czynnik 3 nie występuje!). Z drugiej strony, łatwo sprawdzić, że iloczyn liczb postaci $3x + 1$ jest liczbą tej samej postaci. Liczba N, będąc postaci $3x + 2$, musiałaby być jednocześnie liczbą postaci $3x + 1$. Ta sprzeczność kończy dowód. Q.e.d. ◊

P r z y k ł a d 2. *Liczb pierwszych postaci $4x+3$, $x \in \mathbb{N}$, jest nieskończenie wiele.* Rzeczywiście, załóżmy nie wprost, że takich liczb jest tylko skończenie wiele i że $p_1 = 7$, $p_2 = 11$, $\ldots$, p_r są wszystkimi takimi liczbami. Rozważmy liczbę $N = 4p_1p_2 \cdot \ldots \cdot p_r + 3$. Liczba N jest postaci $4x + 3$, ale nie dzieli się przez żadną z wypisanych liczb pierwszych postaci $4x + 3$, więc w jej rozkładzie na czynniki pierwsze występują tylko czynniki postaci $4x + 1$ (bo ani czynnik 2 ani czynnik 3 nie występuje!). Z drugiej strony, łatwo sprawdzić, że iloczyn liczb postaci $4x + 1$ jest liczbą tej samej postaci. Liczba N, będąc postaci $4x + 3$, musiałaby być jednocześnie liczbą postaci $4x + 1$. Uzyskana sprzeczność kończy dowód. Q.e.d. ◊

Ćwiczenie 5.45 Udowodnić, że liczb pierwszych postaci $6x + 5$ jest nieskończenie wiele.

Ćwiczenie 5.46 Niech q będzie nieparzystą liczbą pierwszą. Udowodnić, że istnieje nieskończenie wiele liczb pierwszych postaci $2qx + 1$. *Wskazówka.* (1) Liczby takiej postaci istnieją: weź dowolny dzielnik pierwszy liczby Mersenne'a M_q, zob. C5.39; (2) Jeżeli $p_1, \ldots, p_r$ są liczbami pierwszymi postaci $2qx + 1$, to rozważ $a = p_1 \cdot \ldots \cdot p_r$ w C5.39.

Chcemy teraz dowieść jeszcze więcej, mianowicie prawdziwości twierdzenia Dirichlet'a w przypadku $a = 1$ (z dowolnym r). Pomysł dowodu jest taki: szukamy takiej liczby pierwszej p i takiej liczby całkowitej c, że $\mathrm{rz}_p(c) = r$ (wówczas $r|p-1$, czyli p jest postaci $rx + 1$). Przedtem nauczymy się inaczej wyznaczać $\mathrm{rz}_p(c)$. Mówi o tym ważny lemat L5.6.

[5] Powiemy tylko, że Dirichlet, za pomocą genialnego (łączącego elementy algebry z elementami analizy matematycznej) rozumowania potrafił udowodnić rozbieżność szeregu $\sum_{p\equiv a \,(\mathrm{mod}\, r)} \frac{1}{p}$. Zob. **[2]**, **[7]**.

[6] Kilka elementarnych przypadków twierdzenia Dirichlet'a (nie objętych przez T5.19) pokażemy w 5.7.6.

Przypomnijmy, że $\Phi_n(X)$ oznacza n-ty wielomian cyklotomiczny, zobacz (3.44). O wielomianach $\Phi_n(X)$ wiemy, że są one unormowane, mają współczynniki całkowite, a ich wyrazy wolne są równe ± 1, zobacz C4.22 i C4.23. Ponadto, w C3.51 i C4.21 pokazujemy dwa wzajemnie möbiusowsko odwrotne rozkłady

$$(1)\quad X^n - 1 = \prod_{k|n} \Phi_k(X), \qquad (2)\quad \Phi_n(X) = \prod_{k|n} (X^k - 1)^{\mu(n/k)}. \tag{5.48}$$

W dowodzie L5.6 wykorzystamy tezę zadania:

ZADANIE 5.16 Niech $p \in \mathbb{P}$ i $n = p^\alpha r$, gdzie $\alpha = v_p(n) \geqslant 1$. Dowieść, że

$$\Phi_n(X) = \frac{\Phi_r(X^{p^\alpha})}{\Phi_r(X^{p^{\alpha-1}})}. \tag{5.49}$$

Rozwiązanie. Pokażemy to w przypadku $\alpha = 1$ (ogólny przypadek rozpatruje się analogicznie). Korzystamy z (5.48(2)). Zbiór $D_+(n)$ (dodatnich) dzielników n jest sumą rozłączną $D_+(r) \sqcup pD_+(r)$ dzielników $d|r$ i dzielników postaci pd, gdzie $d|r$. Mamy więc

$$\Phi_n(X) = \prod_{d|r} (X^d - 1)^{\mu(n/d)} \cdot \prod_{pd|n} (X^{pd} - 1)^{\mu(n/pd)} = \prod_{d|r} (X^d - 1)^{\mu(p)\mu(r/d)} \cdot \prod_{d|r} ((X^p)^d - 1)^{\mu(r/d)}.$$

Stąd, ponieważ $\mu(p) = -1$, mamy równość (5.49) (dla $\alpha = 1$). $\Diamond$

LEMAT 5.6 *Niech $p \in \mathbb{P}$. Wówczas, jeżeli dla pewnego $n \in \mathbb{N}$ i pewnego $c \in \mathbb{Z}$ zachodzi kongruencja $\Phi_n(c) \equiv 0 \pmod p$, to $p \nmid c$ i zachodzi równość $\mathrm{rz}_p(c) = np^{-v_p(n)}$.*

D O W Ó D. Gdyby $p|c$, czyli $c \equiv 0 \pmod p$, to, zob. T5.2, byłoby $\Phi_n(c) \equiv \Phi_n(0) \pmod p$, więc $0 \equiv \pm 1 \pmod p$, zobacz C4.23. Otrzymany nonsens dowodzi, że $p \nmid c$.

Zatem $\mathrm{rz}_p(c)$ istnieje. Oznaczmy $s := \mathrm{rz}_p(c)$. Oznaczmy też $n = p^\alpha r$, gdzie $\alpha = v_p(n)$. Mamy wykazać, że $s = r$. Zaczniemy od przypadku, gdy $\alpha = 0$. Najpierw dowodzimy, że $s|r$. Kładąc $n = r$ i $X = c$ w (5.48(1)), dostajemy równość $c^r - 1 = \prod_{k|r} \Phi_k(c)$. Stąd $\Phi_r(c)|c^r - 1$, więc $p|c^r - 1$, czyli $c^r \equiv 1 \pmod p$. Stąd, na mocy T5.15, $s|r$. Załóżmy więc, nie wprost, że $s < r$. Wówczas, znowu dzięki rozkładowi typu (5.48(1)),

$$\prod_{l|s} \Phi_l(c) = c^s - 1 \equiv 0 \pmod p.$$

Ponieważ p jest liczbą pierwszą, więc widzimy stąd, że $\Phi_l(c) \equiv 0 \pmod p$ dla pewnego $l|s$. Ta liczba l jest właściwym dzielnikiem r (bo $l|s|r$ i $s < r$). Zatem, w iloczynie $\prod_{k|r} \Phi_k(c)$ znajdują się dwa (różne!) czynniki: $\Phi_r(c)$ i $\Phi_l(c)$, oba podzielne przez p. Przeto

$$c^r - 1 = \prod_{k|r} \Phi_k(c) \equiv 0 \pmod{p^2}. \tag{5.50}$$

Rozważmy teraz liczbę $b = c + p$. Ponieważ $b \equiv c \pmod p$, więc $\Phi_r(b) \equiv \Phi_r(c) \pmod p$ oraz $\Phi_l(b) \equiv \Phi_l(c) \pmod p$, zobacz T5.2. Zatem również w iloczynie $\prod_{k|r} \Phi_k(b)$ występują dwa czynniki podzielne przez p. Wobec tego

$$b^r - 1 = \prod_{k|r} \Phi_k(b) \equiv 0 \pmod{p^2}. \tag{5.51}$$

Odejmując stronami (5.50) i (5.51) widzimy, że $p^2|c^r - b^r$, czyli $v_p(c^r - b^r) \geqslant 2$. Jednocześnie $v_p(c^r - b^r) = v_p(c-b) = v_p(-p) = 1$, na mocy Z2.8 (którego założenia $v_p(cb) = 0$ i $v_p(c-b) \geqslant 1$ są oczywiście spełnione). Znaleziona sprzeczność kończy dowód równości $\mathrm{rz}_p(c) = np^{-v_p(n)}$ w przypadku, gdy $v_p(n) = 0$.

Gdy $v_p(n) = \alpha \geqslant 1$ (i $n = rp^\alpha$), wystarczy, na mocy już udowodnionego, uzasadnić, że $\Phi_r(c) \equiv 0 \,(\mathrm{mod}\, p)$. Otóż, dzięki (5.49) mamy równość $\Phi_n(c)\Phi_r(c^{p^{\alpha-1}}) = \Phi_r(c^{p^\alpha})$. Założenie $\Phi_n(c) \equiv 0 \,(\mathrm{mod}\, p)$ daje więc $\Phi_r(c^{p^\alpha}) \equiv 0 \,(\mathrm{mod}\, p)$. MTF (w wersji (5.12)) daje kongruencje $c \equiv c^p \equiv \cdots \equiv c^{p^\alpha} \,(\mathrm{mod}\, p)$. Stąd (zob. T5.2) $\Phi_r(c) \equiv \Phi_r(c^{p^\alpha}) \equiv 0 \,(\mathrm{mod}\, p)$. □

Możemy teraz udowodnić zapowiedziany przypadek szczególny twierdzenia Dirichlet'*a*:

TWIERDZENIE 5.19 *Niech r będzie ustaloną liczbą naturalną. Wówczas istnieje nieskończenie wiele liczb pierwszych postaci $rx + 1$, gdzie $x \in \mathbb{N}$.*

D O W Ó D. Załóżmy, że liczby $p_1, p_2, \ldots, p_k$ są liczbami pierwszymi postaci $rx + 1$. Dopuszczamy możliwość $k = 0$. Rozważmy liczbę naturalną $a = rp_1p_2 \cdot \ldots \cdot p_k$. Gdy $k = 0$ kładziemy $a = r$. Wybierzmy taką liczbę naturalną b, że liczba $N := |\Phi_r(ab)|$ jest liczbą złożoną (to jest możliwe na mocy Z5.3) i połóżmy $c = ab$. Niech p będzie dowolnym dzielnikiem pierwszym liczby N, czyli niech $\Phi_r(c) \equiv 0 \,(\mathrm{mod}\, p)$. Na mocy L5.6 mamy zatem $\mathrm{rz}_p(c) = rp^{-v_p(r)} = r$, bo $p \nmid c$ więc też $p \nmid r$. Stąd, na mocy T5.15 i MTF, $r|p-1$, czyli $p - 1 = rx$. Znaleźliśmy zatem liczbę pierwszą $p = rx + 1$. Ponadto, ponieważ $p \nmid ab$, więc $p \neq p_i$ dla $i = 1, \ldots, k$. Mamy przeto n o w ą liczbę pierwszą postaci $rx + 1$! □

ZADANIE 5.17 Liczbę naturalną bezkwadratową nazwiemy *k-krotną*, gdy jest iloczynem k (oczywiście różnych) liczb pierwszych. Udowodnić, że dla dowolnej ustalonej liczby $r \in \mathbb{N}$ istnieje nieskończenie wiele liczb *k-krotnych* postaci $rx + 1$.

R o z w i ą z a n i e. Rozumujemy przez indukcję względem k. Baza indukcji jest po prostu naszym T5.19. Dla wykonania kroku indukcyjnego załóżmy, że $ry_0 + 1 = p_1p_2 \cdot \ldots \cdot p_k$ dla pewnego $y_0 \in \mathbb{N}$ (gdzie p_i są różnymi liczbami pierwszymi). Wybierzmy taki ciąg nieskończony $y_1 < y_2 < \ldots$ liczb naturalnych, że liczby $q_i := ry_i + 1$ są liczbami pierwszymi większymi niż $\max\{p_1, \ldots, p_k\}$ (jest to możliwe dzięki T5.20). Mając to, wybieramy liczby naturalne $x_i = p_1 \cdot \ldots \cdot p_k y_i + y_0$ dla $i \in \mathbb{N}$ i liczymy: $rx_i + 1 = r(p_1 \cdot \ldots \cdot p_k y_i + y_0) + 1 = p_1 \cdot \ldots \cdot p_k q_i$. W ten sposób widzimy nieskończony, rosnący ciąg liczb $(k+1)$-*krotnych* postaci $rx + 1$. ◊

5.5.6 Twierdzenie Zsigmondy'*ego*

Chcemy teraz udowodnić ciekawe twierdzenie o dzielnikach wyrazów ciągów $(a^n \pm b^n)$.

Zaczniemy od "ujednorodnienia" wielomianów cyklotomicznych. **Jednorodne wielomiany cyklotomiczne** pozwalają otrzymywać systemowe[7] rozkłady liczb postaci $a^n - b^n$ uogólniające rozkłady postaci (5.48(1)) dla liczb $a^n - 1$. Pisząc mianowicie $a^n - b^n = b^n[(a/b)^n - 1]$ i rozkładając czynnik $(a/b)^n - 1$ zgodnie z równością (5.48(1)), dostajemy

$$a^n - b^n = b^n \cdot \prod_{k|n} \Phi_k(a/b).$$

[7] Ponieważ $a^n - b^n = f(a, b)$, gdzie $f(X, Y) = X^n - Y^n \in \mathbb{Z}[X, Y]$, więc każdy rozkład wielomianu $f(X, Y)$ na czynniki w $\mathbb{Z}[X, Y]$ daje rozkład liczby $a^n - b^n$ na iloczyn w $\mathbb{Z}$.

Oznaczmy $\Phi_k(a,\,b) := b^{\varphi(k)}\Phi_k(a/b)$. To pozwala napisać jednorodne wersje (5.48) i (5.49):

$$(1)\quad X^n - Y^n = \prod_{k|n} \Phi_k(X,\,Y), \qquad (2)\quad \Phi_n(X,\,Y) = \prod_{k|n} (X^k - Y^k)^{\mu(n/k)}, \tag{5.52}$$

$$\Phi_n(X,\,Y) = \frac{\Phi_r(X^{p^\alpha},\,Y^{p^\alpha})}{\Phi_r(X^{p^{\alpha-1}},\,Y^{p^{\alpha-1}})}. \tag{5.53}$$

Ćwiczenie 5.47 Udowodnić, że jeżeli $p|m$, to zachodzi równość

$$\Phi_{pm}(X,\,Y) = \Phi_m(X^p,\,Y^p). \tag{5.54}$$

W dalszym ciągu ustalamy $a,\,b \in \mathbb{N}$ spełniające warunki $a > b \geqslant 1$, $a \perp b$. Badamy ciąg (u_n) dany przez $u_n = a^n - b^n$. Liczbę p i e r w s z ą q nazywamy **dzielnikiem pierwotnym** wyrazu u_n tego ciągu, gdy $q|u_n$, ale $q \nmid u_k$ dla wszystkich $1 \leqslant k < n$. Przez $\mathcal{D}_n = \mathcal{D}_n(a,\,b)$ oznaczymy zbiór dzielników (pierwszych) pierwotnych wyrazu u_n.

P r z y k ł a d 1. Rozważmy $(M_n) = (2^n - 1)$. Widzimy, że $\mathcal{D}_1 = \varnothing$, $\mathcal{D}_2 = \{3\}$, $\mathcal{D}_3 = \{7\}$, $\mathcal{D}_4 = \{5\}$, $\mathcal{D}_5 = \{31\}$, $\mathcal{D}_6 = \varnothing$. Wkrótce udowodnimy, że $\mathcal{D}_n(2,\,1) \neq \varnothing$ dla $n \neq 1,\,6$. $\Diamond$

Udowodnimy teraz twierdzenie Zsigmondy'*ego*:

TWIERDZENIE 5.20 (***Zsigmondy* – 1892**) *Zbiór $\mathcal{D}_n = \mathcal{D}_n(a,\,b)$, dla $n \geqslant 2$, jest n i e p u s t y w każdym, poza wymienionymi, przypadku. Wyjątkami są*:

(W1) $\mathcal{D}_6(2,\,1)$;

(W2) $\mathcal{D}_2(a,\,b)$ *dla dowolnych a, b, dla których $a + b = 2^s$.*

D O W Ó D. Będziemy pisać w skrócie $\Phi_k = \Phi_k(a,\,b)$. Przypomnijmy też (zobacz rozwiązanie Z2.C4) oznaczenie $\mathrm{Supp}(c) := \{p \in \mathbb{P} : p|c\}$. Zauważmy najpierw, że równość (5.52(1)) daje równość $u_n = \prod_{k|n} \Phi_k$. Przeto

$$\mathrm{Supp}(u_n) = \bigcup_{k|n} \mathrm{Supp}(\Phi_k).$$

W pierwszym kroku sprawdzamy, że zbiór $\mathcal{D}_n$ jest podzbiorem składnika $\mathrm{Supp}(\Phi_n)$ powyższej sumy i, co więcej, jest rozłączny z pozostałymi składnikami tej sumy:

K r o k 1. $\mathcal{D}_n \subseteq \mathrm{Supp}(\Phi_n)$ *oraz* $\mathcal{D}_n \cap \mathrm{Supp}(\Phi_k) = \varnothing$, *dla* $k|n$ *i* $k < n$.

◄ Założenie $q|u_n$ i równość $u_n = \prod_{k|n} \Phi_k$ dają podzielność $q|\Phi_k$ dla pewnego $k|n$. Gdyby $k < n$, to, ponieważ $u_k = \prod_{l|k} \Phi_l$, mielibyśmy $q|u_k$, co jest sprzeczne z pierwotnością q. ►

Zbiór $\mathrm{Supp}(\Phi_n)$ dzielników pierwszych liczby Φ_n jest więc sumą rozłączną $\mathcal{D}_n \sqcup \mathcal{E}_n$ zbioru $\mathcal{D}_n$ dzielników pierwszych pierwotnych i zbioru $\mathcal{E}_n$ dzielników pierwszych *niepierwotnych*. Dążymy do uzasadnienia, że zbiór $\mathcal{D}_n$ jest n i e p u s t y (poza wyjątkowymi przypadkami). Najpierw pokażemy, że zbiór $\mathcal{E}_n$ jest "mały" (pusty lub jednoelementowy!).

K r o k 2. *Jeżeli $p \in \mathcal{E}_n$, to $p|n$.*

◄ Niepierwotny dzielnik pierwszy wyrazu u_n jest dzielnikiem wyrazu u_d dla pewnego właściwego (tzn. $1 \leqslant d < n$) dzielnika $d|n$. Rzeczywiście, jeżeli $p|u_n$ i $p|u_m$ dla pewnego $1 \leqslant m < n$, to $p|\mathrm{NWD}\,(u_m,\,u_n)$, czyli, zobacz Z2.B9, $p|u_{\mathrm{NWD}\,(m,\,n)}$. Niech więc $p|u_n$ i $p|u_d$

dla pewnego właściwego dzielnika $d|n$. Zakładając nie wprost, że $p \nmid n$ mamy, tym bardziej, $p \nmid \frac{n}{d}$, skąd, na mocy Z2.8 (przy $x = a^d$, $y = b^d$ i $k = n/d$), $v_p(u_n) = v_p(u_d)$. Więc $p \nmid \frac{u_n}{u_d}$. Ale, zob. (5.52(1)), $u_n = \prod_{k|n} \Phi_k$ i $u_d = \prod_{l|d} \Phi_l$, skąd $\Phi_n | \frac{u_n}{u_d}$. Sprzeczność, bo $p|\Phi_n$. ►

K r o k 3. *Jeżeli* $p \in \mathcal{E}_n$ *i* $n = p^\alpha r$, *gdzie* $\alpha = v_p(n)$, *to* $p \nmid b$ *i* $\mathrm{rz}_p(ab^{-1}) = r$.

◄ Na mocy tezy Kroku 2, $p|n$. Zatem $n = p^\alpha r$, gdzie $\alpha := v_p(n) \geqslant 1$. Dzięki (5.53) mamy $\Phi_n \cdot \Phi_r(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}) = \Phi_r(a^{p^\alpha}, b^{p^\alpha})$, skąd $p|\Phi_r(a^{p^\alpha}, b^{p^\alpha})$. MTF, podobnie jak w dowodzie L5.6, daje $\Phi_r(a^{p^\alpha}, b^{p^\alpha}) \equiv \Phi_r(a, b) \,(\mathrm{mod}\, p)$, więc $p|\Phi_r(a, b)$. Zatem $p|u_r$, (bo $\Phi_r|u_r$, zob. (5.52(1))), czyli $p|a^r - b^r$, skąd wnioskujemy, że $p \nmid b$ (gdyby $p|b$, to byłoby kolejno $p|b^r$, $p|(a^r - b^r + b^r)$, $p|a^r$, $p|a$, co jest sprzeczne z założeniem $a \perp b$). Równie łatwo wywnioskować, mnożąc przez $(b^{-1})^k \,(\mathrm{mod}\, p)$, że jeżeli $\sum c_s a^s b^{k-s} \equiv 0 \,(\mathrm{mod}\, p)$, to $\sum c_s (ab^{-1})^s \equiv 0 \,(\mathrm{mod}\, p)$ (przy dowolnych $c_j \in \mathbb{Z}$). Stąd $\Phi_r(ab^{-1}) \equiv 0 \,(\mathrm{mod}\, p)$. Zatem, zob. L5.6, $\mathrm{rz}_p(ab^{-1}) = r$. ►

K r o k 4. $\mathrm{card}(\mathcal{E}_n) \leqslant 1$.

◄ Załóżmy, że $\mathcal{E}_n \neq \varnothing$ i że p jest najmniejszym elementem zbioru $\mathcal{E}_n$. Wówczas $n = p^\alpha r$ i $r = \mathrm{rz}_p(ab^{-1}) \leqslant p - 1$, zob. Krok 3, 5.5.4 (R3) i C2.2. Gdyby $p' \in \mathcal{E}_n$ była inną liczbą pierwszą, to zachodziłaby podzielność $p'|p^\alpha r$, skąd $p'|r$. Czyli $p' \leqslant r < p$. Sprzeczność. ►

Widzimy, że zbiór $\mathcal{E}_n$ dzielników pierwszych niepierwotnych jest "mały". Wykażemy teraz, że ma miejsce fakt jeszcze bardziej sprzyjający niepustości zbioru $\mathcal{D}_n$:

K r o k 5. *Jeżeli* $p > 2$ *i* $p \in \mathcal{E}_n$, *to* $v_p(\Phi_n) = 1$.

◄ Korzystając z (5.52(2)) mamy równość $\Phi_n = \prod_{k|n} u_k^{\mu(n/k)}$. Stąd, na mocy C2.47.1,

$$v_p(\Phi_n) = \sum_{k|n} \mu(n/k) v_p(u_k) \tag{5.55}$$

dla dowolnej liczby pierwszej p. Pokażemy, że, gdy $p \in \mathcal{E}_n$, w tej sumie występują tylko dwa niezerowe wyrazy. Zobaczmy najpierw, dla jakich $k|n$ zachodzi nierówność $v_p(u_k) > 0$, równoważnie, dla jakich $k|n$ zachodzi podzielność $p|u_k$, równoważnie, dla jakich $k|n$ zachodzi $(ab^{-1})^k \equiv 1 \,(\mathrm{mod}\, p)$. Wiemy, zobacz 5.5.4 (R2), że to zachodzi dla wszystkich $k|n$, dla których $r|k$, gdzie $r = \mathrm{rz}_p(ab^{-1})$. Z Kroku 3 wiemy, że $\mathrm{rz}_p(ab^{-1}) = np^{-\alpha}$, gdzie $\alpha = v_p(n) \geqslant 1$. Zatem suma (5.55) redukuje się do sumy $\sum_{s=0}^{\alpha} \mu(n/p^s r) v_p(u_{p^s r}) = \sum_{s=0}^{\alpha} \mu(p^{\alpha-s}) v_p(u_{np^{s-\alpha}})$. Czyli do różnicy $v_p(u_n) - v_p(u_{n/p})$, bo $\mu(p^{\alpha-s}) = 0$ dla $\alpha - s \geqslant 2$. Mamy więc sprawdzić, że $v_p(u_n) - v_p(u_{n/p}) = 1$. Równość ta jest wnioskiem z Z2.9. Czytelnik zechce samodzielnie uzasadnić, że liczby $x = a^{n/p}$, $y = b^{n/p}$ spełniają założenia tego zadania! ►

K r o k 6. *Jeżeli* $x > y > 0$, *to* $(x - y)^{\varphi(m)} \leqslant |\Phi_m(x, y)| \leqslant (x + y)^{\varphi(m)}$.

◄ Oznaczmy $\xi = \frac{x}{y}$. Okrąg jednostkowy $\{z \in \mathbb{C} : |z| = 1\}$, na którym leżą wszystkie pierwiastki z jedynki, zawarty jest w pierścieniu kołowym

$$\mathcal{P}(R_1, R_2) := \{z \in \mathbb{C} : R_1 \leqslant |z| \leqslant R_2\},$$

gdzie $R_1 = \xi - 1$, $R_2 = \xi + 1$. Zatem $\xi - 1 \leqslant |\xi - \omega^k| \leqslant \xi + 1$ dla każdego k. Mnożąc te nierówności dla $1 \leqslant k \leqslant m$, $k \perp m$, dostajemy $(\xi - 1)^{\varphi(m)} \leqslant \Phi_m(\xi) \leqslant (\xi + 1)^{\varphi(m)}$. Wystarczy teraz pomnożyć przez $y^{\varphi(m)}$. U w a g a. Należy zauważyć, że nierówność lewa jest nierównością ścisłą dla wszystkich $m \geqslant 2$, a nierówność prawa jest ścisła dla wszystkich $m \neq 2$. ►

K r o k 7. *Jeżeli* $\mathcal{E}_n = \varnothing$, *to* $\mathcal{D}_n \neq \varnothing$.

◄ Równości $\mathcal{E}_n = \mathcal{D}_n = \varnothing$ mogą zajść jednocześnie tylko w przypadku, gdy $|\Phi_n| = 1$, co, wobec Kroku 6, nigdy nie zachodzi. ►

K r o k 8. *Jeżeli* $\mathcal{E}_n = \{2\}$ *i* $\mathcal{D}_n = \varnothing$, *to* $n = 2$ *i* $a + b = 2^s$.

◄ Warunki $\mathcal{E}_n = \{2\}$, $\mathcal{D}_n = \varnothing$ są równoważne warunkom $|\Phi_n| = 2^s$, $s \geqslant 1$. Wówczas, zob. Krok 2, $2|n$. Niech $n = 2^\alpha r$, gdzie $2 \nmid r$ i $\alpha \geqslant 1$. Krok 3 pokazuje, że $r = \mathrm{rz}_2(ab^{-1})$, skąd $r = 1$, czyli $n = 2^\alpha$. Równość (5.53) (dla $X = a$, $Y = b$, $p = 2$) daje więc równość

$$\Phi_n = \frac{a^{2^\alpha} - b^{2^\alpha}}{a^{2^{\alpha-1}} - b^{2^{\alpha-1}}},$$

bo $\Phi_1(X, Y) = X - Y$. Mamy stąd $2^s = (a^{2^\alpha} - b^{2^\alpha})/(a^{2^{\alpha-1}} - b^{2^{\alpha-1}}) = a^{2^{\alpha-1}} + b^{2^{\alpha-1}}$. Łatwo stąd widać, że $s \geqslant 2$, a wówczas musi być $\alpha = 1$ (wystarczy położyć $a = 1 + 2c$, $b = 1 + 2d$, by, przy założeniu $\alpha \geqslant 2$, dostać absurd $2^s = 2 + 2^2 A$). ►

K r o k 9. *Jeżeli* $\mathcal{E}_n = \{p\}$, $p > 2$ *oraz* $a - b \geqslant 2$, *to* $\mathcal{D}_n \neq \varnothing$.

◄ Warunki $\mathcal{E}_n = \{p\}$, $p > 2$, $\mathcal{D}_n = \varnothing$ implikują, wobec tezy Kroku 5, równość $|\Phi_n| = p$. Taka równość, teza Kroku 6 i założenie $a - b \geqslant 2$ dają nierówność $p > 2^{\varphi(n)}$. Ponieważ $\alpha := v_p(n) \geqslant 1$, zob. Krok 2, więc $\varphi(n) = \varphi(p^\alpha r) = \varphi(p^\alpha)\varphi(r) \geqslant \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} \geqslant p - 1$. Stąd dostajemy absurdalną nierówność $p > 2^{p-1}$. Więc $\mathcal{D}_n \neq \varnothing$. ►

K r o k 10. *Jeżeli* $\mathcal{E}_n = \{p\}$, $p > 2$ *i* $\mathcal{D}_n = \varnothing$ *oraz* $a - b = 1$, *to* $n = 6$ *i* $a = 2$, $b = 1$.

◄ Warunki $\mathcal{E}_n = \{p\}$, $p > 2$, $\mathcal{D}_n = \varnothing$ implikują, wobec tezy Kroku 5, równość $|\Phi_n| = p$. Dzięki tezie Kroku 2 zapiszmy $n = p^\alpha r$, gdzie $v_p(n) = \alpha \geqslant 1$. Załóżmy najpierw, że $\alpha \geqslant 2$ i połóżmy $m = p^{\alpha-1} r$, $X = a$, $Y = b$ w równości (5.54). Dostajemy

$$p = |\Phi_n| = |\Phi_{pm}| = |\Phi_m(a^p, b^p)| \geqslant (a^p - b^p)^{\varphi(m)} \geqslant (a^p - b^p)^{p-1},$$

bo $\varphi(m) = \varphi(p^{\alpha-1} r) = \varphi(p^{\alpha-1})\varphi(r) \geqslant \varphi(p^{\alpha-1}) = p^{\alpha-1} - p^{\alpha-2} \geqslant p - 1$. Otrzymana nierówność $p \geqslant (a^p - b^p)^{p-1}$ jest nonsensowna, ponieważ, przy $a - b = 1$ i $a > b \geqslant 1$,

$$(a^p - b^p)^{p-1} = (a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1})^{p-1} > p^{p-1}.$$

Zatem $\alpha = 1$. W takim przypadku dostajemy

$$p = |\Phi_n| = |\Phi_{pr}| = \frac{|\Phi_r(a^p, b^p)|}{|\Phi_r(a, b)|} \geqslant \frac{(a^p - b^p)^{\varphi(r)}}{(a + b)^{\varphi(r)}} \geqslant \frac{a^p - b^p}{a + b} \geqslant \frac{2^p - 2}{3}, \tag{5.56}$$

gdzie trzecia równość wynika z (5.53), a pierwsza nierówność wynika nierówności Kroku 6. Trzecią nierówność wnioskujemy ze wzoru dwumiennego i założenia $a - b = 1$. Rzeczywiście:

$$\frac{a^p - b^p}{a + b} = \frac{(b + 1)^p - b^p}{2b + 1} = \frac{b}{2b + 1}\left(\sum_{j=0}^{p-1} \binom{p}{j} b^{j-1}\right) \geqslant \frac{1}{3}(2^p - 2),$$

bo $\frac{b}{2b+1} \geqslant \frac{1}{3}$ dla $b \geqslant 1$, a $2^p - 2 = (1 + 1)^p - 2 = \sum_{i=1}^{p-1} \binom{p}{i}$. Nierówność (5.56), $3p \geqslant 2^p - 2$, jest możliwa dla jedynej nieparzystej liczby pierwszej $p = 3$. Zatem $n = 3r$. Jednocześnie, zob. Krok 3, $r = \mathrm{rz}_3(ab^{-1})$, więc $r|3 - 1$ (zob. 5.5.4 (R3)). Mamy zatem dwie możliwości: $n = 3$ lub $n = 6$. Przypadek $n = 3$ odpada, bo $u_1 = a - b = 1$. W przypadku $n = 6$ mamy $3 = |\Phi_6| = |a^2 - ab + b^2| = b^2 + b + 1$. Skąd $(b - 1)(b + 2) = 0$. Ostatecznie, $b = 1$ i $a = 2$. ►

P o d s u m o w a n i e: W Kroku 8 odnaleźliśmy wyjątek (W2). Rzeczywiście, jeżeli $a+b=2^s$, to $u_2=a^2-b^2=(a+b)(a-b)=2^s(a-b)$, więc $\mathrm{Supp}(u_2)=\mathrm{Supp}(a-b)\cup\mathrm{Supp}(2^s)=\mathrm{Supp}(a-b)$, bo $2|a-b$. W Kroku 10 odnaleźliśmy, znany z przykładu P1, wyjątek (W1). Więcej wyjątków n i e m a. □

ZADANIE 5.18 Udowodnić wersję "plusową" twierdzenia Zsigmondy'*ego*: *Jeżeli* $a,b\in\mathbb{N}$ *i* $a>b\geqslant 1$, $a\perp b$, *to każdy wyraz ciągu* $(w_n)=(a^n+b^n)$ *ma dzielnik pierwszy pierwotny. Jedynym w y j ą t k i e m jest wyraz* 2^3+1^3 *ciągu* (2^n+1^n).

R o z w i ą z a n i e. Załóżmy, że wyraz $w_n=a^n+b^n$ n i e ma dzielnika pierwszego pierwotnego i rozważmy liczbę $a^{2n}-b^{2n}$. Jeżeli to nie jest wyjątek (W1) (czyli, jeżeli to nie jest przypadek $a=2$, $b=1$, $n=3$), ani wyjątek (W2) (czyli przypadek $a+b=2^s$, $n=1$), to istnieje $q\in\mathcal{D}_{2n}$. Wówczas $q\nmid a^m-b^m$ przy $m<2n$, w szczególności, $q\nmid a^{2k}-b^{2k}$ przy $k<n$. Zatem $q\nmid a^k+b^k$ dla takich k. ◊

Pokażemy kilka przykładów "działania" twierdzenia Zsigmondy'*ego*.

P r z y k ł a d 2. Dysponując tak ostrym narzędziem jak twierdzenie Zsigmondy'*ego* możemy "za darmo" rozwiązać Z2.F8. Rzeczywiście, niech p_1, p_2 i p_3 będą p i e r w o t n y m i dzielnikami pierwszymi wyrazów $2^{rs}-1$, 2^s-1 i 2^r-1 ciągu $(u_n(2,1))_{n\in\mathbb{N}}$. Takie dzielniki istnieją, bo $2<r<s<rs$ oraz $2+1\neq 2^u$. Mamy więc trzy r ó ż n e dzielniki pierwsze liczby M_{rs}. ◊

P r z y k ł a d 3. Czy istnieją trzy (różne) liczby postaci 7^n-5^n tworzące ciąg geometryczny? Odpowiedź: n i e. Łatwo to uzasadnić. Gdyby bowiem trójka 7^k-5^k, 7^l-5^l, 7^m-5^m, gdzie $k<l<m$ tworzyła ciąg geometryczny, czyli, gdyby środkowy wyraz 7^l-5^l był średnią geometryczną wyrazów skrajnych, to zachodziłaby równość $(7^m-5^m)(7^k-5^k)=(7^l-5^l)^2$. Ale taka równość nie może zachodzić, bo każdy dzielnik pierwszy wyrazu 7^m-5^m musiałby dzielić 7^l-5^l, nie byłby więc dzielnikiem pierwotnym. ◊

Ćwiczenie 5.48 Wyznaczyć wszystkie trójki liczb naturalnych a, m, $n\geqslant 2$, dla których zachodzi równość $a^m+1=(a+1)^n$.

Ćwiczenie 5.49 Wyznaczyć wszystkie takie liczby pierwsze p i takie liczby naturalne k, że liczba $p^k+p^{k-1}+\cdots+p+1$ jest potęgą dwójki.

5.6 Pierwiastki pierwotne

Dla niektórych modułów m grupa $(\mathbb{Z}/m)^*$ ma szczególnie przejrzystą budowę. Jest tak zwaną **grupą cykliczną**, czyli taką, której każdy element jest potęgą jednego ustalonego elementu zwanego **generatorem** (porównaj C1.36).

5.6.1 Definicja i uwagi wstępne

W interesującym nas przypadku grup $(\mathbb{Z}/m)^*$ używamy tradycyjnej terminologii:

Definicja 5.10 Niech $m\geqslant 2$ będzie liczbą naturalną. Liczbę całkowitą g nazywamy **pierwiastkiem pierwotnym modulo** m, gdy $g\perp m$ i $\mathrm{rz}_m(g)=\varphi(m)$. Inaczej mówiąc, g jest pierwiastkiem pierwotnym modulo m wtedy i tylko wtedy, gdy zbiór $\{g, g^2, \ldots, g^{\varphi(m)}\}$ jest zredukowanym układem reszt modulo m.

P r z y k ł a d 1. Weźmy $2 \pmod{37} \in (\mathbb{Z}/37)^*$. Ciąg potęg zaczyna się następująco:

$$2,\ 4,\ 8,\ 16,\ -5,\ -10,\ 17,\ -3,\ -6,\ -12,\ 13,\ -11,\ 15,\ -7,\ -14,\ 9,\ 18,\ \boxed{-1},\ \ldots\ .$$

(Wypisujemy najmniejsze co do wartości bezwzględnej liczby całkowite reprezentujące warstwy.) Widzimy, że $2^{18} \equiv -1 \pmod{37}$. Wobec tego dalsze potęgi $2 \pmod{37}$ wyglądają tak: $2^{18+k} \equiv -2^k \pmod{37}$. Jasne więc, że warstwa $1 \pmod{37}$ pojawi się po raz pierwszy dla $k = 18$. Zatem $\mathrm{rz}_{37}(2) = 36 = \varphi(37)$. Zatem: 2 jest pierwiastkiem pierwotnym $\pmod{37}$. $\Diamond$

Ćwiczenie 5.50 Wyznaczyć zbiór w s z y s t k i c h pierwiastków pierwotnych modulo 13. *Wskazówka.* W przykładzie z ustępu 5.5.4 widzieliśmy, że 6 jest pierwiastkiem pierwotnym modulo 13. Wypisać potęgi $6^k \pmod{13}$ dla $k = 0, 1, \ldots, 11$, i zauważyć, że m n o ż e n i e tych potęg odpowiada d o d a w a n i u wykładników modulo 12. Teraz zobaczyć T5.17.

Ćwiczenie 5.51 Sprawdzić, że 2 jest pierwiastkiem pierwotnym modulo 29, a następnie wyznaczyć wszystkie pierwiastki pierwotne modulo 29. Skorzystać przy tym z C5.38.

ZADANIE 5.19 Rozwiązać kongruencję

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \equiv 0 \pmod{29}. \tag{5.57}$$

R o z w i ą z a n i e. Załóżmy, że $x \in \mathbb{Z}$ jest rozwiązaniem (5.57). Mnożąc obustronnie przez $x - 1$ mamy $x^7 - 1 \equiv 0 \pmod{29}$. Wiemy, że 2 jest pierwiastkiem pierwotnym modulo 29. Kładąc $x \equiv 2^u \pmod{29}$, znajdujemy $2^{7u} \equiv 1 \pmod{29}$. Stąd, na mocy T5.15, $28|7u$, bo $\mathrm{rz}_{29}(2) = 28$. Zatem $4|u$. Więc $x \equiv 2^4,\ 2^8,\ 2^{12},\ 2^{16},\ 2^{20},\ 2^{24} \pmod{29}$. $\Diamond$

U w a g a. W tabelce na stronie vi pokazujemy liczby pierwsze $3 \leqslant p \leqslant 2011$ i odpowiednie najmniejsze dodatnie pierwiastki pierwotne g (dla liczb pierwszych $\leqslant 167$ pokazujemy dodatkowo najmniejsze co do wartości bezwzględnej ujemne pierwiastki pierwotne g').

Ćwiczenie 5.52 Wyjaśnić, dlaczego ż a d e n z pierwiastków pierwotnych g nie jest kwadratem (liczby całkowitej), natomiast niektóre liczby pierwsze mają ujemne pierwiastki pierwotne g' postaci $-a^2$. Jaką wspólną cechę mają te liczby pierwsze?

Ćwiczenie 5.53 Udowodnić, że jeżeli istnieje pierwiastek pierwotny $(\mathrm{mod}\, m)$, to liczba wszystkich (różnych $(\mathrm{mod}\, m)$) pierwiastków pierwotnych $(\mathrm{mod}\, m)$ jest równa $\varphi(\varphi(m))$.

Ćwiczenie 5.54 Udowodnić, że jeżeli $p > 2$ jest liczbą pierwszą, to $g \in \mathbb{Z}$ jest pierwiastkiem pierwotnym $(\mathrm{mod}\, p)$ wtedy i tylko wtedy, gdy

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p} \tag{5.58}$$

i jednocześnie $g^k \not\equiv 1 \pmod{p}$ dla wszystkich $1 \leqslant k \leqslant \frac{p-1}{2}$.

Ćwiczenie 5.55 Dana jest liczba naturalna $m \geqslant 2$ i względnie pierwsza z nią liczba całkowita g. Załóżmy, że dla każdego dzielnika pierwszego $q|\varphi(m)$, zachodzi

$$g^{\frac{\varphi(m)}{q}} \not\equiv 1 \pmod{m}. \tag{5.59}$$

Udowodnić, że g jest pierwiastkiem pierwotnym modulo m.

Teza tego ćwiczenia oznacza, że dla sprawdzenia, czy dana liczba jest pierwiastkiem pierwotnym $(\mathrm{mod}\, m)$ nie musimy wypisywać wszystkich $\varphi(m)$ początkowych wyrazów ciągu typu (5.41). W poniższym przykładzie zobaczymy jak to działa:

P r z y k ł a d 2. Sprawdzimy czy 2 jest pierwiastkiem pierwotnym modulo 67. Mamy rozkład: $\varphi(67) = 66 = 11 \cdot 3 \cdot 2$. Zgodnie z C5.54 badamy 2^6, 2^{22}, 2^{33} $(\mathrm{mod}\, 67)$. Liczymy:

$$2^6 \equiv 64 \equiv -3 \not\equiv 1 \,(\mathrm{mod}\, 67),$$
$$2^{22} = (2^6)^3 \cdot 2^4 \equiv (-3)^3 \cdot 16 \equiv -432 \equiv 37 \not\equiv 1 \,(\mathrm{mod}\, 67),$$
$$2^{33} = (2^6)^5 \cdot 2^3 \equiv (-3)^5 \cdot 8 \equiv -27 \cdot 72 \equiv -27 \cdot 5 = -135 \equiv -1 \not\equiv 1 \,(\mathrm{mod}\, 67).$$

Widzimy stąd, że 2 jest pierwiastkiem pierwotnym $(\mathrm{mod}\, 67)$. ◊

Ćwiczenie 5.56 Udowodnić, że jeżeli g jest pierwiastkiem pierwotnym modulo m, przy czym liczby m i g są nieparzyste, to g jest pierwiastkiem pierwotnym modulo $2m$.

Ćwiczenie 5.57 Dowieść, że liczba 2 jest pierwiastkiem pierwotnym $(\mathrm{mod}\, 27)$, a (oczywiście(!?)) nie jest pierwiastkiem pierwotnym $(\mathrm{mod}\, 54)$, natomiast liczba 5 jest pierwiastkiem pierwotnym zarówno $(\mathrm{mod}\, 27)$ jak i $(\mathrm{mod}\, 54)$.

ZADANIE 5.20 Udowodnić, że $g = 2$ jest pierwiastkiem pierwotnym $(\mathrm{mod}\, 3^e)$.

R o z w i ą z a n i e. Mamy pokazać, że najmniejszą liczbą $n \in \mathbb{N}$, dla której zachodzi kongruencja $2^n \equiv 1 \,(\mathrm{mod}\, 3^e)$ jest $n = \varphi(3^e) = 2 \cdot 3^{e-1}$. Kongruencja $2^n \equiv 1 \,(\mathrm{mod}\, 3^e)$ implikuje kongruencję $2^n \equiv 1 \,(\mathrm{mod}\, 3)$, z której wynika(!) parzystość liczby n. Połóżmy więc $n = 2k$. Wtedy $3^e | 4^k - 1$, czyli $v_3(4^k - 1) \geqslant e$. Ale $v_3(4^k - 1) = v_3(4 - 1) + v_3(k) = 1 + v_3(k)$ na mocy LZW (zob. T2.18). Zatem $v_3(k) \geqslant e - 1$. Najmniejszą liczbą k spełniającą tę nierówność jest $k = 3^{e-1}$. Więc najmniejszą liczbą n jest liczba $2 \cdot 3^{e-1} = \varphi(3^e) = \mathrm{card}\,(\mathbb{Z}/3^e)^*$. ◊

Ćwiczenie 5.58 Udowodnić obserwację młodego Gaussa: 10 *jest pierwiastkiem pierwotnym modulo* $p \neq 2, 5$ *wtedy i tylko wtedy, gdy ciąg cyfr dziesiętnych (po przecinku) liczby* $\frac{1}{p}$ *jest ciągiem czysto-okresowym*[8] *o okresie długości* $p - 1$.

5.6.2 Twierdzenie o istnieniu pierwiastków pierwotnych

Udowodnimy teraz twierdzenie o istnieniu pierwiastków pierwotnych modulo m.

ZADANIE 5.21 Udowodnić, że jeżeli $m = m_1 m_2$, $m_1, m_2 > 2$ i $\mathrm{NWD}\,(m_1, m_2) = 1$, to n i e i s t n i e j e pierwiastek pierwotny modulo m.

R o z w i ą z a n i e. Skorzystamy z multyplikatywności φ-funkcji, zobacz T4.1, i ćwiczenia C4.13. Niech $\varphi(m_1) = 2u_1$, $\varphi(m_2) = 2u_2$ dla pewnych naturalnych u_1, u_2. Zatem, dla dowolnej względnie pierwszej z m liczby całkowitej a, dzięki T5.5:

$$a^{\frac{\varphi(m)}{2}} \equiv (a^{\varphi(m_1)})^{u_2} \equiv 1^{u_2} \equiv 1 \,(\mathrm{mod}\, m_1).$$

[8] Ciąg $(a_n)_{n \geqslant 1}$ nazywa się **ciągiem czysto-okresowym**, gdy istnieje takie $t \in \mathbb{N}$, że $a_{n+t} = a_n$ dla w s z y s t k i c h $n \in \mathbb{N}$.

Podobnie $a^{\frac{\varphi(m)}{2}} \equiv 1 \,(\mathrm{mod}\, m_2)$. Stąd $a^{\frac{\varphi(m)}{2}} \equiv 1 \,(\mathrm{mod}\, m)$, zobacz C2.17. Więc a nie jest pierwiastkiem pierwotnym modulo m. $\Diamond$

W powyższym zadaniu dowiedliśmy, że jedynie względem modułów m postaci $m = p^e$, gdzie p jest liczbą pierwszą, i $m = 2q^e$, gdzie q jest nieparzystą liczbą pierwszą, m o g ą istnieć pierwiastki pierwotne.

TWIERDZENIE 5.21 *Pierwiastek pierwotny* $(\mathrm{mod}\, m)$ *istnieje wtedy i tylko wtedy, gdy moduł* m *jest jednej z następujących postaci* $m = p^e$, $m = 2p^e$, $m = 2$, $m = 4$, *gdzie* p *oznacza n i e p a r z y s t ą liczbę pierwszą, a* e *dowolną liczbę naturalną.*

D O W Ó D. (1) Udowodnimy najpierw, że dla każdej liczby pierwszej p istnieje $\varphi(p-1)$ parami niekongruentnych $(\mathrm{mod}\, p)$ pierwiastków pierwotnych $(\mathrm{mod}\, p)$.

Dla danej liczby naturalnej d oznaczmy $\mathcal{R}(d) := \{\bar{x} \in (\mathbb{Z}/p)^* : \mathrm{rz}_p(x) = d\}$. Ponieważ każdy element $\bar{x} \in (\mathbb{Z}/p)^*$ m a jakiś rząd będący dzielnikiem $p-1$, zobacz T5.14, więc $(\mathbb{Z}/p)^* = \bigsqcup_{d|p-1} \mathcal{R}(d)$ (suma rozłączna = suma składników parami rozłącznych). Stąd

$$p - 1 = \sum_{r|p-1} |\mathcal{R}(d)|. \tag{5.60}$$

Teza jest, oczywiście, równoważna faktowi, że $|\mathcal{R}(p-1)| = \varphi(p-1)$. Wykażemy w i ę c e j: *Dla każdego dodatniego dzielnika* $d|p-1$ *zachodzi równość* $|\mathcal{R}(d)| = \varphi(d)$. Załóżmy w tym celu, że $\mathcal{R}(d) \neq \varnothing$ dla pewnego $d|p-1$ i niech $\bar{a} \in \mathcal{R}(d)$. Rozważmy generowaną przez $\bar{a}$ podgrupę $\Lambda = \{\bar{a}, \bar{a}^2, \ldots, \bar{a}^{d-1}, \bar{a}^d\}$. Zbiór Λ zawiera dokładnie d elementów, z których k a ż d y jest pierwiastkiem kongruencji $x^d - 1 \equiv 0 \,(\mathrm{mod}\, p)$. Ale, zobacz T5.12, kongruencja ta ma co najwyżej d rozwiązań, więc w zbiorze Λ występują w s z y s t k i e jej rozwiązania. Ponieważ każda warstwa rzędu d jest rozwiązaniem naszej kongruencji, więc zbiór $\mathcal{R}(d)$ jest podzbiorem zbioru Λ i ma, zobacz C5.38, $\varphi(d)$ elementów. Widzimy stąd, że jeżeli $|\mathcal{R}(d)| \neq 0$, to $|\mathcal{R}(d)| = \varphi(d)$. Jednocześnie, zobacz (4.5),

$$p - 1 = \sum_{d|p-1} \varphi(d). \tag{5.61}$$

Porównanie tej sumy z sumą (5.60), po uwzględnieniu nierówności $|\mathcal{R}(d)| \leqslant \varphi(d)$, pokazuje, że wszystkie składniki w sumie (5.60) są w istocie równe odpowiednim składnikom w sumie (5.61). W szczególności, $|\mathcal{R}(p-1)| = \varphi(p-1)$. To kończy rozumowanie.

U w a g a. Korzystając z lematu L5.6 można znacznie uprościć przedstawione rozumowanie: Równość $X^{p-1} - 1 = \prod_{d|p-1} \Phi_d(X)$ i C5.30 pokazują, że dla każdego z $\varphi(p-1) = \deg \Phi_{p-1}(X)$ pierwiastków α wielomianu $\Phi_{p-1}(X)$ w $\mathbb{F}_p$ zachodzi równość $\mathrm{rz}_p(\alpha) = p-1$.

(2) Dowodzimy teraz istnienia pierwiastka pierwotnego $(\mathrm{mod}\, p^e)$, dla $p \in \mathbb{P}_{>2}$.

Niech $p > 2$ będzie liczbą pierwszą i niech g będzie pierwiastkiem pierwotnym modulo p. Wtedy $g^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$, czyli $v_p(g^{p-1} - 1) \geqslant 1$. Pokażemy, że

(A) *Jeżeli* $v_p(g^{p-1} - 1) = 1$, *to* $\mathrm{rz}_{p^e}(g) = (p-1)p^{e-1} = \varphi(p^e)$ *dla każdego* $e \in \mathbb{N}$.

Rzeczywiście, niech $d = \mathrm{rz}_{p^e}(g)$. Wtedy $g^d \equiv 1 \,(\mathrm{mod}\, p)$ (bowiem $g^d \equiv 1 \,(\mathrm{mod}\, p^e)$), więc $p-1|d$ (na mocy T5.15, bo $\mathrm{rz}_p(g) = p-1$). Niech $d = (p-1)k$. Liczby $x = g^{p-1}$, $y = 1$ spełniają założenia LZW (zob. T2.18). Mamy więc

$$e \leqslant v_p(g^d - 1) = v_p(x^k - y^k) = v_p(g^{p-1} - 1) + v_p(k) = 1 + v_p(k)$$

(początkowa nierówność jest tylko innym zapisem założenia $p^e|g^d-1$). Zatem $v_p(k) \geqslant e-1$. Więc $d \geqslant (p-1)p^{e-1} = \varphi(p^e) = \mathrm{rz}\,(\mathbb{Z}/p^e)^*$. Jednocześnie, zobacz T5.14, $d|\varphi(p^e)$. Przeto $d=\varphi(p^e)$, więc g jest pierwiastkiem pierwotnym modulo p^e. Pokażemy teraz, że

(B) *Jeżeli g jest pierwiastkiem pierwotnym modulo p, dla którego $v_p(g^{p-1}-1) \geqslant 2$, to dla $g_1 = g+p$ zachodzi równość $v_p(g_1^{p-1}-1)=1$.*

Rzeczywiście, gdyby obie liczby $g^{p-1}-1$ i $g_1^{p-1}-1$ były podzielne przez p^2, to ich różnica, równa (dzięki wzorowi dwumiennemu)

$$(g_1^{p-1}-1)-(g^{p-1}-1) = (g+p)^{p-1}-g^{p-1} = \binom{p-1}{1}pg^{p-2}+p^2A,$$

gdzie $A\in\mathbb{Z}$, byłaby podzielna przez p^2. Stąd dostalibyśmy podzielność $p^2|(p-1)pg^{p-2}$, czyli $p|(p-1)g^{p-2}$. Co, wobec $\mathrm{NWD}\,(p,\,p-1)=1$ i $\mathrm{NWD}\,(p,\,g)=1$, jest niemożliwe.

W ten sposób uzasadniliśmy, że dla każdej nieparzystej liczby pierwszej p istnieje pierwiastek pierwotny modulo p^e przy dowolnym $e\in\mathbb{N}$. Rzeczywiście, z dwóch liczb g, $g+p$, gdzie g jest pierwiastkiem pierwotnym $(\mathrm{mod}\,p)$, co najmniej jedna jest pierwiastkiem pierwotnym $(\mathrm{mod}\,p^e)$.

(3) Jeżeli g jest pierwiastkiem pierwotnym modulo p^e, gdzie $p>2$, i g jest liczbą nieparzystą, to, na mocy C5.55, g jest również pierwiastkiem pierwotnym modulo $2p^e$. Jeżeli zaś g jest liczbą parzystą, to $g_1=g+p^e$ jest również pierwiastkiem pierwotnym modulo p^e, a przy tym jest liczbą nieparzystą. Widzimy więc, że dla wszystkich modułów $m=2p^e$, gdzie $p>2$, istnieją pierwiastki pierwotne.

(4) Pierwiastkiem pierwotnym modulo $m=2$ jest oczywiście $g=1$, zaś pierwiastkiem pierwotnym modulo $m=4$ jest oczywiście $g=3$.

Wobec Z5.21, dla zakończenia dowodu wystarczy się jeszcze przekonać, że dla żadnego modułu postaci $m=2^e$, $e\geqslant 3$, n i e i s t n i e j e pierwiastek pierwotny. To wynika z kongruencji

$$(2k+1)^{2^{e-2}} \equiv 1\,(\mathrm{mod}\,2^e) \tag{5.62}$$

prawdziwej dla $e\in\mathbb{N}_{\geqslant 3}$ i $k\in\mathbb{Z}$. Prosty dowód indukcyjny tej kongruencji pozostawiamy Czytelnikowi (byłoby również dobrze dostrzec tu możliwość zastosowania LZW). Kongruencja (5.62) pokazuje, że $\mathrm{rz}_{2^e}(a) \leqslant 2^{e-2} < 2^{e-1} = \varphi(2^e)$ dla każdej liczby nieparzystej a przy dowolnym $e\geqslant 3$. Żadna więc liczba nieparzysta nie może być pierwiastkiem pierwotnym modulo 2^e, $e\geqslant 3$. Liczby parzyste w ogóle nie wchodzą w rachubę! □

Przypadek $m=2^e$, $e\geqslant 3$, opisuje poniższe ćwiczenie:

Ćwiczenie 5.59 Wykazać, że 5 jest "prawie" pierwiastkiem pierwotnym modulo 2^e, w tym sensie, że dla każdego $b\in(\mathbb{Z}/2^e)^*$ jedna (ale nie obie, w przypadku gdy $e\geqslant 3$) z kongruencji $b\equiv 5^x\,(\mathrm{mod}\,2^e)$ lub $b\equiv -5^x\,(\mathrm{mod}\,2^e)$ ma rozwiązanie $x\in\mathbb{Z}$.

U w a g a. Tezę tego ćwiczenia w języku algebry wyraża się tak: *Jeżeli $e\geqslant 3$, to grupa $((\mathbb{Z}/2^e)^*,\,\cdot)$ jest **iloczynem prostym** swoich podgrup cyklicznych (5) i (-1).*

5.6.3 Jeszcze kilka przykładów

Pokażemy tu parę przykładów zastosowań i wyznaczania pierwiastków pierwotnych $(\mathrm{mod}\,m)$.

ZADANIE 5.22 Niech p będzie liczbą pierwszą. Udowodnić, że

$$\boxed{A_k := 1^k + 2^k + \ldots + (p-1)^k \equiv \begin{cases} 0 \,(\mathrm{mod}\, p), & \text{gdy } p-1 \nmid k, \\ -1 \,(\mathrm{mod}\, p), & \text{gdy } p-1 | k. \end{cases}} \tag{5.63}$$

Rozwiązanie. Niech g będzie ustalonym pierwiastkiem pierwotnym modulo p. Wówczas ciąg $g^k,\ g^{2k}, \ldots,\ g^{(p-1)k}$ jest permutacją ciągu składników sumy A_k w $\mathbb{Z}/p$. Zatem

$$A_k \equiv g^k + g^{2k} + \ldots + g^{(p-1)k} \,(\mathrm{mod}\, p).$$

Jeżeli $p-1|k$, to każdy składnik tej sumy, na mocy MTF, przystaje do $1 \,(\mathrm{mod}\, p)$, a tych składników jest $p-1$, więc ich sumą jest $(-1) \,(\mathrm{mod}\, p)$. Z drugiej strony, tożsamość nieśmiertelna pozwala napisać $(g^k-1)A_k \equiv g^{kp} - g^k \equiv g^k(g^{k(p-1)} - 1) \equiv 0 \,(\mathrm{mod}\, p)$, znowu dzięki MTF. Jeżeli teraz $p-1 \nmid k$, to $g^k - 1 \not\equiv 0 \,(\mathrm{mod}\, p)$, więc musi być $A_k \equiv 0 \,(\mathrm{mod}\, p)$. ♢

Ćwiczenie 5.60 Udowodnić, że iloczyn wszystkich (różnych modulo p) pierwiastków pierwotnych modulo p przystaje do $(-1)^{\varphi(p-1)}$ modulo p.

Ćwiczenie 5.61 Udowodnić, że suma wszystkich (różnych modulo p) pierwiastków pierwotnych modulo p przystaje do $\mu(p-1)$ modulo p. Zobacz D4.6.

Czytelnik, którego zdumiały warunki zachodzenia kongruencji (5.15) może rozwiązać:

Ćwiczenie 5.62 Dla danej liczby $m \in \mathbb{N}$ oznaczmy przez $P(m)$ iloczyn wszystkich liczb ze zbioru $\{k \in \mathbb{N} : 1 \leqslant k \leqslant m,\ k \perp m\}$. Udowodnić, że $P(m) \equiv -1 \,(\mathrm{mod}\, m)$, gdy istnieje pierwiastek pierwotny $(\mathrm{mod}\, m)$.

ZADANIE 5.23 Udowodnić, że jeżeli $p \neq 3$ jest liczbą pierwszą Fermat'a, to -3 jest pierwiastkiem pierwotnym modulo p.

Rozwiązanie. Niech $p = F_n = 2^m + 1$, gdzie $m = 2^n$, będzie liczbą pierwszą. Oznaczmy $a = (-3)^{2^{m-1}}$. Zgodnie z C5.55, liczba -3 jest pierwiastkiem pierwotnym modulo p wtedy i tylko wtedy, gdy $a \not\equiv 1 \,(\mathrm{mod}\, p)$. Załóżmy więc, nie wprost, że $a \equiv 1 \,(\mathrm{mod}\, p)$.

Niech g będzie dowolnym pierwiastkiem pierwotnym modulo p. Wtedy $-3 \equiv g^k \,(\mathrm{mod}\, p)$ dla pewnego wykładnika $k \in \mathbb{N}$. Wykażemy, że k jest liczbą parzystą. Gdyby $k = 2l+1$, to mielibyśmy $1 \equiv a \equiv (g^{2l+1})^{2^{m-1}} \equiv (g^{2^m})^l \cdot g^{2^{m-1}} \equiv 1^l \cdot g^{2^{m-1}} \equiv -1 \,(\mathrm{mod}\, p)$, zobacz C5.54, bo $\frac{p-1}{2} = 2^{m-1}$. Ta niedorzeczność dowodzi, że $k = 2r$. Połóżmy $b = g^r$. Wtedy:

$$-3 \equiv b^2 \,(\mathrm{mod}\, p). \tag{5.64}$$

Niech c spełnia kongruencję $2c \equiv b - 1 \,(\mathrm{mod}\, p)$. Oczywiście takie c istnieje, bo 2 jest odwracalna modulo p. Wówczas, dzięki (5.64):

$$8c^3 \equiv (b-1)^3 \equiv b(b^2+3) - (3b^2+1) \equiv b \cdot 0 - (3(-3)+1) \equiv 8 \,(\mathrm{mod}\, p),$$

skąd $c^3 \equiv 1 \,(\mathrm{mod}\, p)$, bo 8 jest odwracalne modulo p. Warstwa $c \,(\mathrm{mod}\, p)$ ma więc, na mocy T5.15, rząd 1 lub 3 w grupie $(\mathbb{Z}/p)^*$. Sprawdzenie, że ten rząd nie jest równy 1 pozostawiamy Czytelnikowi. Zatem $\mathrm{rz}_p(c) = 3$. To jednakże również nie może mieć miejsca, bo wtedy, na mocy T5.14, mielibyśmy nieprawdziwą podzielność $3|2^m$. To kończy rozwiązanie. ♢

Ćwiczenie 5.63 Dowieść, że jeżeli $p \in \mathbb{P}$ i $p \equiv 1 \,(\mathrm{mod}\, 4)$, to g jest pierwiastkiem pierwotnym $(\mathrm{mod}\, p)$ wtedy i tylko wtedy, gdy $-g$ jest pierwiastkiem pierwotnym $(\mathrm{mod}\, p)$. Wywnioskować (zob. Z5.23), że 3 jest pierwiastkiem pierwotnym modulo F_n, gdy $F_n \in \mathbb{P}$, $n \geqslant 1$.

Ćwiczenie 5.64 Niech $q = 2^m + 1$, $m \geqslant 2$. Udowodnić, że jeżeli $3^{\frac{q-1}{2}} \equiv -1 \,(\mathrm{mod}\, q)$, to q jest liczbą pierwszą (Fermat'a!). *Wskazówka.* Jeżeli $q - 1 | \varphi(q)$, to q jest liczbą pierwszą.

Ćwiczenie 5.65 Dana jest liczba pierwsza postaci $4k + 3$. Udowodnić, że liczba g jest pierwiastkiem pierwotnym modulo p wtedy i tylko wtedy, gdy $\mathrm{rz}_p(-g) = \frac{p-1}{2}$.

Ćwiczenie 5.66 Załóżmy, że $p \equiv 3 \,(\mathrm{mod}\, 8)$ jest taką liczbą pierwszą, że $\frac{p-1}{2}$ jest również liczbą pierwszą. Udowodnić, że 2 jest pierwiastkiem pierwotnym modulo p.

5.6.4 Indeks

Indeks, zwany też **logarytmem dyskretnym**, j e s t logarytmem. I używa się go w teorii liczb tak, jak w analizie matematycznej używa się zwykłego logarytmu.

Definicja 5.11 Niech g będzie ustalonym pierwiastkiem pierwotnym $(\mathrm{mod}\, m)$, gdzie m jest jednej z postaci (5.58). **Indeksem** danej warstwy $a \,(\mathrm{mod}\, m) \in (\mathbb{Z}/m)^*$ **przy podstawie** g nazywamy taką warstwę $\overline{k} = k \,(\mathrm{mod}\, \varphi(m)) \in \mathbb{Z}/\varphi(m)$, że zachodzi

$$g^k \equiv a \,(\mathrm{mod}\, m). \tag{5.65}$$

Taki indeks oznaczamy $\mathrm{ind}_g(a)$, lub, gdy wiemy o jaki pierwiastek pierwotny chodzi, $\mathrm{ind}\,(a)$.

Ćwiczenie 5.67 Załóżmy, że g i h są pierwiastkami pierwotnymi modulo m. Udowodnić, że dla dowolnych a, $b \in (\mathbb{Z}/m)^*$:

(1) $\mathrm{ind}_g(ab) \equiv \mathrm{ind}_g(a) + \mathrm{ind}_g(b) \,(\mathrm{mod}\, \varphi(m))$;

(2) $\mathrm{ind}_g(a) \equiv \mathrm{ind}_g(h) \cdot \mathrm{ind}_h(a) \,(\mathrm{mod}\, \varphi(m))$.

P r z y k ł a d. Weźmy $m = 27 \,(= 3^3)$. Z C5.57 wiemy, że 2 i 5 są pierwiastkami pierwotnymi $(\mathrm{mod}\, 27)$. Oto ciąg typu (5.41) dla $s = 2 \,(\mathrm{mod}\, 27)$:

2 4 8 16 5 10 20 13 26 25 23 19 11 22 17 7 14 1

Stąd dostaniemy tabelę funkcji $(\mathbb{Z}/27)^* \ni x \longmapsto y = \mathrm{ind}_2(x) \in \mathbb{Z}/18$:

x	**1**	**2**	**4**	**5**	**7**	**8**	**10**	**11**	**13**	**14**	**16**	**17**	**19**	**20**	**22**	**23**	**25**	**26**
y	**0**	**1**	**2**	**5**	**16**	**3**	**6**	**13**	**8**	**17**	**4**	**15**	**12**	**7**	**14**	**11**	**10**	**9**

Czytelnik zechce zbudować analogiczną tabelkę indeksów o podstawie 5, a następnie na tej i wyżej zamieszczonej tabelce potrenować logarytmowanie modulo 27. ◊

Ćwiczenie 5.68 Uzasadnić, że dla dowolnej nieparzystej liczby pierwszej p zachodzi równość $\mathrm{ind}_g(-1) = \frac{p-1}{2}$, gdzie g jest dowolnym pierwiastkiem pierwotnym $(\mathrm{mod}\, p)$.

5.6.5 Dwa słowa o liczbach Carmichaela

To jest dobre miejsce na powiedzenie kilku słów o tak zwanych liczbach Carmichaela.

Definicja. Liczba złożona $m \in \mathbb{N}$ nazywa się **liczbą Carmichaela**, gdy dla każdej takiej liczby $a \in \mathbb{Z}$, że $a \perp m$, zachodzi kongruencja $a^{m-1} \equiv 1 \,(\mathrm{mod}\, m)$.

TWIERDZENIE 5.22 (***Kryterium Korselta***) *Liczba naturalna złożona m jest liczbą Carmichaela wtedy i tylko wtedy, gdy (i) m jest liczbą bezkwadratową, (ii) dla każdego dzielnika pierwszego $p|m$ zachodzi podzielność $p-1|m-1$.*

D O W Ó D. $(\Rightarrow)$ (i) Załóżmy, że m jest liczbą Carmichaela. Niech $m = p^k m'$, gdzie $p \in \mathbb{P}$, $k \in \mathbb{N}$ i $p \perp m'$. Wykażemy, że $k = 1$. Załóżmy więc, nie wprost, że $k \geqslant 2$. Na mocy CTR (Chińskiego Twierdzenia o Resztach), istnieje $a \in \mathbb{Z}$ spełniające warunki: $a \equiv p+1 \,(\mathrm{mod}\, p^k)$ i $a \equiv 1 \,(\mathrm{mod}\, m')$. Wtedy $a \perp m$, więc $a^{m-1} \equiv 1 \,(\mathrm{mod}\, m)$, bo m jest liczbą Carmichaela. Redukując to modulo p^2, dostajemy $(1+p)^{m-1} \equiv 1 \,(\mathrm{mod}\, p^2)$. Ale $(1+p)^{m-1} \equiv 1 + (m-1)p \,(\mathrm{mod}\, p^2)$. Ponieważ $p|m$, więc $1 + (m-1)p \equiv 1 - p \,(\mathrm{mod}\, p^2)$. Dostajemy więc sprzeczność $1 \equiv 1 - p \,(\mathrm{mod}\, p^2)$. Dowodzi ona, że $k = 1$.

(ii) Pokazujemy teraz, że $p-1|m-1$ dla każdego $p|m$. Ponieważ m jest bezkwadratowa, więc $p \perp m/p$. Niech g będzie pierwiastkiem pierwotnym modulo p. Na mocy CTR znajdujemy taką liczbę całkowitą a, że $a \equiv g \,(\mathrm{mod}\, p)$ i $a \equiv 1 \,(\mathrm{mod}\, \frac{m}{p})$. Jasne, że $a \perp m$. Zatem $a^{m-1} \equiv 1 \,(\mathrm{mod}\, m)$. Redukując tę kongruencję modulo p dostajemy $g^{m-1} \equiv 1 \,(\mathrm{mod}\, p)$, skąd, na mocy T5.15, $p-1|m-1$, bo $\mathrm{rz}_p(g) = p-1$.

$(\Leftarrow)$ Załóżmy, że m jest taką liczbą naturalną, bezkwadratową i złożoną, że $p-1|m-1$ dla każdego dzielnika pierwszego $p|m$. Weźmy dowolną liczbę $a \perp m$. Wówczas, dla dowolnego dzielnika pierwszego $p|m$, $p \nmid a$, więc $a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$, na mocy MTF. Więc również $a^{m-1} \equiv 1 \,(\mathrm{mod}\, p)$ (bo $p-1|m-1$). To znaczy, że $p_i | a^{m-1} - 1$ dla każdej liczby pierwszej z rozkładu $m = p_1 p_2 \cdot \ldots \cdot p_s$. Wobec tego, że czynniki p_i są parami różne (więc też parami względnie pierwsze), na mocy C2.17 i oczywistej indukcji(!), $m | a^{m-1} - 1$. □

Pokażemy dwa przykłady zastosowania kryterium Korselta:

P r z y k ł a d 1. Załóżmy, że liczby $6n+1$, $12n+1$ i $18n+1$, dla pewnego $n \in \mathbb{N}$, są liczbami pierwszymi. Wtedy: *Liczba $m = (6n+1)(12n+1)(18n+1)$ jest liczbą Carmichaela.* Rzeczywiście, liczba $m = (6n+1)(12n+1)(18n+1)$, jako iloczyn trzech różnych liczb pierwszych, jest liczbą bezkwadratową. Warunek (i) kryterium Korselta jest więc spełniony. Dla sprawdzenia warunku (ii) tego kryterium mamy sprawdzić, że $6n$, $12n$ i $18n$ są dzielnikami liczby $m-1$. To wynika z równości $m = 36N + 18n + 12n + 6n + 1 = 36N' + 1$. Q.e.d. Wprawdzie n i e w i a d o m o czy istnieje nieskończenie wiele $n \in \mathbb{N}$, dla których $6n+1$, $12n+1$, $18n+1 \in \mathbb{P}$, ale nietrudno wskazać takie przykłady. Największe n z naszej tabelki liczb pierwszych to $n = 100$: liczby 601, 1201 i 1801, są pierwsze. Mamy więc "dużą" liczbę Carmichaela: 1 299 963 601. ◊

P r z y k ł a d 2. *Każda liczba Carmichaela ma co najmniej trzy różne dzielniki pierwsze.* Rzeczywiście, gdyby $n = pq$, gdzie $p \neq q \in \mathbb{P}$, było liczbą Carmichaela, to $p-1|pq-1$ i $q-1|pq-1$. Stąd natychmiast dostajemy sprzeczność: $p-1 = q-1$. Q.e.d. ◊

U w a g a. Udowodniono (1992), że liczb Carmichaela jest niekończenie wiele. Najmniejszą jest $561 = 3 \cdot 11 \cdot 17$. Istnienie liczb Carmichaela jest pewną nieprzyjemnością w, ważnym w kryptografii, "fermatowskim" teście pierwszości, zob. [**3**].

5.7 Reszty kwadratowe i prawo wzajemności

Prawo wzajemności dla reszt kwadratowych jest najważniejszym i najpiękniejszym (co zawsze idzie w parze!) twierdzeniem elementarnej teorii liczb. Pierwszy jego dowód pokazał Gauss.

5.7.1 Reszty i niereszty kwadratowe modulo p

Element s danego zbioru $(G, *)$ z działaniem $*$ nazywa się **kwadratem**, gdy istnieje taki element $t \in G$, że $s = t * t = t^2$. W grupie $(\mathbb{R}^*, \cdot)$ liczb rzeczywistych niezerowych (z działaniem mnożenia) kwadratami są liczby d o d a t n i e. W grupie $(\mathbb{C}^*, \cdot)$ niezerowych liczb zespolonych z mnożeniem k a ż d y element jest kwadratem. W grupie $(\mathbb{Z}, +)$ liczb całkowitych z dodawaniem kwadratami są liczby p a r z y s t e, a w grupie $(\mathbb{R}, +)$ liczb rzeczywistych z dodawaniem k a ż d y element jest kwadratem. W zbiorze $(\mathbb{Z}, \cdot)$ liczb całkowitych z mnożeniem kwadratów jest "dość mało": $\{0, 1, 4, 9, 16, \dots\}$. W tym paragrafie będziemy się zajmować charakteryzacją kwadratów w grupach $((\mathbb{Z}/m)^*, \cdot)$.

Definicja 5.12 Kwadrat w grupie $(\mathbb{Z}/m)^*$ nazywa się **resztą kwadratową modulo** m, pozostałe elementy tej grupy nazywa się **nieresztami kwadratowymi modulo** m. Piszemy $a\mathbf{R}m$, gdy $a \pmod m$ jest resztą kwadratową, oraz $a\mathbf{N}m$, gdy jest nieresztą kwadratową.

P r z y k ł a d 1. Niech $m = 30$. Oglądając tabelkę mnożenia w grupie $(\mathbb{Z}/30)^*$ z ustępu 5.4.2 widzimy, że istnieją dwie reszty kwadratowe modulo 30. Są to $1 \pmod{30}$ i $19 \pmod{30}$. Istotnie kongruencja $x^2 \equiv 1 \pmod{30}$ ma (cztery) rozwiązania: $\overline{1}$, $\overline{11}$, $\overline{19}$ i $\overline{29}$, a kongruencja $x^2 \equiv 19 \pmod{30}$ ma również (cztery) rozwiązania: $\overline{7}$, $\overline{13}$, $\overline{17}$ i $\overline{23}$. Pozostałe elementy (warstwy modulo 30) grupy $(\mathbb{Z}/30)^*$, mianowicie $\overline{7}$, $\overline{11}$, $\overline{13}$, $\overline{17}$, $\overline{23}$ i $\overline{29}$ są nieresztami kwadratowymi modulo 30. $\Diamond$

Niech $\mathrm{NWD}(a, m) = 1$. Wówczas $a\mathbf{R}m$, gdy kongruencja $x^2 \equiv a \pmod m$ ma rozwiązanie. Wiemy z WT5.13, że kongruencja ta ma rozwiązania wtedy i tylko wtedy, gdy mają rozwiązania kongruencje $x^2 \equiv a \pmod{p^{v_p(m)}}$ dla każdej liczby pierwszej p. W paragrafie 5.8 przekonamy się, że jeżeli p jest nieparzystą liczbą pierwszą, to $a\mathbf{R}p^n$ wtedy i tylko wtedy, gdy $a\mathbf{R}p$, zobacz T5.29. Wobec tego zajmiemy się dokładnie przypadkiem $m = p > 2$.

TWIERDZENIE 5.23 *Niech p będzie nieparzystą liczbą pierwszą. W grupie $(\mathbb{Z}/p)^*$ jest tyle samo reszt kwadratowych co niereszt kwadratowych.*

D O W Ó D. Oznaczmy $s = \frac{p-1}{2}$. Bardzo łatwo jest wskazać s reszt kwadratowych:

$$1^2 \pmod p,\ 2^2 \pmod p,\ \dots,\ s^2 \pmod p.$$

Sprawdzamy, że wypisaliśmy s r ó ż n y c h warstw. Istotnie, gdyby $a^2 \pmod p = b^2 \pmod p$ dla pewnych $1 \leqslant a \leqslant b \leqslant s$, to byłoby $(b-a)(b+a) \equiv 0 \pmod p$, co może, wobec narzuconych ograniczeń, zachodzić tylko, gdy $a = b$. Ponieważ każda niezerowa warstwa $(\mathrm{mod}\, p)$ równa jest $a \pmod p$ lub $-a \pmod p$ dla pewnego $1 \leqslant a \leqslant s$, a takie dwie dają ten sam kwadrat, więc wypisaliśmy już w s z y s t k i e reszty kwadratowe. $\square$

Ćwiczenie 5.69 Niech p będzie liczbą pierwszą, g dowolnym pierwiastkiem pierwotnym modulo p. Uzasadnić, że $g^k \pmod p$ jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy wykładnik k jest liczbą parzystą.

5.7.2 Symbol Legendre'*a*

Funkcja, która na resztach kwadratowych modulo p przyjmuje wartość 1, a na nieresztach wartość -1 jest, mimo prostoty określenia, tak w a ż n a, że zasługuje na specjalną nazwę.

Definicja 5.13 (**Symbol Legendre'*a***) Niech p będzie n i e p a r z y s t ą liczbą pierwszą. Dla $a \in \mathbb{Z}$ kładziemy

$$(a|p) = \left(\frac{a}{p}\right) = \begin{cases} +1, & \text{gdy} \quad a\mathbf{R}p, \\ -1, & \text{gdy} \quad a\mathbf{N}p, \\ 0, & \text{gdy} \quad p|a. \end{cases} \tag{5.66}$$

5.7.3 Kryterium Eulera

Kryterium Eulera pozwala, za pomocą prostej operacji podnoszenia do potęgi, przekonać się czy dana reszta $(\mathrm{mod}\, p)$ jest resztą kwadratową.

Twierdzenie 5.24 (***Kryterium Eulera***) *Jeżeli p jest nieparzystą liczbą pierwszą, to dla dowolnego $a \in \mathbb{Z}$ zachodzi*

$$\boxed{a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.} \tag{5.67}$$

D O W Ó D. Gdy $p|a$ sprawa jest oczywista. Niech więc $p \nmid a$ i niech $a \equiv g^k \pmod p$ dla danego pierwiastka pierwotnego g. W C5.69 sprawdziliśmy, że $g^k \pmod p$ jest kwadratem wtedy i tylko wtedy, gdy k jest liczbą parzystą. Z drugiej strony, jeżeli $k = 2l$, to

$$a^{\frac{p-1}{2}} \equiv \left(g^k\right)^{\frac{p-1}{2}} \equiv \left(g^{2l}\right)^{\frac{p-1}{2}} \equiv \left(g^{p-1}\right)^l \equiv 1^l \equiv 1 \pmod p.$$

Jeżeli zaś $k = 2l+1$, to

$$a^{\frac{p-1}{2}} \equiv \left(g^k\right)^{\frac{p-1}{2}} \equiv \left(g^{2l+1}\right)^{\frac{p-1}{2}} \equiv \left(g^{p-1}\right)^l g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Ostatnia kongruencja wynika z faktu, że $g^{\frac{p-1}{2}}$ jest taką liczbą, której kwadrat $\equiv 1 \pmod p$, a która sama n i e przystaje do 1 modulo p (musi więc przystawać do -1 modulo p, co wynika z T5.12 zastosowanego do wielomianu $X^2 - 1$). □

P r z y k ł a d 1. Zastosowanie kryterium Eulera dla zbadania charakteru kwadratowego danej warstwy modulo p jest możliwe, choć żmudne. Zbadamy na przykład, czy $31\mathbf{R}97$. Mamy

$$31^{48} \equiv 961^{24} \equiv (-9)^{24} \equiv 81^{12} \equiv (-16)^{12} \equiv 256^6 \equiv (-35)^6 \equiv (-36)^3 \equiv 1 \pmod{97}.$$

Zatem $(31|97) = +1$. Czyli: kongruencja $x^2 \equiv 31 \pmod{97}$ ma rozwiązania. Oczywiście z tego nie wynika, że umiemy je znaleźć. ◊

Mamy dwa natychmiastowe wnioski z T5.24:

WNIOSEK 1. *Symbol Legendre'a jest funkcją ściśle multyplikatywną:*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \quad \square$$

Drugi oczywisty wniosek nazywa się **I *uzupełnieniem prawa wzajemności***:

WNIOSEK 2. *Jeżeli p jest nieparzystą liczbą pierwszą, to*

$$\boxed{\left(\frac{-1}{p}\right) = \begin{cases} +1 & \iff \quad p \equiv 1 \,(\mathrm{mod}\, 4), \\ -1 & \iff \quad p \equiv 3 \,(\mathrm{mod}\, 4). \end{cases}} \quad \square \tag{5.68}$$

Widzimy, że jeżeli p jest nieparzystą liczbą pierwszą, to kongruencja $x^2 + 1 \equiv 0 \,(\mathrm{mod}\, p)$ ma rozwiązania, gdy $p \equiv 1 \,(\mathrm{mod}\, 4)$, i nie ma rozwiązań, gdy $p \equiv 3 \,(\mathrm{mod}\, 4)$.

Pokażemy trzy przykłady:

Przykład 2. Udowodnimy: *Jeżeli $p = F_n = 2^m + 1$, gdzie $m = 2^n$, jest liczbą pierwszą Fermata, to każda niereszta kwadratowa modulo p jest pierwiastkiem pierwotnym modulo p.* Rzeczywiście, g jest pierwiastkiem pierwotnym $(\mathrm{mod}\, p)$ wtedy i tylko wtedy, gdy $g^{\varphi(p)/2} \not\equiv 1 \,(\mathrm{mod}\, p)$, zob. C5.55, bo w badanym przypadku 2 jest jedynym dzielnikiem pierwszym liczby $\varphi(p) = 2^{n-1}$. W tym też przypadku $\varphi(p) = \frac{p-1}{2}$. Zatem, g jest pierwiastkiem pierwotnym $(\mathrm{mod}\, p)$ wtedy i tylko wtedy, gdy $g^{(p-1)/2} \not\equiv 1 \,(\mathrm{mod}\, p)$, czyli wtedy i tylko wtedy, gdy $g\mathbf{N}p$. Q.e.d. $\Diamond$

Przykład 3. Udowodnimy: *Jeżeli dla $n \in \mathbb{N}$ zachodzi równość $\sigma(n) = 2n + 1$, to n jest kwadratem (liczby naturalnej).* Niech $p > 2$ będzie dzielnikiem pierwszym liczby n i niech $k = v_p(n)$. Wówczas $n = p^k n'$ i $p \nmid n'$, więc, na mocy multyplikatywności funkcji σ, zobacz C4.2, mamy $\sigma(n) = \sigma(p^k)\sigma(n') = (1 + p + \ldots + p^k)\sigma(n') = 2n + 1$. To dowodzi, że $k \equiv 0 \,(\mathrm{mod}\, 2)$. Widzimy, że $v_p(n)$ jest liczbą parzystą dla każdej nieparzystej liczby pierwszej p. Zapiszmy więc $n = 2^l m^2$, gdzie $2 \nmid m$. Wówczas

$$2^{l+1}m^2 + 1 = 2n + 1 = \sigma(n) = \sigma(2^l)\sigma(m^2) = (2^{l+1} - 1)\sigma(m^2).$$

Uzyskaną równość przekształcamy do postaci $m^2+1 = (2^{l+1}-1)(\sigma(m^2)-m^2)$, z której widzimy, że $m^2 + 1 \equiv 0 \,(\mathrm{mod}\, q)$ dla każdego dzielnika pierwszego q liczby $2^{l+1} - 1$. Jasne, że gdy $l > 0$, to liczba $2^{l+1} - 1$, będąc sama postaci $4t + 3$, musi mieć dzielnik pierwszy q postaci $4t + 3$. I wtedy $(-1)\mathbf{R}q$, co jest niemożliwe. Ostatecznie $l = 0$ i $n = m^2$. Q.e.d. $\Diamond$

Przykład 4. Udowodnimy: *Jeżeli $p \in \mathbb{P}$, to $\sum_{r=1}^{p-1} (r|p) \cdot r \equiv 0 \,(\mathrm{mod}\, p)$.* Rzeczywiście, niech g będzie dowolnym pierwiastkiem pierwotnym $(\mathrm{mod}\, p)$. Wówczas

$$\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r \equiv \sum_{k=0}^{p-2} \left(\frac{g^k}{p}\right) g^k \equiv \sum_{k=0}^{p-2} (-1)^k g^k \equiv \sum_{k=0}^{p-2} (-g)^k \,(\mathrm{mod}\, p).$$

Mnożąc (w $\mathbb{Z}/p$) sumę z prawej strony przez $1+g$, dostajemy (zobacz tożsamość nieśmiertelną) $(1 + g)\sum_{r=1}^{p-1} (r|p) \cdot r \equiv 1 - (-g)^{p-1} \equiv 0 \,(\mathrm{mod}\, p)$ na mocy MTF. Wystarczy teraz pomnożyć przez $(1 + g)^{-1} \,(\mathrm{mod}\, p)$. Q.e.d. $\Diamond$

Ćwiczenie 5.70 Niech p będzie liczbą pierwszą i niech $p \nmid a$. Udowodnić, że warunkiem koniecznym i wystarczającym rozwiązalności kongruencji $x^n \equiv a \,(\mathrm{mod}\, p)$ jest zachodzenie przystawania $a^{\frac{p-1}{d}} \equiv 1 \,(\mathrm{mod}\, p)$, gdzie $d = \mathrm{NWD}\,(n,\, p-1)$.

5.7.4 Kryterium Gaussa

Jeden ze słynnych lematów Gaussa dostarcza, łatwiejszego w operowaniu niż kryterium Eulera, kryterium odróżniającego reszty kwadratowe $(\mathrm{mod}\, p)$ od niereszt kwadratowych $(\mathrm{mod}\, p)$.

Niech p będzie n i e p a r z y s t ą liczbą pierwszą. Wówczas $s := \frac{p-1}{2}$ jest liczbą naturalną. Niech $S = \{\,[r_1],\ [r_2],\ \ldots,\ [r_s]\,\} \subseteq (\mathbb{Z}/p)^*$ będzie takim s-elementowym podzbiorem, że

$$(\mathbb{Z}/p)^* = S \sqcup S' = \{\,[r_1],\, [r_2],\ \ldots,\, [r_s]\,\} \sqcup \{\,-[r_1],\, -[r_2],\ \ldots,\, -[r_s]\,\}. \tag{5.69}$$

Podzbiorów S spełniających warunek (5.69) jest dużo, mianowicie 2^s. Jeżeli bowiem zapiszemy $(\mathbb{Z}/p)^* = \{[1],\, [p-1]\} \sqcup \{[2],\, [p-2]\} \sqcup \ldots \sqcup \{[s],\, [p-s]\}$, to wybierając z każdej pary po jednym elemencie dostaniemy odpowiedni zbiór S.

P r z y k ł a d 1. Najczęściej używanymi zbiorami S są dwa z nich. Są to:

$$S = \{1,\, 2,\, \ldots,\, s\}, \qquad (\textbf{układ Gaussa}),$$
$$S = \{2,\, 4,\, \ldots,\, p-1\}, \qquad (\textbf{układ Eisensteina}).$$

Tu i dalej, dla oznaczenia warstw $(\mathrm{mod}\, p)$, wypisujemy tylko reprezentanty tych warstw. $\Diamond$

Dla danej, niepodzielnej przez p, liczby całkowitej a i danego podzbioru S spełniającego warunek (5.69), zdefiniujmy zbiór: $aS := \{ar_1,\, ar_2,\, \ldots,\, ar_s\}$. Oznaczmy:

$$\nu(p,\, a) = \mathrm{card}\,(aS \setminus S). \tag{5.70}$$

Dla układu Gaussa, $\nu(p,\, a)$ oznacza liczbę tych elementów zbioru aS, które przy dzieleniu przez p dają (najmniejszą dodatnią!) resztę w i ę k s z ą n i ż s, a dla układu Eisensteina, liczbę tych elementów zbioru aS, które przy dzieleniu przez p dają resztę n i e p a r z y s t ą.

Następne twierdzenie udowodnił K. Gauss w roku 1808.

TWIERDZENIE 5.25 (***Kryterium Gaussa***) *Przy wprowadzonych oznaczeniach, dla dowolnej nieparzystej liczby pierwszej p i liczby całkowitej $a \not\equiv 0 \,(\mathrm{mod}\, p)$, zachodzi równość*

$$\boxed{\left(\frac{a}{p}\right) = (-1)^{\nu(p,\, a)}.} \tag{5.71}$$

D O W Ó D. Wypiszmy s kongruencji

$$\begin{cases} ar_1 \equiv \varepsilon(1) r_{i_1} \,(\mathrm{mod}\, p), \\ ar_2 \equiv \varepsilon(2) r_{i_2} \,(\mathrm{mod}\, p), \\ \ldots \\ ar_s \equiv \varepsilon(s) r_{i_s} \,(\mathrm{mod}\, p), \end{cases} \tag{5.72}$$

gdzie $\varepsilon(k) = \pm 1$. Ponieważ każda (niezerowa) warstwa modulo p jest elementem zbioru S lub jest elementem zbioru S' (czyli jest elementem przeciwnym do pewnego elementu $r_i \in S$), więc takie napisy mają miejsce. Zauważmy, że ilość wyrazów równych -1 w ciągu $(\varepsilon(1), \varepsilon(2), \ldots, \varepsilon(s))$ jest równa $\nu(p, a)$. Zatem

$$\varepsilon(1)\varepsilon(2) \cdot \ldots \cdot \varepsilon(s) = (-1)^{\nu(p,\,a)}. \tag{5.73}$$

Co więcej, ciąg $(r_{i_1}, r_{i_2}, \ldots, r_{i_s})$ jest p e r m u t a c j ą ciągu $(r_1, r_2, \ldots, r_s)$. Istotnie, równość $r_{i_k} = r_{i_l}$, dla pewnych $1 \leqslant k, l \leqslant s$, dzięki kongruencjom (5.72), daje

$$\varepsilon(k)ar_k \equiv r_{i_k} \equiv r_{i_l} \equiv \varepsilon(l)ar_l \,(\mathrm{mod}\, p),$$

skąd $a(\varepsilon(k)r_k - \varepsilon(l)r_l) \equiv 0 \,(\mathrm{mod}\, p)$, co, po uproszczeniu przez a (pamiętamy, że $p \nmid a$) daje

$$r_k \equiv r_l \,(\mathrm{mod}\, p) \quad \text{lub} \quad r_k \equiv -r_l \,(\mathrm{mod}\, p).$$

Ale druga z tych kongruencji zajść nie może, bo $S \cap S' = \varnothing$. Zatem $r_{i_k} = r_{i_l} \Rightarrow r_k = r_l$. Więc rzeczywiście, ciąg $(r_{i_1}, r_{i_2}, \ldots, r_{i_s})$ jest permutacją ciągu $(r_1, r_2, \ldots, r_s)$. Oznaczmy przez R iloczyn (wszystkich) wyrazów pierwszego (i drugiego!) ciągu. Pomnóżmy stronami wszystkie s kongruencji (5.72). Otrzymamy:

$$a^s \cdot R \equiv a^s \prod_{k=1}^{s} r_k \equiv \prod_{k=1}^{s} ar_k \equiv \prod_{k=1}^{s} \varepsilon(k)r_{i_k} \equiv \prod_{k=1}^{s} \varepsilon(k) \prod_{k=1}^{s} r_{i_k} \equiv \prod_{k=1}^{s} \varepsilon(k) \cdot R \,(\mathrm{mod}\, p).$$

Mnożąc to obustronnie przez odwrotność $R^{-1} \,(\mathrm{mod}\, p)$ i korzystając z (5.73), dostajemy

$$a^{\frac{p-1}{2}} = a^s \equiv \prod_{k=1}^{s} \varepsilon(k) \equiv (-1)^{\nu(p,\,a)} \,(\mathrm{mod}\, p).$$

Wobec tego, na mocy (5.67), $(a|p) \equiv (-1)^{\nu(p,\,a)} \,(\mathrm{mod}\, p)$, co daje równość (5.71), bo p jest liczbą nieparzystą. □

P r z y k ł a d 2. Weźmy na przykład $p = 11$, $a = 6$. Wówczas: jeżeli $S = \{1, 2, 5, 7, 8\}$, to $aS = \{-5, 1, 8, -2, -7\}$; jeżeli zaś $S = \{1, 2, 3, 6, 7\}$, to $aS = \{6, 1, 7, 3, -2\}$. W pierwszym przypadku $\nu(p, a) = 3$, w drugim $\nu(p, a) = 1$, ale w obu przypadkach mamy $(-1)^{\nu(p,\,a)} = -1$. Więc $6\mathbf{N}11$. ◊

Udowodnimy teraz tak zwane **II *uzupełnienie prawa wzajemności***. Pozwala ono wyznaczyć charakter kwadratowy liczby 2 modulo p:

TWIERDZENIE 5.26 *Jeżeli p jest nieparzystą liczbą pierwszą, to*

$$\boxed{\left(\frac{2}{p}\right) = \begin{cases} +1 & \Longleftrightarrow \quad p \equiv \pm 1 \,(\mathrm{mod}\, 8), \\ -1 & \Longleftrightarrow \quad p \equiv \pm 3 \,(\mathrm{mod}\, 8). \end{cases}} \tag{5.74}$$

D O W Ó D. Dla dowodu skorzystamy z kryterium Gaussa z S równym układowi Gaussa. Musimy w tym celu rozstrzygnąć ile jest większych niż $s = \frac{p-1}{2}$ liczb w zbiorze

$$2S = \{2, 4, 6, \ldots, p-1\}.$$

Ponieważ $2x \leqslant s$ wtedy i tylko wtedy, gdy $x \leqslant s/2 = \frac{p-1}{4}$, więc widzimy, że

$$\nu(p,\,2) = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor .$$

Każda nieparzysta liczba pierwsza p jest jednej z postaci $8k+2t+1$, gdzie $t = 0,\,1,\,2,\,3$. W tych przypadkach mamy odpowiednio:

$$\frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor = 4k + t - \left\lfloor 2k + \frac{t}{2} \right\rfloor = \begin{cases} 2k, & \text{dla} \quad t = 0 \\ 2k+1, & \text{dla} \quad t = 1 \\ 2k+1, & \text{dla} \quad t = 2 \\ 2k+2, & \text{dla} \quad t = 3 \end{cases}$$

Widzimy, że $\nu(p,\,2)$ jest liczbą parzystą wtedy i tylko wtedy, gdy $p \equiv 1,\,7 \,(\mathrm{mod}\, 8)$ a liczbą nieparzystą wtedy i tylko wtedy, gdy $p \equiv 3,\,5 \,(\mathrm{mod}\, 8)$. To kończy dowód. □

U w a g a. Łatwo sprawdzić, że (5.74) wyrażają dokładnie tę samą treść co równość

$$\boxed{\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.}$$

5.7.5 Prawo wzajemności reszt kwadratowych

Najważniejszym (i najpiękniejszym) twierdzeniem elementarnej teorii liczb jest ***theorema fundamentale*** (twierdzenie podstawowe, zwane również ***theorema aureum*** – twierdzenie złote).

TWIERDZENIE 5.27 (***Prawo wzajemności reszt kwadratowych***) *Jeżeli p i q są różnymi nieparzystymi liczbami pierwszymi, to*

$$\boxed{\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.} \tag{5.75}$$

D O W Ó D. Niech $p \neq q$ będą dwiema nieparzystymi liczbami pierwszymi. Dla wyznaczenia wartości $(q|p)$ wykorzystamy kryterium Gaussa z układem Eisensteina $\{2,\,4,\,\ldots,\,p-1\}$. Mamy $qS = \{2q,\,4q,\,\ldots,\,(p-1)q\}$. Dzielimy z resztą każdy element tego zbioru przez p:

$$2kq = \left\lfloor \frac{2kq}{p} \right\rfloor \cdot p + r_k, \quad \text{gdzie } 1 \leqslant r_k \leqslant p-1, \tag{5.76}$$

dla $k = 1,\,2,\,\ldots,\,s$. Tym razem $\nu(p,\,q)$ oznacza liczbę n i e p a r z y s t y c h spośród reszt r_k. Sprytny pomysł Eisensteina polega na wykorzystaniu równości

$$\left(\frac{q}{p}\right) = (-1)^{\nu(p,\,q)} = (-1)^{\sum' r_k} = (-1)^{\sum r_k}, \tag{5.77}$$

gdzie przez $\sum' r_k$ oznaczyliśmy sumę n i e p a r z y s t y c h spośród reszt r_k, a przez $\sum r_k$ sumę w s z y s t k i c h reszt r_k. Trzecia z tych równości wynika z faktu "neutralności" składników

parzystych w wykładniku potęgi o podstawie (-1). Druga zaś, wynika z oczywistego faktu, że suma pewnej ilości liczb nieparzystych różni się od ich ilości o liczbę parzystą. Wykładnik $\sum r_k$ obliczamy dodając stronami równości (5.76):

$$\sum_{k=1}^{s} r_k = 2 \cdot \sum_{k=1}^{s} kq - p \cdot \sum_{k=1}^{s} \left\lfloor \frac{2kq}{p} \right\rfloor .$$

Stąd, dzięki (5.77),

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{s} \left\lfloor \frac{2kq}{p} \right\rfloor}, \tag{5.78}$$

bo składniki parzyste w wykładniku można zaniedbać, a $(-1)^p = -1$. Dokładnie tak samo dostaniemy

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{l=1}^{t} \left\lfloor \frac{2lp}{q} \right\rfloor}, \tag{5.79}$$

gdzie $t = \frac{q-1}{2}$. Mnożąc stronami równości (5.78), (5.79), dostaniemy

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{s} \left\lfloor \frac{2kq}{p} \right\rfloor + \sum_{l=1}^{t} \left\lfloor \frac{2lp}{q} \right\rfloor}.$$

Porównanie tej równości z równością (5.75), pokazuje, że dla zakończenia dowodu wystarczy udowodnić, że

$$\sum_{k=1}^{s} \left\lfloor \frac{2kq}{p} \right\rfloor + \sum_{l=1}^{t} \left\lfloor \frac{2lp}{q} \right\rfloor \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2. \tag{5.80}$$

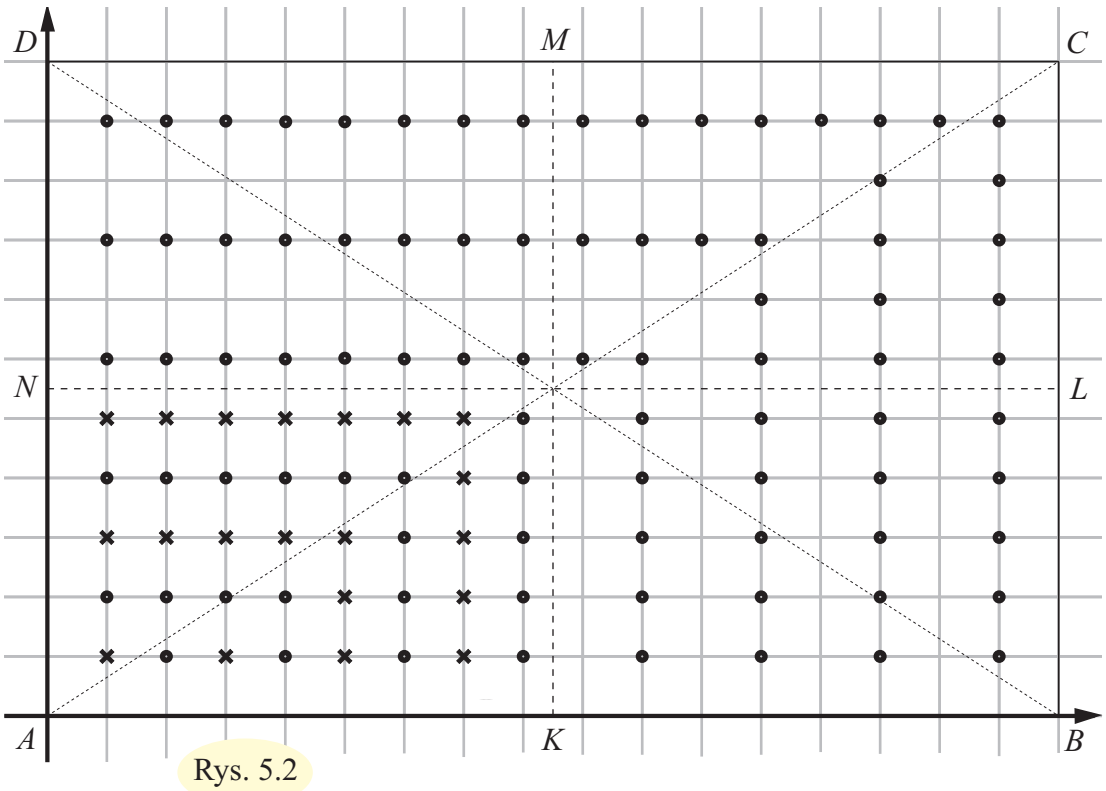
Aby to zrobić zauważmy najpierw, że liczba $\left\lfloor \frac{2kq}{p} \right\rfloor$ może być zinterpretowana jako liczba punktów kratowych o odciętej równej $2k$ i d o d a t n i e j rzędnej, leżących p o d prostą o równaniu $y = \frac{q}{p}x$ (lub na tej prostej). Analogicznie, liczba $\left\lfloor \frac{2lp}{q} \right\rfloor$ oznacza liczbę punktów kratowych o rzędnej równej $2l$ i dodatniej odciętej leżących n a l e w o od prostej o równaniu $y = \frac{q}{p}x$.

Opisane tu punkty kratowe będziemy w dalszym ciągu nazywać *punktami wyróżnionymi*. Na rysunku 5.2 widzimy prostokąt $ABCD$ o wierzchołkach $A = (0, 0)$, $B = (p, 0)$, $C = (p, q)$ i $D = (0, q)$ (przy $p = 17$, $q = 11$). Punkty wyróżnione leżące w e w n ą t r z prostokąta $ABCD$ zaznaczyliśmy czarnymi kółeczkami. Niech K, L, M, N oznaczają środki odpowiednich boków. Niech też S będzie środkiem prostokąta (na rysunku nie oznaczonym). Zauważmy, że na przekątnych wewnątrz prostokąta n i e m a punktów kratowych.

Symetria osiowa o osi l_{NL} przeprowadza trójkąt $\triangle CSL$ na trójkąt $\triangle BSL$. Punkty wyróżnione pierwszego z tych trójkątów p r z e c h o d z ą w punkty wyróżnione drugiego. Zatem, wewnątrz trójkąta $\triangle CSB$ znajduje się p a r z y s t a liczba punktów wyróżnionych. Podobnie, dzięki symetrii osiowej o osi l_{KM}, widzimy, że wewnątrz trójkąta $\triangle DSC$ znajduje się parzysta liczba punktów wyróżnionych. Wobec tego, suma z lewej strony (5.80) jest tej samej parzystości, co liczba punktów wyróżnionych znajdujących się wewnątrz trójkąta $\triangle ABD$.

Jednocześnie, symetria osiowa o osi l_{NL} przeprowadza wyróżnione punkty z wnętrza trójkąta $\triangle DSN$ w niewyróżnione (zaznaczone krzyżykami) punkty kratowe z wnętrza trójkąta

$\triangle ASN$, a symetria osiowa o osi l_{KM} przeprowadza wyróżnione punkty z wnętrza trójkąta $\triangle BSK$ w niewyróżnione (zaznaczone krzyżykami) punkty kratowe z wnętrza trójkąta $\triangle ASK$.



Rys. 5.2

To oznacza, że wyróżnionych punktów we wnętrzu trójkąta $\triangle ABD$ jest dokładnie tyle ile jest wszystkich punktów kratowych we wnętrzu prostokąta $AKSN$, a tych jest $\frac{p-1}{2} \cdot \frac{q-1}{2}$. W ten sposób dowód równości (5.75) jest zakończony. □

Uwaga 1. Pierwszy pełny dowód równości (5.75) pochodzi od Gaussa (data odkrycia: 8 IV 1796, data publikacji: 1801). Zbiór znanych dowodów ma (obecnie) około 200 elementów (sam Gauss opublikował sześć różnych dowodów). Pokazany wyżej dowód jest w zasadzie trzecim dowodem Gaussa. Istotne uproszczenia pochodzą od Eisensteina.

Przykład. Prawo wzajemności (5.75) i jego uzupełnienia (5.68) i (5.74) pozwalają wyznaczać charakter kwadratowy dowolnych liczb całkowitych względem dowolnego modułu pierwszego. Sprawdzimy na przykład, czy -30 jest resztą kwadratową modulo 647. Obliczymy w tym celu wartość symbolu Legendre'a $(-30|647)$. Mamy:

$$\left(\frac{3}{647}\right) = \left(\frac{647}{3}\right) \cdot (-1)^{323 \cdot 1} = \left(\frac{2}{3}\right) \cdot (-1) = (-1) \cdot (-1) = +1,$$

$$\left(\frac{5}{647}\right) = \left(\frac{647}{5}\right) \cdot (-1)^{323 \cdot 2} = \left(\frac{2}{5}\right) \cdot (+1) = -1.$$

Wobec multyplikatywności symbolu Legendre'a, mamy więc

$$\left(\frac{-30}{647}\right) = \left(\frac{-1}{647}\right) \cdot \left(\frac{2}{647}\right) \cdot \left(\frac{3}{647}\right) \cdot \left(\frac{5}{647}\right) = (-1) \cdot (+1) \cdot (+1) \cdot (-1) = +1.$$

Zatem $(-30)\mathbf{R}647$, co oznacza, że kongruencja $x^2 \equiv -30 \,(\mathrm{mod}\, 647)$ ma rozwiązania. $\Diamond$

Ćwiczenie 5.71 Uzasadnić, że jeżeli liczba pierwsza $p \equiv 173 \,(\mathrm{mod}\, 1680)$, to $(-2)\mathbf{N}p$, $(-3)\mathbf{N}p$, $(-5)\mathbf{N}p$ i $(-7)\mathbf{N}p$.

U w a g a 2. Równość (5.75) najłatwiej zapamiętać i stosować następująco: *Jeżeli dane są różne nieparzyste liczby pierwsze* p, q, *to* $(q|p) = -(p|q)$, *gdy obie liczby* p, q *są postaci* $4x+3$, *gdy zaś co najmniej jedna z liczb* p, q *jest postaci* $4x+1$, *to* $(q|p) = (p|q)$.

5.7.6 Prawo wzajemności a ciągi arytmetyczne

Istnieją silne i ważne związki między ciągami arytmetycznymi a prawem wzajemności. Pokażemy teraz parę przykładów takich związków.

Niech p oznacza n i e p a r z y s t ą liczbę pierwszą. I uzupełnienie prawa wzajemności może być sformułowane następująco:

$$\boxed{\boxed{(-1)\mathbf{R}p \quad \Longleftrightarrow \quad p \equiv 1 \,(\mathrm{mod}\, 4).}} \tag{5.81}$$

Zobacz (5.68). Widzimy stąd, że -1 jest resztą kwadratową modulo te liczby pierwsze p, które są wyrazami ciągu arytmetycznego $(4x+1)$. Na przykład $p = 5,\ 13,\ 29,\ 37,\ 41,\ 53$ itd.

II uzupełnienie prawa wzajemności może być sformułowane[9] następująco:

$$\boxed{\boxed{2\mathbf{R}p \quad \Longleftrightarrow \quad p \equiv \pm 1 \,(\mathrm{mod}\, 8).}} \tag{5.82}$$

Zobacz (5.74). Widzimy stąd, że 2 jest resztą kwadratową modulo te liczby pierwsze p, które są wyrazami ciągu arytmetycznego $(8x+1)$ lub ciągu arytmetycznego $(8x+7)$. Na przykład $p = 17,\ 41,\ 73,\ 89,\ 97$ itd., lub $p = 7,\ 23,\ 31,\ 47,\ 71,\ 79$ itd.

P r z y k ł a d 1. Zobaczymy teraz w jakich ciągach arytmetycznych leżą te liczby pierwsze p, dla których $(-2)\mathbf{R}p$. Ponieważ symbol Legendre'a jest funkcją multyplikatywną licznika, zobacz T5.23, więc

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right).$$

Wobec tego $(-2|p) = +1$ wtedy i tylko wtedy, gdy $(-1|p) = (2|p) = +1$ lub $(-1|p) = (2|p) = -1$. Pierwszy przypadek zachodzi wtedy i tylko wtedy, gdy $p \equiv 1,\ 5 \,(\mathrm{mod}\, 8)$ i $p \equiv 1,\ 7 \,(\mathrm{mod}\, 8)$, czyli wtedy i tylko wtedy, gdy $p \equiv 1 \,(\mathrm{mod}\, 8)$. Drugi przypadek zachodzi wtedy i tylko wtedy, gdy $p \equiv 3,\ 7 \,(\mathrm{mod}\, 8)$ i $p \equiv 3,\ 5 \,(\mathrm{mod}\, 8)$, czyli wtedy i tylko wtedy, gdy $p \equiv 3 \,(\mathrm{mod}\, 8)$. Mamy więc:

$$\boxed{\boxed{(-2)\mathbf{R}p \quad \Longleftrightarrow \quad p \equiv 1,\ 3 \,(\mathrm{mod}\, 8).}} \tag{5.83}$$

[9] Napis postaci $a \equiv \pm b \,(\mathrm{mod}\, c)$ jest skrótem alternatywy $a \equiv b \,(\mathrm{mod}\, d)$ l u b $a \equiv -b \,(\mathrm{mod}\, c)$. Podobnie, napis postaci $a \equiv b,\ c \,(\mathrm{mod}\, d)$ znaczy alternatywę a nie koniunkcję!

Zatem, -2 jest resztą kwadratową modulo $p \neq 2$ wtedy i tylko wtedy, gdy p jest wyrazem jednego z ciągów arytmetycznych $(8x+1)$, $(8x+3)$. $\Diamond$

P r z y k ł a d 2. Zobaczymy w jakich ciągach arytmetycznych leżą te liczby pierwsze p, dla których $3\mathbf{R}p$. Niech $p \neq 3$. Rozpatrzmy przypadki: (1) $p \equiv 1 \,(\mathrm{mod}\, 4)$, (2) $p \equiv 3 \,(\mathrm{mod}\, 4)$. W przypadku (1), na mocy 5.7.5 U2, $(3|p) = (p|3)$. Zatem $(3|p) = +1$ wtedy i tylko wtedy, gdy $(p|3) = +1$, czyli wtedy i tylko wtedy, gdy $p \equiv 1 \,(\mathrm{mod}\, 3)$. Warunki $p \equiv 1 \,(\mathrm{mod}\, 4)$ i $p \equiv 1 \,(\mathrm{mod}\, 3)$ są spełnione jednocześnie dla liczb pierwszych p spełniających $p \equiv 1 \,(\mathrm{mod}\, 12)$, i tylko dla takich liczb. W przypadku (2), znów na mocy 5.7.5 U2, $(3|p) = -(p|3)$. Zatem $(3|p) = +1$ wtedy i tylko wtedy, gdy $(p|3) = -1$, czyli wtedy i tylko wtedy, gdy $p \equiv 2 \,(\mathrm{mod}\, 3)$. Warunki $p \equiv 3 \,(\mathrm{mod}\, 4)$ i $p \equiv 2 \,(\mathrm{mod}\, 3)$ są spełnione jednocześnie dla liczb pierwszych p spełniających $p \equiv 11 \,(\mathrm{mod}\, 12)$, i tylko dla takich liczb. Podsumowując, mamy:

$$\boxed{3\mathbf{R}p \iff p \equiv \pm 1 \,(\mathrm{mod}\, 12).} \tag{5.84}$$

Znowu więc znaleźliśmy ciągi arytmetyczne, w których rozmieszczone są te liczby pierwsze p, dla których liczba 3 jest resztą kwadratową modulo p. $\Diamond$

Ćwiczenie 5.72 Udowodnić, że

$$(-3)\mathbf{R}p \iff p \equiv 1,\, 7 \,(\mathrm{mod}\, 12), \tag{5.85}$$

$$5\mathbf{R}p \iff p \equiv \pm 1,\, \pm 3^2 \,(\mathrm{mod}\, 20), \tag{5.86}$$

$$(-5)\mathbf{R}p \iff p \equiv 1,\, 3,\, 7,\, 9 \,(\mathrm{mod}\, 20), \tag{5.87}$$

$$7\mathbf{R}p \iff p \equiv \pm 1,\, \pm 3^2,\, \pm 5^2 \,(\mathrm{mod}\, 28), \tag{5.88}$$

$$(-7)\mathbf{R}p \iff p \equiv 1,\, 9,\, 11,\, 15,\, 23,\, 25 \,(\mathrm{mod}\, 28). \tag{5.89}$$

Spróbujmy uogólnić wyniki (5.84), (5.86) i (5.88):

Ćwiczenie 5.73 Niech q będzie nieparzystą liczbą pierwszą. Udowodnić, że

$$\boxed{q\mathbf{R}p \iff p \equiv \pm 1,\, \pm 3^2,\, \ldots,\, \pm(q-2)^2 \,(\mathrm{mod}\, 4q).} \tag{5.90}$$

Ćwiczenie 5.74 Korzystając tylko z kryterium Gaussa, udowodnić (5.83) i (5.84).

Pokażemy teraz jak można wykorzystać poznane własności symbolu Legendre'a w dowodzie kilku elementarnych przypadków twierdzenia Dirichlet'a T5.19, objętych lub nie przez twierdzenie T5.20.

P r z y k ł a d 3. Zaczniemy od ciągu arytmetycznego $(4x+1)_{x\in\mathbb{N}}$. Udowodnimy, że *Liczb pierwszych postaci* $4x+1$ *jest nieskończenie wiele*. Rzeczywiście, załóżmy, nie wprost, że $p_1 = 5$, $p_2 = 13$, $\ldots$, p_s są w s z y s t k i m i liczbami pierwszymi postaci $4x+1$ i rozważmy liczbę $N = 4(p_1 p_2 \cdot \ldots \cdot p_s)^2 + 1$. Niech p będzie dowolną liczbą pierwszą dzielącą N. Wówczas $(2p_1 p_2 \cdot \ldots \cdot p_s)^2 \equiv -1 \,(\mathrm{mod}\, p)$, co oznacza, że $(-1)\mathbf{R}p$. Zatem, patrz (5.81), $p \equiv 1 \,(\mathrm{mod}\, 4)$. Jednocześnie $p \neq p_i$ dla $1 \leqslant i \leqslant s$. Sprzeczność. Q.e.d. $\Diamond$

Porównajmy powyższy dowód z dowodami pokazanymi w przykładach P1 i P2 z ustępu 5.5.6. W każdym z nich ważną rolę gra stosownie dobrany wielomian. Wielomianami tymi są odpowiednio $4X^2+1$, $3X+2$ i $4X-1$.

Ćwiczenie 5.75 Udowodnić, że każdy z ciągów: $(5x-1)$, $(8x-1)$, $(12x-1)$, $(12x+7)$ zawiera nieskończenie wiele liczb pierwszych. *Wskazówka.* W dowodzie można wykorzystać wielomiany $20X^2-1$, $8X^2-1$, $12X^2-1$, $4X^2+3$ odpowiednio.

5.7.7 Trójmian kwadratowy modulo p

Zobaczymy teraz jak rozwiązuje się równania kwadratowe w ciałach $\mathbb{Z}/p$.

TWIERDZENIE 5.28 *Niech $p>2$ będzie nieparzystą liczbą pierwszą. Kongruencja*

$$ax^2+bx+c\equiv 0\,(\mathrm{mod}\,p), \tag{5.91}$$

gdzie $p\nmid a$, ma rozwiązanie wtedy i tylko wtedy, gdy $\Delta\equiv 0\,(\mathrm{mod}\,p)$ lub $\Delta\mathbf{R}p$. Tu, tak jak w szkole, $\Delta=b^2-4ac$.

DOWÓD. Mnożąc obie strony przez $4a$ otrzymujemy kongruencję równoważną (!)

$$(2ax+b)^2\equiv\Delta\,(\mathrm{mod}\,p).$$

Stąd wynika nie tylko teza, ale i więcej: jeżeli przez $\sqrt{\Delta}$ oznaczymy dowolny pierwiastek kwadratowy z Δ modulo p, czyli element w $\mathbb{Z}/p$ spełniający warunek $(\sqrt{\Delta})^2\equiv\Delta\,(\mathrm{mod}\,p)$, to rozwiązaniami (5.91) są (porównaj wzory (3.10)):

$$x\equiv(2a)^{-1}(-b\pm\sqrt{\Delta})\,(\mathrm{mod}\,p). \tag{5.92}$$

Zauważmy, że odwrotność $(2a)^{-1}\,(\mathrm{mod}\,p)$ istnieje, bo $p\nmid 2a$. □

Przykład. Znajdziemy wszystkie rozwiązania kongruencji $7x^2-2x+5\equiv 0\,(\mathrm{mod}\,79)$. Najpierw wyznaczamy wyróżnik: $\Delta\equiv 2^2-4\cdot 7\cdot 5\equiv 4-70-70\equiv 4+9+9\equiv 22\,(\mathrm{mod}\,79)$. Następnie sprawdzamy czy $22\mathbf{R}79$:

$$\left(\frac{22}{79}\right)=\left(\frac{2}{79}\right)\left(\frac{11}{79}\right)=(+1)\cdot(-1)\left(\frac{79}{11}\right)=(-1)\left(\frac{2}{11}\right)=+1.$$

Wobec tego istnieje $\sqrt{22}\,(\mathrm{mod}\,79)$. Jak go wyznaczyć? Metoda prób i błędów jest oczywiście dość niepraktyczna (wymaga znajdowania reszt z dzielenia kolejnych kwadratów $1^2,\ldots,38^2$ przez 79). Na szczęście, ponieważ $79\equiv 3\,(\mathrm{mod}\,4)$, możemy powołać się na poniższe zadanie Z5.24. Wynika z niego, że $\sqrt{\Delta}=\sqrt{22}\equiv 22^{20}\equiv 10^{10}\equiv 38\,(\mathrm{mod}\,79)$. Ponieważ, jak łatwo sprawdzić, $14^{-1}\,(\mathrm{mod}\,79)=17\,(\mathrm{mod}\,79)$, więc wzory (5.92) dają nam rozwiązania

$$x_1=17\cdot(2+38)\,(\mathrm{mod}\,79)=48\,(\mathrm{mod}\,79),\qquad x_2=17\cdot(2-38)\,(\mathrm{mod}\,79)=20\,(\mathrm{mod}\,79).$$

Zauważmy, że dostajemy stąd rozkład $7X^2-2X+5\equiv 7(X-48)(X-20)\,(\mathrm{mod}\,79)$ na czynniki liniowe nad ciałem $\mathbb{Z}/79$. ◊

ZADANIE 5.24 Udowodnić, że jeżeli $p = 4k + 3$ jest liczbą pierwszą oraz $d\mathbf{R}p$, to $d^{\frac{p+1}{4}} \equiv \sqrt{d} \,(\mathrm{mod}\, p)$.

Rozwiązanie. Mamy uzasadnić, że $(d^{\frac{p+1}{4}})^2 \equiv d \,(\mathrm{mod}\, p)$. Otóż:

$$\left(d^{\frac{p+1}{4}}\right)^2 = d^{\frac{p+1}{2}} = d^{\frac{p-1}{2}} d \equiv (+1)d \equiv d \,(\mathrm{mod}\, p).$$

Przedostatnia kongruencja wynika z założenia, że $d\mathbf{R}p$ i z kryterium Eulera (5.67). ◊

Ćwiczenie 5.76 Rozłożyć na czynniki nierozkładalne nad ciałami współczynników wielomiany: $3X^2 + 5X - 123 \in \mathbb{F}_{131}[X]$, $X^3 + 5X^2 - 397X + 391 \in \mathbb{F}_{647}[X]$.

Ćwiczenie 5.77 Niech $a \not\equiv 0 \,(\mathrm{mod}\, p)$, gdzie p jest liczbą pierwszą. Udowodnić, że jeżeli $h(X) = aX^2 + bX + c$, to (zobacz oznaczenie w D5.2),

$$N(h;\, p) := 1 + \left(\frac{\Delta}{p}\right).$$

Ćwiczenie 5.78 Dana jest liczba pierwsza $p > 2$. Udowodnić, że poniższe dwa zdania są równoważne: (1) istnieje taka liczba całkowita x, że $p|x^2 + 3x + 7$, (2) istnieje taka liczba całkowita y, że $p|y^2 + 22y + 140$.

5.7.8 Kilka zadań

Pokażemy tu kilka typowych zadań, przy rozwiązaniu których przydatna (niezbędna?) jest wiedza na temat reszt i niereszt kwadratowych modulo p.

ZADANIE 5.25 Niech $h(X) = X^8 - 16$. Udowodnić, że $\mathcal{N}(h;\, p) \neq \varnothing$ dla dowolnej liczby pierwszej.

Rozwiązanie. Mamy rozkład $h(X) = (X^2-2)(X^2+2)(X^2-2X+2)(X^2+2X+2)$, zobacz tożsamość Sophie Germain. Wyróżniki występujących tu czterech trójmianów kwadratowych są równe odpowiednio: $\Delta_1 = 8$, $\Delta_2 = -8$, $\Delta_3 = -4$ i $\Delta_4 = -4$. Jeżeli $p \in \mathbb{P}_{>2}$, to mamy

$$\left(\frac{\Delta_1}{p}\right)\left(\frac{\Delta_2}{p}\right)\left(\frac{\Delta_3}{p}\right) = \left(\frac{\Delta_1\Delta_2\Delta_3}{p}\right) = \left(\frac{(2^4)^2}{p}\right) = +1.$$

Stąd wynika, że co najmniej jeden z symboli $(\Delta_i|p)$ jest równy $+1$. Czyli, co najmniej jeden z trzech trójmianów ma pierwiastek $(\mathrm{mod}\, p)$, więc $\mathcal{N}(h;\, p) \neq \varnothing$ dla nieparzystych $p \in \mathbb{P}$. Jasne jest też, że $0 \,(\mathrm{mod}\, 2) \in \mathcal{N}(h;\, 2)$. ◊

ZADANIE 5.26 Udowodnić, że jeżeli $2^n - 1|3^n - 1$, $n \in \mathbb{N}$, to $n = 1$.

Rozwiązanie. Ponieważ $3|2^n - 1$ dla parzystych n (oczywiście!), więc podzielność $2^n - 1|3^n - 1$ może mieć miejsce tylko, gdy $n \equiv 1 \,(\mathrm{mod}\, 2)$. Niech $p|2^n - 1$ będzie dowolnym dzielnikiem pierwszym. Wtedy $p|3^n - 1$, skąd $1 = (1|p) = (3^n|p) = (3|p)^n = (3|p)$, gdzie trzecia równość wynika z multyplikatywności symbolu Legendre'a, a czwarta – z nieparzystości liczby n. Zatem $3\mathbf{R}p$, czyli, zob. (5.84), $p \equiv \pm 1 \,(\mathrm{mod}\, 12)$. Widzimy zatem, że jeżeli $2^n - 1|3^n - 1$, to wszystkie dzielniki pierwsze liczby $2^n - 1$ są postaci $\pm 1 \,(\mathrm{mod}\, 12)$. Więc i sama liczba $2^n - 1$ jest postaci $\pm 1 \,(\mathrm{mod}\, 12)$. Ale równość $2^n - 1 = 12a + 1$ jest możliwa tylko, gdy $n = 1$ (i $a = 0$), a równość $2^n - 1 = 12b - 1$ w ogóle nie jest możliwa! ◊

ZADANIE 5.27 Załóżmy, że p i $q = 2p + 1$ są liczbami pierwszymi. Udowodnić, że w takiej sytuacji, jeżeli $p \equiv 1 \pmod 4$, to 2 jest pierwiastkiem pierwotnym modulo q, jeżeli zaś $p \equiv 3 \pmod 4$, to -2 jest pierwiastkiem pierwotnym modulo q.

Rozwiązanie. (1) $p = 4k + 1$. Niech $d = \mathrm{rz}_q(2)$. Wówczas, jak to już wiemy od dawna, $d|q-1$, czyli $d|2p$. Wobec tego $d = 1$ lub $d = 2$ lub $d = p$ lub $d = 2p$. Chcemy udowodnić, że $d = \varphi(q) = q - 1 = 2p$. Ponieważ przypadki $d = 1$ i $d = 2$ prowadzą do nonsensownych wniosków $2 \equiv 1 \pmod q$ i $2^2 \equiv 1 \pmod q$, więc pozostaje nam uzasadnić, że nie może zachodzić przypadek $d = p$. Załóżmy więc, nie wprost, że $d = p$. Wówczas

$$\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} = 2^p \equiv 1 \pmod q,$$

gdzie pierwsza kongruencja wynika z kryterium Eulera. Zatem $2\mathbf{R}q$. Ale to jest niemożliwe, bo $q = 2p + 1 = 8k + 3$, zobacz (5.74).

(2) $p = 4k + 3$. Niech $d = \mathrm{rz}_q(-2)$. Podobnie jak przed chwilą odrzucamy możliwości $d = 1$ i $d = 2$. Gdyby zaś $d = p$, to mielibyśmy

$$\left(\frac{-2}{q}\right) \equiv (-2)^{\frac{q-1}{2}} \equiv (-2)^p \equiv 1 \pmod q.$$

Więc $(-2)\mathbf{R}q$. Sprzeczność, bo $q = 2p + 1 = 8k + 7 \equiv 7 \not\equiv 1, 3 \pmod 8$, zobacz (5.83). $\Diamond$

Uwaga 1. Liczba pierwsza p, dla której $2p + 1$ jest również liczbą pierwszą, nazywa się **liczbą pierwszą (Sophie) Germain**. W tabelce na stronie vi, wśród 304 liczb pierwszych znajduje się 59 liczb pierwszych Germain. Z tego 28 przystaje do 1 modulo 4 (największą z nich jest 1973), a 31 przystaje do 3 modulo 4 (największą z ich jest 2003). Nie wiadomo, czy liczb pierwszych Germain jest skończenie czy nieskończenie wiele.

ZADANIE 5.28 Załóżmy, że $p \equiv 3 \pmod 4$ jest liczbą pierwszą Germain. Udowodnić, że $M_p = 2^p - 1$ jest liczbą złożoną.

Rozwiązanie. Ponieważ $q = 2p + 1 = 2(4k + 3) + 1 = 8k + 7$, więc, na mocy II uzupełnienia prawa wzajemności, $2\mathbf{R}q$. Niech $a^2 \equiv 2 \pmod q$. Wówczas, dzięki MTF,

$$1 \equiv a^{q-1} \equiv a^{2p} \equiv (a^2)^p \equiv 2^p \pmod q.$$

Zatem $q|M_p$, więc M_p ma dzielnik właściwy, bo $q = 2p + 1 < 2^p - 1$ dla $p > 3$. $\Diamond$

Uwaga 2. Wiemy, że $M_n = 2^n - 1$ może być liczbą pierwszą tylko w przypadku, gdy n jest liczbą pierwszą, zobacz 2.3.3 P3. Ponieważ $p = 11$ jest liczbą pierwszą spełniającą założenia zadania Z5.27, więc widzimy, że $23|M_{11}$. To widzieliśmy już w 2.3.3 P3. Teraz jesteśmy w stanie udowodnić, że $4007|M_{2003}$. Czy umielibyśmy przekonać się o tym "na piechotę"?

ZADANIE 5.29 Wyznaczyć najmniejszą liczbę pierwszą p, dla której zachodzą równości

$$p = s^2 + t^2 = u^2 + 2v^2 = w^2 + 3x^2 = y^2 + 5z^2 \tag{5.93}$$

przy pewnych całkowitych s, t, u, v, w, x, y, z.

R o z w i ą z a n i e. Zauważmy najpierw, że jeżeli dla liczb całkowitych a, b i d zachodzi równość $p = a^2 + db^2$, to $p \nmid b$. Istotnie, gdyby $p|b$, to, na mocy zasady podstawowej, $p|a$ i zachodziłaby nonsensowna równość $p = p^2(a'^2 + db'^2)$. Wobec tego, patrz T5.5, istnieje odwrotność $b^{-1} \,(\mathrm{mod}\, p)$. Wówczas $(ab^{-1})^2 \equiv -d \,(\mathrm{mod}\, p)$, więc $(-d)\mathbf{R}p$.

Widzimy stąd, że jeśli zachodzą równości (5.93), to $(-1)\mathbf{R}p$, $(-2)\mathbf{R}p$, $(-3)\mathbf{R}p$, $(-5)\mathbf{R}p$, czyli, patrz (5.81), (5.83), (5.85), (5.87),

$$p \equiv 1 \,(\mathrm{mod}\, 4), \quad p \equiv 1,\, 3 \,(\mathrm{mod}\, 8), \quad p \equiv 1,\, 7 \,(\mathrm{mod}\, 12), \quad p \equiv 1,\, 3,\, 7,\, 9 \,(\mathrm{mod}\, 20).$$

Ponieważ, $8k + 3 = 4(2k) + 3$, $12k + 7 = 4(3k + 1) + 3$, $20k + 3 = 4(5k) + 3$ oraz $20k + 7 = 4(5k + 1) + 3$, więc z szesnastu powyższych możliwości zostają tylko dwie:

$$(\mathbf{1}) \quad \begin{cases} p \equiv 1 \,(\mathrm{mod}\, 4) \\ p \equiv 1 \,(\mathrm{mod}\, 8) \\ p \equiv 1 \,(\mathrm{mod}\, 12) \\ p \equiv 1 \,(\mathrm{mod}\, 20) \end{cases} \qquad (\mathbf{2}) \quad \begin{cases} p \equiv 1 \,(\mathrm{mod}\, 4) \\ p \equiv 1 \,(\mathrm{mod}\, 8) \\ p \equiv 1 \,(\mathrm{mod}\, 12) \\ p \equiv 9 \,(\mathrm{mod}\, 20) \end{cases}$$

Oba te układy kongruencji mają rozwiązania, zobacz T5.9. Pierwszy układ jest przy tym równoważny kongruencji $p \equiv 1 \,(\mathrm{mod}\, 120)$, a drugi, kongruencji $p \equiv 49 \,(\mathrm{mod}\, 120)$. Najmniejszą liczbą pierwszą spełniającą (**1**) jest $p = 241$, a najmniejszą liczbą pierwszą spełniającą (**2**) jest $p = 409$. Sprawdzimy jeszcze, że spełnione są warunki (5.93). Otóż:

$$241 = 4^2 + 15^2 = 13^2 + 2 \cdot 6^2 = 7^2 + 3 \cdot 8^2 = 14^2 + 5 \cdot 3^2,$$
$$409 = 3^2 + 20^2 = 11^2 + 2 \cdot 12^2 = 19^2 + 3 \cdot 4^2 = 2^2 + 5 \cdot 9^2.$$

Ponieważ $\min\{241,\, 409\} = 241$, więc odpowiedzią jest: $p = 241$. $\Diamond$

ZADANIE 5.30 Udowodnić, że istnieje nieskończenie wiele takich liczb pierwszych p, dla których najmniejszy dodatni pierwiastek pierwotny $(\mathrm{mod}\, p)$ jest większy niż 2017.

R o z w i ą z a n i e. Niech $q_1 = 2$, $q_2 = 3$, $\ldots$, $q_s = 2017$ będą wszystkimi liczbami pierwszymi $\leqslant 2017$. Dzięki T5.20 wiemy, że istnieje nieskończenie wiele liczb pierwszych postaci $4q_1q_2 \cdot \ldots \cdot q_s x + 1$. Twierdzimy, że jeżeli p jest taką liczbą, to żadna liczba $1 \leqslant h \leqslant 2017$ nie jest pierwiastkiem pierwotnym $(\mathrm{mod}\, p)$. Rzeczywiście,

$$\left(\frac{q_j}{p}\right) = \left(\frac{p}{q_j}\right) = \left(\frac{4q_1q_2 \cdot \ldots \cdot q_s x + 1}{q_j}\right) = \left(\frac{1}{q_j}\right) = +1,$$

zob. 5.7.5 U2. Rozkładając liczbę naturalną $h \leqslant 2017$ na iloczyn liczb pierwszych, dostajemy równość $h = \prod_{j=1}^{s} q_j^{e_j}$. Stąd, na mocy multyplikatywności symbolu Legendre'a, $(h|p) = +1$. Każda więc liczba naturalna $h \leqslant 2017$ jest resztą kwadratową $(\mathrm{mod}\, p)$. Ale reszta kwadratowa modulo p nie może być pierwiastkiem pierwotnym modulo p (dlaczego?). $\Diamond$

U w a g a 3. W naszej tabelce liczb pierwszych obok każdej liczby pierwszej p pokazujemy najmniejszy (dodatni) pierwiastek pierwotny $(\mathrm{mod}\, p$. W Z5.30 pokazaliśmy więc, że gdzieś w dostatecznie obszernym rozszerzeniu takiej tabelki znajdzie się $g \geqslant 2017$. Z drugiej strony istnieje h i p o t e z a, że wartość $g = 2$ występuje nieskończenie wiele razy.

Ćwiczenie 5.79 Załóżmy, że p i $q = 4p + 1$ są liczbami pierwszymi. Udowodnić, że w takiej sytuacji 2 jest pierwiastkiem pierwotnym modulo q.

U w a g a 4. W naszej tabelce na stronie vi można znaleźć pary $(p, 4p + 1)$. Na przykład:

$$(3, 13),\ (7, 29),\ (13, 53),\ (37, 149),\ (67, 269),\ (79, 317),\ \ldots\ ,\ (487, 1949).$$

Ćwiczenie 5.80 Niech $a, b, x, y \in \mathbb{Z}$ będą takie, że $\mathrm{NWD}\,(ax, by) = 1$. Dana jest liczba pierwsza p. Załóżmy, że $p|ax^2 + by^2$. Udowodnić, że w takim przypadku $(-ab)\mathbf{R}p$.

Ćwiczenie 5.81 Załóżmy, że $p = 2^{2^n} + 1$ jest liczbą pierwszą Fermat'*a*. Udowodnić, że 7 jest pierwiastkiem pierwotnym $(\mathrm{mod}\, p)$. *Wskazówka.* Z 5.7.3 P2 wiemy, że wystarczy uzasadnić zachodzenie równości $(7|p) = -1$.

Ćwiczenie 5.82 Dowieść, że jeżeli p jest liczbą pierwszą postaci $8t + 5$, to ani liczba $(p - 1)! + 1$ ani liczba $(p - 3)! + 1$ nie są kwadratami (liczb całkowitych).

5.7.9 Liczba lokalnie kwadratowa jest kwadratem (globalnym)

Oczywiste jest, że jeżeli liczba całkowita c jest kwadratem (liczby całkowitej), $c = a^2$, to dla każdego modułu $m \in \mathbb{N}$ warstwa $c\,(\mathrm{mod}\, m)$ jest kwadratem w pierścieniu $\mathbb{Z}/m$. Chcemy teraz udowodnić twierdzenie odwrotne: *Jeżeli* $c\,(\mathrm{mod}\, m)$ *jest kwadratem w* $\mathbb{Z}/m$ *dla każdego* m, *to* c *jest kwadratem w* $\mathbb{Z}$.

Zaczniemy od zadania:

ZADANIE 5.31 Dana jest liczba całkowita postaci $c = \pm 2a^2$, $a \neq 0$. Udowodnić, że istnieje nieskończenie wiele takich liczb pierwszych p, że $p \nmid c$ i $c\mathbf{N}p$.

R o z w i ą z a n i e. Każda liczba pierwsza $p \equiv 5\,(\mathrm{mod}\, 8)$, nie będąca dzielnikiem a, jest dobra. Rzeczywiście, jeżeli p jest taką liczbą, to

$$\left(\frac{c}{p}\right) = \left(\frac{\pm 2a^2}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{a}{p}\right)^2 = -1,$$

bo pierwszy czynnik jest równy $+1$ (bez względu na wybór znaku: $(1|p) = 1$ zawsze, a $(-1|p) = 1$ dla liczb pierwszych postaci $8k+5 = 4(2k+1)+1$, zob. (5.68)), drugi czynnik jest równy -1, zob. (5.74), a trzeci (jako kwadrat) jest równy $+1$. Trzeba jeszcze uzasadnić, że *istnieje nieskończenie wiele liczb pierwszych postaci* $8x + 5$. Można się powołać na twierdzenie Dirichlet'*a* T5.19. Można też rozumować podobnie jak w C5.75: Weźmy wielomian $X^2 + 4$ i jego wartość $N = (p_1 p_2 \cdot \ldots \cdot p_s)^2 + 4$, gdzie $p_1 = 5$, $p_2 = 13$, $\ldots$, p_s są kolejnymi liczbami pierwszymi postaci $8x + 5$. Oznaczmy na chwilę $A = p_1 p_2 \cdot \ldots \cdot p_s$ i niech $p|N$ będzie dowolnym dzielnikiem pierwszym. Wówczas $A^2 \equiv -4\,(\mathrm{mod}\, p)$, skąd $(2^{-1}A)^2 \equiv -1\,(\mathrm{mod}\, p)$. Więc $(-1)\mathbf{R}p$, czyli $p = 4k + 1$, zob. (5.68). Sprawdziliśmy w ten sposób, że w s z y s t k i e dzielniki pierwsze liczby N są postaci $8x + 1$ lub $8x + 5$. Gdyby wszystkie te dzielniki były postaci $8x + 1$, to ich iloczyn również byłby tej postaci. Ale n i e jest (bo nieparzysty kwadrat A^2 przystaje do $1\,(\mathrm{mod}\, 8)$). Wobec tego $p = 8x + 5$. I mamy nową liczbę pierwszą takiej postaci. ◊

Twierdzenie o globalności kwadratów lokalnych łatwo wywiedziemy z poniższego:

TWIERDZENIE 5.29 *Jeżeli liczba całkowita $c \neq 0$ nie jest kwadratem w pierścieniu $\mathbb{Z}$, to istnieje taka liczba pierwsza p, że $p \nmid c$ i $c\mathbf{N}p$.*

D O W Ó D. Niech c nie będzie kwadratem (w $\mathbb{Z}$). Wówczas, albo c jest postaci $\pm 2a^2$ i wtedy Z5.30 załatwia sprawę, albo ma rozkład na czynniki postaci

$$c = \pm 2^\alpha a^2 q_1 \cdot \ldots \cdot q_s,$$

gdzie $s \geqslant 1$, a $q_1, \ldots, q_s$ są nieparzystymi dzielnikami pierwszymi. Oznaczmy przez b dowolną niereszte kwadratową $(\mathrm{mod}\, q_1)$. I niech d będzie taką liczbą całkowitą, że

$$\begin{cases} d \equiv 1 \,(\mathrm{mod}\, 8), \\ d \equiv b \,(\mathrm{mod}\, q_1), \\ d \equiv 1 \,(\mathrm{mod}\, q_2), \\ \quad \ldots \quad \ldots \\ d \equiv 1 \,(\mathrm{mod}\, q_s). \end{cases}$$

Taka liczba d istnieje na mocy CTR. Na mocy zaś twierdzenia Dirichlet'a, istnieje nieskończenie wiele liczb pierwszych p postaci $8q_1 \cdot \ldots \cdot q_s x + d$. Twierdzimy, że każda z nich jest dobra (dla naszych celów). Rzeczywiście, na mocy multyplikatywności symbolu Legendre'a, mamy

$$\left(\frac{c}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^\alpha \left(\frac{a^2}{p}\right)\left(\frac{q_1}{p}\right) \cdot \ldots \cdot \left(\frac{q_s}{p}\right).$$

Pierwszy czynnik jest równy $+1$, bo $p \equiv 1 \,(\mathrm{mod}\, 4)$, zob. I uzupełnienie PWRK, drugi czynnik jest równy $(+1)^\alpha = +1$, bo $p \equiv 1 \,(\mathrm{mod}\, 8)$, zob. II uzupełnienie PWRK, trzeci czynnik jest równy $+1$, bo jest kwadratem $(a|p)^2$ liczby ± 1, zob. W1T5.24. Dla pozostałych czynników mamy równości $(q_j|p) = (p|q_j)$, bo $p \equiv 1 \,(\mathrm{mod}\, 4)$, zob. 5.7.5 U2. Wobec tego

$$\left(\frac{c}{p}\right) = \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right) \cdot \ldots \cdot \left(\frac{p}{q_s}\right) = \left(\frac{d}{q_1}\right)\left(\frac{d}{q_2}\right) \cdot \ldots \cdot \left(\frac{d}{q_s}\right) = \left(\frac{b}{q_1}\right)\left(\frac{1}{q_2}\right) \cdot \ldots \cdot \left(\frac{1}{q_s}\right) = -1,$$

bo $b\mathbf{N}q_1$ i, oczywiście, $1\mathbf{R}q_j$. □

Ćwiczenie 5.83 Niech $a, b, c \in \mathbb{Z}$ i $a \neq 0$. Uzasadnić, że równanie $ax^2 + bx + c = 0$ ma pierwiastek wymierny wtedy i tylko wtedy, gdy kongruencja $ax^2 + bx + c \equiv 0 \,(\mathrm{mod}\, p)$ ma rozwiązania dla w s z y s t k i c h liczb pierwszych p z wyjątkiem być może skończonej ich ilości.

5.8 Kongruencje modulo p^n. Liczby p-adyczne

Udowodnimy teraz ważne i ciekawe twierdzenie o podnoszeniu pierwiastków kongruencji wielomianowych z $\mathbb{Z}/p$ do $\mathbb{Z}/p^n$. Zaczniemy od definicji ogólnej:

Definicja 5.14 Niech $f(X) \in \mathbb{Z}[X]$. I niech $m|m'$. Jeżeli c jest rozwiązaniem kongruencji $f(x) \equiv 0 \,(\mathrm{mod}\, m)$, a d jest takim rozwiązaniem kongruencji $f(x) \equiv 0 \,(\mathrm{mod}\, m')$, że $c \equiv d \,(\mathrm{mod}\, m)$, to mówimy, że d jest **podniesieniem rozwiązania c z $\mathbb{Z}/m$ do $\mathbb{Z}/m'$**.

P r z y k ł a d. $3 \,(\mathrm{mod}\, 7)$ jest p i e r w i a s t k i e m k w a d r a t o w y m z $2 \,(\mathrm{mod}\, 7)$ (czyli rozwiązaniem kongruencji $x^2 \equiv 2 \,(\mathrm{mod}\, 7)$). Jego podniesieniem do $\mathbb{Z}/49$ jest $10 \,(\mathrm{mod}\, 49)$. Kongruencja $x^2 \equiv 2 \,(\mathrm{mod}\, 7)$ ma jeszcze jedno rozwiązanie: $4 \,(\mathrm{mod}\, 7)$. Jego podniesieniem do $\mathbb{Z}/49$ jest $39 \,(\mathrm{mod}\, 49)$. Rozwiązania $3 \,(\mathrm{mod}\, 7)$ n i e d a s i ę p o d n i e ś ć do $\mathbb{Z}/21$. Istotnie, kongruencja $x^2 \equiv 2 \,(\mathrm{mod}\, 21)$ w ogóle nie ma rozwiązań (dlaczego?). ◊

5.8.1 Reszty kwadratowe modulo p^n

Zaczniemy od zbadania podniesień pierwiastków kwadratowych z $\mathbb{Z}/p$ do $\mathbb{Z}/p^n$, $n > 1$.

TWIERDZENIE 5.30 *Niech $p > 2$ będzie liczbą pierwszą i niech $p \nmid a$. Kongruencja*

$$x^2 \equiv a \,(\mathrm{mod}\, p^n), \tag{5.94}$$

przy $n \geqslant 1$, ma rozwiązania wtedy i tylko wtedy, gdy $a\mathbf{R}p$.

DOWÓD. Jeżeli $a\mathbf{R}p^n$ i $c^2 \equiv a \,(\mathrm{mod}\, p^n)$, to, oczywiście, $c^2 \equiv a \,(\mathrm{mod}\, p)$, więc $a\mathbf{R}p$. Wynikanie przeciwne jest trudniejsze. Aby przekonać się o jego prawdziwości pokażemy teraz efektywną metodę znajdowania rozwiązania kongruencji

$$x^2 \equiv a \,(\mathrm{mod}\, p^{n+1}), \tag{5.95}$$

jeżeli znamy rozwiązanie kongruencji (5.94). Załóżmy więc, że c jest rozwiązaniem (5.94), czyli, że $c^2 = a + p^n b$ przy pewnym $b \in \mathbb{Z}$. Twierdzimy, że wówczas istnieje takie $t \in \mathbb{Z}$, że $d = c + tp^n$ jest rozwiązaniem (5.95). Istotnie, ponieważ dla d postaci $c + tp^n$ mamy

$$d^2 = (c + tp^n)^2 = c^2 + 2ctp^n + t^2p^{2n} = a + p^n(b + 2ct) + t^2p^{2n},$$

więc wystarczy znaleźć takie $t \in \mathbb{Z}$, żeby $b + 2ct \equiv 0 \,(\mathrm{mod}\, p)$ (co jest możliwe, bo liczba $2c$, jako względnie pierwsza z p, jest odwracalna modulo p). Wówczas $d^2 \equiv a \,(\mathrm{mod}\, p^{n+1})$. □

Ćwiczenie 5.84 Udowodnić, że jeżeli $a\mathbf{R}p$, to kongruencja (5.94) (przy $p > 2$) ma dokładnie dwa rozwiązania.

Ćwiczenie 5.85 Znaleźć rozwiązania kongruencji $x^2 \equiv 11 \,(\mathrm{mod}\, 625)$.

Ćwiczenie 5.86 Dana jest nieparzysta liczba pierwsza p. Udowodnić, że w grupie $(\mathbb{Z}/p^n)^*$, $n \in \mathbb{N}$, jest tyle samo reszt co niereszt kwadratowych.

Zobaczymy teraz czy da się podnieść pierwiastki kwadratowe w przypadku, gdy $p = 2$. Rzecz jest w tym przypadku nieco bardziej skomplikowana: na przykład 3 jest resztą kwadratową modulo 2, ale nie jest resztą kwadratową modulo 4. Zachodzi jednak

TWIERDZENIE 5.31 *Niech $2 \nmid a$. Wówczas kongruencja*

$$x^2 \equiv a \,(\mathrm{mod}\, 2^n), \tag{5.96}$$

przy $n \geqslant 3$, ma rozwiązania wtedy i tylko wtedy, gdy $a\mathbf{R}8$.

DOWÓD. Zastosujemy technikę podobną do wyżej opowiedzianej. Załóżmy w tym celu, że $c^2 \equiv a \,(\mathrm{mod}\, 2^n)$, $n \geqslant 3$, czyli że $c^2 = a + 2^n b$ i poszukajmy rozwiązania kongruencji $x^2 \equiv a \,(\mathrm{mod}\, 2^{n+1})$ w postaci $d = c + 2^{n-1}t$. Ponieważ wówczas

$$d^2 = (c + 2^{n-1}t)^2 = c^2 + 2^n ct + 2^{2n-2}t^2 = a + 2^n(b + ct) + 2^{n+1} \cdot \text{coś},$$

bo $2n - 2 \geqslant n + 1$, więc wystarczy znaleźć takie t, by $b + ct \equiv 0 \,(\mathrm{mod}\, 2)$. To jest możliwe, bo c jest nieparzyste (dlaczego?). Dowód jest zakończony. □

Ćwiczenie 5.87 Niech $a\mathbf{R}8$ (w szczególności $2 \nmid a$). Udowodnić, że wówczas kongruencja (5.96) ma cztery rozwiązania dla każdego $n \geqslant 3$.

Ćwiczenie 5.88 Udowodnić, że kongruencja $x^2 \equiv 1 \,(\mathrm{mod}\, m)$ ma dokładnie dwa rozwiązania wtedy i tylko wtedy, gdy $m = 4$ albo $m = p^n$, $p > 2$, albo $m = 2p^n$, $p > 2$.

5.8.2 Lemat Hensela

Dowód twierdzenia, które chcemy teraz udowodnić, jest uogólnieniem dowodu T5.30.

Ćwiczenie 5.89 Udowodnić, że dla dowolnego wielomianu $f(X) \in \mathbb{Z}[X]$ istnieje taki wielomian dwóch zmiennych $r(X, Y) \in \mathbb{Z}[X, Y]$, że dla dowolnych liczb x i h zachodzi równość $f(x+h) = f(x) + f'(x) \cdot h + r(x, h) \cdot h^2$. *Wskazówka.* Zapoznać się z D6.1.

TWIERDZENIE 5.32 (***Lemat Hensela***) *Dany jest wielomian $f(X) \in \mathbb{Z}[X]$ i liczba pierwsza p. Załóżmy, że istnieje liczba całkowita a_0 spełniająca warunki $f(a_0) \equiv 0 \pmod p$ i $f'(a_0) \not\equiv 0 \pmod p$. Wówczas istnieje taki ciąg nieskończony $(a_0, a_1, a_2, \ldots, a_n, \ldots)$ liczb całkowitych, że*

$$f(a_n) \equiv 0 \pmod{p^{n+1}} \qquad i \qquad a_n \equiv a_{n-1} \pmod{p^n} \tag{5.97}$$

dla każdego $n \in \mathbb{N}$. Ponadto, jeżeli ciąg $(b_n)_{n\geqslant 0}$ również spełnia te warunki i $b_0 \equiv a_0 \pmod p$, to $b_n \equiv a_n \pmod{p^{n+1}}$ dla każdego $n \in \mathbb{N}$.

D O W Ó D. Poszukajmy najpierw liczby a_1. Ponieważ chcemy by $a_1 \equiv a_0 \pmod p$, więc szukamy a_1 w postaci $a_0 + tp$. Z C5.89 mamy równość

$$f(a_0 + tp) = f(a_0) + f'(a_0) \cdot tp + r(a_0, tp) \cdot t^2 p^2.$$

Z założenia mamy $f(a_0) = cp$ dla pewnej liczby całkowitej c. Widzimy stąd, że dobierając takie $t \in \mathbb{Z}$, by $p|(c + tf'(a_0))$, znajdziemy liczbę $a_1 := a_0 + tp$, dla której $f(a_1) \equiv 0 \pmod{p^2}$. Istnienie (i jednoznaczność modulo p) stosownego t wynika natychmiast z T5.5 (kongruencja $f'(a_0)t \equiv -c \pmod p$ ma dokładnie jedno rozwiązanie, bo $f'(a_0) \not\equiv 0 \pmod p$).

Równie łatwo wykonać krok indukcyjny z n na $n+1$. Rzeczywiście, mając $a_1, \ldots, a_n$ spełniające warunki (5.97) poszukujemy a_{n+1} w postaci $a_n + tp^{n+1}$. Ponieważ

$$f(a_n + tp^{n+1}) = f(a_n) + f'(a_n) \cdot tp^{n+1} + r(a_n, tp^{n+1}) \cdot t^2 p^{2n+2},$$

a $f(a_n) = cp^{n+1}$ dla pewnego $c \in \mathbb{Z}$, więc (tak jak wyżej, bowiem $f'(a_n) \equiv f'(a_0) \pmod p$, zobacz T5.2) widzimy, że istnieje takie $t \in \mathbb{Z}$, że $f(a_n + tp^{n+1}) \equiv 0 \pmod{p^{n+2}}$. Dowód istnienia ciągu (a_n) został zakończony. Dowód jednoznaczności zostawiamy Czytelnikowi. □

Ćwiczenie 5.90 Kongruencja $x^2 + x + 5 \equiv 0 \pmod 7$ ma dwa rozwiązania modulo 7. Podnieść je do rozwiązań w $\mathbb{Z}/343$.

P r z y k ł a d. Rozważmy trójmian kwadratowy $f(X) = X^2 + X + 2$. Ma on pierwiastek $3 \pmod 7$ w $\mathbb{Z}/7$. Poszukamy pierwiastków tego trójmianu modulo 49. Jeżeli c jest takim pierwiastkiem, to $c^2+c+2 \equiv 0 \pmod{49}$. Wówczas oczywiście $c^2+c+2 \equiv 0 \pmod 7$. Ale $f(X)$ ma t y l k o j e d e n pierwiastek $\pmod 7$. Łatwo to sprawdzić. [Jest to związane z faktem, że $\Delta = 1^2 - 4 \cdot 2 \equiv 0 \pmod 7$, zob. T5.28.] Zatem $c = 3 + 7t$ dla pewnego $t \in \mathbb{Z}$. Jednakże

$$f(3 + 7t) = (3 + 7t)^2 + (3 + 7t) + 2 \equiv 49t^2 + 49t + 14 \equiv 14 \pmod{49},$$

więc widzimy, że trójmian $f(X)$ n i e ma pierwiastków w $\mathbb{Z}/49$. Tym bardziej więc nie ma on pierwiastków w $\mathbb{Z}/7^k$ dla $k > 2$. Oczywiście nie jest to sprzeczne z lematem Hensela, ponieważ

$f'(3) = 2 \cdot 3 + 1 \equiv 0 \,(\mathrm{mod}\, 7)$. Klasa $3 \,(\mathrm{mod}\, 7)$ jest pierwiastkiem podwójnym trójmianu $f(X)$. Mamy bowiem $f(X) \equiv (X-3)^2 \,(\mathrm{mod}\, 7)$. $\Diamond$

Przypadkiem szczególnym lematu Hensela jest teza poniższego ćwiczenia (Czytelnik powinien się zastanowić, jakie znaczenie ma warunek $p \nmid r$):

Ćwiczenie 5.91 Niech p będzie liczbą pierwszą, r liczbą naturalną niepodzielną przez p. Niech też $p \nmid a$. Udowodnić, że jeżeli kongruencja $x^r \equiv a \,(\mathrm{mod}\, p)$ ma rozwiązania, to przy dowolnym $n \in \mathbb{N}$ kongruencja $x^r \equiv a \,(\mathrm{mod}\, p^n)$ ma rozwiązania.

Gdy $r = p$, mamy takie ćwiczenie, które rozwiązuje się analogicznie do znanego nam już przypadku $p = 2$:

Ćwiczenie 5.92 Niech $p \nmid a$. Wówczas rozwiązalność kongruencji $x^p \equiv a \,(\mathrm{mod}\, p^3)$ jest warunkiem koniecznym i wystarczającym rozwiązalności kongruencji $x^p \equiv a \,(\mathrm{mod}\, p^n)$ dla wszystkich $n \geqslant 3$.

5.8.3 Jedno interesujące zadanie

Jeśli liczba całkowita c jest pierwiastkiem wielomianu $h(X) \in \mathbb{Z}[X]$, to (warstwa) $c \,(\mathrm{mod}\, m)$ jest pierwiastkiem redukcji $\overline{h}(X) = h \,(\mathrm{mod}\, m)(X)$ tego wielomianu dla dowolnego modułu m, czyli, równoważnie, c jest rozwiązaniem kongruencji

$$h(x) \equiv 0 \,(\mathrm{mod}\, m)$$

dla dowolnego modułu $m \in \mathbb{N}$. To jest oczywiste. Wynikanie odwrotne jest n i e p r a w d z i w e. Najprostszy kontrprzykład pokazaliśmy w 5.4.4 P2. Dotyczył on wielomianu postaci $h(X) = pqX^2 + (p-q)X - 1$, gdzie p, q są różnymi liczbami pierwszymi. Czytelnik z łatwością uogólni rozumowanie z 5.4.4 P2 i wykaże, że wszystkie takie wielomiany $h(X)$ również dostarczają kontrprzykładów. Kontrprzykład innego typu znajdujemy w zadaniu:

ZADANIE 5.32 Niech $h(X) = X^6 + 19X^4 + 56X^2 - 196$. Udowodnić, że kongruencja

$$h(x) \equiv 0 \,(\mathrm{mod}\, m) \tag{5.98}$$

ma rozwiązania dla każdego $m \in \mathbb{N}$, a równanie $h(x) = 0$ nie ma pierwiastków całkowitych.

R o z w i ą z a n i e. (0) Sprawdzamy najpierw, że $h(X) = (X^2-2)(X^2+7)(X^2+14)$. Widzimy stąd, że równanie $h(x) = 0$ nie ma rozwiązań całkowitych.

(1) Rozwiązaniem kongruencji (5.98) przy $m = 2^e$, $e \leqslant 3$, jest $x = 1$. To wynika z oczywistej kongruencji $1^2 + 7 \equiv 0 \,(\mathrm{mod}\, 8)$. Twierdzenie T5.31 poucza nas więc, że $(-7)\mathbf{R}2^e$ przy każdym $e \in \mathbb{N}$. Wobec tego, dla każdego $e \in \mathbb{N}$ istnieje $x \in \mathbb{Z}$ spełniające warunek $x^2 + 7 \equiv 0 \,(\mathrm{mod}\, 2^e)$, zatem i $h(x) \equiv 0 \,(\mathrm{mod}\, 2^e)$.

(2) Sprawdzamy, że $h(3) \equiv 0 \,(\mathrm{mod}\, 7)$ i $h'(3) \equiv 3 \,(\mathrm{mod}\, 7)$. To, na mocy lematu Hensela, pokazuje, że dla każdego $e \in \mathbb{N}$ istnieje $x \in \mathbb{Z}$ spełniające warunek $h(x) \equiv 0 \,(\mathrm{mod}\, 7^e)$.

(3) Niech teraz p będzie liczbą pierwszą $\neq 2, 7$. Wówczas, dzięki multyplikatywności symbolu Legendre'a, mamy $(-14|p) = (-7|p) \cdot (2|p)$. Stąd widzimy, że jeżeli $(-14)\mathbf{N}p$ i $(-7)\mathbf{N}p$, to $2\mathbf{R}p$. Zatem dla każdej liczby pierwszej $p \neq 2, 7$ istnieje takie $x \in \mathbb{Z}$, że co najmniej jeden z czynników $x^2 - 2$, $x^2 + 7$, $x^2 + 14$ przystaje do 0 modulo p. Stąd, na mocy

T5.30, dla każdego $e \in \mathbb{N}$ istnieje takie $x \in \mathbb{Z}$, że $x^2 - 2 \equiv 0 \,(\mathrm{mod}\, p^e)$ lub $x^2 + 7 \equiv 0 \,(\mathrm{mod}\, p^e)$ lub $x^2 + 14 \equiv 0 \,(\mathrm{mod}\, p^e)$, czyli $h(x) \equiv 0 \,(\mathrm{mod}\, p^e)$.

(4) Widzimy z powyższego, że kongruencja (5.98) ma rozwiązania przy każdym m będącym potęgą liczby pierwszej. Wniosek WT5.13 pozwala więc zakończyć rozwiązanie. $\Diamond$

Ćwiczenie 5.93 Czy kongruencja $x^6 + 13x^4 - 45x^2 - 225 \equiv 0 \,(\mathrm{mod}\, m)$ jest rozwiązalna przy dowolnym module m?

Ćwiczenie 5.94 Udowodnić, że jeżeli $p \neq q$ są różnymi liczbami pierwszymi, to kongruencja $pqxy + 1 \equiv px + qy \,(\mathrm{mod}\, m)$ ma rozwiązania dla dowolnego modułu m.

5.8.4 Dwa słowa o liczbach p-adycznych

Wykorzystamy to miejsce dla przytoczenia definicji tak zwanych liczb p-adycznych. Liczby p-adyczne wymyślił Kurt Hensel w roku 1897. Więcej można o tym poczytać w [**7**] i [**9**].

Ciąg $\boldsymbol{c} = (c_0, c_1, c_2, \dots)$ liczb całkowitych nazywamy **nitką p-adyczną**, gdy dla dowolnego $n \in \mathbb{N}$ zachodzi $c_n \equiv c_{n-1} \,(\mathrm{mod}\, p^n)$. Dla danych nitek $\boldsymbol{c} = (c_0, c_1, c_2, \dots)$ i $\boldsymbol{d} = (d_0, d_1, d_2, \dots)$ piszemy $\boldsymbol{c} \sim \boldsymbol{d}$, gdy dla każdego $n \in \mathbb{Z}_{\geqslant 0}$ zachodzi $c_n \equiv d_n \,(\mathrm{mod}\, p^n)$.

Ćwiczenie 5.95 Udowodnić, że tak określona relacja $\sim$ jest relacją równoważności.

Definicja 5.15 Klasę równoważności relacji $\sim$ nazywamy **liczbą całkowitą p-adyczną**. Zbiór liczb p-adycznych całkowitych oznaczamy $\mathbb{Z}_p$.

Liczby p-adyczne dodajemy i mnożymy wyraz po wyrazie:

$$[c_0, c_1, c_2, \dots] + [d_0, d_1, d_2, \dots] := [c_0 + d_0, c_1 + d_1, c_2 + d_2, \dots],$$
$$[c_0, c_1, c_2, \dots] \cdot [d_0, d_1, d_2, \dots] := [c_0 d_0, c_1 d_1, c_2 d_2, \dots].$$

Ćwiczenie 5.96 Udowodnić, że przy takich działaniach zbiór $\mathbb{Z}_p$ jest pierścieniem przemiennym z jedynką bez dzielników zera. *Wskazówka.* Zerem w $\mathbb{Z}_p$ jest liczba p-adyczna $0 := [0, 0, 0, \dots]$, a jedynką jest liczba p-adyczna $1 := [1, 1, 1, \dots]$.

Ćwiczenie 5.97 Dany jest wielomian $f(X) \in \mathbb{Z}[X]$ i liczba p-adyczna $\alpha = [(c_k)]$. Udowodnić, że ciąg $(f(c_0), f(c_1), f(c_2), \dots)$ jest nitką p-adyczną. Jej klasę równoważności oznaczamy $f(\alpha)$ i nazywamy **wartością wielomianu** $f(X)$ dla argumentu $\alpha \in \mathbb{Z}_p$.

Powyższe ćwiczenie mówi, że wielomian $f(X) \in \mathbb{Z}[X]$ wyznacza funkcję

$$f : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p.$$

Lemat Hensela mówi w tym kontekście, że (przy stosownych założeniach) można znaleźć rozwiązanie równania wielomianowego $f(x) = 0$ w pierścieniu $\mathbb{Z}_p$ nawet gdy wielomian $f(X)$ nie ma pierwiastków całkowitych. Istnieją (co najmniej) dwa powody, dla których szukamy pierwiastków równania wielomianowego $f(x) = 0$ w (większym niż $\mathbb{Z}$) pierścieniu $\mathbb{Z}_p$:

- Jeżeli $f(\alpha) = 0$ dla $\alpha = [(c_n)] \in \mathbb{Z}_p$, to mamy za jednym zamachem rozwiązania kongruencji $f(x) \equiv 0 \,(\mathrm{mod}\, p^n)$ dla wszystkich $n \in \mathbb{N}$ (bo $f(c_n) \equiv 0 \,(\mathrm{mod}\, p^n)$).
- Pierścień $\mathbb{Z}_p$ ma własność **zupełności**, która pozwala na stosowanie metod analizy matematycznej (szukanie rozwiązań przybliżonych i przechodzenie do granicy) dla wyznaczania pierwiastków.

My pokażemy tylko, w jaki sposób oblicza się odległość między liczbami p-adycznymi. W rozdziale 2 zdefiniowaliśmy funkcję $v_p : \mathbb{Z} \longrightarrow \mathbb{Z}_{\geqslant 0} \cup \{+\infty\}$ wykładnika p-adycznego. Funkcję tę przedłużamy do funkcji $v_p : \mathbb{Z}_p \longrightarrow \mathbb{Z}_{\geqslant 0} \cup \{+\infty\}$ za pomocą przepisu:

$$v_p([(c_n)]) := \lim_{n\to\infty} v_p(c_n). \tag{5.99}$$

Ćwiczenie 5.98 Udowodnić, że jeżeli $\alpha = [(c_n)]$ jest różną od 0 liczbą całkowitą p-adyczną, to ciąg $(v_p(c_n))$ przyjmuje od pewnego miejsca stałą wartość i, wobec tego, jego granicą jest ta stała wartość.

Oczywiście kładziemy też $v_p(0) = +\infty$. Mając już funkcję v_p wykładnika p-adycznego możemy zdefiniować funkcję odległości, czyli **metrykę** w $\mathbb{Z}_p$. Kładziemy:

$$d_p(\alpha,\, \beta) := p^{-v_p(\alpha-\beta)}. \tag{5.100}$$

Ćwiczenie 5.99 Uznając, że $p^{-\infty} = 0$ udowodnić, że, określona wzorem (5.100), funkcja $d_p : \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow \mathbb{R}_{\geqslant 0}$ ma następujące trzy własności:

(1) $d_p(\alpha,\, \beta) = 0$ wtedy i tylko wtedy, gdy $\alpha = \beta$,

(2) $d_p(\alpha,\, \beta) = d_p(\beta,\, \alpha)$ dla dowolnych $\alpha,\, \beta \in \mathbb{Z}_p$,

(3) $d_p(\alpha,\, \gamma) \leqslant d_p(\alpha,\, \beta) + d_p(\beta,\, \gamma)$ dla dowolnych $\alpha,\, \beta,\, \gamma \in \mathbb{Z}_p$.

Wskazówka. W rzeczywistości zachodzi – mocniejsza niż nierówność (3), która nazywa się **nierównością trójkąta** – tak zwana **ultrametryczna nierówność trójkąta**:

(3)′ $d_p(\alpha,\, \gamma) \leqslant \max\{d_p(\alpha,\, \beta),\, d_p(\beta,\, \gamma)\}$.

Ćwiczenie 5.100 Udowodnić, że równanie $x^2 + 1 = 0$ ma rozwiązania w pierścieniu $\mathbb{Z}_5$, a n i e ma rozwiązań w pierścieniu $\mathbb{Z}_7$.

Ćwiczenie 5.101 Udowodnić, że przestrzeń metryczna $(\mathbb{Z}_p,\, d_p)$ jest **zwarta**, to znaczy, że każdy ciąg (α_n) o wyrazach z pierścienia $\mathbb{Z}_p$ ma podciąg zbieżny. Zobacz $\mathbb{RIN}$.

Rozdział 6

Dodatkowe wiadomości o wielomianach

[...] *wohl die wichtigste Reihe der Mathematik, entdeckte der große englische Mathematiker und Physiker Isaac Newton. Die berühmte Abhandlung, die außer der Exponantialreihe auch die Sinusreihe, Cosinusreihe, Arcussinusreihe, logaritmische Reihe und Binomialreihe enthält, wurde um 1665 verfaßt* [...]

(Heinrich Dörrie)

W tym rozdziale nauczymy się paru nowych rzeczy o wielomianach. Zaczniemy od różniczkowania wielomianów. Potem opowiemy kolejno o wielomianach symetrycznych, o liczbach algebraicznych i uwalnianiu się od niewymierności w mianowniku, o twierdzeniu Liouville'*a* i liczbach przestępnych, o, pochodzącym z końca XX wieku, tak zwanym kombinatorycznym twierdzeniu o zerach i w końcu, o liczbach i wielomianach Bernoulli'*ego*.

6.1 Pochodna wielomianu

Pochodna funkcji ma ogromne znaczenie w **analizie matematycznej**, czyli w badaniu przebiegu zmienności funkcji: pochodna f' funkcji $f : \mathbb{R} \longrightarrow \mathbb{R}$ (jeśli istnieje) jest funkcją wyrażającą szybkość rośnięcia funkcji f. Zobacz $\mathbb{RIN}$, gdzie dowiadujemy się (między innymi), że daleko n i e każda funkcja ma pochodną.

6.1.1 Funkcja wielomianowa

W matematyce szkolnej wielomian jest f u n k c j ą. W matematyce, wielomian $f(X) \in \mathbb{K}[X]$ jest n a p i s e m, który w y z n a c z a funkcję $\mathbb{K} \ni x \longmapsto f(x) \in \mathbb{K}$.

Ćwiczenie 6.1 Udowodnić, że jeżeli $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ lub $\mathbb{C}$ i $f(X) \in \mathbb{K}[X]$ jest wielomianem, to funkcja $x \longmapsto f(x)$ w y z n a c z a wielomian $f(X)$.

K o n t r p r z y k ł a d. Niech $\mathbb{K} = \mathbb{F}_p$. Wielomian $f(X) = X^p - X$, ewidentnie niezerowy, wyznacza funkcję równą 0. To jest tylko inne sformułowanie MTF. Wyjaśnienie tego zjawiska jest proste: w s z y s t k i c h funkcji $\mathbb{F}_p \longrightarrow \mathbb{F}_p$ jest skończenie wiele (mianowicie p^p), a wszystkich wielomianów w $\mathbb{F}_p[X]$ jest nieskończenie wiele (istnieją wielomiany dowolnych stopni). Ciekawostką jest fakt, że k a ż d a funkcja $\mathbb{F}_p \longrightarrow \mathbb{F}_p$ jest funkcją wielomianową. Czytelnik może zechcieć to udowodnić posiłkując się twierdzeniem interpolacyjnym. $\Diamond$

6.1.2 Definicja pochodnej

Dla wielomianów pochodną definiujemy czysto f o r m a l n i e. To znaczy, bez używania pojęcia granicy. Dzięki temu, pojęcie pochodnej wielomianu ma znacznie szerszy zakres znaczeniowy. Pochodna wielomianu $f(X) \in \mathbb{R}[X]$, traktowanego jako funkcja z $\mathbb{R}$ do $\mathbb{R}$, mówi jak rośnie ta funkcja. Pochodna wielomianu $f(X) \in \mathbb{F}_p[X]$, o współczynnikach z ciała skończonego $\mathbb{F}_p$, n i e mówi nic o rośnięciu odpowiedniej funkcji. Przyczyna tego stanu rzeczy jest natury fundamentalnej: w ciele $\mathbb{F}_p$ nie istnieje żaden rozsądny sposób wprowadzenia relacji *mniejszy-równy* $\leqslant$. Zatem nie ma pojęcia funkcji monotonicznej $\mathbb{F}_p \longrightarrow \mathbb{F}_p$.

Definicja 6.1 Niech $f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \in \mathbb{K}[X]$ będzie wielomianem. **Pochodną** tego wielomianu nazywamy wielomian (czytamy: *ef prim*)

$$f'(X) = a_1 + 2a_2X + \ldots + na_nX^{n-1}.$$

Ćwiczenie 6.2 Udowodnić, że dla dowolnych $f, g \in \mathbb{K}[X]$ zachodzą równości:

$$(f+g)'(X) = f'(X) + g'(X), \tag{6.1}$$

$$(fg)'(X) = f'(X)g(X) + f(X)g'(X). \tag{6.2}$$

Pochodna pochodnej danego wielomianu nazywa się **drugą pochodną**, oznaczamy ją $f''(X)$ (czytamy: *ef bis*). Pochodna $(k-1)$-szej pochodnej nazywa się k-**tą pochodną**, oznaczamy ją $f^{(k)}(X)$.

Ćwiczenie 6.3 Udowodnić, że jeżeli $f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \in \mathbb{C}[X]$, to

$$a_0 = f(0),\ a_1 = f'(0),\ a_2 = \frac{1}{2}f''(0),\ \ldots,\ a_k = \frac{1}{k!}f^{(k)}(0),\ \ldots. \tag{6.3}$$

U w a g a. Czytelnik zauważył, że w powyższym ćwiczeniu założyliśmy, że współczynniki rozważanego wielomianu są l i c z b a m i z e s p o l o n y m i (w szczególności: rzeczywistymi lub wymiernymi). Chodzi o to, że w nie każdym ciele $\mathbb{K}$ zachodzi nierówność $k! \neq 0$.

6.1.3 Twierdzenia Rolle'*a* i Lagrange'*a*

Twierdzenie Rolle'*a* i wniosek z niego płynący – twierdzenie Lagrange'*a* o wartości średniej, dotyczą **funkcji różniczkowalnych** (= mających pochodną) określonych na zbiorze liczb rzeczywistych. Jego dowód wymaga czegoś więcej niż czysto formalna definicja pochodnej – mianowicie rozumienia pochodnej jako **granicy** (ilorazu różnicowego), zobacz $\mathbb{RIN}$. Dlatego tutaj opuścimy ten dowód. Samo twierdzenie jest bardzo proste:

TWIERDZENIE 6.1 (***Twierdzenie Rolle'a***) *Jeżeli $a < b$ są pierwiastkami wielomianu $f(X)$ o współczynnikach r z e c z y w i s t y c h, to istnieje takie $c \in [a; b]$, że $f'(c) = 0$.* □

Ćwiczenie 6.4 Udowodnić, że jeżeli dla $a_0, \ldots, a_n \in \mathbb{R}$ zachodzi równość $\sum_{k=0}^{n} \frac{a_k}{k+1} = 0$, to wielomian $a_0 + a_1X + \ldots + a_nX^n$ ma co najmniej jeden pierwiastek rzeczywisty.

Twierdzenie Lagrange'*a* o wartości średniej jest prostym wnioskiem z twierdzenia Rolle'*a*:

TWIERDZENIE 6.2 (***Twierdzenie Lagrange'a o wartości średniej***) *Jeżeli* $f(X)$ *jest dowolnym wielomianem o współczynnikach rzeczywistych,* $a < b$ *są dowolnymi liczbami rzeczywistymi, to istnieje taka liczba* $c \in [\,a;\,b\,]$, *że*

$$\frac{f(b)-f(a)}{b-a} = f'(c).$$

DOWÓD. Rozważmy wielomian

$$g(X) = f(X) - f(a) - \frac{f(b)-f(a)}{b-a}(X-a).$$

Ze wzorów (6.1) i (6.2) na pochodną sumy i pochodną iloczynu widzimy, że

$$g'(X) = f'(X) - \frac{f(b)-f(a)}{b-a}.$$

Ponadto widzimy, że $g(a) = g(b) = 0$. To, na mocy twierdzenia Rolle'a, daje równość $g'(c) = 0$ dla pewnego $c \in [\,a;\,b\,]$, czyli tezę. □

6.1.4 Wzór Maclaurina i wzór Taylora

Równości (6.3) pozwalają napisać równość

$$f(X) = f(0) + f'(0)X + \frac{1}{2}f''(0)X^2 + \ldots + \frac{1}{n!}f^{(n)}(0)X^n \tag{6.4}$$

prawdziwą dla dowolnego wielomianu o współczynnikach zespolonych stopnia n. Tę równość nazywa się czasami ***wzorem Maclaurina***.

Użyteczny bywa wniosek płynący z (6.4), pozwalający zapisywać dany wielomian względem "przesuniętej" zmiennej $X - \alpha$:

Ćwiczenie 6.5 Udowodnić następujący ***wzór Taylora***:

$$f(X) = F(\alpha) + \sum_{k=1}^{\infty} \frac{f^{(k)}(\alpha)}{k!}(X-\alpha)^k, \tag{6.5}$$

dla dowolnego wielomianu $f(X) \in \mathbb{C}[X]$ i dowolnej liczby $\alpha \in \mathbb{C}$. Zauważmy, że suma po prawej stronie w istocie jest skończona (jeżeli bowiem wielomian f ma stopień n, to wszystkie pochodne $f^{(k)}(X)$, dla $k > n$, są wielomianami zerowymi).

Przykład. Rozważmy wielomian $f(X) = X^n$. Zapisujemy go względem zmiennej "przesuniętej" $X - \alpha$:

$$X^n = \alpha^n + \sum_{k=1}^{\infty} \frac{f^{(k)}(\alpha)}{k!}(X-\alpha)^k = \sum_{k=0}^{n} \binom{n}{k} \alpha^{n-k}(X-\alpha)^k,$$

bo $f^{(k)}(\alpha) = n(n-1)\cdot\ldots\cdot(n-k+1)\alpha^{n-k}$ (dla $f(X) = X^n$). Wystarczy położyć $X = \alpha + \beta$, by rozpoznać znany ze szkoły wzór dwumienny, zobacz (1.7). ◊

6.1.5 Pochodna a pierwiastki wielokrotne

Pochodną wielomianu wykorzystuje się przy badaniu pierwiastków wielokrotnych.

Definicja 6.2 Dane jest ciało $\mathbb{K}$ i wielomian $f(X) \in \mathbb{K}[X]$. Element $\alpha \in \mathbb{K}$ nazywa się **pierwiastkiem wielokrotnym** wielomianu $f(X)$, gdy $(X-\alpha)^2 | f(X)$. Mówimy, że pierwiastek wielokrotny α jest **pierwiastkiem k-krotnym**, gdy $k \geqslant 2$ oraz $(X-\alpha)^k | f(X)$ i $(X-\alpha)^{k+1} \nmid f(X)$.

TWIERDZENIE 6.3 *Dany jest wielomian $f(X) \in \mathbb{K}[X]$. Element $\alpha \in \mathbb{K}$ jest jego pierwiastkiem wielokrotnym wtedy i tylko wtedy, gdy $f(\alpha) = f'(\alpha) = 0$.*

DOWÓD. Jeżeli $f(X) = (X-\alpha)^2 g(X)$ dla pewnego wielomianu $g(X)$, to, $f(\alpha) = 0$, oraz, na mocy wzoru (6.2), $f'(X) = 2(X-\alpha)g(X) + (X-\alpha)^2 g'(X)$, skąd $f'(\alpha) = 0$.

Odwrotnie, jeżeli $f(\alpha) = f'(\alpha) = 0$, to $f(X) = (X-\alpha)g(X)$ i $f'(X) = (X-\alpha)h(X)$ dla pewnych wielomianów $g(X), h(X) \in \mathbb{K}[X]$, na mocy twierdzenia Bézout'*a*. Liczymy pochodną iloczynu: $f'(X) = (X-\alpha)'g(X) + (X-\alpha)g'(X) = g(X) + (X-\alpha)g'(X)$. Mamy więc $g(X) + (X-\alpha)g'(X) = (X-\alpha)h(X)$. Skąd $g(X) = (X-\alpha)(h(X) - g'(X))$ i ostatecznie $f(X) = (X-\alpha)^2(h(X) - g'(X))$. □

Ćwiczenie 6.6 Udowodnić, że α jest pierwiastkiem k-krotnym wielomianu $f(X) \in \mathbb{K}[X]$ wtedy i tylko wtedy, gdy $f(\alpha) = f'(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$, oraz $f^{(k)}(\alpha) \neq 0$.

Ćwiczenie 6.7 Udowodnić, że wielomian $f(X) \in \mathbb{C}[X]$ ma pierwiastek wielokrotny wtedy i tylko wtedy, gdy wielomiany $f(X)$ i $f'(X)$ nie są względnie pierwsze. Wywnioskować stąd, że *wielomian $f(X) \in \mathbb{Q}[X]$ nierozkładalny w $\mathbb{Q}[X]$ nie ma pierwiastków wielokrotnych.*

ZADANIE 6.1 Udowodnić, że jeżeli wielomian $f(X) \in \mathbb{K}[X]$ jest względnie pierwszy ze swoją pochodną $f'(X)$, a wielomian $a(X)$ jest wielomianem stopnia $\geqslant 1$, to[1] $a(X)^2 \nmid f(X)$.

Rozwiązanie. Względna pierwszość wielomianów $f(X)$ i $f'(X)$ pociąga, zob. C3.31, istnienie równości $f(X)s(X) + f'(X)t(X) = 1$ dla pewnych wielomianów $s(X)$, $t(X)$. Załóżmy, nie wprost, że $f(X) = a(X)^2 g(X)$ dla pewnego $g(X) \in \mathbb{K}[X]$. Dwukrotne zastosowanie wzoru Leibniza (6.2) daje równość $f'(X) = 2a(X)a'(X)g(X) + a(X)^2 g'(X) = a(X)h(X)$. Stąd dostajemy nonsensowną równość $a(X)[s(X) + h(X)t(X)] = 1$. ◊

6.2 Wielomiany symetryczne

Musimy powiedzieć słów parę na temat wielomianów symetrycznych. Znajomość najprostszych ich własności jest niezbędna każdemu olimpijczykowi. Dotyczy to zwłaszcza zastosowań wzorów Viète'*a* (3.53). Z lewej strony tych wzorów występują bowiem wyrażenia wielomianowe mające własność symetryczności.

[1] Można powiedzieć, że $f(X)$ jest elementem bezkwadratowym w pierścieniu $\mathbb{K}[X]$, por. C2.36.

6.2.1 Definicja

Wielomian wielu zmiennych nazywa się wielomianem symetrycznym, gdy można mu dowolnie permutować zmienne, a on tego nie "czuje".

Definicja 6.3 Wielomian $s(X_1, X_2, \ldots, X_n) \in \mathbb{K}[X_1, X_2, \ldots, X_n]$ nazywa się **wielomianem symetrycznym**, gdy

$$s(X_1, X_2, \ldots, X_n) = s(X_{\tau(1)}, X_{\tau(2)}, \ldots, X_{\tau(n)})$$

dla dowolnej permutacji $\tau \in S_n$.

P r z y k ł a d 1. Jasne, że wielomiany

$$s_k = s_k(X_1, X_2, \ldots, X_n) := X_1^k + X_2^k + \ldots + X_n^k \tag{6.6}$$

są wielomianami symetrycznymi n zmiennych. $\Diamond$

Aby zobaczyć nową serię wielomianów symetrycznych n zmiennych, rozważmy równość

$$(T + X_1)(T + X_2) \cdot \ldots \cdot (T + X_n) = T^n + \sigma_1 T^{n-1} + \sigma_2 T^{n-2} + \ldots + \sigma_{n-1} T + \sigma_n.$$

(Mnożymy i porządkujemy względem potęg T.) Współczynniki σ_k są, oczywiście, wielomianami n zmiennych $X_1, X_2, \ldots, X_n$. Łatwo widzieć, że są one wielomianami symetrycznymi:

Ćwiczenie 6.8 Uzasadnić, że wielomiany σ_k są wielomianami symetrycznymi. Uzasadnić też, że $\deg \sigma_k = k$.

Definicja 6.4 Wielomiany $\sigma_k = \sigma_k(X_1, X_2, \ldots, X_n)$ nazywamy **elementarnymi wielomianami symetrycznymi** n zmiennych.

Wartości elementarnych wielomianów symetrycznych występują we wzorach Viète'a (3.53), które możemy zapisać w postaci

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}, \tag{6.7}$$

gdzie $\sigma_k = \sigma_k(\lambda_1, \lambda_2, \ldots, \lambda_n)$ jest wartością k-tego elementarnego wielomianu symetrycznego na układzie $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ wszystkich (każdy pierwiastek wypisany tyle razy, ile wynosi jego krotność) pierwiastków wielomianu $\sum a_k X^k$ stopnia n.

Najczęściej spotykamy przypadek $n = 3$. Wtedy, porównaj (3.59),

$$\sigma_1 = X_1 + X_2 + X_3, \quad \sigma_2 = X_1X_2 + X_2X_3 + X_3X_1, \quad \sigma_3 = X_1X_2X_3.$$

Ćwiczenie 6.9 Liczby x, y, u, v spełniają warunki $x + y + u + v = \frac{1}{x} + \frac{1}{y} + \frac{1}{u} + \frac{1}{v} = 2$. Udowodnić, że $\frac{1}{1-x} + \frac{1}{1-y} + \frac{1}{1-u} + \frac{1}{1-v} = 2$. *Wskazówka.* Znowu ta *filozofia Viète'a*! Wielomian czwartego stopnia o pierwiastkach x, y, u, v ma postać $T^4 - 2T^3 + aT^2 - 2bT + b$. Jak wobec tego wygląda wielomian o pierwiastkach $1 - x, 1 - y, 1 - u, 1 - v$?

Ćwiczenie 6.10 Niech $a, b, c \in \mathbb{Z}$ i $a + b + c = 0$. Udowodnić, że $32(a^4 + b^4 + c^4)$ jest kwadratem (liczby całkowitej).

6.2.2 Twierdzenie Newtona

Udowodnimy podstawowe twierdzenie Newtona mówiące, że elementarne wielomiany symetryczne są "cegiełkami", z których można zbudować każdy wielomian symetryczny. Przed dowodem musimy wykonać pewną pracę wstępną, dzięki której nauczymy się bardziej systemowo kodować jednomiany danego stopnia k.

Przez $\mathcal{R}(n,\,k)$ oznaczamy zbiór wszystkich ciągów n-wyrazowych $(i_1,\,i_2,\,\ldots,\,i_n)$, gdzie i_j są liczbami całkowitymi nieujemnymi spełniającymi warunek $i_1+\ldots+i_n=k$, zobacz $\mathbb{KOM}$. Ciągi ze zbioru $\mathcal{R}(n,\,k)$ oznaczamy literami I, J, K, itp. Jeżeli $K=(k_1,\,k_2,\,\ldots,\,k_n)\in\mathcal{R}(n,\,k)$, to jednomian $X_1^{k_1}X_2^{k_2}\cdot\ldots\cdot X_n^{k_n}$ będziemy oznaczać w skrócie symbolem X^K. Przez $\mathcal{N}=\mathcal{N}(n,\,k)$ oznaczymy podzbiór zbioru $\mathcal{R}(n,\,k)$ składający się z ciągów nierosnących. Zbiór $\mathcal{N}$ uporządkujmy za pomocą relacji $\prec$ zdefiniowanej tak: $K\prec L$, gdy pierwsza z różnych od 0 różnic

$$l_1-k_1,\;l_2-k_2,\;\ldots,\;l_n-k_n$$

jest liczbą dodatnią. Na przykład $(4,\,2,\,1,\,1,\,1)\prec(4,\,2,\,2,\,1,\,0)$ w $\mathcal{N}(5,\,9)$. Oczywiście $(9,\,0,\,0,\,0,\,0)$ jest największym, a $(2,\,2,\,2,\,2,\,1)$ jest najmniejszym elementem w $\mathcal{N}(5,\,9)$.

Ćwiczenie 6.11 Udowodnić, że relacja $\prec$ jest relacją porządku liniowego w $\mathcal{N}(n,\,k)$.

Gdy $I\in\mathcal{R}(n,\,k)$, przez $r(I)$ oznaczamy ciąg należący do $\mathcal{N}(n,\,k)$ mający te same wyrazy co I (ustawione w porządku nierosnącym). Na przykład, jeżeli $I=(1,\,0,\,3,\,1,\,4)\in\mathcal{R}(5,\,9)$, to $r(I)=(4,\,3,\,1,\,1,\,0)$.

Ćwiczenie 6.12 Niech $J=(j_1,\,j_2,\,\ldots,\,j_n)\in\mathcal{N}(n,\,k)$. Udowodnić, że wielomian

$$F_J:=\sigma_1^{j_1-j_2}\sigma_2^{j_2-j_3}\cdot\ldots\cdot\sigma_{n-1}^{j_{n-1}-j_n}\sigma_n^{j_n} \tag{6.8}$$

jest wielomianem symetrycznym i jednorodnym stopnia k. Ponadto, jednym z jego składników jest jednomian X^J, a wszystkie pozostałe jego składniki są jednomianami postaci cX^I, gdzie $r(I)\prec J$.

TWIERDZENIE 6.4 (***Twierdzenie Newtona***) *Każdy wielomian symetryczny n zmiennych o współczynnikach w pierścieniu $\mathcal{R}$ da się zapisać w postaci wielomianu zmiennych $\sigma_1,\,\sigma_2,\,\ldots,\,\sigma_n$ o współczynnikach w tym samym pierścieniu $\mathcal{R}$.*

DOWÓD. Po rozwiązaniu ćwiczeń C6.11 i C6.12 dowód jest natychmiastowy.

Ponieważ każdy wielomian jest (jednoznacznie) sumą swoich składników jednorodnych, zobacz (3.65), więc wystarczy zapisać w postaci wielomianu zmiennych σ_j dowolny wielomian symetryczny i jednorodny. Niech więc $A(X_1,\,X_2,\,\ldots,\,X_n)$ będzie wielomianem symetrycznym i jednorodnym stopnia k. Zauważmy, że w takiej sytuacji, jeżeli jednomian cX^K jest jego składnikiem, to również jego składnikami są wszystkie jednomiany postaci cX^L, gdzie ciąg $L=(l_1,\,l_2,\,\ldots,\,l_n)$ jest dowolną permutacją ciągu $K=(k_1,\,k_2,\,\ldots,\,k_n)$. To wynika z symetryczności wielomianu (czyli możliwości permutowania zmiennych X_i). W szczególności jednomian $cX^{r(K)}$ jest składnikiem A.

Załóżmy teraz, że aX^J jest występującym w A jednomianem z największym (w sensie relacji $\prec$) **(multi)wykładnikiem** J. Wówczas różnica

$$A - aF_J,$$

jeżeli jest różna od 0, to jest wielomianem symetrycznym i jednorodnym stopnia k, a ponadto wszystkie występujące w niej jednomiany (niezerowe) mają (multi)wykładniki I spełniające nierówność $r(I) \prec J$. Ponieważ zbiór $\mathcal{R}(n, k)$ jest zbiorem skończonym, więc jest jasne, że po skończonej ilości takich operacji ("kasowania" największego (multi)wykładnika) dojdziemy do wielomianu zerowego. To kończy dowód. □

Ćwiczenie 6.13 Korzystając z opisanego w powyższym dowodzie algorytmu, przedstawić wielomiany $s_3(X, Y, Z) = X^3 + Y^3 + Z^3$ oraz $s_4(X, Y, Z) = X^4 + Y^4 + Z^4$ w postaci wielomianów zmiennych $\sigma_1 = X + Y + Z$, $\sigma_2 = XY + YZ + ZX$ i $\sigma_3 = XYZ$.

Ćwiczenie 6.14 Niech x_1, x_2 będą pierwiastkami trójmianu $aX^2 + bX + c$ $(a \neq 0)$. Udowodnić następującą ***formułę Waringa***:

$$x_1^n + x_2^n = n \sum_k (-1)^{n+k} \frac{(n-k-1)!}{k!(n-2k)!} a^{k-n} b^{n-2k} c^k,$$

gdzie sumujemy po wszystkich naturalnych k, dla których $0 \leqslant k \leqslant n/2$. Por. 3.2.7 U1.

6.2.3 Wyróżnik

Szczególnie często używanym wielomianem symetrycznym jest tak zwany wyróżnik:

Definicja 6.5 Następujący wielomian

$$\Delta(X_1, X_2, \ldots, X_n) = \prod_{1 \leqslant k < l \leqslant n} (X_k - X_l)^2 \tag{6.9}$$

nazywamy **wyróżnikiem** n zmiennych $X_1, X_2, \ldots, X_n$.

Jasne, że dla danych liczb (ogólniej, elementów jakiegoś ciała) $x_1, x_2, \ldots, x_n$, wartość $\Delta(x_1, x_2, \ldots, x_n)$ jest równa 0 wtedy i tylko wtedy, gdy pewne dwie z liczb $x_1, x_2, \ldots, x_n$ są równe.

Ćwiczenie 6.15 Uzasadnić, że wyróżnik jest wielomianem symetrycznym. Wyrazić wyróżnik 2 i 3 zmiennych przez elementarne wielomiany symetryczne odpowiedniej liczby zmiennych. W przypadku 3 zmiennych założyć, dla uproszczenia, że $\sigma_1 = 0$.

6.2.4 Funkcje tworzące

Wyrazy α_k danego (skończonego lub nie) ciągu $(\alpha_k)_{k \geqslant 0}$ wygodnie jest uznawać za współczynniki "wielomianu" $\sum_{k \geqslant 0} \alpha_k T^k$ jednej zmiennej T. Cudzysłów można wyrzucić, gdy ciąg jest skończony. W przypadku nieskończonym mówimy raczej o formalnym szeregu potęgowym. Zobacz ustęp 9.2.2, z którego należy zapoznać się z tak zwanym szeregiem Neumanna (9.16). Dobrze też zajrzeć do $\mathbb{KOM}$ 4.3.2.

Definicja 6.6 Niech $(\alpha_k)_{k\geqslant 0}$ będzie danym ciągiem. Formalny szereg potęgowy

$$\sum_{k\geqslant 0} \alpha_k T^k$$

nazywamy **funkcją tworzącą** ciągu (α_k).

Pierwszy nasz przykład funkcji tworzącej jest wielomianem. Niech $\sigma_k = \sigma_k(X_1, \ldots, X_n)$ będą elementarnymi wielomianami symetrycznymi n zmiennych. Umawiamy się dodatkowo, że $\sigma_0 = 1$ i $\sigma_k = 0$ dla $k > n$. Funkcję tworzącą ciągu (σ_k) oznaczymy w skrócie $\Sigma(T)$.

Ćwiczenie 6.16 Uzasadnić, że zachodzi równość

$$\Sigma(T) = (1 + TX_1)(1 + TX_2) \cdot \ldots \cdot (1 + TX_n). \tag{6.10}$$

Drugi nasz przykład funkcji tworzącej nie jest już wielomianem. Rozważmy mianowicie ciąg (s_k) wielomianów danych przez (6.6). Jego funkcja tworząca jest formalnym szeregiem potęgowym:

$$S(T) := \sum_{k=0}^{\infty} s_k T^k.$$

Ćwiczenie 6.17 Umawiamy się, że $s_0 = n$. Udowodnić, że

$$S(T) = \frac{1}{1 - TX_1} + \frac{1}{1 - TX_2} + \ldots + \frac{1}{1 - TX_n}. \tag{6.11}$$

Zdefiniujmy jeszcze jeden ciąg wielomianów symetrycznych. Niech mianowicie

$$r_k = r_k(X_1, X_2, \ldots, X_n) := \sum_{k_1+k_2+\cdots+k_n=k} X_1^{k_1} X_2^{k_2} \cdot \ldots \cdot X_n^{k_n}. \tag{6.12}$$

Sumujemy po wszystkich układach $(k_1, k_2, \ldots, k_n)$ nieujemnych liczb całkowitych o sumie równej k (ta suma ma $\binom{k+n-1}{n-1}$ składników, zobacz $\mathbb{KOM}$ T1.6(4)). Wielomian r_k jest więc sumą wszystkich jednomianów stopnia k (każdy ze współczynnikiem 1). Wobec tego nazywamy go **pełnym wielomianem symetrycznym jednorodnym stopnia** k. Wygodnie jest uznać, że $r_0 = 1$. Funkcję tworzącą ciągu (r_k) oznaczymy symbolem $R(T)$.

Ćwiczenie 6.18 Udowodnić, że zachodzi równość

$$R(T) = \frac{1}{1 - TX_1} \cdot \frac{1}{1 - TX_2} \cdot \ldots \cdot \frac{1}{1 - TX_n}. \tag{6.13}$$

Dla zilustrowania działania techniki funkcji tworzących rozwiążmy:

ZADANIE 6.2 Udowodnić, że dla $n \geqslant 1$ zachodzi równość

$$\sum_{k=0}^{n} (-1)^k \sigma_k r_{n-k} = 0. \tag{6.14}$$

R o z w i ą z a n i e. Mamy, na mocy (6.10) i (6.13):

$$\Sigma(-T) \cdot R(T) = 1.$$

Równość ta jest równoważna z równościami (6.14) dla $n \geqslant 1$ oraz równością $\sigma_0 r_0 = 1$. $\Diamond$

Ćwiczenie 6.19 Stosując technikę funkcji tworzących udowodnić, że

$$nr_n = \sum_{k=1}^{n} s_k r_{n-k}. \tag{6.15}$$

6.3 Liczby algebraiczne i przestępne

Liczby algebraiczne to pierwiastki równań wielomianowych o współczynnikach całkowitych (równoważnie: wymiernych). Pozostałe liczby to liczby przestępne. Niektóre liczby wymierne są całkowite. A niektóre liczby algebraiczne nazywamy liczbami algebraicznymi całkowitymi.

Definicja 6.7 Liczbę zespoloną α nazywamy **liczbą algebraiczną**, gdy istnieje taki niezerowy wielomian $f(X) \in \mathbb{Z}[X]$, że $f(\alpha) = 0$. W przypadku przeciwnym nazywamy ją **liczbą przestępną**. Liczbę zespoloną α nazywamy **liczbą algebraiczną całkowitą**, gdy istnieje taki wielomian u n o r m o w a n y $f(X) \in \mathbb{Z}[X]$, że $f(\alpha) = 0$. Zbiór liczb algebraicznych oznaczamy symbolem $\mathbb{A}$, a zbiór liczb algebraicznych całkowitych, symbolem $\mathbb{I}$.

Ćwiczenie 6.20 Udowodnić, że jeżeli liczba rzeczywista x jest współmierna z liczbą π (to znaczy, że $x/\pi \in \mathbb{Q}$), to $\sin x$ i $\cos x$ są liczbami algebraicznymi. *Wskazówka.* Wykorzystać (1.7) i (1.14).

6.3.1 Wielomian minimalny liczby algebraicznej

Z każdą liczbą algebraiczną związany jest jej wielomian minimalny.

Ćwiczenie 6.21 Niech dana będzie liczba algebraiczna α. Udowodnić, że zbiór

$$I_\alpha = \{f(X) \in \mathbb{Q}[X] : f(\alpha) = 0\} \tag{6.16}$$

jest ideałem w pierścieniu $\mathbb{Q}[X]$. Wywnioskować stąd, że istnieje dokładnie jeden taki wielomian unormowany $m_\alpha(X) \in \mathbb{Q}[X]$, że $I_\alpha = (m_\alpha(X))$.

Definicja 6.8 Niech α będzie liczbą algebraiczną. Zdefiniowany w powyższym ćwiczeniu wielomian $m_\alpha(X)$ nazywamy **wielomianem minimalnym** liczby algebraicznej α. Stopień $\deg m_\alpha(X)$ wielomianu minimalnego liczby algebraicznej α nazywa się **stopniem liczby** α.

P r z y k ł a d 1. Niech $\alpha = \sqrt{2}+\sqrt{3}$. Wówczas $\alpha^2 = 5+2\sqrt{6}$. Stąd $(\alpha^2-5)^2 = (2\sqrt{6})^2 = 24$, więc $\alpha^4 - 10\alpha^2 + 1 = 0$. Widzimy, że α jest pierwiastkiem wielomianu $X^4 - 10X^2 + 1$. Przeto $\alpha \in \mathbb{I}$. Łatwo sprawdzić, że wielomian $X^4 - 10X^2 + 1$ jest nierozkładalny. Czyli, że liczba $\sqrt{2} + \sqrt{3}$ jest liczbą algebraiczną (całkowitą) stopnia 4. $\Diamond$

P r z y k ł a d 2. Niech $\alpha = \sqrt[n]{\sqrt{3}+1}$. Wtedy $\alpha^n - 1 = \sqrt{3}$, skąd $(\alpha^n - 1)^2 = 3$. Widzimy zatem, że α jest pierwiastkiem wielomianu $f(X) = X^{2n} - 2X^n - 2$. Jest więc liczbą algebraiczną całkowitą. Kryterium Eisensteina T3.17 (przy wyborze $p = 2$) pokazuje, że wielomian $f(X)$ jest nierozkładalny. Stąd łatwo wywnioskować, że $f(X) = m_\alpha(X)$. Rzeczywiście, ponieważ $f \in I_\alpha = (m_\alpha)$, więc $f(X) = m_\alpha(X)g(X)$ dla pewnego $g(X) \in \mathbb{Q}[X]$. Ta równość, wobec nierozkładalności wielomianu f, dowodzi, że $\deg g = 0$, więc $g \in \mathbb{Q} \setminus \{0\}$. I wreszcie, ponieważ oba wielomiany f i m_α są unormowane, $g = 1$. ◊

ZADANIE 6.3 Dowieść, że wielomian minimalny liczby algebraicznej jest nierozkładalny.

R o z w i ą z a n i e. Załóżmy, że $m_\alpha(X) = f(X)g(X)$. Wtedy $f(\alpha)g(\alpha) = m_\alpha(\alpha) = 0$, więc $f(\alpha) = 0$ lub $f(\alpha) = 0$. Niech $f(\alpha) = 0$. Wówczas $f(X) \in I_\alpha$, czyli $f(X) = m_\alpha(X)k(X)$ dla pewnego wielomianu $k(X) \in \mathbb{Q}[X]$. Stąd $m_\alpha(X) = m_\alpha(X)k(X)g(X)$. Zatem, na mocy C3.6, $\deg g(X) = 0$. ◊

Ćwiczenie 6.22 Uzasadnić, że zbiór liczb algebraicznych stopnia 1 pokrywa się ze zbiorem liczb wymiernych, a zbiór liczb algebraicznych stopnia 2 jest równy

$$\{x + y\sqrt{\Delta} : x, y \in \mathbb{Q}, \Delta \neq 1 \text{ jest bezkwadratową liczbą całkowitą}\}.$$

Definicja 6.9 Liczbę algebraiczną stopnia 2 nazywamy **niewymiernością kwadratową**.

Ćwiczenie 6.23 Udowodnić równość zbiorów $\mathbb{Q} \cap \mathbb{I} = \mathbb{Z}$.

Ćwiczenie 6.24 Udowodnić, że liczba $\sqrt{3} - \sqrt{5}$ jest liczbą algebraiczną stopnia 4, a liczba $\sqrt{2} + \sqrt[3]{3}$ jest liczbą algebraiczną stopnia 6.

6.3.2 Uwalnianie się od niewymierności w mianowniku

Pokażemy teraz metodę "uwalniania się od niewymierności" w mianowniku, czyli zapisywania liczb postaci $u(\alpha)/v(\alpha)$, gdzie α jest liczbą algebraiczną, a $u(X)$, $v(X) \in \mathbb{Q}[X]$, w postaci $w(\alpha)$, dla pewnego $w(X) \in \mathbb{Q}[X]$. Okazuje się, że dla zrobienia takiej sztuczki wystarczy znać algorytm dzielenia z resztą, zobacz T3.3, i wielomian minimalny $m_\alpha(X)$.

TWIERDZENIE 6.5 *Jeżeli α jest liczbą algebraiczną stopnia n, to zbiór*

$$\mathbb{Q}(\alpha) := \{a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}\}$$

jest ciałem.

D O W Ó D. Zauważmy, że $\mathbb{Q}(\alpha)$ jest zbiorem wartości, dla argumentu α, wszystkich wielomianów o współczynnikach wymiernych, stopnia $< n$. Możliwość[2] dodawania i odejmowania w tym zbiorze jest oczywista. Musimy więc uzasadnić, że zbiór $\mathbb{Q}(\alpha)$ jest zamknięty względem mnożenia i dzielenia (nie przez zero, oczywiście!).

[2]Mówimy, że zbiór $\mathbb{Q}(\alpha)$ jest **zamknięty** względem dodawania i odejmowania.

Niech $f(\alpha)$, $g(\alpha) \in \mathbb{Q}(\alpha)$, gdzie $f(X)$, $g(X) \in \mathbb{Q}[X]$ i $\deg(f)$, $\deg(g) < n$. Podzielmy (z resztą) iloczyn $f(X)g(X)$ przez wielomian minimalny $m_\alpha(X)$. Otrzymamy

$$f(X)g(X) = q(X)m_\alpha(X) + r(X) \quad \text{gdzie} \quad \deg r(X) < n.$$

Zatem $f(\alpha)g(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) = r(\alpha) \in \mathbb{Q}(\alpha)$. Widzimy, że zbiór $\mathbb{Q}(\alpha)$ jest zamknięty względem mnożenia. Ponieważ dzielenie jest mnożeniem przez odwrotność, więc wystarczy uzasadnić, że jeżeli $f(\alpha) \in \mathbb{Q}(\alpha) \setminus \{0\}$, to $\frac{1}{f(\alpha)} \in \mathbb{Q}(\alpha)$. Aby to zrobić zauważmy, że $\mathrm{NWD}\,(f, m_\alpha) \sim 1$ (bo, zob. C3.35, m_α jest wielomianem nierozkładalnym i nie dzieli wielomianu $f(X)$, który jest stopnia $< n$). Zatem

$$f(X)k(X) + m_\alpha(X)l(X) = 1$$

dla pewnych $k(X)$, $l(X) \in \mathbb{Q}[X]$, zobacz T3.11. Kładąc tu $X = \alpha$, mamy $f(\alpha)k(\alpha) = 1$. Jeżeli $r(X)$ jest resztą z dzielenia $k(X)$ przez $m_\alpha(X)$, to $k(\alpha) = r(\alpha)$ i ostatecznie

$$\frac{1}{f(\alpha)} = r(\alpha) \in \mathbb{Q}(\alpha), \tag{6.17}$$

bo $\deg(r) < n$. Dzielenie (nie przez zero!) jest więc wykonalne w zbiorze $\mathbb{Q}(\alpha)$. Ostatecznie, zbiór $\mathbb{Q}(\alpha)$ jest ciałem. □

U w a g a 1. W tym dowodzie poznaliśmy ogólną metodę uwalniania się od niewymierności w mianowniku, czyli metodę odwracania wyrażeń wielomianowych od liczby będącej pierwiastkiem wielomianu. Mówi o tym równość (6.17). W matematyce szkolnej poznaliśmy przypadek szczególny tej metody, gdy mamy do czynienia z niewymiernościami kwadratowymi.

U w a g a 2. Ciało $\mathbb{Q}$ może być w tym twierdzeniu zastąpione przez dowolne ciało. Spróbujcie sformułować i udowodnić odpowiednią wersję ogólną.

Ćwiczenie 6.25 Uwolnić się od niewymierności w mianowniku: $\dfrac{1}{1 + 3\sqrt[3]{2} - 5\sqrt[3]{4}}$.

Ćwiczenie 6.26 Uzasadnić, że zbiór $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ j e s t ciałem (względem zwykłych działań dodawania i mnożenia liczb), a zbiór $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$ n i e j e s t ciałem[3].

6.3.3 Pierścień liczb algebraicznych całkowitych

Wykorzystamy wiedzę dotyczącą wielomianów symetrycznych w dowodzie faktu że zbiór $\mathbb{I}$ liczb algebraicznych całkowitych jest p i e r ś c i e n i e m (względem zwykłych działań). Stąd dostaniemy natychmiastowy wniosek, że zbiór $\mathbb{A}$ wszystkich liczb algebraicznych jest c i a ł e m.

Ćwiczenie 6.27 Udowodnić, że wielomian minimalny liczby algebraicznej całkowitej ma współczynniki całkowite. *Wskazówka.* Jeżeli $f(\alpha) = 0$ dla pewnego wielomianu unormowanego $f(X) \in \mathbb{Z}[X]$, to $f(X) \in I_\alpha$, zobacz (6.16), więc $f(X) = m_\alpha(X)g(X)$ dla pewnego wielomianu $g(X) \in \mathbb{Q}[X]$. Zastosować twierdzenie T3.15.

TWIERDZENIE 6.6 *Zbiór $\mathbb{I}$ liczb algebraicznych całkowitych jest pierścieniem.*

[3] Ale zbiór $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$ jest ciałem (względem zwykłych działań). Por. T6.5.

D O W Ó D. Mamy udowodnić, że jeżeli α, β są liczbami algebraicznymi całkowitymi, to zarówno suma $\alpha+\beta$ jak i iloczyn $\alpha\beta$ są liczbami algebraicznymi całkowitymi.

Niech $m_\alpha = m_\alpha(X)$, $m_\beta = m_\beta(X) \in \mathbb{Z}[X]$ będą wielomianami minimalnymi liczb α, β. Zapiszmy ich rozkłady w $\mathbb{C}[X]$, zobacz T3.18:

$$m_\alpha(X) = a_0 + a_1X + \ldots + X^n = (X-\alpha_1)(X-\alpha_2)\cdot\ldots\cdot(X-\alpha_n),$$
$$m_\beta(X) = b_0 + b_1X + \ldots + X^m = (X-\beta_1)(X-\beta_2)\cdot\ldots\cdot(X-\beta_m).$$

Pierwiastki α_i są parami różne, zobacz C6.7. Również pierwistki β_j są parami różne. Możemy przyjąć, że $\alpha=\alpha_1$ i $\beta=\beta_1$. Rozważmy wielomian u n o r m o w a n y stopnia nm:

$$F(X) = \prod_{i=1}^{n}\prod_{j=1}^{m}(X-\alpha_i-\beta_j). \tag{6.18}$$

Jego pierwiastkiem jest liczba $\alpha+\beta=\alpha_1+\beta_1$. S p r a w d z i m y, że wielomian $F(X)$ ma współczynniki całkowite, co będzie dowodzić, że $\alpha+\beta\in\mathbb{I}$.

Zapiszemy iloczyn (6.18) w postaci $m_\beta(X-\alpha_1)m_\beta(X-\alpha_2)\cdot\ldots\cdot m_\beta(X-\alpha_n)$, czyli

$$[b_0+b_1(X-\alpha_1)+\ldots+(X-\alpha_1)^m]\cdot\ldots\cdot[b_0+b_1(X-\alpha_n)+\ldots+(X-\alpha_n)^m].$$

Widzimy stąd, że $F(X)$ jest wielomianem symetrycznym zmiennych $\alpha_1, \alpha_2, \ldots, \alpha_n$ o współczynnikach w pierścieniu $\mathbb{Z}[X]$. Zatem, na mocy twierdzenia Newtona T6.4, widzimy, że $F(X)$ jest wielomianem o współczynnikach w $\mathbb{Z}[X]$ zmiennych $\sigma_k(\alpha_1,\ldots\alpha_n)$, $i=1,\ldots,n$. Ponieważ, na mocy wzorów Viète'*a*, zobacz (6.7), $\sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n) = (-1)^k a_{n-k} \in \mathbb{Z}$, więc widzimy, że $F(X)$ ma współczynniki całkowite. Zatem $\alpha+\beta\in\mathbb{I}$.

Dla dowodu, że $\alpha\beta\in\mathbb{I}$ rozważmy wielomian

$$G(X) = \prod_{i=1}^{n}\prod_{j=1}^{m}(X-\alpha_i\beta_j).$$

Ponieważ jest on wielomianem unormowanym, a liczba $\alpha\beta=\alpha_1\beta_1$ jest jego pierwiastkiem, więc wystarczy uzasadnić, że jest on wielomianem o współczynnikach całkowitych. Robi się to tak samo jak wyżej zapisując go uprzednio w postaci iloczynu

$$\alpha_1^m\, m_\beta\left(\frac{X}{\alpha_1}\right)\alpha_2^m\, m_\beta\left(\frac{X}{\alpha_2}\right)\cdot\ldots\cdot\alpha_n^m\, m_\beta\left(\frac{X}{\alpha_n}\right),$$

z której widać, że jest on symetryczny względem $\alpha_1, \ldots, \alpha_n$. Reszta rozumowania przebiega jak wyżej. Mamy więc $\alpha\beta\in\mathbb{I}$. □

Ćwiczenie 6.28 Udowodnić, że jeżeli α jest różną od 0 liczbą algebraiczną, to $\frac{1}{\alpha}$ jest liczbą algebraiczną tego samego stopnia.

To ćwiczenie i niewielka modyfikacja dowodu T6.6 (polegająca w gruncie rzeczy wyłącznie na zamianie $\mathbb{Z}$ na $\mathbb{Q}$) pokazują, że prawdziwy jest następujący:

WNIOSEK *Zbiór $\mathbb{A}$ liczb algebraicznych jest c i a ł e m.* □

Ćwiczenie 6.29 Udowodnić, że $\alpha \in \mathbb{A}$ wtedy i tylko wtedy, gdy istnieje taka liczba całkowita $s \in \mathbb{Z}_{\neq 0}$ i taka liczba algebraiczna całkowita α_0, że $\alpha = \alpha_0/s$. *Wskazówka.* Pomnożyć równość $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$ przez a_n^{n-1}.

Pierwszy sposób rozwiązania poniższego zadania wykorzystuje T6.6 i C6.23.

ZADANIE 6.4 Udowodnić, że jeżeli $n \in \mathbb{N}_{\geqslant 2}$, to liczba $L = \sqrt[n]{\sqrt{2}+1} + \sqrt[n]{\sqrt{2}-1}$ nie jest liczbą wymierną (LXVI OM).

Rozwiązanie. Sposób 1. (wg. Pawła Poczobuta) Ponieważ $L = \alpha + \beta$, gdzie $\alpha = \sqrt[n]{\sqrt{2}+1}$, $\beta = \sqrt[n]{\sqrt{2}-1}$, a α i β są liczbami algebraicznymi całkowitymi (liczba α spełnia równanie $(x^n-1)^2 = 2$, czyli jest pierwiastkiem wielomianu unormowanego $f(X) = X^{2n} - 2X^n - 1$, a β, podobnie, jest pierwiastkiem wielomianu $g(X) = X^{2n} + 2X^n - 1$), więc, na mocy T6.6, $L \in \mathbb{I}$. Gdyby więc L była liczbą wymierną, to, na mocy C6.23, byłaby liczbą całkowitą (zwykłą). Ale $2 < \alpha + \beta = L < 3$, gdzie pierwsza nierówność wynika z nierówności AG (bo $\alpha\beta = 1$), a druga nierówność wynika łatwo z nierówności między średnią arytmetyczną a średnią n-potęgową. Sprzeczność.

Sposób 2. (wg. Wojciecha Wawrowa) Zakładając nie wprost, że $L \in \mathbb{Q}$ widzimy, że α i β są (różnymi!) pierwiastkami wielomianu $X^2 - LX + 1 \in \mathbb{Q}[X]$ (bowiem zachodzą równości typu Viète'a $\alpha + \beta = L$ i $\alpha\beta = 1$). Przeto $\alpha = u + \sqrt{\delta}$, $\beta = u - \sqrt{\delta}$, gdzie $u = L/2 \in \mathbb{Q}$, $\delta = (L^2-4)/4 \in \mathbb{Q}$, ale $\sqrt{\delta} \notin \mathbb{Q}$ (gdyby $\sqrt{\delta} \in \mathbb{Q}$, to liczba $\alpha = u + \sqrt{\delta}$ byłaby wymiernym pierwiastkiem wielomianu $f(X) = X^{2n} - 2X^n - 1$, który jednak, jak łatwo widzieć, nie ma pierwiastków wymiernych, zobacz Z2.4). Powołując się teraz na C6.30 dostajemy sprzeczność, bo, jak łatwo sprawdzić, $f(\beta) \neq 0$. $\Diamond$

Ćwiczenie 6.30 Udowodnić, że jeżeli $u + \sqrt{\delta}$, gdzie u, δ są takie jak wyżej, jest pierwiastkiem wielomianu $F(X) \in \mathbb{Q}[X]$, to również $u - \sqrt{\delta}$ jest pierwiastkiem tego wielomianu.

Uwaga. Standardowe rozwiązanie zadania Z6.4 można przeprowadzić według schematu pokazanego w przykładzie P2 w ustępie 9.2.1.

Ćwiczenie 6.31 Niech $\omega = \omega_n$, zob. (3.35), i niech $f(X) \in \mathbb{Z}[X]$. Udowodnić, że iloczyn $f(\omega)f(\omega^2)\cdot\ldots\cdot f(\omega^{n-1})$ jest liczbą całkowitą wymierną[4].

6.3.4 Nierozkładalność wielomianów cyklotomicznych

Chcemy teraz zaprezentować dowód twierdzenia T3.21. W dowodzie wykorzystujemy parę rzeczy z tego rozdziału. Ale najważniejsza sprawa jest taka: w trakcie dowodu będziemy w istotny sposób wykorzystywać prawdziwość tezy T3.14 w pierścieniach wielomianów o współczynnikach w dowolnym ciele (w tym przypadku, ciele skończonym $\mathbb{F}_p$).

LEMAT 6.1 *Jeżeli $p \in \mathbb{P}$, to dla dowolnego wielomianu $f(X) \in \mathbb{Z}[X]$ zachodzi*

$$f(X)^p \equiv f(X^p) \,(\mathrm{mod}\, p).$$

[4]Mówimy tak (i piszemy) dla odróżnienia liczb ze zbioru $\mathbb{Z}$ od liczb z jego nadzbioru $\mathbb{I}$.

D O W Ó D. To jest natychmiastowym wnioskiem z następującej kongruencji

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_r)^p \equiv \alpha_1^p + \alpha_2^p + \cdots + \alpha_r^p \,(\mathrm{mod}\, p),$$

którą łatwo, korzystając z C2.50, udowodnić przez indukcję względem r. Mając to, piszemy

$$(a_0 + a_1X + \cdots + a_nX^n)^p \equiv a_0^p + a_1^pX^p + \cdots + a_n^p(X^n)^p \equiv a_0 + a_1X^p + \cdots + a_nX^{pn} \,(\mathrm{mod}\, p),$$

gdzie druga kongruencja wynika z MTF (w wersji (5.12)). □

Chcemy udowodnić, że wielomian cyklotomiczny $\Phi_n(X)$ jest nierozkładalny w $\mathbb{Q}[X]$, równoważnie, w $\mathbb{Z}[X]$. Oznaczmy przez $m(X)$ wielomian minimalny liczby $\omega := \omega_n$, zob. (3.35). Ponieważ $\omega \in \mathbb{I}$ (ω jest pierwiastkiem wielomianu unormowanego $X^n - 1 \in \mathbb{Z}[X]$), więc $m(X) \in \mathbb{Z}[X]$, zob. C6.27. Z definicji (3.44) widzimy, że ω jest pierwiastkiem wielomianu $\Phi_n(X)$. To, na mocy C6.21, daje podzielność $m(X)|\Phi_n(X)$. Zapiszmy $\Phi_n(X) = m(X)f(X)$. Ponieważ $m(X)$ jest nierozkładalny (zob. Z6.3), więc nierozkładalność wielomianu $\Phi_n(X)$ jest równoważna równości $m(X) = \Phi_n(X)$. Tę równość wyprowadzimy z lematu:

LEMAT 6.2 *Przy przyjętych oznaczeniach, każdy pierwiastek (zespolony) wielomianu $\Phi_n(X)$ jest też pierwiastkiem wielomianu $m(X)$.*

D O W Ó D. Niech p będzie dowolną taką liczbą pierwszą, że $p \nmid n$. Wówczas ω^p, zgodnie z definicją (3.44), jest pierwiastkiem[5] wielomianu $\Phi_n(X)$. Wobec tego zachodzi równość $m(\omega^p)f(\omega^p) = \Phi_n(\omega^p) = 0$. Udowodnimy, że $m(\omega^p) = 0$. Załóżmy, nie wprost, że $m(\omega^p) \neq 0$. Wówczas musi być $f(\omega^p) = 0$. To oznacza, że $g(\omega) = 0$, gdzie $g(X) := f(X^p)$. Wobec tego, zob. C6.21, wielomian $g(X) \in \mathbb{Z}[X]$ należy do ideału głównego (m_ω), czyli zachodzi równość $g(X) = m(X)h(X)$ dla pewnego wielomianu $h(X) \in \mathbb{Q}[X]$. W rzeczywistości, zobacz T3.15, $h(X) \in \mathbb{Z}[X]$. Stąd $f(X^p) = m(X)h(X)$, więc, na mocy L6.1, $f(X)^p \equiv m(X)h(X) \,(\mathrm{mod}\, p)$. Oznaczmy przez $\overline{f}$, $\overline{m}$, $\overline{h}$ redukcje wielomianów f, m, $g \in \mathbb{Z}[X]$ modulo p. Kongruencja $f(X)^p \equiv m(X)g(X) \,(\mathrm{mod}\, p)$ daje równość w pierścieniu $\mathbb{F}_p[X]$:

$$\overline{f}(X)^p = \overline{m}(X)\overline{h}(X). \qquad (*)$$

Załóżmy, że $k(X) \in \mathbb{F}_p[X]$ jest pewnym, nierozkładalnym w $\mathbb{F}_p[X]$, dzielnikiem wielomianu $\overline{m}(X)$. Wówczas, dzięki jednoznaczności rozkładu w $\mathbb{F}_p[X]$, zob. T3.14, i równości $(*)$, dostajemy podzielność $k(X)|f(X)$. Ponieważ jednocześnie $\overline{\Phi_n}(X) = \overline{m}(X)\overline{f}(X)$, więc dostajemy $k(X)^2|\overline{\Phi_n}(X)$ w pierścieniu $\mathbb{F}_p[X]$. Wiemy też, że $\Phi_n(X|X^n - 1$ w $\mathbb{Z}[X]$. Ta podzielność, po redukcji $(\mathrm{mod}\, p)$, daje podzielność $k(X)^2|X^n - \overline{1}$ w $\mathbb{F}_p[X]$. To jest jednakowoż sprzeczne z tezą zadania Z6.1, bo wielomian $X^n - \overline{1}$ jest, oczywiście(?!), względnie pierwszy ze swoją pochodną $\overline{n}X^{n-1}$ (pamiętamy założenie $p \nmid n$, czyli $\overline{n} \neq 0$ w $\mathbb{F}_p$). Otrzymana sprzeczność dowodzi, że $m(\omega^p) = 0$ dla każdej liczby pierwszej $p \nmid n$. Najprościej dokończyć dowód za pomocą twierdzenia Dirichlet'*a* T5.19: Każdy pierwiastek wielomianu $\Phi_n(X)$ jest postaci ω^k, gdzie $k \perp n$. Wybieramy liczbę pierwszą p postaci $qn + k$. Takich jest mnóstwo. I, wobec już dowiedzionego, mamy $0 = m(\omega^p) = m(\omega^k)$. □

Ćwiczenie 6.32 Dokończyć dowód nierozkładalności wielomianów cyklotomicznych.

[5]Po wykonaniu dzielenia z resztą $p = qn + k$, widzimy, że $k \perp n$ i $\omega^p = \omega^k$.

6.3.5 Liczby przestępne

Liczba (zespolona) nie będąca liczbą algebraiczną nazywa się, jak wiemy, liczbą p r z e s t ę p n ą.

I s t n i e n i e liczb przestępnych zostało udowodnione w połowie XIX wieku przez matematyka francuskiego Josepha Liouville'*a*. Metodę Liouville'*a* dowodu istnienia liczb przestępnych zaprezentujemy w kolejnym ustępie.

W roku 1872 Charles Hermite (Francja) udowodnił, że pewna ważna stała matematyczna, liczba e (podstawa logarytmów naturalnych), jest liczbą przestępną. W tym samym mniej więcej czasie Georg Cantor (Niemcy) za pomocą nowatorskiego i genialnie prostego rozumowania uzasadnił, że algebraiczność liczby rzeczywistej (czy zespolonej) jest własnością w y j ą t k o w ą, a przestępność jest własnością t y p o w ą. Schemat jego rozumowania jest następujący:

- ▷ wszystkie liczby wymierne można ponumerować (liczbami naturalnymi), więc
- ▷ wszystkie wielomiany o współczynnikach wymiernych można ponumerować, więc
- ▷ wszystkie liczby algebraiczne można ponumerować, a
- ▷ liczb rzeczywistych (tym bardziej liczb zespolonych) n i e d a się ponumerować.

Mówiąc w skrócie: *zbiór liczb algebraicznych jest zbiorem przeliczalnym, a zbiór liczb rzeczywistych (tym bardziej więc jego nadzbiór – zbiór liczb zespolonych) n i e j e s t przeliczalny*. Porównaj $\mathbb{KOM}$, rozdział 1.

Jednym z piękniejszych twierdzeń matematyki jest

TWIERDZENIE 6.7 (***Lindemann*, 1881**) *Liczba π jest liczbą przestępną.* □

Z twierdzenia Lindemanna wynika n e g a t y w n e rozwiązanie problemu **kwadratury koła**, czyli konstrukcji (za pomocą cyrkla i linijki) kwadratu o polu równym polu koła o promieniu 1. Równoważnie: konstrukcji odcinka długości $\sqrt{\pi}$. Nietrudno udowodnić, że konstruowalne są wyłącznie odcinki o długościach będących liczbami algebraicznymi, a i t o z d e c y d o w a n i e n i e w s z y s t k i e. A liczba $\sqrt{\pi}$ jest przestępna. [Gdyby $\sqrt{\pi} \in \mathbb{A}$, to byłoby $\pi = \sqrt{\pi}\sqrt{\pi} \in \mathbb{A}$, zob. WT6.6.]

6.3.6 Twierdzenie Liouville'*a*

Udowodnimy tu pewną własność liczb algebraicznych rzeczywistych. Mówi ona, że takie liczby niezbyt dobrze dają się przybliżać liczbami wymiernymi.

TWIERDZENIE 6.8 (***Liouville***) *Jeżeli $\alpha \in \mathbb{R}$ jest liczbą algebraiczną stopnia n, to istnieje taka liczba dodatnia C, że dla dowolnej liczby wymiernej h/k zachodzi nierówność*

$$\left|\alpha - \frac{h}{k}\right| > \frac{C}{k^n}. \tag{6.19}$$

D O W Ó D. Niech $f(X) = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$ będzie wielomianem stowarzyszonym z wielomianem minimalnym liczby α. Rozważmy przedział $[\,\alpha - 1;\, \alpha + 1\,]$. W tym przedziale pochodna f' wielomianu f jest ograniczona

$$|f'(x)| \leqslant M.$$

Możemy oczywiście założyć, że $M > 1$. Połóżmy $C = \frac{1}{M}$. Przy takim C nierówność (6.19) jest, oczywiście, spełniona dla każdego h/k leżącego poza przedziałem $[\,\alpha - 1;\, \alpha + 1\,]$. Jeżeli zaś $|\alpha - h/k| \leqslant 1$, to mamy (na mocy twierdzenia o wartości średniej T6.2)

$$\left| f\left(\frac{h}{k}\right)\right| = \left| f\left(\frac{h}{k}\right) - f(\alpha)\right| = |f'(\mu)| \cdot \left|\frac{h}{k} - \alpha\right|,$$

dla pewnego μ leżącego między α a h/k. Stąd

$$\left|\frac{h}{k} - \alpha\right| = \frac{|f(h/k)|}{|f'(\mu)|} \geqslant \frac{1}{M} \cdot \left| f\left(\frac{h}{k}\right)\right| = C \cdot \frac{|a_0k^n + a_1k^{n-1}h + \,\ldots\, + a_nh^n|}{|k^n|} \geqslant \frac{C}{k^n},$$

bo $a_0k^n + a_1k^{n-1}h + \,\ldots\, + a_nh^n = f(h/k)k^n$ jest niezerową liczbą całkowitą, więc jej wartość bezwzględna jest $\geqslant 1$. □

Twierdzenie Liouville'*a* ma wartość teoretyczną: za jego pomocą po raz pierwszy w historii udowodniono (dokładniej: Liouville udowodnił) i s t n i e n i e liczb przestępnych:

ZADANIE 6.5 Udowodnić, że liczba $\lambda = \sum_{s=1}^{\infty} 10^{-s!}$ jest liczbą przestępną.

R o z w i ą z a n i e. Załóżmy, nie wprost, że λ jest liczbą algebraiczną stopnia n i wybierzmy tak duże $N \in \mathbb{N}$, aby

$$N > n \quad \text{oraz} \quad 10^{N!-1} > \frac{1}{C},$$

gdzie C jest stałą występującą w twierdzeniu Liouville'*a*. Niech h/k oznacza sumę N początkowych wyrazów szeregu definiującego liczbę λ. Wówczas $k = 10^{N!}$ i

$$\left|\lambda - \frac{h}{k}\right| = \sum_{s=N+1}^{\infty} 10^{-s!} < \frac{10}{10^{(N+1)!}} = \frac{10}{k^{N+1}} < \frac{C}{k^n},$$

co jest sprzeczne z tezą twierdzenia Liouville'*a*. ◊

U w a g a 1. W zadaniach olimpijskich wykorzystuje się nierówności postaci (6.19) dla liczb algebraicznych małych stopni, zazwyczaj niewymierności kwadratowych, na przykład:

Ćwiczenie 6.33 Udowodnić, że dla dowolnej liczby wymiernej a/b zachodzi:

$$\left|\sqrt{2} - \frac{a}{b}\right| > \frac{1}{(2\sqrt{2}+2)b^2} > \frac{1}{5b^2}. \tag{6.20}$$

Dzięki szacowaniu (6.20) możemy rozwiązać trudne zadanie:

ZADANIE 6.6 Udowodnić, że istnieje taki ciąg nieskończony liczb rzeczywistych (s_n), że $|s_n| \leqslant 5$ dla każdego n oraz dla dowolnych dwóch indeksów $k \neq l$ zachodzi nierówność

$$|s_k - s_l| \geqslant \frac{1}{|k-l|}. \tag{6.21}$$

R o z w i ą z a n i e. Twierdzimy, że ciąg (s_n) dany wzorem $s_n = 5\{n\sqrt{2}\}$ (gdzie $\{x\} = x - \lfloor x \rfloor$ oznacza część ułamkową liczby rzeczywistej x, zobacz paragraf 12.1) jest ciągiem spełniającym warunek (6.21). Istotnie, $0 \leqslant s_n < 5$. Ponadto,

$$|s_k - s_l| = 5|\{k\sqrt{2}\} - \{l\sqrt{2}\}| = 5|k\sqrt{2} - \lfloor k\sqrt{2}\rfloor - l\sqrt{2} + \lfloor l\sqrt{2}\rfloor| = 5|k-l| \cdot \left|\sqrt{2} - \frac{q}{k-l}\right|,$$

gdzie $q = \lfloor k\sqrt{2}\rfloor - \lfloor l\sqrt{2}\rfloor$. To, wobec nierówności (6.20), kończy uzasadnienie. ◊

U w a g a 2. Wartość stałej C z nierówności (6.19) nie jest zazwyczaj ważna. Ważne jest i s t n i e n i e takiej stałej. Stała $C = 1/(2\sqrt{2}+2)$, której istnienia w (6.20) dowodzimy według wzoru z dowodu T6.8 (wielomianem minimalnym liczby $\sqrt{2}$ jest $X^2 - 2$), może być łatwo zwiększona do $C = 1/4$. Na przykład tak: gdy $a/b \in [\,\sqrt{2}-1;\, \sqrt{2}+1\,]$, to

$$\left|\sqrt{2} - \frac{a}{b}\right| = \frac{|2b^2 - a^2|}{b^2\left|\sqrt{2} + \frac{a}{b}\right|} \geqslant \frac{1}{b^2\left|\sqrt{2} + \frac{a}{b}\right|} \geqslant \frac{1}{b^2(\sqrt{2}+\sqrt{2}+1)} > \frac{1}{4b^2}.$$

Gdy $a/b \notin [\,\sqrt{2}-1;\, \sqrt{2}+1\,]$, nierówności $|\sqrt{2} - a/b| > 1/b^2 > 1/4b^2$ są oczywiste.

6.4 O zerach wielomianów wielu zmiennych

W tym paragrafie powiemy kilka słów o zerach (miejscach zerowych) wielomianów wielu zmiennych. W szczególności zaprezentujemy ciekawe uogólnienie T3.4, tak zwane kombinatoryczne twierdzenie o zerach.

Wiemy, że każdy wielomian jednej zmiennej $f(X) \in \mathcal{R}[X]$ w y z n a c z a funkcję wielomianową, $\mathcal{R} \ni \alpha \longmapsto f(\alpha) \in \mathcal{R}$. Oznaczamy ją tą samą literą f. Podobnie dla wielomianów wielu zmiennych: jeżeli $F(X_1, \ldots, X_n) \in \mathcal{R}[X_1, \ldots, X_n]$ jest takim wielomianem, to

$$\mathcal{R}^n \ni (\alpha_1, \ldots, \alpha_n) \longmapsto F(\alpha_1, \ldots, \alpha_n) \in \mathcal{R}$$

jest wyznaczoną przez F funkcją (wielomianową) określoną na $\mathcal{R}^n := \mathcal{R} \times \cdots \times \mathcal{R}$ (n-krotny iloczyn kartezjański), czyli na zbiorze wszystkich ciągów długości n o wyrazach z $\mathcal{R}$. Jeżeli $\mathcal{R} = \mathbb{K}$ jest ciałem (w dalszym ciągu ograniczamy się do takiego przypadku), to zbiór $\mathbb{K}^n$ nazywamy n-wymiarową **arytmetyczną przestrzenią wektorową** nad ciałem $\mathbb{K}$. Element $(\alpha_1, \ldots, \alpha_n)$ przestrzeni $\mathbb{K}^n$ nazywamy **wektorem** i oznaczamy w skrócie $\boldsymbol{\alpha}$.

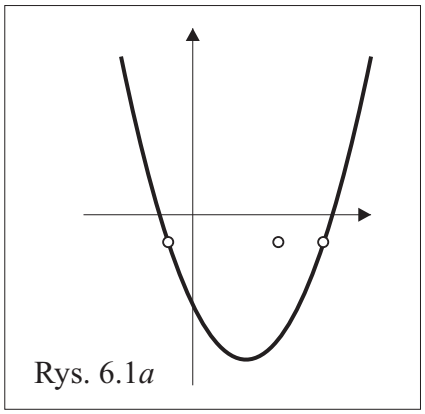
Używamy takiego oznaczenia (zob. też ustęp 5.4.4): Jeżeli $F(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n]$ jest wielomianem o współczynnikach w ciele $\mathbb{K}$, to przez $\mathcal{N}(F; \mathbb{K})$ oznaczamy zbiór miejsc zerowych wielomianu F w $\mathbb{K}^n$. To znaczy:

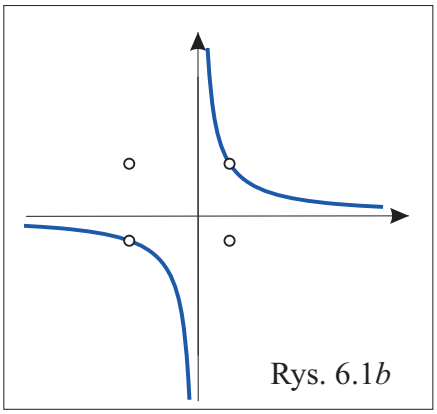
$$\mathcal{N}(F; \mathbb{K}) := \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n : F(\alpha_1, \ldots, \alpha_n) = 0\}. \tag{6.22}$$

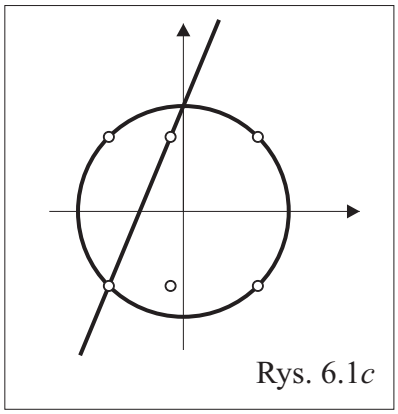
Ćwiczenie 6.34 Jeżeli $F_i(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n]$, dla $i = 1, \ldots, r$, są wielomianami o współczynnikach w ciele, a $P(X_1, \ldots, X_n)$ jest ich iloczynem, to zachodzi równość

$$\mathcal{N}(P; \mathbb{K}) = \mathcal{N}(F_1; \mathbb{K}) \cup \mathcal{N}(F_2; \mathbb{K}) \cup \cdots \cup \mathcal{N}(F_r; \mathbb{K}).$$

Na rysunkach 6.1 widzimy ilustracje zbiorów $\mathcal{N}(F;\mathbb{R})$ dla wielomianów: $X^2-4X-Y-5$, $XY-1$ oraz $-3X^3+Y^3+X^2Y-3XY^2-2X^2-2Y^2+12X-4Y+8$. Przy tym na rysunku 6.1c rozpoznajemy sumę $\mathcal{N}(X^2+Y^2-4;\mathbb{R})\cup\mathcal{N}(-3X+Y-2;\mathbb{R})$.


Rys. 6.1a


Rys. 6.1b


Rys. 6.1c

6.4.1 Combinatorial Nullstellensatz

Imię ***Combinatorial Nullstellensatz***[6] (***Kombinatoryczne Twierdzenie o Zerach***), nadane twierdzeniu T6.9, jest coraz szerzej używane. Jest ono uogólnieniem, na przypadek wielu zmiennych, twierdzenia Lagrange'a T3.4.

Ćwiczenie 6.35 Dany jest wielomian $h(X)\in\mathbb{K}[X]$ stopnia $k\geqslant 0$ o współczynnikach w ciele $\mathbb{K}$. Udowodnić, że jeżeli $A\subseteq\mathbb{K}$ i $|A|>k$, to $A\smallsetminus\mathcal{N}(h;\mathbb{K})\neq\varnothing$, czyli że istnieje takie $\alpha\in A$, że $h(\alpha)\neq 0$. (Pamiętamy, że wielomian stopnia 0 jest s t a ł ą różną od 0.)

Oto uogólnienie tej tezy na przypadek wielomianów wielu zmiennych:

TWIERDZENIE 6.9 (***Combinatorial Nullstellensatz*** **– 1996**) *Dany jest wielomian* $F(X_1,X_2,\ldots,X_n)\in\mathbb{K}[X_1,X_2,\ldots,X_n]$. *Niech* $\deg(F)=k_1+k_2+\ldots+k_n$, *gdzie* k_i *są nieujemnymi liczbami całkowitymi, i niech jednomian* $X_1^{k_1}X_2^{k_2}\cdot\ldots\cdot X_n^{k_n}$ *występuje w wielomianie* F *z n i e z e r o w y m współczynnikiem. Wówczas, dla dowolnych podzbiorów* $A_1,A_2,\ldots,A_n\subseteq\mathbb{K}$ *spełniających warunki* $|A_i|>k_i$ *dla* $i=1,2,\ldots,n$, *istnieje taki ciąg* $(\alpha_1,\alpha_2,\ldots,\alpha_n)\in A_1\times A_2\times\cdots\times A_n$, *że* $F(a_1,a_2,\ldots,a_n)\neq 0$.

D O W Ó D. Dowód przeprowadzimy dla wielomianu dwóch zmiennych Y, X przez indukcję względem stopnia $d=\deg(F)$. Sprawa jest prosta, gdy $d=1$. Rzeczywiście, wówczas $F(Y,X)=bY+aX+c$. Załóżmy, że $a\neq 0$, czyli że jednomian $aX=aX^1Y^0$ występuje w wielomianie F z niezerowym współczynnikiem, i że $|A|>1$, $|B|>0$, i $\alpha_1,\alpha_2\in A\subseteq\mathbb{K}$, $\alpha_1\neq\alpha_2$ i $\beta\in B\subseteq\mathbb{K}$. Równości $F(\beta,\alpha_1)=F(\beta,\alpha_2)=0$, czyli $a\alpha_1=-b\beta-c=a\alpha_2$, wobec założenia $a\neq 0$, dają $\alpha_1=\alpha_2$. Sprzeczność.

Załóżmy więc, że teza jest prawdziwa dla wszystkich wielomianów stopni $<d$ i rozważmy wielomian $F(Y,X)\in\mathbb{K}[Y,X]$ stopnia $d=l+k$, zawierający jednomian bY^lX^k, gdzie $b\neq 0$.

[6]Nazwa nawiązuje do, leżącego u podstaw wielkiej i ważnej dziedziny matematyki – **geometrii algebraicznej**, sto lat wcześniejszego i znacznie mniej elementarnego, **twierdzenia Hilberta o zerach**. Nazwa **Nullstellensatz** używana jest nie tylko w języku niemieckim.

Możemy (b.s.o.) założyć, że $k \geqslant 1$. Zapiszmy $F(Y, X)$ w postaci

$$F(Y, X) = f_0(Y) + f_1(Y)X + \cdots + f_t(Y)X^t \tag{6.23}$$

wielomianu zmiennej X o współczynnikach w $\mathbb{K}[Y]$. Niech $A, B \subseteq \mathbb{K}$ będą podzbiorami spełniającymi warunki $|A| > k$, $|B| > l$. Niech $\alpha \in A$ będzie dowolnym ustalonym elementem. Dokładnie tak samo jak w dowodzie T3.1 obliczamy różnicę $F(Y, X) - F(Y, \alpha)$:

$$\sum_{j=0}^{t} f_j(Y)X^j - \sum_{j=0}^{t} f_j(Y)\alpha^j = \sum_{j=1}^{t} f_j(Y)(X^j - \alpha^j) = (X - \alpha)\sum_{j=1}^{t} f_j(Y)g_{j-1}(X),$$

gdzie $X^j - \alpha^j = (X - \alpha)(X^{j-1} + \alpha X^{j-2} + \cdots + \alpha^{j-1}) =: (X - \alpha)g_{j-1}(X)$. Mamy więc

$$F(Y, X) = (X - \alpha)G(Y, X) + F(Y, \alpha), \tag{6.24}$$

gdzie $G(Y, X) = f_1(Y) + f_2(Y)g_1(X) + \cdots + f_t(Y)g_{t-1}(X)$. Wielomian $G(Y, X)$ jest wielomianem stopnia $d - 1$. Sprawdzamy, że jednomian $Y^l X^{k-1}$ stopnia $d - 1$ występuje w nim ze współczynnikiem równym b. Po pierwsze, w sumie (6.23) jednomian ten znajdujemy (tylko) w iloczynie $f_k(Y)X^k$, więc $f_k(Y) = bY^l +$ *wyrazy niższego stopnia* (wyrazów stopnia wyższego niż l nie ma, bo $\deg F(Y, X) = l + k$), skąd widzimy, że $f_k(Y)g_{k-1}(X)$ jest postaci $bY^l X^{k-1} +$ *wyrazy niższego stopnia względem* Y. Po drugie, ponieważ $\deg g_{j-1}(X) = j - 1$, więc w iloczynach $f_j(Y)g_{j-1}(X)$, dla $j < k$, jednomiany $Y^l X^{k-1}$ nie występują. Po trzecie, w iloczynach $f_j(Y)g_{j-1}(X)$, dla $j > k$, jednomiany $Y^l X^{k-1}$ nie występują, bo wtedy $\deg f_j(Y) + j \leqslant d = l + k < l + j$, czyli $\deg f_j(Y) < l$.

Wobec tego, na mocy założenia indukcyjnego, istnieje $(\beta, \alpha_1) \in B \times (A \setminus \{\alpha\})$, dla którego $G(\beta, \alpha_1) \neq 0$. Wówczas, na mocy (6.24), $F(\beta, \alpha_1) - F(\beta, \alpha) = (\alpha_1 - \alpha)G(\beta, \alpha_1) \neq 0$, skąd $F(\beta, \alpha_1) \neq F(\beta, \alpha)$. Zatem, co najmniej jedna z wartości $F(\beta, \alpha_1)$, $F(\beta, \alpha)$ jest $\neq 0$. W ten sposób kończymy dowód w przypadku dwóch zmiennych. Dowód dla wielomianu większej liczby zmiennych jest prostym uogólnieniem przedstawionego. □

CN (Combinatorial Nullstellensatz), którego ilustracje Czytelnik zechce dostrzec na rysunkach 6.1, stosuje się zazwyczaj w kombinatoryce.

P r z y k ł a d 1. (***Zadanie o broszkach***) Przy okrągłym stole siedzi n posłanek. Każda ma w torebce dwie różne broszki. Czy mogą one tak wybrać jedną z posiadanych broszek i przypiąć sobie do żakietu, by żadne dwie sąsiadki nie miały przypiętej takiej samej? Aby odpowiedzieć na to pytanie rozważmy *cykliczny wielomian broszkowy*

$$B_c(X_1, X_2, \ldots, X_n) := (X_1 - X_2)(X_2 - X_3) \cdot \ldots \cdot (X_{n-1} - X_n)(X_n - X_1)$$

i zauważmy, że $B_c(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ wtedy i tylko wtedy, gdy zachodzi co najmniej jedna równość $\alpha_j = \alpha_{j+1}$ (indeksy liczymy cyklicznie, tzn. $\alpha_{n+1} = \alpha_1$).

Ponumerujmy teraz wszystkie broszki tak, by różne broszki miały różne numery. Niech A_i będzie dwuelementowym zbiorem numerów broszek w i-tej torebce. Możliwość pożądanego wyboru broszek jest równoważna możliwości wyboru takiego $(\alpha_1, \ldots, \alpha_n) \in A_1 \times \cdots \times A_n$, że $B_c(\alpha_1, \ldots, \alpha_n) \neq 0$. Taki wybór, z kolei, na mocy CN, jest na pewno możliwy, gdy w wielomianie B_c występuje jednomian $aX_1X_2 \cdot \ldots \cdot X_n$ z niezerowym współczynnikiem a. Można sprawdzić, że $a = 2$, gdy $2|n$, ale $a = 0$, gdy $2 \nmid n$, zob. C6.35. ◊

Podkreślmy, że najdelikatniejszym momentem w stosowaniu twierdzenia CN jest szukanie jednomianu $aX_1^{k_1}X_2^{k_2} \cdot \ldots \cdot X_n^{k_n}$ stopnia $\deg F$ z niezerowym współczynnikiem.

Ćwiczenie 6.36 Udowodnić, że po wymnożeniu (tzn., "otwarciu nawiasów") w iloczynie $(X_1-X_2)(X_2-X_3)\cdot\ldots\cdot(X_n-X_1)$ dostajemy sumę 2^n jednomianów stopnia n, wśród których jedyną redukcją wyrazów podobnych jest suma $X_1\cdot\ldots\cdot X_n+(-1)^nX_1\cdot\ldots\cdot X_n$. *Wskazówka.* Dobrze jest najpierw zbadać jednomiany (stopnia $n-1$, innych tam nie ma!) w niecyklicznym wielomianie broszkowym[7] $B(X_1,\,X_2,\ldots,\,X_n):=(X_1-X_2)(X_2-X_3)\cdot\ldots\cdot(X_{n-1}-X_n)$.

Czasami stosuje się CN "w drugą stronę".

P r z y k ł a d 2. Udowodnimy, że *jednomian* $X_1X_2X_3X_4$ *n i e występuje w wielomianie*

$$(X_1+X_2+X_3+X_4)(X_1+X_2+X_3-X_4)(X_1+X_2-X_3-X_4)(X_1-X_2-X_3-X_4),$$

to znaczy występuje ze współczynnikiem równym 0. Rzeczywiście, gdyby tak nie było, to, na mocy CN, moglibyśmy w zbiorze $\{1,\,-1\}\times\{1,\,-1\}\times\{1,\,-1\}\times\{1,\,-1\}$ znaleźć ciąg $(\varepsilon_1,\,\varepsilon_2,\,\varepsilon_3,\,\varepsilon_4)$, dla którego liczby $c_1=\varepsilon_1+\varepsilon_2+\varepsilon_3+\varepsilon_4$, $c_2=\varepsilon_1+\varepsilon_2+\varepsilon_3-\varepsilon_4$, $c_3=\varepsilon_1+\varepsilon_2-\varepsilon_3-\varepsilon_4$ i $c_4=\varepsilon_1-\varepsilon_2-\varepsilon_3-\varepsilon_4$ byłyby różne od 0. To jest n i e m o ż l i w e, zobacz C6.37. Łatwo bowiem zauważyć, że wszystkie te liczby są parzyste, a kolejne różnią się o 2, tzn., $|c_1-c_2|=|c_2-c_3|=|c_3-c_4|=2$. ◊

Ćwiczenie 6.37 Udowodnić **dyskretną własność Darboux** ciągów o wyrazach całkowitych: *Jeżeli* (d_n) *jest takim ciągiem o wyrazach całkowitych, że* $|d_n-d_{n+1}|=1$ *dla każdego* n, *a liczba* $a\in\mathbb{Z}$ *spełnia nierówności* $d_k\leqslant a\leqslant d_{k+r}$ *dla pewnych* $k,\,r\in\mathbb{N}$, *to istnieje taka liczba całkowita* $0\leqslant s\leqslant r$, *że* $d_{k+s}=a$.

Ćwiczenie 6.38 Niech $F_k(X_1,\ldots,\,X_n)=\sum_{j=1}^{k}X_j-\sum_{j=k+1}^{n}X_j$ dla $k=1,\ldots,\,n$. Udowodnić, że jeżeli $2|n$, to jednomian $X_1X_2\cdot\ldots\cdot X_n$ nie występuje w iloczynie $F_1F_2\cdot\ldots\cdot F_n$.

ZADANIE 6.7 Dana jest liczba naturalna n i podzbiór przestrzeni trójwymiarowej $\mathbb{R}^3$:

$$\mathcal{A}=\{(x,\,y,\,z)\in\mathbb{R}^3:\,x,\,y,\,z\in\mathbb{Z}\quad\text{oraz}\quad 0\leqslant x,\,y,\,z\leqslant n\}.$$

Wyznaczyć n a j m n i e j s z ą liczbę płaszczyzn, których suma (teoriomnogościowa) zawiera zbiór $\mathcal{A}\setminus\{(0,\,0,\,0)\}$ i n i e zawiera punktu $(0,\,0,\,0)$. (IMO'2007)

R o z w i ą z a n i e. Płaszczyzna o równaniu $ax+by+cz+d=0$ jest zbiorem miejsc zerowych wielomianu $aX+bY+cZ+d\in\mathbb{R}[X,\,Y,\,Z]$, czyli zbiorem $\mathcal{N}(aX+bY+cZ+d;\,\mathbb{R})$. Łatwo wskazać $3n$ płaszczyzn, których suma (teoriomnogościowa) zawiera zbiór $\mathcal{A}\setminus\{(0,\,0,\,0)\}$ i nie zawiera punktu $(0,\,0,\,0)$. To są płaszczyzny $\mathcal{N}(X-1;\,\mathbb{R}),\,\mathcal{N}(X-2;\,\mathbb{R}),\ldots,\,\mathcal{N}(X-n;\,\mathbb{R})$ prostopadłe do osi Ox, płaszczyzny $\mathcal{N}(Y-1;\,\mathbb{R}),\,\mathcal{N}(Y-2;\,\mathbb{R}),\ldots,\,\mathcal{N}(Y-n;\,\mathbb{R})$ prostopadłe do osi Oy i płaszczyzny $\mathcal{N}(Z-1;\,\mathbb{R}),\,\mathcal{N}(Z-2;\,\mathbb{R}),\ldots,\,\mathcal{N}(Z-n;\,\mathbb{R})$ prostopadłe do osi Oz. Sumą tych płaszczyzn jest zbiór $\mathcal{N}(G;\,\mathbb{R})$, gdzie

$$G(X,\,Y,\,Z)=\prod_{j=1}^{n}(X-j)(Y-j)(Z-j),$$

[7]Wielomian broszkowy (cykliczny i niecykliczny) jest przykładem **wielomianu Petersena** danego skończonego grafu prostego $\boldsymbol{G}=(\mathcal{V},\,\mathcal{E})$: $P_{\boldsymbol{G}}(X_1,\ldots,\,X_v):=\prod_{i<j}(X_i-X_j)^{\chi(\{A_i,A_j\})}$, gdzie $\mathcal{V}=\{A_1,\,A_2,\ldots,\,A_v\}$, a $\chi:\mathcal{P}_2(\mathcal{V})\to\{0,\,1\}$ jest funkcją charakterystyczną podzbioru $\mathcal{E}\subseteq\mathcal{P}_2(\mathcal{V})$. Dla oznaczeń zob. $\mathbb{KOM}$.

zobacz C6.34. Pokażemy, że żadna liczba $k < 3n$ płaszczyzn nie jest dobra. Załóżmy nie wprost, że $a_jx+b_jy+c_jz+d_j=0$, dla $j=1, 2, \ldots, k$, są równaniami płaszczyzn czyniących zadość narzuconym wymaganiom i rozważmy wielomian

$$H(X, Y, Z) = \prod_{j=1}^{k} (a_jX + b_jY + c_jZ + d_j).$$

Stopień tego wielomianu jest równy k. Zgodnie z założeniem mamy $H(x, y, z) = 0$ dla każdego $(x, y, z) \in \mathcal{A} \setminus \{(0, 0, 0)\}$, ale $H(0, 0, 0) \neq 0$. Wobec tego różnica $\lambda G - H$, przy dowolnej stałej $\lambda \in \mathbb{R}_{\neq 0}$, zeruje się dla wszystkich $(x, y, z) \in \mathcal{A} \setminus \{(0, 0, 0)\}$. Jednocześnie, ponieważ zarówno $H(0, 0, 0)$ jak i $G(0, 0, 0)$ są różne od 0, więc, dla $\lambda = \frac{H(0,0,0)}{G(0,0,0)}$, wielomian $F = \lambda G - H$ zeruje się na całym zbiorze $\mathcal{A}$. Ale $\deg F = 3n$, (zob. C3.70(2)), i jednomian $X^nY^nZ^n$ występuje w wielomianie F ze współczynnikiem λ, więc, na mocy CN, nie może się zerować na całym $\mathcal{A} = \{0, 1, \ldots, n\} \times \{0, 1, \ldots, n\} \times \{0, 1, \ldots, n\}$. Sprzeczność, $\Diamond$

Ćwiczenie 6.39 (Dla Czytelników nie bojących się przestrzeni n-wymiarowej $\mathbb{R}^n$.) Udowodnić, że jeżeli $H_i = \mathcal{N}(a_{i1}X_1+\cdots+a_{in}X_n+b_i; \mathbb{R})$, $i = 1, \ldots, r$, jest rodziną hiperpłaszczyzn pokrywającą wszystkie punkty zbioru $\{1, 2\}^n$ z wyjątkiem $(1, \ldots, 1)$, to $r \geqslant n$.

6.4.2 Kilka zastosowań

Pokażemy jeszcze kilka klasycznych zastosowań kombinatorycznego twierdzenia o zerach.

Twierdzenie Erdősa, Ginzburga, Ziva

ZADANIE 6.8 Udowodnić ***twierdzenie Erdősa, Ginzburga, Ziva***: *W każdym ciągu długości $2n-1$ o wyrazach całkowitych, istnieje podciąg długości n, suma wyrazów którego jest podzielna przez n.*

Rozwiązanie. Udowodnimy to dla $n = p$ będącego liczbą pierwszą. Weźmy ciąg $2p-1$ liczb całkowitych. Jasne, że obchodzą nas tylko reszty z dzielenia tych liczb przez p. Ustawiamy te reszty następująco $r_1 \leqslant r_2 \leqslant r_3 \leqslant \ldots \leqslant r_{2p-1}$ i traktujemy jako elementy w $\mathbb{F}_p$. Wówczas, jeżeli istnieje taki wskaźnik k, że $r_k = r_{k+p-1}$, to $r_k + r_{k+1} + \ldots + r_{k+p-1} = pr_k$ i mamy podciąg długości p, suma wyrazów którego jest podzielna przez p. Jeżeli zaś nie ma takiego k, to rozważmy podzbiory dwuelementowe

$$A_1 = \{r_1, r_p\},\ A_2 = \{r_2, r_{p+1}\},\ \ldots,\ A_{p-1} = \{r_{p-1}, r_{2p-2}\}$$

ciała $\mathbb{F}_p$ i jeden podzbiór jednoelementowy $A_p = \{r_{2p-1}\}$. Rozważmy wielomian

$$W(X_1, X_2, \ldots, X_p) = (X_1 + X_2 + \ldots + X_p)^{p-1} - 1 \in \mathbb{F}_p[X_1, X_2, \ldots, X_p].$$

Wielomian ten ma stopień równy $p-1$, współczynnik przy $X_1X_2\cdot\ldots\cdot X_{p-1}$ jest równy $(p-1)!$, czyli jest różny od zera w $\mathbb{F}_p$, zobacz twierdzenie Wilsona. Na mocy CN znajdziemy więc taki element $(\alpha_1, \alpha_2, \ldots, \alpha_p) \in A_1 \times A_2 \times \ldots \times A_p$, że $W(\alpha_1, \alpha_2, \ldots, \alpha_p) \neq 0$. To oznacza, że $C := \alpha_1 + \ldots + \alpha_p$ jest podzielna przez p. Gdyby bowiem $p \nmid C$, to, na mocy małego twierdzenia Fermat'a, byłoby $p|C^{p-1} - 1$, czyli $W(\alpha_1, \ldots, \alpha_n) = 0$ w $\mathbb{F}_p$. $\Diamond$

Ćwiczenie 6.40 Udowodnić twierdzenie EGZ dla dowolnego n. *Wskazówka.* Liczbę naturalną n nazwij liczbą *miłą*, gdy dla niej zachodzi teza Z6.8. Udowodnij, że iloczyn liczb miłych jest liczbą miłą.

Twierdzenie Cauchy'*ego*-Davenporta

Wprowadzimy oznaczenie: Jeżeli $\mathcal{A}$, $\mathcal{B}$ są podzbiorami pewnego ciała (lub pierścienia, lub grupy z działaniem $+$), to przez $\mathcal{A}+\mathcal{B}$ oznaczamy zbiór wszystkich sum postaci $\alpha+\beta$, gdzie $\alpha\in\mathcal{A}$, $\beta\in\mathcal{B}$. Twierdzenie Cauchy'*ego*-Davenporta, które udowodnimy za pomocą CN, podaje oszacowanie liczby elementów w zbiorze $\mathcal{A}+\mathcal{B}$, gdzie $\mathcal{A}$, $\mathcal{B}$ są podzbiorami ciała $\mathbb{F}_p$.

TWIERDZENIE 6.10 (***Twierdzenie Cauchy'*ego-*Davenporta***) *Jeżeli $\mathcal{A}$, $\mathcal{B}$ są niepustymi podzbiorami ciała $\mathbb{F}_p$, to $|\mathcal{A}+\mathcal{B}|\geqslant\min(p,\,|\mathcal{A}|+|\mathcal{B}|-1)$.*

D O W Ó D. Sprawdzamy najpierw, że jeżeli $|\mathcal{A}|+|\mathcal{B}|>p$, to $\mathcal{A}+\mathcal{B}=\mathbb{F}_p$. Rzeczywiście, wybierzmy dowolny element $\gamma\in\mathbb{F}_p$ i rozważmy zbiór $\gamma-\mathcal{B}:=\{\gamma-\beta:\ \beta\in\mathcal{B}\}$. Jasne, że $|\gamma-\mathcal{B}|=|\mathcal{B}|$ (bo $\beta\longmapsto\gamma-\beta$ jest bijekcją $\mathcal{B}$ na $\gamma-\mathcal{B}$). Więc $|\mathcal{A}|+|\gamma-\mathcal{B}|>p=|\mathbb{F}_p|$. Zatem zbiory $\mathcal{A}$ i $\gamma-\mathcal{B}$ nie mogą być rozłączne (Zasada Łat na Kapocie!, zob. $\mathbb{KOM}$). Niech $\alpha_0=\gamma-\beta_0$ będzie ich wspólnym elementem. Wtedy $\gamma=\alpha_0+\beta_0\in\mathcal{A}+\mathcal{B}$.

Załóżmy więc, że $|\mathcal{A}|+|\mathcal{B}|\leqslant p$ i, nie wprost, że $|\mathcal{A}+\mathcal{B}|\leqslant|\mathcal{A}|+|\mathcal{B}|-2$. Niech $\mathcal{C}$ będzie takim podzbiorem w $\mathbb{F}_p$, że $\mathcal{A}+\mathcal{B}\subseteq\mathcal{C}$ oraz $|\mathcal{C}|=|\mathcal{A}|+|\mathcal{B}|-2$. I niech

$$F(X,\,Y)=\prod_{\gamma\in\mathcal{C}}(X+Y-\gamma). \tag{6.25}$$

Kładąc $k=|\mathcal{A}|-1$, $l=|\mathcal{B}|-1$ widzimy, że współczynnik przy jednomianie X^kY^l w wielomianie $F(X,\,Y)$ jest równy $\binom{k+l}{k}$, co jest różne od zera w $\mathbb{F}_p$, bo $k+l<p$, a p jest liczbą pierwszą. Combinatorial Nullstellensatz, po wyborze $n=2$, $A_1=\mathcal{A}$, $A_2=\mathcal{B}$, pozwala znaleźć takie $\alpha_0\in\mathcal{A}$, $\beta_0\in\mathcal{B}$, że $F(\alpha_0,\,\beta_0)\neq0$. Ale czynnik $X+Y-(\alpha_0+\beta_0)$ występuje po prawej stronie w (6.25), bo $\alpha_0+\beta_0\in\mathcal{A}+\mathcal{B}\subseteq\mathcal{C}$. Sprzeczność. □

Ćwiczenie 6.41 Udowodnić, że jeżeli p jest liczbą pierwszą, $\mathcal{A}$ jest niepustym podzbiorem ciała $\mathbb{F}_p$, to $|\{x+y:\ x,\,y\in\mathcal{A},\,x\neq y\}|\geqslant\min(p,\,2|\mathcal{A}|-3)$.

Ćwiczenie 6.42 Udowodnić, że jeżeli p jest liczbą pierwszą, $\mathcal{A}$, $\mathcal{B}$ są niepustymi podzbiorami ciała $\mathbb{F}_p$, to $|\{x+y:\ x\in\mathcal{A},\,y\in\mathcal{B},\,xy\neq1\}|\geqslant\min(p,\,|\mathcal{A}|+|\mathcal{B}|-3)$.

6.4.3 Twierdzenia Chevalley'*a* i Warninga

Wykorzystamy CN w dowodzie twierdzenia Chevalley'*a*. Następnie, naśladując Warninga, wzmocnimy to twierdzenie. Te twierdzenia mówią o istnieniu rozwiązań układów równań wielomianowych nad ciałami skończonymi[8] $\mathbb{F}_p$.

Zaczniemy od ważnej o b s e r w a c j i: *Jeżeli $\mathbb{K}$ jest ciałem skończonym i $\varphi:\mathbb{K}\longrightarrow\mathbb{K}$ jest d o w o l n ą funkcją, to istnieje taki wielomian $f(X)\in\mathbb{K}[X]$, że wyznaczona przez niego funkcja wielomianowa jest równa φ.* Dowód jest natychmiastowy, wystarczy powołać się na twierdzenie interpolacyjne Lagrange'*a*. W przypadku, gdy $\mathbb{K}=\mathbb{F}_p$, posługując się MTF, możemy to uzasadnić (w istocie: pozornie) prościej. Rozwiążemy ogólniejsze:

[8] W rozdziale dziewiątym poznamy jeszcze jedną serię ciał skończonych, mianowicie $\mathbb{F}_{p^2}$ dla wszystkich liczb pierwszych p. Można wykazać, że dla każdej liczby pierwszej p i dowolnego wykładnika $n\in\mathbb{N}$ istnieje (jedno z dokładnością do izomorfizmu) ciało mające p^n elementów. I więcej ciał skończonych nie ma.

ZADANIE 6.9 Udowodnić, że jeżeli $\Phi : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p$ jest d o w o l n ą funkcją, to istnieje taki wielomian $F(X_1, \ldots, X_n) \in \mathbb{F}_p[X_1, \ldots, X_n]$, że $F(\boldsymbol{\alpha}) = \Phi(\boldsymbol{\alpha})$ dla każdego $\boldsymbol{\alpha} \in \mathbb{F}_p$.

R o z w i ą z a n i e. Ustalmy dowolny wektor $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Funkcja wielomianowa wyznaczona przez wielomian

$$D_{\boldsymbol{\alpha}}(X_1, X_2, \ldots, X_n) = 1 - (X_1 - \alpha_1)^{p-1}(X_2 - \alpha_2)^{p-1} \cdot \ldots \cdot (X_n - \alpha_n)^{p-1}$$

jest, na mocy MTF, **funkcją charakterystyczną** zbioru jednoelementowego $\{\boldsymbol{\alpha}\}$. To znaczy:

$$D_{\boldsymbol{\alpha}}(\boldsymbol{\beta}) = \begin{cases} 1, & \text{gdy } \boldsymbol{\beta} = \boldsymbol{\alpha}, \\ 0, & \text{gdy } \boldsymbol{\beta} \neq \boldsymbol{\alpha}. \end{cases} \tag{6.26}$$

Stąd: wielomian $\sum_{\boldsymbol{\alpha} \in \mathbb{F}_p^n} \Phi(\boldsymbol{\alpha}) D_{\boldsymbol{\alpha}}(X_1, \ldots, X_n)$ wyznacza funkcję (wielomianową) równą Φ. $\Diamond$

Rozważmy teraz układ równań wielomianowych postaci

$$(\mathscr{U}) \quad \begin{cases} G_1(x_1, x_2, \ldots, x_n) = 0, \\ G_2(x_1, x_2, \ldots, x_n) = 0, \\ \qquad \ldots \\ G_r(x_1, x_2, \ldots, x_n) = 0, \end{cases} \tag{6.27}$$

gdzie $G_i(X_1, \ldots, X_n) \in \mathbb{F}_p[X_1, \ldots, X_n]$, dla $i = 1, \ldots, r$, są danymi wielomianami o współczynnikach w $\mathbb{F}_p$. Przez $\mathcal{N}(G_1, \ldots, G_r; \mathbb{F}_p)$ oznaczamy zbiór rozwiązań takiego układu. Jest to zbiór takich wektorów $\boldsymbol{\alpha} \in \mathbb{F}_p^n$, że $G_i(\boldsymbol{\alpha}) = 0$ dla każdego i. Innymi słowy

$$\mathcal{N}(G_1, \ldots, G_r; \mathbb{F}_p) = \mathcal{N}(G_1; \mathbb{F}_p) \cap \mathcal{N}(G_2; \mathbb{F}_p) \cap \cdots \cap \mathcal{N}(G_r; \mathbb{F}_p).$$

Ćwiczenie 6.43 Udowodnić, że wielomian

$$D_{\mathscr{U}} := (1 - G_1^{p-1})(1 - G_2^{p-1}) \cdot \ldots \cdot (1 - G_r^{p-1}) \tag{6.28}$$

wyznacza funkcję (wielomianową) charakterystyczną podzbioru $\mathcal{N}(G_1, \ldots, G_r; \mathbb{F}_p)$. To znaczy funkcję przyjmującą wartość $1 \in \mathbb{F}_p$ dla argumentów należących do $\mathcal{N}(G_1, \ldots, G_r; \mathbb{F}_p)$ i wartość $0 \in \mathbb{F}_p$ dla pozostałych argumentów.

Łatwo teraz, korzystając z CN, udowodnić

TWIERDZENIE 6.11 (***Twierdzenie Chevalley'a* – 1935**) *Jeżeli wielomiany G_i z układu* (6.27) *spełniają warunek*

$$\deg(G_1) + \deg(G_2) + \cdots + \deg(G_r) < n \tag{6.29}$$

i układ ten ma rozwiązanie, to ma co najmniej d w a rozwiązania.

D O W Ó D. Załóżmy, nie wprost, że $\mathcal{N}(G_1, \ldots, G_r; \mathbb{F}_p) = \{\boldsymbol{\alpha}\}$. Wówczas, na mocy (6.26) i C6.43, wielomian $F = D_{\mathscr{U}} - D_{\boldsymbol{\alpha}}$ wyznacza funkcję wielomianową tożsamościowo równą 0. Jednocześnie $\deg D_{\mathscr{U}} = (p-1)\deg G_1 + \cdots + (p-1)\deg G_r < (p-1)n$ na mocy C3.70(1) i założenia (6.29), a $\deg D_{\boldsymbol{a}} = (p-1)n$ na mocy C3.70(1). Wobec tego $\deg F = (p-1)n$, zob.

C3.70(2). Ponadto, łatwo wskazać niezerowy jednomian maksymalnego stopnia w wielomianie F. Jest to oczywiście $X_1^{p-1} \cdot \ldots \cdot X_n^{p-1}$. Jeżeli więc położymy $A_1 = \cdots = A_n = \mathbb{F}_p$, to, na mocy CN, powinniśmy znaleźć $\boldsymbol{\beta} \in \mathbb{F}_p^n$, dla którego $F(\boldsymbol{\beta}) \neq 0$. Sprzeczność. □

P r z y k ł a d. Dla dowolnej liczby $p \in \mathbb{P}$ istnieją takie liczby całkowite x, y, z, że $x^2+y^2+z^2$ jest niezerową wielokrotnością p. Rzeczywiście, wielomian $G(X, Y, Z) = X^2 + Y^2 + Z^2$ jest wielomianem stopnia 2 trzech zmiennych. Ponieważ $2 < 3$, a $(0, 0, 0)$ jest rozwiązaniem układu $G(x, y, z) = 0$, więc, wobec T6.11, istnieje jeszcze co najmniej jedno rozwiązanie. Porównaj też lemat L8.4, gdzie pokazujemy proste (opierające się na Zasadzie Łat na Kapocie) rozumowanie dowodzące prawdziwości powiedzianego. Trudno byłoby wymyślić podobnie proste rozumowanie w odniesieniu do wielomianu $x^2+5xy+y^2-3yz+2x+11z = 0$ (i podobnych wielomianów stopnia 2 trzech zmiennych i bez wyrazu wolnego – wtedy bowiem istnieje rozwiązanie zerowe!). Obecnie wiemy, że kongruencja $x^2+5xy+y^2-3yz+2x+11z \equiv 0 \,(\mathrm{mod}\, p)$ ma niezerowe rozwiązania. ♢

Dążymy teraz do udowodnienia uzyskanego przez Warninga wzmocnienia twierdzenia Chevalley'*a*. Udowodnimy w tym celu lemat o sumie (wszystkich) wartości wielomianu nad ciałem $\mathbb{F}_p$. Ponieważ przestrzeń $\mathbb{F}_p^n$ jest zbiorem skończonym, więc możemy d o d a ć wszystkie wartości dowolnego wielomianu:

$$\mathcal{S}(F) := \sum_{\boldsymbol{\alpha} \in \mathbb{F}_p^n} F(\boldsymbol{\alpha}).$$

LEMAT 6.3 *Jeżeli w jednomianie* $J = J(X_1, \ldots, X_n) = X_1^{k_1} X_2^{k_2} \cdot \ldots \cdot X_n^{k_n}$ *co najmniej jeden wykładnik* k_i *nie jest podzielny przez* $p-1$, *to* $\mathcal{S}(J) = 0$.

D O W Ó D. Opiera się na tezie Z5.22. Mamy bowiem

$$\mathcal{S}(J) = \sum_{\boldsymbol{\alpha} \in \mathbb{F}_p^n} \alpha_1^{k_1} \cdot \ldots \cdot \alpha_n^{k_n} = (\sum_{\alpha_1 \in \mathbb{F}_p} \alpha_1^{k_1}) \cdot \ldots \cdot (\sum_{\alpha_n \in \mathbb{F}_p} \alpha_n^{k_n}),$$

i co najmniej jeden z n czynników z prawej strony jest równy 0 w $\mathbb{F}_p$. □

Mając ten lemat łatwo dostajemy rzeczone wzmocnienie:

TWIERDZENIE 6.12 (***Twierdzenie Chevalley'a-Warninga*** **– 1935**) *Przy założeniach twierdzenia* T6.11 *zachodzi kongruencja*

$$\boxed{\boxed{\mathrm{card}\, \mathcal{N}(G_1, \ldots, G_r; \mathbb{F}_p) \equiv 0 \,(\mathrm{mod}\, p).}} \tag{6.30}$$

D O W Ó D. Z ćwiczenia C6.43 wiemy, że suma $\mathcal{S}(D_{\mathscr{U}})$ jest sumą tylu jedynek (w $\mathbb{F}_p$) ile elementów ma zbiór $\mathcal{N}(G_1, \ldots, G_r; \mathbb{F}_p)$. Kongruencja (6.30) jest więc równoważna równości $\mathcal{S}(D_{\mathscr{U}}) = 0$ w $\mathbb{F}_p$. W dowodzie T6.11 przekonaliśmy się, że $\deg D_{\mathscr{U}} < (p-1)n$, co oznacza, że w każdym jednomianie $\gamma X_1^{k_1} \cdot \ldots \cdot X_n^{k_k}$ występującym w wielomianie $D_{\mathscr{U}}$ co najmniej jeden wykładnik k_i jest $< p-1$. Więc, na mocy L6.3, $\mathcal{S}(D_{\mathscr{U}}) = 0$. □

Ponieważ liczba całkowita d o d a t n i a i podzielna przez p jest większa od 1, więc jest jasne, że Warning rzeczywiście otrzymał wzmocnienie twierdzenia Chevalley'*a*.

6.5 Wielomiany i liczby Bernoulli'*ego*

Ten paragraf poświęcamy na opowiedzenie o pewnych, ważnych w matematyce, wielomianach.

6.5.1 Sumowanie potęg

Liczby i wielomiany Bernoulli'*ego* pojawiają się przy próbach wyrażania sum

$$S_k(N) := 1^k + 2^k + \ldots + N^k \tag{6.31}$$

k-tych potęg kolejnych liczb naturalnych (od 1 do N) jako wartości pewnych wielomianów.

Z 1.1.2 P wiemy, że $S_1(N) = \frac{1}{2}N^2 + \frac{1}{2}N$, a z C1.2.1, że $S_2(N) = \frac{1}{3}N^3 + \frac{1}{2}N^2 + \frac{1}{6}N$. Pokażemy prostą rekurencyjną (wymyśloną przez Jacoba Bernoulli'*ego*) procedurę wyrażania $S_k(N)$ za pomocą $S_1(N)$, $S_2(N)$, $\ldots$, $S_{k-1}(N)$. Wzór dwumienny (1.7) daje równość:

$$(n+1)^{k+1} = \binom{k+1}{0} n^{k+1} + \binom{k+1}{1} n^k + \ldots + \binom{k+1}{k} n + \binom{k+1}{k+1}.$$

Przesumujmy to w zakresie od $n = 1$ do $n = N$. Dostajemy

$$\sum_{n=1}^{N} (n+1)^{k+1} = \sum_{n=1}^{N} n^{k+1} + \binom{k+1}{1} \sum_{n=1}^{N} n^k + \ldots + \binom{k+1}{k} \sum_{n=1}^{N} n + \sum_{n=1}^{N} 1.$$

Różnica sumy z lewej strony i pierwszej sumy ze strony prawej jest równa $(N+1)^{k+1} - 1$. Stąd

$$(N+1)^{k+1} - 1 = \sum_{j=0}^{k} \binom{k+1}{j} S_j(N),$$

co, po prostym przekształceniu, daje równość rekurencyjną:

$$S_k(N) = \frac{1}{k+1} \left((N+1)^{k+1} - 1 - \sum_{j=0}^{k-1} \binom{k+1}{j} S_j(N) \right). \tag{6.32}$$

Ćwiczenie 6.44 Dowieść, że dla każdego $k \in \mathbb{Z}_{\geqslant 0}$ istnieje (jednoznacznie wyznaczony) wielomian $S_k(X) \in \mathbb{Q}[X]$, którego wartością dla dowolnej liczby naturalnej N jest suma (6.28). Dowieść, że $\deg S_k(X) = k+1$, a jego współczynnik wiodący jest równy $\frac{1}{k+1}$.

6.5.2 Wielomiany i liczby Bernoulli'*ego*

Wyprowadzoną przez Bernoulli'*ego* równość (6.29) wygodnie jest zapisać w nieco innej postaci.

Definicja 6.10 **k-wielomianem Bernoulli'*ego*** nazywamy wielomian

$$B_k(X) := S'_k(X-1).$$

Ćwiczenie 6.45 Udowodnić, że wielomiany Bernoulli'*ego* spełniają poniższe warunki:

(1) $B_k(X+1) - B_k(X) = kX^{k-1}$,

(2) $B_k'(X) = kB_{k-1}(X)$,

(3) $B_k(1-X) = (-1)^k B_k(X)$.

Ćwiczenie 6.46 Udowodnić, że $B_k(X)$ jest jedynym takim wielomianem $\in \mathbb{R}[X]$, że

$$\int_a^{a+1} B_k(x)dx = a^k$$

dla każdej liczby rzeczywistej a.

Ćwiczenie 6.47 Udowodnić, że zachodzi równość wielomianów

$$S_k(X) = \frac{B_k(X+1) - B_k(1)}{k+1}. \tag{6.33}$$

Definicja 6.11 Wartość $B_k(1)$ nazywamy k-tą **liczbą Bernoulli'*ego*** i oznaczamy B_k.

Ćwiczenie 6.48 Udowodnić, że dla każdego $k \in \mathbb{Z}_{\geqslant 0}$ zachodzi równość

$$\sum_{j=0}^{k} \binom{k+1}{j} B_j = k+1. \tag{6.34}$$

Ćwiczenie 6.49 Udowodnić, że funkcja tworząca ciągu wielomianów $\frac{1}{k!}B_k(X)$ jest równa

$$\sum_{k\geqslant 0} \frac{B_k(X)}{k!}\, T^k = \frac{Te^{XT}}{e^T - 1}, \tag{6.35}$$

gdzie $e^Z = \sum_{k\geqslant 0} (k!)^{-1} Z^k$, $0! = 1$.

Rozdział 7

Aproksymacje diofantyczne

J'ai fourni ma carrière; j'ai acquis quelque célébrité
dans les mathématiques. [...];
je n'ai point fait de mal; il faut bien finir.
("ostatnie" słowa Lagrange'*a*)

W tym rozdziale zajmiemy się problemem przybliżania liczb rzeczywistych przez liczby wymierne. Zaczniemy od twierdzenia Dirichlet'*a*, wspomnimy o ciągach Farey'*a* i przejdziemy do głównego tematu tego rozdziału – teorii ułamków łańcuchowych i jej zastosowań do aproksymacji diofantycznych, niewymierności kwadratowych i równania indyjskiego (Pella).

7.1 Twierdzenie Dirichlet'*a*

Jeżeli mamy liczbę rzeczywistą α, to łatwo jest znaleźć liczby wymierne leżące b l i s k o α. Wybieramy dowolny mianownik $k \in \mathbb{N}$ i następnie "skradamy" się do liczby α krokami długości $\frac{1}{k}$. Jasne, że znajdziemy taką (dokładnie jedną) liczbę $h \in \mathbb{Z}$, że $\frac{h}{k} \leqslant \alpha < \frac{h+1}{k}$. Wówczas, oczywiście,

$$\left| \alpha - \frac{h}{k} \right| < \frac{1}{k}.$$

Chcemy jednak osiągnąć więcej. Chodzi o to, by używając niezbyt dużych mianowników "podejść" do danej liczby rzeczywistej znacznie bliżej. To jest możliwe:

P r z y k ł a d 1. Przyjrzyjmy się następującym przybliżeniom liczby π:

$$10^{-3} < \left|\pi - \tfrac{22}{7}\right| < 2 \cdot 10^{-3}, \qquad 10^{-2} < \left|\pi - \tfrac{25}{8}\right| < 2 \cdot 10^{-2}$$

$$2 \cdot 10^{-7} < \left|\pi - \tfrac{355}{113}\right| < 3 \cdot 10^{-7}, \quad 10^{-3} < \left|\pi - \tfrac{358}{114}\right| < 2 \cdot 10^{-3}.$$

Widzimy stąd, że przybliżenie π za pomocą ułamków o mianowniku 7 jest 10 razy lepsze niż za pomocą ułamków o mianowniku 8. Mianownik 113 jest zaś ponadtysiąckrotnie lepszy niż mianownik 114. $\Diamond$

Pierwsze twierdzenie o aproksymacji (= przybliżeniu) pochodzi od Dirichlet'*a*. Przy dowodzie swojego twierdzenia zastosował on tak zwaną **zasadę szufladkową**, zobacz $\mathbb{KOM}$.

TWIERDZENIE 7.1 (***Twierdzenie Dirichlet'a o aproksymacji***) *Dana jest liczba rzeczywista* α *i liczba naturalna* N. *Wtedy istnieje taki mianownik* k, *że* $1 \leqslant k \leqslant N$ *oraz*

$$\left| \alpha - \frac{h}{k} \right| \leqslant \frac{1}{k(N+1)} \tag{7.1}$$

dla odpowiednio dobranego licznika $h \in \mathbb{Z}$.

D O W Ó D. Rozważmy ciąg $(0, \{\alpha\}, \{2\alpha\}, \ldots, \{N\alpha\}, 1)$ długości $N+2$ (przez $\{x\}$ oznaczamy część ułamkową liczby rzeczywistej x, zobacz ustęp 12.1.1) i podzielmy przedział $[\,0;\,1\,]$, do którego należą wszystkie wyrazy tego ciągu, na $N+1$ podzbiorów (*szufladek*)

$$\left[\,\tfrac{0}{N+1};\,\tfrac{1}{N+1}\,\right],\ \left[\,\tfrac{1}{N+1};\,\tfrac{2}{N+1}\,\right],\ \ldots,\ \left[\,\tfrac{N}{N+1};\,\tfrac{N+1}{N+1}\,\right].$$

Ponieważ w naszym ciągu jest $N+2$ wyrazów, a szufladek jest tylko $N+1$, więc w co najmniej jednej szufladce znajdą się dwa wyrazy ciągu. To oznacza, że istnieje takie $1 \leqslant s \leqslant N$, że

$$|1 - \{s\alpha\}| \leqslant \frac{1}{N+1},$$

(tzn. 1 i $\{s\alpha\}$ leżą w tej samej szufladce), l u b istnieje takie $1 \leqslant t \leqslant N$, że

$$|\{t\alpha\} - 0| \leqslant \frac{1}{N+1},$$

(tzn. $\{t\alpha\}$ i 0 leżą w tej samej szufladce), l u b istnieją takie $1 \leqslant t < s \leqslant N$, że

$$|\{s\alpha\} - \{t\alpha\}| \leqslant \frac{1}{N+1}.$$

W pierwszym przypadku kładziemy $h = \lfloor s\alpha \rfloor + 1$, $k = s$, w drugim kładziemy $h = \lfloor t\alpha \rfloor$, $k = t$, a w trzecim kładziemy $h = \lfloor s\alpha \rfloor - \lfloor t\alpha \rfloor$, $k = s - t$. □

Ćwiczenie 7.1 Udowodnić, że dla danej liczby rzeczywistej α istnieje n i e s k o ń c z e n i e wiele takich par $(h,\, k) \in \mathbb{Z} \times \mathbb{N}$, że

$$\left| \alpha - \frac{h}{k} \right| \leqslant \frac{1}{k^2}. \tag{7.2}$$

7.2 Ciągi Farey'*a*

Za pomocą tych ciągów można udowodnić pewne wzmocnienie tezy ostatniego ćwiczenia.

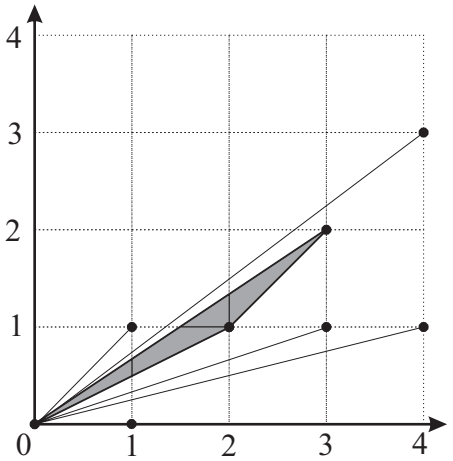
Definicja 7.1 Dla danej liczby naturalnej $n \geqslant 1$, symbolem $\mathcal{F}_n$ oznaczamy ciąg ustawionych w kolejności rosnącej wszystkich ułamków nieskracalnych $\frac{a}{b}$, gdzie $0 \leqslant a \leqslant b \leqslant n$ i $a + b \neq 0$. Na przykład $\mathcal{F}_5$ to ciąg

$$\left(\frac{0}{1},\ \frac{1}{5},\ \frac{1}{4},\ \frac{1}{3},\ \frac{2}{5},\ \frac{1}{2},\ \frac{3}{5},\ \frac{2}{3},\ \frac{3}{4},\ \frac{4}{5},\ \frac{1}{1}\right).$$

Ciąg $\mathcal{F}_n$ nazywamy n-tym **ciągiem Farey'a**.

TWIERDZENIE 7.2 (***Twierdzenie Cauchy'ego-Farey'a***) *Jeżeli* $\frac{a}{b} < \frac{c}{d}$ *są dwoma kolejnymi ułamkami w danym ciągu Farey'a, to* $bc - ad = 1$.

D O W Ó D. Twierdzenie to wyraża prosty fakt geometryczny. Weźmy (w prostokątnym kartezjańskim układzie współrzędnych) punkty $K = (b, a)$, $L = (d, c)$ i $O = (0, 0)$. [Na rysunku 7.1 widzimy przypadek $n = 4$. Zaznaczyliśmy punkty $(t,\, s)$ odpowiadające wszystkim ułamkom s/t ciągu $\mathcal{F}_4$ w tym punkt $K = (2,\, 1)$ i punkt $L = (3,\, 2)$.] Wówczas na brzegu i wewnątrz trójkąta $\triangle KLO$ nie ma żadnych punktów kratowych poza punktami K, L, O (należy to szczegółowo uzasadnić!).



Rys. 7.1

Trójkąt $\triangle KLO$ ma, na mocy ***twierdzenia Picka*** (dowód tego twierdzenia podamy w części $\mathbb{GEO}$ poświęconej geometrii kombinatorycznej), pole równe $\frac{1}{2}$. Z geometrii analitycznej wiemy, że pole tego trójkąta wynosi $\frac{1}{2}|bc - ad|$. Stąd teza. □

TWIERDZENIE 7.3 *Jeżeli* $\frac{a}{b} < \frac{k}{l} < \frac{c}{d}$ *są trzema kolejnymi ułamkami w danym ciągu Farey'a* $\mathcal{F}_n$, *to zachodzi równość*

$$\boxed{\frac{k}{l} = \frac{a+c}{b+d}.}$$

D O W Ó D. Z twierdzenia Cauchy'*ego*-Farey'*a* wiemy, że $bk - al = 1 = cl - dk$. Przeto, $k(b + d) = l(a + c)$, czyli $\frac{k}{l} = \frac{a+c}{b+d}$. □

Jeżeli $\frac{a}{b} < \frac{c}{d}$ są dwoma ułamkami, gdzie $a,\, b,\, c,\, d \in \mathbb{Z}_{\geqslant 0}$, to ułamek

$$\frac{a+c}{b+d}$$

nazywa się **mediantą** tych dwóch ułamków. Możemy więc powiedzieć, że środkowy wyraz w każdej trójce kolejnych wyrazów danego ciągu Farey'*a* jest mediantą dwóch skrajnych.

Zastosujemy teraz naszą wiedzę o ciągach Farey'*a* w dowodzie następującego wzmocnienia tezy ćwiczenia C7.1:

TWIERDZENIE 7.4 (***twierdzenie o aproksymacji diofantycznej***) *Dla danej liczby rzeczywistej* α *istnieje nieskończenie wiele par* $(h,\, k) \in \mathbb{Z} \times \mathbb{N}$, *dla których*

$$\left| \alpha - \frac{h}{k} \right| < \frac{1}{2k^2}. \tag{7.3}$$

D O W Ó D. Załóżmy, że α jest liczbą niewymierną, $\alpha \in (\,0;\, 1\,)$. Przypadek ogólny Czytelnik zechce rozważyć samodzielnie. Pokażemy, że jeżeli α leży między dwoma kolejnymi ułamkami w danym ciągu Fareya $\mathcal{F}_n$, $n \geqslant 2$,

$$\frac{a}{b} < \alpha < \frac{c}{d},$$

to co najmniej jeden z ułamków $\frac{a}{b}$ lub $\frac{c}{d}$ spełnia nierówność (7.3). Istotnie, załóżmy nie wprost, że

$$\alpha - \frac{a}{b} \geqslant \frac{1}{2b^2} \qquad \text{i} \qquad \frac{c}{d} - \alpha \geqslant \frac{1}{2d^2}.$$

Wówczas, po dodaniu stronami i wykorzystaniu T7.2, mamy

$$\frac{1}{2d^2} + \frac{1}{2b^2} \leqslant \left(\frac{c}{d} - \alpha\right) + \left(\alpha - \frac{a}{b}\right) = \frac{bc - ad}{bd} = \frac{1}{bd},$$

co jest równoważne z $b^2 + d^2 \leqslant 2bd$, czyli z $(b-d)^2 \leqslant 0$. To jednakże jest możliwe tylko, gdy $b = d$. Ale dwa kolejne ułamki w danym ciągu Fareya $\mathcal{F}_n$, $n \geqslant 2$, nigdy nie mają równych mianowników (dlaczego?). Sprzeczność. □

U w a g a. Nierówności (7.2) i (7.3) są postaci

$$\left| \alpha - \frac{h}{k} \right| < \frac{1}{\lambda k^2},$$

dla stałej $\lambda = 1$ i $\lambda = 2$. Oczywiście, im większa stała λ tym mniejsze szanse na znalezienie nieskończenie wielu par (h, k) spełniających nierówność. W ustępie 7.3.3 udowodnimy twierdzenie Hurwitza mówiące, że stała $\lambda = \sqrt{5}$ jest jeszcze dobra.

7.3 Ułamki łańcuchowe

Najefektywniejszej metody przybliżania liczb rzeczywistych liczbami wymiernymi dostarcza teoria ułamków łańcuchowych. Przedstawimy tu tylko jeden ze sposobów tworzenia ułamków łańcuchowych i podamy najbardziej elementarne własności tej konstrukcji.

7.3.1 Kanoniczne rozwinięcia. Reguła Eulera

Zaczynamy od tak zwanego **kanonicznego rozwinięcia liczby rzeczywistej na ułamek łańcuchowy** i ustalamy notacje.

Definicja 7.2 Jeżeli $\gamma = \gamma_0$ jest daną liczbą rzeczywistą, to tworzymy ciąg (c_n) liczb całkowitych i ciąg (γ_n) liczb rzeczywistych następująco:

$$c_n = \lfloor \gamma_n \rfloor \tag{7.4}$$

i, jeżeli $\gamma_n \in \mathbb{Z}$, to kończymy procedurę, jeżeli zaś $\gamma_n \notin \mathbb{Z}$, to kładziemy

$$\gamma_{n+1} = \frac{1}{\gamma_n - c_n}. \tag{7.5}$$

Zauważmy, że wszystkie, z wyjątkiem być może γ_0, wyrazy ciągu (γ_n) leżą w przedziale otwartym $(1; \infty)$, a wśród liczb całkowitych c_n jedynie liczba c_0 może być ujemna – pozostałe są ściśle dodatnie. Liczby c_k nazywamy **mianownikami**, a liczby γ_k nazywamy **pseudomianownikami** kanonicznego rozwinięcia liczby γ na ułamek łańcuchowy.

P r z y k ł a d 1. Weźmy liczbę $\gamma = \frac{43}{30}$. Wówczas

$$c_0 = 1, \quad \gamma_1 = \frac{30}{13}, \quad c_1 = 2, \quad \gamma_2 = \frac{13}{4}, \quad c_2 = 3, \quad \gamma_3 = c_3 = 4. \quad \Diamond$$

Łatwo zauważyć ścisły związek między kanonicznym rozwinięciem liczby wymiernej na ułamek łańcuchowy a algorytmem Euklidesa wyznaczania największego wspólnego dzielnika.

Ćwiczenie 7.2 Opisać ten związek.

P r z y k ł a d 2. Weźmy liczbę $\gamma = \sqrt{2}$. Wówczas

$$c_0 = 1, \quad \gamma_1 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1, \quad c_1 = 2, \quad \gamma_2 = \frac{1}{\sqrt{2}+1-2} = \gamma_1.$$

Tym razem otrzymaliśmy nieskończone ciągi

$$(c_i) = (1,\, 2,\, 2,\, 2,\, \dots), \quad (\gamma_i) = (\sqrt{2},\, \sqrt{2}+1,\, \sqrt{2}+1,\, \sqrt{2}+1,\, \dots). \quad \Diamond$$

Przyjrzyjmy się jeszcze innym przykładom: Stosując opisany w D7.2 algorytm, znajdujemy przykładowe

Ciągi mianowników kanonicznych rozwinięć liczb $\sqrt{D}$ na ułamki łańcuchowe

D	Ciąg mianowników rozwinięcia $\sqrt{D}$	A	B	$A^2 - DB^2$
2	$(1,\, \overline{2})$	1	1	-1
3	$(1,\, \overline{1,\, 2})$	2	1	$+1$
5	$(2,\, \overline{4})$	2	1	-1
6	$(2,\, \overline{2,\, 4})$	5	2	$+1$
7	$(2,\, \overline{1,\, 1,\, 1,\, 4})$	8	3	$+1$
8	$(2,\, \overline{1,\, 4})$	3	1	$+1$
10	$(3,\, \overline{6})$	3	1	-1
11	$(3,\, \overline{3,\, 6})$	10	3	$+1$
12	$(3,\, \overline{2,\, 6})$	7	2	$+1$
13	$(3,\, \overline{1,\, 1,\, 1,\, 1,\, 6})$	18	5	-1
14	$(3,\, \overline{1,\, 2,\, 1,\, 6})$	15	4	$+1$
19	$(4,\, \overline{2,\, 1,\, 3,\, 1,\, 2,\, 8})$	170	39	$+1$
21	$(4,\, \overline{1,\, 1,\, 2,\, 1,\, 1,\, 8})$	55	12	$+1$
31	$(5,\, \overline{1,\, 1,\, 3,\, 5,\, 3,\, 1,\, 1,\, 10})$	1520	273	$+1$
43	$(6,\, \overline{1,\, 1,\, 3,\, 1,\, 5,\, 1,\, 3,\, 1,\, 1,\, 12})$	3482	531	$+1$
46	$(6,\, \overline{1,\, 3,\, 1,\, 1,\, 2,\, 6,\, 2,\, 1,\, 1,\, 3,\, 1,\, 12})$	24335	3588	$+1$

Jak widzimy wszystkie otrzymane ciągi mianowników są okresowe (okres zaznaczono kreską) i okres rozpoczyna się od miejsca c_1. Znaczenie trzeciej, czwartej i piątej kolumny zostanie wyjaśnione w 11.4.1 i 11.4.4.

Ćwiczenie 7.3 Rozwinąć na ułamek łańcuchowy liczby $\dfrac{1+\sqrt{5}}{2}$ i $\sqrt{n^2+1}$.

Ćwiczenie 7.4 Udowodnić, że kanoniczne rozwinięcie liczby $\gamma \in \mathbb{R}$ na ułamek łańcuchowy jest skończone wtedy i tylko wtedy, gdy γ jest liczbą wymierną.

Łatwo zobaczyć, że jeżeli istnieją wypisane wyrazy (w kanonicznym rozwinięciu liczby γ), to zachodzi równość

$$\gamma = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{\gamma_3}}}. \tag{7.6}$$

Pisanie ułamków takich jak (7.6) jest kłopotliwe, wprowadzimy więc specjalne skróty:

Definicja 7.3 Niech X, X_0, X_1, X_2, $\ldots$ będą zmiennymi. Określamy indukcyjnie

$$\langle X\rangle = X, \quad \langle X_0, X_1, \ldots, X_n\rangle = X_0 + \frac{1}{\langle X_1, X_2, \ldots, X_n\rangle}.$$

Na przykład mamy

$$\langle c_0, c_1, c_2, \gamma_3\rangle = c_0 + \frac{1}{\langle c_1, c_2, \gamma_3\rangle} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{\langle c_2, \gamma_3\rangle}} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{\gamma_3}}} = \gamma,$$

na mocy (7.6). Ogólnie, dla dowolnego $n \geqslant 0$ zachodzi równość

$$\gamma = \langle c_0, c_1, \ldots, c_{n-1}, \gamma_n\rangle, \tag{7.7}$$

gdzie $c_k = \lfloor \gamma_k \rfloor$ są liczbami określonymi przez (7.4) i (7.5).

U w a g a. W literaturze spotyka się inne sposoby "jednolinijkowego" zapisu ułamków postaci (7.6). Najczęstszym jest taki:

$$c_0 + \frac{1}{c_1 +|}\,\frac{1}{c_2 +|}\,\frac{1}{c_3 +|}\,\frac{1}{\gamma_4}.$$

Z drugiej strony możemy przedstawiać ułamki łańcuchowe w postaci zwykłych ułamków. Na przykład ułamek (7.6) jest, jak łatwo sprawdzić, równy

$$\frac{c_0c_1c_2\gamma_3 + c_2\gamma_3 + c_0\gamma_3 + c_0c_1 + 1}{c_1c_2\gamma_3 + \gamma_3 + c_1}$$

Poeksperymentowawszy nieco z takimi zapisami przekonujemy się, że zachodzą równości

$$\langle X_0, X_1, \ldots, X_n\rangle = \frac{K(X_0, X_1, \ldots, X_n)}{K(X_1, X_2, \ldots, X_n)}, \tag{7.8}$$

gdzie K są wielomianami wypisanych zmiennych. Wielomian $K(Y_1, Y_2, \ldots, Y_s)$ nazwiemy **kontynuantą** zmiennych $Y_1, \ldots, Y_s$. To, że zarówno w liczniku jak i w mianowniku stoi kontynuanta, nie jest niczym dziwnym: wszak mianownik ułamka $\langle X_0, X_1, \ldots, X_n\rangle$ jest, zgodnie z D7.3, r ó w n y licznikowi ułamka $\langle X_1, \ldots, X_n\rangle$.

Jeżeli $(Y_1, Y_2, \ldots, Y_s)$ jest ciągiem (kolejność jest w a ż n a) zmiennych, to iloczyn postaci $Y_{i_1}Y_{i_2}\cdot\ldots\cdot Y_{i_r}$, gdzie $1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant s$, nazwiemy *wyróżnionym*, gdy zbiór $\{1, 2, \ldots, s\} \setminus \{i_1, i_2, \ldots, i_r\}$ da się przedstawić w postaci sumy r o z ł ą c z n e j zbiorów dwuelementowych postaci $\{k, k+1\}$. W szczególności iloczyn "pełny" $Y_1Y_2\cdot\ldots\cdot Y_s$ jest wyróżniony. Również wyróżnionym jest iloczyn pusty, z definicji równy 1, w przypadku, gdy $s \equiv 0 \pmod 2$.

Reguła Eulera *$K(Y_1, Y_2, \ldots, Y_s)$ jest sumą wszystkich iloczynów wyróżnionych.*

Ćwiczenie 7.5 Udowodnić poprawność Reguły Eulera. *Wskazówka.* Korzystając z definicji D7.3 udowodnić tożsamość $K(Y_1, Y_2, \ldots, Y_s) = Y_1K(Y_2, \ldots, Y_s) + K(Y_3, \ldots, Y_s)$.

7.3.2 Nieskończone ułamki łańcuchowe

Oznaczmy przez $\mathscr{C}$ zbiór wszystkich takich ciągów nieskończonych $(c_n)_{n\geqslant 0}$ o wyrazach całkowitych, że $c_n \geqslant 1$ dla wszystkich $n \neq 0$. W poprzednim ustępie zdefiniowaliśmy funkcję $\mathrm{M} : \mathbb{R} \setminus \mathbb{Q} \longrightarrow \mathscr{C}$, która liczbie niewymiernej γ przyporządkowuje ciąg $(c_0, c_1, c_2, \ldots)$ mianowników kanonicznego rozwinięcia liczby γ na ułamek łańcuchowy. Teraz przekonamy się, że funkcja M jest b i j e k c j ą zbioru $\mathbb{R} \setminus \mathbb{Q}$ liczb niewymiernych n a zbiór $\mathscr{C}$.

Definicja 7.4 Niech $(c_0, c_1, c_2, c_3, \ldots)$ będzie dowolnym elementem zbioru $\mathscr{C}$. Liczbę

$$R_n = \langle c_0, c_1, c_2, \ldots, c_n\rangle = \frac{P_n}{Q_n},$$

gdzie $P_n = K(c_0, c_1, \ldots, c_n)$, $Q_n = K(c_1, c_2, \ldots, c_n)$ (porównaj równości (7.8)), nazywamy n-**tym reduktem** (nieskończonego) ułamka łańcuchowego $\langle c_0, c_1, c_2, c_3, \ldots\rangle$.

Wygodnie jest też przyjąć, że $P_{-1} = 1$, $Q_0 = 1$, $Q_{-1} = 0$. Łatwo spostrzec rekurencyjne zależności między wielomianami P_n i Q_n:

Ćwiczenie 7.6 Udowodnić przez indukcję, że dla $n \geqslant 1$ zachodzą tożsamości

$$P_n = c_nP_{n-1} + P_{n-2}, \tag{7.9}$$

$$Q_n = c_nQ_{n-1} + Q_{n-2}, \tag{7.10}$$

$$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n-1}. \tag{7.11}$$

Wskazówka. Tożsamości (7.11) dowodzi się za pomocą oczywistej indukcji korzystając z tożsamości (7.9) i (7.10), których prawdziwość wynika natychmiast z Reguły Eulera.

Ćwiczenie 7.7 Udowodnić, że $Q_{n+1} > Q_n \geqslant n$ dla każdego $n \geqslant 1$.

Twierdzenie 7.5 *Ciąg (R_n) jest (oscylującym) ciągiem zbieżnym.*

D O W Ó D. Korzystając z równości (7.9) i (7.10) możemy zapisać dla dowolnego $n \geqslant 0$

$$R_{n+2} - R_n = \frac{P_{n+2}}{Q_{n+2}} - \frac{P_n}{Q_n} = \frac{c_{n+2}P_{n+1} + P_n}{c_{n+2}Q_{n+1} + Q_n} - \frac{P_n}{Q_n} = \frac{c_{n+2}(P_{n+1}Q_n - Q_{n+1}P_n)}{Q_n(c_{n+2}Q_{n+1} + Q_n)}.$$

To, dzięki równości (7.11), daje:

$$R_{n+2} - R_n = \frac{c_{n+2} \cdot (-1)^n}{Q_n(c_{n+2}Q_{n+1} + Q_n)}. \tag{7.12}$$

Ponieważ liczby c_{n+2} i Q_k są dodatnie, więc równość (7.12) pokazuje, że

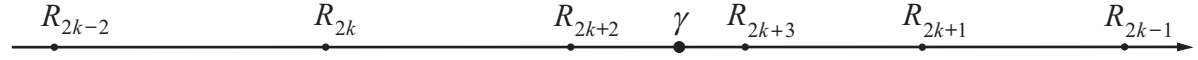
$$R_{2k+3} - R_{2k+1} < 0 \qquad \text{i} \qquad R_{2k+2} - R_{2k} > 0 \tag{7.13}$$

dla dowolnego $k \geqslant 0$. Nierówności (7.13) mówią, że parzystoindeksowy podciąg (R_{2k}) ciągu reduktów jest ciągiem (ściśle) rosnącym, a nieparzystoindeksowy podciąg (R_{2k+1}) jest ciągiem (ściśle) malejącym. Podobnie obliczamy:

$$R_{2k+1} - R_{2k} = \frac{(-1)^{2k}}{Q_{2k}Q_{2k+1}} = \frac{1}{Q_{2k}Q_{2k+1}}. \tag{7.14}$$

Z tej równości widać, że $R_{2k} < R_{2k+1}$ dla wszystkich $k \geqslant 0$. W rzeczywistości k a ż d y wyraz R_{2n} jest mniejszy niż k a ż d y wyraz R_{2m+1}. Aby to uzasadnić połóżmy $k = \max(n, m)$. Wtedy, na mocy już udowodnionego, $R_{2n} \leqslant R_{2k} < R_{2k+1} \leqslant R_{2m+1}$.

Położenie reduktów na osi liczbowej pokazujemy (schematycznie) poniżej:



Rys. 7.2

Ciąg rosnący (R_{2k}) i ograniczony od góry (przez R_1 na przykład) ma granicę. Oznaczmy ją przez γ. Łatwo widzieć, że $\gamma < R_{2k+1}$ dla każdego k. Istotnie, gdyby $\gamma \geqslant R_{2k+1}$, to $\gamma > R_{2k+3}$ i w przedziale (R_{2k+3}, γ) znaleźlibyśmy pewien (naprawdę nieskończenie wiele) wyraz R_{2m}, co jest niemożliwe. Ciąg (R_{2k+1}), jako malejący i ograniczony od dołu przez γ, ma granicę $\gamma' \geqslant \gamma$. Dowód twierdzenia będzie skończony, gdy uzasadnimy, że $\gamma' = \gamma$. Załóżmy więc nie wprost, że $\gamma' - \gamma = \varepsilon > 0$. Wtedy

$$\varepsilon = \gamma' - \gamma \leqslant R_{2k+1} - R_{2k} = \frac{1}{Q_{2k}Q_{2k+1}} \leqslant \frac{1}{2k(2k+1)}$$

dla każdego k, na mocy (7.14) i tezy ćwiczenia C7.7. Jasne, że to jest niemożliwe. □

Granicę γ nazywamy **wartością** nieskończonego ułamka łańcuchowego $\langle c_0, c_1, c_2, \ldots \rangle$ wyznaczonego przez ciąg $(c_n) \in \mathscr{C}$ i piszemy $\gamma = \langle c_0, c_1, c_2, \ldots \rangle$. W ten sposób określiliśmy funkcję $\mathrm{W} : \mathscr{C} \longrightarrow \mathbb{R}$, która ciągowi $(c_n)_{n\geqslant 0}$ przyporządkowuje wartość $\mathrm{W}((c_n)) = \langle c_0, c_1, \ldots \rangle$ nieskończonego ułamka łańcuchowego.

Spróbujmy teraz kanonicznie rozwinąć otrzymaną liczbę $\gamma = \langle c_0, c_1, \dots \rangle$ na ułamek łańcuchowy, czyli wyznaczyć ciąg $\mathrm{M}(\gamma)$. Z dowodu T7.5 wiemy, że $c_0 = R_0 < \gamma < R_1 = c_0 + \frac{1}{c_1}$. To dowodzi, że $\lfloor \gamma \rfloor = c_0$ (bowiem z założenia $c_1 \geqslant 1$). Zatem c_0 jest zerowym mianownikiem kanonicznego rozwinięcia liczby γ na ułamek łańcuchowy. Ogólniej, jeżeli przez γ_n oznaczymy wartość $\langle c_n, c_{n+1}, c_{n+2}, \dots \rangle$, to $c_n < \gamma_n < c_n + \frac{1}{c_{n+1}}$ co dowodzi, że $c_n = \lfloor \gamma_n \rfloor$ dla każdego n. Udowodniliśmy w ten sposób, że jeżeli $\gamma = \langle c_0, c_1, c_2, \dots \rangle$ jest wartością nieskończonego ułamka łańcuchowego wyznaczonego przez ciąg $(c_n) \in \mathscr{C}$, to n-tym mianownikiem kanonicznego rozwinięcia liczby γ na ułamek łańcuchowy jest liczba c_n (a n-tym pseudomianownikiem jest wartość $\gamma_n = \langle c_n, c_{n+1}, \dots \rangle$). To oznacza, że $\mathrm{M} \circ \mathrm{W} = \mathrm{Id}_{\mathscr{C}}$. Mamy więc udowodnioną pierwszą połowę ważnego twierdzenia:

TWIERDZENIE 7.6 *Funkcja* $\mathrm{M} : \mathbb{R} \setminus \mathbb{Q} \longrightarrow \mathscr{C}$ *jest bijekcją.*

D O W Ó D. Pozostało nam uzasadnić, że $\mathrm{W} \circ \mathrm{M} = \mathrm{Id}_{\mathbb{R}\setminus\mathbb{Q}}$, czyli że jeżeli γ jest dowolną liczbą rzeczywistą niewymierną, a $c_0, c_1, c_2, \dots$ są mianownikami jej kanonicznego rozwinięcia na ułamek łańcuchowy, to $\lim_{n\to\infty} \langle c_0, c_1, \dots, c_n \rangle = \gamma$. Otóż, ponieważ

$$\gamma = \langle c_0, c_1, \dots, c_{n-1}, \gamma_n \rangle = \frac{\gamma_n P_{n-1} + P_{n-2}}{\gamma_n Q_{n-1} + Q_{n-2}} \tag{7.15}$$

(patrz (7.7), (7.8), (7.9) i (7.10)), więc widzimy, że odległość $|\gamma - \langle c_0, c_1, \dots, c_n \rangle|$ jest równa

$$\left| \frac{\gamma_n P_{n-1} + P_{n-2}}{\gamma_n Q_{n-1} + Q_{n-2}} - \frac{c_n P_{n-1} + P_{n-2}}{c_n Q_{n-1} + Q_{n-2}} \right| = \left| \frac{(\gamma_n - c_n) \cdot (-1)^{n-2}}{(\gamma_n Q_{n-1} + Q_{n-2})(c_n Q_{n-1} + Q_{n-2})} \right|.$$

Odległość ta jest zatem dowolnie mała dla wszystkich dostatecznie dużych n (bo $c_n = \lfloor \gamma_n \rfloor$, więc $|\gamma_n - c_n| < 1$, a $\gamma_n Q_{n-1} + Q_{n-2} > c_n Q_{n-1} + Q_{n-2} \geqslant 2n - 3$, zobacz C7.7). □

WNIOSEK *Dla dowolnego ciągu* $(c_n) \in \mathscr{C}$ *wartość* $\langle c_0, c_1, c_2, \dots \rangle$ *nieskończonego ułamka łańcuchowego jest liczbą niewymierną.* □

Opisana przez twierdzenie T7.6 wzajemnie jednoznaczna odpowiedniość

$$\mathrm{M} : \mathbb{R} \setminus \mathbb{Q} \ni \gamma \longleftrightarrow (c_0, c_1, c_2, \dots) \in \mathscr{C} : \mathrm{W}$$

między liczbami niewymiernymi a nieskończonymi ciągami mianowników ich kanonicznych rozwinięć na ułamki łańcuchowe pozwala w dalszym ciągu mówić sensownie o reduktach liczb niewymiernych. n-ty redukt $\langle c_0, c_1, \dots, c_n \rangle$ liczby niewymiernej γ oznaczamy $R_n(\gamma)$.

Ćwiczenie 7.8 Udowodnić, że kolejne redukty $R_n = R_n(\gamma)$ są coraz lepszymi przybliżeniami liczby niewymiernej γ, to znaczy:

$$|\gamma - R_0| > |\gamma - R_1| > |\gamma - R_2| > \dots > |\gamma - R_n| > \dots .$$

Ćwiczenie 7.9 Udowodnić tak zwane ***prawo najlepszego przybliżenia***: *Jeżeli dana liczba wymierna* $\frac{h}{k}$, *gdzie* $h \in \mathbb{Z}$, $k \in \mathbb{N}$, *lepiej przybliża daną liczbę niewymierną* γ *niż* n*-ty redukt* $R_n(\gamma)$, *gdzie* $n \geqslant 1$, *to mianownik* k *jest większy niż mianownik* Q_n *reduktu* $R_n = R_n(\gamma)$:

$$\left| \gamma - \frac{h}{k} \right| < \left| \gamma - \frac{P_n}{Q_n} \right| \quad \Longrightarrow \quad k > Q_n.$$

P r z y k ł a d. Dzięki rozwinięciom pokazanym w tabelce z ustępu 7.3.1 wyznaczamy kolejne redukty $R_n(\sqrt{2})$: $R_0 = \langle 1\rangle = 1$, $R_1 = \langle 1,\, 2\rangle = 3/2$, $R_2 = \langle 1,\, 2,\, 2\rangle = 7/5$, $R_3 = \langle 1,\, 2,\, 2,\, 2\rangle = 17/12$, $R_4 = \langle 1,\, 2,\, 2,\, 2,\, 2\rangle = 41/29$, $R_5 = \langle 1,\, 2,\, 2,\, 2,\, 2,\, 2\rangle = 99/70$. Przyjrzyjmy się jak dobrze przybliżają one $\sqrt{2}$:

$$|\sqrt{2} - R_0| \approx 0,414216, \quad |\sqrt{2} - R_1| \approx 0,085786, \quad |\sqrt{2} - R_2| \approx 0,014214,$$
$$|\sqrt{2} - R_3| \approx 0,002453, \quad |\sqrt{2} - R_4| \approx 0,000420, \quad |\sqrt{2} - R_5| \approx 0,000072.$$

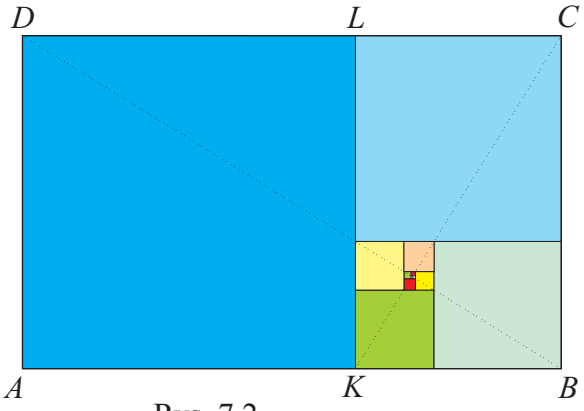
Przybliżenia podajemy w zapisie dziesiętnym, by łatwiej widzieć ich "dobroć". $\Diamond$

7.3.3 Złota liczba. Twierdzenie Hurwitza

Poznamy teraz jedną liczbę niewymierną w pewnym sensie najgorzej przybliżalną liczbami wymiernymi. Następnie udowodnimy metodą Borela zapowiedziane w paragrafie 7.2 twierdzenie Hurwitza.

Definicja 7.5 Liczbę $\tau = \dfrac{1+\sqrt{5}}{2}$ nazywamy **liczbą złotą**.

U w a g a. Czytelnik, który rozwiązał C7.3, być może postawił hipotezę, skąd się bierze taka nazwa. I być może wymyślił, że τ jest "najprostszą" liczbą niewymierną w przyrodzie matematycznej. (Liczby równoważne liczbie złotej również czasami nazywamy **liczbami złotymi**.) Tymczasem to już starożytni Grecy natrafili na tę liczbę poszukując "najbardziej prostokątnego" prostokąta czyli takiego, który nie jest "za długi" ani "za kwadratowy". Uznano, że jest tylko jeden (z d o k ł a d n o ś c i ą d o p o d o b i e ń s t w a) taki prostokąt: mianowicie prostokąt $ABCD$, który jest sumą kwadratu $AKLD$ i prostokąta $LKBC \sim ABCD$, zobacz rysunek 7.2.



Rys. 7.2

Ćwiczenie 7.10 Co to ma wspólnego z równością $\tau = \langle 1,\, 1,\, 1,\, \ldots\rangle$?

Ćwiczenie 7.11 Uzasadnić, że n-ty redukt liczby złotej jest równy f_{n+2}/f_{n+1}, gdzie f_n oznacza n-tą liczbę Fibonacci'*ego*, zobacz rozdział 9.

W trakcie dowodu poniższego twierdzenia Hurwitza możemy zauważyć ważną rolę jaką gra liczba złota (istotny jest fakt, że prawie wszystkie mianowniki liczby złotej są najmniejsze możliwe).

TWIERDZENIE 7.7 (***Hurwitz*** **– 1891**) *Dla danej liczby rzeczywistej γ istnieje nieskończenie wiele takich par $(h,\, k) \in \mathbb{Z} \times \mathbb{N}$, że*

$$\left|\gamma - \frac{h}{k}\right| < \frac{1}{\sqrt{5}k^2}. \tag{7.16}$$

D O W Ó D. Udowodnimy, że jeżeli P_n/Q_n, P_{n+1}/Q_{n+1}, P_{n+2}/Q_{n+2} są kolejnymi reduktami liczby niewymiernej γ, to co najmniej jedna z par $(h,\,k) = (P_n,\,Q_n)$, $(P_{n+1},\,Q_{n+1})$, $(P_{n+2},\,Q_{n+2})$ spełnia nierówność (7.16). Rozpoczniemy od następującej obserwacji:

O b s e r w a c j a. Załóżmy, że $a/b < c/d$ są takimi liczbami wymiernymi, że $b,\,d > 0$ i $bc - ad = 1$. Wówczas, jeżeli $c/d - a/b \geqslant 1/\sqrt{5}b^2 + 1/\sqrt{5}d^2$, to $1/\tau < b/d < \tau$.

D o w ó d o b s e r w a c j i. Założona nierówność jest równoważna $\sqrt{5}b/d \geqslant 1 + b^2/d^2$ (widać to po obustronnym pomnożeniu przez $\sqrt{5}b^2$). To oznacza, że wartość wielomianu $f(X) = X^2 - \sqrt{5}X + 1$ dla argumentu $x = \frac{b}{d}$ jest liczbą niedodatnią. Ponieważ pierwiastkami tego wielomianu są liczby τ i $\frac{1}{\tau}$, więc widzimy, że $\frac{1}{\tau} \leqslant \frac{b}{d} \leqslant \tau$. Nierówności są w istocie ścisłe, bo τ jest liczbą niewymierną. Q.e.d.

Przechodzimy do dowodu twierdzenia. Załóżmy, nie wprost, że nierówność (7.16) nie zachodzi dla żadnej z trzech wymienionych par $(h,\,k)$. To znaczy, że zachodzą nierówności

$$\left|\gamma - \frac{P_n}{Q_n}\right| \geqslant \frac{1}{\sqrt{5}Q_n^2}, \qquad \left|\gamma - \frac{P_{n+1}}{Q_{n+1}}\right| \geqslant \frac{1}{\sqrt{5}Q_{n+1}^2}, \qquad \left|\gamma - \frac{P_{n+2}}{Q_{n+2}}\right| \geqslant \frac{1}{\sqrt{5}Q_{n+2}^2}. \tag{7.17}$$

Z dowodu T7.5 wiemy, że kolejne redukty liczby niewymiernej leżą z różnych stron tej liczby. Wobec tego

$$\text{(P)}\quad \frac{P_n}{Q_n} < \frac{P_{n+2}}{Q_{n+2}} < \gamma < \frac{P_{n+1}}{Q_{n+1}} \qquad \text{lub} \qquad \text{(N)}\quad \frac{P_{n+1}}{Q_{n+1}} < \gamma < \frac{P_{n+2}}{Q_{n+2}} < \frac{P_n}{Q_n}$$

w zależności od tego, czy n jest liczbą parzystą czy nieparzystą.

Nierówności (7.17) dają więc w przypadku (P):

$$\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} = \left|\frac{P_{n+1}}{Q_{n+1}} - \gamma\right| + \left|\gamma - \frac{P_n}{Q_n}\right| \geqslant \frac{1}{\sqrt{5}Q_{n+1}^2} + \frac{1}{\sqrt{5}Q_n^2},$$

$$\frac{P_{n+1}}{Q_{n+1}} - \frac{P_{n+2}}{Q_{n+2}} = \left|\frac{P_{n+1}}{Q_{n+1}} - \gamma\right| + \left|\gamma - \frac{P_{n+2}}{Q_{n+2}}\right| \geqslant \frac{1}{\sqrt{5}Q_{n+1}^2} + \frac{1}{\sqrt{5}Q_{n+2}^2}.$$

Dzięki *o b s e r w a c j i* (zobacz też (7.11)) mamy stąd

$$\frac{1}{\tau} < \frac{Q_{n+1}}{Q_n} < \tau, \quad \frac{1}{\tau} < \frac{Q_{n+1}}{Q_{n+2}} < \tau. \tag{7.18}$$

[Analogicznie dowodzimy nierówności (7.18) w przypadku nieparzystym (N).] Nierówności (7.18) pozwalają napisać (pamiętamy o równości (7.10) i nierówności $c_{n+2} \geqslant 1$)

$$\tau > \frac{Q_{n+2}}{Q_{n+1}} = \frac{c_{n+2}Q_{n+1} + Q_n}{Q_{n+1}} = c_{n+2} + \frac{Q_n}{Q_{n+1}} > 1 + \frac{1}{\tau},$$

co jest niemożliwe, bo $\tau = 1 + 1/\tau$. □

Ćwiczenie 7.12 Udowodnić, że istnieje nieskończenie wiele takich par $(h,\,k) \in \mathbb{Z} \times \mathbb{N}$, że $|\sqrt{2} - h/k| < 1/\sqrt{8}k^2$.

Ćwiczenie 7.13 Udowodnić, że jeżeli τ jest liczbą złotą, $\lambda > \sqrt{5}$, to istnieje tylko s k o ń c z e n i e w i e l e takich par $(h,\,k) \in \mathbb{Z} \times \mathbb{N}$, że $|\tau - h/k| < 1/\lambda k^2$.

7.3.4 Grupa $\mathbf{GL}_2(\mathbb{Z})$

W tym ustępie poznamy pierwszą ważną w teorii liczb grupę n i e p r z e m i e n n ą. Przed dalszym czytaniem należy zapoznać się z ustępami 9.4.1 i 9.4.2, gdzie poznajemy macierze 2×2 i ich wyznaczniki. Iloczyn macierzy $\mathbf{A}$, $\mathbf{B}$ oznaczamy $\mathbf{A}\cdot\mathbf{B}$ lub $\mathbf{AB}$. **Macierz odwrotną** danej macierzy $\mathbf{A}\in\mathbf{GL}_2(\mathbb{Z})$ oznaczamy symbolem $\mathbf{A}^{-1}$. Wyznaczona jest ona (jednoznacznie!) przez zależność $\mathbf{AA}^{-1}=\mathbf{A}^{-1}\mathbf{A}=\mathbf{E}$, gdzie $\mathbf{E}=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ jest **macierzą jednostkową**.

Zbiór wszystkich macierzy $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ o wyrazach całkowitych i wyznaczniku $ad-bc=\pm 1$ oznaczamy symbolem $\mathbf{GL}_2(\mathbb{Z})$.

P r z y k ł a d. Jeżeli P_n/Q_n, P_{n+1}/Q_{n+1} są dwoma kolejnymi reduktami danej liczby niewymiernej γ, to macierz

$$\begin{pmatrix} P_n & P_{n+1}\\ Q_n & Q_{n+1}\end{pmatrix} \tag{7.19}$$

należy do $\mathbf{GL}_2(\mathbb{Z})$, zobacz (7.11). Jeżeli $\frac{a}{b}<\frac{c}{d}$ są dwoma kolejnymi wyrazami ciągu Farey'a $\mathcal{F}_n$, to $\left(\begin{smallmatrix}a&c\\b&d\end{smallmatrix}\right)\in\mathbf{GL}_2(\mathbb{Z})$, zobacz T7.2. $\Diamond$

Ćwiczenie 7.14 Udowodnić, że $(\mathbf{GL}_2(\mathbb{Z}),\cdot)$, gdzie $\cdot$ jest mnożeniem macierzy, jest grupą. Zobacz D1.5. *Wskazówka.* Elementem neutralnym jest macierz jednostkowa $\mathbf{E}$. Sprawdzić, że $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)^{-1}=\left(\begin{smallmatrix}wd&-wb\\-wc&wa\end{smallmatrix}\right)$, gdzie $w=ad-bc$.

Ćwiczenie 7.15 Udowodnić, że podzbiór $\mathbf{SL}_2(\mathbb{Z})$ zbioru $\mathbf{GL}_2(\mathbb{Z})$ składający się z macierzy o wyznaczniku równym $+1$ jest podgrupą grupy $\mathbf{GL}_2(\mathbb{Z})$, zobacz D5.8.

Wprowadzimy specjalne oznaczenia czterech elementów grupy $\mathbf{GL}_2(\mathbb{Z})$:

$$\mathbf{T}=\begin{pmatrix}1&1\\0&1\end{pmatrix},\quad \mathbf{S}=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\quad \mathbf{J}=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \mathbf{R}=\begin{pmatrix}-1&0\\0&1\end{pmatrix}. \tag{7.20}$$

Macierze $\mathbf{T}$ i $\mathbf{S}$ należą do podgrupy $\mathbf{SL}_2(\mathbb{Z})$. Zaś $\mathbf{J}$, $\mathbf{R}\in\mathbf{GL}_2(\mathbb{Z})\setminus\mathbf{SL}_2(\mathbb{Z})$.

Ćwiczenie 7.16 Udowodnić, że macierz $\mathbf{S}$ jest elementem rzędu 4, a macierze $\mathbf{J}$ i $\mathbf{R}$ są elementami rzędu 2 w grupie $\mathbf{GL}_2(\mathbb{Z})$. Macierz $\mathbf{T}$ jest elementem rzędu nieskończonego.

Twierdzenie 7.8 *Każda macierz, $\mathbf{A}\in\mathbf{GL}_2(\mathbb{Z})$ da się przedstawić w postaci iloczynu potęg (o wykładnikach $\in\mathbb{Z}$) macierzy $\mathbf{T}$, $\mathbf{S}$ i $\mathbf{R}$.*

D O W Ó D. Niech $\mathbf{A}=\begin{pmatrix}a&b\\c&d\end{pmatrix}$. Rozważymy najpierw przypadek, gdy $b=0$. Wówczas $ad=\pm 1$. Zatem $a\in\{+1,-1\}$ i $d\in\{+1,-1\}$. Łatwo sprawdzić, że

$$\begin{pmatrix}1&0\\c&1\end{pmatrix}=\mathbf{JT}^c\mathbf{J},\ \begin{pmatrix}1&0\\c&-1\end{pmatrix}=\mathbf{JT}^c\mathbf{S},\ \begin{pmatrix}-1&0\\c&1\end{pmatrix}=\mathbf{ST}^c\mathbf{J},\ \begin{pmatrix}-1&0\\c&-1\end{pmatrix}=\mathbf{ST}^c\mathbf{S}. \tag{7.21}$$

Ponieważ $\mathbf{J} = \mathbf{RS}$, więc w przypadku $b = 0$ teza jest prawdziwa. Pokażemy teraz metodę zmniejszania "b", gdy $b \neq 0$. W takim przypadku zapiszmy $a = qb + r$, gdzie $0 \leqslant r < |b|$. Równość

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} b & r \\ d & s \end{pmatrix} \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & r \\ d & s \end{pmatrix} \mathbf{T}^q\mathbf{RS},$$

jak łatwo sprawdzić, zachodzi dla $s = c - qd$. Mamy $bs - rd = b(c - qd) - (a - qb)d = bc - ad = \pm 1$, zatem $\left(\begin{smallmatrix} b & r \\ d & s \end{smallmatrix}\right) \in \mathbf{GL}_2(\mathbb{Z})$. Jeżeli $r = 0$, to jedna z równości (7.21) pozwala zakończyć rozumowanie. Jeżeli zaś $r > 0$, to powtarzamy sztukę: jeżeli $b = q_1 r + r_1$ i $s_1 = d - q_1 s$, to

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} b & r \\ d & s \end{pmatrix} \mathbf{T}^q\mathbf{RS} = \begin{pmatrix} r & r_1 \\ s & s_1 \end{pmatrix} \mathbf{T}^{q_1}\mathbf{RST}^q\mathbf{RS}.$$

Postępując tak dalej widzimy, że kolejne linijki algorytmu Euklidesa (2.8) pozwalają zapisać równość $\mathbf{A} = \left(\begin{smallmatrix} r_{n-1} & 0 \\ s_{n-1} & s_n \end{smallmatrix}\right)\mathbf{T}^{q_n}\mathbf{RS} \cdot \ldots \cdot \mathbf{T}^{q_1}\mathbf{RST}^q\mathbf{RS}$, gdzie r_{n-1} jest ostatnią niezerową resztą w algorytmie (czyli, jak wiemy $r_{n-1} = \mathrm{NWD}\,(a,\, b) = 1$). To kończy dowód. □

Ćwiczenie 7.17 Przedstawić macierz $\left(\begin{smallmatrix} 11 & 71 \\ 2 & 13 \end{smallmatrix}\right)$ w postaci iloczynu potęg macierzy $\mathbf{T}$, $\mathbf{S}$.

7.3.5 Równoważność liczb

Powiemy parę słów na temat pewnej relacji równoważności w zbiorze liczb rzeczywistych. Relacja ta jest ściśle związana z (kanonicznym) rozwijaniem liczb na ułamki łańcuchowe.

Definicja 7.6 Liczby $\gamma,\, \beta \in \mathbb{R}$ nazywamy **równoważnymi**, co zapisujemy $\gamma \simeq \beta$, gdy istnieją takie liczby całkowite $a,\, b,\, c,\, d$, że $|ad - bc| = 1$ oraz

$$\beta = \frac{a\gamma + b}{c\gamma + d}. \tag{7.22}$$

Równość (7.22) będziemy w dalszym ciągu zapisywać w postaci: $\beta = \mathbf{A}(\gamma)$, gdzie

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z}).$$

Ćwiczenie 7.18 Udowodnić, że jeżeli $\mathbf{A},\, \mathbf{B} \in \mathbf{GL}_2(\mathbb{Z})$, to dla dowolnej liczby $\gamma \in \mathbb{R}$ zachodzą warunki:

$$(1) \quad \mathbf{A}(\mathbf{B}(\gamma)) = (\mathbf{AB})(\gamma), \qquad (2) \quad \beta = \mathbf{A}(\gamma) \Leftrightarrow \gamma = \mathbf{A}^{-1}(\beta) \tag{7.23}$$

Ćwiczenie 7.19 Udowodnić, że relacja $\simeq$ jest relacją równoważności, zobacz $\mathbb{KOM}$.

Ćwiczenie 7.20 Udowodnić, że każde dwie liczby wymierne są równoważne i że każda liczba równoważna liczbie wymiernej jest liczbą wymierną. Innymi słowy, zbiór $\mathbb{Q}$ liczb wymiernych jest klasą równoważności względem relacji $\simeq$.

Ćwiczenie 7.21 Udowodnić, że jeżeli $\gamma = \gamma_0$ jest liczbą rzeczywistą niewymierną i (γ_n) jest opisanym w definicji D7.2 ciągiem pseudomianowników, to dla każdego n zachodzi $\gamma \simeq \gamma_n$ i, ogólniej, $\gamma_n \simeq \gamma_m$ dla dowolnych n, m. *Wskazówka.* Zobacz (7.15) i (7.11).

Ogonem ciągu nieskończonego $(x_n)_{n\geqslant 0}$ nazwiemy podciąg $(x_{s+n})_{n\geqslant 0}$.

Opisana w definicji D7.2 procedura przyporządkowuje liczbie rzeczywistej γ jednoznacznie wyznaczony ciąg mianowników $\mathrm{M}(\gamma) = (c_n)_{n\geqslant 0}$. Wiemy, zobacz C7.4, że ciąg $\mathrm{M}(\gamma)$ jest skończony wtedy i tylko wtedy, gdy $\gamma \in \mathbb{Q}$.

Ćwiczenie 7.22 Udowodnić, że jeżeli γ jest liczbą niewymierną, to pewien ogon ciągu $\mathrm{M}(\gamma+1)$ równy jest pewnemu ogonowi ciągu $\mathrm{M}(\gamma)$.

Ćwiczenie 7.23 Udowodnić, że jeżeli γ jest liczbą niewymierną, to pewien ogon ciągu $\mathrm{M}(1/\gamma)$ równy jest pewnemu ogonowi ciągu $\mathrm{M}(\gamma)$.

Ćwiczenie 7.24 Udowodnić, że jeżeli $\gamma = \langle c_0, c_1, c_2, \dots\rangle$ jest wartością nieskończonego ułamka łańcuchowego, to pewien ogon ciągu $\mathrm{M}(-\gamma)$ równy jest pewnemu ogonowi ciągu $\mathrm{M}(\gamma)$. Dokładniej: $\mathrm{M}(-\gamma) = (-c_0-1, c_2+1, c_3, c_4, \dots)$, gdy $c_1 = 1$, natomiast, gdy $c_1 \geqslant 2$, to $\mathrm{M}(-\gamma) = (-c_0-1, 1, c_1-1, c_2, c_3, \dots)$.

TWIERDZENIE 7.9 *Liczby niewymierne γ i β są równoważne wtedy i tylko wtedy, gdy pewien ogon ciągu $\mathrm{M}(\gamma)$ r ó w n y jest pewnemu ogonowi ciągu $\mathrm{M}(\beta)$.*

D O W Ó D. Jeżeli ciągi $(c_n) = \mathrm{M}(\gamma)$ i $(b_n) = \mathrm{M}(\beta)$ mają równe ogony, to $\gamma_k = \beta_l$ dla pewnych indeksów k, l. Wtedy, na mocy C7.21 i C7.19, $\gamma \simeq \gamma_k = \beta_l \simeq \beta$, więc $\gamma \simeq \beta$. Odwrotnie, gdy $\gamma = \mathbf{A}(\beta)$ dla pewnej macierzy $\mathbf{A} \in \mathbf{GL}_2(\mathbb{Z})$, to korzystając z opisanego w twierdzeniu T7.8 rozkładu macierzy $\mathbf{A}$ i faktu, że $\mathbf{T}(\gamma) = \gamma+1$, $\mathbf{R}(\gamma) = -\gamma$, $\mathbf{RS}(\gamma) = 1/\gamma$, kończymy dowód dzięki C7.22, C7.23 i C7.24. Czytelnik powinien samodzielnie uzupełnić odpowiednie szczegóły rozumowania. □

7.3.6 Niewymierności kwadratowe

Niewymierności kwadratowe są najprostszymi liczbami niewymiernymi, a ich rozwinięcia na ułamki łańcuchowe są szczególnie sympatyczne. Zobaczymy to w kolejnych ustępach.

Definicja 7.7 Liczbę niewymierną $\gamma \in \mathbb{R}$ nazywamy **niewymiernością kwadratową**, gdy istnieje taki trójmian kwadratowy $f(X) = AX^2 + BX + C \in \mathbb{Z}[X]$ $(A \neq 0)$, że $f(\gamma) = 0$. Zbiór wszystkich niewymierności kwadratowych oznaczymy symbolem $\mathcal{Q}$.

Znane ze szkoły wzory na pierwiastki równania kwadratowego, porównaj (3.10), pokazują, że każda niewymierność kwadratowa jest postaci

$$\frac{x+\sqrt{\Delta}}{y}, \tag{7.24}$$

gdzie x, y, Δ są liczbami całkowitymi, przy czym Δ jest liczbą naturalną nie będącą kwadratem, a $\sqrt{\Delta}$ oznacza p i e r w i a s t e k a r y t m e t y c z n y (= dodatni).

ZADANIE 7.1 Udowodnić, że jeżeli liczba niewymierna γ jest pierwiastkiem trójmianów AX^2+BX+C, $A'X^2+B'X+C' \in \mathbb{Z}[X]$ i $\mathrm{NWD}\,(A,\,B,\,C)=1$, to istnieje taka liczba $d\in\mathbb{Z}$, że $A'=dA$, $B'=dB$, $C'=dC$.

Rozwiązanie. Oznaczmy $f(X)=AX^2+BX+C$ i $g(X)=A'X^2+B'X+C'$. W ustępie 6.3.1 dowiedzieliśmy się, że istnieje taka liczba wymierna d, że $g(X)=df(X)$. Oba wielomiany $f(X)$, $g(X)$ są bowiem generatorami ideału I_γ, zobacz C6.15. W naszym aktualnym przypadku rozumowanie wygląda następująco: Oznaczmy $d=A'/A$. Równość

$$g(X)-df(X)=(B'-dB)X+C'-dC$$

pokazuje, że γ jest pierwiastkiem wielomianu $(B'-dB)X+C'-dC$. Stąd, ponieważ γ jest liczbą niewymierną, wnioskujemy, że $B'-dB=0$ i następnie, że $C'-dC=0$. Wobec tego $A'=dA$, $B'=dB$ i $C'=dC$. Czyli $AB'=A'B$ i $AC'=A'C$. Mamy wykazać, że $d=A'/A\in\mathbb{Z}$. Załóżmy, że nie, czyli że istnieje liczba pierwsza $p|A$, ale $p\nmid A'$. Wtedy, na mocy T2.15, $p|B$ i $p|C$. To jest niemożliwe, bo z założenia $\mathrm{NWD}\,(A,\,B,\,C)=1$. $\lozenge$

Widzimy, że każda niewymierność kwadratowa γ wyznacza jednoznacznie taki trójmian $f(X)=AX^2+BX+C\in\mathbb{Z}[X]$, że $f(\gamma)=0$, $\mathrm{NWD}\,(A,\,B,\,C)=1$ i $A>0$. Nazwijmy go **trójmianem minimalnym** niewymierności (kwadratowej) γ. Wyróżnik $\Delta=B^2-4AC$ tego trójmianu nazwiemy **wyróżnikiem niewymierności kwadratowej** γ. Zbiór wszystkich niewymierności kwadratowych o wyróżniku Δ oznaczymy symbolem $\mathcal{Q}(\Delta)$.

Ćwiczenie 7.25 Uzasadnić, że wyróżnik Δ niewymierności kwadratowej spełnia warunek $\Delta\equiv 0,\,1\,(\mathrm{mod}\,4)$. Udowodnić też, że każda liczba naturalna Δ spełniająca ten warunek i nie będąca kwadratem jest wyróżnikiem co najmniej jednej niewymierności kwadratowej.

Z każdą niewymiernością kwadratową γ związana jest jednoznacznie liczba γ' będąca drugim pierwiastkiem trójmianu minimalnego niewymierności γ. Wiemy ze szkoły, że jeżeli γ jest zadana przez (7.24), to $\gamma'=\frac{x-\sqrt{\Delta}}{y}$. Liczbę γ' nazywamy **sprzężoną** z (niewymiernością kwadratową) γ. Niewymierność kwadratowa γ i jej sprzężona γ' mają ten sam wyróżnik (bo mają ten sam trójmian minimalny).

Ćwiczenie 7.26 Udowodnić, że jeżeli $\gamma\in\mathbb{R}$ jest niewymiernością kwadratową, to γ' jest jedyną taką liczbą rzeczywistą, że $\gamma+\gamma'$ i $\gamma\gamma'$ są liczbami wymiernymi.

ZADANIE 7.2 Udowodnić, że jeżeli $\gamma\in\mathcal{Q}(\Delta)$, a $\mathbf{A}\in\mathbf{GL}_2(\mathbb{Z})$, to $\mathbf{A}(\gamma)\in\mathcal{Q}(\Delta)$. Ponadto $\mathbf{A}(\gamma)'=\mathbf{A}(\gamma')$.

Rozwiązanie. Niech $AX^2+BX+C\in\mathbb{Z}[X]$ będzie trójmianem minimalnym liczby γ. Niech $\beta=\mathbf{A}(\gamma)$. Sprawdzamy, czy teza zachodzi dla trzech konkretnych macierzy $\mathbf{A}$.

(1) Niech $\mathbf{A}=\mathbf{T}$. Wówczas $\beta=\gamma+1$, więc $\gamma=\beta-1$ i $\gamma^2=\beta^2-2\beta+1$. Zatem

$$0=A\gamma^2+B\gamma+C=A\beta^2+(B-2A)\beta+(A-B+C).$$

Wobec tego $AX^2+(B-2A)X+(A-B+C)$ jest trójmianem minimalnym liczby β. (Łatwo sprawdzić, że jest to wielomian pierwotny.) Ponadto $(B-2A)^2-4A(A-B+C)=B^2-4AC$. Więc $\gamma+1\in\mathcal{Q}(\Delta)$. Musimy jeszcze uzasadnić, że $\beta'=\gamma'+1$. To wynika z C7.26, bo

$$(\gamma+1)+(\gamma'+1)=(\gamma+\gamma')+2=2-\frac{B}{A}\in\mathbb{Q},$$
$$(\gamma+1)(\gamma'+1)=\gamma\gamma'+\gamma+\gamma'+1=\frac{C}{A}-\frac{B}{A}+1\in\mathbb{Q}$$

na mocy wzorów Viète'*a*.

(2) Niech $\mathbf{A}=\mathbf{S}$. Wówczas $\beta=-1/\gamma$. Łatwo widzieć, że CX^2-BX+A jest trójmianem minimalnym liczby β. Więc $\beta\in\mathcal{Q}(\Delta)$. Sprawdzenie, że $\beta'=-1/\gamma'$ za pomocą wzorów Viète'*a* i tezy ćwiczenia C7.26 jest natychmiastowe.

(3) Niech $\mathbf{A}=\mathbf{R}$. Wówczas $\beta=-\gamma$. Jasne, że trójmianem minimalnym liczby β jest AX^2-BX+C o tym samym wyróżniku Δ. Również jasne, że $\beta'=-\gamma'$.

Twierdzenie T7.8 pozwala zakończyć rozwiązanie (jak?). ◊

7.3.7 Okresowe ułamki łańcuchowe

Rozwijanie liczb rzeczywistych na ułamki łańcuchowe jest koncepcyjnie podobne do rozwijania (dodatnich) liczb rzeczywistych na ułamki dziesiętne (zobacz paragraf 12.2). Jest jednak z teorioliczbowego punktu widzenia znacznie ważniejsze. W tym ustępie przyjrzymy się okresowym ułamkom łańcuchowym.

P r z y k ł a d. Najprostszym ciągiem okresowym jest ciąg stały. Niech $c\in\mathbb{N}$. Wartość γ ułamka $\langle c,\,c,\,c,\,\dots\rangle$ jest, zobacz (7.15), liczbą spełniającą warunek $\gamma=\langle c,\,\gamma\rangle$, czyli $\gamma=c+1/\gamma$. Wobec tego γ jest większym niż c pierwiastkiem trójmianu kwadratowego X^2-cX-1. Mamy więc do czynienia z niewymiernością kwadratową

$$\langle c,\,c,\,c,\,\dots\rangle=\frac{c+\sqrt{c^2+4}}{2}.$$

Sprzężoną niewymiernością kwadratową jest $\gamma'=\frac{c-\sqrt{c^2+4}}{2}$. Zwróćmy uwagę, że $\gamma>1$, a $-1<\gamma'<0$. Więc γ jest tak zwaną zredukowaną niewymiernością kwadratową: ◊

Definicja 7.8 Niewymierność kwadratowa γ nazywa się **zredukowaną niewymiernością kwadratową**, gdy $\gamma>1$ i jednocześnie $-1<\gamma'<0$.

Ćwiczenie 7.27 Uzasadnić, że jeżeli $a,\,b\in\mathbb{N}$, to wartość okresowego ułamka łańcuchowego $\langle a,\,b,\,a,\,b,\,\dots\rangle$ jest zredukowaną niewymiernością kwadratową.

TWIERDZENIE 7.10 *Jeżeli* $(c_0,\,c_1,\,c_2,\,\dots)$ *jest czysto-okresowym ciągiem o wyrazach naturalnych, to wartość* $\langle c_0,\,c_1,\,c_2,\,\dots\rangle$ *jest zredukowaną niewymiernością kwadratową.*

D O W Ó D. Niech $\gamma=\langle c_0,\,c_1,\,\dots\rangle$ będzie wartością nieskończonego ułamka łańcuchowego wyznaczonego przez ciąg czysto-okresowy (c_n). [Ciąg $(x_0,\,x_1,\,\dots)$ nazywa się **ciągiem czysto-okresowym**, gdy istnieje taka liczba $s\in\mathbb{N}$, że $x_{n+s}=x_n$ dla każdego $n\in\mathbb{Z}_{\geqslant 0}$.]

Wiemy, że γ jest liczbą niewymierną. Załóżmy, że okres ma długość s, czyli że $c_{s+n} = c_n$ dla każdego $n = 0, 1, \ldots$. Wówczas

$$\gamma_s := \langle c_s, c_{s+1}, \ldots \rangle = \langle c_0, c_1, \ldots \rangle = \gamma.$$

Jednocześnie, zobacz (7.15), $\gamma = \langle c_0, c_1, \ldots, c_{s-1}, \gamma_s \rangle$. Wobec tego, zob. (7.8) i (7.9), (7.10),

$$\gamma = \frac{K(c_0, c_1, \ldots, c_{s-1}, \gamma)}{K(c_1, c_2, \ldots, c_{s-1}, \gamma)} = \frac{\gamma P_{s-1} + P_{s-2}}{\gamma Q_{s-1} + Q_{s-2}}.$$

Zatem γ jest większym niż 1 (niewymiernym!) pierwiastkiem trójmianu kwadratowego

$$f(X) = Q_{s-1}X^2 + (Q_{s-2} - P_{s-1})X - P_{s-2}. \tag{7.25}$$

Oznaczmy przez γ' drugi pierwiastek tego trójmianu. Ponieważ $f(0) = -P_{s-2} < 0$ (dlaczego?), a $f(-1) = Q_{s-1} - Q_{s-2} + P_{s-1} - P_{s-2} > 0$ (zob. C7.7), więc $-1 < \gamma' < 0$. □

WNIOSEK. *Jeżeli ciąg $(c_n) \in \mathscr{C}$ jest okresowy od pewnego miejsca, to wartość nieskończonego ułamka łańcuchowego jest niewymiernością kwadratową.*

DOWÓD. Okresowość (od pewnego miejsca) ciągu (c_n) oznacza istnienie takich s i k, że $c_{s+n} = c_n$ dla wszystkich $n \geqslant k$. Czyli czystą okresowość ciągu $(c_k, c_{k+1}, c_{k+2}, \ldots)$. Z twierdzenia T7.10 wiemy, że wartość $\gamma_k = \langle c_k, c_{k+1}, \ldots \rangle$ jest (zredukowaną) niewymiernością kwadratową. Jednocześnie, zobacz (7.15), $\gamma = \langle c_0, c_1, \ldots, c_{k-1}, \gamma_k \rangle$, czyli

$$\gamma = \mathbf{A}(\gamma_k), \quad \text{gdzie} \quad \mathbf{A} = \begin{pmatrix} P_{k-1} & P_{k-2} \\ Q_{k-1} & Q_{k-2} \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z})$$

(zobacz (7.19)). Dla zakończenia dowodu wystarczy zauważyć, że $\gamma_k = \mathbf{A}^{-1}(\gamma)$ (patrz C7.18 (7.23)(2)) i powołać się na Z7.2. □

Tezę poniższego zadania wykorzystamy w następnym ustępie.

ZADANIE 7.3 *Załóżmy, że $\gamma = \langle \overline{c_0, c_1, \ldots, c_{s-1}} \rangle$ jest wartością czysto-okresowego ułamka łańcuchowego. Udowodnić, że wówczas $-1/\gamma' = \langle \overline{c_{s-1}, c_{s-2}, \ldots, c_0} \rangle$.*

Rozwiązanie. Oznaczmy na chwilę $b_0 = c_{s-1}, b_1 = c_{s-2}, \ldots, b_{s-1} = c_0$. Wtedy $\langle \overline{c_{s-1}, c_{s-2}, \ldots, c_0} \rangle = \langle \overline{b_0, b_1, \ldots, b_{s-1}} \rangle$. Oznaczmy wartość tego ułamka łańcuchowego przez β. Wiemy, że γ jest (większym niż 1) pierwiastkiem trójmianu (7.25). Analogicznie, β jest pierwiastkiem trójmianu

$$g(X) = Q'_{s-1}X^2 + (Q'_{s-2} - P'_{s-1})X - P'_{s-2},$$

gdzie oznaczyliśmy $P'_n = K(b_0, b_1, \ldots, b_n)$ i $Q'_n = K(b_1, b_2, \ldots, b_n)$. Z ćwiczenia C7.28 dowiadujemy się, że zachodzą równości $P'_{s-1} = P_{s-1}$, $P'_{s-2} = Q_{s-1}$, $Q'_{s-1} = P_{s-2}$ i $Q'_{s-2} = Q_{s-2}$. Wobec tego

$$g(X) = -X^2 \cdot f\left(-\frac{1}{X}\right), \tag{7.26}$$

gdzie $f(X)$ jest trójmianem (7.25). Ponieważ $g(\beta) = 0$, więc równość (7.26) pokazuje, że $f(-1/\beta) = 0$, czyli $-1/\beta$ jest (ujemnym, bo $\beta > 1$) pierwiastkiem trójmianu $f(X)$. Zatem $-1/\beta = \gamma'$. ◊

Ćwiczenie 7.28 Udowodnić, że kontynuanty mają następujące własności symetrii:

$$K(Y_1, Y_2, \ldots, Y_n) = K(Y_n, Y_{n-1}, \ldots, Y_1).$$

7.3.8 Twierdzenia Lagrange'*a* i Galois'*a*

W poprzednim ustępie przekonaliśmy się, że wartości okresowych ułamków łańcuchowych są niewymiernościami kwadratowymi. Okazuje się, że jest też odwrotnie. Mówią o tym udowodnione w tym ustępie twierdzenia Lagrange'*a* i Galois'*a*.

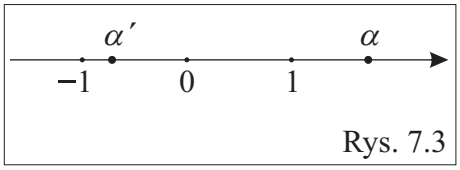
Ćwiczenie 7.29 Udowodnić, że jeżeli γ jest zredukowaną niewymiernością kwadratową, to wszystkie pseudomianowniki γ_n kanonicznego rozwinięcia liczby $\gamma = \gamma_0$ na ułamek łańcuchowy są również zredukowanymi niewymiernościami kwadratowymi.

Ćwiczenie 7.30 Udowodnić, że jeżeli γ jest zredukowaną niewymiernością kwadratową, to $-1/\gamma'$ też jest zredukowaną niewymiernością kwadratową.

LEMAT 7.1 *Istnieje tylko skończenie wiele zredukowanych niewymierności kwadratowych danego wyróżnika.*

D O W Ó D. Niech $\gamma = \frac{x+\sqrt{\Delta}}{y} \in \mathcal{Q}(\Delta)$ będzie zredukowaną niewymiernością kwadratową o wyróżniku Δ. To oznacza, że $\gamma > 1$, a liczba sprzężona $\gamma' = \frac{x-\sqrt{\Delta}}{y}$ leży w przedziale otwartym $(-1;\, 0)$, zobacz rysunek 7.3.

Widzimy, że $\gamma - \gamma' > 1$. Więc $2\sqrt{\Delta}/y > 1$. Stąd $y > 0$ i $y < 2\sqrt{\Delta}$. Również $\gamma + \gamma' > 0$, więc $2x/y > 0$, czyli $x > 0$. Zaś z warunku $\gamma' > -1$ wnioskujemy, że $-y < x - \sqrt{\Delta}$. Mamy więc



Rys. 7.3

$$0 < x < \sqrt{\Delta} \qquad \text{i} \qquad 0 < y < 2\sqrt{\Delta}.$$

Ponieważ, przy ustalonym Δ, istnieje tylko skończenie wiele par $(x,\, y)$ liczb całkowitych spełniających te warunki, więc dowód jest zakończony. □

TWIERDZENIE 7.11 (***Twierdzenie Galois'a* – 1828**) *Jeżeli γ jest zredukowaną niewymiernością kwadratową, to ciąg (c_n) mianowników jej kanonicznego rozwinięcia na ułamek łańcuchowy jest ciągiem czysto-okresowym.*

D O W Ó D. Popatrzmy na ciąg (γ_n) pseudomianowników kanonicznego rozwinięcia liczby $\gamma = \gamma_0$ na ułamek łańcuchowy. Z ćwiczenia C7.21 wiemy, że wszystkie liczby γ_n są równoważne liczbie γ. Wobec tego zadanie Z7.2 poucza nas, że $\gamma_n \in \mathcal{Q}(\Delta)$ dla każdego $n = 0, 1, \ldots$. Z ćwiczenia C7.29 wiemy, że wszystkie liczby γ_n są zredukowanymi niewymiernościami kwadratowymi o wyróżniku Δ. Ponieważ (zobacz L7.1) takich niewymierności jest tylko skończenie wiele, więc istnieją takie indeksy $0 \leqslant m < n$, że $\gamma_m = \gamma_n$. To dowodzi, że ciąg mianowników (c_k) jest ciągiem okresowym (od pewnego miejsca – mianowicie od miejsca c_m). Gdy $m = 0$, to mamy do czynienia z czystą okresowością. Załóżmy więc, że $m > 0$.

Równość $\gamma_{m-1} = c_{m-1} + \frac{1}{\gamma_m}$ po sprzężeniu daje równość $\gamma'_{m-1} = c_{m-1} + \frac{1}{\gamma'_m}$ (zobacz Z7.2), co z kolei zapiszemy następująco:

$$-\frac{1}{\gamma'_m} = c_{m-1} + \frac{1}{-\dfrac{1}{\gamma'_{m-1}}}. \tag{7.27}$$

Ponieważ, zgodnie z C7.30, zarówno $-1/\gamma'_m$ jak i $-1/\gamma'_{m-1}$ są zredukowanymi niewymiernościami kwadratowymi, czyli są większe niż 1, więc równość (7.27) dowodzi, że $\lfloor -1/\gamma'_m \rfloor = c_{m-1}$. Dokładnie tak samo sprawdzamy, że $\lfloor -1/\gamma'_n \rfloor = c_{n-1}$. Ale $\gamma_m = \gamma_n$, więc $\gamma'_m = \gamma'_n$, czyli też $-1/\gamma'_m = -1/\gamma'_n$. Liczby równe mają równe części całkowite, więc $c_{m-1} = c_{n-1}$. Zatem

$$\gamma_{m-1} = \langle c_{m-1},\, \gamma_m \rangle = \langle c_{n-1},\, \gamma_n \rangle = \gamma_{n-1}.$$

W ten sposób po skończonej liczbie kroków dojdziemy do równości $\gamma = \gamma_0 = \gamma_{n-m}$, czyli do równości $\gamma = \langle\, \overline{c_0,\, c_1,\, \ldots,\, c_{s-1}}\, \rangle$, gdzie $s = n - m$. □

Z twierdzenia Galois'*a* wyprowadzimy dwa (historycznie wcześniejsze) twierdzenia.

TWIERDZENIE 7.12 (***Twierdzenie Lagrange'a* – 1768**) *Jeżeli γ jest niewymiernością kwadratową, to ciąg (c_n) mianowników jej kanonicznego rozwinięcia na ułamek łańcuchowy jest ciągiem okresowym (od pewnego miejsca).*

D O W Ó D. Wobec twierdzenia Galois'*a* wystarczy udowodnić, że pewien pseudomianownik γ_n jest zredukowaną niewymiernością kwadratową. Ponieważ $\gamma_n > 1$ dla każdego n, więc wystarczy udowodnić, że $-1 < \gamma'_n < 0$ dla pewnego n. Równość (7.15) daje po sprzężeniu (zobacz Z7.2)

$$\gamma' = \frac{\gamma'_n P_{n-1} + P_{n-2}}{\gamma'_n Q_{n-1} + Q_{n-2}}.$$

Wyznaczając stąd γ'_n (zobacz też (7.23)(2)) otrzymamy

$$\gamma'_n = \frac{\gamma' Q_{n-2} - P_{n-2}}{-\gamma' Q_{n-1} + P_{n-1}} = (-1) \cdot \frac{Q_{n-2}}{Q_{n-1}} \cdot \frac{\dfrac{P_{n-2}}{Q_{n-2}} - \gamma'}{\dfrac{P_{n-1}}{Q_{n-1}} - \gamma'}. \tag{7.28}$$

Z twierdzenia T7.5 wiemy, że redukty P_k/Q_k są zbieżne do $\gamma > 1$. Istnieje więc taka parzysta liczba n, że $1 < P_{n-2}/Q_{n-2} < P_{n-1}/Q_{n-1}$. Dla takiego n licznik drugiego ułamka w (7.28) jest mniejszy niż mianownik i oba są dodatnie. Ponieważ jednocześnie $0 < Q_{n-2}/Q_{n-1} < 1$, zobacz C7.7, więc $-1 < \gamma'_n < 0$ dla takiego n. To kończy dowód. □

Przyjrzyjmy się jeszcze raz przykładom w tabelce z ustępu 7.3.1. Zauważamy, że wszystkie wypisane rozwinięcia są o k r e s o w e (okres zaznaczono kreską). Okresy te zaczynają się od wyrazu c_1, a kończą na wyrazie o wartości $2c_0$. Nie jest to zjawisko przypadkowe. Zachodzi mianowicie poniższe twierdzenie:

TWIERDZENIE 7.13 (***Twierdzenie Lagrange'a***) *Jeżeli $D \in \mathbb{N}$ nie jest kwadratem, to kanoniczne rozwinięcie liczby $\sqrt{D}$ na ułamek łańcuchowy jest okresowe:*

$$\sqrt{D} = \langle\, c_0,\, \overline{c_1,\, \ldots,\, c_{s-1},\, c_s}\, \rangle \tag{7.29}$$

(okres pewnej długości s, zaznaczono kreską). Ponadto zachodzi równość $c_s = 2c_0$, a część $(c_1, \ldots, c_{s-1})$ okresu jest ciągiem palindromicznym.

D O W Ó D. Niech $\lfloor\sqrt{D}\rfloor = c_0$. I niech $\beta = c_0+\sqrt{D}$. Łatwo widzieć, że β jest zredukowaną niewymiernością kwadratową. Niech $\beta = \langle\, \overline{b_0,\, b_1,\, \ldots,\, b_{s-1}}\,\rangle$. Taka równość ma miejsce wobec twierdzenia Galois'*a*. Oczywiście $b_0 = 2c_0$. Z zadania Z7.3 wiemy, że

$$-\frac{1}{\beta'} = \langle\, \overline{b_{s-1},\, b_{s-2},\, \ldots,\, b_0}\,\rangle.$$

Jednocześnie, ponieważ $\beta' = c_0 - \sqrt{D}$,

$$-\frac{1}{\beta'} = \frac{1}{\sqrt{D}-c_0} = \frac{1}{\beta - b_0} = \frac{1}{\langle\, 0,\, \overline{b_1,\, \ldots,\, b_{s-1},\, b_0}\,\rangle} = \langle\, \overline{b_1,\, \ldots,\, b_{s-1},\, b_0}\,\rangle.$$

To kończy dowód. □

Poniższy wniosek z twierdzenia T7.13 był podstawowym powodem, dla którego Lagrange zajmował się ułamkami łańcuchowymi (zobacz też paragraf 11.4):

WNIOSEK *Niech D będzie liczbą naturalną nie będącą kwadratem. Wówczas, jeżeli P_n/Q_n oznacza n-ty redukt ułamka łańcuchowego* (7.29)*, to dla każdego $k \in \mathbb{N}$ zachodzi równość*

$$P_{ks-1}^2 - DQ_{ks-1}^2 = (-1)^{ks}. \tag{7.30}$$

D O W Ó D. Równość (7.15) ma dla $n = ks$ w tym przypadku postać

$$\sqrt{D} = \frac{(c_0+\sqrt{D})P_{ks-1} + P_{ks-2}}{(c_0+\sqrt{D})Q_{ks-1} + Q_{ks-2}}.$$

Przekształcając to, otrzymamy $c_0P_{ks-1} + P_{ks-2} - DQ_{ks-1} = (c_0Q_{ks-1} + Q_{ks-2} - P_{ks-1})\sqrt{D}$, skąd, wobec wymierności P_i, Q_i i niewymierności $\sqrt{D}$, mamy

$$\begin{aligned} P_{ks-2} &= DQ_{ks-1} - c_0P_{ks-1}, \\ Q_{ks-2} &= P_{ks-1} - c_0Q_{ks-1}. \end{aligned}$$

Kładąc $n = ks-1$ w tożsamości (7.11), znajdujemy więc

$$\begin{aligned} (-1)^{ks-2} &= P_{ks-1}Q_{ks-2} - Q_{ks-1}P_{ks-2} \\ &= P_{ks-1}(P_{ks-1} - c_0Q_{ks-1}) - Q_{ks-1}(DQ_{ks-1} - c_0P_{ks-1}) \\ &= P_{ks-1}^2 - DQ_{ks-1}^2, \end{aligned}$$

co kończy dowód. □

Ćwiczenie 7.31 Brahmagupta napisał, że ktoś, kto w ciągu roku potrafi znaleźć nietrywialne (to znaczy różne od $(x,\, y) = (1,\, 0)$) rozwiązanie równania $x^2 - 92y^2 = 1$ w liczbach naturalnych, jest matematykiem. I co ty na to Czytelniku?

Rozdział 8

Sumy kwadratów

Tout nombre premier,
qui surpasse de l'unité un multiple du quaternaire,
est une seule fois la somme de deux carrés.

(Pierre Fermat w liście do Mersenne'*a* - 1640)

Theorema. Omnis numerus primus formae $4n+1$
est summa duorum quadratorum.

(Leonhard Euler - 1747)

Liczba $5 = 1^2 + 2^2$ nie jest kwadratem, ale jest sumą dwóch kwadratów. Jak scharakteryzować te liczby całkowite (nieujemne!), które dadzą się przedstawić w postaci sumy dwóch kwadratów? W tym rozdziale pokażemy kilka częściowych odpowiedzi na to pytanie. Podstawowym twierdzeniem rozdziału jest T8.1, sformułowane (i prawdopodobnie udowodnione), jak widać z "motta", przez Fermat'*a* i (z pewnością) udowodnione ponad sto lat później przez Eulera. Podamy kilka dowodów tego twierdzenia. Następnie, wykorzystując twierdzenie Minkowskiego o figurze wypukłej, zajmiemy się możliwością przedstawiania liczb całkowitych w postaci $x^2 + 2y^2$, $x^2 + 3y^2$ i, ogólniej, w postaci $x^2 + cy^2$. Jeszcze ogólniej, można się pytać o możliwość przedstawiania liczb całkowitych w postaci $ax^2 + bxy + cy^2$, gdzie $a, b, c \in \mathbb{Z}$. Powiemy parę słów na ten temat. W szczególności, pokażemy (pochodzący od Lagrange'*a*) pomysł redukowania form kwadratowych $aX^2 + bXY + cY^2$ do postaci prostszych, które łatwiej poddają się badaniu. Kolejnym, prezentowanym tu, osiągnięciem Lagrange'*a* jest dowód twierdzenia o możliwości przedstawienia dowolnej liczby naturalnej w postaci sumy czterech kwadratów. Rozdział kończymy (piątym) dowodem TFE.

8.1 Jedna ważna tożsamość

Zaczniemy od pewnej tożsamości. Jej ślady odnaleźć można już u Diofantosa, a szczególne jej przypadki znali i używali Brahmagupta i Leonardo z Pizy (Fibonacci).

Definicja 8.1 Następującą tożsamość:

$$\boxed{(x^2 + cy^2)(u^2 + cv^2) = (xu \pm cyv)^2 + c(xv \mp yu)^2,} \tag{8.1}$$

której dowód jest oczywistym rachunkiem, nazywać będziemy ***tożsamością Brahmagupty***, a w przypadku $c = 1$ – ***tożsamością Fibonacci'ego***.

Ustalmy $c \in \mathbb{Z}$ i rozważmy równanie $x^2 + cy^2 = n$, gdzie n jest liczbą całkowitą. Załóżmy, że badamy rozwiązania tego równania w liczbach naturalnych $x,\, y \in \mathbb{N} := \{k \in \mathbb{Z} :\, k > 0\}$. Z tożsamości Brahmagupty łatwo wyciągnąć dwa wnioski:

WNIOSEK 1 *Jeżeli* $(x_1,\, y_1)$ *jest rozwiązaniem równania* $x^2 + cy^2 = n_1$, *a* $(x_2,\, y_2)$ *jest rozwiązaniem równania* $x^2 + cy^2 = n_2$, *to równanie* $x^2 + cy^2 = n_1 n_2$ *ma (co najmniej) dwa rozwiązania* $(|x_1x_2 - cy_1y_2|,\, |x_1y_2 + x_2y_1|)$ *oraz* $(|x_1x_2 + cy_1y_2|,\, |x_1y_2 - x_2y_1|)$ *(różne!).* □

WNIOSEK 2 *Jeżeli* $n = (-1)^e p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ *jest rozkładem na czynniki pierwsze, to* w a r u n k i e m w y s t a r c z a j ą c y m *rozwiązalności równania* $x^2 + cy^2 = n$ *jest rozwiązalność równań* $x^2 + cy^2 = (-1)^e$ *i* $x^2 + cy^2 = p_i$ *dla* $i = 1,\, 2,\, \ldots,\, s$. □

P r z y k ł a d 1. Równanie $x^2 + 2y^2 = 59$ ma rozwiązanie $(3,\, 5)$, a równanie $x^2 + 2y^2 = 114$ ma rozwiązanie $(4,\, 7)$. Wobec tego równanie $x^2 + 2y^2 = 6726$ ma (co najmniej) dwa rozwiązania. Rzeczywiście:

$$(3^2 + 2 \cdot 5^2)(4^2 + 2 \cdot 7^2) = \mathbf{58^2 + 2 \cdot 41^2 = 82^2 + 2 \cdot 1^2} = (3^2 + 2 \cdot (-5)^2)(4^2 + 2 \cdot 7^2)\ \lozenge.$$

P r z y k ł a d 2. Szczególnie ciekawy przykład zastosowania wniosku 1 mamy, gdy $n_1 = 1$. Na przykład $2^2 - 3 \cdot 1^2 = 1$ i $3^2 - 3 \cdot 2^2 = -3$. Więc para $(2,\, 1)$ jest rozwiązaniem równania $x^2 - 3y^2 = 1$, a para $(3,\, 2)$ jest rozwiązaniem równania $x^2 - 3y^2 = -3$. Wobec tego para $(12,\, 7)$ jest nowym rozwiązaniem równania $x^2 - 3y^2 = -3$. Tę sztuczkę możemy powtarzać! To prowadzi do rekurencyjnie zadanego ciągu $(a_n,\, b_n)$ rozwiązań równania $x^2 - 3y^2 = -3$: Jeżeli $a_n^2 - 3b_n^2 = -3$, to $(a_{n+1},\, b_{n+1}) = (2a_n + 3b_n,\, a_n + 2b_n)$. $\lozenge$

Wielomian $X^2 + cY^2$ jest przykładem binarnej formy kwadratowej $aX^2 + bXY + cY^2$, zobacz paragraf 8.4. Jeżeli $a,\, b,\, c$ są dowolnymi liczbami całkowitymi, to symbolem $\mathcal{W}_{(a,\,b,\,c)}$ oznaczać będziemy zbiór wszystkich liczb całkowitych dających się przedstawić w postaci $ax^2 + bxy + cy^2$ dla pewnych całkowitych $x,\, y$:

$$\mathcal{W}_{(a,\,b,\,c)} = \{ax^2 + bxy + cy^2 \,:\, x,\, y \in \mathbb{Z}\}.$$

Na przykład $\mathcal{W}_{(1,\,0,\,0)} = \mathcal{W}_{(0,\,0,\,1)}$ jest zbiorem kwadratów, $\mathcal{W}_{(1,\,0,\,1)}$ jest zbiorem liczb całkowitych będących sumami dwóch kwadratów, a $\mathcal{W}_{(0,\,1,\,0)}$ jest całym zbiorem $\mathbb{Z}$.

Niech $c \in \mathbb{Z}$ będzie dowolną liczbą całkowitą. Dzięki tożsamości Brahmagupty dowodzimy ciekawej i ważnej własności zbioru $\mathcal{W}_{(1,\,0,\,c)}$:

$$\boxed{m \in \mathcal{W}_{(1,\,0,\,c)} \quad \wedge \quad n \in \mathcal{W}_{(1,\,0,\,c)} \quad \Longrightarrow \quad m \cdot n \in \mathcal{W}_{(1,\,0,\,c)}.}$$

Mówimy, że zbiór $\mathcal{W}_{(1,\,0,\,c)}$ jest **multyplikatywnie zamknięty**.

Sympatyczne wykorzystanie multyplikatywnej zamkniętości zbioru $\mathcal{W}_{(1,\,0,\,6)}$ zobaczyć można w rozwiązaniu zadania z drugiego etapu LXII Olimpiady Matematycznej:

ZADANIE 8.1 Udowodnić, że n i e ma takich liczb całkowitych $x_1,\, x_2,\, \ldots,\, x_{2011}$, ani $y_1,\, y_2,\, \ldots,\, y_{2011}$, dla których liczba $L = (2x_1^2 + 3y_1^2)(2x_2^2 + 3y_2^2) \cdot \ldots \cdot (2x_{2011}^2 + 3y_{2011}^2)$ byłaby kwadratem liczby naturalnej.

R o z w i ą z a n i e. Załóżmy, nie wprost, że wskazana liczba L jest kwadratem. Wówczas $2^{2012}L$ również jest kwadratem. Czyli

$$M^2 = 2^{2012}L = 2 \cdot [(2x_1)^2 + 6y_1^2)((2x_2)^2 + 6y_2^2) \cdot \ldots \cdot ((2x_{2011})^2 + 6y_{2011}^2)].$$

Korzystając z multyplikatywnej zamkniętości zbioru $\mathcal{W}_{(1,0,6)}$, możemy zapisać powyższą równość skrótowo tak: $M^2 = 2(A^2 + 6C^2)$ przy pewnych A, $C \in \mathbb{Z}$. Kładąc $B = 2C$, dostajemy

$$M^2 = 2A^2 + 3B^2.$$

Ale to jest niemożliwe! [Aby to zobaczyć wystarczy zredukować (mod 3) i zastosować metodę desantu.] ◊

Elementarnym, ale bardzo ważnym, ćwiczeniem jest poniższe:

Ćwiczenie 8.1 Udowodnić, że jeżeli p jest liczbą pierwszą, $p \nmid c$ i $p \in \mathcal{W}_{(1,0,c)}$, to liczba $(-c)$ jest resztą kwadratową modulo p.

8.2 Sumy dwóch kwadratów

W tym paragrafie udowodnimy (dwiema metodami) twierdzenie Fermat'*a*-Eulera. W literaturze nazywa się je częściej twierdzeniem Fermat'*a*, ale, ponieważ pierwsze znane dowody pochodzą od Eulera, więc nazywamy je twierdzeniem Fermat'*a*-Eulera. TFE pozwoli scharakteryzować te liczby naturalne, które dadzą się przedstawić w postaci sumy dwóch kwadratów (liczb całkowitych).

8.2.1 Twierdzenie Fermat'*a*-Eulera

Pierwszy prezentowany przez nas dowód TFE opiera się na twierdzeniu T7.1.

LEMAT 8.1 *Jeżeli* n, a, $b \in \mathbb{N}$, $\mathrm{NWD}\,(a,b) = 1$ *oraz* $n|a^2 + b^2$, *to istnieją takie liczby całkowite* x, y, *że* $n = x^2 + y^2$.

D O W Ó D. Udowodnimy to najpierw w przypadku, gdy $b = 1$. Zastosujemy w tym celu T7.1 do liczb $\alpha = \frac{a}{n}$ i $N = \lfloor \sqrt{n} \rfloor$. Znajdziemy wówczas takie h, k, że

$$\left| \frac{a}{n} - \frac{h}{k} \right| \leqslant \frac{1}{k(N+1)} \qquad \text{oraz} \qquad k \leqslant N. \tag{8.2}$$

Twierdzimy, że $x = ak - nh$ i $y = k$ są dobre. Aby to sprawdzić pokażemy, że $x^2 + y^2$ jest niezerową wielokrotnością liczby n mniejszą niż $2n$. To, oczywiście, skończy dowód w przypadku $b = 1$. Mamy

$$x^2 + y^2 = (ak - nh)^2 + k^2 = a^2k^2 - 2ahkn + n^2h^2 + k^2 = k^2(a^2 + 1) + n(nh^2 - 2ahk).$$

Założenie, $n|a^2 + 1$ daje więc $n|x^2 + y^2$. Z drugiej strony mnożąc nierówność (8.2) przez nk i podnosząc do kwadratu dostajemy

$$x^2 = |ak - nh|^2 \leqslant \left(\frac{n}{N+1} \right)^2 < n.$$

Ostania nierówność wynika z oczywistej nierówności $n < (N+1)^2$. Ponadto, ponieważ $1 \leqslant k \leqslant N$, więc $y^2 = k^2 \leqslant N^2 = \lfloor\sqrt{n}\rfloor^2 \leqslant \sqrt{n}^2 = n$. Zatem $0 < x^2 + y^2 < 2n$.

Jeżeli $b \neq 1$, to dobieramy takie $u, v \in \mathbb{Z}$, by $au + bv = 1$. Wówczas, na mocy tożsamości Fibonacci'*ego* (8.1):

$$(a^2+b^2)(u^2+v^2) = (av-bu)^2 + (au+bv)^2 = A^2 + 1.$$

Zatem $n|A^2+1$, więc n jest sumą dwóch kwadratów. □

Ćwiczenie 8.2 Udowodnić, że jeżeli liczba naturalna n jest dzielnikiem liczby

$$34x^2 - 42xy + 13y^2,$$

gdzie $x, y \in \mathbb{Z}$ są względnie pierwsze, to n jest sumą dwóch kwadratów (liczb całkowitych).

TWIERDZENIE 8.1 (***Twierdzenie Fermat'a-Eulera*, TFE**) *Nieparzysta liczba pierwsza p da się przedstawić w postaci $x^2 + y^2$ wtedy i tylko wtedy, gdy $p \equiv 1 \pmod 4$.*

P I E R W S Z Y D O W Ó D TFE. Konieczność warunku $p \equiv 1 \pmod 4$ jest oczywista. Dla dowodu dostateczności weźmy $a \in \mathbb{Z}$ spełniające $a^2 \equiv -1 \pmod p$ (zob. WT5.24). Wtedy $p|a^2+1$. Zatem, na mocy lematu L8.1, p jest sumą dwóch kwadratów. □

P r z y k ł a d. Weźmy nasze ulubione liczby pierwsze **1777** i **1801** (łatwo je zapamiętać: oznaczają rok urodzenia Gaussa i rok wydania jego słynnych *Disquisitiones Arithmeticae*). Dają one resztę 1 z dzielenia przez 4, więc muszą się dać przedstawić w postaci sumy dwóch kwadratów. Rzeczywiście:

$$\mathbf{1777} = 16^2 + 39^2, \qquad \mathbf{1801} = 24^2 + 35^2. \ \Diamond$$

Z przytoczonego na początku rozdziału "motta" widzimy, że Fermat zdawał sobie sprawę z niezwykle ważnej okoliczności, mianowicie j e d y n o ś c i p r z e d s t a w i e n i a (*une seule fois*). Udowodnimy to w poniższym zadaniu:

ZADANIE 8.2 Udowodnić, że przedstawienie $p = x^2 + y^2$ liczby pierwszej w postaci sumy dwóch kwadratów jest j e d n o z n a c z n e (z dokładnością do zamiany x^2 na y^2).

R o z w i ą z a n i e. Niech

$$p = x_1^2 + y_1^2 = x_2^2 + y_2^2 \tag{8.3}$$

będą dwoma przedstawieniami liczby pierwszej p w postaci sumy dwóch kwadratów. Wówczas $\mathrm{NWD}\,(x_i, y_i) = 1$ (bo kwadrat wspólnego dzielnika x_i i y_i jest dzielnikiem p) oraz $p \nmid x_i$ i $p \nmid y_i$. Mnożąc obustronnie kongruencję $x_i^2 + y_i^2 \equiv 0 \pmod p$ przez odwrotność $(y_i^2)^{-1}$ otrzymamy $(x_i y_i^{-1})^2 \equiv -1 \pmod p$. Widzimy więc, że $x_1 y_1^{-1}$ i $x_2 y_2^{-1}$ są rozwiązaniami kongruencji $z^2 + 1 \equiv 0 \pmod p$. Ale, zobacz T5.12, kongruencja ta ma co najwyżej dwa rozwiązania (jeżeli $a \pmod p$ jest rozwiązaniem, to drugim rozwiązaniem jest $-a \pmod p$). Zatem $x_1 y_1^{-1} \equiv \pm\, x_2 y_2^{-1} \pmod p$, co, po obustronnym pomnożeniu przez $y_1 y_2$, daje $x_1 y_2 \equiv \pm\, x_2 y_1 \pmod p$. Zmieniając ewentualnie y_1 na $-y_1$, mamy $x_1 y_2 \equiv x_2 y_1 \pmod p$. Równości (8.3) i tożsamość

podstawowa (8.1) (przy $c = 1$) dają $p^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2$. Ponieważ $p|x_1y_2 - x_2y_1$, więc też $p|x_1x_2 + y_1y_2$. Po podzieleniu przez p^2 otrzymamy

$$1 = \left(\frac{x_1x_2 + y_1y_2}{p}\right)^2 + \left(\frac{x_1y_2 - x_2y_1}{p}\right)^2.$$

Stąd $x_1x_2 = -y_1y_2$ lub $x_1y_2 = x_2y_1$. Jeżeli zachodzi pierwsza z tych równości, to, wobec względnej pierwszości x_1 i y_1, na mocy ZTA, mamy $x_1|y_2$, a wobec względnej pierwszości x_2 i y_2, $y_2|x_1$. Zatem $x_1 = \pm y_2$ i wtedy $x_2 = \pm y_1$. Podobnie rozpatrujemy drugi przypadek i dostajemy: $x_1 = \pm x_2$ i $y_1 = \pm y_2$. To kończy rozwiązanie. ◊

U w a g a. Wobec równości (które Czytelnik z pewnością zechce sprawdzić!)

$$F_6 = (2^{32})^2 + 1^2 = 4\,046\,803\,256^2 + 1\,438\,793\,759^2 \tag{8.4}$$

i powyższego, widzimy, że liczba Fermat'a F_6 n i e j e s t liczbą pierwszą. Podobnie, równości $F_5 = (2^{16})^2 + 1^2 = 62\,264^2 + 20\,449^2$ dowodzą złożoności piątej liczby Fermat'a, por. 5.5.5 U2.

8.2.2 Drugi dowód twierdzenia Fermat'a-Eulera

Twierdzenie Fermat'a-Eulera jest tak ważne, że pokażemy drugi jego dowód. Tym razem nie korzystamy z aproksymacji diofantycznej ani z prawa wzajemności.

LEMAT 8.2 *Jeżeli liczba pierwsza* $p \equiv 1 \pmod 4$, *to istnieje* $0 < m < p$ *i takie liczby* $x, y \in \mathbb{Z}$, *że* $mp = x^2 + y^2$.

D O W Ó D. Najpierw, nie korzystając z kryterium Eulera, sprawdzamy, że jeżeli p jest liczbą pierwszą postaci $4k + 1$, to $(-1)\mathbf{R}p$. Mamy, dzięki twierdzeniu Wilsona,

$$-1 \equiv (p-1)! \equiv 1 \cdot (p-1) \cdot 2(p-2) \cdot \ldots \cdot 2k(p-2k) \equiv (-1)^{2k}(1 \cdot 2 \cdot \ldots \cdot 2k)^2 \pmod p.$$

Widzimy stąd, że jeżeli $p \equiv 1 \pmod 4$, to istnieje taka $a \in \mathbb{Z}$, że $a^2 \equiv -1 \pmod p$, czyli $a^2 + 1 = sp$ dla pewnego $s \in \mathbb{N}$. Wybierzmy takie x, by $a \equiv x \pmod p$ i by $|x| < p/2$. Wówczas $x^2+1 = mp$ dla pewnej liczby naturalnej m. Ponadto $mp = x^2+1 < (p/2)^2+1 < p^2$. Stąd $0 < m < p$. Wystarczy teraz przyjąć $y = 1$. □

U w a g a. Pokazane powyżej zastosowanie twierdzenia Wilsona daje rozwiązanie kongruencji $z^2 \equiv -1 \pmod p$ dla liczb pierwszych $p \equiv 1 \pmod 4$. Rozwiązaniem tym jest $(2k)! \pmod p$.

Przechodzimy do naszego d r u g i e g o d o w o d u twierdzenia Fermat'a-Eulera (ponieważ w dowodzie tym wykorzystuje się pomysł **desantu**, więc jest wysoce prawdopodobne, że podobnie rozumował sam Fermat):

D R U G I D O W Ó D TFE. Lemat L8.2 poucza nas, że i s t n i e j ą wielokrotności mp liczby p będące sumami dwóch kwadratów. Niech $mp = x^2 + y^2$, gdzie $0 < m < p$, będzie taką wielokrotnością. Pokażemy, że jeżeli $m > 1$, to istnieje taka m n i e j s z a liczba naturalna $m' < m$, że $m'p$ r ó w n i e ż jest sumą dwóch kwadratów. Rozważamy osobno przypadki, gdy m jest parzysta i gdy m jest nieparzysta. W pierwszym przypadku, niech $m = 2m'$. Wówczas $x \equiv y \pmod 2$. Wobec tego

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = \frac{x^2+y^2}{2} = m'p$$

jest sumą kwadratów liczb całkowitych. W przypadku nieparzystego $m \geqslant 3$ zapiszmy:

$$\begin{cases} x = x_1 m + a & \text{przy pewnym} \quad |a| < \frac{m}{2}, \\ y = y_1 m + b & \text{przy pewnym} \quad |b| < \frac{m}{2}. \end{cases} \tag{8.5}$$

Możliwość takiego dzielenie z resztą wynika z nieparzystości m. Wtedy mamy $a^2 + b^2 = (x - x_1 m)^2 + (y - y_1 m)^2 = (x^2 + y^2) + m \cdot \text{coś} = m \cdot \text{cóś}$. Oznaczmy $a^2 + b^2 = mm'$. Wówczas

$$mm' = a^2 + b^2 < \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 = \frac{m^2}{2},$$

skąd $m' < \frac{m}{2}$. Korzystając teraz z tożsamości Fibonacci'*ego* możemy napisać

$$mm' \cdot mp = (a^2 + b^2)(x^2 + y^2) = (xb - ya)^2 + (xa + yb)^2.$$

Ponieważ bardzo łatwo, dzięki równościom (8.5), sprawdzamy, że $m | xb - ya$, więc powyższa równość daje $m^2 | (xa + yb)^2$. Możemy podzielić obustronnie przez m^2:

$$m'p = \left(\frac{xb - ya}{m}\right)^2 + \left(\frac{xa + yb}{m}\right)^2.$$

Jeżeli teraz $m' = 1$, to mamy przedstawienie p w postaci sumy dwóch kwadratów. Jeżeli zaś $m' > 1$, to możemy powtórzyć "sztuczkę". Jasne, że po nie więcej niż $\log_2 m$ takich "sztuczek" dojdziemy do przedstawienia $1 \cdot p = x^2 + y^2$. □

W poniższym (niełatwym!) ćwiczeniu pokazujemy, pochodzące od Gaussa, rozwiązanie zadania przedstawienia liczby pierwszej $p = 4k + 1$ w postaci $x^2 + y^2$:

Ćwiczenie 8.3 Udowodnić, że jeżeli $p = 4k + 1$ jest liczbą pierwszą i

$$x \equiv (2k + 1)\binom{2k}{k} \pmod{p}, \quad y \equiv (2k + 1)(2k)!\binom{2k}{k} \pmod{p}$$

oraz $|x|, |y| \leqslant 2k$, to $x^2 + y^2 = p$.

8.2.3 Twierdzenie o przedstawieniu

Udowodnimy teraz twierdzenie charakteryzujące liczby naturalne dające się przedstawić w postaci sumy dwóch kwadratów liczb całkowitych.

TWIERDZENIE 8.2 *Liczba naturalna n da się przedstawić w postaci sumy dwóch kwadratów wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p postaci $4k + 3$, wykładnik p-adyczny $v_p(n)$ jest liczbą parzystą.*

DOWÓD. ($\Longleftarrow$) Przedstawmy n w postaci $n = k^2 m$, gdzie m jest iloczynem różnych liczb pierwszych postaci $4k + 1$ i (ewentualnie) dwójki. Dzięki T8.1, równości $2 = 1^2 + 1^2$ i wielokrotnemu zastosowaniu tożsamości (8.1) możemy napisać $m = x^2 + y^2$. Stąd $n = (kx)^2 + (ky)^2$.

($\Longrightarrow$) Załóżmy teraz, że $n = x^2 + y^2$ jest sumą dwóch kwadratów i że liczba pierwsza $p \equiv 3 \pmod 4$ dzieli n. Twierdzimy, że wówczas $p|x$ i $p|y$. Gdyby bowiem $p \nmid x$, to, oznaczając przez u odwrotność x modulo p, mielibyśmy

$$nu^2 = (xu)^2 + (yu)^2,$$

skąd $1 + (yu)^2 \equiv 0 \pmod p$, co jest niemożliwe (bo -1 jest nieresztą kwadratową modulo $p \equiv 3 \pmod 4$). Podobnie sprawdzamy, że $p|y$. Zatem $n = x^2 + y^2 = (pa)^2 + (pb)^2$, więc $p^2|n$. Dokończenie rozumowania jest teraz natychmiastowe. □

8.2.4 Funkcja $r(n)$

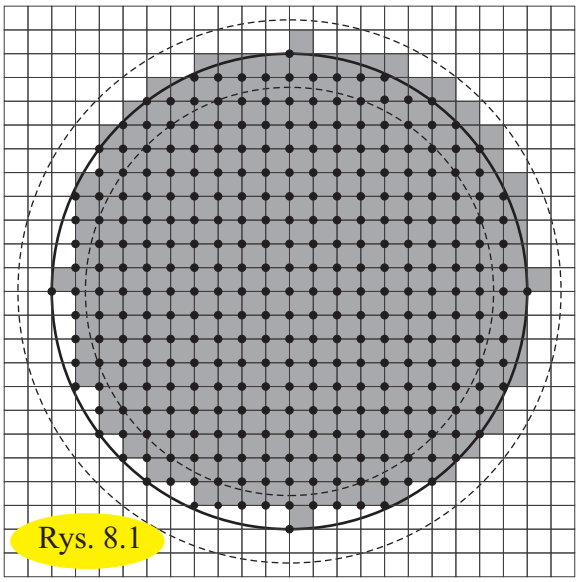
Oznaczmy przez $r(n)$ liczbę wszystkich takich par $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, że $x^2 + y^2 = n$. Inaczej mówiąc, $r(n)$ oznacza liczbę punktów kratowych leżących na okręgu $\mathcal{K}((0, 0), \sqrt{n})$ o środku w początku układu (współrzędnych prostokątnych) i promieniu $\sqrt{n}$.

Wiemy, że $r(n) = 0$ dla każdej liczby naturalnej $n \equiv 3 \pmod 4$. Wiemy też, że $r(p) = 8$ dla każdej liczby pierwszej $p \equiv 1 \pmod 4$. To oznacza, że – na przykład – okrąg o promieniu $\sqrt{37}$ i środku w punkcie kratowym przechodzi przez dokładnie osiem punktów kratowych.

Funkcja arytmetyczna r zachowuje się bardzo nieregularnie i nie znamy żadnego wzoru wyrażającego wartości funkcji r. Dużo łatwiej jest zbadać **wartość średnią**:

$$R(n) = \frac{1 + r(1) + \ldots + r(n)}{n}.$$

Licznik tego wyrażenia oznacza, jak łatwo widzieć, liczbę całkowitoliczbowych rozwiązań nierówności $x^2 + y^2 \leqslant n$, czyli liczbę punktów kratowych zawartych w kole $\mathcal{D}((0, 0), \sqrt{n})$. Ponieważ każdy (z wyjątkiem "paru" skrajnych) punkt kratowy zawiera się w tym kole wraz z odpowiadającym mu kwadratem jednostkowym, więc liczba tych punktów kratowych jest w przybliżeniu równa polu $\pi(\sqrt{n})^2$ tego koła. Stąd dostajemy równość


Rys. 8.1

$$\boxed{\lim_{n\to\infty} R(n) = \pi,}$$

którą interpretujemy tak: *Liczba naturalna ma przeciętnie π rozkładów na sumę dwóch kwadratów.*

Ćwiczenie 8.4 Udowodnić powyższą równość. *Wskazówka.* Sumaryczne pole kwadracików jednostkowych, których lewy dolny róg należy do koła o środku w początku układu i promieniu $\sqrt{N}$, jest liczbą zawartą między polem koła o promieniu $\sqrt{N} - \sqrt{2}$ a polem koła o promieniu $\sqrt{N} + \sqrt{2}$. Zobacz rysunek 8.1.

8.3 Nieco geometrii w teorii liczb

Opowiemy teraz jak można zastosować w teorii liczb proste pojęcia z geometrii płaszczyzny.

Posługujemy się przy tym płaszczyzną z wyróżnionym prostokątnym układem współrzędnych. Prostokątny układ współrzędnych pozwala utożsamiać punkty płaszczyzny z parami uporządkowanymi $\boldsymbol{u} = (a, b)$ liczb rzeczywistych. Zbiór wszystkich takich par, czyli iloczyn kartezjański $\mathbb{R} \times \mathbb{R}$, oznaczany w skrócie $\mathbb{R}^2$ (czytamy: *er kwadrat*), jest grupą względem **dodawania punktów** określonego następująco: jeżeli $\boldsymbol{u} = (a, b)$, $\boldsymbol{w} = (c, d)$, to kładziemy

$$\boldsymbol{u} + \boldsymbol{w} := (a + c, b + d). \tag{8.6}$$

[Oczywiście tak określone działanie jest łączne, przemienne, ma element neutralny $\mathbf{0} = (0, 0)$ i każdy punkt $\boldsymbol{w} = (a, b)$ ma **element przeciwny** $-\boldsymbol{w} := (-a, -b)$.] Czytelnik, oczywiście, wie, że geometrycznie oznacza to, że punkty $\mathbf{0}$, $\boldsymbol{u}$, $\boldsymbol{u} + \boldsymbol{w}$, $\boldsymbol{w}$ są kolejnymi wierzchołkami równoległoboku. Punkty można też mnożyć przez liczby. **Iloczyn** punktu $\boldsymbol{v} = (a, b)$ przez liczbę s jest punktem $s\boldsymbol{v} := (sa, sb)$. Odległość punktu $\boldsymbol{v}$ od zera $\mathbf{0}$ oznaczać będziemy $\|\boldsymbol{v}\|$. Ponieważ przeciwległe boki równoległoboku są równej długości, więc odległość punktów $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ równa jest odległości punktu $\boldsymbol{v}_1 - \boldsymbol{v}_2$ od $\mathbf{0}$, czyli $\|\boldsymbol{v}_1 - \boldsymbol{v}_2\|$. **Nierówność trójkąta** ma przy tych oznaczeniach postać $\|\boldsymbol{v}_1 - \boldsymbol{v}_3\| \leqslant \|\boldsymbol{v}_1 - \boldsymbol{v}_2\| + \|\boldsymbol{v}_2 - \boldsymbol{v}_3\|$, zobacz $\mathbb{GEO}$.

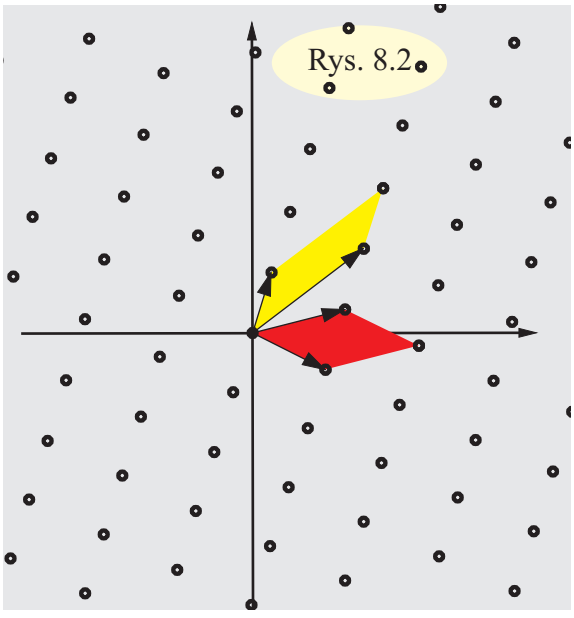
8.3.1 Kraty w płaszczyźnie

Spotykaliśmy już parokrotnie zbiór punktów kratowych, czyli punktów o obu współrzędnych całkowitych. Zbiór ten nazywamy też **kratą Gaussa**. Uogólnieniem tego pojęcia jest pojęcie kraty w płaszczyźnie.

Definicja 8.2 Niech dane będą dwa punkty $\boldsymbol{u}$, $\boldsymbol{w}$ nie leżące na jednej prostej przechodzącej przez początek układu. Wówczas zbiór wszystkich **kombinacji liniowych** postaci

$$k\boldsymbol{u} + l\boldsymbol{w},$$

gdzie $k, l \in \mathbb{Z}$, nazywa się **kratą** generowaną przez punkty $\boldsymbol{u}$, $\boldsymbol{w}$. Oznaczamy ją $\Lambda(\boldsymbol{u}, \boldsymbol{w})$.



Ćwiczenie 8.5 Narysować kratę generowaną przez punkty $(1, 3)$ i $(-2, 4)$.

Szczególnie ładną jest **krata Eisensteina** generowana przez punkty $(1, 0)$ i $(\frac{1}{2}, \frac{\sqrt{3}}{2})$, zobacz rysunek 10.5.

Ćwiczenie 8.6 Udowodnić, że $\Lambda(\boldsymbol{u}, \boldsymbol{w}) = \Lambda(\boldsymbol{u}', \boldsymbol{w}')$ wtedy i tylko wtedy, gdy istnieją takie, spełniające warunek $|ad - bc| = 1$, liczby całkowite a, b, c, d, że

$$\boldsymbol{u}' = a\boldsymbol{u} + b\boldsymbol{w},$$
$$\boldsymbol{w}' = c\boldsymbol{u} + d\boldsymbol{w}.$$

Definicja 8.3 Równoległobok o wierzchołkach $\mathbf{0} = (0, 0)$, $\boldsymbol{u}$, $\boldsymbol{w}$ i $\boldsymbol{u}+\boldsymbol{w}$ nazywa się **równoległobokiem podstawowym** kraty $\Lambda(\boldsymbol{u}, \boldsymbol{w})$, a pole tego równoległoboku nazywa się **wyróżnikiem** kraty $\Lambda(\boldsymbol{u}, \boldsymbol{w})$ i oznacza $d(\Lambda)$. Zobacz rysunek 8.2.

Ćwiczenie 8.7 Udowodnić, że takie oznaczenie jest sensowne, to znaczy, że $d(\Lambda)$ nie zależy od wyboru punktów generujących kratę, a tylko od samej kraty Λ.

8.3.2 Dyskretne podgrupy płaszczyzny

Każda krata jest podgrupą płaszczyzny. Pokażemy teraz prostą ale ważną topologiczną charakteryzację krat.

Grupa $(\mathbb{R}^2, +)$ punktów płaszczyzny z dodawaniem zadanym przez (8.6) ma mnóstwo podgrup (zobacz D5.8 w ustępie 5.5.1).

P r z y k ł a d. Zbiór (wszystkich) punktów dowolnej prostej przechodzącej przez $\mathbf{0}$ jest podgrupą w $\mathbb{R}^2$. Zbiór wszystkich **punktów wymiernych**, czyli takich punktów (a, b), że a, b są liczbami wymiernymi, jest podgrupą w $\mathbb{R}^2$. Dowolna krata jest podgrupą w $\mathbb{R}^2$. $\Diamond$

Definicja 8.4 Podgrupę Γ grupy $(\mathbb{R}^2, +)$ nazywamy **podgrupą dyskretną**, gdy istnieje taka liczba $\varepsilon > 0$, że w kole $\mathcal{D}(\mathbf{0}, \varepsilon) := \{\boldsymbol{v} \in \mathbb{R}^2 : \|\boldsymbol{v}\| \leqslant \varepsilon\}$ o środku w $\mathbf{0}$ i promieniu ε nie leży żaden, różny od $\mathbf{0}$, punkt podgrupy Γ. Czyli, gdy $\mathcal{D}(\mathbf{0}, \varepsilon) \cap \Gamma = \{\mathbf{0}\}$.

ZADANIE 8.3 Udowodnić, że krata jest podgrupą dyskretną w $\mathbb{R}^2$.

R o z w i ą z a n i e. Niech $\Lambda = \Lambda(\boldsymbol{u}, \boldsymbol{w})$, gdzie $\boldsymbol{u} = (a, b)$, $\boldsymbol{w} = (c, d)$, będzie daną kratą. I niech $x\boldsymbol{u} + y\boldsymbol{w} = (ax + cy, bx + dy)$ będzie dowolnym punktem kraty Λ. Oznaczmy $A := a^2 + b^2$, $C := c^2 + d^2$ i $B = 2(ac + bd)$. Wówczas:

$$\begin{aligned}\|x\boldsymbol{u} + y\boldsymbol{w}\|^2 &= (ax + cy)^2 + (bx + dy)^2 = (a^2 + b^2)x^2 + 2(ac + bd)xy + (c^2 + d^2)y^2 \\ &= Ax^2 + Bxy + Cy^2 = \frac{(2Ax + By)^2}{4A} + \frac{4AC - B^2}{4A}y^2 \geqslant -\frac{\Delta}{4A}y^2,\end{aligned}$$

gdzie $\Delta := B^2 - 4AC$. Jasne, że tak samo dostaniemy nierówność $\|x\boldsymbol{u} + y\boldsymbol{w}\|^2 \geqslant -(\Delta/4C)x^2$. Dodając te dwie nierówności dostaniemy

$$\|x\boldsymbol{u} + y\boldsymbol{w}\|^2 \geqslant -\frac{\Delta}{8}\left(\frac{x^2}{C} + \frac{y^2}{A}\right).$$

Zauważmy, że $\Delta < 0$. To wynika z nierówności Schwarza $(ac + bd)^2 \leqslant (a^2 + b^2)(c^2 + d^2)$, która staje się równością wtedy i tylko wtedy, gdy $ad - bc = 0$, co oznacza, że punkty $\boldsymbol{u}$, $\boldsymbol{w}$, $\mathbf{0}$ leżą na jednej prostej i zostało wykluczone. Oznaczając $\mu = \max(A, C)$ i $r^2 = -\Delta/(8\mu)$ możemy więc napisać

$$\|x\boldsymbol{u} + y\boldsymbol{w}\|^2 \geqslant -\frac{\Delta}{8}\left(\frac{x^2}{\mu} + \frac{y^2}{\mu}\right) = -\frac{\Delta}{8\mu}(x^2 + y^2) \geqslant r^2(x^2 + y^2) \geqslant r^2,$$

bo $x^2 + y^2 \geqslant 1$ dla wszystkich $x\boldsymbol{u} + y\boldsymbol{w} \neq \mathbf{0}$. Zatem $\mathcal{D}(\mathbf{0}, r/2) \cap \Lambda = \{\mathbf{0}\}$. $\Diamond$

Udowodnimy teraz "prawie" odwrócenie tezy Z8.3:

TWIERDZENIE 8.3 *Jeżeli Γ jest dyskretną podgrupą punktów płaszczyzny, to zachodzi jedna z trzech możliwości:*

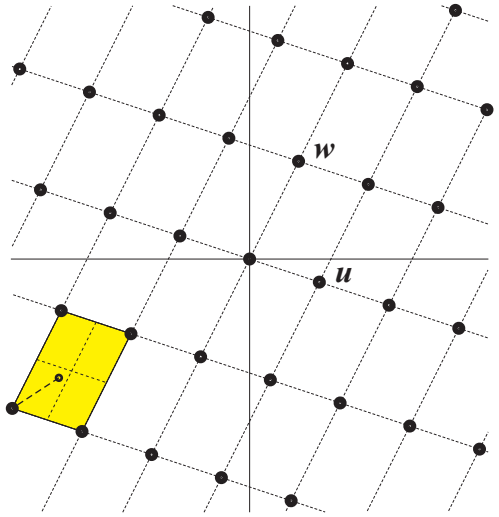
(0) $\Gamma = \{\mathbf{0}\}$,

(1) Γ *jest grupą* $\mathbb{Z}\boldsymbol{u} = \{k\boldsymbol{u} : k \in \mathbb{Z}\}$ *dla pewnego* $\boldsymbol{u} \neq \mathbf{0}$,

(2) Γ *jest kratą.*

DOWÓD. Zauważmy najpierw, że jeżeli $\varepsilon > 0$ jest taką liczbą, że $\mathcal{D}(\mathbf{0}, \varepsilon) \cap \Gamma = \{\mathbf{0}\}$, to $\mathcal{D}(\boldsymbol{v}_1, \varepsilon/3) \cap \mathcal{D}(\boldsymbol{v}_2, \varepsilon/3) = \varnothing$ dla dowolnych dwóch różnych punktów $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \Gamma$. Istotnie, gdyby $\boldsymbol{v} \in \mathcal{D}(\boldsymbol{v}_1, \varepsilon/3) \cap \mathcal{D}(\boldsymbol{v}_2, \varepsilon/3)$, to $\|\boldsymbol{v}_1 - \boldsymbol{v}_2\| = \|\boldsymbol{v}_1 - \boldsymbol{v} + \boldsymbol{v} - \boldsymbol{v}_2\| \leqslant \|\boldsymbol{v}_1 - \boldsymbol{v}\| + \|\boldsymbol{v} - \boldsymbol{v}_2\| \leqslant \varepsilon/3 + \varepsilon/3 < \varepsilon$, więc $\boldsymbol{v}_1 - \boldsymbol{v}_2 = \mathbf{0}$.

Załóżmy teraz, że $\Gamma \neq \{\mathbf{0}\}$. Wówczas możemy wybrać niezerowy punkt $\boldsymbol{u} \in \Gamma$ leżący najbliżej punktu $\mathbf{0}$. Możliwość takiego wyboru jest intuicyjnie oczywista. [Dowód można przeprowadzić tak: Wybieramy dowolny niezerowy punkt $\boldsymbol{u}_0 \in \Gamma$. Niech $\|\boldsymbol{u}_0\| = r_0 > 0$. Jeżeli nie ma punktów w Γ leżących bliżej $\mathbf{0}$, to kładziemy $\boldsymbol{u} = \boldsymbol{u}_0$. Jeżeli zaś w grupie Γ istnieją niezerowe punkty leżące bliżej $\mathbf{0}$, to wybieramy dowolny z nich. Niech to będzie $\boldsymbol{u}_1$. Niech $\|\boldsymbol{u}_1\| = r_1$. Oczywiście $r_1 < r_0$. Jeżeli $\boldsymbol{u}_1$ nie jest najbliższy $\mathbf{0}$, to znajdujemy $\boldsymbol{u}_2$ jeszcze bliższy $\mathbf{0}$ i tak dalej. Po n takich wyborach mamy punkty $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$. Wszystkie one leżą w kole $\mathcal{D}(\mathbf{0}, r_0)$ i to tak, że koła $\mathcal{D}(\boldsymbol{u}_j, \varepsilon/3)$ są (zgodnie z uwagą uczynioną na początku) parami rozłączne i wszystkie zawarte w kole $\mathcal{D}(\mathbf{0}, r_0 + \varepsilon/3)$. Wobec tego suma pól tych kół, czyli liczba $n\pi\varepsilon^2/9$ jest mniejsza niż pole koła $\mathcal{D}(\mathbf{0}, r_0 + \varepsilon/3)$, czyli liczba $\pi(r_0 + \varepsilon/3)^2$. Jasne, że wobec tego n nie może być zbyt duża. Zatem możliwych jest tylko skończenie wiele wyborów punktów $\boldsymbol{u}_j$.] Mając punkt $\boldsymbol{u}$ rozważmy zbiór



Rys. 8.3

$$\mathbb{Z}\boldsymbol{u} := \{k\boldsymbol{u} : k \in \mathbb{Z}\} = \{\ldots, -2\boldsymbol{u}, -\boldsymbol{u}, \mathbf{0}, \boldsymbol{u}, 2\boldsymbol{u}, \ldots\} \tag{8.7}$$

wszystkich jego całkowitoliczbowych wielokrotności. Tworzą one grupę, której wszystkie elementy leżą na jednej prostej, mianowicie na prostej $\mathbb{R}\boldsymbol{u} = \{a\boldsymbol{u} : a \in \mathbb{R}\}$. Czytelnik sam uzasadni, że $\Gamma \cap \mathbb{R}\boldsymbol{u} = \mathbb{Z}\boldsymbol{u}$.

Zachodzi jeden z dwóch przypadków: albo $\mathbb{Z}\boldsymbol{u} = \Gamma$, albo $\mathbb{Z}\boldsymbol{u} \neq \Gamma$. Pierwszy przypadek daje **(1)**. W drugim przypadku wybierzmy ze zbioru $\Gamma \setminus \mathbb{R}\boldsymbol{u}$ punkt najbliższy $\mathbf{0}$. Niech to będzie $\boldsymbol{w}$. Twierdzimy, że $\Lambda(\boldsymbol{u}, \boldsymbol{w}) = \Gamma$. Zawieranie $\Lambda(\boldsymbol{u}, \boldsymbol{w}) \subseteq \Gamma$ jest oczywiste (bo Γ jest grupą, więc zawiera wszystkie kombinacje liniowe $k\boldsymbol{u} + l\boldsymbol{w}$ dla $k, l \in \mathbb{Z}$). Wykażemy więc, że każdy punkt $\boldsymbol{v} \in \Gamma$ należy do $\Lambda(\boldsymbol{u}, \boldsymbol{w})$. Aby to zobaczyć narysujmy rodzinę prostych równoległych do prostej $\mathbf{0}\boldsymbol{w}$ przechodzących przez wszystkie punkty $x\boldsymbol{u}$, $x \in \mathbb{Z}$ i rodzinę prostych równoległych do prostej $\mathbf{0}\boldsymbol{u}$ przechodzących przez wszystkie punkty $y\boldsymbol{w}$, $y \in \mathbb{Z}$. Proste te tworzą rodzinę równoległoboków, których wierzchołkami są punkty kraty $\Lambda(\boldsymbol{u}, \boldsymbol{w})$, zobacz rysunek 8.3. Gdyby teraz pewien punkt $\boldsymbol{v} \in \Gamma$ nie należał do $\Lambda(\boldsymbol{u}, \boldsymbol{w})$, to leżałby w pewnym ze wskazanych równoległoboków. Jeżeli leży w ćwiartce tego równoległoboku wyznaczonej przez wierzchołek $k\boldsymbol{u} + l\boldsymbol{w}$ (jak na rysunku), to, jak łatwo widać z nierówności trójkąta,

$\|\boldsymbol{v} - (k\boldsymbol{u} + l\boldsymbol{w})\| < \frac{1}{2}\|\boldsymbol{u}\| + \frac{1}{2}\|\boldsymbol{w}\| \leqslant \|\boldsymbol{w}\|$. Ale to jest niemożliwe, bo punkt $\boldsymbol{w}$ był wybrany najbliżej punktu $\mathbf{0}$. Wobec tego $\Gamma = \Lambda(\boldsymbol{u}, \boldsymbol{w})$. □

8.3.3 Twierdzenie Minkowskiego o figurze wypukłej

Udowodnimy bardzo ładne i bardzo przydatne twierdzenie Minkowskiego.

Mówimy, że dana figura na płaszczyźnie jest **centralnie symetryczna**, gdy punkt zerowy (czyli początek układu) jest środkiem symetrii tej figury. Przypomnijmy, że figurę nazywamy **wypukłą**, gdy wraz z dowolnymi dwoma punktami zawiera c a ł y o d c i n e k łączący te punkty.

TWIERDZENIE 8.4 (***Twierdzenie Minkowskiego o figurze wypukłej***) *Niech dana będzie krata $\Lambda(\boldsymbol{u}, \boldsymbol{w})$ i centralnie symetryczna, ograniczona figura wypukła $\mathcal{F}$, której pole $S(\mathcal{F})$ spełnia warunek*

$$S(\mathcal{F}) > 4d(\Lambda). \tag{8.8}$$

Wówczas pewien, różny od zerowego, punkt kraty $\Lambda(\boldsymbol{u}, \boldsymbol{w})$ należy do figury $\mathcal{F}$.

D O W Ó D. Niech $\mathcal{G}$ oznacza obraz figury $\mathcal{F}$ przy jednokładności o środku w początku układu i skali $1/2$. Jasne, że $\mathcal{G}$ jest również figurą wypukłą i centralnie symetryczną. Pole $S(\mathcal{G})$, jako równe $S(\mathcal{F})/2^2$, pełnia warunek $S(\mathcal{G}) > d(\Lambda)$. Niech $S(\mathcal{G}) = d(\Lambda) + \varepsilon$, gdzie $\varepsilon > 0$. Oznaczmy przez $\mathcal{H}_{\boldsymbol{x}}$ obraz dowolnego zbioru $\mathcal{H}$ przy translacji o wektor $\boldsymbol{x} \in \Lambda$. Wówczas $S(\mathcal{H}_{\boldsymbol{x}}) = S(\mathcal{H})$, bo przesuwanie nie zmienia pola. Oznaczmy przez k taką liczbę naturalną, że

$$\mathcal{G} \subseteq \bigcup_{|a|,\,|b| \leqslant k} \mathcal{R}_{a\boldsymbol{u}+b\boldsymbol{w}}, \tag{8.9}$$

gdzie $\mathcal{R}_{a\boldsymbol{u}+b\boldsymbol{w}}$ oznacza przesunięcie równoległoboku podstawowego $\mathcal{R}$ kraty Λ o wektor wodzący punktu $a\boldsymbol{u} + b\boldsymbol{w}$. Istnienie takiej liczby k wynika z ograniczoności figury $\mathcal{G}$.

Z inkluzji (8.9) wynika, że dla dowolnego $N \in \mathbb{N}$ zachodzi

$$\bigcup_{|a|,\,|b| \leqslant N} \mathcal{G}_{a\boldsymbol{u}+b\boldsymbol{w}} \subseteq \bigcup_{|a|,\,|b| \leqslant N+k} \mathcal{R}_{a\boldsymbol{u}+b\boldsymbol{w}}. \tag{8.10}$$

Twierdzimy, że zbiory $\mathcal{G}_{\boldsymbol{x}}$ dla różnych $\boldsymbol{x} \in \Lambda$ n i e m o g ą być parami rozłączne. Rzeczywiście, gdyby były parami rozłączne, to, dzięki (8.10), mielibyśmy

$$(2N+1)^2(d(\Lambda) + \varepsilon) = (2N+1)^2 S(\mathcal{G}) \leqslant (2N+2k+1)^2 S(\mathcal{R}) = (2N+2k+1)^2 d(\Lambda).$$

Taka nierówność nie może jednak zachodzić dla wszystkich N. Wynika z niej bowiem, że

$$\varepsilon \leqslant \frac{4k^2 d(\Lambda)}{(2N+1)^2} + \frac{4kd(\Lambda)}{2N+1},$$

co nie może zachodzić dla wszystkich N, bo $\varepsilon > 0$. Wobec tego istnieją takie dwa różne punkty $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$, że

$$\mathcal{G}_{\boldsymbol{x}} \cap \mathcal{G}_{\boldsymbol{y}} \neq \varnothing.$$

Czyli istnieją takie punkty $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{G}$, że $\boldsymbol{x} + \boldsymbol{a} = \boldsymbol{y} + \boldsymbol{b}$. Stąd

$$\boldsymbol{x} - \boldsymbol{y} = 2 \cdot \left(\frac{1}{2}\boldsymbol{b} + \frac{1}{2}(-\boldsymbol{a}) \right).$$

Ale $-\boldsymbol{a} \in \mathcal{G}$, bo $\mathcal{G}$ jest centralnie symetryczny. Zatem wektor $\boldsymbol{z} = \frac{1}{2}(\boldsymbol{b} + (-\boldsymbol{a}))$, jako środek odcinka łączącego punkty $\boldsymbol{b}$ i $-\boldsymbol{a}$ wypukłego zbioru $\mathcal{G}$, należy do $\mathcal{G}$. Czyli $2\boldsymbol{z} \in \mathcal{F}$. Ostatecznie, niezerowy wektor $\boldsymbol{x} - \boldsymbol{y}$ kraty Λ należy do $\mathcal{F}$. □

U w a g a 1. Jeżeli niezerowy punkt $\boldsymbol{u}$ kraty Λ należy do $\mathcal{F}$, to symetryczny względem początku układu punkt $-\boldsymbol{u}$ kraty Λ również należy do $\mathcal{F}$. Widzimy więc, że przy założeniach twierdzenia, co najmniej d w a n i e z e r o w e punkty należą do $\Lambda \cap \mathcal{F}$.

U w a g a 2. Twierdzenie Minkowskiego spotykamy też w $\mathbb{KOM}$. Tam pokazujemy nieco inny dowód nieco innej wersji twierdzenia. Po pierwsze robimy to tam w przestrzeni n-wymiarowej (w miejscu liczby 4 z nierówności (8.8) występuje tam liczba 2^n). Po drugie nierówność jest "tępa", ale za to trzeba dołożyć założenie d o m k n i ę t o ś c i figury (bryły) $\mathcal{F}$ (jest ono ważne: na przykład zbiór $\{(x, y) : |x|, |y| < 1\}$, kwadrat, ma pole 4 i nie zawiera żadnego niezerowego punktu kraty Gaussa). Po trzecie tam ograniczyliśmy się do kraty całkowitoliczbowej (chociaż to założenie łatwo odrzucić).

8.3.4 Dwa zastosowania

Pokażemy teraz dwa zastosowania twierdzenia Minkowskiego o figurze wypukłej.

TWIERDZENIE 8.5 (***Twierdzenie Thue'go***) *Jeżeli $m \geqslant 2$ jest liczbą naturalną i liczba całkowita a jest względnie pierwsza z m, to istnieją r ó ż n e o d z e r a liczby całkowite x, y spełniające warunki:*

$$x \equiv ay \,(\mathrm{mod}\, m), \qquad \textit{oraz} \qquad |x|,\, |y| \leqslant \sqrt{m}.$$

D O W Ó D. Pokażemy dwa sposoby rozumowania. Pierwszy jest całkowicie elementarny, drugi wykorzystuje twierdzenie Minkowskiego. W rzeczywistości te dowody nie różnią się niczym istotnym i drugi można uznać za ilustrację geometryczną pierwszego.

S p o s ó b 1. Niech $A = \lfloor \sqrt{m} \rfloor$. Rozważmy dowolnie ustawione w ciąg liczby $x + ay$, gdzie x i y przebiegają zbiór $\{0, 1, \ldots, A\}$. Ponieważ w tym ciągu jest $(A+1)^2$ wyrazów, a $(A+1)^2 > m$, to możemy wybrać dwa r ó ż n e wyrazy dające tę samą resztę z dzielenia przez m. Niech to będą $x_1 + ay_1$ i $x_2 + ay_2$. Wówczas,

$$(x_1 - x_2) + a(y_1 - y_2) \equiv 0 \,(\mathrm{mod}\, m). \tag{8.11}$$

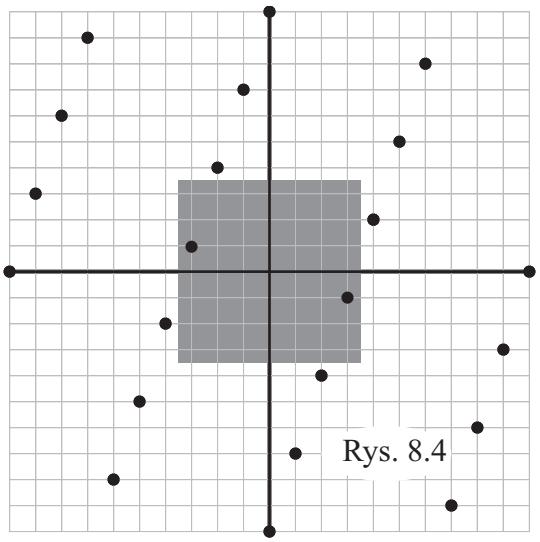
Ponieważ $0 \leqslant x_1, x_2 \leqslant A$, więc $|x_1 - x_2| \leqslant A \leqslant \sqrt{m}$. Podobnie, $|y_1 - y_2| \leqslant \sqrt{m}$. Kładziemy $x = x_1 - x_2$, $y = y_2 - y_1$. Pozostaje nam sprawdzić, że $x \neq 0$ i $y \neq 0$. Otóż, gdyby $y = 0$, to, wobec (8.11), mielibyśmy $m | x_1 - x_2$. Jednocześnie $|x_1 - x_2| \leqslant \sqrt{m} < m$. Stąd $x_1 - x_2 = 0$, więc $(x_1, y_1) = (x_2, y_2)$ wbrew dokonanemu wyborowi różnych wyrazów ciągu. Gdyby zaś $x_1 = x_2$, to kongruencja (8.11) dałaby $m | a(y_1 - y_2)$. W takim przypadku założona względna pierwszość m i a oraz ZTA dają podzielność $m | y_1 - y_2$, która, tak jak przed chwilką, prowadzi do równości $y_1 = y_2$. Uzyskane sprzeczności dowodzą, że $x \neq 0$ i $y \neq 0$. □

S p o s ó b 2. Rozważmy kratę Λ generowaną przez punkty $\boldsymbol{u} = (a, 1)$ i $\boldsymbol{w} = (m, 0)$. Jasne, że $d(\Lambda) = m$. Niech $\mathcal{F}$ będzie zbiorem wypukłym i centralnie symetrycznym (kwadratem!):

$$\mathcal{F} = \{(x, y) : |x|, |y| \leqslant \sqrt{m}\}.$$

(Przypadek gdy $m = 10$, $a = 13$ widzimy na rysunku 8.4.) Wówczas

$$\mu(\mathcal{F}) = (2\sqrt{m})^2 = 4m \geqslant 4d(\Lambda).$$


Rys. 8.4

Stosując twierdzenie Minkowskiego widzimy, że istnieją takie, nie równe jednocześnie 0, liczby całkowite k, l, że punkt $\boldsymbol{q} = k\boldsymbol{u} + l\boldsymbol{w} = (ka + lm, k)$ jest niezerowym punktem należącym do kwadratu $\mathcal{F}$. Sprawdzamy, że współrzędne $x = ka + lm$ i $y = k$ punktu $\boldsymbol{q}$ s p e ł n i a j ą w y m a g a n i a postawione w tezie. Kongruencja $x \equiv ay \,(\mathrm{mod}\, m)$ jest oczywista. Nierówności $|x|, |y| \leqslant \sqrt{m}$ również są jasne, bo $\boldsymbol{q} \in \mathcal{F}$. Pozostaje wykazać, że $x \neq 0$ i $y \neq 0$. Gdyby $y = k = 0$, to $\boldsymbol{q} = (lm, 0)$ byłby punktem kwadratu $\mathcal{F}$, więc $|lm| \leqslant \sqrt{m}$, co jest możliwe tylko dla $l = 0$, bo $m \geqslant 2$. Wtedy punkt $\boldsymbol{q}$ byłby punktem zerowym, wbrew wyborowi. Gdyby zaś $x = 0$, to $ka = -lm$, skąd, patrz ZTA, $m|k$, co dałoby $|y| = |k| \geqslant m$, co znowu jest niemożliwe. □

A oto dowód twierdzenia Fermat'*a*-Eulera, tym razem za pomocą twierdzenia Thue'*go*:

T R Z E C I D O W Ó D TFE. Załóżmy, że -1 jest resztą kwadratową modulo m, gdzie $m \geqslant 2$ jest d o w o l n ą liczbą naturalną nie będącą kwadratem. Mamy więc

$$a^2 \equiv -1 \,(\mathrm{mod}\, m) \tag{8.12}$$

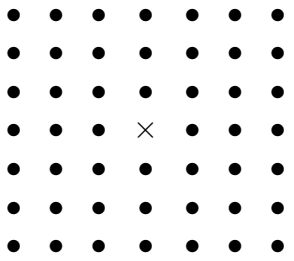
dla pewnego $a \in \mathbb{Z}$. Jasne, że wtedy $\mathrm{NWD}\,(a, m) = 1$. Wybierzmy takie x i y jak w tezie twierdzenia Thue'*go*. Wówczas, po pierwsze:

$$x^2 + y^2 \equiv x^2 - a^2y^2 = (x - ay)(x + ay) \equiv 0 \cdot (x + ay) \equiv 0 \,(\mathrm{mod}\, m).$$

A po drugie $0 < x^2 + y^2 < (\sqrt{m})^2 + (\sqrt{m})^2 = 2m$. Druga nierówność jest też ostra, bo $\sqrt{m}$ n i e j e s t liczbą całkowitą. Zatem $x^2 + y^2$ jest mniejszą niż $2m$ i niezerową wielokrotnością m. Stąd $x^2 + y^2 = m$. Wiemy dobrze, że jeżeli $m = p \equiv 1 \,(\mathrm{mod}\, 4)$, to założenie (8.12) jest spełnione. Przeto, każda liczba pierwsza $\equiv 1 \,(\mathrm{mod}\, 4)$ jest sumą dwóch kwadratów. □

Zabawnym zastosowaniem twierdzenia Minkowskiego jest dowód ***twierdzenia o partyzantach***, które jest tezą poniższego zadania:

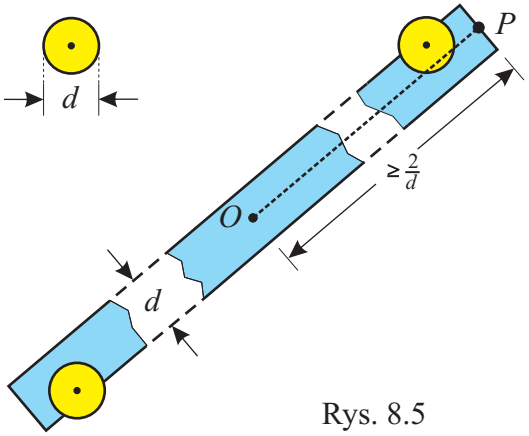
ZADANIE 8.4 Na rysunku obok widzimy plan fragmentu lasu. Tworzące "kratę" kółka to drzewa . Ich pnie mają taką samą średnicę d. Odległość między środkami najbliższych drzew wynosi 1. W punkcie oznaczonym krzyżykiem znajduje się obserwator. Udowodnić, że nie może on dostrzec partyzanta znajdującego się w odległości większej lub równej $2/d$.



Rozwiązanie. Oznaczmy przez O punkt, w którym znajduje się obserwator. Nasze zadanie sprowadza się do wykazania, że jeżeli P jest takim punktem płaszczyzny lasu, że $|OP| \geqslant 2/d$, to odcinek $\overline{OP}$ "zahacza" o pewne drzewo. Aby zobaczyć, że to rzeczywiście zachodzi rozważmy prostokąt $\mathcal{R}$ o szerokości d, długości $2|OP|$, środku w punkcie O i dłuższym boku równoległym do prostej l_{OP}. Prostokąt $\mathcal{R}$ jest centralnie symetrycznym zbiorem wypukłym o polu spełniającym

$$|\mathcal{R}| = 2|OP| \cdot d \geqslant 4.$$

Na mocy twierdzenia Minkowskiego (i uwagi po nim), co najmniej jedno drzewo ma środek w prostokącie $\mathcal{R}$ leżący z tej samej strony obserwatora co punkt P partyzanta. Zatem, pień tego drzewa "zasłania" punkt P. ◊



Rys. 8.5

8.3.5 Liczby naturalne postaci $x^2 + 2y^2$ i $x^2 + 3y^2$

Scharakteryzujemy teraz liczby naturalne ze zbiorów $\mathcal{W}_{(1,0,2)}$ i $\mathcal{W}_{(1,0,3)}$. Zaczniemy od udowodnionego przez Lagrange'a (znanego już Fermat'owi) następującego twierdzenia:

TWIERDZENIE 8.6 (***Lagrange* – 1775**) *Nieparzysta liczba pierwsza p da się przedstawić w postaci $x^2 + 2y^2$ wtedy i tylko wtedy, gdy $p \equiv 1, 3 \pmod 8$.*

DOWÓD. Ponieważ kwadraty modulo 8 to 0, 1, 4, a podwojone kwadraty to 0, 2, więc jasne, że suma kwadratu i podwojonego kwadratu może dawać resztę 0, 1, 2, 3, 4, 6 nigdy zaś reszty 5, 7. Stąd wynika, że nie tylko liczby pierwsze $\equiv 5, 7 \pmod 8$ ale w ogóle żadne liczby naturalne $\equiv 5, 7 \pmod 8$ nie mogą być sumami kwadratu i podwojonego kwadratu. Pozostaje nam wykazać, że liczby pierwsze $\equiv 1, 3 \pmod 8$ są sumami kwadratu i podwojonego kwadratu. Niech więc $p \equiv 1, 3 \pmod 8$ będzie liczbą pierwszą. To, na mocy (5.83), oznacza, że $(-2)\mathbf{R}p$, czyli że istnieje liczba całkowita a spełniająca kongruencję:

$$a^2 \equiv -2 \pmod p. \tag{8.13}$$

Jasne, że $p \nmid a$. Stosując twierdzenie Thue'go (z $m = p$ i $a = a$), znajdujemy takie niezerowe liczby całkowite x, y, że $x \equiv ay \pmod p$, a ponadto $|x|, |y| < \sqrt{p}$. Wówczas, na mocy (8.13),

$$x^2 + 2y^2 \equiv x^2 - a^2y^2 \equiv (x - ay)(x + ay) \equiv 0 \pmod p,$$

a, ponieważ $|x|$ i $|y|$ są "małe", więc $x^2 + 2y^2 < (\sqrt{p})^2 + 2(\sqrt{p})^2 = 3p$. Zatem $x^2 + 2y^2$ jest dodatnią wielokrotnością liczby p ściśle mniejszą od $3p$, co oznacza, że $x^2 + 2y^2 = p$ lub $2p$. Jeżeli $x^2 + 2y^2 = p$, to dobra nasza. Jeżeli zaś $x^2 + 2y^2 = 2p$, to zachodzi równość $x = 2z$ dla pewnego $z \in \mathbb{Z}$. Skąd $2z^2 + y^2 = p$, i znowu liczba p okazała się być równą sumie kwadratu i podwojonego kwadratu. □

P r z y k ł a d 1. Niektóre z naszych ulubionych liczb pierwszych dają resztę 1 lub 3 przy dzieleniu przez 8. Są więc sumami kwadratu i podwojonego kwadratu:

$$\mathbf{1777} = 25^2 + 2 \cdot 24^2, \qquad \mathbf{1801} = 1^2 + 2 \cdot 30^2, \qquad \mathbf{2011} = 43^2 + 2 \cdot 9^2. \ \Diamond$$

Ćwiczenie 8.8 Udowodnić, że jeżeli $p > 2$ jest taką liczbą pierwszą, że $p|s^2 + 2t^2$ dla pewnych względnie pierwszych liczb całkowitych s, t, to $(-2)\mathbf{R}p$, więc, że $p = x^2 + 2y^2$ dla pewnych względnie pierwszych liczb calkowitych x, y.

Ćwiczenie 8.9 Udowodnić, że przedstawienie liczby pierwszej postaci $8k + 1$ lub $8k + 3$ jako sumy kwadratu i podwojonego kwadratu jest (z dokładnością do znaku) jednoznaczne.

ZADANIE 8.5 Udowodnić, że liczba naturalna n da się przedstawić w postaci $x^2 + 2y^2$ wtedy i tylko wtedy, gdy dla każdej liczby pierwszej $p \equiv 5, 7 \pmod 8$ wykładnik $v_p(n)$ jest liczbą parzystą.

R o z w i ą z a n i e. ($\Longleftarrow$) Przedstawiając liczbę naturalną n w postaci $n = k^2 m$, gdzie m jest iloczynem różnych liczb pierwszych postaci 2, $8k+1$, $8k+3$, i pisząc (dzięki wielokrotnemu zastosowaniu T8.6 i tożsamości (8.1) dla $c = 2$, jest to możliwe) $m = x^2 + 2y^2$ otrzymamy $n = (kx)^2 + 2(ky)^2$.

($\Longrightarrow$) Załóżmy teraz, że

$$n = x^2 + 2y^2 \tag{8.14}$$

jest sumą kwadratu i podwojonego kwadratu i że liczba pierwsza $p \equiv 5, 7 \pmod 8$ dzieli n. Twierdzimy, że wówczas $p|x$ i $p|y$. Gdyby bowiem $p \nmid y$, to oznaczając przez u odwrotność y modulo p mielibyśmy

$$nu^2 = (xu)^2 + 2(yu)^2,$$

skąd $0 \equiv (xu)^2 + 2 \pmod p$ co jest niemożliwe, bo -2 jest nieresztą kwadratową modulo $p \equiv 5, 7 \pmod 8$. Zatem $p|y$. Równość (8.14) pokazuje więc wtedy, że również $p|x$. Stąd $n = x^2 + 2y^2 = (pa)^2 + 2(pb)^2$, więc $p^2|n$. Dokończenie rozumowania jest oczywiste. $\Diamond$

Proponujemy Czytelnikowi, żeby zechciał sprawdzić czy zrozumiał wyżej zaprezentowaną technikę, ćwicząc ją na formie (kwadratowej) $X^2 + 3Y^2$:

Ćwiczenie 8.10 Udowodnić (udowodnione przez Eulera) twierdzenie T8.7.

TWIERDZENIE 8.7 *Liczba pierwsza p da się przedstawić w postaci $x^2 + 3y^2$ wtedy i tylko wtedy, gdy $p \equiv 1, 7 \pmod{12}$.* $\square$

Ćwiczenie 8.11 Udowodnić, że przedstawienie liczby pierwszej $p \equiv 1 \pmod 6$ (czyli $\equiv 1, 7 \pmod{12}$) w postaci sumy kwadratu i potrojonego kwadratu jest, z dokładnością do znaku, j e d n o z n a c z n e.

Ćwiczenie 8.12 Udowodnić, że liczba naturalna n jest postaci $x^2 + 3y^2$ wtedy i tylko wtedy, gdy wykładnik p-adyczny $v_p(n)$ jest liczbą parzystą dla $p = 2$ i dla każdej liczby pierwszej $p \equiv 5, 11 \pmod{12}$.

P r z y k ł a d 2. Niektóre z naszych ulubionych liczb pierwszych dają resztę 1 lub 7 przy dzieleniu przez 12. Są więc sumami kwadratu i potrojonego kwadratu:

$$\mathbf{1777} = 7^2 + 3 \cdot 24^2, \qquad \mathbf{1783} = 14^2 + 3 \cdot 23^2, \qquad \mathbf{1801} = 37^2 + 3 \cdot 12^2.$$

Liczba $7204 = 4 \cdot 1801$ spełnia warunki z ćwiczenia C8.12 i ma następujące dwa przedstawienia w postaci $x^2 + 3y^2$:

$$\mathbf{7204} = 4 \cdot 1801 = 4 \cdot (37^2 + 3 \cdot 12^2) = 74^2 + 3 \cdot 24^2,$$
$$\mathbf{7204} = (1^2 + 3 \cdot 1^2)(37^2 + 3 \cdot 12^2) = (37 - 3 \cdot 12)^2 + 3(12 + 37)^2 = 1^2 + 3 \cdot 49^2.$$

Drugie przedstawienie dostajemy za pomocą tożsamości podstawowej (8.1). ◊

8.3.6 Liczby pierwsze postaci $x^2 + 5y^2$

W tym ustępie powiemy trochę na temat przedstawiania liczb naturalnych w postaci $x^2 + 5y^2$. Sprawa jest bardziej skomplikowana niż w dotychczas rozważanych przypadkach.

Zaczniemy od rozwiązania zadania z finału LIX Olimpiady Matematycznej.

ZADANIE 8.6 Udowodnić, że jeżeli liczba pierwsza $p \equiv 3 \pmod 4$ jest dzielnikiem liczby $s^2 + 5t^2$ przy pewnych względnie pierwszych $s, t \in \mathbb{Z}$, to istnieją takie względnie pierwsze liczby całkowite x, y, że $2p = x^2 + 5y^2$.

R o z w i ą z a n i e. S p o s ó b 1. (Szkic rozwiązania firmowego) Warunek $p|s^2+5t^2$, czyli kongruencja $s^2 \equiv -5t^2 \pmod p$ przy względnie pierwszych s, t, implikuje, że $p \nmid t$. Więc $t \pmod p$ jest odwracalne. Niech u będzie odwrotnością t modulo p. Wtedy $(su)^2 \equiv -5 \pmod p$. To oznacza, że $a = su$ spełnia kongruencję:

$$a^2 \equiv -5 \pmod p. \tag{8.15}$$

Ponieważ $p \nmid a$, więc możemy przywołać twierdzenie Thue'*go*, T8.5, i znaleźć x, $y \in \mathbb{Z} \setminus \{0\}$ spełniające warunki: $x \equiv ay \pmod p$ i $|x|, |y| \leqslant \sqrt{p}$. Wówczas, podobnie jak w trzecim dowodzie TFE i w dowodzie T8.6, sprawdzamy, że

$$x^2 + 5y^2 \equiv x^2 - a^2y^2 \equiv (x - ay)(x + ay) \equiv 0 \pmod p, \tag{8.16}$$

czyli, że $x^2 + 5y^2$ jest niezerową wielokrotnością p. Ponadto, nierówności $|x|, |y| < \sqrt{p}$ dają

$$x^2 + 5y^2 < (\sqrt{p})^2 + 5(\sqrt{p})^2 = 6p. \tag{8.17}$$

Widzimy stąd, że $x^2 + 5y^2 = p$, $2p$, $3p$, $4p$ lub $5p$. W rozwiązaniu firmowym należało w tym miejscu wykluczyć wszystkie możliwości z wyjątkiem $x^2 + 5y^2 = 2p$. Jeżeli wykorzystamy założenie, że $p \equiv 3 \pmod 4$, to odrzucenie możliwości p i $5p$ jest proste. Wystarczy zredukować modulo 4:

$$p \equiv 5p \equiv x^2 + 5y^2 \equiv x^2 + y^2 \equiv 0,\ 1,\ 2 \pmod 4. \tag{8.18}$$

I dostajemy sprzeczność z założeniem, że $p \equiv 3 \pmod 4$. Odrzucenie możliwości $3p$ i $4p$ jest nieco bardziej wymagające. Czytelnik może zechce to zrobić samodzielnie, my tymczasem zaproponujemy sposób trochę bardziej "uczony". $\Diamond$

S p o s ó b 2. Wykorzystamy twierdzenie Minkowskiego T8.4, ze stosownie dobraną e l i p s ą w charakterze figury wypukłej.

Początek rozwiązania jest taki sam jak wyżej. Niech więc a spełnia (8.15). Rozważmy tę samą kratę co w drugim sposobie dowodu twierdzenia Thue'*go* (przy $m = p$): $\Lambda(\boldsymbol{u}, \boldsymbol{w})$, gdzie $\boldsymbol{u} = (a, 1)$, $\boldsymbol{w} = (p, 0)$ (wyróżnik $d(\Lambda)$ tej kraty jest równy p). Wybierzemy natomiast lepszy (dla naszych celów) zbiór wypukły. Mianowicie, niech $\mathcal{F}$ będzie elipsą (pełną):

$$\mathcal{F} = \left\{(x, y) \,:\, x^2 + 5y^2 \leqslant K\right\},$$

gdzie $K = 4\sqrt{5}\,\pi^{-1}p$. Elipsa $\mathcal{F}$ ma półosie $\sqrt{K}$ i $\sqrt{K/5}$, więc jej pole wynosi $\mu(\mathcal{F}) = \pi\sqrt{K}\,\sqrt{K/5} = 4p \geqslant 4d(\Lambda)$. Ponadto, elipsa ta jest zbiorem centralnie symetrycznym, wypukłym i domkniętym (zobacz $\mathbb{GEO}$). Z twierdzenia Minkowskiego wnosimy więc, że zawiera ona niezerowy punkt kraty Λ. Niech to będzie

$$(x, y) = k\boldsymbol{u} + l\boldsymbol{w} = (ka + lp, k).$$

Ponieważ $x \equiv ay \pmod p$, więc tak samo jak w (8.16) widzimy, że $p|x^2 + 5y^2$. Przewaga tego sposobu rozwiązania nad sposobem 1 polega na tym, że możemy znacznie poprawić szacowanie (8.17). Mamy mianowicie

$$x^2 + 5y^2 \leqslant K = 4\sqrt{5}\pi^{-1}\,p,$$

ponieważ punkt (x, y) należy do elipsy $\mathcal{F}$. Stąd, ponieważ $4\sqrt{5}\pi^{-1} \approx 2,8470 < 3$, więc $x^2 + 5y^2 = p$ lub $x^2 + 5y^2 = 2p$. Przypadek $x^2 + 5y^2 = p$ odrzucamy jak wyżej. Względna pierwszość x i y jest oczywista. $\Diamond$

Analizując sposób 2 przedstawionego wyżej rozwiązania udowodnimy:

Twierdzenie 8.8 *Liczba pierwsza $p > 5$ da się przedstawić w postaci $x^2 + 5y^2$ wtedy i tylko wtedy, gdy $p \equiv 1, 9 \pmod{20}$.*

D O W Ó D. Liczby pierwsze $p > 5$ są jednej z ośmiu postaci: $20k \pm 1$, $20k \pm 3$, $20k \pm 7$ lub $20k \pm 9$. [Wiemy z twierdzenia Dirichlet'*a*, że każda z tych postaci jest reprezentowana przez nieskończenie wiele liczb pierwszych.] Jeżeli $p = x^2 + 5y^2$, to $(-5)\mathbf{R}p$, zobacz C8.1. Ale, zobacz (5.87), $(-5)\mathbf{R}p$ wtedy i tylko wtedy, gdy $p \equiv 1, 3, 7, 9 \pmod{20}$. Wobec tego liczby pierwsze $p \equiv 19, 17, 13, 11 \pmod{20}$ n i e są postaci $x^2 + 5y^2$. Również liczby pierwsze $p \equiv 3, 7 \pmod{20}$ n i e są postaci $x^2 + 5y^2$. Łatwo to zobaczyć badając reszty z dzielenia przez 4: $x^2 + 5y^2 \equiv 0, 1, 2 \pmod 4$, zobacz (8.18), a $p \equiv 3, 7 \pmod{20}$ daje resztę 3 modulo 4. Widzimy, że jedynie liczby pierwsze $p \equiv 1, 9 \pmod{20}$ mają szansę na bycie postaci $x^2 + 5y^2$.

Niech $p \equiv 1, 9 \pmod{20}$ będzie taką liczbą pierwszą. W sposobie 2 rozwiązania Z8.6 wykazaliśmy, że istnieją takie liczby x, y, że $x^2 + 5y^2 = p$ lub $x^2 + 5y^2 = 2p$. Badając modulo 8 łatwo widzimy, że $x^2 + 5y^2 \neq 2p$. (Istotnie, jeżeli $p \equiv 1, 9 \pmod{20}$, to $2p \equiv 2 \pmod 8$. Jednocześnie $x^2 + 5y^2 \equiv 0, 1, 4, 5, 6 \pmod 8$. Zatem $x^2 + 5y^2 \not\equiv 2p \pmod 8$, więc tym bardziej $x^2 + 5y^2 \neq 2p$.) Wobec tego $x^2 + 5y^2 = p$. $\square$

P r z y k ł a d 1. Liczby pierwsze 1801 i 1789 dają resztę 1 i 9 modulo 20. Zatem:

$$\mathbf{1801} = 26^2 + 5 \cdot 15^2, \qquad \mathbf{1789} = 13^2 + 5 \cdot 18^2. \ \Diamond$$

Ćwiczenie 8.13 Udowodnić, że przedstawienie liczby pierwszej w postaci $x^2 + cy^2$ (jeżeli istnieje) jest jednoznaczne z dokładnością do znaku. *Wskazówka.* Zobacz Z8.2.

Pierre Fermat przyglądał się liczbom pierwszym $\equiv 3, 7 \pmod{20}$, o których wiemy, że nie są postaci $x^2 + 5y^2$, i zauważył, że *iloczyn każdych dwóch takich liczb jest postaci* $x^2 + 5y^2$. Weźmy na przykład $p = 23$, $q = 47$. Wówczas

$$pq = 19^2 + 5 \cdot 12^2, \quad p^2 = 22^2 + 5 \cdot 3^2, \quad q^2 = 2^2 + 5 \cdot 21^2.$$

ZADANIE 8.7 Uzasadnić spostrzeżenie Fermata.

Rozwiązanie. Z rozwiązania zadania Z8.6 wiemy, że jeżeli $p \equiv 3, 7 \pmod{20}$, to $2p$ da się przedstawić w postaci $x^2 + 5y^2$. Niech więc $p_1, p_2 \equiv 3, 7 \pmod{20}$ i niech $2p_1 = x_1^2 + 5y_1^2$, $2p_2 = x_2^2 + 5y_2^2$. Wówczas, na mocy tożsamości Brahmagupty,

$$4p_1p_2 = (x_1x_2 \pm 5y_1y_2)^2 + 5(x_1y_2 \mp x_2y_1)^2.$$

Zauważmy, że liczby x_1, x_2, y_1, y_2 są nieparzyste(?!) i podzielmy obustronnie przez 4.

Podkreślmy też, że mamy swobodę wyboru znaków w nawiasach. Stąd, obok przedstawienia $23 \cdot 47 = 19^2 + 5 \cdot 12^2$ dostajemy również przedstawienie $23 \cdot 47 = 26^2 + 5 \cdot 9^2$, a obok przedstawienia $23^2 = 22^2 + 5 \cdot 3^2$ przedstawienie trywialne $23^2 = 23^2 + 5 \cdot 0^2$. I podobnie dla 47^2. $\Diamond$

W następnym paragrafie a także w rozdziale 10 rzucimy jeszcze trochę światła na to intrygujące zjawisko. Tymczasem rozwiążmy takie ćwiczenie:

Ćwiczenie 8.14 Niech c będzie dodatnią liczbą całkowitą. Niech też $m \geqslant 2$ oznacza ustalony moduł. Załóżmy, że $(-c)\mathbf{R}m$. (Przypomnijmy, że w tym jest zawarty warunek $\mathrm{NWD}\,(m, c) = 1$, zobacz D5.12). Udowodnić, że wówczas co najmniej jedna z liczb

$$m, 2m, \ldots, \lfloor \mathcal{M}_c \rfloor m$$

da się zapisać w postaci $x^2 + cy^2$ dla całkowitych x, $y \neq 0$. Tu $\mathcal{M}_c = \frac{4}{\pi}\sqrt{c}$.

Liczbę $\mathcal{M}_c$ nazywamy **stałą Minkowskiego** (dla wyróżnika $\Delta = -4c$). Stała $\mathcal{M}_6$ jest równa w przybliżeniu $3,1188$. Możemy to wykorzystać w rozwiązaniu poniższego ćwiczenia:

Ćwiczenie 8.15 Dowieść, że liczba pierwsza p da się przedstawić w postaci $x^2 + 6y^2$ wtedy i tylko wtedy, gdy $p \equiv 1, 7 \pmod{24}$. Udowodnić, że iloczyn dwóch liczb pierwszych p_1, $p_2 \equiv 5, 11 \pmod{24}$ da się przedstawić w postaci $x^2 + 6y^2$.

8.4 Binarne formy kwadratowe

Wielomiany $X^2 + cY^2 \in \mathbb{Z}[X, Y]$, których zbiorami wartości (dla argumentów całkowitych) zajmowaliśmy się dotychczas, są przykładami tak zwanych (binarnych) form kwadratowych. Badanie zbiorów wartości binarnych form kwadratowych jest fascynujące i prowadzi do rozległych dziedzin matematyki, takich jak **algebraiczna teoria liczb** czy **teoria form modularnych**. Nasz cel jest nierównie skromniejszy: przedstawienie dowodu Lagrange'*a* twierdzenia Fermat'*a*-Eulera TFE.

Definicja 8.5 Wielomian dwóch zmiennych o współczynnikach całkowitych

$$f(X,\,Y) = aX^2 + bXY + cY^2 \tag{8.19}$$

nazywamy **binarną formą kwadratową**. Mówimy, że forma $f(X,\,Y)$ **przedstawia** liczbę całkowitą n, gdy istnieją takie liczby całkowite $x,\,y$, że $f(x,\,y) = n$. Gdy, dodatkowo, można znaleźć takie $x,\,y$, że $\mathrm{NWD}\,(x,\,y) = 1$ i $f(x,\,y) = n$, to mówimy, że forma f **właściwie przedstawia** liczbę n. Dla skrócenia zapisu formę $aX^2+bXY+cY^2$ będziemy oznaczać symbolem $(a,\,b,\,c)$. Zbiór liczb, które przedstawia ta forma oznaczamy $\mathcal{W}_{(a,\,b,\,c)} = \mathcal{W}_f$. [*Binarny* oznacza tu: dwóch zmiennych.]

P r z y k ł a d. Dotychczas zajmowaliśmy się formami $(1,\,0,\,c) = X^2+cY^2$. Wiemy, na przykład, że liczby pierwsze $p \equiv 1\,(\mathrm{mod}\,4)$ są w ł a ś c i w i e przedstawiane przez formę $(1,\,0,\,1)$. Ogólniej, jasne jest, że każde przedstawienie liczby pierwszej p przez formę kwadratową jest przedstawieniem w ł a ś c i w y m, bo kwadrat (każdego) wspólnego dzielnika $x,\,y$ jest dzielnikiem p. Również przedstawienie liczby bezkwadratowej jest przedstawieniem właściwym. W przykładzie P2 z ustępu 8.3.5 widzieliśmy, że forma $(1,\,0,\,3)$ przedstawia zarówno właściwie jak i niewłaściwie liczbę 7204. ◊

8.4.1 Wyróżnik formy

Wyróżnik formy kwadratowej zawiera ważne informacje na jej temat.

Definicja 8.6 Liczbę $\Delta = b^2 - 4ac$ nazywamy **wyróżnikiem** formy kwadratowej (8.19).

Jasne, że wyróżnik formy jest liczbą całkowitą spełniającą warunek $\Delta \equiv 0,\,1\,(\mathrm{mod}\,4)$.

ZADANIE 8.8 Udowodnić, że dla dowolnej liczby całkowitej $\Delta \equiv 0,\,1\,(\mathrm{mod}\,4)$ istnieje forma kwadratowa, której wyróżnik równy jest Δ.

R o z w i ą z a n i e. Jeżeli $\Delta \equiv 0\,(\mathrm{mod}\,4)$, to forma $X^2 - \frac{1}{4}\Delta Y^2$ jest oczywiście dobra. Jeżeli zaś $\Delta \equiv 1\,(\mathrm{mod}\,4)$, to oczywiście dobrą jest forma $X^2 + XY + \frac{1}{4}(1-\Delta)Y^2$. ◊

8.4.2 Równoważność form

Wprowadzimy teraz ważne pojęcie równoważności form. Formy równoważne przedstawiają dokładnie te same liczby.

Definicja 8.7 Mówimy, że forma $f(X,\,Y)$ jest **równoważna** formie $g(X,\,Y)$, gdy istnieje taka macierz $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathbf{GL}_2(\mathbb{Z})$ (zobacz 7.3.4), że

$$g(x,\,y) = f(Ax + By,\,Cx + Dy)$$

dla wszystkich $(x,\,y) \in \mathbb{Z} \times \mathbb{Z}$. Piszemy w takim przypadku $f\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = g$. Fakt, że formy f i g są równoważne zapisujemy tak: $f \simeq g$.

P r z y k ł a d 1. Równość $(2x+3y)^2+(x+2y)^2 = 5x^2+16xy+13y^2$ prawdziwa dla wszystkich $(x,\,y) \in \mathbb{Z} \times \mathbb{Z}$ pokazuje, że $(1,\,0,\,1)\left(\begin{smallmatrix} 2 & 3 \\ 1 & 2 \end{smallmatrix}\right) = (5,\,16,\,13)$. ◊

Ćwiczenie 8.16 Udowodnić, że relacja $\simeq$ jest relacją równoważności, zobacz $\mathbb{KOM}$.

Ćwiczenie 8.17 Formy równoważne mają równe wyróżniki. Dowieść. *Wskazówka.* Eleganckie rozwiązanie korzysta z T7.8.

ZADANIE 8.9 Udowodnić, że jeżeli formy $aX^2+bXY+cY^2$ i $a_1X^2+b_1XY+c_1Y^2$ są równoważne, to zbiory $\mathcal{W}_{(a,b,c)}$ i $\mathcal{W}_{(a_1,b_1,c_1)}$ są równe.

R o z w i ą z a n i e. Teza wynika z możliwości "odwrócenia" zależności

$$\begin{cases} x' = Ax + By, \\ y' = Cx + Dy, \end{cases}$$

gdzie $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathbf{GL}_2(\mathbb{Z})$. Istotnie, równości te są równoważne równościom

$$\begin{cases} x = Dwx' - Bwy', \\ y = -Cwx' + Awy', \end{cases}$$

gdzie $w = AD - BC =: \det\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$. $\Diamond$

P r z y k ł a d 2. Zauważmy, że oczywista równość

$$a(x+ry)^2 + b(x+ry)y + cy^2 = ax^2 + (b+2ar)xy + (c+br+ar^2)y^2$$

pokazuje, że forma $(a,\, b,\, c)$ jest równoważna formie ze współczynnikiem środkowym niewiększym co do wartości bezwzględnej niż współczynnik lewy. Wystarczy dobrać taką liczbę całkowitą r, by $|b+2ra| \leqslant |a|$. Na przykład, równość

$$3(x+2y)^2 - 11(x+2y)y + y^2 = 3x^2 + xy - 9y^2$$

pokazuje, że $(3,\, -11,\, 1) \simeq (3,\, 1,\, -9)$, przy czym macierzą realizującą tę równoważność jest $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbb{Z})$. $\Diamond$

Formy równoważne przedstawiają te same liczby. Jednak nie musi być na odwrót:

P r z y k ł a d 3. Uzasadnimy, że $\mathcal{W}_{(1,1,1)} = \mathcal{W}_{(1,0,3)}$ mimo, że $(1,\, 1,\, 1) \not\simeq (1,\, 0,\, 3)$ [bo pierwsza z tych form ma wyróżnik -3, a druga ma wyróżnik -12]. Tymczasem równość

$$x^2 + 3y^2 = (x-y)^2 + (x-y)\cdot 2y + (2y)^2$$

pokazuje, że każda liczba będąca sumą kwadratu i potrojonego kwadratu jest przedstawialna przez formę $(1,\, 1,\, 1)$. Zatem $\mathcal{W}_{(1,0,3)} \subseteq \mathcal{W}_{(1,1,1)}$. Odwrotnie, weźmy liczbę u^2+uv+v^2 przedstawianą przez formę $(1,\, 1,\, 1)$. Wówczas

$$u^2+uv+v^2 = \begin{cases} \left(u+\frac{v}{2}\right)^2 + 3\cdot\left(\frac{v}{2}\right)^2, & \text{gdy } v \equiv 0 \,(\mathrm{mod}\, 2), \\ \left(\frac{u}{2}+v\right)^2 + 3\cdot\left(\frac{u}{2}\right)^2, & \text{gdy } u \equiv 0 \,(\mathrm{mod}\, 2), \\ \left(\frac{u-v}{2}\right)^2 + 3\cdot\left(\frac{u+v}{2}\right)^2, & \text{gdy } u \equiv v \equiv 1 \,(\mathrm{mod}\, 2), \end{cases}$$

co dowodzi zawierania $\mathcal{W}_{(1,1,1)} \subseteq \mathcal{W}_{(1,0,3)}$. $\Diamond$

8.4.3 Lemat Lagrange'*a*

Udowodnimy teraz ważny lemat. Dzięki niemu można rozstrzygać problem przedstawiania liczb całkowitych przez formy kwadratowe danego wyróżnika.

LEMAT 8.3 *Forma $f(X, Y)$ właściwie przedstawia liczbę całkowitą n wtedy i tylko wtedy, gdy istnieje równoważna jej forma postaci $g(X, Y) = nX^2 + kXY + mY^2$.*

D O W Ó D. ($\Longrightarrow$) Załóżmy, że forma $f(X, Y) = aX^2 + bXY + cY^2$ przedstawia właściwie liczbę n. Wówczas istnieją takie względnie pierwsze liczby A i C, że $f(A, C) = n$. Ze względnej pierwszości wynika istnienie takich liczb całkowitych B, D, że $AD - BC = 1$, zobacz T2.6. Wtedy

$$\begin{aligned} f(Ax + By, Cx + Dy) &= a(Ax + By)^2 + b(Ax + By)(Cx + Dy) + c(Cx + Dy)^2 \\ &= (aA^2 + bAC + cC^2)x^2 + \ldots = nx^2 + kxy + my^2 =: g(x, y), \end{aligned}$$

gdzie $k = 2aAB + bBC + bAD + 2cCD$ i $m = f(B, D) = aB^2 + bBD + cD^2$. Zatem $g \simeq f$ i $g(1, 0) = n$, więc forma $g(X, Y)$ właściwie przedstawia liczbę n.

($\Longleftarrow$) Wynikanie w tę stronę jest natychmiastowym wnioskiem z Z8.9. □

Udowodnimy teraz dwa twierdzenia o możliwości przedstawiania liczb całkowitych przez formy kwadratowe.

TWIERDZENIE 8.9 *Jeżeli forma $f(X, Y)$ ma wyróżnik Δ i właściwie przedstawia liczbę n, a d jest dzielnikiem liczby n, to istnieje forma $h(X, Y)$ mająca ten sam wyróżnik Δ, która właściwie przedstawia liczbę d.*

D O W Ó D. Niech $n = de$. Z lematu Z8.3 wiemy, że istnieje forma (n, k, m) równoważna formie $f(X, Y)$. Wówczas $\Delta = k^2 - 4mn = k^2 - 4med$. Zatem forma $h(X, Y) = dX^2 + kXY + meY^2$ ma wyróżnik Δ i właściwie przedstawia liczbę $d = h(1, 0)$. □

TWIERDZENIE 8.10 *Niech $\Delta \equiv 0, 1 \pmod 4$. Wówczas liczba $n \in \mathbb{Z}$ może być właściwie przedstawiona przez p e w n ą formę o wyróżniku Δ wtedy i tylko wtedy, gdy istnieje liczba całkowita k spełniająca*

$$k^2 \equiv \Delta \pmod{4|n|}. \tag{8.20}$$

D O W Ó D. ($\Longrightarrow$) Załóżmy, że $n = ax^2 + bxy + cy^2$ dla pewnych a, b, $c \in \mathbb{Z}$ i pewnych względnie pierwszych x, $y \in \mathbb{Z}$. Wówczas, jak wiemy z lematu L8.3, istnieje forma (n, k, m) równoważna formie (a, b, c). W szczególności, zobacz C8.16, wyróżnik $\Delta = b^2 - 4ac$ równa się wyróżnikowi formy (n, k, m). Zatem $\Delta = k^2 - 4mn$. Więc (8.20) zachodzi.

($\Longleftarrow$) Odwrotnie, jeżeli zachodzi (8.20), czyli zachodzi równość $k^2 - \Delta = 4mn$ dla pewnej liczby całkowitej m, to forma $f(X, Y) = nX^2 + kXY + mY^2$ ma wyróżnik równy Δ i $f(1, 0) = n$. Zatem p e w n a forma o wyróżniku Δ właściwie przedstawia n. □

P r z y k ł a d 2. Rozważmy wyróżnik $\Delta = -4$. Twierdzenie T8.10 mówi, że liczba całkowita n da się właściwie przedstawić przez p e w n ą formę o wyróżniku -4 wtedy i tylko wtedy, gdy istnieje rozwiązanie kongruencji $u^2 \equiv -4 \pmod{4|n|}$. Jasne, że rozwiązanie tej kongruencji jest

liczbą parzystą: $u = 2t$. To prowadzi do badania kongruencji $t^2 \equiv -1 \,(\mathrm{mod}\, |n|)$, czyli do problemu istnienia pierwiastków kongruencji wielomianowej

$$t^2 + 1 \equiv 0 \,(\mathrm{mod}\, |n|). \tag{8.21}$$

Rozłóżmy liczbę naturalną $|n|$ na czynniki pierwsze

$$|n| = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}.$$

Z wniosku WT5.13 wiemy, że kongruencja (8.21) ma rozwiązanie wtedy i tylko wtedy, gdy mają rozwiązania wszystkie kongruencje

$$t^2 + 1 \equiv 0 \,(\mathrm{mod}\, p_i^{e_i}) \tag{8.22}$$

dla każdego $i = 1, 2, \ldots, s$. Jeżeli $p_i > 2$, to kongruencja (8.22) ma rozwiązanie wtedy i tylko wtedy, gdy $p_i \equiv 1 \,(\mathrm{mod}\, 4)$, zobacz T5.30. Zaś kongruencja $t^2 \equiv -1 \,(\mathrm{mod}\, 2^e)$ ma rozwiązanie wtedy i tylko wtedy, gdy $e \leqslant 1$.

Podsumowując, widzimy, że liczba całkowita n da się w ł a ś c i w i e przedstawić przez pewną formę o wyróżniku -4 wtedy i tylko wtedy, gdy $4 \nmid n$ i $v_p(n) = 0$ dla wszystkich liczb pierwszych $p \equiv 3 \,(\mathrm{mod}\, 4)$. W szczególności *każda liczba pierwsza* $p \equiv 1 \,(\mathrm{mod}\, 4)$ *da się przedstawić przez pewną formę o wyróżniku* -4. Pomysł Lagrange'*a* dowodu twierdzenia Fermat'*a*-Eulera polega na wykazaniu, że k a ż d a forma o wyróżniku -4 jest równoważna formie $(1, 0, 1)$ lub formie $(-1, 0, -1)$. Zobaczymy to w następnym ustępie. ◊

Ćwiczenie 8.18 Scharakteryzować te liczby całkowite, które można właściwie przedstawić przez pewną formę o wyróżniku -3 i te liczby całkowite, które można przedstawić przez pewną formę o wyróżniku -12. Jakie stąd płyną wnioski?

Ćwiczenie 8.19 Scharakteryzować wszystkie liczby całkowite, które dadzą się przedstawić przez pewną formę o wyróżniku 8.

8.4.4 Redukcja form dodatnio-określonych

Formy kwadratowe (8.19) dzielą się na dwa typy: formy o wyróżniku d o d a t n i m, są to tak zwane **formy nieokreślone** i formy o wyróżniku u j e m n y m, są to tak zwane **formy określone**. Dla uproszczenia ograniczymy się tu do form określonych. Dla danej formy dodatnio-określonej będziemy poszukiwać – wśród form jej równoważnych – formy najprostszej.

Definicja 8.8 Forma kwadratowa przyjmująca wyłącznie w a r t o ś c i n i e u j e m n e, przy czym wartość 0 tylko dla $(x, y) = (0, 0)$, nazywa się formą **dodatnio-określoną**.

ZADANIE 8.10 Udowodnić, że forma $f(X, Y) = aX^2 + bXY + cY^2$ jest dodatnio-określona wtedy i tylko wtedy, gdy $a, c > 0$ i $\Delta < 0$.

R o z w i ą z a n i e. To wynika z oczywistej tożsamości

$$4af(x, y) = (2ax + by)^2 - \Delta y^2, \tag{8.23}$$

czyli z postaci kanonicznej trójmianu kwadratowego, patrz ustęp 3.2.5. ◊

TWIERDZENIE 8.11 *Jeżeli* (a, b, c) *jest formą dodatnio-określoną, to istnieje równoważna jej forma* (a_0, b_0, c_0) *spełniająca warunki*

$$|b_0| \leqslant a_0 \leqslant c_0, \tag{8.24}$$

przy czym, jeżeli $a_0 = c_0$, *to można wybrać* b_0 *nieujemne.*

D O W Ó D. Dla dowodu podamy algorytm pozwalający w skończonej liczbie kroków z r e d u k o w a ć daną formę do postaci spełniającej (8.24). Algorytm ten polega na kolejnym wykonywaniu jednej z następujących procedur:

(1) Jeżeli $c < a$, to zamieniamy formę (a, b, c) na równoważną jej formę $(c, -b, a)$,

(2) Jeżeli $|b| > a$, to zamieniamy formę (a, b, c) na równoważną jej formę (a, b_1, c_1), gdzie $b_1 = b + 2ra$ i $r \in \mathbb{Z}$ jest tak wybrane, żeby $|b_1| \leqslant a$. Przy tym c_1 wyznaczamy z równości $b_1^2 - 4ac_1 = \Delta$.

Macierz $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ realizująca równoważność w procedurze **(1)** jest równa $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ (macierz zamiany (X, Y) na $(-Y, X)$). W procedurze **(2)** używamy macierzy $\left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right)$. Widzimy, że używamy wyłącznie macierzy $\mathbf{S}$ i $\mathbf{T}$ zdefiniowanych w (7.20), bo $\left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right) = \mathbf{T}^r$. □

P r z y k ł a d. Weźmy formę $(10, 34, 29)$ o wyróżniku -4. Tu $b > a$. Stosując procedurę **(2)**, znajdujemy b_1 z przedziału $[-10; 10]$. W tym celu odejmujemy od b odpowiednią wielokrotność 20, w tym przypadku 40. Po tym otrzymujemy formę $(10, -6, c_1)$, gdzie c_1 spełnia warunek $-4 = (-6)^2 - 4 \cdot 10 c_1$, więc $c_1 = 1$. Mamy więc równoważną formę $(10, -6, 1)$. Stosujemy teraz procedurę **(1)**. Dostajemy formę $(1, 6, 10)$. Stosujemy ponownie procedurę **(2)**. Dostaniemy formę $(1, 0, c_2)$, gdzie c_2, wyliczone z równości $-4 = 0^2 - 4 \cdot 1 \cdot c_2$, jest równe 1. Widzimy więc, że $10X^2 + 34XY + 29Y^2 \simeq X^2 + Y^2$. ◊

Dodatnio-określoną formę spełniającą warunki (8.24) nazywa się formą **zredukowaną**.

To, że forma $(10, 34, 29)$ o wyróżniku -4 jest równoważna formie $(1, 0, 1)$ nie jest niczym dziwnym, bowiem:

ZADANIE 8.11 Udowodnić, że wszystkie dodatnio-określone formy o wyróżniku -4 są równoważne formie $(1, 0, 1) = X^2 + Y^2$.

R o z w i ą z a n i e. Niech (a_0, b_0, c_0) będzie zredukowaną formą dodatnio-określoną o wyróżniku -4. Wtedy $b_0^2 = 4a_0c_0 - 4 \geqslant 4b_0^2 - 4$. Stąd $|b_0| \leqslant \sqrt{4/3}$, czyli $|b_0| \leqslant 1$. Ale b_0 jest parzyste. Więc $b_0 = 0$. Wobec tego $4a_0c_0 = 4$, czyli $a_0 = c_0 = 1$. ◊

Dzięki temu możemy udowodnić twierdzenie Fermat'*a*-Eulera m e t o d ą L a g r a n g e' *a*:

C Z W A R T Y D O W Ó D TFE. Jeżeli $p \equiv 1 \pmod 4$, to, jak wiemy, zobacz dowód lematu L8.2 z ustępu 8.2.2 lub I uzupełnienie prawa wzajemności, kongruencja $u^2 \equiv -4 \pmod{4p}$ ma rozwiązania. Wobec tego, zobacz T8.10, p e w n a forma $f(X, Y)$ o wyróżniku -4 przedstawia liczbę p. Ale $f(X, Y) \simeq X^2 + Y^2$, więc i $X^2 + Y^2$ przedstawia p, zobacz Z8.9. □

Ćwiczenie 8.20 Udowodnić podobnie twierdzenie T8.2. Zob. 8.4.3 P2.

Tabelka dodatnio-określonych form zredukowanych dla małych $|\Delta|$

Δ	Wszystkie zredukowane dodatnio-określone formy o wyróżniku Δ	$h(\Delta)$
-3	X^2+XY+Y^2	1
-4	X^2+Y^2	1
-7	$X^2+XY+2Y^2$	1
-8	X^2+2Y^2	1
-11	$X^2+XY+3Y^2$	1
-12	X^2+3Y^2	1
-15	$X^2+XY+4Y^2, \quad 2X^2+XY+2Y^2$	2
-19	$X^2+XY+5Y^2$	1
-20	$X^2+5Y^2, \quad 2X^2+2XY+3Y^2$	2
-23	$X^2+XY+6Y^2, \quad 2X^2-XY+3Y^2, \quad 2X^2+XY+3Y^2$	3

Ćwiczenie 8.21 Udowodnić, że w powyższej tabelce jest wszystko w porządku.

Ćwiczenie 8.22 Wyznaczyć rozwiązania równania $57x^2+144xy+91y^2=1801$ w liczbach całkowitych, zobacz P2 z ustępu 8.3.5.

Ćwiczenie 8.23 Udowodnić, że jeżeli nieparzysta liczba pierwsza p jest dzielnikiem liczby a^2+3, to forma X^2+XY+Y^2 przedstawia liczbę p.

Ćwiczenie 8.24 Dowieść, że jeżeli -7 jest resztą kwadratową modulo $p \equiv 1 \pmod 2$, to równanie $x^2+xy+2y^2=p$ ma rozwiązania w liczbach całkowitych.

ZADANIE 8.12 Rozwiązać jeszcze raz zadanie Z8.6.

Rozwiązanie. Jeżeli liczba pierwsza p jest dzielnikiem liczby s^2+5t^2 przy pewnych względnie pierwszych s, t, to istnieje a spełniające $a^2 \equiv -5 \pmod p$. Wówczas $2a$ jest rozwiązaniem kongruencji $u^2 \equiv -20 \pmod{4p}$. Zatem, na mocy T8.10, liczba p może być właściwie przedstawiona przez pewną formę o wyróżniku -20. Czyli (zobacz tabelkę) przez formę X^2+5Y^2 lub przez formę $2X^2+2XY+3Y^2$. Ponieważ forma X^2+5Y^2 nie przedstawia liczb pierwszych $p \equiv 3 \pmod 4$ (co pokazuje redukcja modulo 4), więc "robi" to forma $2X^2+2XY+3Y^2$. Istnieją więc względnie pierwsze $x, y \in \mathbb{Z}$, dla których $2x^2+2xy+3y^2=p$. Wówczas $(2x+y)^2+5y^2=2p$. $\Diamond$

8.5 Sumy więcej niż dwóch kwadratów

Powiemy tu co nieco na temat przedstawiania liczb naturalnych w postaci sumy trzech lub czterech kwadratów. Zaczniemy od wyniku pozytywnego.

8.5.1 Twierdzenie o sumach czterech kwadratów

Pokażemy teraz dowód twierdzenia Lagrange'*a* mówiącego, że każda liczba naturalna d a s i ę (niejednoznacznie!) przedstawić w postaci sumy czterech kwadratów liczb całkowitych.

Podstawową rolę odegra przy tym następująca ***tożsamość Eulera***:

$$\begin{aligned}(a^2+b^2+c^2+d^2)(x^2+y^2+u^2+v^2) = \\ = (ax+by+cu+dv)^2+(ay-bx+cv-du)^2+ \\ +(au-bv-cx+dy)^2+(av+bu-cy-dx)^2.\end{aligned} \tag{8.25}$$

Tożsamość Eulera jest uogólnieniem tożsamości Brahmagupty-Fibonacci'*ego* (8.1) (dla $c=1$). Jej dowód polega na oczywistym rachowaniu. Wykorzystamy ją w dowodzie twierdzenia Lagrange'*a* T8.12 (podobnie jak wykorzystywaliśmy tożsamość Fibonacci'*ego* w drugim dowodzie twierdzenia Fermat'*a*-Eulera). Znający **kwaterniony** rozpoznają w tożsamości Eulera inny zapis faktu, że moduł iloczynu dwóch kwaternionów równy jest iloczynowi modułów tych kwaternionów. Leonhard Euler, próbując udowodnić twierdzenie T8.12 "odkrył" tę tożsamość w roku 1748 (więc na blisko sto lat przed "odkryciem" kwaternionów przez Hamiltona). Jasne, że (dzięki tożsamości Eulera) wystarczy udowodnić, że każda liczba p i e r w s z a da się przedstawić w postaci sumy czterech kwadratów.

Przechodzimy do sformułowania i dowodu twierdzenia Lagrange'*a*:

TWIERDZENIE 8.12 (***Lagrange'a o czterech kwadratach***) *Każda liczba naturalna da się przedstawić w postaci sumy czterech kwadratów (liczb całkowitych).*

D O W Ó D. Dowód jest podobny do przedstawionego w ustępie 8.2.2 dowodu twierdzenia Fermat'*a*-Eulera T8.1. Zaczniemy od łatwego lematu.

LEMAT 8.4 *Jeżeli p jest dowolną nieparzystą liczbą pierwszą, to istnieje liczba naturalna $m<p$ i takie liczby całkowite x, y, u, v, że $mp=x^2+y^2+u^2+v^2$.*

D O W Ó D. Niech $s=\frac{p-1}{2}$. Rozważmy dwa podzbiory w $\mathbb{Z}/p$:

$$A=\{x^2 \,(\mathrm{mod}\, p) : 0 \leqslant x \leqslant s\}, \quad B=\{-y^2-1 \,(\mathrm{mod}\, p) : 0 \leqslant y \leqslant s\}.$$

Z łatwością sprawdzamy, że każdy z tych zbiorów ma dokładnie $s+1$ elementów. Zatem $A \cap B \neq \varnothing$. Istnieją więc takie liczby całkowite $0 \leqslant x, y \leqslant s$, że

$$x^2 \equiv -y^2-1 \,(\mathrm{mod}\, p),$$

czyli, że $x^2+y^2+1^2+0^2=mp$ dla pewnej liczby naturalnej m. Ponadto $x^2+y^2+1^2+0^2 \leqslant s^2+s^2+1<p^2$. Wystarczy położyć $u=1$, $v=0$. □

W kolejnym lemacie będziemy "zmniejszali" m.

LEMAT 8.5 *Każdą liczbę p i e r w s z ą da się przedstawić w postaci sumy czterech kwadratów liczb całkowitych.*

D O W Ó D. Rzecz jest oczywista dla $p = 2$. Załóżmy więc, że p jest nieparzystą liczbą pierwszą i że (istniejąca na mocy poprzedniego lematu) liczba $m > 0$ w przedstawieniu

$$mp = x^2 + y^2 + u^2 + v^2 \tag{8.26}$$

jest n a j m n i e j s z a z możliwych. Udowodnimy, że wówczas:

(1) m n i e j e s t liczbą parzystą,

(2) m n i e j e s t liczbą nieparzystą $\geqslant 3$.

(1) Gdyby $m = 2m'$, to dwie spośród liczb x, y, u, v byłyby tej samej parzystości i dwie pozostałe również tej samej parzystości. Nie zmniejszając ogólności możemy założyć, że $x \equiv y \pmod 2$ i $u \equiv v \pmod 2$. Wówczas

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{u+v}{2}\right)^2 + \left(\frac{u-v}{2}\right)^2 = \frac{x^2+y^2+u^2+v^2}{2} = m'p,$$

co jest niemożliwe, bo m miało być najmniejsze.

(2) Załóżmy teraz, że $m \geqslant 3$ jest liczbą nieparzystą i podzielmy liczby x, y, u, v przez m z najmniejszą, co do wartości bezwzględnej, resztą:

$$\begin{cases} x = x_1 m + a, & \text{gdzie} \quad |a| < \frac{m}{2}, \\ y = y_1 m + b, & \text{gdzie} \quad |b| < \frac{m}{2}, \\ u = u_1 m + c, & \text{gdzie} \quad |c| < \frac{m}{2}, \\ v = v_1 m + d, & \text{gdzie} \quad |d| < \frac{m}{2}. \end{cases} \tag{8.27}$$

Z tych równości otrzymujemy

$$a^2 + b^2 + c^2 + d^2 = (x - x_1 m)^2 + (y - y_1 m)^2 + (u - u_1 m)^2 + (v - v_1 m)^2 = mp + Am,$$

gdzie $A \in \mathbb{Z}$. Stąd

$$mm' = a^2 + b^2 + c^2 + d^2 \tag{8.28}$$

dla pewnego $m' \in \mathbb{Z}$. Z nierówności $\max\{|a|, |b|, |c|, |d|\} < m/2$ otrzymujemy

$$a^2 + b^2 + c^2 + d^2 < 4 \cdot \left(\frac{m}{2}\right)^2 = m^2,$$

co, wobec równości (8.28), dowodzi, że $m' < m$. Pomnóżmy teraz równości (8.28) i (8.26) stronami i skorzystajmy z tożsamości Eulera. Dostaniemy

$$mm' \cdot mp = X^2 + Y^2 + U^2 + V^2, \tag{8.29}$$

gdzie

$$X = ax + by + cu + dv, \quad Y = ay - bx + cv - du,$$
$$U = au - bv - cx + dy, \quad V = av + bu - cy - dx.$$

Dzięki równościom (8.27) łatwo sprawdzić, że Y, U, $V \equiv 0 \,(\mathrm{mod}\, m)$. Na przykład: $U =$

$$(x - x_1 m)u - (y - y_1 m)v - (u - u_1 m)x + (v - v_1 m)y = m(-x_1 u + y_1 v + u_1 x - v_1 y).$$

Wobec równości (8.29) widzimy stąd, że również X jest podzielne przez m. Dzieląc więc obustronnie równość (8.29) przez m^2 znajdujemy:

$$m'p = (X/m)^2 + (Y/m)^2 + (U/m)^2 + (V/m)^2.$$

Ale mp miała być najmniejszą wielokrotnością p przedstawialną w postaci sumy czterech kwadratów! Mamy więc sprzeczność, bo $m' < m$. To kończy dowód lematu. □

Jasnym jest teraz jak, wykorzystując ponownie tożsamość Eulera, dokończyć dowód twierdzenia Lagrange'*a* o czterech kwadratach. □

8.5.2 Uwagi o sumach trzech kwadratów

Trudniej jest scharakteryzować te liczby naturalne, które dadzą się przedstawić w postaci sumy trzech kwadratów.

Ćwiczenie 8.25 Udowodnić, że jeżeli liczba naturalna $n \equiv 7 \,(\mathrm{mod}\, 8)$, to n nie jest sumą trzech kwadratów.

Ćwiczenie 8.26 Udowodnić, że jeżeli liczba naturalna $n = 4k$ da się przedstawić w postaci sumy trzech kwadratów, to i liczba k da się tak przedstawić.

Z ostatnich ćwiczeń łatwo wywnioskować, że żadna liczba postaci $4^n(8k + 7)$ nie da się przedstawić w postaci sumy trzech kwadratów. Okazuje się, że zachodzi:

TWIERDZENIE 8.13 (***Twierdzenie Gaussa-Legendre'a***) *Każda liczba naturalna nie będąca postaci* $4^n(8k + 7)$ *jest sumą trzech kwadratów liczb całkowitych.* □

Uwaga 1. Dowód twierdzenia T8.13 jest trudny. Podany w końcu XVIII wieku przez Legendre'*a* dowód był niepełny. Wykorzystywał bowiem fakt, że w każdym ciągu arytmetycznym $(rn + a)$ spełniającym warunek $\mathrm{NWD}\,(r, a) = 1$, występuje nieskończenie wiele wyrazów będących liczbami pierwszymi. Fakt ten jest prawdziwy, zobacz T5.19, wszelako został udowodniony przez Dirichlet'*a* później, bo w roku 1837. Pierwszy pełny dowód twierdzenia T8.13 pochodzi od Gaussa.

Uwaga 2. Widzieliśmy, że w naszym drugim dowodzie twierdzenia Fermat'*a*-Eulera T8.1, zobacz ustęp 8.2.2, ważną rolę grała tożsamość podstawowa (8.1) (z $c = 1$). Jeszcze większą rolę grała tożsamość Eulera (8.25) w dowodzie twierdzenia Lagrange'*a*. Wspomnieliśmy już, że tożsamość Eulera jest prostym wnioskiem z faktu istnienia takiego mnożenia w zbiorze $\mathbb{R}^4$ punktów przestrzeni czterowymiarowej, dzięki któremu $\mathbb{R}^4$ staje się ciałem (co prawda nieprzemiennym), tak zwanym **ciałem kwaternionów** ("odkrytym" przez Hamiltona w 1843 roku – zobacz na przykład [**10**]). Podobnie, tożsamość (8.1) z $c = 1$ jest w istocie tylko innym zapisem równości (1.12) wyrażającej ważną własność mnożenia liczb zespolonych, czyli punktów płaszczyzny $\mathbb{R}^2$. Otóż, punktów przestrzeni trójwymiarowej $\mathbb{R}^3$ nie daje się mnożyć w tak porządny sposób. Nie istnieje też (wobec tego) żadna tożsamość wyrażająca iloczyn dwóch sum trzech kwadratów w postaci sumy trzech kwadratów. Jest to ważna przyczyna trudności dowodu twierdzenia Gaussa-Legendre'*a*.

Ćwiczenie 8.27 Liczby $T_k = 1+2+\ldots+k$ nazywają się **liczbami trójkątnymi** (umowa: $T_0 = 0$). Korzystając z twierdzenia Gaussa-Legendre'*a* udowodnić, że każda liczba naturalna jest sumą trzech liczb trójkątnych. *Wskazówka.* Zauważyć równoważność

$$(2u+1)^2 + (2v+1)^2 + (2w+1)^2 = 8n+3 \quad \Longleftrightarrow \quad \frac{u(u+1)}{2} + \frac{v(v+1)}{2} + \frac{w(w+1)}{2} = n.$$

8.6 Dodatek. Piąty dowód TFE

Pokażemy tu nasz piąty dowód twierdzenia Fermat'*a*-Eulera. Ten dowód jest najprostszym dowodem w książce. Nie musimy nawet wiedzieć, że kongruencja $x^2 \equiv -1 \,(\mathrm{mod}\, p)$ ma rozwiązania (przy $p \equiv 1 \,(\mathrm{mod}\, 4)$). Możemy też nic nie wiedzieć o aproksymacjach diofantycznych. Wykorzystamy za to rozwinięcia liczb wymiernych na ułamki łańcuchowe.

Własności kontynuant.

Wiemy, że skończony ułamek łańcuchowy $\langle a_0, a_1, \ldots, a_n\rangle$, pisze się jako zwykły ułamek w postaci ilorazu kontynuant:

$$\langle a_0, a_1, \ldots, a_n\rangle = \frac{K(a_0, a_1, \ldots, a_n)}{K(a_1, \ldots, a_n)}. \tag{8.30}$$

Znamy też Regułę Eulera pozwalającą wyznaczać te kontynuanty. Zobacz ustęp 7.3.1. Z tej reguły wywiedliśmy już równość $K(c_1, c_2, \ldots, c_n) = c_1K(c_2, \ldots, c_n) + K(c_3, \ldots, c_n)$ (zobacz wskazówkę do C7.5) i równość (7.11), z której natychmiast wynika nieskracalność ułamków postaci (8.30), gdy $a_0 \in \mathbb{Z}$ i $a_i \in \mathbb{N}$, przy $i = 1, \ldots, n$. Z jeszcze paru wniosków z Reguły Eulera będziemy korzystać w dalszym ciągu:

Ćwiczenie 8.28 Udowodnić, że dla dowolnych c_i i dowolnego $1 \leqslant k < n$ zachodzi równość

$$K(c_1, \ldots, c_n) = K(c_1, \ldots, c_{k-1})K(c_{k+2}, \ldots, c_n) + K(c_1, \ldots, c_k)K(c_{k+1}, \ldots, c_n).$$

Umawiamy się tu, że $K(\,) = 1$.

Ćwiczenie 8.29 Uzasadnić, że jeżeli $\boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{N}^n$ jest ciągiem palindromicznym długości nieparzystej $n \geqslant 3$, oraz $c_1 \geqslant 2$, to $K(\boldsymbol{c})$ jest liczbą złożoną.

Ćwiczenie 8.30 Uzasadnić, że jeżeli $\boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{N}^n$ jest ciągiem palindromicznym długości parzystej, to $K(\boldsymbol{c})$ jest sumą dwóch kwadratów.

Kanoniczne rozwinięcia liczb wymiernych na ułamki łańcuchowe.

Czytelnik, który rozwiązał ćwiczenie C7.2 wie doskonale, że kanoniczne rozwinięcie liczby wymiernej $\frac{n}{m}$ (zakładamy tu, że $m > 0$) na ułamek łańcuchowy jest zakodowane w algorytmie Euklidesa zastosowanym do pary n, m. Na przykład, pierwsza linijka tego algorytmu, czyli $n = a_0m + r_0$, daje, po obustronnym podzieleniu przez m, równość

$$\frac{n}{m} = a_0 + \frac{r_0}{m} = a_0 + \cfrac{1}{\cfrac{m}{r_0}}. \tag{8.31}$$

Druga linijka (która istnieje w przypadku, gdy $r_0 \neq 0$), czyli $m = a_1 r_0 + r_1$, po obustronnym podzieleniu przez r_1 (jeżeli $r_1 \neq 0$, oczywiście!), pozwala zapisać równość (8.31) w postaci:

$$\frac{n}{m} = a_0 + \frac{1}{a_1 + \dfrac{r_1}{r_0}} = a_0 + \frac{1}{a_1 + \dfrac{1}{\dfrac{r_0}{r_1}}}.$$

Itd. Dwie ostatnie linijki algorytmu mają postać $r_{s-3} = a_{s-1} r_{s-2} + r_{s-1}$ (przedostatnia linijka algorytmu; tu, jak wiemy, $r_{s-1} = \mathrm{NWD}\,(n, m)$) i $r_{s-2} = a_s r_{s-1}$ (ostania linijka). Ponieważ $r_{s-2} > r_{s-1}$, więc widzimy, że ostatni mianownik a_s (kanonicznego rozwinięcia liczby wymiernej na ułamek łańcuchowy) jest ściśle większy niż 1. Każda zatem liczba wymierna $u = \frac{n}{m}$ da się zapisać w postaci

$$u = \langle a_0,\, a_1,\, \ldots,\, a_s \rangle, \tag{8.32}$$

gdzie $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_s \in \mathbb{N}$ oraz (jeżeli $s > 0$, równoważnie, jeżeli $u \notin \mathbb{Z}$) $a_s \geqslant 2$. Taki zapis jest (przy narzuconych ograniczeniach) jednoznaczny.

O pewnej inwolucji.

Powyższe spostrzeżenie pozwala określić pewną inwolucję.

Definicja 8.9 Odwzorowanie $f : X \longrightarrow X$ danego zbioru X w ten sam zbiór X nazywa się **inwolucją**, gdy zachodzi równość $f \circ f = \mathrm{Id}_X$.

Ćwiczenie 8.31 Udowodnić, że każda inwolucja jest bijekcją.

Rozważmy teraz zbiór $\mathbb{Q}_{\geqslant 2}$ wszystkich liczb wymiernych większych lub równych 2. Każda liczba $u \in \mathbb{Q}_{\geqslant 2}$ ma, jak wiemy, dokładnie jedno przedstawienie postaci (8.32), w którym $a_0 \geqslant 2$ i $a_s \geqslant 2$. Zdefiniujemy odwzorowanie $I : \mathbb{Q}_{\geqslant 2} \longrightarrow \mathbb{Q}_{\geqslant 2}$ następująco:

$$u = \langle a_0,\, a_1,\, \ldots,\, a_{s-1},\, a_s \rangle \longmapsto \langle a_s,\, a_{s-1},\, \ldots,\, a_1,\, a_0 \rangle = I(u). \tag{8.33}$$

Ponieważ $a_s = \lfloor I(u) \rfloor \geqslant 2$, więc $I(u)$ rzeczywiście należy do $\mathbb{Q}_{\geqslant 2}$. Jasne jest, że odwzorowanie I jest inwolucją.

Niech $p > 2$ będzie nieparzystą liczbą pierwszą. Oznaczmy $s = \frac{p-1}{2}$ i niech

$$\mathcal{A}_p = \left\{ \frac{p}{1},\, \frac{p}{2},\, \ldots,\, \frac{p}{s} \right\} \tag{8.34}$$

będzie(!) podzbiorem zbioru $\mathbb{Q}_{\geqslant 2}$.

ZADANIE 8.13 Udowodnić, że obcięcie inwolucji I do zbioru $\mathcal{A}_p$ jest inwolucją na tym zbiorze. To znaczy, że $I(u) \in \mathcal{A}_p$ dla każdego $u \in \mathcal{A}_p$.

Rozwiązanie. Niech $\frac{p}{k}$, gdzie $1 \leqslant k \leqslant s$, będzie elementem zbioru $\mathcal{A}_p$. I niech

$$\frac{p}{k} = \langle a_0,\, a_1,\, \ldots,\, a_n \rangle = \frac{K(a_0,\, a_1,\, \ldots,\, a_n)}{K(a_1,\, \ldots,\, a_n)} \tag{8.35}$$

będzie kanonicznym rozwinięciem liczby $\frac{p}{k}$ na ułamek łańcuchowy. Ponieważ stojące po obu stronach tej równości ułamki są n i e s k r a c a l n e, więc, zobacz C2.18, $p = K(a_0, a_1, \ldots, a_n)$. Zapiszmy teraz analogicznie liczbę $I(\frac{p}{k})$:

$$I\left(\frac{p}{k}\right) = \langle a_n, a_{n-1}, \ldots, a_0\rangle = \frac{K(a_n, a_{n-1}, \ldots, a_0)}{K(a_{n-1}, \ldots, a_0)}. \tag{8.36}$$

Z C7.28 wiemy, że $K(a_n, a_{n-1}, \ldots, a_0) = K(a_0, a_1, \ldots, a_n)$. To oznacza, że nieskracalny ułamek z prawej strony równości (8.36) ma licznik równy p. Ponadto, część całkowita liczby $I(\frac{p}{k})$, czyli a_n, spełnia $a_n \geqslant 2$. Zatem liczba wymierna $I(\frac{p}{k})$ jest $\geqslant 2$ i ma w liczniku p. Należy więc do zbioru $\mathcal{A}_p$. $\Diamond$

Lemat o inwolucji.

Udowodnimy prosty lemat o punktach stałych inwolucji na zbiorach skończonych. Dla dowolnego odwzorowania $f : X \longrightarrow X$ przez $\mathrm{Fix}(f)$ oznaczamy zbiór $\{x \in X : f(x) = x\}$ **punktów stałych** odwzorowania f.

LEMAT 8.6 *Dany jest zbiór skończony X i inwolucja $I : X \longrightarrow X$. Wówczas*

$$|\mathrm{Fix}(I)| \equiv |X| \,(\mathrm{mod}\, 2). \tag{8.37}$$

D O W Ó D. Niech $\mathrm{Fix}(I) = \{x_1, x_2, \ldots, x_s\}$. Pozostałe elementy zbioru X występują w parach postaci $\{x, I(x)\}$. Mamy więc rozbicie

$$X = \{x_1\} \sqcup \ldots \sqcup \{x_s\} \sqcup \{x_{s+1}, I(x_{s+1})\} \sqcup \ldots \sqcup \{x_t, I(x_t)\},$$

z którego wynika równość $|X| = s + 2(t - s)$ pociągająca kongruencję (8.37). $\square$

Oto dwa oczywiste wnioski z tego lematu:

WNIOSEK 1 *Inwolucja określona na zbiorze (skończonym) mającym nieparzystą liczbę elementów ma co najmniej jeden punkt stały.* $\square$

WNIOSEK 2 *Jeżeli x_0 jest punktem stałym inwolucji określonej na zbiorze parzystoelementowym, to ta inwolucja ma jeszcze co najmniej jeden punkt stały $x_1 \neq x_0$.* $\square$

Piąty dowód TFE.

Dzięki powyższym uwagom jesteśmy w stanie jeszcze raz udowodnić TFE:

P I Ą T Y D O W Ó D TFE. Niech $p = 4m+1$ będzie liczbą pierwszą. Wówczas zbiór (8.34) ma $2m$ elementów. Element $\frac{p}{1}$ tego zbioru jest, oczywiście, punktem stałym inwolucji I. Na mocy wniosku W2L8.6, w zbiorze $\mathcal{A}_p$ musi istnieć jeszcze co najmniej jeden punkt stały inwolucji I. Niech to będzie liczba $\frac{p}{k}$ i niech zachodzą równości (8.35). Wówczas ciąg $(a_0, a_1, \ldots, a_n)$ jest ciągiem palindromicznym długości parzystej (gdyby był długości nieparzystej, to, na mocy C8.29, liczba $p = K(a_0, \ldots, a_n)$ byłaby złożona). Zatem ciąg $(a_0, a_1, \ldots, a_n)$ jest postaci $(a_0, \ldots, a_s, a_s, \ldots, a_0)$. Po rozwiązaniu C8.30 wiemy, że wtedy:

$$p = K(a_0, \ldots, a_s, a_s, \ldots, a_0) = K(a_0, \ldots, a_s)^2 + K(a_0, \ldots, a_{s-1})^2. \quad \square$$

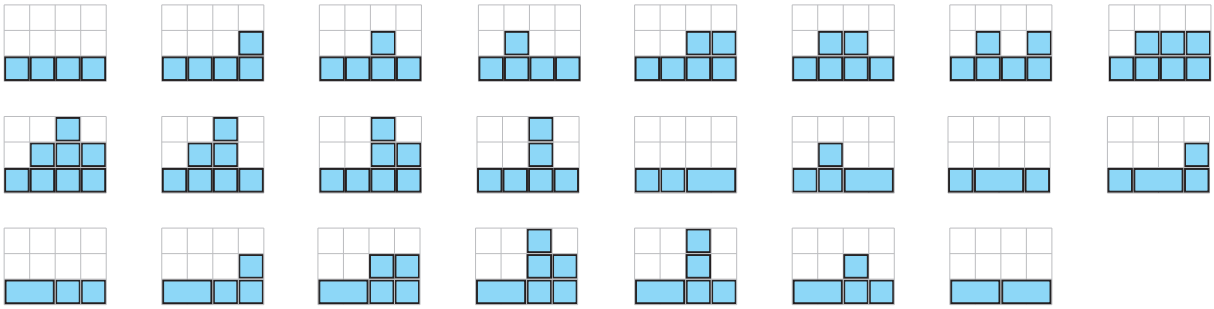
U w a g a 1. Pokazany dowód pochodzi z pracy A.T.Benjamin, D.Zeilberger *Pythagorean primes and palindromic continued fractions*[1]. Tam znaleźć można również dowód jednoznacz-

[1]Za zwrócenie uwagi na tę pozycję autor jest wdzięczny koledze Wojtkowi Wawrowowi

ności (por. Z8.2).

U w a g a 2. Omówienie słynnego *One-sentence Proof that every Prime* $p \equiv 1 \pmod 4$ *is a Sum of Two Squares* Dona Zagiera znaleźć można w [**0**]. Dowód ten również wykorzystuje lemat L8.6.

U w a g a 3. W pracy Benjamina i Zeilbergera znaleźć też można interesującą i przydatną interpretację kombinatoryczną (wartości) kontynuanty $K(c_1, c_2, \ldots, c_n)$ w przypadku, gdy $c_i \in \mathbb{N}$. Mianowicie, $K(c_1, c_2, \ldots, c_n)$ oznacza liczbę możliwych ułożeń kostek 1×2 i 1×1 na szachownicy o c wierszach i n kolumnach (tu $c = \max\{c_1, \ldots, c_n\}$), zgodnie z następującymi zasadami: (1) wszystkie kostki leżą r e g u l a r n i e (tzn. kostka 1×1 pokrywa jedno pole szachownicy, a kostka 1×2, dwa sąsiednie pola), (2) dolny wiersz jest cały pokryty tymi kostkami, (3) kostki 1×2 mogą leżeć t y l k o w dolnym wierszu, (4) w j-tej kolumnie może leżeć co najwyżej c_j kostek 1×1, tworzących spójną "kolumnę", (5) w kolumnach, których dolne pola są zakryte przez kostki 1×2, n i e leżą żadne inne kostki. Na rysunku poniżej widzimy wszystkie takie ułożenia kostek dla ciągu $(c_1, c_2, c_3, c_4) = (1, 2, 3, 2)$.



Widzimy tu, że $K(1, 2, 3, 2) = 23$.

Ćwiczenie 8.32 Udowodnić prawdziwość opisanej interpretacji kontynuant. Udowodnić za jej pomocą Regułę Eulera i rozwiązać C8.28.

Rozdział 9

Arytmetyka ciągów rekurencyjnych

When the emperor Frederic II sejourned there [in Pisa],
Leonardo [Fibonacci] was [...] introduced into the court circle,
at that time a meeting point for Latin, Arabic and Greek culture.
(André Weil)

W elementarnej teorii ciągów rekurencyjnych badamy ciągi (a_n) spełniające warunki

$$\boxed{a_{n+2} = Pa_{n+1} + Qa_n,} \tag{9.1}$$

dla każdego $n \in \mathbb{Z}_{\geqslant 0}$. Tu P, Q są zadanymi s t a ł y m i. Równanie postaci (9.1) nazywamy **równaniem rekurencyjnym liniowym** (drugiego rzędu o stałych współczynnikach). Jasne, że ciąg (a_n) spełniający równanie (9.1) jest j e d n o z n a c z n i e wyznaczony przez podanie dwóch początkowych wyrazów a_0, a_1 (są to tak zwane **warunki początkowe**).

Wielomian (trójmian kwadratowy)

$$\boxed{W(X) = X^2 - PX - Q} \tag{9.2}$$

nazywa się **wielomianem charakterystycznym** równania (9.1) i (spełniającego to równanie) ciągu (a_n). Pierwiastki wielomianu $W(X)$ będziemy oznaczać literami α, β i nazywać **pierwiastkami charakterystycznymi** równania (9.1). Spełniają one zależności

$$\boxed{\alpha + \beta = P, \qquad \alpha\beta = -Q, \qquad \alpha^2 = P\alpha + Q, \qquad \beta^2 = P\beta + Q.} \tag{9.3}$$

Zbiór wszystkich ciągów spełniających (9.1) będziemy oznaczać symbolem $\mathcal{R}ek(P, Q)$.

9.1 Klasyczny ciąg Fibonacci'*ego*

Definicja 9.1 (Klasyczny) **ciąg Fibonacci'*ego*** (f_n) jest elementem $\mathcal{R}ek(1, 1)$ wyznaczonym przez warunki początkowe $f_0 = 0$, $f_1 = 1$. Jego początek wygląda więc tak:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ 233, \ldots .$$

Jasne jest również, że jest to ciąg rosnący o wyrazach całkowitych (nieujemnych).

9.1.1 Wzór Binet'*a*

Zaczniemy od podania zwartej postaci n-tego wyrazu klasycznego ciągu Fibonacci'*ego*.

ZADANIE 9.1 Udowodnić tak zwany ***wzór Binet'a***:

$$\boxed{f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.}$$

R o z w i ą z a n i e. Niech $\alpha = (1+\sqrt{5})/2$, $\beta = (1-\sqrt{5})/2$. Te liczby są pierwiastkami wielomianu charakterystycznego $X^2 - X - 1$. Zależności (9.3) mają w tym przypadku postać:

$$\alpha + \beta = 1, \qquad \alpha\beta = -1, \qquad \alpha^2 = \alpha + 1, \qquad \beta^2 = \beta + 1. \tag{9.4}$$

Z prawej strony dowodzonego wzoru stoi więc liczba

$$g_n := \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{9.5}$$

Mamy udowodnić, że dla każdego $n \in \mathbb{Z}_{\geqslant 0}$ zachodzi równość $f_n = g_n$. Sprawdzenie, że taka równość ma miejsce dla $n = 0$ i $n = 1$ jest natychmiastowe. Tożsamość

$$x^{n+2} - y^{n+2} = (x+y)(x^{n+1} - y^{n+1}) - xy(x^n - y^n),$$

po podzieleniu przez $x - y$ i podstawieniu $x = \alpha$, $y = \beta$, daje równość $g_{n+2} = g_{n+1} + g_n$. To kończy rozwiązanie. ♢

U w a g a. Ponieważ $|\beta| < 1$, więc mamy równość przybliżoną $f_n \approx \alpha^n/\sqrt{5}$.

9.1.2 Kilka tożsamości

Pokażemy teraz pewną ilość tożsamości spełnianych przez wyrazy klasycznego ciągu Fibonacci'*ego*. Dobrze jest przeprowadzić jak najwięcej dowodów samodzielnie, zarówno za pomocą indukcji jak i za pomocą wzoru Binet'*a*.

ZADANIE 9.2 Udowodnić tożsamość

$$f_{2n} = \sum_{k=0}^{n} \binom{n}{k} f_{n-k}.$$

R o z w i ą z a n i e. Na mocy wzoru Binet'*a* (9.5) mamy równość:

$$(\alpha - \beta) f_{2n} = \alpha^{2n} - \beta^{2n} = (\alpha^2)^n - (\beta^2)^n,$$

gdzie α i β spełniają (9.4). Zatem, na mocy (9.4),

$$(\alpha - \beta) f_{2n} = (\alpha + 1)^n - (\beta + 1)^n.$$

Na mocy wzoru dwumiennego dostajemy:

$$(\alpha+1)^n-(\beta+1)^n=\sum_{k=0}^{n}\binom{n}{k}\alpha^{n-k}-\sum_{k=0}^{n}\binom{n}{k}\beta^{n-k}=\sum_{k=0}^{n}\binom{n}{k}(\alpha^{n-k}-\beta^{n-k}).$$

Wobec tego

$$(\alpha-\beta)f_{2n}=\sum_{k=0}^{n}\binom{n}{k}(\alpha^{n-k}-\beta^{n-k}).$$

Wystarczy teraz podzielić przez $\alpha-\beta$. $\Diamond$

Ćwiczenie 9.1 Udowodnić przez indukcję, że dla każdej liczby całkowitej $n\geqslant 0$ zachodzą poniższe równości. Następnie udowodnić te równości korzystając ze wzoru Binet'*a* (jak to pokazujemy w rozwiązaniach zadań Z9.2, Z9.3) i wykryć gdzie "zginęła" indukcja.

(1) $f_0+f_1+\ldots+f_n=f_{n+2}-1$,

(2) $f_1+f_3+\ldots+f_{2n-1}=f_{2n}$,

(3) $f_0+f_2+\ldots+f_{2n}=f_{2n+1}-1$,

(4) $f_0^2+f_1^2+\ldots+f_n^2=f_nf_{n+1}$,

(5) $f_0f_1+f_1f_2+\ldots+f_{2n-1}f_{2n}=f_{2n}^2$,

(6) $f_0f_1+f_1f_2+\ldots+f_{2n}f_{2n+1}=f_{2n+1}^2-1$.

Przed rozwiązaniem następnego zadania proponujemy Czytelnikowi udowodnienie tezy:

Ćwiczenie 9.2 Udowodnić dwiema metodami poniższe równości

$$\alpha^n=f_n\cdot\alpha+f_{n-1},\quad \beta^n=f_n\cdot\beta+f_{n-1},\tag{9.6}$$

gdzie f_k oznacza k-ty wyraz (klasycznego) ciągu Fibonacci'*ego*, a α, β są pierwiastkami charakterystycznymi tego ciągu, czyli liczbami opisanymi przez równości (9.4).

ZADANIE 9.3 Udowodnić tak zwaną ***tożsamość Cesàro***:

$$f_{mn}=\sum_{k=1}^{m}\binom{m}{k}f_kf_n^kf_{n-1}^{m-k}.\tag{9.7}$$

Rozwiązanie. Podobnie jak w zadaniu poprzednim zapiszmy f_{mn} za pomocą wzoru Binet'*a*

$$(\alpha-\beta)f_{mn}=(\alpha^n)^m-(\beta^n)^m.$$

Na mocy równości (9.6) i wzoru dwumiennego, dostajemy zatem:

$$\begin{aligned}(\alpha-\beta)f_{mn}&=(f_n\cdot\alpha+f_{n-1})^m-(f_n\cdot\beta+f_{n-1})^m=\\&=\sum_{k=0}^{m}\binom{m}{k}\left((\alpha f_n)^kf_{n-1}^{m-k}-(\beta f_n)^kf_{n-1}^{m-k}\right)=\sum_{k=0}^{m}\binom{m}{k}f_n^kf_{n-1}^{m-k}(\alpha^k-\beta^k).\end{aligned}$$

Dzieląc przez $(\alpha-\beta)$ i uwzględniając wzory Binet'*a*, mamy (9.7). $\Diamond$

Ćwiczenie 9.3 Udowodnić następujące równości

$$f_{n+1}f_{n-1} - f_n^2 = (-1)^n, \tag{9.8}$$

$$f_{m+1}f_n + f_{n-1}f_m = f_{n+m}. \tag{9.9}$$

Równość (9.8) nosi nazwę ***wzoru Cassini'ego***. W dalszym ciągu zobaczymy, że wzór Cassini'*ego* jest w istocie przypadkiem szczególnym wzoru (9.9).

9.1.3 Dwie interpretacje ciągu (f_n)

Ciąg Fibonacci'*ego* występuje w różnych sytuacjach kombinatorycznych. Opiszemy tu dwie. Dla innych interpretacji zobacz $\mathbb{KOM}$.

Interpretacja Piechura. Wyobraźmy sobie, że w punkcie 1 osi liczbowej stoi piechur i ma dojść do punktu $n \in \mathbb{N}$. Pozwalamy mu iść tylko w prawo i tylko krokami długości 1 lub 2. Postaramy się odpowiedzieć na pytanie: *Na ile sposobów może on pokonać tę drogę*?

Oznaczmy liczbę tych sposobów przez p_n. Jasne, że $p_1 = 1$ ("nicnierobić" można na jeden sposób!). Równie jasne, że $p_2 = 1$ (piechur wykonuje jeden krok długości 1). Rozważmy teraz dowolną liczbę $n \geqslant 3$. Istnieją dwa różne typy marszrut naszego piechura od punktu 1 do punktu n: do pierwszego typu należą te marszruty, których ostatni krok ma długość 1, a do drugiego te, których ostatni krok ma długość 2. Marszrut pierwszego typu jest tyle, na ile sposobów piechur może dojść do punktu $n-1$, czyli p_{n-1}. W czasie marszrut drugiego typu, piechur dociera do liczby $n-2$, na dokładnie p_{n-2} sposoby(!), a następnie wykonuje (jednoznacznie wyznaczony) krok długości 2. Widzimy więc, że: $p_n = p_{n-1} + p_{n-2}$. Ciąg (p_n) spełnia więc to samo równanie rekurencyjne co ciąg Fibonacci'*ego* i ma te same dwie wartości początkowe $p_1 = f_1$, $p_2 = f_2$. Zatem $p_n = f_n$ dla wszystkich $n \in \mathbb{N}$.

Ćwiczenie 9.4 Udowodnić równość (9.9) posługując się interpretacją piechura.

Ćwiczenie 9.5 Niech P_n oznacza ilość sposobów przejścia z punktu 1 do punktu n przez piechura o nogach tak długich, że może stawiać kroki długości 1 lub 2 lub 3. Wyznaczyć związek rekurencyjny jaki spełniają liczby P_n.

Pokażemy jeszcze jedną interpretację wyrazów ciągu Fibonacci'*ego*:

Ćwiczenie 9.6 Uzasadnić, że $f_n = K(1, \ldots, 1)$ (wartość kontynuanty na ciągu $(1, \ldots, 1)$ długości $n-1$). Wywnioskować stąd, że liczba f_{2k+1}, $k \geqslant 1$, jest sumą dwóch kwadratów, a liczba f_{2k}, $k \geqslant 3$, jest liczbą złożoną. *Wskazówka.* Zobacz C8.30 i C8.29.

9.1.4 Ciąg (f_n) jest NWD-ciągiem

Ciąg Fibonacci'*ego* (klasyczny) ma własność podzielności, a nawet jest NWD-ciągiem.

Przypomnijmy (zobacz rozwiązanie Z2.B9), że to oznacza zachodzenie równości

$$\boxed{\boxed{f_{\mathrm{NWD}\,(m,\,n)} = \mathrm{NWD}\,(f_m,\, f_n)}} \tag{9.10}$$

dla dowolnych m, $n \in \mathbb{N}$.

Każdy NWD-ciąg, jak wiemy (zob. U1 w rozwiązaniu Z2.B9), *ma własność podzielności*. Wykazujemy najpierw, że klasyczny ciąg Fibonacci'*ego* ma tę własność:

ZADANIE 9.4 Udowodnić, że ciąg (f_n) spełnia warunek: $\boxed{m|n \Rightarrow f_m|f_n.}$

R o z w i ą z a n i e. Podamy rozwiązanie z wykorzystaniem równości (9.9). Dowodzimy mianowicie przez indukcję względem $q \geqslant 1$, że $f_m|f_{qm}$. Ponieważ jest to oczywiste dla $q = 1$, więc załóżmy, że $f_{qm} = Kf_m$ i podstawmy $n = qm$ w równości (9.9). Wówczas

$$f_{(q+1)m} = f_{qm+m} = f_{m+1}f_{qm} + f_{qm-1}f_m = f_{m+1}Kf_m + f_{qm-1}f_m = K'f_m.$$

To, na mocy zasady indukcji, kończy rozwiązanie. U w a g a. Teza zadania da się też natychmiast wyprowadzić z tożsamości Cesàro (9.7). ◊

Łatwo też wykazać, że k o l e j n e wyrazy ciągu Fibonacci'*ego* są względnie pierwsze:

Ćwiczenie 9.7 Udowodnić, że $\mathrm{NWD}\,(f_n,\ f_{n+1}) = 1$.

Okazuje się, że prawdziwe jest twierdzenie ogólniejsze:

TWIERDZENIE 9.1 *Ciąg Fibonacci'*ego (f_n) *jest* NWD*-ciągiem.*

D O W Ó D. Załóżmy, że $n > m$ i wykonajmy dzielenie z resztą: $n = qm + r$, gdzie $0 \leqslant r < m$. Tożsamość (9.9) i równość $f_{qm} = Kf_m$ pozwalają napisać

$$f_n = f_{qm+r} = f_{r+1}f_{qm} + f_{qm-1}f_r = Kf_{r+1}f_m + f_{qm-1}f_r.$$

Z tej równości widzimy, że $D(f_m,\ f_r) \subseteq D(f_n,\ f_m)$. W istocie między tymi zbiorami wspólnych dzielników zachodzi równość. Rzeczywiście, jeżeli $d|f_n$ i $d|f_m$, to z powyższej równości wnosimy, że $d|f_{qm-1}f_r$. Ale wiemy, że f_{qm-1} i f_{qm} są względnie pierwsze, więc d, jako dzielnik f_m, czyli też f_{qm}, jest względnie pierwsze z f_{qm-1}. Zatem, na mocy ZTA, $d|f_r$. To dowodzi, że $D(f_m,\ f_r) = D(f_n,\ f_m)$, skąd: $\mathrm{NWD}\,(f_n,\ f_m) = \mathrm{NWD}\,(f_m,\ f_r)$. Jasnym teraz być powinno jak skończyć dowód, doprowadzając do końca algorytm Euklidesa wyznaczania największego wspólnego dzielnika liczb n i m. □

Ćwiczenie 9.8 Udowodnić, że dla $3 \leqslant m \leqslant n$ zachodzi wynikanie: $f_m|f_n \Rightarrow m|n$.

9.2 Metoda Eulera i metoda funkcji tworzących

W zadaniu Z9.1 pokazaliśmy wzór Binet'*a* wyrażający w sposób zwarty n-tą liczbę ciągu Fibonacci'*ego*. W tym paragrafie poznamy uogólnienie tego wzoru na przypadek dowolnego ciągu spełniającego (9.1). Następnie poznamy tak zwane funkcje tworzące badanych ciągów.

9.2.1 Metoda Eulera

Euler szukał rozwiązania równania rekurencyjnego (9.1) w postaci $a_n = \xi^n$. Będziemy go naśladować, bo (mistrzów zawsze) warto!

Ćwiczenie 9.9 Udowodnić, że jeżeli ciąg $(a_n) = (\xi^n)$ spełnia równanie (9.1) i $\xi \neq 0$, to ξ jest pierwiastkiem wielomianu charakterystycznego (9.2).

Niech więc dany będzie ciąg $(a_n) \in \mathcal{R}ek(P, Q)$ wyznaczony (jednoznacznie) przez warunki początkowe a_0 i a_1. Oznaczmy (jak zwykle) przez α, β pierwiastki wielomianu charakterystycznego $X^2 - PX - Q$. Przy tych oznaczeniach zachodzi:

TWIERDZENIE 9.2 *Jeżeli $\alpha \neq \beta$, to istnieją takie stałe A, B, że*

$$\boxed{\boxed{a_n = A \cdot \alpha^n + B \cdot \beta^n}} \tag{9.11}$$

dla każdego $n \in \mathbb{Z}_{\geqslant 0}$. Jeżeli zaś $\alpha = \beta$, to istnieją takie stałe C, D, że

$$\boxed{\boxed{a_n = C \cdot \alpha^n + D \cdot n\alpha^{n-1}}} \tag{9.12}$$

dla każdego $n \in \mathbb{Z}_{\geqslant 0}$.

D O W Ó D. Sprawdzenie, że ciąg (x_n) zadany przez $x_n = A\alpha^n + B\beta^n$, przy d o w o l n y c h stałych A, B, spełnia równanie (9.1), jest natychmiastowe:

$$\begin{aligned} x_{n+2} &= A\alpha^{n+2} + B\beta^{n+2} = A\alpha^n(P\alpha + Q) + B\beta^n(P\beta + Q) \\ &= P(A\alpha^{n+1} + B\beta^{n+1}) + Q(A\alpha^n + B\beta^n) = Px_{n+1} + Qx_n. \end{aligned}$$

(Druga równość wynika z faktu, że α i β są pierwiastkami wielomianu charakterystycznego, czyli z równości $\alpha^2 = P\alpha + Q$ i $\beta^2 = P\beta + Q$.) Jeżeli zaś $\alpha = \beta$, to ciąg (x_n) zadany przez $x_n = C\alpha^n + Dn\alpha^{n-1}$, przy d o w o l n y c h stałych C, D, również spełnia równanie (9.1):

$$\begin{aligned} x_{n+2} &= C \cdot \alpha^{n+2} + D \cdot (n+2)\alpha^{n+1} = C \cdot \alpha^n(P\alpha + Q) + D \cdot (n+2)\alpha^{n-1}(P\alpha + Q) \\ &= P(C \cdot \alpha^{n+1} + D \cdot (n+1)\alpha^n) + Q(C \cdot \alpha^n + D \cdot n\alpha^{n-1}) + D\alpha^{n-1}(P\alpha + 2Q) \\ &= Px_{n+1} + Qx_n. \end{aligned}$$

Ostatnia równość wynika z faktu, że $P\alpha + 2Q = 0$ (bo $\Delta = P^2 + 4Q = 0$ i $\alpha = P/2\,(= \beta)$).

Aby zakończyć dowód równości (9.11) i (9.12) musimy dobrać takie stałe A, B w pierwszym przypadku i C, D w drugim przypadku, aby spełnione były warunki początkowe. Innymi słowy, wyznaczyć stałe A, B i C, D z układów równań:

$$\begin{cases} A + B = a_0 \\ A\alpha + B\beta = a_1, \end{cases} \qquad \begin{cases} C = a_0 \\ C\alpha + D = a_1. \end{cases}$$

Układy te mają (jednoznacznie wyznaczone(!)) rozwiązania:

$$A = \frac{a_1 - a_0\beta}{\alpha - \beta}, \quad B = \frac{a_0\alpha - a_1}{\alpha - \beta}; \qquad C = a_0, \quad D = a_1 - a_0\alpha \tag{9.13}$$

(w pierwszym przypadku korzystamy z faktu, że $\alpha \neq \beta$). To kończy dowód. □

Wzory (9.11) i (9.12) wraz z wyznaczonymi stałymi nazywamy ***wzorami Eulera-Binet'a***.

U w a g a. Zauważmy, że pisząc warunek (9.1), nie określiliśmy wyraźnie czym są stałe P, Q, ani czym są wyrazy a_n badanego ciągu. Umawiamy się w dalszym ciągu, że zarówno

współczynniki P, Q jak i wyrazy początkowe badanego ciągu są elementami pewnego pierścienia $\mathcal{R}$. Wówczas, oczywiście, wszystkie wyrazy tego ciągu są elementami pierścienia $\mathcal{R}$, a wielomian charakterystyczny jest wielomianem o współczynnikach w $\mathcal{R}$. Aliści pierwiastki tego wielomianu, których używamy do zapisu wyrazów badanego ciągu, nie muszą należeć do $\mathcal{R}$. Na przykład klasyczny ciąg Fibonacci'*ego* ma, oczywiście, wszystkie wyrazy będące liczbami całkowitymi, ale pierwiastki jego wielomianu charakterystycznego nie są nawet liczbami wymiernymi. Wzór Binet'*a* pokazuje, że za pomocą stosownie dobranych kombinacji liczb niewymiernych wyrazić można zwykłe liczby naturalne. Jeszcze zabawniejsza sytuacja ma miejsce dla ciągu rekurencyjnego danego przez warunek $a_{n+2} = a_{n+1} - a_n$:

Ćwiczenie 9.10 Wyznaczyć wyraz ogólny ciągu danego przez $a_0 = 1$, $a_1 = 2$ i warunek rekurencyjny $a_{n+2} = a_{n+1} - a_n$.

Pierścień $\mathcal{R}$ może być pierścieniem wielomianów:

Ćwiczenie 9.11 Niech $A_0(X) = 1$, $A_1(X) = X$ będą danymi wielomianami. Wyznaczyć n-ty wyraz ciągu $(A_n(X))$, jeżeli

$$A_{n+2}(X) = XA_{n+1}(X) + (1 - X)A_n(X)$$

dla każdego $n \geqslant 0$.

Przykład 1. Ważnym przykładem ciągu rekurencyjnego o wyrazach będących wielomianami jest ciąg $(T_n(X))$ wielomianów zmiennej X zadany przez równanie rekurencyjne

$$T_{n+2}(X) = 2X \cdot T_{n+1}(X) - T_n(X) \tag{9.14}$$

i warunki początkowe $T_0(X) = 1$, $T_1(X) = X$. Warunki te wyznaczają jednoznacznie wielomian $T_n(X)$ dla każdego $n \geqslant 0$. Wielomian T_n nazywa się n-tym **wielomianem Czebyszewa**. Początkowe wyrazy ciągu wielomianów Czebyszewa: $T_0(X) = 1$, $T_1(X) = X$ oraz

$$T_2(X) = 2X^2 - 1, \quad T_3(X) = 4X^3 - 3X, \quad T_4(X) = 8X^4 - 8X^2 + 1, \quad \text{itd.}$$

A oto pierwiastki wielomianu charakterystycznego równania rekurencyjnego (9.14):

$$\alpha = X + \sqrt{X^2 - 1}, \quad \beta = X - \sqrt{X^2 - 1}.$$

Wzory (9.11) i (9.13) dają więc ***wzór Eulera-Binet'a*** na n-ty wielomian Czebyszewa:

$$T_n(X) = \frac{1}{2}\left[(X + \sqrt{X^2 - 1})^n + (X - \sqrt{X^2 - 1})^n\right]. \ \Diamond \tag{9.15}$$

Ćwiczenie 9.12 Udowodnić, że dla dowolnej liczby $z \neq 0$ zachodzi równość

$$T_n(\tfrac{1}{2}(z + z^{-1})) = \tfrac{1}{2}(z^n + z^{-n}).$$

Przykład 2. Jako przykład zastosowania powyższego ćwiczenia udowodnimy: *Liczba*

$$\lambda_n := \sqrt[n]{\sqrt{7} + \sqrt{6}} + \sqrt[n]{\sqrt{7} - \sqrt{6}}$$

jest liczbą niewymierną dla każdego $n \in \mathbb{N}$. Rzeczywiście, łatwo sprawdzić, że $\lambda_n = z + \frac{1}{z}$, gdzie $z = \sqrt[n]{\sqrt{7} + \sqrt{6}}$, a liczba $\frac{1}{2}\left(z^n + \frac{1}{z^n}\right)$ jest równa $\sqrt{7}$, więc, dzięki C9.12, mamy

$$\sqrt{7} = T_n(\tfrac{1}{2}\lambda_n).$$

Gdyby λ_n była liczbą wymierną, to, wobec tego, że wielomian T_n ma współczynniki całkowite, liczba $\sqrt{7} = T_n(\frac{1}{2}\lambda_n)$ też byłaby liczbą wymierną. Sprzeczność. Q.e.d. $\Diamond$

9.2.2 Pierścień formalnych szeregów potęgowych

Funkcja tworząca danego ciągu (a_n) (która, ściśle rzecz ujmując, n i e j e s t f u n k c j ą) jest po prostu n a p i s e m postaci:

$$\sum_{k=0}^{\infty} a_k X^k = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n + \ldots .$$

Takie napisy ("nieskończone wielomiany") nazywają się w matematyce **formalnymi szeregami potęgowymi**.

Definicja 9.2 Zbiór wszystkich napisów postaci $a(X) = \sum_{k=0}^{\infty} a_k X^k$, gdzie $a_k \in \mathbb{K}$, oznaczamy symbolem $\mathbb{K}[[X]]$ i nazywamy **pierścieniem formalnych szeregów potęgowych** o współczynnikach z ciała $\mathbb{K}$. W zbiorze tym wprowadzamy naturalne działania dodawania i mnożenia.

Oczywistym jest, że każdy wielomian o współczynnikach z ciała $\mathbb{K}$ można uważać za formalny szereg potęgowy, w którym prawie wszystkie (czyli wszystkie z wyjątkiem co najwyżej skończenie wielu) współczynniki są równe zero. Uważamy więc, że

$$\mathbb{K}[X] \subseteq \mathbb{K}[[X]].$$

Najważniejszym p o w o d e m takiego u o g ó l n i e n i a pojęcia wielomianu jest m o ż l i w o ś ć o d w r a c a n i a (niektórych) wielomianów o współczynnikach z $\mathbb{K}$. Na przykład, piękne, "sięgające nieskończoności", **uogólnienie tożsamości nieśmiertelnej**:

$$(1 - \lambda X)(1 + \lambda X + \lambda^2 X^2 + \lambda^3 X^3 + \ldots) = 1$$

pokazuje, że wielomian $1 - \lambda X$ jest elementem odwracalnym w pierścieniu $\mathbb{K}[[X]]$. Możemy więc napisać

$$\frac{1}{1 - \lambda X} = (1 - \lambda X)^{-1} = 1 + \lambda X + \lambda^2 X^2 + \lambda^3 X^3 + \ldots = \sum_{k \geqslant 0} \lambda^k X^k. \tag{9.16}$$

Szereg (9.16) nosi nazwę **szeregu Neumanna**.

ZADANIE 9.5 Udowodnić, że $a(X) = \sum_{k \geqslant 0} a_k X^k$ jest elementem odwracalnym w pierścieniu $\mathbb{K}[[X]]$ wtedy i tylko wtedy, gdy $a_0 \neq 0$.

R o z w i ą z a n i e. Jeżeli istnieje taki (formalny) szereg potęgowy $b(X) = \sum_{k \geqslant 0} b_k X^k$, że $a(X)b(X) = 1$, to $a_0 b_0 = 1$. Stąd $a_0 \neq 0$. Z drugiej strony, jeżeli $a_0 \neq 0$, to kładąc

$$b_0 = \frac{1}{a_0},$$

a następnie kolejno

$$b_1 = -\frac{a_1 b_0}{a_0}, \quad b_2 = -\frac{a_1 b_1 + a_2 b_0}{a_0}, \quad \text{itd.}$$

widzimy, że istnieje taki szereg $b(X)$, że $a(X)b(X) = 1$. $\Diamond$

Ćwiczenie 9.13 Udowodnić, że każdy ideał w pierścieniu $\mathbb{K}[[X]]$ jest ideałem głównym. *Wskazówka.* Zdefiniować pojęcie **stopnia dolnego** formalnego szeregu potęgowego.

9.2.3 Metoda funkcji tworzących

Metodę funkcji tworzących objaśnimy na przykładzie ciągu (a_n) spełniającego równanie (9.1). Inne przykłady poznamy w $\mathbb{KOM}$.

Napiszmy **funkcję tworzącą** dla ciągu (a_n):

$$a(X) = a_0 + a_1X + a_2X^2 + \dots .$$

Jest to formalny szereg potęgowy, którego współczynnikami są kolejne wyrazy badanego ciągu. Warunki (9.1), jak łatwo widzieć, można zapisać w postaci równości

$$a(X) - a_0 - a_1X = P(a(X) - a_0)X + Qa(X)X^2.$$

Stąd wyliczamy

$$a(X) = \frac{a_0 + (a_1 - Pa_0)X}{1 - PX - QX^2}. \tag{9.17}$$

Ponieważ umiemy "na piechotę" odwracać wielomiany pierwszego stopnia, porównaj równość (9.16), więc rozłożymy tę funkcję wymierną na ułamki proste, zobacz ustęp 3.4.11. W tym celu rozkładamy mianownik na czynniki nierozkładalne:

Ćwiczenie 9.14 Sprawdzić, że jeżeli α, β są pierwiastkami trójmianu $X^2 - PX - Q$, to zachodzi równość $1 - PX - QX^2 = (1 - \alpha X)(1 - \beta X)$.

Po rozwiązaniu tego ćwiczenia wyznaczamy takie stałe A, B, że

$$\frac{a_0 + (a_1 - Pa_0)X}{1 - PX - QX^2} = \frac{A}{1 - \alpha X} + \frac{B}{1 - \beta X}.$$

Ta strategia zakończy się pełnym sukcesem w przypadku, gdy $\alpha \neq \beta$ (przypadek, gdy $\alpha = \beta$ omawiamy w $\mathbb{KOM}$ 4.3.2). Stąd, dzięki równości (9.16), otrzymujemy równość:

$$a(X) = A\sum_{k\geqslant 0} \alpha^k X^k + B\sum_{k\geqslant 0} \beta^k X^k = \sum_{k\geqslant 0} (A\alpha^k + B\beta^k)X^k,$$

co, po porównaniu współczynników, daje znaną nam już równość (9.11):

$$a_k = A\alpha^k + B\beta^k.$$

Ćwiczenie 9.15 Wykonać te czynności dla przypadku ciągów o wyrazach początkowych $b_0 = 0$, $b_1 = 1$ i wielomianach charakterystycznych $X^2 - X + 2$ oraz $X^2 + 4X + 4$.

9.3 Ciągi Lucas'*a*

W zbiorze wszystkich ciągów rekurencyjnych spełniających równanie (9.1), przy założeniu $\Delta = P^2 + 4Q \neq 0$, Lucas wyróżnił dwa ciągi mające duże znaczenie w teorii liczb.

9.3.1 Przestrzeń $\mathcal{R}ek(P, Q)$

Przyjrzymy się najpierw nieco bliżej zbiorowi $\mathcal{R}ek(P, Q)$ wszystkich ciągów (a_n) o wyrazach z ustalonego ciała $\mathbb{K}$, spełniających równanie rekurencyjne (9.1). Zakładamy też, że $P, Q \in \mathbb{K}$.

Ćwiczenie 9.16 Udowodnić, że $\mathcal{R}ek(P, Q)$ jest przestrzenią liniową nad ciałem $\mathbb{K}$. To znaczy, że jeżeli $(a_n), (b_n) \in \mathcal{R}ek(P, Q)$, to $(a_n + b_n) \in \mathcal{R}ek(P, Q)$. Oraz, że $(\lambda a_n) \in \mathcal{R}ek(P, Q)$ dla dowolnego $\lambda \in \mathbb{K}$.

ZADANIE 9.6 Udowodnić, że $\mathcal{R}ek(P, Q)$ jest przestrzenią dwuwymiarową.

Rozwiązanie. Teza oznacza, że w przestrzeni $\mathcal{R}ek(P, Q)$ istnieje **baza** dwuelementowa. Czyli takie dwa ciągi $(u_n), (v_n)$, że każdy ciąg $(a_n) \in \mathcal{R}ek(P, Q)$ jest **kombinacją liniową** $A(u_n) + B(v_n)$ przy pewnych stałych $A, B \in \mathbb{K}$, oraz że stałe A, B są wyznaczone jednoznacznie.

To zostało uzasadnione w dowodzie T9.2, gdzie widzieliśmy, że w przypadku $\Delta \neq 0$ można przyjąć $u_n = \alpha^n$, $v_n = \beta^n$, a w przypadku $\Delta = 0$ można przyjąć $u_n = \alpha^n$, $v_n = n\alpha^{n-1}$. ◊

Dzięki temu możemy rozwiązać zadanie, którego tezę wykorzystamy w dalszym ciągu:

ZADANIE 9.7 Udowodnić, że jeżeli $(a_n) \in \mathcal{R}ek(P, Q)$, to istnieją takie stałe P_d, Q_d, że ciąg (c_n) zadany przez $c_n = a_{dn+r}$ należy do $\mathcal{R}ek(P_d, Q_d)$.

Rozwiązanie. Liczymy:

$$c_n = a_{dn+r} = A\alpha^{dn+r} + B\beta^{dn+r} = A\alpha^r(\alpha^d)^n + B\beta^r(\beta^d)^n.$$

Kładąc $A' = A\alpha^r$, $B' = B\beta^r$ i $\varphi = \alpha^d$, $\psi = \beta^d$ widzimy stąd, że $c_n = A'\varphi^n + B'\psi^n$ dla każdego $n \in \mathbb{Z}_{\geqslant 0}$. Niech $P_d = \alpha^d + \beta^d$, $Q_d = -\alpha^d\beta^d$. Wtedy $(c_n) \in \mathcal{R}ek(P_d, Q_d)$. ◊

Przykład. Jeżeli (f_n) jest klasycznym ciągiem Fibonacci'*ego*, to zarówno $(e_n) := (f_{2n})$ jak i $(o_n) := (f_{2n+1})$ spełniają równanie rekurencyjne $x_{n+2} = 3x_{n+1} - x_n$. ◊

9.3.2 Definicja ciągów Lucas'*a*

W zbiorze (przestrzeni liniowej) $\mathcal{R}ek(P, Q)$ wszystkich ciągów spełniających równanie (9.1), przy założeniu $\alpha \neq \beta$ (czyli, równoważnie, $\Delta \neq 0$), Lucas wyróżnia dwa ciągi. Tworzą one bazę w przestrzeni $\mathcal{R}ek(P, Q)$.

Definicja 9.3 Niech α, β będą takie jak wyżej. Określmy

$$u_n = u(P, Q)_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{i} \qquad v_n = v(P, Q)_n = \alpha^n + \beta^n \tag{9.18}$$

dla każdego $n \in \mathbb{Z}_{\geqslant 0}$. Ciąg $(u(P, Q)_n)$ nazywamy **ciągiem Lucas'a** wyznaczonym przez parę (P, Q). Ciąg $(v(P, Q)_n)$ nazywamy **stowarzyszonym ciągiem Lucas'a** wyznaczonym przez parę (P, Q). Gdy wiemy jakie stałe P, Q mamy na myśli, piszemy po prostu u_n i v_n.

Ponieważ zarówno (u_n) jak i (v_n) są kombinacjami liniowymi $A(\alpha^n)+B(\beta^n)$, więc (zobacz Z9.6) oba należą do przestrzeni $\mathcal{R}ek(P, Q)$. Co więcej, ponieważ, jak łatwo sprawdzić,

$$\alpha^n = \frac{\alpha-\beta}{2}\cdot u_n + \frac{1}{2}\cdot v_n, \qquad \beta^n = \frac{\beta-\alpha}{2}\cdot u_n + \frac{1}{2}\cdot v_n,$$

a ciągi (α^n), (β^n) stanowią b a z ę w przestrzeni $\mathcal{R}ek(P, Q)$, więc i ciągi Lucas'*a* (u_n), (v_n) stanowią bazę w $\mathcal{R}ek(P, Q)$.

P r z y k ł a d 1. Ciąg Lucas'*a* $(u(1, 1)_n)$ jest, oczywiście, znanym nam (klasycznym) ciągiem Fibonacci'*ego*. Stowarzyszony z nim ciąg $(v(1, 1)_n)$ nazywa się (**klasycznym) ciągiem Lucas'a** i oznacza zazwyczaj (l_n). Zaczyna się on następująco

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, \ldots . \lozenge$$

P r z y k ł a d 2. Liczby $P = 3$, $Q = -2$ dają **ciąg Mersenne'a** i **ciąg Fermat'a**:

$$u(3, -2)_n = 2^n - 1, \quad v(3, -2)_n = 2^n + 1. \lozenge$$

Zauważmy, że (przy zadanych P, Q) ciąg Lucas'*a* $(u_n) = (u(P, Q)_n)$ jest wyznaczony przez warunki początkowe $u_0 = 0$, $u_1 = 1$, zaś stowarzyszony ciąg $(v_n) = (v(P, Q)_n)$ przez warunki początkowe $v_0 = 2$, $v_1 = P$.

9.3.3 Kilka tożsamości

Przytoczymy tu kilka tożsamości wiążących wyrazy ciągów Lucas'*a* i stowarzyszonych ciągów Lucas'*a*. Tożsamości dla wyrazów ciągu u_n są (oczywiście) uogólnieniami analogicznych tożsamości dla wyrazów klasycznego ciągu Fibonacci'*ego*. Dowody są natychmiastowe i należy je zrobić samodzielnie.

Ćwiczenie 9.17 Uzasadnić, że dla dowolnego $n \in \mathbb{Z}_{\geqslant 0}$ zachodzą równości

$$\alpha^n = u_{n+1} - \beta u_n, \quad \beta^n = u_{n+1} - \alpha u_n, \tag{9.19}$$

$$\alpha^n = Q u_{n-1} + \alpha u_n, \quad \beta^n = Q u_{n-1} + \beta u_n. \tag{9.20}$$

Ćwiczenie 9.18 Udowodnić, że dla dowolnych liczb m, $n \in \mathbb{Z}_{\geqslant 0}$ zachodzą równości

$$u_{m+n} = u_m u_{n+1} + Q u_{m-1} u_n, \tag{9.21}$$

$$u_{m+n} = u_m u_n - (-Q)^n u_{m-n}, \tag{9.22}$$

$$2u_{m+n} = u_m v_n + u_n v_m, \tag{9.23}$$

$$u_{2n} = u_n v_n, \tag{9.24}$$

$$v_{m+n} = v_m v_n - (-Q)^n v_{m-n}, \tag{9.25}$$

$$2v_{m+n} = v_m v_n + \Delta u_m u_n, \tag{9.26}$$

$$v_{2n} = v_n^2 - 2(-Q)^n. \tag{9.27}$$

Ćwiczenie 9.19 Udowodnić ***tożsamość kwadratową***:

$$v_n^2 - \Delta u_n^2 = 4(-Q)^n. \tag{9.28}$$

Ćwiczenie 9.20 Udowodnić ***wzór Cassini'ego***:

$$u_n^2 - u_{n-1}u_{n+1} = (-Q)^{n-1}. \tag{9.29}$$

Ćwiczenie 9.21 Udowodnić ***formuły konwersji***:

$$\Delta u_n = v_{n+1} + Qv_{n-1}, \tag{9.30}$$

$$v_n = u_{n+1} + Qu_{n-1}. \tag{9.31}$$

Uogólnionych tożsamości Cesàro dla ciągu Lucas'*a* $u(P, Q)_n$ dowodzimy wykorzystując tak samo ćwiczenie C9.17, jak w rozwiązaniu zadania Z9.3 wykorzystywaliśmy C9.2:

ZADANIE 9.8 Udowodnić, że zachodzą ***uogólnione tożsamości Cesàro***:

$$u_{kn} = \sum_{j=1}^{k} \binom{k}{j} Q^{k-j} u_{n-1}^{k-j} u_n^j u_j, \tag{9.32}$$

$$u_{kn} = \sum_{j=1}^{k} \binom{k}{j} (-1)^{j-1} u_{n+1}^{k-j} u_n^j u_j. \tag{9.33}$$

R o z w i ą z a n i e. Podnosząc obie strony równości (9.20) do potęgi k, a następnie odejmując stronami, znajdujemy:

$$\alpha^{kn} - \beta^{kn} = \sum_{j=0}^{k} \binom{k}{j} Q^{k-j} u_{n-1}^{k-j} u_n^j (\alpha^j - \beta^j).$$

Wystarczy teraz podzielić obie strony przez $\alpha - \beta$ i otrzymamy równość (9.32). Składnik sumy odpowiadający wskaźnikowi $j = 0$ możemy opuścić, bo $u_0 = 0$. Podobnie postępujemy przy dowodzie (9.33). W tym przypadku korzystamy z równości (9.19). ◊

9.3.4 Podzielność wyrazów ciągów Lucas'*a*

Zajmiemy się tu podzielnością wyrazów u_n ciągów Lucas'*a*. Z definicji D9.3 wiemy, że $u_0 = 0$, $u_1 = 1$, a wszystkie wyrazy u_n są liczbami całkowitymi, gdy, jak t e r a z zakładamy, $P, Q \in \mathbb{Z}$.

Poniższe ćwiczenie można rozwiązać przez indukcję, korzystając z (9.21), tak jak w rozwiązaniu Z9.4 korzystaliśmy z (9.9). Można też skorzystać bezpośrednio z uogólnionej tożsamości Cesàro (9.32) lub (9.33).

Ćwiczenie 9.22 Udowodnić, że jeżeli $m, q \geqslant 1$, to $u_m | u_{qm}$.

Załóżymy teraz dodatkowo, że liczby P i Q są w z g l ę d n i e p i e r w s z e. Przy tym założeniu z łatwością rozwiążemy dwa dalsze ćwiczenia:

Ćwiczenie 9.23 Udowodnić, że $\mathrm{NWD}\,(u_k,\, u_{k+1}) = 1$ dla dowolnego $k \geqslant 0$.

Ćwiczenie 9.24 Udowodnić, że jeżeli $\mathrm{NWD}\,(P,\, Q) = 1$, to dla każdego $n \geqslant 1$ mamy $\mathrm{NWD}\,(u_n,\, Q) = 1$ i $\mathrm{NWD}\,(v_n,\, Q) = 1$.

Ciąg Lucas'*a* $u(P,\, Q)_n$ bywa NWD-ciągiem:

Ćwiczenie 9.25 Udowodnić, że jeżeli $\mathrm{NWD}\,(P,\, Q) = 1$, to

$$\mathrm{NWD}\,(u_m,\, u_n) \sim u_{\mathrm{NWD}\,(m,\,n)}. \tag{9.34}$$

Rozwiązanie tego ćwiczenia jest prostym uogólnieniem dowodu T9.1. Znaczek $\sim$ w zbiorze liczb całkowitych oznacza: *równy z dokładnością do znaku*.

Przy okazji rozwiążmy:

Ćwiczenie 9.26 Udowodnić, że jeżeli liczby naturalne $k > l$ są względnie pierwsze, to ciąg $a_n = k^n - l^n$ jest NWD-ciągiem, co znaczy, że $\mathrm{NWD}\,(a_n,\, a_m) = a_{\mathrm{NWD}\,(n,\,m)}$ dla dowolnych $n,\, m \in \mathbb{N}$.

9.4 Ilustracja geometryczna

Badając ciąg rekurencyjny dany przez (9.1) wygodnie jest patrzeć na stowarzyszony ciąg punktów $\boldsymbol{a}_n = (a_n,\, a_{n+1})$ płaszczyzny (w ustalonym prostokątnym układzie współrzędnych). Jasne, że ciąg punktów płaszczyzny $(\boldsymbol{a}_n)$ wyznacza ciąg (a_n) i odwrotnie. Okaże się, że ciąg $(\boldsymbol{a}_n)$ jest c i ą g i e m g e o m e t r y c z n y m o ilorazie będącym macierzą.

9.4.1 Macierze odwzorowań liniowych

Rozpatrzymy tu prosty przypadek odwzorowań płaszczyzny $\mathbb{R}^2$: odwzorowania liniowe.

Przypomnijmy, że (po ustaleniu prostokątnego układu współrzędnych) każdy punkt $\boldsymbol{w}$ płaszczyzny utożsamiamy z parą $(x,\, y)$ liczb rzeczywistych (odcięta i rzędna punktu).

Definicja 9.4 Odwzorowaniem liniowym płaszczyzny nazywamy funkcję daną przez

$$F(x,\, y) = (ax + by,\, cx + dy), \tag{9.35}$$

gdzie $a,\, b,\, c,\, d$ są ustalonymi liczbami. Takie odwzorowanie będziemy kodować za pomocą **macierzy** 2×2 (czyli tabliczki złożonej z czterech liczb)

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{9.36}$$

W takiej sytuacji mówimy, że $\mathbf{A}$ jest **macierzą odwzorowania liniowego** F i zamiast $F(\boldsymbol{w})$ piszemy po prostu $\mathbf{A}\boldsymbol{w}$. W postaci rozpisanej:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Dla wygody zapisujemy punkt (wektor) $\boldsymbol{w} = (x,\, y)$ w postaci k o l u m n o w e j.

W zbiorze $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ wszystkich macierzy o dwóch wierszach i dwóch kolumnach wprowadzamy działanie **mnożenia macierzy**. Odpowiada ono składaniu odwzorowań: jeżeli F i G są odwzorowaniami liniowymi zadanymi przez macierze

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{i} \quad \mathbf{B} = \begin{pmatrix} k & l \\ m & n \end{pmatrix},$$

odpowiednio, to złożenie $F \circ G$ jest odwzorowaniem liniowym zadanym przez macierz

$$\mathbf{A} \cdot \mathbf{B} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} k & l \\ m & n \end{pmatrix} := \begin{pmatrix} ak+bm & al+bn \\ ck+dm & cl+dn \end{pmatrix}.$$

Ćwiczenie 9.27 Sprawdzić to.

Ćwiczenie 9.28 Narysować obrazy $F(\triangle \boldsymbol{uvw})$ trójkąta o wierzchołkach $\boldsymbol{u} = (1, 2)$, $\boldsymbol{v} = (-2, 5)$, $\boldsymbol{w} = (3, 7)$, gdzie F oznacza każde z trzech odwzorowań liniowych danych przez macierze $\mathbf{A}$, $\mathbf{B}$ i $\mathbf{C}$ z następnego ćwiczenia.

Ćwiczenie 9.29 Niech $\mathbf{A} = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$, $\mathbf{B} = \left(\begin{smallmatrix} 0 & 1 \\ -2 & 3 \end{smallmatrix}\right)$, $\mathbf{C} = \left(\begin{smallmatrix} 2 & 3 \\ 3 & 4 \end{smallmatrix}\right)$. Wyznaczyć iloczyny $\mathbf{A} \cdot \mathbf{B}$, $\mathbf{B} \cdot \mathbf{A}$ i $\mathbf{C}^2 := \mathbf{C} \cdot \mathbf{C}$.

Przy wprowadzonych wyżej oznaczeniach, dla każdego $n \geqslant 0$ zachodzi równość:

$$\boldsymbol{a}_{n+1} = \mathbf{U}\boldsymbol{a}_n, \tag{9.37}$$

gdzie $\mathbf{U}$ jest macierzą

$$\mathbf{U} = \begin{pmatrix} 0 & 1 \\ Q & P \end{pmatrix}. \tag{9.38}$$

Ćwiczenie 9.30 Sprawdzić to.

Równość (9.37) można interpretować następująco: ciąg $(\boldsymbol{a}_n)$ jest ciągiem geometrycznym o ilorazie będącym macierzą $\mathbf{U}$. Dzięki tej interpretacji można w postaci zwartej zapisać n-ty wyraz ciągu $(\boldsymbol{a}_n)$:

$$\boldsymbol{a}_n = \mathbf{U}^n \boldsymbol{a}_0 = \begin{pmatrix} 0 & 1 \\ Q & P \end{pmatrix}^n \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}.$$

Cała trudność wyznaczenia ciągu danego przez (9.1) sprowadza się do wyznaczenia n-tej potęgi macierzy $\mathbf{U} = \left(\begin{smallmatrix} 0 & 1 \\ Q & P \end{smallmatrix}\right)$. W algebrze liniowej poznajemy metodę **diagonalizacji** macierzy, która pozwala w zwartej postaci obliczać potęgi danej macierzy. Metoda ta jest dokładnie r ó w n o w a ż n a z metodą Eulera i nie będziemy jej tu przedstawiać.

Ćwiczenie 9.31 Niech $\mathbf{F} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ będzie macierzą (9.38) dla ciągu Fibonacci'*ego*. Wykazać, że n-ta potęga macierzy $\mathbf{F}$ dana jest przez

$$\mathbf{F}^n = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix}.$$

9.4.2 Wyznacznik odwzorowania liniowego

Wyznacznik odwzorowania liniowego jest bardzo ważną charakterystyką tego odwzorowania: "czuje" on, czy odwzorowanie jest czy nie jest bijekcją.

Definicja 9.5 Jeżeli F, zadane wzorem (9.35), jest odwzorowaniem liniowym o macierzy $\mathbf{A}$ zadanej przez (9.36), to liczbę

$$\det F = \det \mathbf{A} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} := ad - bc$$

nazywamy **wyznacznikiem** odwzorowania F lub **wyznacznikiem** macierzy $\mathbf{A}$.

Ćwiczenie 9.32 Sprawdzić, że dla dowolnych macierzy 2×2 zachodzi równość

$$\det(\mathbf{A} \cdot \mathbf{B}) = \det \mathbf{A} \cdot \det \mathbf{B}.$$

Wywnioskować stąd równość (9.8). *Wskazówka.* Zobacz C9.31.

Ćwiczenie 9.33 Udowodnić, że odwzorowanie liniowe F jest bijekcją wtedy i tylko wtedy, gdy $\det F \neq 0$.

9.4.3 Pola trójkątów

Wyznacznik ma arcyważną interpretację geometryczną. Jest zorientowaną objętością. W szczególności, wyznacznik macierzy 2×2 jest zorientowanym polem równoległoboku rozpiętego na wektorach kolumnowych.

Dla danych dwóch punktów $\boldsymbol{v} = (v_1, v_2)$ i $\boldsymbol{w} = (w_1, w_2)$ oznaczmy przez $S(\boldsymbol{v}, \boldsymbol{w})$ zorientowane pole trójkąta o wierzchołkach

$$\mathbf{0} = (0, 0), \quad \boldsymbol{v} = (v_1, v_2), \quad \boldsymbol{w} = (w_1, w_2).$$

Zorientowaność pola oznacza tu, że $S(\boldsymbol{w}, \boldsymbol{v}) = -S(\boldsymbol{v}, \boldsymbol{w})$ oraz że pole $S(\boldsymbol{v}, \boldsymbol{w})$ jest nieujemne, gdy wektor $\overrightarrow{\mathbf{0}\boldsymbol{v}}$ musimy obrócić o kąt niewiększy niż 180° w kierunku przeciwnym do ruchu wskazówek zegara aby "padł" na wektor $\overrightarrow{\mathbf{0}\boldsymbol{w}}$.

Ćwiczenie 9.34 Udowodnić, że dla danych punktów $\boldsymbol{v} = (v_1, v_2)$, $\boldsymbol{w} = (w_1, w_2)$ zachodzi równość

$$S(\boldsymbol{v}, \boldsymbol{w}) = \frac{1}{2} \begin{vmatrix} v_1 & w_1 \\ v_2 & w_2 \end{vmatrix}.$$

Ćwiczenie 9.35 Udowodnić, że jeżeli $\boldsymbol{v}$, $\boldsymbol{w}$ są dwoma punktami, $\mathbf{B} \in \mathrm{Mat}_{2\times 2}$, to

$$S(\mathbf{B}\boldsymbol{v}, \mathbf{B}\boldsymbol{w}) = \det \mathbf{B} \cdot S(\boldsymbol{v}, \boldsymbol{w}). \tag{9.39}$$

9.4.4 Ogólny wzór Cassini'*ego*

Wzór Cassini'*ego* (9.8) ma interpretację geometryczną, o której teraz powiemy dwa słowa. Dla uproszczenia zakładamy tu, że rozpatrywane ciągi $(a_n) \in \mathcal{R}ek(P, Q)$ są ciągami o wyrazach r z e c z y w i s t y c h (w szczególności $P, Q \in \mathbb{R}$).

ZADANIE 9.9 Udowodnić, że jeżeli $(a_n) \in \mathcal{R}ek(P, Q)$, to dla każdego $n \geqslant 0$ zachodzi

$$a_{n-1}a_{n+1} - a_n^2 = (-Q)^{n-1}(a_0a_2 - a_1^2). \tag{9.40}$$

R o z w i ą z a n i e. Liczba stojąca po lewej stronie równości (9.40) jest podwojonym polem trójkąta $\triangle \mathbf{0}\boldsymbol{a}_{n-1}\boldsymbol{a}_n$. Jest więc ona, na mocy C9.35, równa podwojonemu polu trójkąta $\triangle \mathbf{0}\boldsymbol{a}_{n-2}\boldsymbol{a}_{n-1}$ pomnożonemu przez $\det \mathbf{U} = -Q$. Reszta jest oczywistą indukcją. ◊

Równość (9.40), której przypadkiem szczególnym jest wzór Cassini'*ego* (9.8), może być nazwana ***uogólnionym wzorem Cassini'ego***.

Ciągi, jakie badamy w tym rozdziale są funkcjami określonymi na zbiorze $\mathbb{Z}_{\geqslant 0}$ nieujemnych liczb całkowitych. Jeżeli $a : \mathbb{Z}_{\geqslant 0} \longrightarrow \mathbb{C}$ jest takim ciągiem (zgodnie z tradycją piszemy a_n zamiast $a(n)$, a sam ciąg a oznaczamy symbolem (a_n)), to dowolna taka funkcja $\widetilde{a} : \mathbb{Z} \longrightarrow \mathbb{C}$, że $\widetilde{a}(n) = a(n)$ dla wszystkich $n \in \mathbb{Z}_{\geqslant 0}$ nazywa się **przedłużeniem ciągu** a **na** $\mathbb{Z}$. Dany ciąg $a = (a_n)$ może być oczywiście na nieskończenie wiele sposobów przedłużony na $\mathbb{Z}$. Interesujemy się tu jednak tylko takimi przedłużeniami ciągów z $\mathcal{R}ek(P, Q)$, które s p e ł n i a j ą równanie (9.1) dla w s z y s t k i c h $n \in \mathbb{Z}$. Łatwo się przekonać, że takie przedłużenie klasycznego ciągu Fibonacci'*ego* istnieje i jest tylko jedno. Jego "początek" wygląda tak:

$$\ldots,\ 34,\ -21,\ 13,\ -8,\ 5,\ -3,\ 2,\ -1,\ 1,\ 0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ \ldots$$

Ćwiczenie 9.36 Niech $(a_n) \in \mathcal{R}ek(P, Q)$, przy $Q \neq 0$. Udowodnić, że wówczas istnieje d o k ł a d n i e j e d n o przedłużenie ciągu (a_n) na $\mathbb{Z}$. Jeżeli ponadto $a_0 = 0$, to

$$a_{-n} = (-1)^{n+1}Q^{-n}a_n \tag{9.41}$$

dla każdego $n \in \mathbb{Z}$.

ZADANIE 9.10 Załóżmy, że ciąg $(a_n)_{n\in\mathbb{Z}}$ spełnia (9.1), przy czym $Q \neq 0$ i $a_0 = 0$. Udowodnić, że dla dowolnych $m, n \in \mathbb{Z}$ zachodzi równość

$$a_m a_{n+1} + Q a_{m-1} a_n = a_1 a_{n+m}. \tag{9.42}$$

R o z w i ą z a n i e. Rozważmy trójkąt o wierzchołkach

$$\mathbf{0} = (0,\, 0), \quad \boldsymbol{a}_{s+t} = (a_{s+t},\, a_{s+t+1}), \quad \boldsymbol{a}_s = (a_s,\, a_{s+1}).$$

Ponieważ $\boldsymbol{a}_{s+t} = \mathbf{U}^s\boldsymbol{a}_t$, $\boldsymbol{a}_{s+t+1} = \mathbf{U}^s\boldsymbol{a}_{t+1}$, a $\det \mathbf{U} = -Q$, więc, na mocy C9.35 i C9.32, $S(\boldsymbol{a}_{s+t},\, \boldsymbol{a}_s) = (-Q)^s S(\boldsymbol{a}_t,\, \boldsymbol{a}_0)$. Zatem $a_{s+t}a_{s+1} - a_{s+t+1}a_s = (-Q)^s a_1 a_t$ dla wszystkich $s, t \in \mathbb{Z}$. Kładąc tu $s = -m$, $t = n + m$ i wykorzystując równości (9.41), po uproszczeniu przez $(-1)^m Q^m$, dostajemy równość (9.42). ◊

Równość (9.42) jest zapowiadanym uogólnieniem równości (9.9). Dowód tej równości za pomocą standardowego rozumowania indukcyjnego dla $n, m \geqslant 0$ nie przedstawia żadnych trudności i Czytelnik z łatwością zrobi go samodzielnie.

Ćwiczenie 9.37 Ciąg (a_n) zadany jest przez warunki początkowe $a_0 = 4$, $a_1 = 10$ i równanie rekurencyjne $a_{n+2} = 3a_{n+1} + a_n$. Dowieść, że jeśli dla pewnego wskaźnika parzystego n i pewnej liczby pierwszej p zachodzą warunki $a_n \equiv 4 \pmod p$ i $a_{n+1} \not\equiv 2 \pmod p$, to $a_{n+1} \equiv 10 \pmod p$.

9.5 Ciągi rekurencyjne modulo p

W tym paragrafie będziemy chcieli powiedzieć parę słów na temat ciągów rekurencyjnych modulo p, gdzie p jest liczbą pierwszą. Przyda się nam do tego celu nowe ciało, którego konstrukcja jest analogiczna do konstrukcji ciała liczb zespolonych z liczb rzeczywistych.

9.5.1 Warstwy "zespolone" modulo p

Ciało liczb zespolonych $\mathbb{C}$ powstaje z ciała liczb rzeczywistych przez dołączenie pierwiastka kwadratowego z -1: $\mathbb{C} = \mathbb{R}(\sqrt{-1})$. Powód, dla którego się to robi jest prosty: chodzi o to, by równanie wielomianowe $x^2+1 = 0$ miało pierwiastki. Okazuje się, że zysk znacznie przewyższa oczekiwania: po takim rozszerzeniu, nie tylko każde równanie kwadratowe ma pierwiastki, ale w ogóle każde równanie wielomianowe ma pierwiastki (Zasadnicze Twierdzenie Algebry!). W sytuacji, którą chcemy teraz omówić, już tak dobrze nie jest.

Niech $p > 2$ będzie ustaloną liczbą pierwszą nieparzystą, a g ustalonym pierwiastkiem pierwotnym modulo p. Zbiór wszystkich napisów postaci

$$a + b\iota,$$

gdzie $a, b \in \mathbb{Z}/p$ oznaczymy symbolem $\mathbb{F}_p(\iota)$. Symbol ι gra tu podobną rolę jak jednostka urojona i w teorii liczb zespolonych. Zbiór $\mathbb{F}_p(\iota)$ ma, jak widać, p^2 elementów. W zbiorze $\mathbb{F}_p(\iota)$ wprowadzamy działanie **dodawania**

$$(a + b\iota) + (c + d\iota) = (a + c) + (b + d)\iota$$

i działanie **mnożenia**

$$(a + b\iota) \cdot (c + d\iota) = (ac + bdg) + (ad + bc)\iota.$$

Działania w nawiasach po prawych stronach wykonujemy (oczywiście) modulo p. Przy wykonywaniu działań w $\mathbb{F}_p(\iota)$ mamy więc prostą regułę:

rób wszystko modulo p ***pamiętając, że*** $\iota^2 = g$.

Utożsamiając napis $a + 0\iota$ z warstwą $a \in \mathbb{Z}/p$ traktujemy ciało $\mathbb{Z}/p$ jako podzbiór w $\mathbb{F}_p(\iota)$. W szczególności w zbiorze $\mathbb{F}_p(\iota)$ mamy wyróżniony element $0 = 0 + 0\iota$ ("zero" – element neutralny względem dodawania) i $1 = 1+0\iota$ ("jedynkę" – element neutralny względem mnożenia). Ponadto, zamiast $0 + b\iota$ piszemy po prostu $b\iota$.

Łatwo widzieć, że $\mathbb{F}_p(\iota)$ z tymi elementami wyróżnionymi i wprowadzonymi działaniami jest pierścieniem przemiennym z jedynką. Znamy już zatem dwa pierścienie mające p^2 elementów: $\mathbb{F}_p(\iota)$ i $\mathbb{Z}/p^2$. Musimy wyraźnie podkreślić, że są to radykalnie różne pierścienie.

P r z y k ł a d. Weźmy $p = 3$, $g = 2$. Napiszemy tabliczkę mnożenia w zbiorze niezerowych elementów w $\mathbb{F}_3(\sqrt{2})$:

$\cdot$	1	2	ι	$1+\iota$	$2+\iota$	2ι	$1+2\iota$	$2+2\iota$
1	1	2	ι	$1+\iota$	$2+\iota$	2ι	$1+2\iota$	$2+2\iota$
2	2	1	2ι	$2+2\iota$	$1+2\iota$	ι	$2+\iota$	$1+\iota$
ι	ι	2ι	2	$2+\iota$	$2+2\iota$	1	$1+\iota$	$1+2\iota$
$1+\iota$	$1+\iota$	$2+2\iota$	$2+\iota$	2ι	1	$1+2\iota$	2	ι
$2+\iota$	$2+\iota$	$1+2\iota$	$2+2\iota$	1	ι	$1+\iota$	2ι	2
2ι	2ι	ι	1	$1+2\iota$	$1+\iota$	2	$2+2\iota$	$2+\iota$
$1+2\iota$	$1+2\iota$	$2+\iota$	$1+\iota$	2	2ι	$2+2\iota$	ι	1
$2+2\iota$	$2+2\iota$	$1+\iota$	$1+2\iota$	ι	2	$2+\iota$	1	2ι

Z tabliczki tej można wyczytać, że każdy niezerowy element w $\mathbb{F}_3(\sqrt{2})$ jest odwracalny (czyli, że $\mathbb{F}_3(\sqrt{2})$ jest ciałem, porównaj D1.10) oraz, że każdy z elementów

$$1+\iota, \quad 1+2\iota, \quad 2+2\iota, \quad 2+\iota$$

jest generatorem ośmioelementowej grupy $\mathbb{F}_3(\sqrt{2})^* = \mathbb{F}_3(\sqrt{2}) \setminus \{0\}$. $\Diamond$

Ćwiczenie 9.38 Sprawdzić to.

Ćwiczenie 9.39 Rozwiązać równanie wielomianowe $x^3 + x^2 + \iota x + \iota = 0$ w $\mathbb{F}_3(\sqrt{2})$.

U w a g a. Gdy chcemy wyraźnie zaznaczyć zależność $\mathbb{F}_p(\iota)$ od wyboru pierwiastka pierwotnego g, to piszemy $\mathbb{F}_p(\sqrt{g})$. Zależność od wyboru g n i e j e s t jednak zbyt istotna, dlatego często oznaczamy zbiór $\mathbb{F}_p(\iota)$ jeszcze prostszym symbolem $\mathbb{F}_{p^2}$.

W zbiorze (pierścieniu) $\mathbb{F}_p(\iota)$ wprowadzimy jeszcze operację **sprzęgania w** $\mathbb{F}_p(\iota)$: jeżeli $\varphi = a + b\iota \in \mathbb{F}_p(\iota)$, to kładziemy

$$\overline{\varphi} = a - b\iota.$$

Ćwiczenie 9.40 Przekonać się, że dla dowolnych $\varphi, \chi \in \mathbb{F}_p(\iota)$ zachodzą równości

$$\overline{\varphi + \chi} = \overline{\varphi} + \overline{\chi}, \qquad \overline{\varphi \cdot \chi} = \overline{\varphi} \cdot \overline{\chi}.$$

Ćwiczenie 9.41 Udowodnić, że jeżeli funkcja $\Phi : \mathbb{F}_p(\iota) \longrightarrow \mathbb{F}_p(\iota)$ jest bijekcją spełniającą dwa warunki

$$\Phi(\alpha + \beta) = \Phi(\alpha) + \Phi(\beta), \qquad \Phi(\alpha\beta) = \Phi(\alpha)\Phi(\beta),$$

to albo $\Phi(\alpha) = \alpha$ dla każdego α albo $\Phi(\alpha) = \overline{\alpha}$ dla każdego α.

9.5.2 $\mathbb{F}_p(\iota)$ jest ciałem

W dwóch kolejnych twierdzeniach udowodnimy, że $\mathbb{F}_p(\iota)$ jest c i a ł e m, w którym każdy t r ó j m i a n k w a d r a t o w y o współczynnikach z ciała $\mathbb{Z}/p$ ma pierwiastki.

TWIERDZENIE 9.3 *Zbiór $\mathbb{F}_p(\iota)$ wraz z wprowadzonymi działaniami jest ciałem.*

D O W Ó D. Pokażemy, że jeżeli $0 \neq \alpha = a+b\iota \in \mathbb{F}_p(\iota)$, to istnieje taki element $\alpha^{-1} \in \mathbb{F}_p(\iota)$, że $\alpha\alpha^{-1} = 1$. Oznaczmy przez c warstwę odwrotną do $a^2 - b^2 g$ w $\mathbb{Z}/p$ i połóżmy $\alpha^{-1} = ac + (-bc)\iota$. Sprawdzenie, że $\alpha\alpha^{-1} = 1$, jest natychmiastowe. Pozostaje do sprawdzenia, że c istnieje, czyli, że $a^2 - b^2 g \neq 0$ w $\mathbb{Z}/p$. Gdyby $a^2 - b^2 g = 0$, to albo $b = 0$ i wtedy $a = 0$, co jest niemożliwe, bo $\alpha \neq 0$, albo $b \neq 0$ i wtedy $(ab^{-1})^2 = g$, co również jest niemożliwe, bo g, jako generator grupy $(\mathbb{Z}/p)^*$, nie jest kwadratem. Zauważmy, że α^{-1} obliczamy tak jak w przypadku liczb zespolonych: mnożąc licznik i mianownik przez element sprzężony:

$$\frac{1}{a+b\iota} = \frac{a-b\iota}{(a+b\iota)(a-b\iota)} = \frac{a-b\iota}{a^2-b^2g} = a(a^2-b^2g)^{-1} + (-b)(a^2-b^2g)^{-1}\iota.$$

To kończy dowód "ciałowości" pierścienia $\mathbb{F}_p(\iota)$. □

Powodem, dla którego tworzymy ciało $\mathbb{F}_p(\sqrt{g}) = \mathbb{F}_p(\iota)$, jest fakt, że w s z y s t k i e trójmiany kwadratowe $aX^2 + bX + c \in \mathbb{F}_p[X]$ m a j ą tam pierwiastki:

TWIERDZENIE 9.4 *Każde równanie kwadratowe $ax^2 + bx + c = 0$, gdzie a, b, $c \in \mathbb{Z}/p$, ma pierwiastki w $\mathbb{F}_p(\iota)$.*

D O W Ó D. Niech $a \neq 0$, b, $c \in \mathbb{Z}/p$ i niech $\Delta = b^2 - 4ac \in \mathbb{Z}/p$ będzie wyróżnikiem trójmianu kwadratowego $aX^2 + bX + c \in \mathbb{Z}/p[X]$. Możliwe są trzy przypadki:

$$(1)\ \left(\frac{\Delta}{p}\right) = +1, \qquad (2)\ \left(\frac{\Delta}{p}\right) = -1, \qquad (3)\ \left(\frac{\Delta}{p}\right) = 0,$$

czyli: Δ jest r e s z t ą k w a d r a t o w ą modulo p, albo Δ jest n i e r e s z t ą k w a d r a t o w ą modulo p, albo Δ jest z e r e m modulo p. W przypadku (1) mamy $\Delta = g^{2k}$ przy pewnym naturalnym k (reszty kwadratowe są, zobacz C5.69, parzystymi potęgami generatora), więc

$$\alpha = (2a)^{-1}(-b + g^k), \quad \beta = (2a)^{-1}(-b - g^k) \tag{9.43}$$

są (sprawdźcie!) różnymi pierwiastkami naszego trójmianu. W przypadku (2) mamy $\Delta = g^{2l+1}$ przy pewnym $l \in \mathbb{N}$ (niereszty kwadratowe są nieparzystymi potęgami generatora) i

$$\alpha = (2a)^{-1}(-b + g^l\iota), \quad \beta = (2a)^{-1}(-b - g^l\iota) \tag{9.44}$$

są (sprawdźcie!!) różnymi pierwiastkami naszego trójmianu. Wreszcie, w przypadku (3), $(2a)^{-1}(-b)$ jest, jak łatwo sprawdzić, pierwiastkiem (podwójnym) naszego trójmianu. □

U w a g a. Zauważmy, że trzy przypadki rozważone w dowodzie są doskonale analogiczne trzem przypadkom: (1) "delta dodatnia", (2) "delta ujemna", i (3) "delta równa zero", dla trójmianu kwadratowego o współczynnikach rzeczywistych.

Ćwiczenie 9.42 W którym miejscu istotnym było założenie, że $p > 2$?

9.5.3 Dwa słowa o grupie multyplikatywnej $\mathbb{F}_p(\iota)^*$

Jeżeli $\mathbb{K}$ jest dowolnym ciałem, to podzbiór $\mathbb{K}^*$ jego odwracalnych (czyli niezerowych!) elementów jest grupą względem mnożenia. Nazywamy ją **grupą multyplikatywną ciała** $\mathbb{K}$. W tym ustępie powiemy parę słów na temat grupy multyplikatywnej ciała $\mathbb{F}_p(\iota)$.

Przypomnijmy, zobacz C1.36, że jeżeli w grupie Γ istnieje taki element γ, że

$$\{\gamma^k : k \in \mathbb{Z}\} = \Gamma$$

(w przypadku addytywnym: $\{k\gamma : k \in \mathbb{Z}\} = \Gamma$), to grupę Γ nazywamy **grupą cykliczną**, a element γ nazywamy **generatorem** tej grupy.

P r z y k ł a d 1. Grupa $(\mathbb{Z}, +)$ liczb całkowitych z dodawaniem jest grupą cykliczną i ma (dokładnie) dwa generatory: 1 i -1. Jeżeli m jest taką liczbą naturalną, dla której istnieje pierwiastek pierwotny modulo m, zobacz D5.10, to grupa $(\mathbb{Z}/m)^*$ jest grupą cykliczną. Wiemy, zobacz T5.22, że to ma miejsce dla m równych 2, 4, p^e i $2p^e$. Grupa $\mu_n(\mathbb{C})$ pierwiastków z jedynki stopnia n jest grupą cykliczną. Jej generatorem jest element $\omega = \omega_n$ o najmniejszym dodatnim argumencie, zobacz (3.35). $\Diamond$

Ćwiczenie 9.43 Udowodnić, że element ω^k grupy $\mu_n(\mathbb{C})$ jest generatorem tej grupy wtedy i tylko wtedy, gdy $\mathrm{NWD}\,(k,\, n) = 1$. Porównaj też C5.38.

Ćwiczenie 9.44 Udowodnić, że grupa $(\mathbb{Z}/n, +)$ klas reszt liczb całkowitych modulo n z dodawaniem modulo n jest grupą cykliczną, a jej generatorami są te i tylko te warstwy $k\,(\mathrm{mod}\, n)$, dla których $\mathrm{NWD}\,(k,\, n) = 1$.

Ćwiczenie 9.45 Udowodnić, że grupy $(\mu_n(\mathbb{C}),\, \cdot)$ i $(\mathbb{Z}/n,\, +)$ są **izomorficzne**, to znaczy, że istnieje bijekcja $\varphi : \mathbb{Z}/n \longleftrightarrow \mu_n(\mathbb{C})$ spełniająca warunek $\varphi([k] + [l]) = \varphi([k]) \cdot \varphi([l])$ dla wszystkich $[k],\, [l] \in \mathbb{Z}/n$.

Ćwiczenie 9.46 Ile generatorów ma grupa cykliczna rzędu n?

TWIERDZENIE 9.5 *Grupa multyplikatywna $\mathbb{F}_p(\iota)^*$ jest grupą cykliczną.*

D O W Ó D. W części (1) dowodu T5.22 dowodzimy, że grupa multyplikatywna $(\mathbb{Z}/p)^*$ jest grupą cykliczną. Ten dowód można, bez istotnych zmian, "dopasować" do przypadku grupy $\mathbb{F}_p(\iota)^*$. Uważny Czytelnik zechce się samodzielnie o tym przekonać. $\square$

Ćwiczenie 9.47 Udowodnić, że jeżeli $0 \neq \alpha \in \mathbb{F}_p(\iota)$, to:

$$\alpha^{p^2-1} = 1. \tag{9.45}$$

Równość (9.45) jest analogonem kongruencji (5.11). Mogłaby więc być nazwana małym twierdzeniem Fermat'*a* w $\mathbb{F}_p(\iota)$. Wolimy jednak nazwać tak tezę poniższego twierdzenia:

TWIERDZENIE 9.6 (***Małe Twierdzenie Fermat'*a *w*** $\mathbb{F}_p(\iota)$) *Dla każdego elementu $\alpha \in \mathbb{F}_p(\iota)$ zachodzi równość:*

$$\boxed{\alpha^p = \overline{\alpha}.} \tag{9.46}$$

D O W Ó D. Mamy

$$(a+b\iota)^p = a^p + b^p\iota^p = a + b(\iota^2)^{\frac{p-1}{2}}\iota = a + bg^{\frac{p-1}{2}}\iota = a - b\iota.$$

Uzasadnienie tych równości jest natychmiastowe: pierwsza wynika z wzoru dwumiennego i C2.50, druga z MTF, trzecia z równości $\iota^2 = g$. Jasne jest też, że $g^{\frac{p-1}{2}} \equiv -1 \,(\mathrm{mod}\, p)$. □

Ćwiczenie 9.48 Udowodnić, że $\alpha^{p+1} = \overline{\alpha}^{p+1}$ dla dowolnego $\alpha \in \mathbb{F}_p(\iota)$.

U w a g a 1. Kluczowym momentem w części (1) dowodu T5.22, a więc i T9.5, było wykorzystanie faktu, że niezerowy wielomian o współczynnikach z c i a ł a ma w tym ciele co najwyżej tyle pierwiastków ile wynosi jego stopień, zobacz T3.4. To samo można więc zrobić w przypadku dowolnej s k o ń c z o n e j podgrupy grupy multyplikatywnej dowolnego ciała:

TWIERDZENIE 9.5′ *Jeżeli $\mathbb{K}$ jest ciałem, $\Lambda \subseteq \mathbb{K}^*$ jest podgrupą s k o ń c z o n ą grupy multyplikatywnej (niezerowych elementów) ciała $\mathbb{K}$, to Λ jest grupą cykliczną.* □

U w a g a 2. Grupa multyplikatywna $\mathbb{R}^*$ ciała liczb rzeczywistych n i e j e s t c y k l i c z n a. Również grupy $\mathbb{Q}^*$ i $\mathbb{C}^*$ nie są grupami cyklicznymi.

ZADANIE 9.11 Udowodnić, że grupa T liczb zespolonych o module równym 1, zobacz (5.40), nie jest grupą cykliczną.

R o z w i ą z a n i e. Niech $z \in T$ będzie dowolnym elementem. Pokażemy, że podgrupa (z) generowana przez z n i e jest równa całej grupie T. To wynika z porównania mocy, zobacz $\mathbb{KOM}$. Mianowicie, zbiór (z) jest s k o ń c z o n y (gdy $\pi/\mathrm{Arg}\, z$ jest liczbą wymierną – udowodnić!) lub n i e s k o ń c z o n y a l e p r z e l i c z a l n y (gdy $\pi/\mathrm{Arg}\, z$ jest liczbą niewymierną – udowodnić!), natomiast T jest zbiorem nieprzeliczalnym (udowodnić!). ◊

9.5.4 Wzory Eulera-Binet'a modulo p

Pokażemy teraz trzy przykłady wzorów Eulera-Binet'a modulo p. Badamy ciąg rekurencyjny (9.1), tym razem traktując zarówno współczynniki P, Q jak i same wyrazy a_n jako klasy reszt (liczb całkowitych) modulo p, gdzie p jest ustaloną liczbą pierwszą nieparzystą.

Zauważmy po pierwsze, że ciągi takie powstają zazwyczaj jako **redukcje modulo** p ciągów o wyrazach całkowitych. Zauważmy po drugie, że twierdzenie T9.2 i jego dowód przenoszą się bez żadnych istotnych zmian na rozważany teraz przypadek. Warunek $\Delta \neq 0$ należy oczywiście rozumieć modulo p, to znaczy $\Delta \not\equiv 0 \,(\mathrm{mod}\, p)$.

W trzech poniższych przykładach będziemy redukować modulo różne liczby pierwsze p jeden ustalony ciąg o wyrazach całkowitych. Wybraliśmy (bo przyda się nam później) ciąg (b_n) spełniający warunki początkowe $b_0 = 0$, $b_1 = 1$ i równanie rekurencyjne

$$b_{n+2} = b_{n+1} - 2b_n. \tag{9.47}$$

P r z y k ł a d 1. Niech $p = 79$. Wielomian charakterystyczny $X^2 - X + 2$ ma wyróżnik $\Delta = -7$. Sprawdzamy, który z trzech przypadków z T9.4 ma miejsce:

$$\left(\frac{\Delta}{79}\right) = \left(\frac{-7}{79}\right) = \left(\frac{-1}{79}\right)\left(\frac{7}{79}\right) = (-1)(-1)\left(\frac{79}{7}\right) = \left(\frac{2}{7}\right) = +1.$$

Widzimy, że $\Delta\mathbf{R}79$. Wobec tego równanie charakterystyczne $x^2 - x + 2 = 0$ ma dwa (różne) pierwiastki w $\mathbb{Z}/79$. Używając pierwiastka pierwotnego $g = -2$ modulo 79, po skończonej ilości mnożeń, znajdujemy kongruencję $\Delta = -7 \equiv (-2)^{62} \pmod{79}$. Stąd, zobacz (9.43), znajdujemy pierwiastki

$$\alpha = 2^{-1}(1 + (-2)^{31}) = 2^{-1}(1 + 25) = 13 \pmod{79}, \quad \beta = 2^{-1}(1 - 25) = -12 \pmod{79}$$

równania charakterystycznego w $\mathbb{Z}/79$. Wzory (9.13) dają teraz $A = -B = 19$. Wobec tego wzór Eulera-Binet'a dla ciągu $(b_n \pmod{79})$ wygląda tak:

$$b_n \equiv 19 \cdot 13^n - 19 \cdot (-12)^n \pmod{79}. \ \Diamond$$

Przykład 2. Rozważmy ten sam ciąg (b_n) modulo $p = 17$. Tym razem

$$\left(\frac{\Delta}{17}\right) = \left(\frac{-7}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{5}{17}\right) = (+1)\left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Zatem $\Delta\mathbf{N}17$, więc $\Delta \pmod{17}$ jest nieparzystą potęgą generatora (pierwiastka pierwotnego). Rzeczywiście: $g^3 \equiv 10 \pmod{17}$ dla $g = 3$. Wybraliśmy $g = 3$ dzięki naszej tabelce liczb pierwszych (mogliśmy byli też skorzystać z C5.63). Wzory (9.44) dają pierwiastki równania charakterystycznego (pamiętamy, że $\iota = \sqrt{3}$ w $\mathbb{F}_{17}(\iota)$):

$$\alpha = 2^{-1}(1 + 3\iota) = 9(1 + 3\iota) = 9 - 7\iota, \quad \beta = 2^{-1}(1 - 3\iota) = 9(1 - 3\iota) = 9 + 7\iota.$$

Wzory (9.13) dają w naszym przypadku:

$$A = (\alpha - \beta)^{-1} = (-14\iota)^{-1} = (3\iota)^{-1} = 2\iota, \quad B = -A.$$

Wzór Eulera-Binet'a dla ciągu $(b_n \pmod{17})$ wygląda więc tak:

$$b_n \pmod{17} = 2\iota(9 - 7\iota)^n - 2\iota(9 + 7\iota)^n. \ \Diamond$$

Przykład 3. Rozważmy jeszcze ten sam ciąg modulo $p = 7$. Mamy więc do czynienia z przypadkiem, gdy wielomian charakterystyczny $X^2 - X + 2$ ma pierwiastek podwójny:

$$\alpha \equiv \beta \equiv 4 \pmod{7}.$$

Wzory (9.13) dają więc $C = 0$, $D = 1$. Zaś wzór Eulera-Binet'a wygląda następująco:

$$b_n \equiv 4^{n-1}n \pmod{7}. \ \Diamond$$

Ćwiczenie 9.49 Napisać wzory Eulera-Binet'a dla redukcji modulo 5, 23 i 31 klasycznego ciągu Fibonacci'*ego*.

9.5.5 Okresowość ciągów rekurencyjnych modulo p

Powiemy słów parę o zjawisku okresowości ciągów rekurencyjnych modulo p.

Ćwiczenie 9.50 Udowodnić, że jeżeli $P, Q \in \mathbb{Z}$ i $(a_n) \in \mathcal{R}ek(P, Q)$ jest całkowitoliczbowy, to jego redukcja modulo m (to znaczy ciąg warstw $(a_n \pmod{m})$) jest ciągiem okresowym (od pewnego miejsca). Ponadto długość okresu jest $\leqslant m^2$.

Ćwiczenie 9.51 Udowodnić, że jeżeli dodatkowo Q jest odwracalna modulo m, to ciąg $(a_n \,(\mathrm{mod}\, m))$ jest czysto-okresowy.

Jak długi jest rzeczony okres? Oto odpowiedź częściowa:

TWIERDZENIE 9.7 *Dana jest liczba pierwsza $p > 2$. Niech $P, Q \in \mathbb{Z}$ oraz $p \nmid Q$. Załóżmy, że ciąg (a_n) liczb całkowitych spełnia równanie rekurencyjne* (9.1). *Oznaczmy przez Δ wyróżnik $P^2 + 4Q$ wielomianu charakterystycznego. Wówczas,*

(1) *jeżeli $\Delta \mathbf{R} p$, to dla każdego n zachodzi*

$$a_{n+p-1} \equiv a_n \,(\mathrm{mod}\, p), \tag{9.48}$$

(2) *jeżeli $\Delta \mathbf{N} p$, to dla każdego n zachodzi*

$$a_{n+p+1} \equiv -Q a_n \,(\mathrm{mod}\, p), \tag{9.49}$$

(3) *jeżeli $\Delta \equiv 0 \,(\mathrm{mod}\, p)$, to dla każdego n zachodzi*

$$a_{n+p} \equiv 2^{-1} P a_n \,(\mathrm{mod}\, p). \tag{9.50}$$

DOWÓD. **(1)** Wiemy, że w tym przypadku istnieją dwa (różne!) pierwiastki $\alpha, \beta \in \mathbb{Z}/p$ wielomianu charakterystycznego (9.2) modulo p i istnieją takie elementy $A, B \in \mathbb{Z}/p$, że dla każdego $n \geqslant 0$ zachodzi równość Eulera-Binet'a:

$$a_n = A\alpha^n + B\beta^n \tag{9.51}$$

w ciele $\mathbb{Z}/p$. Wobec tego mamy:

$$a_{n+p-1} = A\alpha^{n+p-1} + B\beta^{n+p-1} = A\alpha^n\alpha^{p-1} + B\beta^n\beta^{p-1} = A\alpha^n + B\beta^n = a_n.$$

Kluczem jest tu oczywiście równość $\varphi^{p-1} = 1$ prawdziwa dla n i e z e r o w y c h $\varphi \in \mathbb{Z}/p$ (jest to doskonale nam znane MTF!). Zauważmy, że założenie $p \nmid Q$ implikuje niezerowość pierwiastków α, β w $\mathbb{Z}/p$.

(2) W tym przypadku równanie charakterystyczne ma dwa różne pierwiastki α, β w ciele $\mathbb{F}_p(\iota)$, przy czym, zobacz wzory (9.44), są one wzajemnie sprzężone: $\beta = \overline{\alpha}$, $\alpha = \overline{\beta}$. Równość (9.51) ma również miejsce, chociaż tym razem stałe A, B są elementami ciała $\mathbb{F}_p(\iota)$. Wobec tego, na mocy MTF w $\mathbb{F}_p(\iota)$, zobacz (9.46), mamy:

$$a_{n+p+1} = A\alpha^n\alpha^p\alpha + B\beta^n\beta^p\beta = A\alpha^n\beta\alpha + B\beta^n\alpha\beta = \alpha\beta(A\alpha^n + B\beta^n) = -Qa_n.$$

(3) W tym przypadku, zobacz T9.4, $\alpha = \beta = 2^{-1}P$ jest podwójnym pierwiastkiem wielomianu charakterystycznego. Istnieją więc takie stałe C, $D \in \mathbb{Z}/p$, że zachodzi równość

$$a_n = C\alpha^n + Dn\alpha^{n-1}$$

dla każdego $n \geqslant 0$. Wobec tego $a_{n+p} = C\alpha^{n+p} + D(n+p)\alpha^{n+p-1} = \alpha^p(C\alpha^n + Dn\alpha^{n-1}) = \alpha a_n$, na mocy równości $\alpha^p = \alpha$ prawdziwej dla każdego $\alpha \in \mathbb{Z}/p$ (zobacz (5.12)). To kończy dowód równości (9.50), bo $\alpha = 2^{-1}P$. □

Łatwo stąd wyciągnąć taki:

WNIOSEK *Ciąg* $(a_n \,(\mathrm{mod}\, p))$ *jest okresowy, przy czym długość okresu jest*

(1) *dzielnikiem liczby* $p-1$, *gdy* $\Delta \mathbf{R} p$,

(2) *dzielnikiem liczby* $k(p+1)$, *gdy* $\Delta \mathbf{N} p$. *Tu* $k = \mathrm{rz}_p(-Q)$,

(3) *dzielnikiem liczby* lp, *gdy* $\Delta \equiv 0 \,(\mathrm{mod}\, p)$. *Tu* $l = \mathrm{rz}_p(2^{-1}P)$.

Ćwiczenie 9.52 Udowodnić te tezy. W przypadku **(3)** należy zauważyć, że l istnieje.

Ćwiczenie 9.53 Niech $(a_n) \in \mathcal{R}ek(1,\,1)$ będzie ciągiem Fibonacci'*ego* o wyrazach początkowych $a_0 = 2$, $a_1 = 1$. Udowodnić, że jeżeli $a_{2k} \equiv 2 \,(\mathrm{mod}\, p)$, to $a_{2k+1} \equiv 1 \,(\mathrm{mod}\, p)$.

Ćwiczenie 9.54 Niech $p \in \mathbb{P}_{>2}$ i niech (f_n) będzie klasycznym ciągiem Fibonacci'*ego*. Udowodnić, że **(1)** jeżeli $p \equiv \pm 1 \,(\mathrm{mod}\, 5)$, to $p | f_{p-1}$; **(2)** jeżeli $p \equiv \pm 2 \,(\mathrm{mod}\, 5)$, to $p | f_{p+1}$.

Ćwiczenie 9.55 Udowodnić, że jeżeli $p > 5$ jest liczbą pierwszą, to zachodzi

$$f_p \equiv \left(\frac{5}{p}\right) \,(\mathrm{mod}\, p),$$

gdzie $\left(\frac{5}{p}\right)$ jest symbolem Legendre'*a*.

Rozdział 10

Pierścienie kwadratowe

Gauss reconnut qu'il n'y a pas de résultat simple à espérer
en restant dans le domaine des entiers ordinaires
et qu'il faut passer aux entiers "complexes" $a + b\sqrt{-1}$.
(André Weil w liście do siostry Simone)

Dotychczas do badania pierścienia liczb całkowitych używaliśmy pierścieni skończonych $\mathbb{Z}/m$ klas reszt liczb całkowitych modulo m. Są to **pierścienie ilorazowe** pierścienia $\mathbb{Z}$. Obecnie chcemy pokazać jak można wykorzystać pewne **nadpierścienie** pierścienia $\mathbb{Z}$ zawarte w zbiorze (ciele) liczb zespolonych.

Ustalmy bezkwadratową liczbę całkowitą $D \neq 1$. Przez $\mathbb{Q}(\sqrt{D})$ oznaczamy zbiór wszystkich liczb zespolonych postaci

$$\alpha = x + y\sqrt{D}, \tag{10.1}$$

gdzie $x, y \in \mathbb{Q}$. Umawiamy się, że $\sqrt{D}$ oznacza **pierwiastek arytmetyczny** (dodatni), gdy $D > 0$, oraz $\sqrt{D} = i\sqrt{-D}$, gdy $D < 0$. Zbiór $\mathbb{Q}(\sqrt{D})$ (czyt. $\mathbb{Q}$ *rozszerzone o* $\sqrt{D}$) wraz ze zwykłymi działaniami dodawania i mnożenia nazywamy **ciałem kwadratowym** .

Ćwiczenie 10.1 Uzasadnić, że $\mathbb{Q}(\sqrt{D})$ jest ciałem.

Jeżeli $\alpha = x + y\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, to liczbę $\alpha' := x - y\sqrt{D}$ nazywamy **liczbą sprzężoną** liczby α. Zauważmy, że $\alpha' = \overline{\alpha}$ (sprzężenie zespolone) w przypadku gdy $D < 0$.

Ćwiczenie 10.2 Uzasadnić, że jeżeli $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$, to $\alpha' + \beta' = (\alpha + \beta)'$, $\alpha' - \beta' = (\alpha - \beta)'$, $\alpha'\beta' = (\alpha\beta)'$ oraz $\alpha'/\beta' = (\alpha/\beta)'$ dla $\beta \neq 0$. Porównaj C1.22.

Liczbę $\alpha\alpha' = x^2 - Dy^2$ oznaczamy symbolem $\mathbf{N}(\alpha)$ i nazywamy **normą** liczby α.

Ćwiczenie 10.3 Uzasadnić, że $\mathbf{N}(\alpha) = 0$ wtedy i tylko wtedy, gdy $\alpha = 0$. Uzasadnić ponadto, że norma jest ściśle multyplikatywna. To znaczy, że dla $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$:

$$\boxed{\boxed{\mathbf{N}(\alpha\beta) = \mathbf{N}(\alpha)\,\mathbf{N}(\beta).}} \tag{10.2}$$

10.1 Pierścień liczb całkowitych Gaussa

Najprostszym przykładem pierścienia kwadratowego jest pierścień liczb całkowitych Gaussa.

10.1.1 Definicja i podstawowe własności

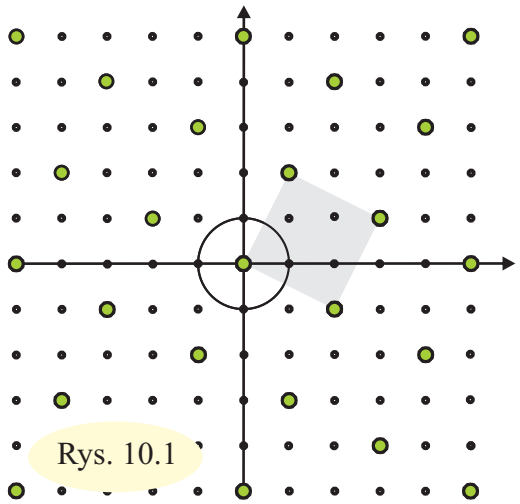
Pierścień liczb całkowitych Gaussa jest **podpierścieniem** w $\mathbb{Q}(\sqrt{-1})$.

Zakładamy, że Czytelnik rozumie geometryczną naturę liczb zespolonych na tyle, że poniższe ćwiczenie jest w stanie rozwiązać w czasie około 2 minut:

Ćwiczenie 10.4 Przedstawić liczby i^{-2013}, $(1+i)^8$, $(1-i)^8$ w postaci $a+bi$. Wyznaczyć pole czworokąta wypukłego o wierzchołkach $2-\alpha$, $2-i\alpha$, $2+\alpha$, $2+i\alpha$, gdzie $\alpha = 3+4i$.

Definicja 10.1 Liczba zespolona $a+bi$ nazywa się **liczbą całkowitą Gaussa**, gdy a, b są (zwykłymi) liczbami całkowitymi. Zbiór wszystkich liczb całkowitych Gaussa oznaczamy symbolem $\mathbb{Z}[\,i\,]$ i nazywamy **pierścieniem (liczb całkowitych) Gaussa**.

Ilustracją geometryczną zbioru liczb całkowitych Gaussa jest krata Gaussa, o której wspominaliśmy już parokrotnie (zobacz też ogólną definicję kraty na płaszczyźnie w ustępie 8.3.1). Na rysunku 10.1 widzimy **kratę Gaussa** i zaznaczoną grubszymi kółeczkami **podkratę** generowaną przez dwie liczby $2-i$, $1+2i$, oraz jeden z jej obszarów fundamentalnych, zobacz D8.3.



Rys. 10.1

Norma liczby całkowitej Gaussa jest kwadratem odległości tej liczby od zera.

Ćwiczenie 10.5 Udowodnić, że dla danej liczby $\alpha \in \mathbb{Z}[\,i\,]$ norma $\mathbf{N}(\alpha)$ jest równa polu kwadratu o wierzchołkach 0, α, $i\alpha$ oraz $\alpha+i\alpha$.

Badanie każdego pierścienia zaczynamy od wyznaczenia grupy elementów odwracalnych.

ZADANIE 10.1 Wyznaczyć grupę jedności $\mathbb{Z}[\,i\,]^*$ w pierścieniu liczb całkowitych Gaussa.

Rozwiązanie. Załóżmy, że $\xi = x+yi \in \mathbb{Z}[\,i\,]^*$, zobacz D1.8. To oznacza, że istnieje taka liczba $\eta \in \mathbb{Z}[\,i\,]$, że $\xi\eta = 1$. Wówczas, na mocy (10.2), $\mathbf{N}(\xi)\mathbf{N}(\eta) = 1$, więc $\mathbf{N}(\xi) = 1$, czyli $x^2+y^2 = 1$. To równanie ma cztery rozwiązania: $(1,\,0)$, $(-1,\,0)$, $(0,\,1)$ i $(0,\,-1)$. Odpowiadają one liczbom 1, -1, i $-i$, z których każda jest (!) jednością w $\mathbb{Z}[\,i\,]$. Przeto:

$$\mathbb{Z}[\,i\,]^* = \{\xi \in \mathbb{Z}[\,i\,] : \mathbf{N}(\xi) = 1\} = \{1,\, i,\, -1,\, -i\} = \{i^0,\, i,\, i^2,\, i^3\}.$$

Widzimy, że jedności w pierścieniu liczb całkowitych Gaussa są punktami kraty Gaussa leżącymi na okręgu jednostkowym (o środku w zerze), zobacz rysunek 10.1. Tworzą one grupę $\mu_4(\mathbb{C})$ pierwiastków czwartego stopnia z jedynki, zobacz C1.35. $\Diamond$

Ćwiczenie 10.6 Uzasadnić, że w pierścieniu Gaussa $\mathbb{Z}[\,i\,]$ nie ma dzielników zera, to znaczy, że równość $\alpha\beta = 0$ implikuje $\alpha = 0$ lub $\beta = 0$. Wywnioskować stąd **prawo skracania**: *Jeżeli* $\alpha\beta = \alpha\gamma$ *i* $\alpha \neq 0$, *to* $\beta = \gamma$.

10.1.2 Dzielenie z resztą i podzielność w $\mathbb{Z}[i]$

Pamiętamy jak duże usługi oddało nam **dzielenie z resztą** w pierścieniu $\mathbb{Z}$ zwykłych liczb całkowitych. Bardzo obiecującym jest fakt, że w pierścieniu liczb całkowitych Gaussa również istnieje możliwość dzielenia z resztą.

TWIERDZENIE 10.1 *Jeżeli* $\alpha, \beta \in \mathbb{Z}[i]$ *i* $\beta \neq 0$, *to istnieje taka para* $\varphi, \varrho \in \mathbb{Z}[i]$, *że*

$$\boxed{\alpha = \varphi\beta + \varrho \qquad \text{oraz} \qquad \mathbf{N}(\varrho) < \mathbf{N}(\beta).} \tag{10.3}$$

D O W Ó D. Niech $\alpha/\beta = s + ti$, gdzie $s, t \in \mathbb{Q}$. Wybierzmy takie liczby całkowite k, l, by $|s-k| \leqslant 1/2$ i $|t-l| \leqslant 1/2$ i połóżmy $\varphi = k + li$. Wówczas

$$\mathbf{N}(\alpha - \varphi\beta) = \mathbf{N}(\beta)\mathbf{N}(\alpha\beta^{-1} - \varphi) \tag{10.4}$$

Ale

$$\mathbf{N}(\alpha\beta^{-1} - \varphi) = \mathbf{N}(s + ti - (k + li)) = (s-k)^2 + (t-l)^2 \leqslant \frac{1}{4} + \frac{1}{4} < 1.$$

To, wobec równości (10.4), daje nierówność $\mathbf{N}(\alpha - \varphi\beta) < \mathbf{N}(\beta)$. Wystarczy więc położyć $\varrho = \alpha - \varphi\beta$. □

Występujące w (10.3) liczby φ i ϱ nazywamy odpowiednio (niepełnym) **ilorazem** i **resztą** z dzielenia α przez β. Należy tu zwrócić uwagę, że, w przeciwieństwie do twierdzenia T2.2, gdzie wykazaliśmy jedyność ilorazu i reszty, tym razem n i e o c z e k u j e m y jednoznaczności.

P r z y k ł a d. Niech $\alpha = 11-5i, \beta = 7-i$. Wówczas

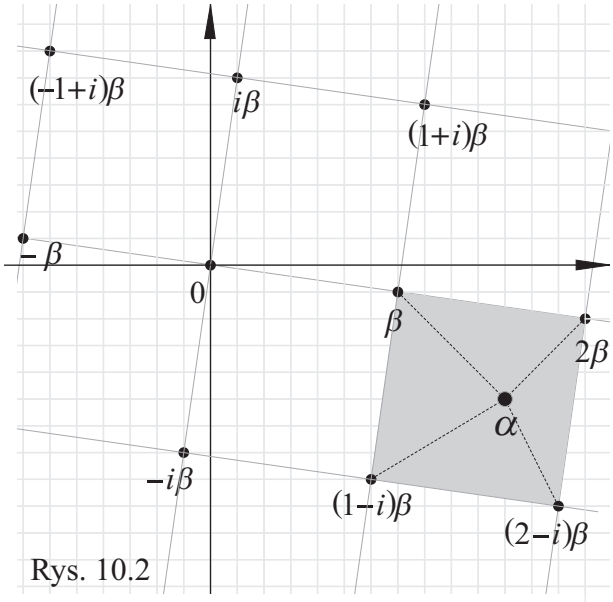
$$\frac{\alpha}{\beta} = \frac{11-5i}{7-i} = \frac{41}{25} - \frac{12}{25}i.$$

Zatem kładziemy $\varphi = 2$ i znajdujemy

$$11 - 5i = 2(7-i) + (-3-3i),$$

przy czym $\mathbf{N}(-3-3i) = 18 < 50 = \mathbf{N}(\beta)$. Zauważmy, że możemy napisać również

$$11 - 5i = (2-i)(7-i) + (-2+4i),$$
$$11 - 5i = 1(7-i) + (4-4i),$$
$$11 - 5i = (1-i)(7-i) + (5+3i)$$



Rys. 10.2

Każda z tych równości jest prawidłowym dzieleniem z resztą w $\mathbb{Z}[i]$, bowiem $\mathbf{N}(-2+4i) = 20$, $\mathbf{N}(4-4i) = 32$ i $\mathbf{N}(5+3i) = 34$. Geometryczną treść dzielenia z resztą w pierścieniu $\mathbb{Z}[i]$ zobaczyć można na rysunku 10.2. Widzimy na nim kratę wszystkich liczb postaci $\varphi\beta$ (wielokrotności β w pierścieniu Gaussa). Liczba α "wpada" do jednego kwadratu tej kraty – w naszym przykładzie jest to kwadrat o wierzchołkach β, 2β, $(2-i)\beta$ i $(1-i)\beta$. Wybierając taki

wierzchołek tego kwadratu, którego odległość od α jest mniejsza od długości boku kwadratu znajdujemy iloraz φ (w naszym przykładzie wszystkie cztery wierzchołki są odpowiednie – ale tak, oczywiście, nie musi być zawsze!). Normą reszty ϱ jest kwadrat odległości wybranego wierzchołka od α. $\Diamond$

Definicja 10.2 Jeżeli $\alpha, \beta \in \mathbb{Z}[i]$, to mówimy, że α **dzieli** β, gdy istnieje taka liczba $\varphi \in \mathbb{Z}[i]$, że $\beta = \varphi\alpha$. Piszemy wtedy $\alpha|\beta$. Mówimy też w takiej sytuacji, że α jest **dzielnikiem** β, lub że β jest **wielokrotnością** α. Jeżeli $\alpha \in \mathbb{Z}[i]$, to zbiór

$$(\alpha) := \{\varphi\alpha : \varphi \in \mathbb{Z}[i]\} \tag{10.5}$$

wszystkich wielokrotności liczby α nazywamy **ideałem głównym** generowanym przez α.

Sprawdzenie, czy dana liczba $\alpha \in \mathbb{Z}[i]$ dzieli daną liczbę $\beta \in \mathbb{Z}[i]$ jest bardzo proste: znajdujemy iloraz α/β w zbiorze (wszystkich) liczb zespolonych, przedstawiamy go w postaci $x + yi$ i sprawdzamy, czy $x, y \in \mathbb{Z}$.

Ćwiczenie 10.7 Sprawdzić, że $(1+i)|(3+3i)$, $(1+i)|2$, $(2-i)|5$, $(3+4i)|(5+10i)$ oraz $(2-3i) \nmid (2+3i)$.

Ćwiczenie 10.8 Udowodnić, że $\alpha|\beta$ wtedy i tylko wtedy, gdy $\alpha'|\beta'$.

Ćwiczenie 10.9 Uzasadnić, że jeżeli $\alpha|\beta$ w $\mathbb{Z}[i]$, to $\mathbf{N}(\alpha)|\mathbf{N}(\beta)$.

Ćwiczenie 10.10 Dowieść, że jeżeli $\alpha \neq 0$, to $\alpha|\alpha'$ wtedy i tylko wtedy, gdy $\alpha \in \mathbb{Z}$ lub $|\mathrm{Re}(\alpha)| = |\mathrm{Im}(\alpha)|$ lub $\alpha \in \mathbb{Z}i$. [Jasne, że przez $\mathbb{Z}i$ oznaczamy $\{\xi \in \mathbb{Z}[i] : \mathrm{Re}(\xi) = 0\}$, a przez $\mathbb{Z}$ oznaczamy tu $\{\xi \in \mathbb{Z}[i] : \mathrm{Im}(\xi) = 0\}$.]

Ćwiczenie 10.11 Sformułować i udowodnić analogony tez **(1), (2), (3), (4)** z T2.1 w przypadku $\mathbb{Z}[i]$. *Wskazówka.* **(1)** powinna zawierać zdanie "$\varepsilon|\alpha$ dla każdego $\varepsilon \in \mathbb{Z}[i]^*$". Również tezę **(3)** należy odpowiednio zmodyfikować.

Definicja 10.3 Jeżeli $\alpha, \beta \in \mathbb{Z}[i]$ i istnieje taka jedność $\varepsilon \in \mathbb{Z}[i]^*$, że $\alpha\varepsilon = \beta$, to mówimy, że liczby α i β są **stowarzyszone** w $\mathbb{Z}[i]$. Zapisujemy to tak $\alpha \sim \beta$. Geometrycznie oznacza to, że β da się uzyskać z α przez obrót wokół zera o kąt 0°, $\pm 90^\circ$ lub 180°.

Ćwiczenie 10.12 Udowodnić, że α jest jednością wtedy i tylko wtedy, gdy $\alpha \sim 1$.

Ćwiczenie 10.13 Uzasadnić, że jeżeli $\alpha, \beta \in \mathbb{Z}[i]$, to $\alpha|\beta \Leftrightarrow (\beta) \subseteq (\alpha)$. Wywnioskować stąd, że $(\alpha) = (\beta) \Leftrightarrow \alpha \sim \beta$.

Ćwiczenie 10.14 "Narysować" ideały główne $(1+i)$, (2), $(3-2i)$ w $\mathbb{Z}[i]$.

Ćwiczenie 10.15 Udowodnić, że jeżeli $\alpha \neq 0$, to ideał główny (α) w interpretacji geometrycznej jest kratą $\Lambda(\alpha, i\alpha)$, porównaj D8.2.

Już dwa razy definiowaliśmy ideał w pierścieniu: po raz pierwszy w pierścieniu $\mathbb{Z}$ (zwykłych) liczb całkowitych (zobacz D2.2), po raz drugi w p i e r ś c i e n i a c h wielomianów $\mathbb{K}[X]$ (zobacz D3.12). Zrobimy to po raz trzeci:

Definicja 10.4 Podzbiór $I \subseteq \mathbb{Z}[i]$ nazywamy **ideałem**, gdy zawiera liczbę 0 oraz spełnia poniższe dwa warunki:

(1) jeżeli $\alpha \in I$ i $\beta \in I$, to $\alpha + \beta \in I$,

(2) jeżeli $\varphi \in \mathbb{Z}[i]$ i $\alpha \in I$, to $\varphi\alpha \in I$.

W preambule do rozdziału 2 wymieniliśmy pięć wniosków, które można wyprowadzić z możliwości wykonywania dzielenia z resztą w pierścieniu $\mathbb{Z}$. Podobną sytuację widzieliśmy w paragrafie 3.3 w odniesieniu do pierścieni $\mathbb{K}[X]$ wielomianów (jednej zmiennej) o współczynnikach w ciele. Najbardziej fundamentalnym z tych wniosków jest fakt dig'owości pierścienia (zobacz T2.3 i T3.11). W pierścieniu $\mathbb{Z}[i]$ rzecz ma się podobnie:

TWIERDZENIE 10.2 *Każdy ideał w pierścieniu $\mathbb{Z}[i]$ jest ideałem głównym.*

DOWÓD. Jeżeli I składa się z jednego tylko elementu, czyli $I = \{0\}$, to $I = (0)$. Jeżeli I zawiera liczby różne od zera, to zawiera liczbę o najmniejszej normie dodatniej (Zasada Minimum!). Niech $\delta \in I$ będzie taką liczbą. Twierdzimy, że wówczas $I = (\delta)$. Aby to zobaczyć sprawdzamy, że (1) $(\delta) \subseteq I$, i (2) $I \subseteq (\delta)$. Pierwsze zawieranie jest natychmiastowym wnioskiem warunku D10.4(2). Aby uzasadnić zawieranie przeciwne wybierzmy dowolną liczbę $\alpha \in I$. Dzieląc ją z resztą przez δ znajdujemy rozkład $\alpha = \varphi\delta + \varrho$. Stąd $\varrho = \alpha - \varphi\delta \in I$, bo $\alpha \in I$ i $\delta \in I$. Ale $\mathbf{N}(\varrho) < \mathbf{N}(\delta)$, zatem $\mathbf{N}(\varrho) = 0$, więc $\varrho = 0$, czyli $\alpha = \varphi\delta$. Zatem $I \subseteq (\delta)$. □

W kolejnych czterech ćwiczeniach proponujemy Czytelnikowi aby zechciał sprawdzić, że analogony innych, wymienionych w preambule do rozdziału 2, wniosków z dig'owości mają miejsce w pierścieniu liczb całkowitych Gaussa. Oczywiste jest przy tym, że przyjmujemy następującą definicję:

Definicja 10.5 Załóżmy, że $\alpha, \beta \in \mathbb{Z}[i]$. **Największym wspólnym dzielnikiem** pary (α, β) nazywamy taki wspólny dzielnik liczb α i β, który jest dzielnikiem każdego wspólnego dzielnika tych liczb. Porównaj D2.4 i D3.9.

Ćwiczenie 10.16 Udowodnić, że każde dwie (nie równe jednocześnie zero) liczby całkowite Gaussa mają największy wspólny dzielnik i jest on wyznaczony jednoznacznie z dokładnością do relacji stowarzyszenia. *Wskazówka.* Zobacz T2.4 i T3.11.

Dla wskazania, że δ (i każda liczba stowarzyszona z δ) jest największym wspólnym dzielnikiem pary, (α, β) piszemy $\mathrm{NWD}\,(\alpha, \beta) \sim \delta$. Mówimy, że α i β są **względnie pierwsze** w $\mathbb{Z}[i]$, gdy $\mathrm{NWD}\,(\alpha, \beta) \sim 1$.

Ćwiczenie 10.17 Udowodnić, że jeżeli $\alpha, \beta \in \mathbb{Z}[i]$ nie są jednocześnie równe zero, to największy wspólny dzielnik α i β da się zapisać w postaci kombinacji liniowej $\alpha\xi + \beta\zeta$ dla pewnych $\xi, \zeta \in \mathbb{Z}[i]$. *Wskazówka.* Zobacz T2.6 i T3.11.

Ćwiczenie 10.18 Sformułować i udowodnić Zasadnicze Twierdzenie Arytmetyki w pierścieniu $\mathbb{Z}[i]$. *Wskazówka.* Zobacz T2.7 i T3.12.

Ćwiczenie 10.19 Udowodnić, że jeżeli $\alpha, \beta \in \mathbb{Z}[i]$ oraz $\alpha^n | \beta^n$ dla $n \geqslant 1$, to $\alpha | \beta$. *Wskazówka.* Zobacz Z2.3.

10.1.3 Algorytm Euklidesa w $\mathbb{Z}[\,i\,]$

Poznany przez nas algorytm Euklidesa w pierścieniu $\mathbb{Z}$ (zobacz T2.11) i w pierścienich $\mathbb{K}[X]$ (zobacz C3.29) może być bez żadnych istotnych zmian uzasadniony również w pierścieniu liczb całkowitych Gaussa. We wszystkich tych sytuacjach algorytm Euklidesa pozwala wyznaczyć NWD dwóch elementów za pomocą skończonej ilości dzieleń z resztą.

Ćwiczenie 10.20 Uzasadnić, że jeżeli w $\mathbb{Z}[\,i\,]$ zachodzi równość $\alpha = \varphi\beta + \varrho$, to $D(\alpha,\, \beta) = D(\beta,\, \varrho)$. *Wskazówka.* Zobacz T2.10.

Ćwiczenie 10.21 Sformułować i udowodnić algorytm Euklidesa w pierścieniu $\mathbb{Z}[\,i\,]$.

ZADANIE 10.2 Udowodnić, że jeżeli $a \in \mathbb{Z}$, to

$$\mathrm{NWD}\,(a+i,\, a-i) \sim \begin{cases} 1, & \text{gdy} \quad 2|a, \\ 1+i, & \text{gdy} \quad 2 \nmid a. \end{cases}$$

R o z w i ą z a n i e. Jeżeli $a = 2k$ jest różną od zera liczbą parzystą, to algorytm Euklidesa wygląda następująco:

$$\begin{aligned} a+i &= 1\cdot(a-i) + 2i, & \mathbf{N}(2i) &< \mathbf{N}(a-i), \\ a-i &= (-ki)\cdot(2i) - i, & \mathbf{N}(-i) &< \mathbf{N}(2i), \\ 2i &= (-2)\cdot(-i) + 0. \end{aligned}$$

Zatem, w tym przypadku, $\mathrm{NWD}\,(a+i,\, a-i) \sim -i \sim 1$.

Jeżeli $a = 2k+1$ jest różną od ± 1 liczbą nieparzystą, to algorytm Euklidesa ma postać:

$$\begin{aligned} a+i &= 1\cdot(a-i) + 2i, & \mathbf{N}(2i) &< \mathbf{N}(a-i), \\ a-i &= (-ki)\cdot(2i) + (1-i), & \mathbf{N}(1-i) &< \mathbf{N}(2i), \\ 2i &= (-1+i)\cdot(1-i) + 0. \end{aligned}$$

Skąd, w tym przypadku, $\mathrm{NWD}\,(a+i,\, a-i) \sim 1-i \sim 1+i$. Oczywiste przypadki $a = 0$ i $a = \pm 1$ pozostawiamy Czytelnikowi. $\Diamond$

Ćwiczenie 10.22 Wykonać algorytm Euklidesa dla elementów $11 - 5i$, $7 - i$.

10.1.4 Liczby pierwsze w $\mathbb{Z}[\,i\,]$

Liczbę pierwszą w pierścieniu $\mathbb{Z}$ (zwykłych) liczb całkowitych definiujemy w szkole jako taką (dodatnią!) liczbę $p \in \mathbb{Z}$, która ma d o k ł a d n i e cztery dzielniki w $\mathbb{Z}$: 1, -1, p, $-p$, zobacz D2.7. To oznacza, że jej jedynymi rozkładami na iloczyn dwóch czynników są rozkłady trywialne: takie, w których jednym z czynników jest element odwracalny.

Przyjmijmy taką definicję:

Definicja 10.6 Liczba całkowita Gaussa $\nu \in \mathbb{Z}[\,i\,]$ nie będąca zerem ani jednością nazywa się **liczbą nierozkładalną Gaussa**, gdy spełnia warunek:

$$\boxed{\boxed{\text{jeżeli} \quad \nu = \alpha\beta, \quad \text{to} \quad \alpha \sim 1 \quad \text{lub} \quad \beta \sim 1.}} \tag{10.6}$$

W twierdzeniu T2.15 pokazaliśmy, że liczba pierwsza w $\mathbb{Z}$ może być z dokładnością do znaku s c h a r a k t e r y z o w a n a przez warunek (2.16). Wygodnie jest taki warunek przyjąć za d e f i n i c j ę pierwszości. Tak zrobimy teraz:

Definicja 10.7 Liczbę $\pi \in \mathbb{Z}[\,i\,]$ nazywamy **liczbą pierwszą Gaussa**, gdy $\mathbf{N}(\pi) > 1$ i spełniony jest warunek:

$$\boxed{\boxed{\text{jeżeli} \quad \pi|\alpha\beta, \quad \text{to} \quad \pi|\alpha \quad \text{lub} \quad \pi|\beta.}} \tag{10.7}$$

P r z y k ł a d. (1) Liczba 2 n i e jest liczbą pierwszą Gaussa. Istotnie, $2|(1+i)(1-i)$, ale $2 \nmid (1+i)$ (bo $\mathbf{N}(2) = 4$, $\mathbf{N}(1+i) = 2$ – porównaj C10.9) oraz $2 \nmid (1-i)$.

(2) Liczba 3 j e s t liczbą pierwszą Gaussa. Załóżmy bowiem, że $3|\alpha\beta$ dla $\alpha, \beta \in \mathbb{Z}[\,i\,]$. Wówczas, zobacz C10.9, $9|\mathbf{N}(\alpha)\mathbf{N}(\beta)$. Stąd $3|\mathbf{N}(\alpha)\mathbf{N}(\beta)$, więc $3|\mathbf{N}(\alpha)$ lub $3|\mathbf{N}(\beta)$, bo 3 jest (zwykłą) liczbą pierwszą, zobacz (2.16). Niech $\alpha = a + bi$ i niech $3|\mathbf{N}(\alpha)$, czyli $3|a^2 + b^2$. Z dowodu T8.2 wiemy, że wówczas $3|a$ i $3|b$. Zatem $\alpha = 3a_1 + 3b_1 i = 3(a_1 + b_1 i)$, więc $3|\alpha$.

(3) Liczba 5 n i e jest liczbą pierwszą Gaussa. Istotnie $5|(2+i)(2-i)$, ale $5 \nmid (2+i)$ oraz $5 \nmid (2-i)$, co sprawdzamy przez porównanie norm. ◊

Przed dowodem (bardzo ważnego) twierdzenia T10.3 rozwiążmy takie ćwiczenie:

Ćwiczenie 10.23 Udowodnić, że jeżeli ν jest liczbą nierozkładalną w $\mathbb{Z}[\,i\,]$, to dla danego $\alpha \in \mathbb{Z}[\,i\,]$, albo $\nu|\alpha$, albo $\mathrm{NWD}\,(\nu,\, \alpha) \sim 1$. *Wskazówka.* Zobacz C2.32 i C3.35.

TWIERDZENIE 10.3 *Liczba całkowita Gaussa nie będąca zerem ani jednością jest liczbą nierozkładalną Gaussa wtedy i tylko wtedy, gdy jest liczbą pierwszą Gaussa.*

D O W Ó D. ($\Longrightarrow$) Niech ν będzie liczbą nierozkładalną Gaussa i niech $\nu|\alpha\beta$. Mamy wykazać, że $\nu|\alpha$ lub $\nu|\beta$. To jest oczywistym wnioskiem z C10.23: gdyby $\nu \nmid \alpha$, to musiałoby być $\mathrm{NWD}\,(\alpha,\, \nu) \sim 1$, więc, na mocy ZTA, zobacz C10.18, $\nu|\beta$.

($\Longleftarrow$) Załóżmy, że π jest liczbą pierwszą w $\mathbb{Z}[\,i\,]$ i że $\pi = \alpha\beta$ jest jej rozkładem na iloczyn w $\mathbb{Z}[\,i\,]$. Wówczas $\pi|\alpha$ lub $\pi|\beta$. Niech $\pi|\alpha$, czyli niech $\alpha = \pi\gamma$ dla pewnego $\gamma \in \mathbb{Z}[\,i\,]$. Stąd $\pi \cdot 1 = \pi = \pi\gamma\beta$, więc, na mocy prawa skracania, $1 = \gamma\beta$. Zatem β jest jednością. □

Ćwiczenie 10.24 Udowodnić, że π jest liczbą pierwszą Gaussa wtedy i tylko wtedy, gdy liczba sprzężona π' jest liczbą pierwszą Gaussa.

Ćwiczenie 10.25 Uzasadnić, że jeżeli $\mathbf{N}(\xi) \in \mathbb{P}$, to ξ jest liczbą pierwszą Gaussa.

Ćwiczenie 10.26 Udowodnić, że liczba pierwsza $p \in \mathbb{P}$ jest liczbą pierwszą Gaussa wtedy i tylko wtedy, gdy $p \equiv 3 \,(\mathrm{mod}\, 4)$.

Ćwiczenie 10.27 Jeżeli π_1, π_2 są liczbami pierwszymi Gaussa i $\pi_1|\pi_2$, to $\pi_1 \sim \pi_2$.

Jako zastosowanie T10.3 pokażemy teraz, pochodzący od Dedekinda, piękny dowód twierdzenia Fermat'*a*-Eulera T8.1.

S Z Ó S T Y D O W Ó D TFE. Niech $p \equiv 1 \pmod 4$ będzie liczbą pierwszą. Wiemy (zobacz I uzupełnienie PWRK), że istnieje $a \in \mathbb{Z}$, dla którego $p|a^2+1$, czyl $p|(a+i)(a-i)$ w $\mathbb{Z}[\,i\,]$. Ale $p \nmid (a+i)$ i $p \nmid (a-i)$. Rzeczywiście, gdy $p|(a \pm i)$, to $a \pm i = p(k+li)$, więc $\pm 1 = pl$, co jest niemożliwe. Wnosimy stąd, że p nie spełnia warunku (10.7). N i e j e s t w i ę c l i c z b ą p i e r w s z ą G a u s s a. Wobec tego p nie jest liczbą nierozkładalną Gaussa. Przeto istnieje taki rozkład $p = \alpha\beta$, że $\mathbf{N}(\alpha) > 1$ i $\mathbf{N}(\beta) > 1$. Stąd, na mocy (10.2):

$$\mathbf{N}(p) = p^2 = \mathbf{N}(\alpha)\mathbf{N}(\beta).$$

A ponieważ $\mathbf{N}(\alpha), \mathbf{N}(\beta) \neq 1$, więc $p = \mathbf{N}(\alpha) = x^2 + y^2$. □

U w a g a. Przytoczony dowód twierdzenia Fermat'*a*-Eulera mógłby stanowić wystarczającą nagrodę za pracę włożoną w poznanie elementarnych własności pierścienia $\mathbb{Z}[\,i\,]$. Ponadto pokazuje on, że wyjście z prostej rzeczywistej (*le domaine des entiers ordinaires*), gdzie "żyją" zwykłe liczby całkowite i przejście na płaszczyznę zespoloną (*passer aux entiers "complexes"* $a+b\sqrt{-1}$), gdzie "mieszkają" liczby całkowite Gaussa, może być p r z y d a t n e w badaniu tych pierwszych. Już w początkach XIX wieku Gauss zrozumiał, że przejście to jest n i e z b ę d n e (*qu'il faut passer*). Pamiętajmy jednak, że ważne dla nas są te zwykłe liczby całkowite i tylko nadzieja lepszego ich oglądu pcha nas w dziedziny zespolone.

10.1.5 Twierdzenie o jednoznaczności rozkładu w $\mathbb{Z}[\,i\,]$

W ustępie 2.3.2 udowodniliśmy twierdzenie T2.16 o istnieniu i jednoznaczności rozkładu liczb naturalnych na czynniki pierwsze. Z tego twierdzenia wynika natychmiast istnienie (i jednoznaczność, z dokładnością do porządku czynników) rozkładów postaci 2.4.1 (RK) niezerowych liczb całkowitych (zwykłych!). Podobnie, w twierdzeniu T3.14 pokazujemy jednoznaczność rozkładu na czynniki nierozkładalne w pierścieniach wielomianów jednej zmiennej nad ciałem. Analogicznie rzecz się ma w pierścieniu liczb całkowitych Gaussa:

TWIERDZENIE 10.4 *Każda niezerowa i nie będąca jednością liczba całkowita Gaussa* α *da się zapisać w postaci iloczynu liczb pierwszych Gaussa:*

$$\alpha = \pi_1\pi_2 \cdot \ldots \cdot \pi_s. \tag{10.8}$$

Ponadto przedstawienie takie jest jednoznaczne w takim sensie: Jeżeli $\alpha = \nu_1\nu_2 \cdot \ldots \cdot \nu_t$ *jest również przedstawieniem liczby* α *w postaci iloczynu liczb pierwszych Gaussa, to* $s = t$ *i, po ewentualnym przenumerowaniu,* $\pi_1 \sim \nu_1$, $\pi_2 \sim \nu_2$, $\ldots$, $\pi_s \sim \nu_s$.

D O W Ó D. Czytelnik, który zrozumiał poprzednie dowody (czy ich szkice) nie powinien mieć najmniejszych trudności z samodzielnym przedstawieniem dowodu obecnie. Można też przeczytać dowód ogólniejszego twierdzenia w następnym paragrafie. □

P r z y k ł a d 1. Rozkład $2 = (1+i)(1-i)$ jest rozkładem na iloczyn liczb pierwszych Gaussa. To wynika z C10.25, bo $\mathbf{N}(1+i) = \mathbf{N}(1-i) = 2 \in \mathbb{P}$. Ten rozkład zapisujemy często

w postaci kanonicznej $2 = (-i)(1+i)^2$ dodając odpowiedni czynnik odwracalny. Widzimy, że 2 traktowana jako liczba całkowita Gaussa jest stowarzyszona z kwadratem liczby pierwszej Gaussa, chociaż sama n i e j e s t kwadratem. ◊

P r z y k ł a d 2. Jeżeli $p \in \mathbb{P}$ i $p \equiv 1 \pmod 4$, to, jak już pięciokrotnie udowodniliśmy, istnieją takie $x, y \in \mathbb{N}$, że $p = x^2 + y^2$. Jasne, że w takim przypadku

$$p = (x + yi)(x - yi) \tag{10.9}$$

jest rozkładem na iloczyn liczb pierwszych Gaussa. Dzięki udowodnionej w T10.4 jednoznaczności rozkładu łatwo jeszcze raz rozwiązać zadanie Z8.2. Mianowicie, każde inne przedstawienie $p = x_1^2 + y_1^2$ daje rozkład $p = (x_1 + y_1 i)(x_1 - y_1 i)$ na iloczyn czynników pierwszych (w $\mathbb{Z}[\,i\,]$). Jednoznaczność rozkładu daje więc jedną z równości $x_1 + y_1 i = i^k(x + yi)$ przy $k = 0,\ 1,\ 2$ lub 3, albo $x_1 + y_1 i = i^k(x - yi)$ przy $k = 0,\ 1,\ 2$ lub 3. ◊

Wzmocnimy teraz tezę zadania Z10.2:

ZADANIE 10.3 Dana jest liczba całkowita Gaussa $\alpha = a + bi$. Niech $\mathrm{NWD}\,(a,\, b) = d$ w pierścieniu $\mathbb{Z}$ i niech $a = da_1$, $b = db_1$. Udowodnić, że wówczas

$$\mathrm{NWD}\,(\alpha,\, \alpha') \sim \begin{cases} d, & \text{gdy} \quad a_1 \not\equiv b_1 \pmod 2, \\ (1+i)d, & \text{gdy} \quad a_1 \equiv b_1 \pmod 2. \end{cases} \tag{10.10}$$

R o z w i ą z a n i e. Przedstawmy $a = da_1$, $b = db_1$. Niech δ będzie wspólnym dzielnikiem liczb $a_1 + b_1 i$, $a_1 - b_1 i$. Wtedy δ dzieli sumę i różnicę tych liczb: $\delta | 2a_1$ i $\delta | 2b_1 i$. Ale $a_1 x + b_1 y = 1$ dla pewnych $x, y \in \mathbb{Z}$. Stąd widzimy, że δ dzieli $2a_1 x - 2b_1 i \cdot yi = 2$. Czyli $\delta | 2$. Zatem $\delta \sim 1$ lub $\delta \sim 1 + i$ lub $\delta \sim 2$. Ostatni przypadek nie może zachodzić (!). Łatwo sprawdzić, że $(1+i) | (u + wi)$ wtedy i tylko wtedy, gdy $u \equiv w \pmod 2$. Istotnie, $u \equiv w \pmod 2$ wtedy i tylko wtedy, gdy układ równań $x - y = u$, $x + y = w$ ma rozwiązanie w liczbach całkowitych, czyli wtedy i tylko wtedy, gdy $u + wi = (x + yi)(1 + i)$. Jasne, że to kończy rozwiązanie. ◊

Ilustracją wykorzystania jednoznaczności rozkładu w pierścieniu Gaussa $\mathbb{Z}[\,i\,]$ jest dowód znanego nam już opisu wszystkich trójek pitagorejskich. Zaczniemy od ***triku***, porównaj T2.19, który teraz ma postać:

Ćwiczenie 10.28 Jeśli iloczyn dwóch względnie pierwszych liczb w $\mathbb{Z}[\,i\,]$ jest k-tą potęgą pewnej liczby w $\mathbb{Z}[\,i\,]$, to każdy z czynników jest s t o w a r z y s z o n y z k-tą potęgą.

Korzystając z tego triku udowodnimy jeszcze raz:

TWIERDZENIE 10.5 *Jeżeli trójka $(a,\, b,\, c)$ liczb całkowitych względnie pierwszych spełnia* ***równanie Pitagorasa*** $x^2 + y^2 = z^2$, *to*

$$a = \pm(u^2 - v^2), \quad b = \pm 2uv, \quad c = \pm(u^2 + v^2),$$

(z ewentualną zamianą miejscami a i b) przy pewnych całkowitych względnie pierwszych u, v różnej parzystości.

D O W Ó D. Zapisujemy równość $a^2+b^2=c^2$ w postaci iloczynowej $(a+ib)(a-ib)=c^2$ w $\mathbb{Z}[\,i\,]$. Udowodnimy, że czynniki $a+ib$ i $a-ib$ są względnie pierwsze w $\mathbb{Z}[\,i\,]$. Z Z10.3 wiemy, że to jest równoważne z warunkiem $a \not\equiv b \pmod 2$, który, jak łatwo sprawdzić, zachodzi. Wobec tego dzięki trikowi z ćwiczenia C10.28, możemy zapisać:

$$a+ib=\varepsilon(u+iv)^2,$$

gdzie $\varepsilon=\pm1, \pm i$. Czyli $a=\pm(u^2-v^2)$, $b=\pm2uv$ lub $a=\pm2uv$, $b=\pm(u^2-v^2)$. Wtedy też, oczywiście, $c=\pm(u^2+v^2)$. □

ZADANIE 10.4 Udowodnić, że równanie

$$y^2=x^3-1 \tag{10.11}$$

nie ma rozwiązań w niezerowych liczbach całkowitych.

R o z w i ą z a n i e. Oczywiście $(x,\,y)=(1,\,0)$ jest rozwiązaniem. Łatwo sprawdzić, że $y\equiv0\pmod2$. Gdyby bowiem $y=2v+1$, to $x=2u$ i wtedy $4v^2+4v+2=8u^3$, co nie jest możliwe. Jeżeli $2|y$, to przepisując (10.11) w postaci:

$$(y+i)(y-i)=x^3,$$

widzimy, dzięki Z10.2, że czynniki $y+i$ i $y-i$ są względnie pierwsze w $\mathbb{Z}[\,i\,]$. Korzystając teraz z triku możemy napisać (przy pewnej jedności $\varepsilon\in\mathbb{Z}[\,i\,]^*$)

$$y+i=\varepsilon^3(a+bi)^3=(c+di)^3. \tag{10.12}$$

Korzystamy tu z faktu, że każda jedność w $\mathbb{Z}[\,i\,]$ jest sześcianem (sprawdźcie!). Porównując części urojone znajdujemy

$$1=3c^2d-d^3=d(3c^2-d^2).$$

Zatem albo $d=1$, $3c^2-d^2=1$ albo $d=-1$, $3c^2-d^2=-1$. W drugim przypadku mamy $c=0$, a pierwszy przypadek zajść nie może(!). Kładąc w (10.12) $c=0$, $d=-1$ znajdujemy więc jedyne rozwiązanie równania (10.11) w liczbach całkowitych: $x=1$, $y=0$. ◊

Ćwiczenie 10.29 Suma dwóch kwadratów bywa trzecią potęgą. Na przykład $2^2+2^2=2^3$, $2^2+11^2=5^3$, $18^2+26^2=10^3$. Wskazać nieskończenie wiele takich przykładów. Wyznaczyć wszystkie rozwiązania równania $x^2+y^2=z^3$ w liczbach całkowitych.

Ćwiczenie 10.30 Zbadać równanie $x^2+y^2=z^n$ przy dowolnym n.

Ćwiczenie 10.31 Dane są względnie pierwsze liczby całkowite a, b. Załóżmy, że liczba pierwsza p dzieli a^2+b^2. Udowodnić, że jeżeli $\mathrm{NWD}\,(p,\,a+bi)\sim x+yi$, to $p=x^2+y^2$.

C10.31 pozwala za pomocą algorytmu Euklidesa w pierścieniu $\mathbb{Z}[\,i\,]$ znajdować przedstawienia liczb pierwszych w postaci sumy dwóch kwadratów. Pokażemy to w przykładzie:

P r z y k ł a d. Ten przykład pochodzi z [**3**]. Wiemy, że każdy dzielnik pierwszy p liczby $2^{36}+1$ przystaje do 1 modulo 4, bo $(2^{18})^2 \equiv -1 \,(\mathrm{mod}\, p)$, więc $(-1)\mathbf{R}p$. Ponieważ $2^{36}+1 = 38737 \cdot 433 \cdot 241 \cdot 17$ jest rozkładem na czynniki pierwsze (!), a jednocześnie

$$2^{36}+1 = (2^{12})^3+1 = (2^{12}+1)(2^{24}-2^{12}+1) = 17 \cdot 241 \cdot ((2^{12}-1)^2+2^{12}),$$

więc $38737 | 4095^2+64^2$. Poszukamy $\mathrm{NWD}\,(38737,\, 4095+64i)$ w pierścieniu $\mathbb{Z}[\,i\,]$:

$$\begin{aligned} 38737 &= 9 \cdot (4095+64i) + (1882-576i) \\ 4095+64i &= (2+i) \cdot (1882-576i) - (245+666i) \\ 1882-576i &= (-3i) \cdot (245+666i) - (116-159i) \\ 245+666i &= (-2+3i) \cdot (116-159i) + 0 \end{aligned}$$

Widzimy, że $\mathrm{NWD}\,(38737,\, 4095+64i) \sim 116-159i$. Zatem $38737 = 116^2+159^2$. Rozkłady pozostałych czynników na sumy kwadratów są (z powodu ich małości) proste: $433 = 12^2+17^2$ oraz $241 = 4^2+15^2$ i $17 = 1^2+4^2$. ◊

10.1.6 Rozkład liczb pierwszych wymiernych w $\mathbb{Z}[\,i\,]$

Pokażemy teraz jak wyglądają rozkłady liczb $p \in \mathbb{P}$ (nazywamy je, dla odróżnienia od liczb pierwszych Gaussa, **liczbami pierwszymi wymiernymi**) na czynniki pierwsze w $\mathbb{Z}[\,i\,]$.

Niech $p \in \mathbb{P}$ będzie liczbą pierwszą (wymierną). Liczba ta, traktowana jako element $\mathbb{Z}[\,i\,]$, ma rozkład kanoniczny

$$p = \varepsilon \pi_1^{e_1} \pi_2^{e_2} \cdot \ldots \cdot \pi_s^{e_s}, \quad \text{gdzie } \varepsilon \sim 1, \tag{10.13}$$

na czynniki pierwsze (= nierozkładalne) w $\mathbb{Z}[\,i\,]$ (*kanoniczność* rozkładu oznacza, podobnie jak w rozdziale 2, że czynniki π_i są parami niestowarzyszone). Wówczas, zobacz (10.2), $p^2 = \mathbf{N}(p) = \mathbf{N}(\varepsilon)\mathbf{N}(\pi_1)^{e_1}\mathbf{N}(\pi_2)^{e_2} \cdot \ldots \cdot \mathbf{N}(\pi_s)^{e_s}$. Stąd wnioskujemy, że $s \leqslant 2$. Wobec tego *a priori* zachodzi jedna z trzech możliwości: (1) $p = \varepsilon\pi_1^2$, (2) $p = \varepsilon\pi_1\pi_2$, (3) $p = \varepsilon\pi_1$. Wiemy z poprzednich rozważań, że każda z tych możliwości zachodzi. Konkretnie:

Twierdzenie 10.6 *Rozkład* (10.13) *liczb pierwszych* $p \in \mathbb{P}$ *w* $\mathbb{Z}[\,i\,]$ *ma postać:*

(1) $2 = (-i)(1+i)^2$,

(2) $p = (x+iy)(x-iy)$, *gdzie* $x+iy \not\sim x-iy$, *gdy* $p \equiv 1 \,(\mathrm{mod}\, 4)$,

(3) $p = p$, *gdy* $p \equiv 3 \,(\mathrm{mod}\, 4)$. □

W ten sposób wskazaliśmy nieskończenie wiele liczb pierwszych Gaussa. Ale czy wszystkie? Okazuje się, że (z dokładnością do stowarzyszenia) t a k. To wynika z poniższego zadania:

ZADANIE 10.5 Udowodnić, że jeżeli $\pi \in \mathbb{Z}[\,i\,]$ jest liczbą pierwszą Gaussa, to istnieje d o k ł a d n i e j e d n a taka wymierna liczba pierwsza p, że $\pi | p$ w $\mathbb{Z}[\,i\,]$.

R o z w i ą z a n i e. Uzasadnimy najpierw, że π może dzielić co najwyżej jedną liczbę pierwszą wymierną. Gdyby $\pi|p$ i $\pi|q$, dla różnych $p, q \in \mathbb{P}$, to, ponieważ $pa+qb = 1$ dla pewnych

$a, b \in \mathbb{Z} \subseteq \mathbb{Z}[\,i\,]$, więc liczba π byłaby dzielnikiem 1, co jest niemożliwe. W istocie pokazaliśmy, że π nie może dzielić dwóch liczb całkowitych względnie pierwszych.

Popatrzmy teraz na normę $\mathbf{N}(\pi)$. To jest liczba naturalna > 1, zobacz D10.6. Jako taka, zobacz T2.14, dzieli się przez pewną liczbę pierwszą p. Mamy więc

$$\mathbf{N}(\pi) = \pi\pi' = pa \tag{10.14}$$

dla pewnego $a \in \mathbb{Z}$. Wobec tego $\pi | pa$. Ponieważ π jest liczbą pierwszą Gaussa, więc $\pi | p$ lub $\pi | a$. Jeżeli $\pi | p$, to dobrze. Załóżmy więc, że $\pi | a$. Wówczas $a = \pi\alpha$ dla pewnego $\alpha \in \mathbb{Z}[\,i\,]$. Stąd $\pi' a = \pi'\pi\alpha = \mathbf{N}(\pi)\alpha = ap\alpha$, więc $\pi' = p\alpha$ (na mocy prawa skracania, bo $a \neq 0$). Ale π', jako liczba pierwsza Gaussa jest nierozkładalna, więc $\alpha \sim 1$ (bo $\mathbf{N}(p) = p^2 \neq 1$). Zatem $\pi' \sim p$, więc też $\pi = \pi'' \sim p' = p$ i, oczywiście, $\pi | p$. $\Diamond$

Definicja 10.8 Jeżeli π jest liczbą pierwszą Gaussa, a $p \in \mathbb{P}$ jest jedyną taką wymierną liczbą pierwszą, że $\pi | p$, to mówimy, że π **leży nad** p.

Ćwiczenie 10.32 Udowodnić, że jeżeli liczba pierwsza Gaussa π leży nad liczbą pierwszą wymierną p, to $\mathbf{N}(\pi) = p$ lub $\mathbf{N}(\pi) = p^2$.

10.2 Pierścienie kwadratowe

Pierścień $\mathbb{Z}[\,i\,]$ liczb całkowitych Gaussa jest najprostszym przykładem pierścienia kwadratowego. Jest on podpierścieniem ciała kwadratowego $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. Łatwo wykazać, że zachodzi równość $\mathbb{Q}(i) \cap \mathbb{I} = \mathbb{Z}[\,i\,]$. Rzeczywiście, liczba $\alpha = a + bi \in \mathbb{Q}(i)$ jest pierwiastkiem unormowanego wielomianu $X^2 - 2aX + a^2 + b^2 \in \mathbb{Q}[X]$. Wielomian ten, będący, przy $b \neq 0$, wielomianem minimalnym liczby α, ma współczynniki całkowite wtedy i tylko wtedy, gdy $a, b \in \mathbb{Z}$. Czytelnik z łatwością to sprawdzi.

Podobnie, zbiór $\mathbb{Q}(\sqrt{D}) \cap \mathbb{I}$, czyli zbiór tych elementów ciała kwadratowego $\mathbb{Q}(\sqrt{D})$, które jednocześnie są liczbami algebraicznymi całkowitymi, jest p i e r ś c i e n i e m, zob. T6.6. Takie pierścienie (przy różnych bezkwadratowych $D \neq 1$) nazywamy pierścieniami kwadratowymi. Można (podobnie jak powyżej dla przypadku $D = -1$) wykazać zbiór $\mathbb{Q}(\sqrt{D}) \cap \mathbb{I}$ daje się opisać następująco:

Jeżeli $D \neq 1$ jest bezkwadratową liczbą całkowitą, to oznaczamy

$$\tau_D := \begin{cases} \dfrac{1+\sqrt{D}}{2}, & \text{gdy } D \equiv 1 \,(\mathrm{mod}\, 4), \\ \sqrt{D}, & \text{gdy } D \equiv 2,\, 3 \,(\mathrm{mod}\, 4). \end{cases} \tag{10.15}$$

Definicja 10.9 Dla danej bezkwadratowej liczby całkowitej $D \neq 1$ określamy

$$\mathbb{Z}[\tau_D] := \{x + y\tau_D : x, y \in \mathbb{Z}\}. \tag{10.16}$$

Określony w ten sposób zbiór $\mathbb{Z}[\tau_D]$ nazywamy **pierścieniem kwadratowym** wyznaczonym przez liczbę D. Gdy $D > 0$, to pierścień $\mathbb{Z}[\tau_D]$ nazywamy **rzeczywistym pierścieniem kwadratowym** (jasne, że wówczas $\mathbb{Z}[\tau_D] \subset \mathbb{R}$), gdy zaś $D < 0$, to **urojonym pierścieniem kwadratowym**.

Ćwiczenie 10.33 Udowodnić, że jeżeli $x_1,\ y_1,\ x_2,\ y_2 \in \mathbb{Q}$, to $x_1+y_1\tau_D = x_2+y_2\tau_D$ wtedy i tylko wtedy, gdy $x_1 = x_2$ i $y_1 = y_2$.

Ćwiczenie 10.34 Udowodnić, że jeżeli $\alpha \in \mathbb{Z}[\tau_D]$, to $\alpha' \in \mathbb{Z}[\tau_D]$. Udowodnić też, że jeżeli $\alpha = x + y\tau_D \in \mathbb{Z}[\tau_D]$, to norma $\mathbf{N}(\alpha) = \alpha\alpha'$ jest równa

$$\mathbf{N}(\alpha) = \begin{cases} x^2 - Dy^2, & \text{gdy } D \equiv 2,\ 3 \,(\mathrm{mod}\, 4), \\ x^2 + xy + \dfrac{1-D}{4}\, y^2, & \text{gdy } D \equiv 1 \,(\mathrm{mod}\, 4). \end{cases}$$

Wywnioskować stąd, że liczba $\mathbf{N}(\alpha)$ jest liczbą całkowitą dla każdego $\alpha \in \mathbb{Z}[\tau_D]$. Ponadto, $\mathbf{N}(\alpha) = 0$ wtedy i tylko wtedy, gdy $\alpha = 0$.

10.2.1 Jedności w $\mathbb{Z}[\tau_D]$

Istnieje proste kryterium, za pomocą którego rozpoznajemy jedności (= elementy odwracalne, zobacz D1.8) w pierścieniach kwadratowych $\mathbb{Z}[\tau_D]$. W dalszym ciągu używamy oznaczeń wprowadzonych we wstępie do tego rozdziału.

TWIERDZENIE 10.7 *$\alpha \in \mathbb{Z}[\tau_D]^*$ wtedy i tylko wtedy, gdy $|\mathbf{N}(\alpha)| = 1$.*

D O W Ó D. Załóżmy, że $\alpha \in \mathbb{Z}[\tau_D]$ jest odwracalny i że $\alpha\beta = 1$. Wówczas $\mathbf{N}(\alpha)\mathbf{N}(\beta) = \mathbf{N}(\alpha\beta) = \mathbf{N}(1) = 1$. Stąd $\mathbf{N}(\alpha) = \pm 1$. Odwrotnie, jeżeli $\mathbf{N}(\alpha) = \pm 1$, to $1/\alpha = \pm\alpha'$, więc α jest odwracalny (w pierścieniu $\mathbb{Z}[\tau_D]$!). □

Ćwiczenie 10.35 Udowodnić, że grupa jedności $\mathbb{Z}[\tau_D]^*$ w urojonym pierścieniu kwadratowym jest grupą skończoną. Konkretnie: $\mathbb{Z}[\tau_{-3}]^* = \{1,\ \tau_{-3},\ \tau_{-3}^2,\ \tau_{-3}^3,\ \tau_{-3}^4,\ \tau_{-3}^5\}$ oraz $\mathbb{Z}[\tau_{-1}]^* = \{1,\ \tau_{-1},\ -1,\ \tau_{-1}^3\}$, i $\mathbb{Z}[\tau_D]^* = \{-1,\ +1\}$ dla $D < 0$ i $D \neq -1,\ -3$.

Ćwiczenie 10.36 Niech $(1+\sqrt{2})^n = a_n+b_n\sqrt{2}$, gdzie $a_n,\ b_n \in \mathbb{Z}$. Udowodnić, że $a_n+b_n\tau_2$ jest jednością w $\mathbb{Z}[\tau_2]$ dla każdego $n \in \mathbb{Z}$.

10.2.2 Dzielenie z resztą w $\mathbb{Z}[\tau_D]$

W pierścieniu $\mathbb{Z}$ liczb całkowitych (zobacz T2.2), w pierścieniach $\mathbb{K}[X]$ wielomianów jednej zmiennej o współczynnikach w ciele (zobacz T3.3), a także w pierścieniu $\mathbb{Z}[i\,]$ (zobacz T10.1) istnieje możliwość d z i e l e n i a z r e s z t ą. Istnieją i inne pierścienie kwadratowe, w których daje[1] się dzielić z resztą. Opowiemy teraz o tym.

Niech $\alpha,\ \beta \in \mathbb{Z}[\tau_D]$, przy czym $\beta \neq 0$. Chcielibyśmy podzielić z resztą α przez β. To znaczy, chcielibyśmy móc napisać (prawdziwe) równość i nierówność:

$$\alpha = \varphi\beta + \varrho, \qquad |\mathbf{N}(\varrho)| < |\mathbf{N}(\beta)| \tag{10.17}$$

dla pewnych $\varphi,\ \varrho \in \mathbb{Z}[\tau_D]$.

[1] Chodzi o to, by reszta ϱ w równości $\alpha = \varphi\beta + \varrho$ była w jakimś d o b r y m sensie mniejsza niż dzielnik β.

Definicja 10.10 Jeżeli dla dowolnych $\alpha, \beta \in \mathbb{Z}[\tau_D]$, $\beta \neq 0$ istnieją $\varphi, \varrho \in \mathbb{Z}[\tau_D]$ spełniające warunki (10.17), to pierścień kwadratowy $\mathbb{Z}[\tau_D]$ nazywa się **pierścieniem normowo-euklidesowym**.

Udowodnimy lemat podający kryterium normowej euklidesowości $\mathbb{Z}[\tau_D]$:

LEMAT 10.1 *Niech $D \neq 0$ będzie liczbą całkowitą bezkwadratową. Wówczas, pierścień $\mathbb{Z}[\tau_D]$ jest normowo-euklidesowy wtedy i tylko wtedy, gdy dla dowolnych liczb wymiernych x, y istnieje taki element $\varphi \in \mathbb{Z}[\tau_D]$, że*

$$|\mathbf{N}(x + y\sqrt{D} - \varphi)| < 1. \tag{10.18}$$

D O W Ó D. ($\Longrightarrow$) Załóżmy, że $\mathbb{Z}[\tau_D]$ jest normowo-euklidesowy i niech $x, y \in \mathbb{Q}$. Sprowadzamy do wspólnego mianownika: $x = s/w$, $y = t/w$ dla $s, t, w \in \mathbb{Z}$. Wówczas $s + t\sqrt{D}$, $w \in \mathbb{Z}[\tau_D]$. Ponieważ $w \neq 0$, więc, zgodnie z (10.17), możemy napisać:

$$s + t\sqrt{D} = \varphi w + \varrho, \quad |\mathbf{N}(\varrho)| < |\mathbf{N}(w)|,$$

dla pewnych $\varphi, \varrho \in \mathbb{Z}[\tau_D]$. Wówczas

$$|\mathbf{N}(x + y\sqrt{D} - \varphi)| = \left|\mathrm{N}\left(\frac{s + t\sqrt{D}}{w} - \varphi\right)\right| = \left|\mathrm{N}\left(\frac{\varrho}{w}\right)\right| = \frac{|\mathbf{N}(\varrho)|}{|\mathbf{N}(w)|} < 1.$$

($\Longleftarrow$) Niech $\alpha, \beta \in \mathbb{Z}[\tau_D]$, $\beta \neq 0$. Rozważmy liczbę zespoloną α/β i przedstawmy (mnożąc licznik i mianownik przez β') ją w postaci

$$\frac{\alpha}{\beta} = x + y\sqrt{D},$$

gdzie $x, y \in \mathbb{Q}$. Niech $\varphi \in \mathbb{Z}[\tau_D]$ spełnia nierówność (10.18). Wtedy dla $\varrho = \alpha - \varphi\beta$:

$$|\mathbf{N}(\varrho)| = \left|\mathbf{N}(\beta)\mathrm{N}\left(\frac{\alpha}{\beta} - \varphi\right)\right| = |\mathbf{N}(\beta)| \cdot |\mathbf{N}(x + y\sqrt{D} - \varphi)| < |\mathbf{N}(\beta)|$$

i, oczywiście, $\alpha = \varphi\beta + \varrho$. □

Dzięki temu kryterium rozwiążemy:

ZADANIE 10.6 Dowieść, że pierścień $\mathbb{Z}[\tau_D]$ jest pierścieniem normowo-euklidesowym dla $D = -1, -2, -3, -7, -11$ oraz dla $D = 2, 3, 5, 6$.

R o z w i ą z a n i e. Przypadek $D = -1$ jest już nam znany, zobacz T10.1. Równie łatwo można rozprawić się z przypadkami $D = -2, 2, 3$. Ponieważ $-2, 2, 3 \not\equiv 1 \pmod 4$, więc $\tau = \sqrt{-2}, \sqrt{2}, \sqrt{3}$ w tych przypadkach. Stosujemy lemat L10.1: dla danej liczby $x + y\tau$, gdzie $x, y \in \mathbb{Q}$, wybierzmy takie $a, b \in \mathbb{Z}$, by $|x - a| \leqslant 1/2$ i $|y - b| \leqslant 1/2$. Niech $\varphi = a + b\tau$. Wówczas

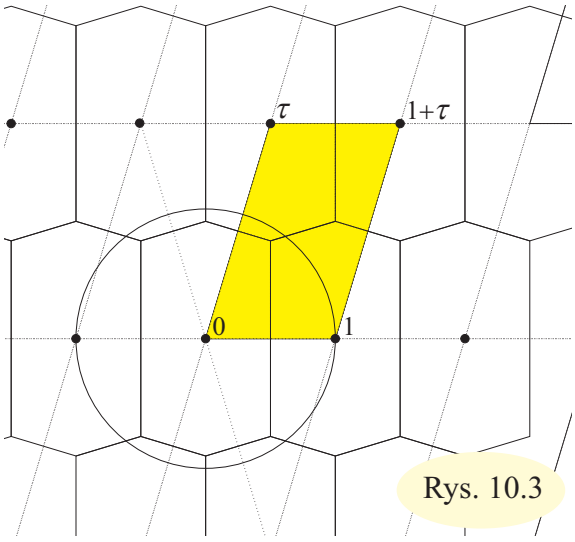
$$|\mathbf{N}(x + y\tau - \varphi)| = |\mathbf{N}((x - a) + (y - b)\tau)| = |(x - a)^2 - \tau^2(y - b)^2| \leqslant \frac{3}{4} < 1.$$

Zbadamy teraz przypadek $D = 5$. Dla danych $x, y \in \mathbb{Q}$ wybieramy $a, b \in \mathbb{Z}$ tak, by $|2x - a| \leqslant 1$ i $|2y - b| \leqslant 1/2$ oraz $a \equiv b \,(\mathrm{mod}\, 2)$. Chwila zastanowienia pokazuje, że to jest możliwe. Kładąc $\varphi = (a + b\sqrt{5})/2$ mamy

$$|\mathbf{N}(x + y\sqrt{5} - \varphi)| = \left|\left(x - \frac{a}{2}\right)^2 - 5\left(y - \frac{b}{2}\right)^2\right| \leqslant \frac{5}{16} < 1.$$

P r z y p a d k i $D = -3, -7, -11$ badamy "rysunkowo". Rzecz polega na tym, że urojone pierścienie kwadratowe $\mathbb{Z}[\tau_D]$, dla $D < 0$, w naturalny sposób utożsamiamy z kratami $\Lambda(1, \tau_D)$ (rzeczywiste pierścienie kwadratowe również można utożsamiać z kratami w płaszczyźnie, jest to jednak trudniejsze i nie będziemy tego tu robić).

Rozważymy przypadek $D = -11$. Przypadki $D = -3, -7$ bada się tak samo (prościej!). Na rysunku obok widzimy kratę $\Lambda(1, \tau)$, gdzie $\tau = (1 + \sqrt{-11})/2$. Każdy punkt ψ tej kraty jest środkiem sześciokąta składającego się z tych i tylko tych punktów płaszczyzny, których odległość od ψ jest niewiększa niż odległość od wszystkich innych punktów kraty. Łatwo sprawdzić, że cały taki sześciokąt zawarty jest w kole o środku ψ i promieniu 1. Ponieważ każdy punkt $x + y\sqrt{-11}$ wpada do (co najmniej) jednego sześciokąta, więc widzimy, że środek φ tego sześciokąta spełnia nierówność (10.18). To wynika z faktu, że $|\mathbf{N}(\psi)|$ (dla $\psi = x + y\sqrt{D}$, przy $D < 0$) jest kwadratem z w y k ł e j odległości liczby zespolonej ψ od 0.



Rys. 10.3

Pozostał nam jeszcze do zbadania p r z y p a d e k $D = 6$. Załóżmy, wbrew tezie, że $\mathbb{Z}[\tau_6]$ nie jest pierścieniem normowo-euklidesowym. Wówczas, wobec lematu L10.1, istnieją takie liczby $s, t \in \mathbb{Q}$, że

$$|(s - x)^2 - 6(t - y)^2| \geqslant 1 \tag{10.19}$$

dla dowolnych $x, y \in \mathbb{Z}$. Wybierzmy takie liczby całkowite a i b, by

$$|s - a| \leqslant \frac{1}{2}, \quad |t - b| \leqslant \frac{1}{2} \tag{10.20}$$

i oznaczmy przez K liczbę $(s-a)^2 - 6(t-b)^2$. Nierówności (10.20) dają oszacowanie $-3/2 \leqslant K \leqslant 1/4$, zaś nierówność (10.19) przy $x = a$, $y = b$ daje $K \geqslant 1$ lub $K \leqslant -1$. Stąd

$$-\frac{3}{2} \leqslant K \leqslant -1. \tag{10.21}$$

Możliwe są dwa przypadki

$$\text{i)} \quad 0 \leqslant s - a \leqslant \frac{1}{2}, \qquad \text{ii)} \quad -\frac{1}{2} \leqslant s - a \leqslant 0. \tag{10.22}$$

W przypadku (10.22i) położymy w nierówności (10.19) $x = a - 1$, $y = b$. Mamy wówczas

$$1 \leqslant |(s-a+1)^2 - 6(t-b)^2| = |K + 2(s-a) + 1|. \tag{10.23}$$

Dodając $2(s-a)+1$ do obu stron nierówności (10.21) otrzymamy, po uwzględnieniu (10.22i),

$$-\frac{1}{2} \leqslant -\frac{3}{2} + 2(s-a) + 1 \leqslant K + 2(s-a) + 1 \leqslant 2(s-a) \leqslant 1.$$

Nierówność ta może, wobec (10.21) i (10.23), zachodzić tylko, gdy $K = -1$ i $s - a = 1/2$.

W przypadku (10.22ii) położymy w nierówności (10.19) $x = a + 1$, $y = b$. Mamy wówczas

$$1 \leqslant |(s-a-1)^2 - 6(t-b)^2| = |K - 2(s-a) + 1|. \tag{10.24}$$

Dodając $-2(s-a)+1$ do obu stron nierówności (10.21) otrzymamy, po uwzględnieniu nierówności (10.22ii),

$$-\frac{1}{2} \leqslant -\frac{3}{2} - 2(s-a) + 1 \leqslant K - 2(s-a) + 1 \leqslant -2(s-a) \leqslant 1.$$

Nierówność ta może, wobec (10.21) i (10.24), zachodzić tylko, gdy $K = -1$ i $s - a = -1/2$.

Widzimy więc, że w obu przypadkach (10.22) mamy $|s-a| = 1/2$ i $K = -1$. Wówczas $-1 = K = \frac{1}{4} - 6(t-b)^2$, skąd $(t-b)^2 = 5/24$, co jest niemożliwe, bo $t, b \in \mathbb{Q}$. Uzyskana sprzeczność kończy rozumowanie. ◊

Ćwiczenie 10.37 Udowodnić, że istnieje d o k ł a d n i e pięć urojonych pierścieni kwadratowych, które są normowo-euklidesowe. Są to te $\mathbb{Z}[\tau_D]$, dla których $D = -1, -2, -3, -7, -11$.

Wyznaczenie wszystkich rzeczywistych normowo-euklidesowych pierścieni kwadratowych jest dużo trudniejsze. Ostateczny wynik uzyskano dopiero w połowie XX wieku:

Twierdzenie 10.8 *Istnieje d o k ł a d n i e szesnaście rzeczywistych pierścieni kwadratowych $\mathbb{Z}[\tau_D]$, które są normowo-euklidesowe. Są to te pierścienie $\mathbb{Z}[\tau_D]$, dla których $D = 2$, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57 i 73.* □

Ćwiczenie 10.38 Dowieść, że rzeczywisty pierścień kwadratowy $\mathbb{Z}[\tau_{13}]$ jest pierścieniem normowo-euklidesowym.

10.2.3 Podzielność, NWD i ideały w $\mathbb{Z}[\tau_D]$

Zdefiniujemy (znane nam już w kontekście pierścienia $\mathbb{Z}$, pierścieni $\mathbb{K}[X]$ i pierścienia liczb całkowitych Gaussa) podstawowe pojęcia dotyczące podzielności.

Przyjmujemy następujące definicje:

Definicja 10.11 (Porównaj D2.1, D3.6 i D10.2.) Jeżeli α, β są elementami pierścienia $\mathbb{Z}[\tau_D]$, to mówimy, że α dzieli β, gdy istnieje taki element $\varphi \in \mathbb{Z}[\tau_D]$, że $\beta = \varphi\alpha$. Piszemy wtedy $\alpha|\beta$. Mówimy też w takiej sytuacji, że α jest **dzielnikiem** β, lub że β jest **wielokrotnością** α. Jeżeli $\alpha \in \mathbb{Z}[\tau_D]$, to zbiór

$$(\alpha) := \{\varphi\alpha \,:\, \varphi \in \mathbb{Z}[\tau_D]\} \tag{10.25}$$

wszystkich wielokrotności α nazywamy **ideałem głównym** generowanym przez α.

Ćwiczenie 10.39 Sformułować i udowodnić analogony tez (1), (2), (3) i (4) z T2.1 w przypadku dowolnego $\mathbb{Z}[\tau_D]$. *Wskazówka.* Porównaj Z3.14 i C10.11.

Ćwiczenie 10.40 Dowieść, że $\alpha|\beta \Rightarrow \mathbf{N}(\alpha)|\mathbf{N}(\beta)$. (Wynikanie $\Leftarrow$ n i e zachodzi!)

Definicja 10.12 (Porównaj D3.7 i D10.3.) Jeżeli $\alpha, \beta \in \mathbb{Z}[\tau_D]$ i istnieje taka jedność $\varepsilon \in \mathbb{Z}[\tau_D]^*$, że $\alpha\varepsilon = \beta$, to mówimy, że elementy α i β są **stowarzyszone** w $\mathbb{Z}[\tau_D]$. Zapisujemy to tak $\alpha \sim \beta$.

Ćwiczenie 10.41 Udowodnić, że relacja stowarzyszenia jest relacją równoważności.

Ćwiczenie 10.42 Dowieść, że $\alpha \in \mathbb{Z}[\tau_D]^*$ wtedy i tylko wtedy, gdy $\alpha \sim 1$.

Ćwiczenie 10.43 Uzasadnić, że jeżeli $\alpha \sim \beta$ w $\mathbb{Z}[\tau_D]$, to $|\mathbf{N}(\alpha)| = |\mathbf{N}(\beta)|$.

Definicja 10.13 Niech dane będą dwa, nie równe jednocześnie zero, elementy $\alpha, \beta \in \mathbb{Z}[\tau_D]$. Element $\delta \in \mathbb{Z}[\tau_D]$ nazywamy **największym wspólnym dzielnikiem** pary α, β, gdy spełnione są poniższe warunki:

(1) $\delta|\alpha$ i $\delta|\beta$,

(2) jeżeli $\gamma|\alpha$ i $\gamma|\beta$, to $\gamma|\delta$.

Piszemy wtedy $\delta \sim \mathrm{NWD}(\alpha, \beta)$ lub, po prostu, $\mathrm{NWD}(\alpha, \beta) = \delta$. O elementach α, β mówimy, że są **względnie pierwsze**, gdy $\mathrm{NWD}(\alpha, \beta) \sim 1$.

Ćwiczenie 10.44 Udowodnić, że jeżeli istnieje $\mathrm{NWD}(\alpha, \beta)$, to jest on wyznaczony z dokładnością do stowarzyszenia j e d n o z n a c z n i e.

Ćwiczenie 10.45 Załóżmy, że $\mathbb{Z}[\tau_D]$ jest pierścieniem normowo-euklidesowym. Wzorując się na T2.11 (por. też C3.29), opisać **algorytm Euklidesa** wyznaczania największego wspólnego dzielnika w $\mathbb{Z}[\tau_D]$.

Musimy tu wyraźnie zaznaczyć, że istnienie NWD jest raczej w y j ą t k i e m niż regułą. Przykłady zobaczymy wkrótce.

Definicja 10.14 (Porównaj D2.2, D3.8 i D10.4.) Podzbiór $I \subseteq \mathbb{Z}[\tau_D]$ nazywamy **ideałem**, gdy zawiera liczbę 0 oraz spełnia poniższe dwa warunki:

(1) jeżeli $\alpha \in I$ i $\beta \in I$, to $\alpha + \beta \in I$,

(2) jeżeli $\varphi \in \mathbb{Z}[\tau_D]$ i $\alpha \in I$, to $\varphi\alpha \in I$.

Ćwiczenie 10.46 Udowodnić, że dla dowolnych $\alpha, \beta \in \mathbb{Z}[\tau_D]$ zbiór

$$(\alpha, \beta) := \{\alpha\xi + \beta\zeta \,:\, \xi, \zeta \in \mathbb{Z}[\tau_D]\}$$

jest ideałem w $\mathbb{Z}[\tau_D]$. Nazywamy go **ideałem generowanym** przez elementy α, β.

Definicja 10.15 Pierścień bez dzielników zera, w którym każdy ideał jest ideałem głównym nazywa się **dziedziną ideałów głównych**, w skrócie **dig**'iem.

Udowodnimy teraz, że każdy (pamiętamy, że jest ich 21) normowo-euklidesowy pierścień kwadratowy jest dig'*iem*:

TWIERDZENIE 10.9 *Jeżeli $\mathbb{Z}[\tau_D]$ jest normowo-euklidesowy, I jest ideałem w $\mathbb{Z}[\tau_D]$, to istnieje taki element $\delta \in \mathbb{Z}[\tau_D]$, że zachodzi równość $I = (\delta)$.*

D O W Ó D. Dowód jest niewielką modyfikacją dowodu T2.3. Jeżeli I jest ideałem zerowym, to $I = (0)$, więc I jest ideałem głównym. Jeżeli zaś I zawiera elementy różne od zera, to zawiera taki element δ, dla którego $|\mathbf{N}(\delta)|$ jest najmniejsze. Twierdzimy, że wówczas $I = (\delta)$. Istotnie, jeżeli $\alpha \in I$, to, zgodnie z (10.17), mamy $\alpha = \varphi\delta + \varrho$. Stąd, po pierwsze $\varrho = \alpha - \varphi\delta \in I$, a po drugie $|\mathbf{N}(\varrho)| < |\mathbf{N}(\delta)|$, więc $\varrho = 0$. Zatem $\alpha = \varphi\delta \in (\delta)$. Wykazaliśmy w ten sposób, że $I \subseteq (\delta)$. Ponieważ zawieranie odwrotne $(\delta) \subseteq I$ jest oczywiste, więc mamy równość $I = (\delta)$. Czyli każdy ideał jest ideałem głównym. □

10.2.4 Dig'*owość* pierścieni kwadratowych

Okazuje się, że pierścień kwadratowy $\mathbb{Z}[\tau_D]$ może być dziedziną ideałów głównych nawet w przypadku, gdy nie jest on pierścieniem euklidesowym.

TWIERDZENIE 10.10 *Istnieje d o k ł a d n i e 9 urojonych pierścieni kwadratowych $\mathbb{Z}[\tau_D]$ będących dig'*ami. *Są to te, dla których $-D = 1, 2, 3, 7, 11, 19, 43, 67, 163$.* □

U w a g a 1. Dowód twierdzenia T10.10 jest trudny. Sprawdzenie dig'*owości* wymienionych pierścieni nie przekracza naszych możliwości (zrobiliśmy to dla pierwszych pięciu przypadków!). Dużo trudniej wykazać, że (poza wymienionymi) więcej dig'*ów* wśród urojonych pierścieni kwadratowych n i e m a.

U w a g a 2. Istnieje d u ż o (być może nawet nieskończenie wiele) rzeczywistych pierścieni kwadratowych, które są dig'*ami*. Poza wymienionymi w T10.8 są to na przykład te, dla których $D = 14, 22, 29, 31, 33, 38, 43, 46, 47, \ldots$. Liczb bezkwadratowych $1 < D \leqslant 197$ jest 120, wśród nich występuje 67 takich, dla których $\mathbb{Z}[\tau_D]$ jest dziedziną ideałów głównych (z czego, jak wiemy, 16 pierścieni euklidesowych).

10.2.5 Wnioski z dig'*owości*

W tym ustępie wypiszemy kilka wniosków z dig'*owości* pierścienia. Są one takie: (1) każda para elementów ma NWD, (2) NWD danych elementów pisze się w postaci kombinacji liniowej tych elementów, (3) prawdziwe jest Zasadnicze Twierdzenie Arytmetyki, (4) każdy element nierozkładalny jest elementem pierwszym, (5) zachodzi twierdzenie o istnieniu i jednoznaczności rozkładu na czynniki nierozkładalne.

Ćwiczenie 10.47 Prześledzić dokładnie jak analogony powyższych tez były udowodnione w pierścieniu $\mathbb{Z}$ liczb całkowitych i w pierścieniu $\mathbb{K}[X]$ wielomianów o współczynnikach w $\mathbb{K}$.

TWIERDZENIE 10.11 *Jeżeli pierścień $\mathbb{Z}[\tau_D]$ jest dziedziną ideałów głównych, to każda para niezerowych elementów w $\mathbb{Z}[\tau_D]$ m a największy wspólny dzielnik. Ponadto, największy wspólny dzielnik pary $\alpha, \beta \in \mathbb{Z}[\tau_D]$ daje się zapisać w postaci $\alpha\xi + \beta\zeta$ dla pewnych elementów $\xi, \zeta \in \mathbb{Z}[\tau_D]$.*

D O W Ó D. [Dowód jest prostym uogólnieniem dowodu twierdzenia T2.4.] Załóżmy, że $\mathbb{Z}[\tau_D]$ jest dig'*iem* i weźmy dwa niezerowe elementy $\alpha,\ \beta \in \mathbb{Z}[\tau_D]$. Rozważmy ideał

$$(\alpha,\ \beta) := \{\alpha\varphi + \beta\psi :\ \varphi,\ \psi \in \mathbb{Z}[\tau_D]\}$$

pierścienia $\mathbb{Z}[\tau_D]$. Ponieważ jest on (jak każdy ideał w $\mathbb{Z}[\tau_D]$) ideałem głównym, więc istnieje taki element $\delta \in \mathbb{Z}[\tau_D]$, że $(\alpha,\ \beta) = (\delta)$. Twierdzimy, że $\delta \sim \mathrm{NWD}\,(\alpha,\ \beta)$.

Sprawdzamy, że spełniony jest warunek D10.13(1): Zauważmy, że $\alpha = \alpha\cdot 1 + \beta\cdot 0 \in (\alpha,\ \beta)$, więc $\alpha \in (\delta)$, czyli $\delta|\alpha$. Podobnie sprawdzamy, że $\delta|\beta$.

Sprawdzamy, że spełniony jest warunek D10.13(2): Ponieważ $\delta = \delta\cdot 1 \in (\delta)$, więc $\delta = \alpha\xi + \beta\zeta$ dla pewnych $\xi,\ \zeta \in \mathbb{Z}[\tau_D]$. Stąd, jeżeli $\gamma|\alpha$ i $\gamma|\beta$, czyli $\alpha = \gamma\sigma$ i $\beta = \gamma\vartheta$ dla pewnych $\sigma,\ \vartheta \in \mathbb{Z}[\tau_D]$, to $\delta = \alpha\xi + \beta\zeta = (\gamma\sigma)\xi + (\gamma\vartheta)\zeta = \gamma(\sigma\xi + \vartheta\zeta)$. Skąd $\gamma|\delta$. □

Ćwiczenie 10.48 Udowodnić, że w dowolnym pierścieniu euklidesowym prawdziwe jest Zasadnicze Twierdzenie Arytmetyki: *Jeżeli* $\alpha|\beta\gamma$ *i* $\mathrm{NWD}\,(\alpha,\ \beta) \sim 1$, *to* $\alpha|\gamma$.

Definicja 10.16 (Porównaj D3.11 i D10.7.) Element $\nu \in \mathbb{Z}[\tau_D]$ nie będący zerem ani jednością nazywa się **elementem nierozkładalnym** w $\mathbb{Z}[\tau_D]$, gdy spełnia warunek:

$$\boxed{\boxed{\text{jeżeli}\quad \nu = \alpha\beta,\quad \text{to}\quad \alpha \sim 1\quad \text{lub}\quad \beta \sim 1.}} \tag{10.26}$$

Ćwiczenie 10.49 Uzasadnić, że jeżeli $\sigma \in \mathbb{Z}[\tau_D]$ jest takim elementem, że $|\mathbf{N}(\sigma)|$ jest liczbą pierwszą, to σ jest elementem nierozkładalnym.

Ćwiczenie 10.50 Załóżmy, że $\mathbb{Z}[\tau_D]$ jest dig'*iem*. Udowodnić, że jeżeli $\nu \in \mathbb{Z}[\tau_D]$ jest elementem nierozkładalnym, to dla dowolnego elementu $\alpha \in \mathbb{Z}[\tau_D]$ zachodzi dokładnie jedna z możliwości: $\nu|\alpha$ albo $\mathrm{NWD}\,(\alpha,\ \nu) \sim 1$. *Wskazówka.* Zobacz C10.23.

Definicja 10.17 (Porównaj D10.6.) Element $\pi \in \mathbb{Z}[\tau_D]$ nie będący ani zerem ani jednością nazywa się **elementem pierwszym** w $\mathbb{Z}[\tau_D]$, gdy spełnia warunek:

$$\boxed{\boxed{\text{jeżeli}\quad \pi|\alpha\beta,\quad \text{to}\quad \pi|\alpha\quad \text{lub}\quad \pi|\beta.}} \tag{10.27}$$

Ćwiczenie 10.51 Udowodnić, że jeżeli element pierwszy jest dzielnikiem innego elementu pierwszego, to elementy te są stowarzyszone. Czyli: jeżeli $\pi_1|\pi_2$, to $\pi_1 \sim \pi_2$.

Ćwiczenie 10.52 Udowodnić, że każdy element pierwszy w $\mathbb{Z}[\tau_D]$ jest elementem nierozkładalnym. *Wskazówka.* Porównaj część ($\Longleftarrow$) dowodu T10.3. Zauważmy, że nie korzystamy tu z dig'*owości* pierścienia $\mathbb{Z}[\tau_D]$.

Ćwiczenie 10.53 Udowodnić, że jeżeli $\mathbb{Z}[\tau_D]$ jest dig'*iem*, to każdy element nierozkładalny w $\mathbb{Z}[\tau_D]$ jest elementem pierwszym. *Wskazówka.* Porównaj część ($\Longrightarrow$) dowodu T10.3. Zauważmy jak ważną rolę gra tu dig'*owość* $\mathbb{Z}[\tau_D]$.

U w a g a. Elementy nierozkładalne zazwyczaj n i e są elementami pierwszymi.

P r z y k ł a d. Rozważmy element 2 w pierścieniu $\mathbb{Z}[\tau_{-5}]$. Sprawdzimy, że jest to element nierozkładalny. Załóżmy, że zachodzi równość $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Wówczas również $2 = (a - b\sqrt{-5})(c - d\sqrt{-5})$ (bo sprzężenie iloczynu równe jest iloczynowi sprzężeń). Mnożąc te dwie równości stronami otrzymamy

$$4 = (a^2 + 5b^2)(c^2 + 5d^2),$$

co jest możliwe tylko, gdy $a = \pm 1$, $b = 0$, $c = \pm 2$, $d = 0$ lub $a = \pm 2$, $b = 0$, $c = \pm 1$, $d = 0$. Zatem albo $a + b\sqrt{-5}$, albo $c + d\sqrt{-5}$ jest jednością. Z drugiej strony 2 nie jest elementem pierwszym w $\mathbb{Z}[\tau_{-5}]$. Istotnie: $2|(1+\sqrt{-5})(1-\sqrt{-5})$, ale, jak łatwo sprawdzić, $2 \nmid (1+\sqrt{-5})$ oraz $2 \nmid (1 - \sqrt{-5})$. $\Diamond$

Ponieważ w dig'*ach* każdy element nierozkładalny jest elementem pierwszym, więc z powyżej pokazanego przykładu wnosimy, że pierścień $\mathbb{Z}[\tau_{-5}]$ n i e j e s t dig'*iem*. Można to też zobaczyć bezpośrednio:

Ćwiczenie 10.54 Udowodnić, że zbiór $I = \{2\varphi + (1 - \sqrt{-5})\psi : \varphi, \psi \in \mathbb{Z}[\tau_{-5}]\}$ jest niegłównym(!) ideałem w pierścieniu $\mathbb{Z}[\tau_{-5}]$.

10.2.6 Związek z formami kwadratowymi

Arytmetyka pierścienia $\mathbb{Z}[\tau_D]$ może być wykorzystana do badania form kwadratowych. W tym ustępie powiemy słów kilka o tym jak się to robi. Podstawową jest tu obserwacja, że norma elementu $x + y\tau_D \in \mathbb{Z}[\tau_D]$ jest, zgodnie z C10.34, wartością pewnej formy kwadratowej na parze (x, y).

Definicja 10.18 Niech $D \neq 1$ będzie liczbą całkowitą bezkwadratową. Zdefiniujmy:

$$f_D(X, Y) = \begin{cases} X^2 - DY^2, & \text{gdy } D \equiv 2, 3 \,(\mathrm{mod}\, 4), \\ X^2 + XY + \frac{1}{4}(1 - D)\, Y^2, & \text{gdy } D \equiv 1 \,(\mathrm{mod}\, 4). \end{cases} \tag{10.28}$$

Tak zdefiniowaną formę $f_D(X, Y)$ nazywamy **formą kanoniczną** wyznaczoną przez liczbę bezkwadratową D.

Będziemy teraz zakładać, że $\mathbb{Z}[\tau_D]$ jest dziedziną ideałów głównych. Wiemy, że istnieje 21 liczb bezkwadratowych D, dla których $\mathbb{Z}[\tau_D]$ jest pierścieniem normowo-euklidesowym. W każdym z tych pierścieni nierozkładalność jest r ó w n o w a ż n a pierwszości, zobacz C10.52 i C10.53. Dzięki tej równoważności mogliśmy podać w ustępie 10.1.4 piękny dowód twierdzenia Fermat'*a*-Eulera. Taki sam argument zastosować można w pozostałych 20 przypadkach:

TWIERDZENIE 10.12 *Niech D będzie taką bezkwadratową liczbą całkowitą, że w pierścieniu $\mathbb{Z}[\tau_D]$ każdy element nierozkładalny jest elementem pierwszym. Niech $p > 2$ będzie taką liczbą pierwszą, że $D\mathbf{R}p$. Wówczas forma kanoniczna $f_D(X, Y)$ przedstawia (właściwie) co najmniej jedną z liczb p, $-p$.*

D O W Ó D. Niech $D\mathbf{R}p$, czyli niech $a^2 \equiv D \pmod p$ dla pewnego $a \not\equiv 0 \pmod p$. Mamy więc równość $a^2 - D = pu$ dla pewnego $u \in \mathbb{Z}$, którą możemy zapisać tak:

$$pu = (a + \sqrt{D})(a - \sqrt{D}).$$

Równość tę zapisujemy (w zależności od reszty z dzielenia D przez 4) w jednej z postaci:

$$pu = \begin{cases} (a - 1 + 2\tau_D)(a + 1 - 2\tau_D), & \text{gdy } D \equiv 1 \pmod 4, \\ (a + \tau_D)(a - \tau_D), & \text{gdy } D \equiv 2,\, 3 \pmod 4, \end{cases} \tag{10.29}$$

zobacz (10.15). Stąd widzimy, że p dzieli iloczyn dwóch czynników w pierścieniu $\mathbb{Z}[\tau_D]$. Ale p n i e dzieli żadnego z czynników tego iloczynu. Istotnie, gdyby $p|(a-1+2\tau_D)$, czyli $a-1+2\tau_D = p(b + c\tau_D)$ dla pewnego $b + c\tau_D \in \mathbb{Z}[\tau_D]$, to zachodziłaby równość $2 = pc$, zobacz C10.33. Ponieważ $p > 2$, więc to jest niemożliwe. Podobnie sprawdzamy, że p nie dzieli (w $\mathbb{Z}[\tau_D]$ (!)) innych czynników w rozkładzie (10.29). Wobec tego p nie jest elementem pierwszym w $\mathbb{Z}[\tau_D]$. Ponieważ zakładamy, że w $\mathbb{Z}[\tau_D]$ każdy element nierozkładalny jest elementem pierwszym, a p nie jest pierwszy, więc p nie jest nierozkładalny. Zatem istnieją takie $\alpha,\, \beta \in \mathbb{Z}[\tau_D]$, że $p = \alpha\beta$ i $\alpha \not\sim 1$, $\beta \not\sim 1$. Wtedy $p^2 = |\mathbf{N}(p)| = |\mathbf{N}(\alpha)| \cdot |\mathbf{N}(\beta)|$ i $|\mathbf{N}(\alpha)| \neq 1$, $|\mathbf{N}(\beta)| \neq 1$. Niech $\alpha = x + y\tau_D$. Wówczas

$$p = |\mathbf{N}(\alpha)| = \left.\begin{cases} |x^2 + xy + \frac{1}{4}(1 - D)y^2|, & \text{gdy } D \equiv 1 \pmod 4, \\ |x^2 - Dy^2|, & \text{gdy } D \equiv 2,\, 3 \pmod 4 \end{cases}\right\} = |f_D(x,\, y)|,$$

patrz C10.34 i (10.28). To kończy dowód. □

Ćwiczenie 10.55 Wyprowadzić z powyższego nowy dowód T8.6 ($\Longleftarrow$).

P r z y k ł a d 1. Rozwiążemy teraz jeszcze raz ćwiczenie C8.10: Niech $p \in \mathbb{P}$ i niech $p \equiv 1,\, 7 \pmod{12}$. Wówczas, zobacz (5.85), $a^2 \equiv -3 \pmod p$ dla pewnego $a \in \mathbb{Z}$. Więc $p|(a + \sqrt{-3})(a - \sqrt{-3})$ w $\mathbb{Z}[\tau_{-3}]$. Łatwo jednak sprawdzić, że $p \nmid (a \pm \sqrt{-3})$. Zatem p n i e jest elementem pierwszym w $\mathbb{Z}[\tau_{-3}]$, więc nie jest też elementem nierozkładalnym (zobacz C10.53). Wobec tego istnieją takie $\alpha,\, \beta \in \mathbb{Z}[\tau_{-3}]$, że $p = \alpha\beta$ i $\alpha \not\sim 1$, $\beta \not\sim 1$. Wtedy $p^2 = \mathbf{N}(p) = \mathbf{N}(\alpha)\mathbf{N}(\beta)$ i $\mathbf{N}(\alpha) \neq 1$, $\mathbf{N}(\beta) \neq 1$. Niech $\alpha = a + b\tau_{-3}$. Wówczas $p = \mathbf{N}(\alpha) = a^2 + ab + b^2$, zobacz C10.34. W ten sposób znowu(?) rozwiązaliśmy ćwiczenie C8.23. Zauważmy teraz, że suma $a^2 + ab + b^2$ jest równa

$$\left(\frac{a-b}{2}\right)^2 + 3\left(\frac{a+b}{2}\right)^2 = \left(a + \frac{b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2 = \left(\frac{a}{2} + b\right)^2 + 3\left(\frac{a}{2}\right)^2,$$

porównaj P3 z ustępu 8.4.2. Stąd widać, że jeżeli w równości $p = a^2+ab+b^2$ obie liczby a, b są nieparzyste, to kładąc $x = (a-b)/2$, $y = (a+b)/2$ mamy przedstawienie $p = x^2 + 3y^2$. Jeżeli b jest parzyste, to kładziemy $x = a + b/2$, $y = b/2$, jeżeli zaś a jest parzyste, to kładziemy $x = a/2 + b$, $y = a/2$ i znów mamy przedstawienie $p = x^2 + 3y^2$, $x,\, y \in \mathbb{Z}$. ◊

Ćwiczenie 10.56 Wykorzystując fakt, że pierścień $\mathbb{Z}[\tau_{-7}]$ jest pierścieniem normowo-euklidesowym udowodnić, że każda liczba pierwsza $p \equiv 1,\, 9,\, 11,\, 15,\, 23,\, 25 \pmod{28}$ da się przedstawić w postaci $x^2 + 7y^2$. Zobacz też C8.24.

Ćwiczenie 10.57 Udowodnić, że jeżeli $p > 2$ jest taką liczbą pierwszą, że $(-11)\mathbf{R}p$, to p da się przedstawić w postaci $x^2 + xy + 3y^2$. Udowodnić też, że wówczas liczba $4p$ da się przedstawić w postaci $x^2 + 11y^2$. Zastanowić się nad charakteryzacją tych liczb pierwszych, które dają się przedstawić przez formę $X^2 + 11Y^2$.

Również rzeczywiste normowo-euklidesowe pierścienie kwadratowe można wykorzystać dla przedstawiania liczb pierwszych przez formy kwadratowe:

P r z y k ł a d 2. Wyznaczymy wszystkie liczby pierwsze $p \neq 2, 5$, które dają się przedstawić przez formę $X^2 - 5Y^2$. Załóżmy, że zachodzi równość $\pm p = x^2 - 5y^2$ dla pewnych liczb całkowitych x, y. Wówczas(!) $p \nmid y$. Mnożąc kongruencję $x^2 \equiv 5y^2 \,(\mathrm{mod}\, p)$ przez odwrotność $y^{-1} \,(\mathrm{mod}\, p)$, zobacz D5.3, mamy $(xy^{-1})^2 \equiv 5 \,(\mathrm{mod}\, p)$. I widzimy, że $5\mathbf{R}p$. Czyli że $(5|p) = +1$. Ale, zobacz 5.7.5 U2, $(5|p) = (p|5)$. Wobec tego $p \equiv \pm 1 \,(\mathrm{mod}\, 5)$.

Odwrotnie, załóżmy, że $p \equiv \pm 1 \,(\mathrm{mod}\, 5)$. Wtedy $+1 = (p|5) = (5|p)$. Czyli $5\mathbf{R}p$. Z twierdzenia T10.12 wnosimy więc, że $|f_5(a, b)| = |a^2 + ab - b^2| = p$ dla pewnych $a, b \in \mathbb{Z}$. Ponadto suma $a^2 + ab - b^2$ jest równa

$$\left(\frac{3a-b}{2}\right)^2 - 5\left(\frac{a-b}{2}\right)^2 = \left(\frac{3a+4b}{2}\right)^2 - 5\left(\frac{a+2b}{2}\right)^2 = \left(\frac{2a+b}{2}\right)^2 - 5\left(\frac{b}{2}\right)^2.$$

Stąd widać, że jeżeli w równości $p = |a^2 + ab - b^2|$ obie liczby a, b są nieparzyste, to kładąc $x = (3a - b)/2$, $y = (a - b)/2$ mamy przedstawienie $p = |x^2 - 5y^2|$. Gdy a jest parzyste, to kładziemy $x = (3a + 4b)/2$, $y = (a + 2b)/2$, gdy zaś b jest parzyste, to kładziemy $x = (2a + b)/2$, $y = b/2$ i znów mamy przedstawienie $p = |x^2 - 5y^2|$, $x, y \in \mathbb{Z}$. Na koniec zauważmy, że $(2x + 5y)^2 - 5(x + 2y)^2 = -(x^2 - 5y^2)$. To pozwala nam dać wyczerpującą o d p o w i e d ź: *Jeżeli* $p \equiv \pm 1 \,(\mathrm{mod}\, 5)$ *jest liczbą pierwszą, to istnieją takie liczby całkowite* x, y, *że* $x^2 - 5y^2 = p$ *i takie liczby całkowite* x_1, y_1, *że* $x_1^2 - 5y_1^2 = -p$. *Odwrotnie, jeżeli* $p = |x^2 - 5y^2|$ *jest liczbą pierwszą i* $p \neq 5$, *to* $p \equiv \pm 1 \,(\mathrm{mod}\, 5)$. ◊

Ćwiczenie 10.58 Udowodnić, że jeżeli równanie $x^2 - 5y^2 = n$ ma rozwiązanie, to ma nieskończenie wiele rozwiązań.

Ćwiczenie 10.59 Scharakteryzować zbiór $\{x^2 - 5y^2 : x, y \in \mathbb{Z}\}$. *Wskazówka.* Zobacz T8.2 i tożsamość Brahmagupty (8.1).

P r z y k ł a d 3. Przypatrzymy się teraz formie $X^2 - 6Y^2$. Zgodnie z filozofią tego ustępu wykorzystujemy pierścień $\mathbb{Z}[\tau_6]$. Wiemy, że jest on normowo-euklidesowy, zobacz Z10.6. Zatem każdy element nierozkładalny w $\mathbb{Z}[\tau_6]$ jest pierwszy. Dzięki prawu wzajemności sprawdzamy, że $6\mathbf{R}p$ wtedy i tylko wtedy, gdy $p \equiv 1, 5, 19, 23 \,(\mathrm{mod}\, 24)$. Wobec tego, jeżeli p jest liczbą pierwszą z jednego z ciągów $(24t + 1)$, $(24t + 5)$, $(24t + 19)$ lub $(24t + 23)$, to istnieje taka liczba $a \in \mathbb{Z}$, że $p|a^2 - 6$, czyli $p|(a + \sqrt{6})(a - \sqrt{6})$ w pierścieniu $\mathbb{Z}[\tau_6]$. Sprawdzenie, że $p \nmid (a \pm \sqrt{6})$ w $\mathbb{Z}[\tau_6]$, jest natychmiastowe. Zatem p nie jest elementem pierwszym w $\mathbb{Z}[\tau_6]$. Nie jest więc też elementem nierozkładalnym. Przeto istnieje rozkład $p = (a + b\sqrt{6})(c + d\sqrt{6})$, w którym $|\mathbf{N}(a + b\sqrt{6})| \neq 1$ i $|\mathbf{N}(c + d\sqrt{6})| \neq 1$. Podobnie jak wyżej znajdujemy stąd, że $|\mathbf{N}(a + b\sqrt{6})| = p$. Więc $a^2 - 6b^2 = \pm p$.

Teraz należy odróżnić dwa przypadki: (1) $p \equiv 1, 19 \,(\mathrm{mod}\, 24)$, (2) $p \equiv 5, 23 \,(\mathrm{mod}\, 24)$.

W przypadku (1) nie może zachodzić równość $a^2-6b^2=-p$, co łatwo sprawdzić redukując modulo 6. Byłoby wtedy $-1, -19 \equiv 5 \equiv a^2 \pmod 6$, co jest niemożliwe (bo kwadratami modulo 6 są 0, 1, 4, 3). Zachodzi więc równość $x^2-6y^2=p$ dla pewnych $x, y \in \mathbb{Z}$.

W przypadku (2) nie może zachodzić równość $a^2-6b^2=p$, co łatwo sprawdzić redukując modulo 6. Byłoby wtedy $5, 23 \equiv 5 \equiv a^2 \pmod 6$, co jest niemożliwe. Zachodzi więc równość $x^2-6y^2=-p$ dla pewnych $x, y \in \mathbb{Z}$. $\Diamond$

Ćwiczenie 10.60 Sprawdzić, że jeżeli para $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ jest rozwiązaniem równania $x^2-6y^2=n$, to również para $(5x+12y, 2x+5y)$ jest rozwiązaniem tego równania.

Ćwiczenie 10.61 Opisać liczby całkowite przedstawiane przez formę X^2-13Y^2.

10.2.7 Jednoznaczność rozkładu

Pierścienie normowo-euklidesowe są **dziedzinami z jednoznacznością rozkładu**:

TWIERDZENIE 10.13 *Jeżeli pierścień $\mathbb{Z}[\tau_D]$ jest pierścieniem normowo-euklidesowym, to każdy niezerowy i nie będący jednością element α da się przedstawić w postaci iloczynu*

$$\alpha = \nu_1\nu_2 \cdot \ldots \cdot \nu_s, \tag{10.30}$$

elementów nierozkładalnych. Ponadto, przedstawienie (10.30) *jest jednoznaczne w tym sensie, że jeżeli dla elementów nierozkładalnych μ_i, zachodzi równość*

$$\alpha = \mu_1\mu_2 \cdot \ldots \cdot \mu_t, \tag{10.31}$$

to $t=s$ i, po ewentualnym przenumerowaniu, $\nu_1 \sim \mu_1$, $\nu_2 \sim \mu_2$, $\ldots$, $\nu_s \sim \mu_s$.

DOWÓD. Dowód jest natychmiastowym uogólnieniem dowodów twierdzeń T2.16 i T3.14.

Najpierw dowodzimy analogonu twierdzenia T2.14, czyli że każdy nie będący jednością niezerowy element dzieli się przez jakiś element nierozkładalny. Załóżmy nie wprost, że w zbiorze $\mathbb{Z}[\tau_D] \setminus (\mathbb{Z}[\tau_D]^* \cup \{0\})$ istnieją elementy, które nie są podzielne przez elementy nierozkładalne. Spośród wszystkich takich elementów wybierzmy taki element α, dla którego $|\mathbf{N}(\alpha)|$ jest najmniejsze (Zasada Minimum!). Ponieważ α nie jest nierozkładalny (bo każdy element dzieli się przez siebie), więc można zapisać go w postaci iloczynu $\beta\gamma$, gdzie $\beta, \gamma \notin \mathbb{Z}[\tau_D]^*$. Ale wtedy $|\mathbf{N}(\alpha)| = |\mathbf{N}(\beta)| \cdot |\mathbf{N}(\gamma)|$ i, wobec tego, że $|\mathbf{N}(\beta)|, |\mathbf{N}(\gamma)| > 1$, $|\mathbf{N}(\beta)| < |\mathbf{N}(\alpha)|$. Zatem β, a więc i α, dzieli się przez element nierozkładalny. Sprzeczność.

Dzięki temu możemy udowodnić istnienie rozkładu (10.30). Robi się to znowu nie wprost i znowu korzystając z Zasady Minimum. Gdyby istniały *złe* elementy nie dające się zapisać w postaci (10.30), to istniałby *zły* element α, dla którego $|\mathbf{N}(\alpha)|$ jest najmniejsze. Wówczas, na mocy poprzedniej części $\nu_1|\alpha$ dla pewnego elementu nierozkładalnego ν_1. Zatem $\alpha=\nu_1\beta$ dla pewnego β. Wtedy $|\mathbf{N}(\alpha)| = |\mathbf{N}(\nu_1)| \cdot |\mathbf{N}(\beta)|$, skąd widzimy, że $|\mathbf{N}(\beta)| < |\mathbf{N}(\alpha)|$, bo $|\mathbf{N}(\nu_1)| > 1$. I, jeżeli $|\mathbf{N}(\beta)| = 1$, to β jest jednością, więc $\alpha \sim \nu_1$, czyli $\alpha = \alpha$ jest rozkładem typu (10.30). Jeżeli zaś $|\mathbf{N}(\beta)| > 1$, to $|\mathbf{N}(\beta)| < |\mathbf{N}(\alpha)|$, więc β może być przedstawiony w postaci iloczynu $\nu_2 \cdot \ldots \cdot \nu_s$ elementów nierozkładalnych. Stąd $\alpha = \nu_1\nu_2 \cdot \ldots \cdot \nu_s$. Sprzeczność.

Dowód jednoznaczności rozkładu można przeprowadzić niemal tak samo jak odpowiedni fragment dowodu T2.16: zakładając, że istnieją *złe* elementy mające istotnie różne

rozkłady na iloczyn czynników nierozkładalnych, przypuśćmy, że α jest złym elementem, dla którego $|\mathbf{N}(\alpha)|$ jest najmniejsze i (10.30) i (10.31) są istotnie różnymi rozkładami. Wtedy $\nu_1|\mu_1\mu_2\cdot\ldots\cdot\mu_t$. Wykorzystamy teraz fakt, że k a ż d y element nierozkładalny jest elementem pierwszym, zobacz T10.9 i C10.53. Skoro element pierwszy ν_1 dzieli iloczyn, to musi dzielić któryś z czynników. Przenumerowując, możemy uznać, że $\nu_1|\mu_1$. Ale μ_1 też jest elementem pierwszym, więc, na mocy C10.51, $\mu_1=\nu_1\varepsilon$, gdzie $\varepsilon\in\mathbb{Z}[\tau_D]^*$. Dzięki temu dostajemy równość $\nu_1\nu_2\cdot\ldots\cdot\nu_s=\nu_1\varepsilon\mu_2\cdot\ldots\cdot\mu_t$. Skąd, po uproszczeniu przez ν_1, mamy $\nu_2\cdot\ldots\cdot\nu_s=(\varepsilon\mu_2)\cdot\ldots\cdot\mu_t=:\beta$. Ponieważ $|\mathbf{N}(\beta)|=|\mathbf{N}(\alpha)|/|\mathbf{N}(\nu_1)|<|\mathbf{N}(\alpha)|$, więc β ma jednoznaczny rozkład na czynniki nierozkładalne. Wobec tego, po ewentualnym przenumerowaniu, $\nu_2\sim\mu_2$, $\ldots$, $\nu_s\sim\mu_s$ i $s=t$. □

Pokażemy przykład wykorzystania jednoznaczności rozkładu w $\mathbb{Z}[\tau_{-11}]$:

P r z y k ł a d. Znajdziemy rozwiązania równania

$$y^2=x^3-11 \tag{10.32}$$

w liczbach całkowitych. Technika poszukiwania rozwiązań jest taka sama jak w zadaniu Z10.4. Załóżmy, że para $(x,\,y)$ jest rozwiązaniem. Wówczas w pierścieniu $\mathbb{Z}[\tau_{-11}]$ zachodzi równość

$$(y+\sqrt{-11})(y-\sqrt{-11})=x^3. \tag{10.33}$$

Oznaczmy $\delta=\mathrm{NWD}\,(y+\sqrt{-11},\,y-\sqrt{-11})$. Liczba δ, jako dzielnik liczb $y+\sqrt{-11}$ i $y-\sqrt{-11}$, jest dzielnikiem ich sumy i różnicy: $\delta|2y$ i $\delta|2\sqrt{-11}$. Ponieważ 2 i $\sqrt{-11}$ są elementami nierozkładalnymi w $\mathbb{Z}[\tau_{-11}]$, zobacz Z10.7 i C10.62, więc, na mocy jednoznaczności rozkładu, mamy tylko cztery możliwe przypadki:

$$(1)\ \delta\sim 1,\quad (2)\ \delta\sim 2,\quad (3)\ \delta\sim\sqrt{-11},\quad (4)\ \delta\sim 2\sqrt{-11}.$$

Pokażemy, że w rzeczywistości zachodzi tylko przypadek (1). W przypadkach (3) i (4) mamy bowiem $\sqrt{-11}|\delta$, więc $\sqrt{-11}|2y$, skąd $11|4y^2$, zobacz C10.40, zatem $11|y$. Wówczas równość (10.32) pokazuje, że $11|x$ i daje $11^2y_1=11^3x_1-11$, co jest niemożliwe. Również przypadek (2) nie ma miejsca. Jeżeli bowiem $2|y\pm\sqrt{-11}$, czyli $2|y\mp 1\pm 2\tau$, to $2|y\pm 1$. (Piszemy w skrócie $\tau=\tau_{-11}$, wobec czego $\sqrt{-11}=2\tau-1$.) I równość (10.33) możemy napisać w postaci

$$\left(\frac{y-1}{2}+\tau\right)\left(\frac{y+1}{2}-\tau\right)=2x_1^3,$$

z której wynika (dzięki nierozkładalności, czyli pierwszości liczby 2 (!)), że 2 dzieli co najmniej jeden czynnik z lewej strony. Ale, jeżeli $2|a+b\tau$, to $2|b$. Mamy więc sprzeczność.

Pozostał nam do zbadania p r z y p a d e k $\delta\sim 1$. Korzystamy z *triku*. [Czytelnik z łatwością sformułuje i udowodni prawdziwość *triku* w każdej dziedzinie z jednoznacznością rozkładu, por. T2.19 i C10.28.] Dzięki niemu możemy napisać

$$y+\sqrt{-11}=y-1+2\tau=(a+b\tau)^3=A+B\tau,$$

gdzie $A=a^3-9ab^2-3b^3$, $B=3a^2b+3ab^2-2b^3$, co łatwo sprawdzić, bo $\tau^2=\tau-3$ i $\tau^3=-3-2\tau$. Wystarczy teraz rozwiązać równanie $2=B=b(3a^2+3ab-2b^2)$. Dzięki jednoznaczności rozkładu w pierścieniu $\mathbb{Z}$ badamy tylko cztery przypadki: $b=\pm1,\pm2$. I znajdujemy rozwiązania $(a,\,b)=(0,\,-1)$, $(1,\,-1)$, $(1,\,2)$, $(-3,\,2)$. Te wartości dają kolejno $y=A+1=-4,\,4,\,-58,\,58$. Widzimy stąd, że $(x,\,y)=(3,\,\pm4)$, $(15,\,\pm58)$ są wszystkimi rozwiązaniami równania (10.32). ◊

ZADANIE 10.7 Udowodnić, że jeżeli $D \equiv 5 \,(\mathrm{mod}\, 8)$, to liczba 2 traktowana jako element pierścienia kwadratowego $\mathbb{Z}[\tau_D]$ jest elementem nierozkładalnym.

R o z w i ą z a n i e. Załóżmy, że $2 = \alpha\beta = (a + b\tau)(c + d\tau)$, gdzie $\tau = \tau_D$, jest rozkładem elementu 2 na iloczyn. Wówczas $2 = \alpha'\beta' = (a + b\tau')(c + d\tau')$, zobacz C10.2. Mnożąc te dwie równości stronami dostajemy

$$4 = \mathbf{N}(\alpha)\mathbf{N}(\beta) = (a^2 + ab - (2s+1)b^2)(c^2 + cd - (2s+1)d^2),$$

gdzie położyliśmy $D = 8s+5$, zobacz C10.34. Chcemy uzasadnić, że $|\mathbf{N}(\alpha)| = 1$ lub $|\mathbf{N}(\beta)| = 1$. Wystarczy w tym celu udowodnić, że żaden z dwóch czynników po prawej stronie powyższej równości n i e może być równy ± 2. To wynika z prostej analizy parzystości: jeżeli $a \equiv b \equiv 0 \,(\mathrm{mod}\, 2)$, to $a^2 + ab - (2s+1)b^2$ jest liczbą podzielną przez 4 (więc $\neq \pm 2$), a w pozostałych trzech przypadkach $a^2 + ab - (2s+1)b^2$ jest liczbą nieparzystą (więc $\neq \pm 2$). $\Diamond$

Ćwiczenie 10.62 Uzasadnić, że jeżeli $|D|$ jest liczbą pierwszą, to $\sqrt{D}$ jest elementem nierozkładalnym w pierścieniu $\mathbb{Z}[\tau_D]$.

10.2.8 Pierścienie $\mathbb{Z}[\tau_{-2}]$, $\mathbb{Z}[\tau_{-3}]$ i $\mathbb{Z}[\tau_{-5}]$

Powiemy teraz kilka słów o nazwanych w tytule ustępu pierścieniach kwadratowych. Dwa pierwsze są przykładami pierścieni z jednoznacznością rozkładu. Trzeci jest przykładem pierścienia b e z jednoznaczności rozkładu.

Pierścień Eulera $\mathbb{Z}[\sqrt{-2}\,]$

Poznamy bliżej pierścień $\mathbb{Z}[\tau_{-2}]$. Ponieważ Euler używał tego pierścienia rozwiązując równanie $y^2 = x^3 - 2$, więc proponujemy nazwę: **pierścień Eulera**. Ponieważ $-2 \equiv 2 \,(\mathrm{mod}\, 4)$, więc, zgodnie z (10.15), pierścień $\mathbb{Z}[\tau_{-2}]$ składa się ze wszystkich liczb postaci $a + b\sqrt{-2}$, gdzie $a, b \in \mathbb{Z}$. Używamy więc również oznaczenia $\mathbb{Z}[\sqrt{-2}\,]$.

Ćwiczenie 10.63 Uzasadnić, że $\mathbb{Z}[\sqrt{-2}\,]^*$ jest grupą dwuelementową $\{-1, +1\}$.

ZADANIE 10.8 Rozwiązać równanie $y^2 = x^3 - 2$ w liczbach całkowitych.

R o z w i ą z a n i e. Załóżmy, że para $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ jest rozwiązaniem. Łatwo sprawdzić, że wówczas y jest liczbą nieparzystą [gdy $y = 2u$, to $x = 2v$, więc $2u^2 = 4v^3 - 1$ co jest niemożliwe]. Piszemy w skrócie $\tau = \tau_{-2} = \sqrt{-2}$. W pierścieniu $\mathbb{Z}[\sqrt{-2}\,]$ mamy rozkład

$$(y + \tau)(y - \tau) = x^3. \tag{10.34}$$

Wykażemy, że czynniki $y + \tau$ i $y - \tau$ są względnie pierwsze w $\mathbb{Z}[\sqrt{-2}\,]$. Załóżmy, że $\delta \in \mathbb{Z}[\sqrt{-2}\,]$ jest wspólnym dzielnikiem czynników $y + \tau$ i $y - \tau$ tego rozkładu. Wówczas δ dzieli ich różnicę: $\delta | 2\tau$. Ale $2\tau = -\tau^3$ jest rozkładem na czynniki nierozkładalne w $\mathbb{Z}[\sqrt{-2}\,]$ (sprawdźcie!). Na mocy jednoznaczności rozkładu widzimy stąd, że $\delta \sim \tau^k$ przy pewnym $k = 0, 1, 2, 3$. Gdy $k > 0$, to $\tau | y + \tau$, więc $\tau | y$, stąd $\mathbf{N}(\tau) | \mathbf{N}(y)$, czyli $2 | y^2$, co jest niemożliwe, bo $y \equiv 1 \,(\mathrm{mod}\, 2)$. Wobec tego $\delta \sim 1$. Teraz możemy zastosować *trik* w pierścieniu

$\mathbb{Z}[\sqrt{-2}]$, zobacz C10.64. Ponieważ lewa strona równości (10.34) jest iloczynem czynników względnie pierwszych, więc każdy z czynników jest stowarzyszony z sześcianem:

$$y + \tau = (a + b\tau)^3$$

dla pewnego $a+b\tau \in \mathbb{Z}[\sqrt{-2}]$. Możemy napisać równość, ponieważ każda jedność w $\mathbb{Z}[\sqrt{-2}]$ jest sześcianem (!). Porównując części urojone obu stron tej równości mamy: $1 = 3a^2b - 2b^3$. Stąd $b = \pm 1$. Jeżeli $b = 1$, to $a = \pm 1$. Jeżeli $b = -1$, to $-1 = -3a^2$, co jest niemożliwe. Mamy stąd jedyne rozwiązania $x = 3$, $y = \pm 5$. ◊

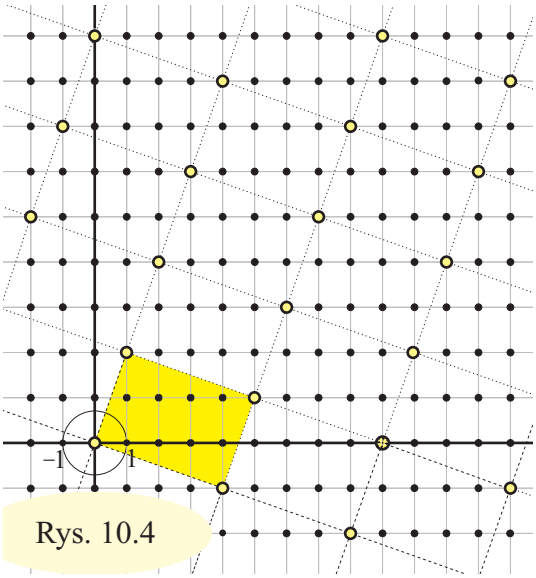
Ćwiczenie 10.64 Sformułować i udowodnić *trik* w $\mathbb{Z}[\sqrt{-2}]$.

Ćwiczenie 10.65 Spróbujcie rozwiązać w liczbach całkowitych równanie $y^2 = x^p - 2$ dla paru innych (może dla wszystkich?) wykładników pierwszych p.

Na rysunku 10.4 pokazujemy pierścień $\mathbb{Z}[\sqrt{-2}]$. Grubszymi kółeczkami zaznaczyliśmy ideał (główny, bo w $\mathbb{Z}[\sqrt{-2}]$ każdy ideał jest główny!) $(1 + 2\sqrt{-2})$. Cały pierścień $\mathbb{Z}[\sqrt{-2}]$ jest kratą $\Lambda(1, \sqrt{-2})$. Wskazany ideał jest kratą

$$\Lambda(4 - \sqrt{-2},\ 1 + 2\sqrt{-2}).$$

Zaznaczono równoległobok podstawowy kraty.



Rys. 10.4

Ćwiczenie 10.66 Uzasadnić, że każdy ideał w $\mathbb{Z}[\sqrt{-2}]$ jest kratą p o d o b n ą do kraty

$$(1) = \Lambda(1, \sqrt{-2}).$$

Ćwiczenie 10.67 Udowodnić, że pole równoległoboku podstawowego dowolnego ideału (α) jest równe $\mathbf{N}(\alpha)\sqrt{2}$. Zauważyć też, że ta teza jest równoważna faktowi, że w każdym równoległoboku podstawowym ideału (α) leży dokładnie $\mathbf{N}(\alpha) - 1$ punktów kraty (1) nie należących do kraty (α).

Zobaczmy jak rozkładają się liczby pierwsze $p \in \mathbb{P}$ na czynniki nierozkładalne w $\mathbb{Z}[\sqrt{-2}]$:

ZADANIE 10.9 Dowieść, że rozkład (10.30) liczby $p \in \mathbb{P}$ w $\mathbb{Z}[\sqrt{-2}]$ ma postać:

(1) $2 = -\sqrt{-2}\sqrt{-2}$,

(2) $p = (x + y\sqrt{-2})(x - y\sqrt{-2})$ gdy $p \equiv 1, 3 \pmod 8$,

(3) $p = p$, gdy $p \equiv 5, 7 \pmod 8$.

R o z w i ą z a n i e. Ponieważ $\mathbf{N}(\sqrt{-2}) = \mathbf{N}(-\sqrt{-2}) = 2$, więc elementy $\pm\sqrt{-2}$ są nierozkładalne w $\mathbb{Z}[\sqrt{-2}]$, zobacz C10.49. Równość $p = (x+y\sqrt{-2})(x-y\sqrt{-2})$ dla $p \equiv 1, 3 \pmod 8$ znamy z T8.6 (zobacz też C10.55). Pozostała nam do wykazania nierozkładalność liczb pierwszych $p \equiv 5, 7 \pmod 8$ w pierścieniu $\mathbb{Z}[\sqrt{-2}]$. Załóżmy, że taką liczbę pierwszą da się rozłożyć na czynniki w $\mathbb{Z}[\sqrt{-2}]$. Niech $p = \alpha\beta$ będzie rozkładem. Wówczas $p = \alpha'\beta'$, bo $p' = p$,

a sprzężenie iloczynu równe jest iloczynowi sprzężeń. Stąd $p^2 = \alpha\beta \cdot \alpha'\beta' = \mathbf{N}(\alpha)\mathbf{N}(\beta)$ i, jeżeli $\mathbf{N}(\alpha) \neq 1$, $\mathbf{N}(\beta) \neq 1$, to $p = \mathbf{N}(\alpha)$ i $p = \mathbf{N}(\beta)$. Jeżeli więc $\alpha = a + b\sqrt{-2}$, to $p = \mathbf{N}(\alpha) = a^2 + 2b^2$. Stąd, jak to już wielokrotnie robiliśmy, wnioskujemy, że $(-2)\mathbf{R}p$, czyli $p \equiv 1, 3 \,(\mathrm{mod}\, 8)$. Sprzeczność. ◊

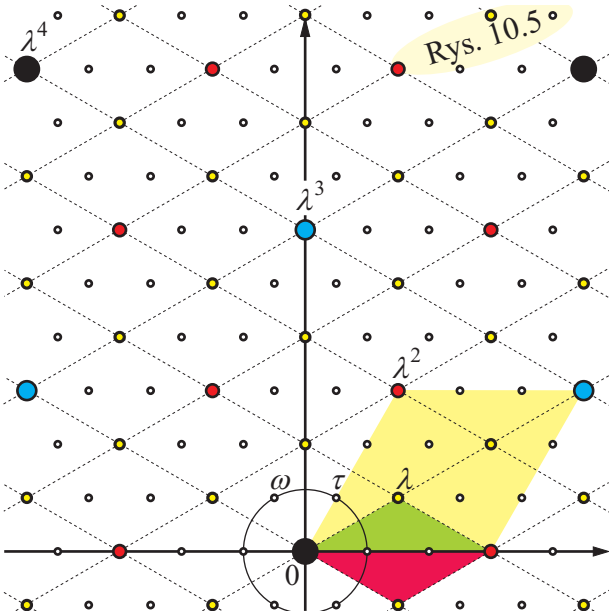
Pierścień Eisensteina

Przyjrzyjmy się teraz bliżej pierścieniowi $\mathbb{Z}[\tau_{-3}]$. Nazywamy go **pierścieniem Eisensteina** na cześć Eisensteina, który używał go do badania reszt sześciennych.

Elementy pierścienia $\mathbb{Z}[\tau_{-3}]$ zwane też **liczbami całkowitymi Eisensteina** tworzą piękną kratę. Na rysunku 10.5 oznaczyliśmy

$$\tau = \tau_{-3}, \quad \omega = \tau^2, \quad \lambda = \tau + 1.$$

Widzimy "siatkę" rombów, której węzły tworzą ideał główny (λ). Widzimy też romb podstawowy ideału (λ^2). Jasne, że krata (λ) jest obrazem kraty (1) względem podobieństwa spiralnego będącego złożeniem jednokładności o skali $\sqrt{3}$ i obrotu o kąt $30°$. Podobnie, z kraty (λ) powstaje krata (λ^2), z kraty (λ^2) powstaje krata (λ^3), itd. Łatwo widzieć, że krata (λ^4) pokrywa się z kratą (9).



Ćwiczenie 10.68 "Narysować" ideały główne (τ), $(2 - 3\omega)$ w pierścieniu Eisensteina.

Ćwiczenie 10.69 Uzasadnić, że $\mathbb{Z}[\tau_{-3}] = \mathbb{Z}[\,\omega\,]$.

Ćwiczenie 10.70 Korzystając z równości $\mathbf{N}(x + y\tau) = x^2 + xy + y^2$ udowodnić, że grupa $\mathbb{Z}[\,\omega\,]^*$ jedności pierścienia Eisensteina składa się ze wszystkich pierwiastków szóstego stopnia z jedynki. Zobacz rysunek 10.5.

Ćwiczenie 10.71 Udowodnić, że iloczyn liczb całkowitych, z których każda jest postaci $x^2 + xy + y^2$ jest również liczbą tej postaci. Napisać odpowiednią tożsamość algebraiczną.

Ćwiczenie 10.72 Udowodnić, że λ jest liczbą pierwszą Eisensteina. I że $3 = -\omega\lambda^2$ jest rozkładem liczby Eisensteina 3 na czynniki nierozkładalne w pierścieniu $\mathbb{Z}[\,\omega\,]$.

Jeżeli α, β i μ są liczbami całkowitymi Eisensteina, to zapis

$$\alpha \equiv \beta \,(\mathrm{mod}\, \mu)$$

oznacza, że $\mu | \alpha - \beta$, porównaj D5.1. Tak określona relacja **kongruencji modulo** μ ma wszystkie własności z twierdzenia T5.1. To znaczy, że jest relacją równoważności **zgodną z działaniami dodawania i mnożenia** (takiego zwrotu używamy dla powiedzenia, że kongruencje można dodawać i mnożyć stronami).

Ćwiczenie 10.73 Uzasadnić to. Wykazać również, że jeżeli $\mu_1 \sim \mu_2$, to kongruencja $\alpha \equiv \beta \,(\mathrm{mod}\, \mu_1)$ jest równoważna kongruencji $\alpha \equiv \beta \,(\mathrm{mod}\, \mu_2)$.

Ćwiczenie 10.74 Udowodnić, że jeżeli $\alpha \in \mathbb{Z}[\,\omega\,]$, to zachodzi dokładnie jedna z kongruencji: $\alpha \equiv 0 \,(\mathrm{mod}\, \lambda)$, $\alpha \equiv 1 \,(\mathrm{mod}\, \lambda)$ lub $\alpha \equiv 2 \equiv -1 \,(\mathrm{mod}\, \lambda)$. *Wskazówka.* To doskonale widać na rysunku 10.5, gdzie rozpoznajemy romby o wierzchołkach w punktach kraty (λ). Wewnątrz każdego takiego rombu leżą dwa punkty kraty Eisensteina $(1) = \mathbb{Z}[\,\omega\,]$. Na przykład w rombie o wierzchołkach 0, $\overline{\lambda}$, 3, λ leżą punkty 1, 2, a w rombie o wierzchołkach 0, λ, $\sqrt{-3}$, $\omega - 1$ leżą punkty ω, τ. Widzimy stąd, że jeżeli $\alpha \in \mathbb{Z}[\,\omega\,]$, to również zachodzi dokładnie jedna z kongruencji $\alpha \equiv 0 \,(\mathrm{mod}\, \lambda)$, $\alpha \equiv \omega \,(\mathrm{mod}\, \lambda)$ lub $\alpha \equiv \tau \,(\mathrm{mod}\, \lambda)$.

Tezę poniższego zadania wykorzystamy w ustępie 11.2.3:

ZADANIE 10.10 Udowodnić, że jeżeli $\alpha \in \mathbb{Z}[\,\omega\,]$ i $\lambda \nmid \alpha$, to $\alpha^3 \equiv \pm 1 \,(\mathrm{mod}\, 9)$.

Rozwiązanie. Ponieważ $\alpha \not\equiv 0 \,(\mathrm{mod}\, \lambda)$, więc, na mocy poprzedniego ćwiczenia, $\alpha \equiv \omega \,(\mathrm{mod}\, \lambda)$ lub $\alpha \equiv \tau \,(\mathrm{mod}\, \lambda)$. Zapiszmy więc w pierwszym przypadku $\alpha = \beta\lambda + \omega$, a w drugim przypadku $\alpha = \beta\lambda + \tau$ dla pewnego $\beta \in \mathbb{Z}[\,\omega\,]$. W pierwszym przypadku mamy:

$$\alpha^3 = (\beta\lambda + \omega)^3 = \lambda^3\beta^3 + 3\beta^2\lambda^2\omega + 3\beta\lambda\omega^2 + \omega^3.$$

Stąd, ponieważ $\omega^3 = 1$, $\lambda^2 = 3\tau$, a $\omega^2 = -\tau$, mamy

$$\alpha^3 - 1 = 3\tau\lambda\beta^3 + 9\beta^2\tau\omega - 3\beta\lambda\tau = 3\tau\lambda\beta(\beta^2 - 1) - 9\beta^2 = 3\tau\lambda\,[\beta(\beta - 1)(\beta + 1)] - 9\beta^2.$$

Ponieważ (dokładnie) jeden z czynników iloczynu w nawiasie kwadratowym jest podzielny przez λ, a $\lambda^2 = 3\tau$, więc widać stąd, że $9 | \alpha^3 - 1$. W przypadku gdy $\alpha \equiv \tau \,(\mathrm{mod}\, \lambda)$ sprawdzamy analogicznie, że $\alpha^3 - \tau^3 = \alpha^3 + 1$ jest podzielne przez 9. $\Diamond$

Zobaczymy jak rozkładają się liczby pierwsze $p \in \mathbb{P}$ na czynniki nierozkładalne w $\mathbb{Z}[\,\omega\,]$.

Ćwiczenie 10.75 Dowieść, że rozkład (10.30) liczby $p \in \mathbb{P}$ w $\mathbb{Z}[\,\omega\,]$ ma postać:

(1) $3 = -\omega\lambda^2$,

(2) $p = (x + y\omega)(x + y\omega^2)$ gdy $p \equiv 1 \,(\mathrm{mod}\, 3)$,

(3) $p = p$, gdy $p \equiv 2 \,(\mathrm{mod}\, 3)$.

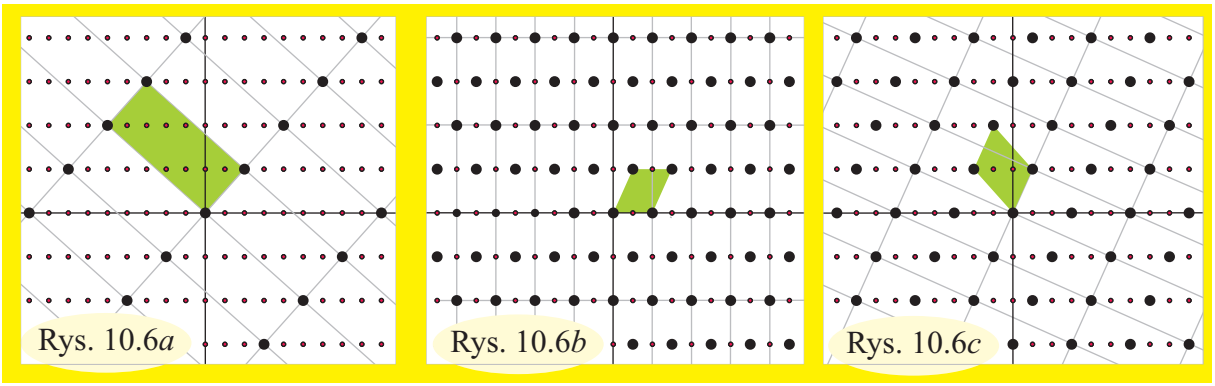
Pierścień Dedekinda

Pierścień $\mathbb{Z}[\tau_{-5}]$ nazwiemy **pierścieniem Dedekinda**. Warto się dowiedzieć czegoś na jego temat. Jest on bowiem przykładem pierścienia kwadratowego, który n i e j e s t dziedziną ideałów głównych i nie ma w nim jednoznaczności rozkładu elementów na czynniki nierozkładalne.

Na rysunkach 10.6 przedstawiamy ilustracje trzech ideałów w pierścieniu Dedekinda. Na rysunku 10.6*a* widzimy ideał g ł ó w n y $I = (2 + \sqrt{-5})$. Elementy tego ideału są iloczynami $(2 + \sqrt{-5})\alpha$, gdzie $\alpha \in \mathbb{Z}[\tau_{-5}]$. To znaczy, że I jest obrazem $I = M_{2+\sqrt{5}i}(\mathbb{Z}[\tau_{-5}])$ kraty Dedekinda względem podobieństwa spiralnego $M_{2+\sqrt{5}i}$. Wobec tego ideał I (jako podzbiór płaszczyzny) jest p o d o b n y do $(1) = \mathbb{Z}[\tau_{-5}]$. Ogólniej: *Jeżeli $D < 0$, to wszystkie niezerowe ideały główne w pierścieniu $\mathbb{Z}[\tau_D]$ są podobne.*

W pierścieniu Dedekinda istnieją ideały n i e g ł ó w n e, zobacz C10.54. Na rysunkach 10.6*b* i 10.6*c* pokazujemy dwa takie ideały: $I_2 = (2,\, 1 + \sqrt{-5})$ i $I_3 = (3,\, 1 + \sqrt{-5})$.

Ćwiczenie 10.76 Udowodnić, że podobieństwo spiralne M_φ, gdzie $\varphi = (1+\sqrt{-5})/2$ przeprowadza ideał (kratę) I_2 na ideał (kratę) I_3.



ZADANIE 10.11 Udowodnić, że w pierścieniu Dedekinda istnieją dokładnie dwa kształty ideałów niezerowych. To znaczy, że jeżeli I jest niegłównym ideałem w $\mathbb{Z}[\tau_{-5}]$, to istnieje taka liczba zespolona ψ, że $M_\psi(I) = (2,\, 1+\sqrt{-5})$.

Rozwiązanie. Niech I będzie niezerowym ideałem w $\mathbb{Z}[\sqrt{-5}]$. Załóżmy, że ideał I nie jest ideałem głównym. Pamiętając dowód twierdzenia T8.3, wybierzmy niezerowy element $\alpha \in I$ najbliższy punktu (liczby) 0. Wówczas wszystkie punkty $x\alpha + y\tau\alpha$, gdzie $x, y \in \mathbb{Z}$, kraty $\Lambda = \Lambda(\alpha, \tau\alpha)$ należą do ideału I. Łatwo sprawdzić, że $\Lambda = (\alpha)$. Ponieważ założyliśmy, że ideał I nie jest ideałem głównym, więc do I należą elementy ξ nie należące do Λ.

Niech $\xi = x\alpha + y\tau\alpha \in I \setminus \Lambda$ będzie dowolnym elementem ideału I nie należącym do $\Lambda = (\alpha)$. Wybierzmy takie liczby całkowite k, l, by $|x-k| \leqslant 1/2$ i $|y-l| \leqslant 1/2$. Wówczas

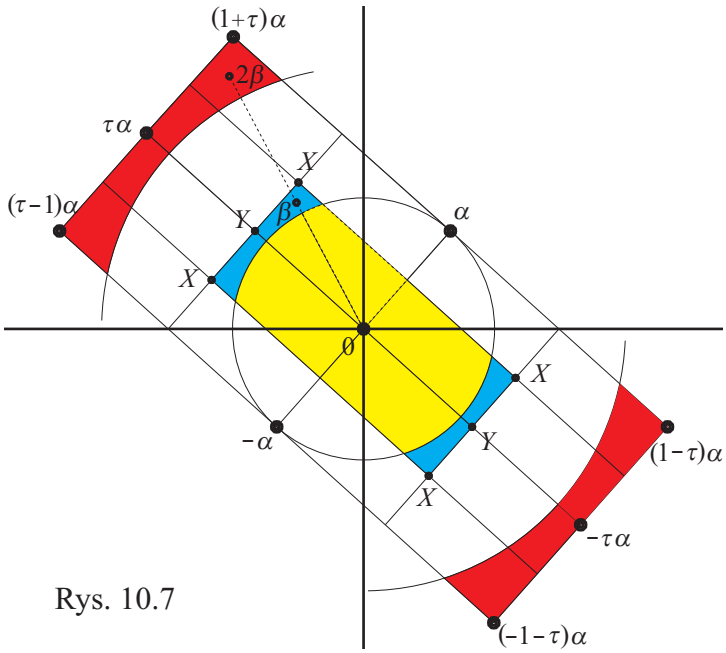
$$\zeta := k\alpha + l\tau\alpha = (k+l\tau)\alpha \in (\alpha) \subset I.$$

Wobec tego

$$\beta := \xi - \zeta = (x-k)\alpha + (y-l)\tau\alpha$$

należy do I i leży w prostokącie

$$\mathcal{P} = \{x\alpha + y\tau\alpha :\ |x| \leqslant \tfrac{1}{2},\ |y| \leqslant \tfrac{1}{2}\}.$$



Rys. 10.7

Wierzchołki tego prostokąta oznaczyliśmy na rysunku 10.7 literą X. Ponieważ α jest najbliższym 0 punktem ideału I, więc β leży na zewnątrz koła $\mathcal{D}(0, |\alpha|)$ lub na okręgu tego koła. Wobec tego β leży gdzieś w jednym z dwóch zacieniowanych trapezików krzywoliniowych w prostokącie $\mathcal{P}$. Pokażemy, że β może być tylko jednym z wierzchołków prostokąta $\mathcal{P}$. Aby to zobaczyć rozważmy element $2\beta \in I$. Widać

gołym okiem, że jego odległość od pewnego punktu γ ideału (α) jest mniejsza(!) niż $|\alpha|$. Wtedy $\gamma - 2\beta \in I$ i $|\gamma - 2\beta| < |\alpha|$, co, wobec wyboru α, jest możliwe tylko gdy $\gamma - 2\beta = 0$. Więc β jest albo jednym z wierzchołków X, albo jednym ze środków $Y = \pm\tau\alpha/2$. Gdyby jednakże $\beta = \tau\alpha/2$, to $\tau\beta + 3\alpha = \alpha/2$ byłby elementem ideału I bliższym 0 niż α. Podobnie sprawdzamy, że $\beta \neq -\tau\alpha/2$. Wobec tego β jest jednym z wierzchołków X. Jasne, że wówczas pozostałe wierzchołki X również należą do I (jeżeli β jest "górnym" wierzchołkiem na rysunku, to pozostałymi wierzchołkami są $\beta - \alpha$, $\beta - \tau\alpha$ i $\beta - \alpha - \tau\alpha$).

Widzimy więc, że ideał niegłówny I jest sumą teoriomnogościową ideału głównego (α) generowanego przez element najbliższy 0 i zbioru środków wszystkich prostokątów o wierzchołkach $\varphi\alpha$, $\varphi\alpha+\alpha$, $\varphi\alpha+\tau\alpha$, $\varphi\alpha+\alpha+\tau\alpha$, gdzie φ jest elementem pierścienia Dedekinda. Łatwo się przekonać, że wobec tego jest on podobny do I_2 z rysunku 10.6*b*, na którym widzimy sumę teoriomnogościową ideału głównego (2) i zbioru środków wyznaczonych przez niego prostokątów. [Na rysunku 10.6*c* również możemy dostrzec sumę teoriomnogościową ideału głównego $(1+\sqrt{-5})$ i zbioru środków odpowiednich prostokątów.] $\Diamond$

Fakt, że w pierścieniu Dedekinda istnieją ideały niegłówne jest oczywiście ściśle związany z faktem, że pierścień ten n i e j e s t dziedziną z jednoznacznością rozkładu:

Ćwiczenie 10.77 Uzasadnić, że element 6 pierścienia $\mathbb{Z}[\tau_{-5}]$ ma dwa istotnie różne rozkłady na iloczyn elementów nierozkładalnych: $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Znaleźć jeszcze inne przykłady niejednoznaczności rozkładu w pierścieniu $\mathbb{Z}[\tau_{-5}]$.

U w a g a. Niezerowy ideał I w urojonym pierścieniu kwadratowym jest kratą w płaszczyźnie. Z dowodu twierdzenia T8.3 wiemy, że ta krata jest postaci $\Lambda(\alpha, \beta)$, gdzie α jest najbliższym od 0 elementem ideału I, a β jest najbliższym od 0 elementem ideału I, który nie leży na prostej $l_{0\alpha}$. Takie dwa elementy α, β wyznaczają formę kwadratową

$$f(X, Y) = (\alpha X + \beta Y)(\alpha' X + \beta' Y) = \mathbf{N}(\alpha)X^2 + (\alpha\beta' + \beta\alpha')XY + \mathbf{N}(\beta)Y^2. \qquad (10.35)$$

Ćwiczenie 10.78 Napisać formy kwadratowe wyznaczone przez ideały pokazane na rysunkach 10.6. Porównać otrzymane wyniki z wierszem $\Delta = -20$ w tabelce z ustępu 8.4.4.

Ćwiczenie 10.79 Wskazać trzy parami niepodobne ideały w pierścieniu $\mathbb{Z}[\tau_{-23}]$.

10.3 Teoria podzielności w dig'*ach*

W tym paragrafie, który ma charakter pewnego podsumowania i jednocześnie wstępu do teorii pierścieni, opiszemy krótko teorię podzielności w **dziedzinach ideałów głównych**. Okaże się, że jeżeli dany pierścień $\mathcal{R}$ jest dig'*iem*, to w pierścieniu tym zachodzi twierdzenie o istnieniu i jednoznaczności rozkładu na czynniki nierozkładalne.

10.3.1 Dziedziny całkowitości

Zaczniemy od ogólnych uwag na temat pierścieni, w których nie ma dzielników zera.

Definicja 10.19 Pierścień $\mathcal{R}$ nazywa się **dziedziną całkowitości**, gdy nie ma w nim dzielników zera, co oznacza, że jeżeli $\alpha, \beta \in \mathcal{R}$ oraz $\alpha\beta = 0$, to $\alpha = 0$ lub $\beta = 0$.

P r z y k ł a d. Pierścień $\mathbb{Z}$ liczb całkowitych jest dziedziną całkowitości. Dziedzinami całkowitości są wszystkie ciała, zobacz C1.19. Również pierścienie $\mathbb{K}[X]$ wielomianów jednej zmiennej o współczynnikach w ciele są dziedzinami całkowitości, zobacz C3.32. Pierścień $\mathbb{Z}/m$ klas reszt liczb całkowitych modulo m jest dziedziną całkowitości wtedy i tylko wtedy, gdy jest ciałem, czyli wtedy i tylko wtedy, gdy m jest liczbą pierwszą, zob. T5.11 i C1.20. $\Diamond$

Ćwiczenie 10.80 Udowodnić, że w dowolnych dziedzinach całkowitości prawdziwe jest ***prawo skracania***: *Jeżeli dla* $\alpha, \beta, \gamma \in \mathcal{R}$ *zachodzi równość* $\alpha\beta = \alpha\gamma$ *i* $\alpha \neq 0$, *to* $\beta = \gamma$.

Ćwiczenie 10.81 Udowodnić, że jeżeli $\mathcal{R}$ jest dziedziną całkowitości, to pierścień $\mathcal{R}[X]$ wielomianów jednej zmiennej o współczynnikach w $\mathcal{R}$ jest dziedziną całkowitości. Wywnioskować stąd, że pierścień wielomianów n zmiennych o współczynnikach w ciele jest dziedziną całkowitości.

Ćwiczenie 10.82 Udowodnić uogólnienie twierdzenia T3.4: *Jeżeli* $f(X) \in \mathcal{R}[X]$ *jest wielomianem stopnia* $n \geqslant 1$ *o współczynnikach w dziedzinie całkowitości* $\mathcal{R}$, *to w* $\mathcal{R}$ *istnieje co najwyżej* n *pierwiastków wielomianu* $f(X)$.

10.3.2 Relacja podzielności. Relacja stowarzyszenia

W dalszym ciągu $\mathcal{R}$ oznaczać będzie dowolną dziedzinę całkowitości. Przypomnijmy, że przez $\mathcal{R}^*$ oznaczamy zbiór (grupę!) jedności, czyli elementów odwracalnych pierścienia $\mathcal{R}$.

Definicja 10.20 Jeżeli $\alpha, \beta \in \mathcal{R}$, to mówimy, że α **dzieli** β, gdy istnieje takie $\gamma \in \mathcal{R}$, że $\beta = \alpha \cdot \gamma$. Piszemy wtedy $\alpha|\beta$. Mówimy też w takiej sytuacji, że α jest **dzielnikiem** β, lub że β jest **wielokrotnością** α. Jeżeli $\alpha \in \mathcal{R}$, to zbiór $(\alpha) := \{\alpha\varphi : \varphi \in \mathcal{R}\}$ wszystkich wielokrotności elementu α nazywamy **ideałem głównym** generowanym przez α.

ZADANIE 10.12 Sformułować i udowodnić analogony tez (1), (2), (3), (4) z T2.1 w przypadku dowolnych dziedzin całkowitości.

R o z w i ą z a n i e. Pewnego komentarza wymaga tylko teza (3), której prawidłowe sformułowanie jest następujące:

(3a) jeżeli $\alpha|\beta$ i $\beta|\alpha$, to istnieje taka jedność (= element odwracalny) ε, że $\alpha = \varepsilon\beta$.

Dowód jest prosty: Niech $\beta = \alpha\gamma$ i $\alpha = \beta\delta$ dla pewnych $\gamma, \delta \in \mathcal{R}$. Wówczas $\beta \cdot 1 = \beta = \alpha\gamma = (\beta\delta)\gamma = \beta(\delta\gamma)$. Jeżeli $\beta \neq 0$, to, dzięki prawu skracania, zobacz C10.80, $1 = \delta\gamma$, więc $\delta \in \mathcal{R}^*$ i wystarczy położyć $\varepsilon = \delta$. Jeżeli zaś $\beta = 0$, to $\alpha = \beta\gamma = 0 \cdot \gamma = 0$, zobacz Z1.6(1), więc $\alpha = 1 \cdot \beta$. $\Diamond$

Ćwiczenie 10.83 Udowodnić, że jeżeli $\alpha, \beta \in \mathcal{R}$, a $\varepsilon, \eta \in \mathcal{R}^*$, to $\alpha|\beta$ wtedy i tylko wtedy, gdy $\varepsilon\alpha|\eta\beta$.

Z ćwiczenia C10.83 widzimy, że jedności pierścienia $\mathcal{R}$ są, z punktu widzenia podzielności, "bytami nieistotnymi". Wobec tego przyjmujemy:

Definicja 10.21 Niech $\mathcal{R}$ będzie dziedziną całkowitości. Elementy $\alpha, \beta \in \mathcal{R}$ nazywamy **stowarzyszonymi**, gdy istnieje taka jedność $\varepsilon \in \mathcal{R}^*$, że $\alpha = \varepsilon\beta$. Zapisujemy to tak: $\alpha \sim \beta$.

Ćwiczenie 10.84 Uzasadnić, że relacja stowarzyszenia $\sim$ jest relacją równoważności, to znaczy, zobacz $\mathbb{KOM}$, że (1) $\alpha \sim \alpha$; (2) $\alpha \sim \beta \Rightarrow \beta \sim \alpha$; (3) $\alpha \sim \beta$, $\beta \sim \gamma \Rightarrow \alpha \sim \gamma$.

Ćwiczenie 10.85 Udowodnić, że α jest jednością wtedy i tylko wtedy, gdy $\alpha \sim 1$.

Ćwiczenie 10.86 Uzasadnić, że jeżeli $\alpha, \beta \in \mathcal{R}$, to

$$\alpha|\beta \quad \Longleftrightarrow \quad (\beta) \subseteq (\alpha).$$

Wywnioskować stąd, że $(\alpha) = (\beta) \Leftrightarrow \alpha \sim \beta$.

10.3.3 Ideał. Dziedzina ideałów głównych

Definicja ideału w dowolnym pierścieniu naśladuje odpowiednie definicje w przypadku pierścieni $\mathbb{Z}$, zobacz D2.2, i $\mathbb{K}[X]$, zobacz D3.8.

Definicja 10.22 Niepusty podzbiór $I \subseteq \mathcal{R}$ nazywamy **ideałem w pierścieniu** $\mathcal{R}$, gdy

(1) jeżeli $\alpha, \beta \in I$, to $\alpha \pm \beta \in I$,

(2) jeżeli $\varphi \in \mathcal{R}$ i $\alpha \in I$, to $\varphi\alpha \in I$.

Ćwiczenie 10.87 Udowodnić, że każdy ideał główny w $\mathcal{R}$ jest ideałem.

Ćwiczenie 10.88 Udowodnić, że pierścień $\mathcal{R}$ jest ciałem wtedy i tylko wtedy, gdy zawiera t y l k o dwa ideały, ideał zerowy $\{0\} = (0)$ i ideał $(1) = \mathcal{R}$.

Definicja 10.23 Nie będąca ciałem dziedzina całkowitości $\mathcal{R}$ nazywa się **dziedziną ideałów głównych** (w skrócie **dig**), gdy każdy ideał w $\mathcal{R}$ jest ideałem głównym.

P r z y k ł a d. Znamy już nieskończenie wiele dig'*ów*. Obok pierścienia $\mathbb{Z}$ liczb całkowitych, patrz T2.3, i pierścieni $\mathbb{Q}[X]$, $\mathbb{R}[X]$ i $\mathbb{C}[X]$ wielomianów jednej zmiennej o współczynnikach wymiernych, rzeczywistych i zespolonych odpowiednio, są to pierścienie $\mathbb{F}_p[X]$ wielomianów o współczynnikach w ciele $\mathbb{F}_p = \mathbb{Z}/p$ dla każdej liczby pierwszej p, zobacz T3.10. Jeszcze jedną serię dig'*ów* otrzymujemy biorąc pierścienie wielomianów $\mathbb{F}_{p^2}[X]$ o współczynnikach w ciałach $\mathbb{F}_{p^2} = \mathbb{F}_p(\iota)$, zobacz T9.3. Każdy z 21 pierścieni kwadratowych będących pierścieniami normowo-euklidesowymi jest dig'*iem*, zobacz T10.9. $\Diamond$

Ćwiczenie 10.89 Dowieść, że pierścień $\mathbb{Z}[X]$ wielomianów jednej zmiennej o współczynnikach całkowitych n i e jest dig'*iem*. *Wskazówka.* Zbiór wszystkich wielomianów o współczynnikach całkowitych i parzystym wyrazie wolnym j e s t ideałem w $\mathbb{Z}[X]$.

10.3.4 Największy wspólny dzielnik

Definicja największego wspólnego dzielnika elementów danej dziedziny całkowitości naśladuje znane nam już definicje NWD w pierścieniu $\mathbb{Z}$ liczb całkowitych czy w pierścieniach $\mathbb{K}[X]$ wielomianów jednej zmiennej o współczynnikach z ciała $\mathbb{K}$.

Definicja 10.24 Niech $\mathcal{R}$ będzie dziedziną całkowitości. Niech dane będą dwa, nie równe jednocześnie zero, elementy $\alpha, \beta \in \mathcal{R}$. Element $\delta \in \mathcal{R}$ nazywamy **największym wspólnym dzielnikiem** pary α, β, gdy spełnione są poniższe warunki:

(1) $\delta|\alpha$ i $\delta|\beta$,

(2) jeżeli $\gamma|\alpha$ i $\gamma|\beta$, to $\gamma|\delta$.

Piszemy wtedy $\delta \sim \mathrm{NWD}\,(\alpha, \beta)$ lub, po prostu, $\mathrm{NWD}\,(\alpha, \beta) = \delta$. O elementach α, β mówimy, że są **względnie pierwsze**, gdy $1 \sim \mathrm{NWD}\,(\alpha, \beta)$.

Ćwiczenie 10.90 Udowodnić, że jeżeli istnieje największy wspólny dzielnik danych elementów w $\mathcal{R}$, to jest on wyznaczony jednoznacznie z dokładnością do stowarzyszenia.

Musimy tu wyraźnie zaznaczyć, że największy wspólny dzielnik zazwyczaj nie istnieje. Zachodzi jednakże ważne uogólnienie twierdzenia T2.4, porównaj też T3.11 i T10.11:

TWIERDZENIE 10.14 *Jeżeli pierścień $\mathcal{R}$ jest dziedziną ideałów głównych, to każda para niezerowych elementów w $\mathcal{R}$ ma największy wspólny dzielnik. Ponadto, największy wspólny dzielnik pary $\alpha, \beta \in \mathcal{R}$ można zapisać w postaci $\alpha\varphi + \beta\psi$ dla pewnych elementów $\varphi, \psi \in \mathcal{R}$.*

DOWÓD. Weźmy dwa niezerowe elementy $\alpha, \beta \in \mathcal{R}$ i rozważmy ideał

$$(\alpha, \beta) := \{\alpha\varphi + \beta\psi : \varphi, \psi \in \mathcal{R}\}$$

pierścienia $\mathcal{R}$. Ponieważ jest on (jak każdy ideał w $\mathcal{R}$) ideałem głównym, więc istnieje taki element $\delta \in \mathcal{R}$, że $(\alpha, \beta) = (\delta)$. Twierdzimy, że $\delta \sim \mathrm{NWD}\,(\alpha, \beta)$. Sprawdzamy, że spełniony jest warunek (1) definicji D10.24. Zauważmy w tym celu, że $\alpha = \alpha \cdot 1 + \beta \cdot 0 \in (\alpha, \beta)$, więc $\alpha \in (\delta)$, czyli $\alpha = \delta \cdot \varphi$ i ostatecznie $\delta|\alpha$. Podobnie sprawdzamy, że $\delta|\beta$.

Z drugiej strony $\delta = \delta \cdot 1 \in (\delta)$, więc $\delta = \alpha\varphi_0 + \beta\psi_0$ dla pewnych $\varphi_0, \psi_0 \in A$. Stąd, jeżeli $\gamma|\alpha$ i $\gamma|\beta$, to $\delta = \alpha\varphi_0 + \beta\psi_0 = (\gamma\rho)\varphi_0 + (\gamma\tau)\psi_0 = \gamma(\rho\varphi_0 + \tau\psi_0)$, czyli $\gamma|\delta$, więc i warunek (2) definicji D10.24 jest spełniony. □

10.3.5 Elementy nierozkładalne i pierwsze w $\mathcal{R}$

Liczba pierwsza jest (dodatnim) nierozkładalnym elementem pierścienia $\mathbb{Z}$: każdy jej rozkład na czynniki jest trywialny w tym sensie, że wszystkie czynniki tego rozkładu z wyjątkiem jednego są odwracalne. Wygodnie jest przyjąć ogólną definicję:

Definicja 10.25 Niech $\mathcal{R}$ będzie daną dziedziną całkowitości. Element $\nu \in \mathcal{R}$ nie będący zerem ani jednością nazywa się **elementem nierozkładalnym** w $\mathcal{R}$, gdy spełnia warunek:

$$\boxed{\text{jeżeli} \quad \nu = \alpha\beta, \quad \text{to} \quad \alpha \in \mathcal{R}^* \quad \text{lub} \quad \beta \in \mathcal{R}^*.} \tag{10.36}$$

To oznacza, że elementy nierozkładalne mają "mało" dzielników: każdy dzielnik elementu nierozkładalnego ν jest albo jednością albo jest stowarzyszony z ν.

Liczba pierwsza ma bardzo w a ż n ą własność: jeżeli dzieli iloczyn, to dzieli jeden z czynników tego iloczynu (zobacz T2.15). Tę własność przyjmuje się za własność charakteryzującą elementy pierwsze:

Definicja 10.26 Niech $\mathcal{R}$ będzie daną dziedziną całkowitości. Element $\pi \in \mathcal{R}$ nie będący ani zerem ani jednością nazywa się **elementem pierwszym** w $\mathcal{R}$, gdy ma własność:

$$\boxed{\text{jeżeli} \quad \pi|\alpha\beta, \quad \text{to} \quad \pi|\alpha \quad \text{lub} \quad \pi|\beta.} \tag{10.37}$$

Ćwiczenie 10.91 Udowodnić, że jeżeli element pierwszy jest dzielnikiem innego elementu pierwszego, to elementy te są stowarzyszone. Czyli: jeżeli $\pi_1|\pi_2$, to $\pi_1 \sim \pi_2$.

W d o w o l n e j dziedzinie całkowitości zachodzi:

Twierdzenie 10.15 *Element pierwszy (w danej dziedzinie całkowitości) jest elementem nierozkładalnym.*

D O W Ó D. Załóżmy, że element pierwszy π jest iloczynem: $\pi = \alpha\beta$. Wówczas (zamieniając ewentualnie α i β) możemy założyć, że $\pi|\alpha$, czyli że $\alpha = \pi\gamma$ dla pewnego $\gamma \in \mathcal{R}$. Stąd mamy $\pi(1 - \gamma\beta) = 0$, zatem, ponieważ $\pi \neq 0$, mamy $1 = \gamma\beta$, czyli $\beta \in \mathcal{R}^*$. □

Elementy nierozkładalne zazwyczaj n i e są elementami pierwszymi, zob. 10.2.5 P. Jednakże:

Twierdzenie 10.16 *Jeżeli pierścień $\mathcal{R}$ jest dig'*iem*, to w tym pierścieniu każdy element nierozkładalny jest elementem pierwszym.*

D O W Ó D. Niech $\nu \in \mathcal{R}$ będzie elementem nierozkładalnym w pierścieniu $\mathcal{R}$. Niech $\nu|\alpha\beta$ i niech $\nu \nmid \alpha$. Wiemy, że w $\mathcal{R}$ każda para elementów ma największy wspólny dzielnik, zobacz T10.14. Niech więc $\delta = \mathrm{NWD}\,(\nu, \alpha)$. Ponieważ δ, jako dzielnik elementu nierozkładalnego ν, spełnia $\delta \sim \nu$ lub $\delta \sim 1$, a nie może być stowarzyszony z ν (bo wtedy $\nu|\alpha$!), więc $\delta \sim 1$. Stąd, na mocy T10.14, zachodzi równość $1 = \nu\varphi + \alpha\psi$ dla pewnych elementów φ, ψ. Mnożąc tę równość obustronnie przez β znajdujemy podzielność $\nu|\beta$. To kończy dowód. □

10.3.6 Jednoznaczność rozkładu w dig'*ach*

W tym ustępie pokażemy jak z dig'*owości* pierścienia wynika, że jest on **dziedziną z jednoznacznością rozkładu** na czynniki nierozkładalne.

W dotychczasowych dowodach twierdzeń o jednoznaczności rozkładu, zob. T2.16, T3.14, T10.4 i T10.13, ważną rolę grała Zasada Minimum. Można ją było zastosować, bo w badanych tam pierścieniach mieliśmy metodę porównywania "wielkości" elementów. W pierścieniu $\mathbb{Z}$ porównywaliśmy elementy za pomocą wartości bezwzględnej $|n|$, w pierścieniach $\mathbb{K}[X]$ za pomocą stopnia wielomianu, a w pierścieniach kwadratowych za pomocą modułu normy $|\mathbf{N}(\alpha)|$. W przypadku ogólnego dig'*u* substytutem Zasady Minimum jest poniższy lemat:

LEMAT 10.2 *Jeżeli $\mathcal{R}$ jest dziedziną ideałów głównych, a*

$$I_1 \subset I_2 \subset I_3 \subset \ldots \tag{10.38}$$

jest dowolnym ciągiem ideałów w pierścieniu $\mathcal{R}$, przy czym inkluzje są ścisłe, to ciąg ten jest skończony.

D O W Ó D. Oznaczmy przez I sumę teoriomnogościową $\bigcup I_k$. Łatwo sprawdzić, że I jest ideałem w $\mathcal{R}$. Jeżeli bowiem $\alpha, \beta \in I$, to $\alpha \in I_j$ i $\beta \in I_k$ dla pewnych j, k. Wtedy oba elementy α, β należą do $I_{\max(j,k)}$, więc $\alpha \pm \beta \in I_{\max(j,k)} \subseteq I$. Jeszcze łatwiej sprawdzamy zachodzenie warunku (2) z definicji D10.24.

Skoro I jest ideałem, a każdy ideał w $\mathcal{R}$ jest główny, więc istnieje takie $\alpha \in \mathcal{R}$, że $I = (\alpha)$. Wtedy $\alpha \in I$, czyli $\alpha \in I_k$ dla pewnego k. Wówczas $I = (\alpha) \subseteq I_k \subseteq I$. Zatem ciąg (10.38) kończy się na wyrazie I_k. □

Pierścień, w którym każdy **wstępujący łańcuch ideałów** (taki jak (10.38)) jest skończony, nazywa się **pierścieniem noetherowskim** (od nazwiska Emmy Nöther). Jak widać z powyższego lematu wszystkie dig'*i* są pierścieniami noetherowskimi. Noetherowskość pierścienia jest tą jego własnością, która pozwala do pewnego stopnia zastąpić Zasadę Minimum. Oto jak to się robi w dowodzie analogonu twierdzenia T2.14:

TWIERDZENIE 10.17 *Jeżeli $\mathcal{R}$ jest dig'*iem *i $\alpha \in \mathcal{R} \setminus (\mathcal{R}^* \cup \{0\})$, to istnieje element nierozkładalny dzielący α.*

D O W Ó D. Jeżeli α jest nierozkładalny, to $\alpha|\alpha$ i koniec. Jeżeli nie, to niech $\alpha = \alpha_1\beta$, gdzie $\alpha_1, \beta \notin \mathcal{R}^*$. Wówczas, na mocy C10.86, $(\alpha) \subseteq (\alpha_1)$. Łatwo zobaczyć, że ta inkluzja jest ścisła. Gdyby bowiem $(\alpha) = (\alpha_1)$, to, znowu na mocy C10.86, $\alpha \sim \alpha_1$, więc $\alpha_1\beta = \alpha = \alpha_1\varepsilon$ dla pewnej jedności ε. Stąd, na mocy prawa skracania, zobacz C10.80, $\beta = \varepsilon$, co jest niemożliwe. Mamy więc ścisłą inkluzję $(\alpha) \subset (\alpha_1)$ między ideałami w $\mathcal{R}$. Jeżeli teraz α_1 jest elementem nierozkładalnym, to $\alpha_1|\alpha$ i koniec. Jeżeli zaś α_1 nie jest elementem nierozkładalnym, to możemy postąpić z nim tak samo jak przed chwilą postąpiliśmy z α. Wówczas znajdziemy kolejną ścisłą inkluzję $(\alpha_1) \subset (\alpha_2)$. Postępując tak dalej znajdziemy ciąg ścisłych inkluzji

$$(\alpha) \subset (\alpha_1) \subset (\alpha_2) \subset \ldots \subset (\alpha_k),$$

którego, wobec L10.2, już n i e da się przedłużyć. W ten sposób znajdzie się element nierozkładalny α_k będący, patrz C10.86, dzielnikiem α. □

Jeszcze raz zobaczymy jak "działa" noetherowskość w dowodzie istnienia rozkładu na iloczyn elementów nierozkładalnych:

TWIERDZENIE 10.18 *Dziedzina ideałów głównych jest pierścieniem, w którym każdy niezerowy i nie będący jednością element da się jednoznacznie (z dokładnością do porządku czynników i relacji stowarzyszenia) rozłożyć na iloczyn elementów nierozkładalnych.*

D O W Ó D. Zaczynamy od dowodu i s t n i e n i a. Bierzemy $\alpha \in \mathcal{R} \setminus (\mathcal{R}^* \cup \{0\})$. Twierdzimy, że istnieją takie elementy nierozkładalne $\nu_1, \nu_2, \ldots, \nu_s$ w $\mathcal{R}$, że zachodzi równość

$$\alpha = \nu_1\nu_2 \cdot \ldots \cdot \nu_s. \tag{10.39}$$

Aby to uzasadnić znajdujemy nierozkładalny dzielnik ν_1 elementu α. Taki istnieje na mocy T10.17. Zapisujemy $\alpha = \nu_1\alpha_1$ i szukamy nierozkładalnego dzielnika elementu α_1. To się uda jeżeli α_1 nie jest odwracalny. Jeżeli $\nu_2|\alpha_1$, czyli $\alpha_1 = \nu_2\alpha_2$, to szukamy nierozkładalnego dzielnika elementu α_2. I tak dalej. Podobnie jak w poprzednim dowodzie dostaniemy w ten sposób ciąg ścisłych inkluzji

$$(\alpha) \subset (\alpha_2) \subset (\alpha_3) \subset \ldots \subset (\alpha_s),$$

którego nie da się przedłużyć. W świetle powiedzianego wyżej, niemożność dalszego przedłużania tego ciągu oznacza, że α_s jest jednością (i wtedy $(\alpha_s) = (1) = \mathcal{R}$). To kończy dowód istnienia rozkładu (10.39).

Dowód jednoznaczności można poprowadzić za pomocą Zasady Minimum. Załóżmy nie wprost, że istnieją takie *złe* elementy w $\mathcal{R} \setminus (\mathcal{R}^* \cup \{0\})$, które mają dwa różne rozkłady. Niech α będzie takim złym elementem, który oprócz rozkładu (10.39) ma jeszcze rozkład

$$\alpha = \mu_1\mu_2 \cdot \ldots \cdot \mu_t$$

na iloczyn elementów nierozkładalnych, przy czym tak, że rozkłady te są "sumarycznie" najkrótsze, czyli z najmniejszym $s + t$. Po ewentualnym przenumerowaniu, możemy założyć, że $\nu_1|\mu_1$, bo ν_1 jest elementem pierwszym, zobacz T10.16. Wobec tego $\nu_1 \sim \mu_1$, zobacz C10.91, i możemy "skrócić" przez ν_1, zobacz C10.80. Dostaniemy wtedy równość $\nu_2 \cdot \ldots \cdot \nu_s = (\varepsilon\mu_2) \cdot \ldots \cdot \mu_t$ o mniejszej sumarycznej długości. Sprzeczność. □

Uwaga. Zwróćmy uwagę, że dla istnienia rozkładu ważna jest noetherowskość pierścienia, a dla jednoznaczności rozkładu ważna jest pierwszość elementów nierozkładalnych.

10.4 Jedności rzeczywiste

Wiemy, że grupa jedności (= elementów odwracalnych) w urojonych pierścieniach kwadratowych jest grupą dwuelementową $\{-1, +1\}$, z wyjątkiem przypadków $D = -1, -3$, zobacz C10.35. Zajmiemy się więc jednościami w rzeczywistych pierścieniach kwadratowych.

10.4.1 Lemat o równaniu $x^2 - Dy^2 = 1$

Dla opisania grupy elementów odwracalnych w rzeczywistych pierścieniach kwadratowych wykorzystamy lemat dotyczący rozwiązań w liczbach rzeczywistych równania

$$x^2 - Dy^2 = 1, \tag{10.40}$$

gdzie D jest daną liczbą rzeczywistą dodatnią. W dalszym ciągu $\sqrt{D}$ oznacza pierwiastek arytmetyczny (dodatni).

LEMAT 10.3 *Jeżeli pary* $(u_1, v_1), (u_2, v_2) \in \mathbb{R} \times \mathbb{R}$ *są takimi rozwiązaniami równania* (10.40)*, że zachodzą nierówności*

$$1 \leqslant u_1 + v_1\sqrt{D} < u_2 + v_2\sqrt{D}, \tag{10.41}$$

to $0 < u_1 < u_2$.

D O W Ó D. Fakt, że (u_1, v_1) i (u_2, v_2) są rozwiązaniami równania (10.40) daje równości

$$u_1 - v_1\sqrt{D} = \frac{1}{u_1 + v_1\sqrt{D}}, \quad u_2 - v_2\sqrt{D} = \frac{1}{u_2 + v_2\sqrt{D}}.$$

Nierówności (10.41) dają więc

$$0 < u_2 - v_2\sqrt{D} < u_1 - v_1\sqrt{D} \leqslant 1. \tag{10.42}$$

Lewa nierówność (10.41) i prawa nierówność (10.42) dają $u_1 - v_1\sqrt{D} \leqslant u_1 + v_1\sqrt{D}$, skąd $v_1 \geqslant 0$. Podobnie, $u_2 - v_2\sqrt{D} < 1 < u_2 + v_2\sqrt{D}$ daje nierówność $v_2 > 0$. Wobec tego, nierówności $0 < u_2 - v_2\sqrt{D} < u_1 - v_1\sqrt{D}$ dają $u_2 > 0$ i $u_1 > 0$.

Dodając teraz środkową z nierówności (10.42) do prawej nierówności (10.41) dostajemy $u_1 + u_2 + (v_1 - v_2)\sqrt{D} < u_2 + u_1 + (v_2 - v_1)\sqrt{D}$, skąd $2(v_2 - v_1)\sqrt{D} > 0$, czyli $v_2 - v_1 > 0$. Wreszcie, równość $u_2^2 - Dv_2^2 = u_1^2 - Dv_1^2$, czyli $u_2^2 - u_1^2 = D(v_2^2 - v_1^2)$ daje, wobec poprzednio udowodnionych nierówności, tezę: $0 < u_1 < u_2$. □

10.4.2 Jedności fundamentalne

W każdym rzeczywistym pierścieniu kwadratowym istnieje n i e s k o ń c z e n i e wiele jedności, a wśród nich jedna wyróżniona jedność, zwana jednością fundamentalną, czyli taka, która w sposób opisany w poniższym twierdzeniu generuje wszystkie pozostałe.

Będziemy zapisywać elementy pierścienia $\mathbb{Z}[\tau_D]$ w postaci

$$\frac{a + b\sqrt{D}}{2}, \tag{10.43}$$

gdzie $a, b \in \mathbb{Z}$ oraz $a \equiv b \pmod 2$.

Ćwiczenie 10.92 Udowodnić, że zapis (10.43) elementu pierścienia $\mathbb{Z}[\tau_D]$ istnieje i jest jednoznaczny.

TWIERDZENIE 10.19 *W rzeczywistym pierścieniu kwadratowym $\mathbb{Z}[\tau_D]$ istnieje taka jedność η, że każda jedność w tym pierścieniu jest postaci $\pm\eta^n$, gdzie $n \in \mathbb{Z}$.*

D O W Ó D. Z twierdzenia T10.7 wiemy, że $\varepsilon \in \mathbb{Z}[\tau_D]$ jest jednością wtedy i tylko wtedy, gdy $|\mathbf{N}(\varepsilon)| = 1$. Zatem jedności mogą mieć normę równą 1 lub -1.

Zajmiemy się najpierw jednościami o n o r m i e 1.

Dwie takie jedności istnieją w każdym pierścieniu kwadratowym. Są to 1 i -1. Będziemy je nazywali jednościami **trywialnymi**. Aby wykazać, że istnieją, poza trywialnymi, jeszcze jakieś inne jedności, powołamy się na WT7.13. Wybierając dowolne parzyste $k \geqslant 2$ w równości (7.30) widzimy, że istnieje nieskończenie wiele rozwiązań równania (10.40) w liczbach naturalnych. Każde takie rozwiązanie (a, b) wyznacza element $\varepsilon = a + b\sqrt{D} \in \mathbb{Z}[\tau_D]$ będący nietrywialną jednością. Wówczas jedna (i tylko jedna) z czterech jedności ε, $1/\varepsilon$, $-\varepsilon$, $-1/\varepsilon$ jest liczbą większą od 1. Wobec tego, i s t n i e j ą j e d n o ś c i w i ę k s z e o d 1. Uzasadnimy teraz, że każdy ściśle malejący ciąg jedności

$$\varepsilon_1 > \varepsilon_2 > \varepsilon_3 > \ldots > 1 \tag{10.44}$$

jest skończony. To jest prostym wnioskiem z L10.3. Istotnie, niech

$$\varepsilon_k = \frac{a_k + b_k\sqrt{D}}{2},$$

gdzie $a_k,\ b_k \in \mathbb{Z},\ a_k \equiv b_k \pmod 2$. Wówczas nierówności (10.44), na mocy L10.3, dają nierówności

$$\frac{a_1}{2} > \frac{a_2}{2} > \frac{a_3}{2} > \ldots > 0,$$

co, wobec zasady minimum, oznacza skończoność ciągu. Wynika stąd, że istnieje dokładnie jedna najmniejsza, większa od 1, jedność w $\mathbb{Z}[\tau_D]$. Oznaczmy ją σ.

Weźmy teraz d o w o l n ą jedność $\varepsilon > 1$ o normie 1. Wówczas, wobec tego, że ciąg (σ^n) jest ciągiem rosnącym do nieskończoności, mamy $\sigma^k \leqslant \varepsilon < \sigma^{k+1}$ dla pewnego $k \in \mathbb{N}$. Mnożąc te nierówności przez liczbę dodatnią σ^{-k} otrzymamy nierówności równoważne $1 \leqslant \varepsilon\sigma^{-k} < \sigma$. Stąd, wobec minimalności σ, mamy $1 = \varepsilon\sigma^{-k}$, czyli

$$\varepsilon = \sigma^k, \quad k \in \mathbb{N}. \tag{10.45}$$

Widzimy więc, że każda większa niż 1 jedność o normie 1 jest równa σ^k dla pewnego $k \in \mathbb{N}$. Jeżeli teraz jedność ε o normie 1 spełnia nierówność $0 < \varepsilon < 1$, to $1/\varepsilon$ jest jednością (o normie 1) większą od 1. Zatem $1/\varepsilon = \sigma^k$ przy pewnym $k \in \mathbb{N}$. Stąd

$$\varepsilon = \sigma^{-k}, \quad k \in \mathbb{N}. \tag{10.46}$$

Z równości (10.45) i (10.46) widzimy, że wszystkie d o d a t n i e jedności ε o normie 1 są postaci $\sigma^k,\ k \in \mathbb{Z}$. Jeżeli wreszcie ε jest jednością ujemną o normie 1, to $-\varepsilon$ jest dodatnia i, wobec powyższego, jest postaci $-\varepsilon = \sigma^k$. Ostatecznie więc, wszystkie jedności o normie 1 są postaci $\pm\sigma^k,\ k \in \mathbb{Z}$.

Załóżmy teraz, że w $\mathbb{Z}[\tau_D]$ i s t n i e j ą jedności o normie równej -1.

Niech ε będzie pewną jednością o normie -1. Wówczas jedność ε^2 ma normę 1, jest więc postaci $\pm\sigma^k$. Ponieważ ε^2 jako kwadrat liczby rzeczywistej jest liczbą dodatnią, więc mamy $\varepsilon^2 = \sigma^k$. Twierdzimy, że k nie jest liczbą parzystą. Gdyby $k = 2l$, to mielibyśmy $\varepsilon = \pm\sigma^l$ i ε miałaby normę 1. Zatem $k = 2l + 1$. Połóżmy $\gamma = \varepsilon\sigma^{-l}$. Jedność γ ma normę -1. Ponadto $\gamma^2 = \sigma$.

Niech teraz ε będzie dowolną jednością w $\mathbb{Z}[\tau_D]$. Jeżeli $\mathbf{N}(\varepsilon) = 1$, to $\varepsilon = \pm\sigma^k = \pm\gamma^{2k}$. Jeżeli zaś $\mathbf{N}(\varepsilon) = -1$, to $\varepsilon\gamma$ jest jednością o normie $+1$, więc $\varepsilon\gamma = \pm\sigma^k = \pm\gamma^{2k}$, skąd $\varepsilon = \pm\gamma^{2k-1}$. Widzimy więc, że jeżeli wszystkie jedności w $\mathbb{Z}[\tau_D]$ mają normy równe 1, to każda z nich jest postaci $\pm\sigma^k,\ k \in \mathbb{Z}$. Jeżeli zaś w $\mathbb{Z}[\tau_D]$ istnieją jedności o normie -1, to każda jedność jest postaci $\pm\gamma^k,\ k \in \mathbb{Z}$. Aby zakończyć dowód wystarczy więc położyć $\eta = \sigma$ w pierwszym przypadku i $\eta = \gamma$ w drugim. □

Jedność, której istnienie właśnie wykazaliśmy, nazywamy **jednością fundamentalną** (rzeczywistego) pierścienia kwadratowego $\mathbb{Z}[\tau_D]$.

P r z y k ł a d 1. Najczęściej "używaną" jednością (poza jednościami ±1) jest jedność $1+\sqrt{2}$ pierścienia kwadratowego $\mathbb{Z}[\tau_2]$. Jest ona jednością fundamentalną tego pierścienia.

P r z y k ł a d 2. Przytoczona niżej tabelka podaje parę dalszych przykładów. Podajemy w niej, dla bezkwadratowych $2 \leqslant D \leqslant 41$, jedności fundamentalne w pierścieniach $\mathbb{Z}[\tau_D]$. Pokazujemy też typ odpowiedniego pierścienia kwadratowego. $\Diamond$

Jedności fundamentalne i typ $\mathbb{Z}[\tau_D]$ dla $2 \leqslant D \leqslant 41$

D	Jedność fundamentalna η	$\mathbf{N}(\eta)$	D	Jedność fundamentalna η	$\mathbf{N}(\eta)$
2	$1+\sqrt{2}$	-1	**22**	$197+42\sqrt{22}$	$+1$
3	$2+\sqrt{3}$	$+1$	**23**	$24+5\sqrt{23}$	$+1$
5	$\frac{1}{2}+\frac{1}{2}\sqrt{5}$	-1	**26**	$5+\sqrt{26}$	-1
6	$5+2\sqrt{6}$	$+1$	**29**	$\frac{5}{2}+\frac{1}{2}\sqrt{29}$	-1
7	$8+3\sqrt{7}$	$+1$	**30**	$11+2\sqrt{30}$	$+1$
10	$3+\sqrt{10}$	-1	**31**	$1520+273\sqrt{31}$	$+1$
11	$10+3\sqrt{11}$	$+1$	**33**	$23+4\sqrt{33}$	$+1$
13	$\frac{3}{2}+\frac{1}{2}\sqrt{13}$	-1	**34**	$35+6\sqrt{34}$	$+1$
14	$15+4\sqrt{14}$	$+1$	**35**	$6+\sqrt{35}$	$+1$
15	$4+\sqrt{15}$	$+1$	**37**	$6+\sqrt{37}$	-1
17	$4+\sqrt{17}$	-1	**38**	$37+6\sqrt{38}$	$+1$
19	$170+39\sqrt{19}$	$+1$	**39**	$25+4\sqrt{39}$	$+1$
21	$\frac{5}{2}+\frac{1}{2}\sqrt{21}$	$+1$	**41**	$32+5\sqrt{41}$	-1

P r z y k ł a d 3. Pokażemy zastosowanie faktu istnienia jedności fundamentalnej w pierścieniu $\mathbb{Z}[\tau_5]$. W ćwiczeniu C3.17 proponowaliśmy wyznaczenie "dużych" rozwiązań równania

$$x^2+y^2+1=3xy \tag{10.47}$$

w liczbach naturalnych. Teraz chcemy wyznaczyć w s z y s t k i e rozwiązania tego równania w liczbach całkowitych. Zapiszmy to równanie w postaci równoważnej: $(2x-3y)^2-5y^2=-4$. Równość tę zapisujemy w **postaci normowej**:

$$\mathbf{N}\left(\frac{2x-3y}{2}+\frac{y}{2}\sqrt{5}\right)=-1.$$

Szukamy więc wszystkich jedności o normie -1 w pierścieniu $\mathbb{Z}[\tau_5]$. Ponieważ $\eta=\frac{1}{2}+\frac{1}{2}\sqrt{5}$ jest tam jednością fundamentalną, więc widzimy, że para $(x,\,y)$ jest rozwiązaniem (10.47) wtedy i tylko wtedy, gdy

$$\frac{2x-3y}{2}+\frac{y}{2}\sqrt{5}=\pm\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)^{2k+1},$$

przy pewnym $k\in\mathbb{Z}$. Lub, równoważnie,

$$2x-3y+y\sqrt{5}=\pm\frac{(3+\sqrt{5})^k(1+\sqrt{5})}{2^k}.$$

Czytelnik, który odczuwa niedosyt z takiej postaci odpowiedzi proszony jest o jej poprawienie. W przypadku nie dających się przezwyciężyć trudności, niech czeka do ustępu poświęconego równaniu indyjskiemu. $\Diamond$

10.4.3 Pierścienie typu (-1) i $(+1)$

Rozstrzygnięcie czy w danym pierścieniu kwadratowym rzeczywistym istnieją jedności o normie -1 nie jest łatwe. Powiemy teraz dwa słowa na ten temat.

Rozróżnimy dwie kategorie rzeczywistych pierścieni kwadratowych: **pierścienie typu** (-1), w których istnieją jedności o normie równej -1 i **pierścienie typu** $(+1)$, w których wszystkie jedności mają normę równą 1.

P r z y k ł a d 1. Najczęściej używaną jednością w zadaniach OM jest jedność $1+\sqrt{2}$ pierścienia $\mathbb{Z}[\tau_2]$. Jej norma $\mathbf{N}(1+\sqrt{2}) = -1$. Pierścień $\mathbb{Z}[\tau_2]$ jest więc typu (-1). Ogólniej, jeżeli $D = n^2+1$ dla $n \in \mathbb{N}$, to pierścień $\mathbb{Z}[\tau_D]$ jest pierścieniem typu (-1). Równość $n^2 - D\cdot 1^2 = -1$ pokazuje bowiem, że $n+\sqrt{n^2+1}$ jest jednością o normie -1 w pierścieniu $\mathbb{Z}[\tau_{n^2+1}]$. $\Diamond$

P r z y k ł a d 2. Pierścień $\mathbb{Z}[\tau_3]$ jest pierścieniem typu $(+1)$. Rzeczywiście, gdyby element $a+b\sqrt{3}$ miał normę -1, to $a^2-3b^2 = -1$ co, po zredukowaniu modulo 3, dałoby kongruencję fałszywą $a^2 \equiv -1 \pmod 3$. $\Diamond$

Ćwiczenie 10.93 Udowodnić, że jeżeli istnieje taka liczba pierwsza $p \equiv 3 \pmod 4$, że $p|D$, to pierścień $\mathbb{Z}[\tau_D]$ jest pierścieniem typu $(+1)$. (D jest bezkwadratowa!).

ZADANIE 10.13 Udowodnić, że jeżeli $p \equiv 1 \pmod 4$ jest liczbą pierwszą, to istnieją takie liczby naturalne u, w, że $u^2 - pw^2 = -1$.

R o z w i ą z a n i e. Niech $x^2 - py^2 = 1$ i niech $x > 1$ będzie najmniejsze możliwe. Wówczas $1 \equiv x^2 - py^2 \equiv x^2 - y^2 \pmod 4$. Stąd, wobec znanych kongruencji $x^2,\, y^2 \equiv 0,\, 1 \pmod 4$, widzimy, że $x \equiv 1 \pmod 2$ i $y \equiv 0 \pmod 2$. Niech $y = 2z$. Wtedy

$$\frac{x-1}{2}\cdot\frac{x+1}{2} = pz^2. \tag{10.48}$$

Ponieważ liczby (naturalne) $(x-1)/2$, $(x+1)/2$ różnią się o 1, więc są względnie pierwsze. Ponieważ liczba pierwsza p dzieli ich iloczyn, więc dzieli jedną z nich. Pokażemy, że p n i e dzieli czynnika $(x-1)/2$. Gdyby tak było, to mielibyśmy równość $(x-1)/2p\cdot(x+1)/2 = z^2$, która, na mocy *triku* T2.19, pozwalałaby napisać $(x-1)/2p = b^2$, $(x+1)/2 = a^2$ dla pewnych naturalnych a, b. Stąd dostalibyśmy równość $a^2 - pb^2 = (x+1)/2 - (x-1)/2 = 1$. Czyli rozwiązanie $(a,\, b)$ równania $x^2 - py^2 = 1$ z mniejszym x. Wobec tego p dzieli czynnik drugi z lewej strony równości (10.48). Możemy więc zastosować *trik* do równości $(x-1)/2\cdot(x+1)/2p = z^2$. Dostaniemy $(x-1)/2 = u^2$, $(x+1)/2p = w^2$ dla pewnych naturalnych u, w. Wówczas $pw^2 - u^2 = 1$, więc $u^2 - pw^2 = -1$. $\Diamond$

Ćwiczenie 10.94 Udowodnić, że $\mathbb{Z}[\tau_{34}]$ jest pierścieniem typu $(+1)$.

Rozdział 11

Równania diofantyczne

Diophante (Διόφαντος) a sû manier tellement les inconnues ou l'innconue, que le quarré et les plus hautes puissances de cette inconnue disparaissent de l'équation, et qu'il ne reste que l'innconue au premier degré.

(J. le Rond D'Alembert)

Równania diofantyczne są centralnym tematem teorii liczb. My ograniczymy się tu do opowiedzenia o paru ideach i paru konkretnych przypadkach szukania rozwiązań (całkowitych lub wymiernych) równań diofantycznych.

11.1 Metody podstawowe

Opiszemy tu pokrótce, za pomocą przykładów, podstawowe metody rozwiązywania równań diofantycznych. Polegają one na wykorzystaniu nierówności, wykorzystaniu desantu nieskończonego, wykorzystaniu kongruencji i wykorzystaniu jednoznaczności rozkładu.

11.1.1 Wykorzystanie nierówności

W zbiorze liczb całkowitych (i naturalnych) mamy zadane (pochodzące ze zbioru liczb rzeczywistych) uporządkowanie – relację mniejszości $\leqslant$. Mimo, że jest ona strukturą obcą arytmetyce (zajmującej się głównie podzielnością) jest często wykorzystywana w teorii równań diofantycznych, na przykład do ograniczania zbioru potencjalnych rozwiązań.

Przykład 1. Rozważmy równanie $x^2 + x + 1 = y^2$. Pytamy o jego rozwiązalność w liczbach całkowitych. Dla $x > 0$ mamy

$$x^2 < x^2 + x + 1 < x^2 + 2x + 1 = (x + 1)^2.$$

Widzimy, że dla każdego $x \in \mathbb{N}$ liczba $x^2 + x + 1$ leży (ściśle) między dwoma kolejnymi kwadratami. Nie jest więc kwadratem i nie może być równa y^2. Podobnie, gdy $x < -1$,

$$(x + 1)^2 < x^2 + x + 1 < x^2.$$

I znowu $x^2 + x + 1$ leży między dwoma kolejnymi kwadratami, więc nie jest kwadratem. Pozostały dwa przypadki: $x = 0$ (wtedy $y = \pm 1$) i $x = -1$ (wtedy również $y = \pm 1$). $\Diamond$

Ćwiczenie 11.1 Dowieść, że jedynymi rozwiązaniami równania $x^3+8x^2-6x+8=y^3$ w liczbach całkowitych nieujemnych są pary $(x,\,y)=(0,\,2),\,(9,\,11)$.

Ćwiczenie 11.2 Rozwiązać w $\mathbb{Z}$ równanie $x^4+y^2=x^3+y$. *Wskazówka.* Udowodnić, że równanie $u^2+au+b=0,\ a,\,b\in\mathbb{Z},$ ma rozwiązania całkowite wtedy i tylko wtedy, gdy $\Delta=a^2-4b$ jest kwadratem liczby całkowitej.

ZADANIE 11.1 Rozwiązać w liczbach naturalnych równanie

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1.$$

Rozwiązanie. Załóżmy, że $0<x\leqslant y\leqslant z$. Wówczas

$$1=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\leqslant\frac{3}{x},$$

skąd $x\leqslant 3$. Ponieważ, oczywiście, $x\neq 1$, więc $x=2$ lub $x=3$. Oba te przypadki badamy kolejno. Jeżeli $x=2$, to mamy

$$\frac{2}{y}\geqslant\frac{1}{y}+\frac{1}{z}=\frac{1}{2}.$$

Stąd $y\leqslant 4$. Badamy kolejno przypadki $y=2$ (co jest niemożliwe), $y=3$ (co daje $z=6$) i $y=4$ (co daje $z=4$). Jeżeli zaś $x=3$, to mamy

$$\frac{2}{y}\geqslant\frac{1}{y}+\frac{1}{z}=\frac{2}{3},$$

skąd $y\leqslant 3$. Wówczas $y=3$ i $z=3$. Ostatecznie, rozwiązaniami są trójki $(2,\,3,\,6)$, $(2,\,4,\,4)$, $(3,\,3,\,3)$ i wszystkie ich permutacje. ◊

Ćwiczenie 11.3 Udowodnić, że równanie $\dfrac{1}{x_1}+\dfrac{1}{x_2}+\ldots+\dfrac{1}{x_{2000}}=1$ ma skończenie wiele rozwiązań w liczbach naturalnych.

11.1.2 Metoda zstępowania

Metoda zstępowania, zwana też **desantem (nieskończonym)**, opiera się na (pokrewnej Zasadzie Minimum) obserwacji, że każdy ściśle malejący ciąg liczb naturalnych jest skończony. Metodę tę już spotykaliśmy (zob. 3.2.7 U2, czy Z5.5). Rozpropagował ją Fermat, zobacz na przykład dowód T11.1. W ustępach 11.2.3 i 11.6.4 pokażemy dwa piękne desanty Eulera. Istotę metody pokazują poniższe przykłady i zadania.

Przykład. Chcemy udowodnić, że *jeżeli liczba naturalna D nie jest n-tą potęgą liczby naturalnej, to $\sqrt[n]{D}$ nie jest liczbą wymierną.* Załóżmy w tym celu nie wprost, że $\sqrt[n]{D}$ jest liczbą wymierną i przedstawmy ją w postaci $\sqrt[n]{D}=a/b$, gdzie $a,\,b\in\mathbb{N}$. Wówczas $a^n=Db^n$. Wybierzmy taką liczbą pierwszą p, że $n\nmid v_p(D)$, zobacz C2.44. Niech $v_p(a)=l$. Równość $a^n=Db^n$, na mocy C2.43.1, daje: $nl=v_p(a^n)=v_p(Db^n)=v_p(D)+v_p(b^n)$. Stąd wnosimy, że $v_p(b^n)\neq 0$, czyli $p|b^n$, więc $p|b$. Ponadto, $l\neq 0$. Kładąc $a=pa_1$ i $b=pb_1$ dostajemy,

po podzieleniu przez p^n, równość $a_1^n = Db_1^n$. Jednocześnie $a + b > a_1 + b_1$. Możemy teraz z parą (a_1, b_1) postąpić tak samo. W ten sposób, przy założeniu, że $\sqrt[n]{D}$ jest liczbą wymierną, możemy zbudować nieskończony i ściśle malejący ciąg $a + b > a_1 + b_1 > a_2 + b_2 > \ldots$ liczb naturalnych, co jest niemożliwe. ◊

ZADANIE 11.2 Rozwiązać równanie $x^3 + 9y^3 = 3z^3$ w liczbach całkowitych.

R o z w i ą z a n i e. Jasne, że trójka $(0, 0, 0)$ jest rozwiązaniem. Załóżmy, że (a, b, c) jest n i e z e r o w y m rozwiązaniem równania. Wówczas $3|a^3$, więc $3|a$. Kładąc $a = 3a_1$, znajdujemy, po podzieleniu przez 3, równość $9a_1^3 + 3b^3 = c^3$. Stąd $3|c^3$, czyli $3|c$. Kładąc tym razem $c = 3c_1$ i znów dzieląc przez 3 otrzymamy $3a_1^3 + b^3 = 9c_1^3$. Stąd, podobnie jak wyżej, $3|b$. Kładąc $b = 3b_1$ otrzymujemy (jeszcze raz dzieląc przez 3):

$$a_1^3 + 9b_1^3 = 3c_1^3.$$

Wobec tego trójka (a_1, b_1, c_1) jest r o z w i ą z a n i e m naszego równania. Przy tym

$$|a_1| + |b_1| + |c_1| < |a| + |b| + |c|.$$

Nierówność tu jest ostra, bo co najmniej jedna z liczb a, b, c jest różna od zera. Możemy teraz wykonać analogiczne manipulacje na (niezerowej(!)) trójce (a_1, b_1, c_1). To prowadzi do sprzeczności (bo n i e istnieje ściśle malejący nieskończony ciąg liczb naturalnych). ◊

Ćwiczenie 11.4 Udowodnić, że równanie $x^2 + y^2 = 3z^2$ nie ma niezerowych rozwiązań w liczbach całkowitych. A nawet niezerowych rozwiązań w liczbach wymiernych.

Ćwiczenie 11.5 Udowodnić, że jeżeli $p \geqslant 5$ jest liczbą pierwszą, a n liczbą naturalną, to równanie $x^3 + y^3 = p^n$ nie ma rozwiązań w liczbach naturalnych x, y. *Wskazówka.* Rozłożyć: $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$, i zastosować desant względem n.

11.1.3 Wykorzystanie kongruencji

Kongruencje dostarczają całego (nieskończonego!) szeregu warunków koniecznych rozwiązalności danego równania diofantycznego (w liczbach całkowitych). Warunki te dają ograniczenia jakie muszą spełniać liczby całkowite, które "chcą" być rozwiązaniami badanego równania. Czasami te ograniczenia są tak silne, że żadne liczby całkowite nie są rozwiązaniami równania.

ZADANIE 11.3 Rozwiązać równanie $2^x - 1 = y^2$ w liczbach całkowitych.

R o z w i ą z a n i e. Mamy oczywiste rozwiązania $(x, y) = (0, 0), (1, 1), (1, -1)$. Zauważamy, że x nie może być ujemne. Jeżeli zaś $x \geqslant 2$, to liczba $2^x - 1$ przystaje do $3 \pmod 4$, a żadna taka liczba nie jest kwadratem. ◊

ZADANIE 11.4 Udowodnić, że równanie $x^2 + 4 = y^5$ nie ma rozwiązań w $\mathbb{Z}$.

R o z w i ą z a n i e. Popatrzmy co się dzieje modulo 11. Wiemy, że $y^5 \equiv 0, \pm 1 \pmod{11}$, zobacz C5.11. Z drugiej strony, $x^2 + 4 \equiv 4, 5, 8, 2, 9, 7 \pmod{11}$, bo kwadratami modulo 11 są: 0, 1, 4, 9, 5, 3. Zatem $x^2 + 4 \not\equiv y^5 \pmod{11}$ dla dowolnych $x, y \in \mathbb{Z}$. ◊

U w a g a. Warto zwrócić uwagę na moduł 11 w powyższym rozwiązaniu. Jego wybór jest związany z faktem, że $(11 - 1)/2 = 5$, czyli z możliwością zastosowania ćwiczenia C5.11.

Ćwiczenie 11.6 Uzasadnić, że równanie

$$(x+1)^5+(y+2)^5+(z+3)^5=(x-1)^5+(y-2)^5+(z-3)^5+2016$$

nie ma rozwiązań w liczbach całkowitych. *Wskazówka.* Skorzystać z (5.12).

ZADANIE 11.5 Wykazać, że równanie

$$8x^3+9y^3+11z^3=6xyz \tag{11.1}$$

ma tylko jedno rozwiązanie w liczbach całkowitych.

Rozwiązanie. Zauważmy najpierw, że jeżeli którakolwiek z niewiadomych x, y, z jest równa 0, to pozostałe również są równe 0. Na przykład, jeżeli $z=0$, to $8x^3+9y^3=0$. I wtedy $x=y=0$ (gdyby $y\neq 0$, to $\sqrt[3]{9}=(-2x)/y$ co, jak wiemy z 11.1.2 P, jest niemożliwe). Znajdujemy więc rozwiązanie trywialne (oczywiste) $(0,\,0,\,0)$ równania (11.1).

Pokażemy, że innych rozwiązań w liczbach całkowitych nie ma. Załóżmy, że $(x,\,y,\,z)$, $z\neq 0$, jest rozwiązaniem. Redukując (11.1) modulo 7 mamy

$$x^3+2y^3+4z^3\equiv -xyz\,(\mathrm{mod}\,7). \tag{11.2}$$

Niech $k=v_7(z)$ będzie wykładnikiem 7-adycznym liczby z. I niech $k>0$. Wtedy (11.2) daje $x^3+2y^3\equiv 0\,(\mathrm{mod}\,7)$. Ale $x^3,\,y^3\equiv\pm 1,\,0\,(\mathrm{mod}\,7)$, zobacz znów C5.11. Zatem $x^3+2y^3\equiv 0\,(\mathrm{mod}\,7)$ jest możliwe tylko, gdy $x^3\equiv y^3\equiv 0\,(\mathrm{mod}\,7)$. Czyli, gdy $x=7x_1$, $y=7y_1$ i, również, $z=7z_1$ dla pewnych $x_1,\,y_1,\,z_1\in\mathbb{Z}$. Wówczas (11.1), po podzieleniu przez 7^3, daje $x_1^3+2y_1^3+4z_1^3=6x_1y_1z_1$. Otrzymana trójka $(x_1,\,y_1,\,z_1)$ jest więc rozwiązaniem równania (11.1), przy czym $v_7(z_1)=k-1$. Jeżeli teraz $k-1>0$, to rozumujemy tak samo. W ten sposób po k krokach znajdziemy rozwiązanie $(a,\,b,\,c)$ równania (11.1), w którym $7\nmid c$. Oznaczmy wówczas przez d odwrotność c modulo 7, zobacz T5.5. Mnożąc kongruencję (11.2) dla $x=a$, $y=b$, $z=c$ przez d^3 znajdujemy

$$-u^3-2w^3-4\equiv uw\,(\mathrm{mod}\,7), \tag{11.3}$$

gdzie $u=ad$, $w=bd$. Gdy teraz $u\equiv 0\,(\mathrm{mod}\,7)$, to (11.3) daje $2w^3+4\equiv 0\,(\mathrm{mod}\,7)$, co jest niemożliwe. Podobnie niemożliwe jest $w\equiv 0\,(\mathrm{mod}\,7)$. Pozostały nam do rozpatrzenia cztery przypadki (wszystkie kongruencje modulo 7):

(1) $u^3,\,w^3\equiv 1$. Wówczas $0\equiv uw$, sprzeczność.
(2) $u^3\equiv 1$, $w^3\equiv -1$. Wówczas $4\equiv uw$, więc $1\equiv 4^3\equiv u^3w^3$, sprzeczność.
(3) $u^3\equiv -1$, $w^3\equiv 1$. Wówczas $2\equiv uw$, więc $1\equiv 2^3\equiv u^3w^3$, sprzeczność.
(4) $u^3,\,w^3\equiv -1$. Wówczas $-1\equiv uw$, więc $-1\equiv(-1)^3\equiv u^3w^3$, sprzeczność. ◊

Często wykorzystujemy wiedzę pozwalającą nam odróżniać reszty kwadratowe od niereszt kwadratowych modulo m:

ZADANIE 11.6 Rozwiązać w liczbach całkowitych równanie $y^2=x^3+11$.

Rozwiązanie. Załóżmy, że para $(x,\,y)$ jest rozwiązaniem. Redukujemy modulo 4. Ponieważ $y^2\equiv 0,\,1\,(\mathrm{mod}\,4)$, więc $x^3\equiv y^2-11\equiv 1,\,2\,(\mathrm{mod}\,4)$. To jest możliwe tylko dla $x\equiv 1\,(\mathrm{mod}\,4)$, bo $0^3\equiv 2^3\equiv 0\,(\mathrm{mod}\,4)$, a $3^3\equiv 3\,(\mathrm{mod}\,4)$. Wobec tego $x\equiv 1\,(\mathrm{mod}\,4)$. Mamy

$$y^2+16=x^3+27=(x+3)(x^2-3x+9).$$

Ponieważ x^2-3x+9 jest liczbą naturalną większą od 1 i, przy $x \equiv 1 \,(\mathrm{mod}\, 4)$, daje resztę 3 z dzielenia przez 4, więc istnieje liczba pierwsza $p \equiv 3 \,(\mathrm{mod}\, 4)$ dzieląca x^2-3x+9, a zatem i y^2+16. (Gdy wszystkie dzielniki pierwsze liczby d o d a t n i e j są postaci $4t+1$, to i sama ta liczba jest postaci $4t+1$.) W takim razie $y^2 \equiv -16 \,(\mathrm{mod}\, p)$. To jednakże jest niemożliwe, bo $(-16|p) = (-1|p)(4^2|p) = (-1|p) = -1$ dla $p \equiv 3 \,(\mathrm{mod}\, 4)$. Zatem badane równanie nie ma rozwiązań w liczbach całkowitych. ◊

Ćwiczenie 11.7 Udowodnić, że równania $y^2 = x^3 - 5$ i $y^2 = x^3 + 23$ nie mają rozwiązań w liczbach całkowitych.

Ćwiczenie 11.8 Udowodnić, że jeżeli trójka (x, y, z) liczb całkowitych jest rozwiązaniem równania $x^2+3+y = 6yz$, to $y < 0$. *Wskazówka.* Jasne, że $y \neq 0$. Równość $x^2+3 = y(6z-1)$, dla $y > 0$, pokazuje, że $6z-1 > 0$ i $(-3)\mathbf{R}p$ dla każdego pierwszego dzielnika $p|6z-1$. Teraz zobacz (5.85) i zauważ, że iloczyn liczb postaci $6t+1$ jest liczbą tej postaci.

11.1.4 Wykorzystanie jednoznaczności rozkładu

Postać iloczynowa (multyplikatywna) równania jest zwykle pożądana. Umożliwia ona wykorzystanie jednoznaczności rozkładu na czynniki nierozkładalne (jeżeli w danej sytuacji taka jednoznaczność ma miejsce).

ZADANIE 11.7 Rozwiązać w liczbach całkowitych równanie $2^x + 1 = y^2$.

R o z w i ą z a n i e. Przechodzimy do równoważnej postaci multyplikatywnej

$$2^x = (y+1)(y-1) \tag{11.4}$$

i wykorzystujemy jednoznaczność rozkładu na czynniki pierwsze w $\mathbb{Z}$. Z tej jednoznaczności wynika, że oba czynniki po prawej stronie (11.4) są potęgami dwójki lub *minus* potęgami dwójki. Zatem

$$y+1 = \pm 2^k, \quad y-1 = \pm 2^l,$$

gdzie $k, l \in \mathbb{Z}_{\geqslant 0}$ i $k+l = x$. Odejmując stronami znajdujemy równość $2 = \pm 2^k - (\pm 2^l)$, co jest możliwe tylko dla $k = 2$, $l = 1$ lub $k = 1$, $l = 2$. Ostatecznie: $x = 3$, $y = \pm 3$ są jedynymi rozwiązaniami. ◊

Ćwiczenie 11.9 Rozwiązać w liczbach całkowitych równanie $2^x + y^2 = z^2$.

Przypomnijmy stosowany już przez nas

TRIK *Jeżeli α, β, γ są elementami dziedziny z jednoznacznością rozkładu $\mathcal{R}$, i w $\mathcal{R}$ zachodzi równość $\alpha \cdot \beta = \gamma^k$, a przy tym elementy α, β są względnie pierwsze, to elementy α i β są stowarzyszone z k-tymi potęgami, to znaczy, że istnieją takie jedności $\varepsilon, \eta \in \mathcal{R}^*$ i elementy $\varphi, \psi \in \mathcal{R}$, że $\alpha = \varepsilon \cdot \varphi^k$ oraz $\beta = \eta \cdot \psi^k$.*

Równie łatwa w dowodzie jest teza następującego ćwiczenia:

Ćwiczenie 11.10 Udowodnić, że jeżeli dla liczb naturalnych x, y, u, w zachodzi równość $xy = uw$, to istnieją takie liczby naturalne a, b, m, n, że zachodzą równości

$$x = am,\ y = bn,\ u = an,\ w = bm$$

i przy tym liczby m, n są względnie pierwsze. (***Twierdzenie Eulera o czterech liczbach***.)

Ćwiczenie 11.11 Uogólnić to twierdzenie na przypadek dowolnego pierścienia z jednoznacznością rozkładu.

Pokażemy teraz na przykładach jak to działa.

ZADANIE 11.8 Rozwiązać w liczbach naturalnych równanie $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{z}$.

Rozwiązanie. Równanie to jest równoważne równaniu $(x - z)(y - z) = z^2$. Chciałoby się teraz skorzystać z *triku*, ale czynniki po lewej stronie tej równości nie muszą być względnie pierwsze. Niech $d = \mathrm{NWD}\,(x - z,\, y - z)$. Wtedy $d^2 | z^2$, czyli $d | z$. Stąd

$$\frac{x - z}{d} \cdot \frac{y - z}{d} = \left(\frac{z}{d}\right)^2.$$

Teraz już możemy zastosować *trik*. Otrzymujemy $\dfrac{x - z}{d} = a^2$, $\dfrac{y - z}{d} = b^2$, gdzie $ab = \dfrac{z}{d}$. Wobec tego

$$(x,\, y,\, z) = (da(a + b),\, db(a + b),\, dab).$$

Sprawdzenie, że każda taka trójka jest rozwiązaniem, nie przedstawia trudności. ◊

Ćwiczenie 11.12 Udowodnić, że wszystkie rozwiązania równania $\dfrac{1}{x^2} + \dfrac{1}{y^2} = \dfrac{1}{z^2}$ w liczbach naturalnych dane są przez

$$x = d(u^2 + v^2)(u^2 - v^2), \quad y = d(u^2 + v^2) \cdot 2uv, \quad z = d(u^2 - v^2) \cdot 2uv,$$

gdzie u, v są względnie pierwsze różnej parzystości, $u > v$, a $d \geqslant 1$ jest dowolną liczbą naturalną. Ponadto można zamienić miejscami x i y.

Już parę razy spotkaliśmy **równanie Bachet'a**

$$y^2 = x^3 + B, \tag{11.5}$$

gdzie B jest ustaloną liczbą całkowitą (zobacz Z10.4 dla $B = -1$, 10.2.7 P dla $B = -11$, Z10.8 dla $B = -2$, Z11.6 dla $B = 11$ oraz C11.7 dla $B = -5$ i $B = 23$). Rozważymy teraz przypadek $B = -4$. Dla zbadania tego przypadku równania Bachet'a wykorzystamy (podobnie jak w przypadku $B = -1$) jednoznaczność rozkładu w pierścieniu Gaussa $\mathbb{Z}[\,i\,]$.

ZADANIE 11.9 Wyznaczyć wszystkie rozwiązania równania

$$y^2 = x^3 - 4 \tag{11.6}$$

w liczbach całkowitych.

R o z w i ą z a n i e. Załóżmy najpierw, że (x, y) jest rozwiązaniem z n i e p a r z y s t y m y. Wówczas równość (11.6) zapisujemy w pierścieniu $\mathbb{Z}[i]$ w postaci iloczynowej:

$$(y + 2i)(y - 2i) = x^3.$$

Wiemy, że $\mathrm{NWD}\,(y + 2i, y - 2i) = 1$, zobacz (10.10). Wobec tego *trik* w pierścieniu $\mathbb{Z}[i]$ pozwala napisać $y+2i = (a+bi)^3$ dla pewnych $a, b \in \mathbb{Z}$. Stąd $2 = 3a^2b-b^3$. Sprawdzamy kolejne możliwe wartości $b = \pm 1, \pm 2$. Dostajemy cztery rozwiązania $(a, b) = (\pm 1, 1), (\pm 1, -2)$. Pierwsze dwie z tych par dają parzyste $y = a^3 - 3ab^2$, więc nie są dla nas interesujące. Pozostałe dwie z tych par dają $y = \pm 11$. Wówczas $x = 5$. Mamy więc dwa rozwiązania równania (11.6) z nieparzystym y: $(x, y) = (5, 11), (5, -11)$.

Załóżmy teraz, że y jest p a r z y s t e. Wówczas również x jest parzyste. Kładąc $y = 2y_1$ i $x = 2x_1$ dostajemy więc $y_1^2 = 2x_1^3 - 1$, czyli y_1 jest nieparzyste i

$$(y_1 + i)(y_1 - i) = 2x_1^3. \tag{11.7}$$

Tym razem $\mathrm{NWD}\,(y_1 + i, y_1 - i) \sim 1 + i$, zobacz Z10.2. Ponieważ $2 = (1 + i)(1 - i)$, więc możemy podzielić obustronnie równość (11.7) przez 2. Otrzymamy iloczyn dwóch w z g l ę d n i e p i e r w s z y c h czynników równy sześcianowi w $\mathbb{Z}[i]$:

$$x_1^3 = \frac{y_1 + i}{1 + i} \cdot \frac{y_1 - i}{1 - i} = (u + 1 - ui) \cdot (u + 1 + ui),$$

gdzie $y_1 = 2u+1$. Dzięki *trikowi* możemy napisać równość $u+1-ui = (a+bi)^3$ dla pewnych $a, b \in \mathbb{Z}$. Więc $u + 1 = a^3 - 3ab^2$ i $-u = 3a^2b - b^3$. Stąd

$$1 = (u + 1) - u = (a^3 - 3ab^3) + (3a^2b - b^3) = (a - b)(a^2 + ab + b^2) + 3ab(a - b).$$

Zatem $a - b = a^2 + 4ab + b^2 = \pm 1$. Łatwo znajdujemy wszystkie możliwe a, b. I ostatecznie $y = \pm 2$ oraz $x = 2$. ◊

Ćwiczenie 11.13 Udowodnić, że jeżeli $y^2 = x^5 - 1$ i $x, y \in \mathbb{Z}$, to $y = 0$.

Ćwiczenie 11.14 Dana jest liczba pierwsza $p > 3$. Udowodnić, że jeżeli $y^2 = x^p - 1$ dla pewnych liczb całkowitych x, y, to $y = 0$.

11.2 Wielkie Twierdzenie Fermat'*a*

Najsłynniejszym równaniem diofantycznym (a właściwie, najsłynniejszą serią równań diofantycznych) jest równanie

$$\boxed{x^n + y^n = z^n.} \tag{11.8}$$

Około[1] 1640 Pierre de Fermat sformułował (i twierdził, że umie udowodnić) następujące:

[1]Dokładniejsza data nie jest znana. Na marginesie swojego egzemplarza, wydanej przez Bachet'*a* w 1621, *Arytmetyki* Diofantosa, Fermat zapisał słynne zdanie: *Nie można podzielić sześcianu na dwa sześciany ani czwartej potęgi na dwie czwarte potęgi, ani ogólnie żadnej potęgi wyższej niż druga na dwie takie same potęgi; znalazłem naprawdę zadziwiający dowód, który nie zmieści się na tym zbyt wąskim marginesie.*

Wielkie Twierdzenie Fermat'a *Jeżeli trójka* (x, y, z) *liczb całkowitych jest rozwiązaniem równania* (11.8) *przy* $n \geqslant 3$, *to* $xyz = 0$.

Fermat podał dowód w przypadku $n = 4$, reprodukujemy go poniżej. Prawdopodobieństwo, że podobnymi metodami da się udowodnić twierdzenie dla dowolnego n, jest znikome. Próbowały tego dziesiątki matematyków – dwie takie próby pokażemy w ustępach 11.2.2 i 11.2.3, i tysiące *fermatowców* – każdy wydział matematyczny na świecie otrzymywał wiele listów z "dowodami" wielkiego twierdzenia. Teza WTF okazała się prawdziwą w roku 1994, kiedy to Wiles'*owi* udało się zwieńczyć wysiłki poprzedników (Taniyamy, Shimury, Frey'*a*, Serre'*a*, Ribeta, Taylora i innych). O ich strategii dowodu twierdzenia Fermat'*a* nie możemy tu (z braku miejsca i wiedzy) opowiedzieć. Zobacz [**9**].

Ćwiczenie 11.15 Uzasadnić, że WTF wystarczy udowodnić dla $n = 4$ i dla $n = p$, gdzie p jest dowolną nieparzystą liczbą pierwszą.

11.2.1 Twierdzenia Fermat'a

Rozpatrzymy teraz przypadek $n = 4$. Poniżej przedstawiony dowód pochodzi w istocie od Fermat'*a*, który pokazał nam, na czym polega metoda nieskończonego desantu.

Twierdzenie 11.1 *Równanie* $x^4 + y^4 = z^4$ *nie ma rozwiązań w liczbach naturalnych. Więcej: równanie*

$$x^4 + y^4 = z^2 \tag{11.9}$$

nie ma rozwiązań w liczbach naturalnych.

Dowód. Załóżmy, nie wprost, że trójka (a, b, c) liczb naturalnych jest rozwiązaniem tego równania. Pokażemy jak można z trójki (a, b, c) skonstruować nową trójkę (a_1, b_1, c_1), która również jest rozwiązaniem (11.9), przy czym $0 < c_1 < c$. Jasne, że w ten sposób uzyskamy sprzeczność.

Procedura konstruowania rozwiązania (a_1, b_1, c_1) z danego rozwiązania (a, b, c) jest dwukrokowa. Krok pierwszy wykonujemy, gdy liczby a i b nie są względnie pierwsze. Jeżeli $d > 1$ jest wspólnym dzielnikiem liczb a i b, to $d^4 | c^2$, więc $d^2 | c$ i trójka $(a_1, b_1, c_1) = \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2}\right)$ jest rozwiązaniem (11.9) z mniejszym z. W kroku drugim zakładamy więc, że $\mathrm{NWD}\,(a, b) = 1$. Wówczas (a^2, b^2, c) jest pierwotnym rozwiązaniem równania Pitagorasa, więc, jak wiemy, istnieją takie liczby względnie pierwsze u, v, że

$$a^2 = 2uv, \quad b^2 = u^2 - v^2, \quad c = u^2 + v^2,$$

(po ewentualnej zamianie a na b). Ponadto, liczby u, v są różnej parzystości. Łatwo zobaczyć, że w tej sytuacji v jest parzysta. Gdyby bowiem v była nieparzysta, a u parzysta, to byłoby $b^2 = u^2 - v^2 \equiv 0 - 1 \equiv 3 \pmod 4$, co jest niemożliwe. Oznaczając $v = 2w$ widzimy, że

$$\left(\frac{a}{2}\right)^2 = uw,$$

co, wobec względnej pierwszości u i w, na mocy *triku* T2.19, daje

$$u = c_1^2, \quad w = d^2,$$

gdzie c_1 i d są liczbami względnie pierwszymi, przy czym $c_1 \equiv 1 \pmod 2$.

Równość $b^2 = u^2 - v^2$ możemy teraz zapisać w postaci $(2d^2)^2 + b^2 = c_1^4$, gdzie $2d^2$ i b^2 są względnie pierwsze. Stąd znów znajdujemy

$$2d^2 = 2mn, \quad c_1^2 = m^2 + n^2 \tag{11.10}$$

dla pewnych względnie pierwszych m, n. Jeszcze raz stosujemy *trik* do równości $d^2 = mn$ i dostajemy $m = a_1^2$ i $n = b_1^2$. Druga z równości (11.10) daje więc

$$a_1^4 + b_1^4 = c_1^2.$$

I znów znaleźliśmy rozwiązanie równania (11.9) z mniejszym z, bo, oczywiście, $c_1 < c$. □

Widzimy więc, że suma niezerowych **bikwadratów** (= czwartych potęg) nigdy nie jest kwadratem (a tym bardziej bikwadratem!). Również różnica różnych niezerowych bikwadratów nie jest nigdy kwadratem:

Ćwiczenie 11.16 Udowodnić, że równanie

$$x^4 - y^4 = z^2 \tag{11.11}$$

nie ma rozwiązań w niezerowych liczbach całkowitych. *Wskazówka.* Zakładając to co trzeba założyć, uzasadnić kolejne wynikania: $x^4 - y^4 = z^2$, więc $x^2 = a^2 + b^2$, $y^2 = 2ab$, $z = a^2 - b^2$, więc $a = c^2 - d^2$, $b = 2cd$, więc $y^2 = 4cd(c^2 - d^2)$, więc $c = e^2$, $d = f^2$, $c^2 - d^2 = g^2$, więc $e^4 - f^4 = g^2$ i $(e, f) \prec (x, y)$.

ZADANIE 11.10 Udowodnić, że jeżeli w trójkącie prostokątnym wszystkie boki mają długość całkowitą, to pole tego trójkąta nie jest kwadratem liczby całkowitej. (***Zadanie Fermat'a***)

Rozwiązanie. Niech $a, b \in \mathbb{N}$ oznaczają długości przyprostokątnych, a $c \in \mathbb{N}$ długość przeciwprostokątnej danego trójkąta prostokątnego. Załóżmy, że pole $S = \frac{1}{2}ab$ tego trójkąta jest kwadratem: $\frac{1}{2}ab = d^2$. Dodając do obu stron równości $a^2 + b^2 = c^2$ liczbę $\pm 2ab = \pm(2d)^2$ znajdujemy

$$(a + b)^2 = c^2 + (2d)^2, \quad \text{oraz} \quad (a - b)^2 = c^2 - (2d)^2.$$

Mnożymy te dwie równości stronami. To daje $c^4 - (2d)^4 = (a^2 - b^2)^2$. Ponieważ $a \neq b$ (dlaczego?) więc znaleźliśmy niezerowe rozwiązanie równania (11.11). Sprzeczność. ◊

Ćwiczenie 11.17 Udowodnić, że równanie $x^4 + y^4 = 2z^2$ ma tylko trywialne rozwiązania $(x, y, z) = (a, a, a^2)$, gdzie $a \in \mathbb{Z}$. *Wskazówka.* Jeżeli $x > y$, to $2u = x^2 + y^2$, $2v = x^2 - y^2$ są parzyste. Wówczas $u^2 + v^2 = z^2$ i $u^2 - v^2 = (u + v)(u - v) = (xy)^2$. Stąd $u^4 - v^4 = \square$ (jest kwadratem).

11.2.2 Twierdzenie Sophie Germain

Zgodnie z ćwiczeniem C11.15 zajmujemy się równaniem (11.8) dla $n = p > 2$. W czasie prób dowodu WTF rozróżniono dwa przypadki: tak zwany **przypadek I**, gdy zakładamy dodatkowo, że $p \nmid xyz$ i tak zwany **przypadek II**, gdy $p|xyz$. Przypadek I jest zdecydowanie łatwiejszy w badaniu. Sophie (Zofia) Germain uzyskała całkowicie elementarnymi metodami największy w jej czasach progres na drodze dowodu przypadku I WTF.

LEMAT 11.1 *Załóżmy, że $q = 2n + 1 > 3$ jest liczbą pierwszą. Jeżeli (przy dowolnym wyborze znaków) zachodzi kongruencja $a^n \pm b^n \pm c^n \equiv 0 \pmod q$, to $abc \equiv 0 \pmod q$.*

D O W Ó D. Załóżmy, nie wprost, że $abc \not\equiv 0 \pmod q$. Wtedy $a, b, c \not\equiv 0 \pmod q$. Z ćwiczenia C5.11 wiemy więc, że $a^n \equiv \pm 1 \pmod q$, $b^n \equiv \pm 1 \pmod q$ i $c^n \equiv \pm 1 \pmod q$. Zatem $0 \equiv a^n \pm b^n \pm c^n \equiv \pm 1 \pm 1 \pm 1 \equiv \pm 1, \pm 3 \pmod q$. Sprzeczność. □

TWIERDZENIE 11.2 (***Twierdzenie Sophie Germain***) *Załóżmy, że p jest liczbą pierwszą Sophie Germain* (zob. 5.7.8 U1). *Załóżmy, że dla liczb całkowitych x, y, z zachodzi równość*

$$x^p + y^p = z^p. \tag{11.12}$$

Wówczas $xyz \equiv 0 \pmod p$.

D O W Ó D. Załóżmy nie wprost, że istnieją takie $x, y, z \in \mathbb{Z}$, że zachodzi równość (11.12) i że $x \not\equiv 0 \pmod p$, $y \not\equiv 0 \pmod p$ i $z \not\equiv 0 \pmod p$. Pisząc równość (11.12) w postaci $x^p + y^p + (-z)^p = 0$ i dzieląc $x, y, -z$ przez $\mathrm{NWD}(x, y, -z)$ znajdujemy p i e r w o t n ą trójkę a, b, c, dla której $a^p + b^p + c^p = 0$ i, oczywiście, $p \nmid abc$. Korzystamy teraz z tożsamości nieśmiertelnej (1.8) i piszemy:

$$(-a)^p = (b + c)(b^{p-1} - b^{p-2}c + \ \ldots\ - bc^{p-2} + c^{p-1}). \tag{11.13}$$

Pokażemy, że czynniki stojące po prawej stronie tej równości są względnie pierwsze. Załóżmy w tym celu, że pewna liczba pierwsza r dzieli czynnik $(b + c)$. Wtedy $c \equiv -b \pmod r$, więc drugi czynnik jest sumą p składników, z których każdy przystaje do b^{p-1} modulo r. Gdyby więc drugi czynnik był również podzielny przez r, to musiałoby być $r|pb^{p-1}$. Ponieważ jednak $r \nmid b$ (gdy $r|b$, to, ponieważ $r|(b + c)$, $r|c$, więc i $r|a$, co jest niemożliwe wobec pierwotności trójki a, b, c), więc $r|p$, czyli $r = p$. Wobec tego $p|(-a)^p$, skąd $p|a$, co zostało wykluczone. [Zauważmy, że dla dowodu względnej pierwszości czynników z prawej strony równości (11.13) mogliśmy byli powołać się na Z2.B6.] *Trik* pokazuje więc, że czynnik $(b + c)$ iloczynu (11.13) jest p-tą potęgą (pamiętamy, że p jest liczbą nieparzystą, więc $-u^p = (-u)^p$) liczby całkowitej. Podobnie pokazujemy, że również liczby $(c+a)$ i $(a+b)$ są p-tymi potęgami liczb całkowitych. Mamy więc

$$b + c = A^p, \quad c + a = B^p, \quad a + b = C^p \tag{11.14}$$

dla pewnych liczb całkowitych A, B, C.

Równość $a^p + b^p + c^p = 0$ pociąga kongruencję $a^p + b^p + c^p \equiv 0 \pmod q$, z której dzięki lematowi L11.1 wnosimy, że $q|abc$. Zatem q dzieli (co najmniej) jedną z liczb a, b, c. B e z o g r a n i c z e n i a ogólności rozważań możemy założyć, że $q|a$. Wtedy $q|B^p + C^p - A^p$, bo, jak

widać z równości (11.14), $B^p+C^p-A^p=2a$. Mamy więc $B^p+C^p-A^p\equiv 0\,(\mathrm{mod}\,q)$, co, znowu dzięki L11.1, daje $q|ABC$. Stąd wnosimy, że $q|A$ (gdy $q|B$, to $q|B^p-a$, więc $q|c$, co jest niemożliwe, bo a, c są względnie pierwsze; gdy zaś $q|C$, to, podobnie, $q|b$, co jest niemożliwe, bo a, b są względnie pierwsze).

Wróćmy teraz do równości (11.13). Drugi czynnik z prawej strony tej równości również jest p-tą potęgą. Oznaczmy go E^p. Mamy zatem $(-a)^p = A^p\cdot E^p$. Ponieważ czynniki A^p, E^p są względnie pierwsze, a $q|A^p$, więc $q\nmid E^p$. Czyli $q\nmid E$. Wobec tego (zobacz C5.11) $E^p\equiv\pm 1\,(\mathrm{mod}\,q)$. Ale $q|A^p$, czyli $c\equiv -b\,(\mathrm{mod}\,q)$, więc

$$E^p = b^{p-1}-b^{p-2}c+\,\ldots\,-bc^{p-2}+c^{p-1}\equiv pb^{p-1}\,(\mathrm{mod}\,q).$$

Otrzymujemy stąd $\pm 1\equiv pb^{p-1}\,(\mathrm{mod}\,q)$. Jednocześnie trzecia z równości (11.14) pokazuje, że $b\equiv C^p\,(\mathrm{mod}\,q)$ (bo $q|a$, czyli $q|C^p-b$). Wiemy, że $q\nmid C$, więc (jeszcze raz zobacz C5.11) $C^p\equiv\pm 1\,(\mathrm{mod}\,q)$. Czyli $b\equiv\pm 1\,(\mathrm{mod}\,q)$, skąd $b^{p-1}\equiv 1\,(\mathrm{mod}\,q)$, bo $p-1$ jest parzyste. Mamy zatem sprzeczność: $\pm 1\equiv p\,(\mathrm{mod}\,q)$. □

Ćwiczenie 11.18 Niech $p>2$ będzie liczbą pierwszą Sophie Germain (zob. 5.7.8 U1). Udowodnić, że równanie $x^p+2y^p+5z^p=0$ nie ma rozwiązań w liczbach całkowitych.

Ćwiczenie 11.19 Udowodnić, że jeżeli $x^7+y^7=z^7$ dla liczb całkowitych x, y, z, to $7|xyz$. *Wskazówka.* Wykorzystać liczbę pierwszą $q=29=4\cdot 7+1$.

11.2.3 Metoda Eulera dowodu WTF(3)

Leonhard Euler "prawie" udowodnił WTF(3) (Wielkie Twierdzenie Fermata dla wykładnika $n=3$). Pomysł Eulera dowodu WTF(3) polegał na wykorzystaniu arytmetyki pierścienia $\mathbb{Z}[\sqrt{-3}]=\{a+b\sqrt{-3}:\,a,\,b\in\mathbb{Z}\}$. Pierścień ten jednak ma poważną wadę: n i e jest dziedziną z jednoznacznością rozkładu. Wady tej nie ma, jak wiemy, większy od $\mathbb{Z}[\sqrt{-3}]$, pierścień Eisensteina $\mathbb{Z}[\tau_{-3}]$. Okaże się, że równanie $x^3+y^3+z^3=0$ nie ma rozwiązań nie tylko w niezerowych liczbach całkowitych, ale również w niezerowych liczbach Eisensteina. W trakcie dowodu tego faktu korzystamy swobodnie z oznaczeń i wyników omówionych w ustępie 10.2.8.

Załóżmy, że α, β, $\gamma\in\mathbb{Z}[\,\omega\,]\setminus\{0\}$ i że zachodzi równość

$$\alpha^3+\beta^3+\gamma^3=0, \tag{11.15}$$

przy czym $\mathrm{NWD}\,(\alpha,\,\beta,\,\gamma)\sim 1$. Dzieląc ewentualnie przez NWD możemy tak założyć.

(1) Udowodnimy najpierw, że jedna i tylko jedna z liczb α, β, γ dzieli się przez λ. To wynika z Z10.10: gdyby żadna z liczb α, β, γ nie była podzielna przez λ, to byłoby α^3, β^3, $\gamma^3\equiv\pm 1\,(\mathrm{mod}\,9)$ skąd dostalibyśmy nieprawdę $\pm 1\pm 1\pm 1\equiv 0\,(\mathrm{mod}\,9)$. Wobec tego co najmniej jedna z liczb α, β, γ jest podzielna przez λ. Gdyby dwie z nich były podzielne przez λ, to, wobec równości (11.15), i trzecia byłaby podzielna przez λ, co jest niemożliwe, bo założyliśmy względną pierwszość. Niech $\gamma=\lambda^k\delta$ i $\lambda\nmid\delta$. Możemy więc zapisać (11.15) w postaci

$$\alpha^3+\beta^3=\varepsilon\lambda^{3k}\delta^3, \tag{11.16}$$

gdzie ε jest jednością (tu $\varepsilon=-1$) oraz $\lambda\nmid\alpha$, $\lambda\nmid\beta$, $\lambda\nmid\delta$, i $k\in\mathbb{N}$.

(2) Wykażemy teraz, że k w równości (11.16) spełnia warunek $k \geqslant 2$. Istotnie, dzięki Z10.10 wiemy, że α^3, β^3, $\delta^3 \equiv \pm 1 \,(\mathrm{mod}\, 9)$. Załóżmy, nie wprost, że $k = 1$ i zredukujmy równość (11.16) modulo 9. Dostaniemy kongruencję postaci $\pm 1 \pm 1 \equiv \pm\varepsilon\lambda^3 \,(\mathrm{mod}\, 9)$. Łatwo sprawdzić, że to jest niemożliwe przy żadnym wyborze znaków i jedności ε (proponujemy Czytelnikowi zobaczenie tego na rysunku 10.5).

(3) Zapiszemy teraz równość (11.16) w postaci iloczynowej

$$(\alpha+\beta)(\alpha+\omega\beta)(\alpha+\omega^2\beta) = \varepsilon(\lambda^k\delta)^3, \tag{11.17}$$

zob. C11.20(1). Ponieważ liczba pierwsza Eisensteina λ (zobacz C10.72) dzieli prawą stronę tej równości więc dzieli co najmniej jeden z czynników strony lewej. Z ćwiczenia C11.20(2) wiemy, że te czynniki przystają do siebie modulo λ. Wobec tego λ dzieli każdy z tych trzech czynników. Co więcej, zobacz C11.20(3), największym wspólnym dzielnikiem każdej pary tych czynników jest λ. Wobec tego jeden z tych czynników dzieli się przez λ^{3k-2}, a dwa pozostałe dzielą się przez λ.

(4) Dzieląc więc przez λ^3 obie strony równości (11.17) dostajemy równość

$$\frac{\alpha+\beta}{\lambda}\cdot\frac{\alpha+\omega\beta}{\lambda}\cdot\frac{\alpha+\omega^2\beta}{\lambda} = \varepsilon(\lambda^{k-1}\delta)^3, \tag{11.18}$$

przy czym czynniki z lewej strony są (parami) względnie pierwsze. Ponieważ ich iloczyn jest stowarzyszony z sześcianem, więc każdy z czynników jest stowarzyszony z sześcianem (*trik*!). Mamy zatem równości:

$$\frac{\alpha+\beta}{\lambda} = \varepsilon_1\alpha_1^3, \quad \frac{\alpha+\omega\beta}{\lambda} = \varepsilon_2\beta_1^3, \quad \frac{\alpha+\omega^2\beta}{\lambda} = \varepsilon_3\gamma_1^3, \tag{11.19}$$

gdzie ε_1, ε_2, ε_3 są pewnymi jednościami. Ponadto (ewentualnie przemianowując) możemy uważać, że $\lambda \nmid \alpha_1$, $\lambda \nmid \beta_1$ i $\lambda^{k-1} | \gamma_1$.

(5) Wykorzystamy teraz twierdzenie "o strażakach" T3.20. Daje ono równość

$$\varepsilon_1\alpha_1^3 + \omega\varepsilon_2\beta_1^3 + \omega^2\varepsilon_3\gamma_1^3 = \frac{1}{\lambda}\left(\alpha+\omega\alpha+\omega^2\alpha+\beta+\omega^2\beta+\omega^4\beta\right) = 0.$$

Przenosząc wyraz $\omega^2\varepsilon_3\gamma_1^3$ na drugą stronę i mnożąc obustronnie przez ε_1^{-1} dostajemy:

$$\alpha_1^3 + \varepsilon_4\beta_1^3 = \varepsilon_5(\lambda^{k-1}\delta_1)^3 \tag{11.20}$$

gdzie ε_4, ε_5 są pewnymi jednościami. Położyliśmy tu $\gamma_1 = \lambda^{k-1}\delta_1$.

(6) Z punktu (2) wiemy, że $k-1 \geqslant 1$. Redukując równość (11.20) modulo λ^3 otrzymamy więc $\pm 1 \pm \varepsilon_4 \equiv 0 \,(\mathrm{mod}\, \lambda^3)$, czyli $\varepsilon_4 \equiv \pm 1 \,(\mathrm{mod}\, \lambda^4)$. Rzut oka na rysunek 10.5 przekonuje nas, że to jest możliwe tylko, gdy $\varepsilon_4 = \pm 1$. Więc $\varepsilon_4^3 = \varepsilon_4$. Wobec tego równość (11.20) może być zapisana tak:

$$\alpha_1^3 + (\varepsilon_4\beta_1)^3 = \varepsilon_5\lambda^{3(k-1)}\delta_1^3.$$

Dostaliśmy więc równość postaci (11.16) z tą różnicą, że k jest zamienione na $k-1$.

Powyższe rozważania pozwalają udowodnić WTF(3):

TWIERDZENIE 11.3 *Jeżeli x, y, $z \in \mathbb{Z}$ i zachodzi równość $x^3+y^3=z^3$, to $xyz = 0$.* □

Ćwiczenie 11.20 **(1)** Udowodnić tożsamość $x^3+y^3=(x+y)(x+\omega y)(x+\omega^2 y)$. Porównać z tożsamością (3.41). **(2)** Udowodnić, że dla dowolnych $\alpha,\ \beta\in\mathbb{Z}[\,\omega\,]$ zachodzą kongruencje $\alpha+\beta\equiv\alpha+\omega\beta\equiv\alpha+\omega^2\beta\,(\mathrm{mod}\,\lambda)$. **(3)** Udowodnić, że dla czynników z lewej strony równości (11.17) zachodzi: $\mathrm{NWD}\,(\alpha+\beta,\ \alpha+\omega\beta)\sim\mathrm{NWD}\,(\alpha+\beta,\ \alpha+\omega^2\beta)\sim\mathrm{NWD}\,(\alpha+\omega\beta,\ \alpha+\omega^2\beta)\sim\lambda$. **(4)** Uzasadnić, że $\lambda^4\sim 9$ w $\mathbb{Z}[\,\omega\,]$.

Ćwiczenie 11.21 Udowodnić T11.3.

Ćwiczenie 11.22 Jeżeli $x,\ y,\ w\in\mathbb{Q}$ spełniają równanie $x^3+y^3=w^3$, to $xyw=0$.

Ćwiczenie 11.23 Uzasadnić, że $1\,001\,000$ nie jest sześcianem liczby naturalnej.

Ćwiczenie 11.24 Rozwiązać w liczbach wymiernych równanie $3y^2=2x^3-4$. *Wskazówka.* Zauważyć, że jest ono równoważne równaniu $(2+y)^3+(2-y)^3=8x^3$.

Ćwiczenie 11.25 Niech $f(X)=X^{18}-8X^9$. Udowodnić, że jeżeli $u\neq w$ są liczbami wymiernymi, to $f(u)\neq f(w)$.

11.2.4 Równanie $x^3+y^3+z^3=w^3$

Z C11.22 wiemy, że niezerowy sześcian liczby wymiernej n i e może być sumą dwóch niezerowych sześcianów liczb wymiernych. Pokażemy za Eulerem, że istnieje mnóstwo niezerowych wymiernych sześcianów będących sumami trzech niezerowych wymiernych sześcianów.

Załóżmy, że liczby wymierne $x,\ y,\ z$ i w spełniają równanie

$$x^3+y^3+z^3=w^3. \tag{11.21}$$

Jeżeli przy tym $z\neq w$, to możemy powyższą równość zapisać w postaci

$$\frac{x+y}{w-z}=\frac{w^2+wz+z^2}{x^2-xy+y^2}=\frac{\mathbf{N}(w+z\tau)}{\mathbf{N}(x-y\tau)}=\mathbf{N}(P+Q\tau)=P^2+PQ+Q^2=:N, \tag{11.22}$$

gdzie $\tau=\tau_{-3}$. Jasne, że $\mathbf{N}$ oznacza tu normę w $\mathbb{Q}(\sqrt{-3})$, patrz (10.2) i C10.34. Oznaczyliśmy tu przez $P+Q\tau$ iloraz $(w+z\tau)/(x-y\tau)$ w $\mathbb{Q}(\sqrt{-3})$, więc $P,\ Q\in\mathbb{Q}$. Równość $w+z\tau=(P+Q\tau)(x-y\tau)$ daje, na mocy C10.33, równości $Px+Qy=w$ i $Qx-(P+Q)y=z$. Zapisując równość (11.22) w postaci $x+y=Nw-Nz$ otrzymujemy więc układ równości:

$$\begin{cases} Px+Qy=w,\\ Qx-(P+Q)y-z=0,\\ x+y+Nz=Nw. \end{cases}$$

Rozwiązujemy ten układ względem $x,\ y,\ z$. Dostajemy:

$$x=\frac{[(P+2Q)N-1]w}{N^2+Q-P},\quad y=\frac{[(Q-P)N+1]w}{N^2+Q-P},\quad z=\frac{[N^2-(P+2Q)]w}{N^2+Q-P}.$$

Oznaczmy jeszcze $M = w(N^2 + Q - P)^{-1}$. Wówczas mamy:

$$\begin{cases} x = [(P + 2Q)N - 1]\, M, \\ y = [(Q - P)N + 1]\, M, \\ z = [N^2 - (P + 2Q)]\, M, \\ w = [N^2 + (Q - P)]\, M. \end{cases}$$

Kładąc w tych równościach dowolne wymierne wartości M, P, Q (pamiętając cały czas, że $N = P^2 + PQ + Q^2$) dostajemy (wszystkie) rozwiązania wymierne równania (11.21). Możemy powiedzieć, że otrzymaliśmy t r z y p a r a m e t r o w ą rodzinę rozwiązań wymiernych równania (11.21). Kładąc tu $P = Q = \lambda$ i $M = 1$ znajdujemy j e d n o p a r a m e t r o w ą rodzinę rozwiązań całkowitoliczbowych równania (11.21): dla każdego $\lambda \in \mathbb{Z}$ czwórka

$$(x,\, y,\, z,\, w) = (9\lambda^3 - 1,\, 1,\, 9\lambda^4 - 3\lambda,\, 9\lambda^4) \tag{11.23}$$

jest rozwiązaniem (11.21) w liczbach całkowitych. U w a g a. Nie należy sądzić, że w ten sposób uzyskamy wszystkie rozwiązania równania (11.21) w $\mathbb{Z}$!

Ćwiczenie 11.26 Kładąc $\lambda = -1$ w równościach (11.23) odnajdujemy ***równość Ramanujana***: $1^3 + 12^3 = 9^3 + 10^3$. Ramanujan (w pamięci(?)) sprawdził, że liczba 1729 jest n a j m n i e j s z ą liczbą naturalną, którą da się przedstawić w postaci sumy dwóch sześcianów liczb naturalnych na dwa r ó ż n e sposoby. Czy potraficie to uzasadnić na kartce?

11.3 Równanie Ramanujana

Pokażemy tu rozwiązanie problemu Ramanujana z roku 1913. Pierwsze (nieco inne niż niżej przytoczone) rozwiązanie tego problemu pochodzi od Nagella (1948). Rozwiązanie, które przytaczamy poniżej wykorzystuje jednoznaczność rozkładu w pierścieniu $\mathbb{Z}[\tau_{-7}]$. Ponadto, ważną w nim rolę grają ciągi rekurencyjne.

Twierdzenie 11.4 *Jedynymi rozwiązaniami* ***równania Ramanujana***

$$y^2 + 7 = 2^m \tag{11.24}$$

w liczbach całkowitych są pary $(y,\, m) = (\pm 1,\, 3),\ (\pm 3,\, 4),\ (\pm 5,\, 5),\ (\pm 11,\, 7),\ (\pm 181,\, 15)$.

D O W Ó D. Podstawową metodą w dowodzie jest rozkład lewej strony na czynniki w pierścieniu $\mathbb{Z}[\tau_{-7}]$. Pierścień $\mathbb{Z}[\tau_{-7}]$ jest pierścieniem normowo-euklidesowym, zobacz Z10.6. Jest więc dziedziną z j e d n o z n a c z n o ś c i ą r o z k ł a d u na czynniki nierozkładalne, zobacz T10.13. W dalszym ciągu piszemy w skrócie $\tau = \tau_{-7}$.

Oznaczmy przez $\overline{\tau}$ liczbę sprzężoną z τ. Przypomnijmy, że

$$\tau + \overline{\tau} = 1, \quad \tau \cdot \overline{\tau} = 2 \quad \text{i} \quad \tau^2 = \tau - 2, \quad \overline{\tau}^2 = \overline{\tau} - 2. \tag{11.25}$$

Załóżmy, że para $(y,\, m)$ jest rozwiązaniem równania Ramanujana. Wówczas $y \in \mathbb{Z}$ jest, oczywiście, liczbą nieparzystą. Niech $y = 2x + 1$. Oznaczmy

$$\xi = \frac{y + \sqrt{-7}}{2} = x + \tau.$$

Wówczas w $\mathbb{Z}[\tau]$ zachodzi równość

$$\xi \cdot \overline{\xi} = 2^n = \tau^n \cdot \overline{\tau}^n \tag{11.26}$$

gdzie $n = m - 2$. Ponieważ rozkład $2 = \tau \cdot \overline{\tau}$ jest rozkładem na (niestowarzyszone!) czynniki nierozkładalne więc, dzięki jednoznaczności rozkładu, mamy

$$\xi = \pm\tau^k \cdot \overline{\tau}^l, \quad \text{i (wobec tego)} \quad \overline{\xi} = \pm\overline{\tau}^k \cdot \tau^l.$$

Wymnażając stronami i porównując z (11.26), widzimy, że $k + l = n$. Gdyby $k, l > 0$, to mielibyśmy $\xi = \pm\tau\overline{\tau} \cdot \tau^{k-1}\overline{\tau}^{l-1} = \pm 2 \cdot \tau^{k-1}\overline{\tau}^{l-1}$, co jest niemożliwe, bo ξ nie dzieli się przez 2 (sprawdzić!). Zatem $k = n$, $l = 0$ lub $k = 0$, $l = n$. Widzimy więc, że

$$\tau^n = \pm(x + \tau) \quad \text{lub} \quad \tau^n = \pm(x + \overline{\tau}) = \pm(x + 1 - \tau).$$

Wobec tego, jeżeli para $(y, m) = (2x + 1, n + 2)$ jest rozwiązaniem równania Ramanujana, to w zapisie liczby $\tau^n \in \mathbb{Z}[\tau]$, w postaci

$$\tau^n = a_n + b_n\tau, \tag{11.27}$$

gdzie $a_n, b_n \in \mathbb{Z}$ (a taki zapis, jak wiemy, jest jednoznaczny) zachodzi równość $b_n = \pm 1$. Odwrotnie, jeżeli przy pewnym $a \in \mathbb{Z}$ i przy pewnym $n \in \mathbb{N}$ zachodzi równość $\tau^n = a \pm \tau$, to sprzęgając i wymnażając stronami znajdujemy

$$2^{n+2} = 4\tau^n\overline{\tau}^n = 4(a \pm \tau)(a \pm \overline{\tau}) = 4(a^2 \pm a(\tau + \overline{\tau}) + \tau\overline{\tau}) = (2a \pm 1)^2 + 7,$$

czyli rozwiązanie $(2a \pm 1, n + 2)$ równania Ramanujana.

Musimy się więc bliżej przyjrzeć liczbom całkowitym b_n wyznaczonym przez (11.27). Mnożąc tę równość stronami przez τ i korzystając z równości $\tau^2 = \tau - 2$ znajdujemy zależności $a_{n+1} = -2b_n$ i $b_{n+1} = a_n + b_n$. Stąd z łatwością sprawdzamy, że

$$b_{n+2} = b_{n+1} - 2b_n \tag{11.28}$$

dla każdego $n \geqslant 0$. Ponadto, $b_0 = 0$ i $b_1 = 1$. W lemacie L11.2 dowodzimy, że $|b_n| = 1$ dla $n = 1, 2, 3, 5, 13$ i tylko dla takich n. To daje wymienione rozwiązania równania (11.24). I to są w s z y s t k i e r o z w i ą z a n i a tego równania. □

Udowodnimy więc:

LEMAT 11.2 *Jedynymi wyrazami ciągu (b_n) zadanego przez (11.28) i warunki początkowe $b_0 = 0$, $b_1 = 1$, takimi że $|b_n| = 1$, są wyrazy $b_1 = b_2 = 1$ i $b_3 = b_5 = b_{13} = -1$.*

D O W Ó D. Wśród początkowych wyrazów:

$$0, \boxed{1}, \boxed{1}, \boxed{-1}, -3, \boxed{-1}, 5, 7, -3, -17, -11, 23, 45, \boxed{-1}, -91, -89, 93, 271, 85$$

ciągu (b_n) znajdujemy pięć przypadków wystąpienia wyrazu równego ± 1: $b_1 = b_2 = 1$ i $b_3 = b_5 = b_{13} = -1$.

Będziemy teraz dowodzić, że, poza wskazanymi, w ciągu (b_n) n i e w y s t ę p u j ą ż a d n e inne wyrazy równe ± 1. Łatwo uzasadnić, że poza b_1, b_2 nie ma więcej wyrazów równych $+1$. Istotnie, redukując ciąg (b_n) modulo 64, dostajemy:

$$\mathbf{0},\ \mathbf{1},\ \mathbf{1},\ \mathbf{-1},\ \mathbf{-3},\ \mathbf{-1},\ (\mathbf{5},\ \mathbf{7},\ \mathbf{61},\ \mathbf{47},\ \mathbf{53},\ \mathbf{23},\ \mathbf{45},\ \boxed{\mathbf{-1}},\ \mathbf{37},\ \mathbf{39},\ \mathbf{29},\ \mathbf{15},\ \mathbf{21},\ \mathbf{55},\ \mathbf{13},\ \mathbf{31})$$

czyli ciąg (nieczysto) okresowy (okres wzięliśmy w nawias) o okresie długości 16. Wnosimy stąd, że jedyne wartości n, dla których $b_n = 1$ to $n = 1,\ 2$. Ponadto $b_3 = b_5 = -1$, a jedyne $n > 5$, dla których wyraz b_n m o ż e być równy -1 to n postaci $16k + 13$. Udowodnimy dwoma sposobami, że $k = 0$ jest jedyną wartością k, dla której $b_{16k+13} = -1$.

S p o s ó b 1. W tym sposobie, który pochodzi z pracy A. Schinzel, J. Browkin *Sur les nombres de Mersenne qui sont triangulaires*, wykorzystamy fakt, że ciąg (b_n) jest ciągiem Lucas'*a* $(u(1,\ -2)_n)$, w szczególności, że ma on własność podzielności (zob. C9.22):

$$m|n \implies b_m|b_n. \tag{11.29}$$

Rozważmy ciąg $(c_k \,(\mathrm{mod}\, 17))$ dany przez $c_k = b_{16k+13}$. Żmudny (choć prosty) rachunek pokazuje, że

$$(c_k \,(\mathrm{mod}\, 17)): \quad (\boxed{\mathbf{-1}},\ \mathbf{-5},\ \mathbf{0},\ \mathbf{5},\ \mathbf{1},\ \mathbf{2},\ \mathbf{-4},\ \mathbf{4},\ \mathbf{-2}), \ldots .$$

Widzimy stąd, że ciąg $(c_k \,(\mathrm{mod}\, 17))$ jest ciągiem czysto-okresowym o okresie długości 9, a -1 występuje na początku okresu. Wobec tego $c_k \equiv -1 \,(\mathrm{mod}\, 17)$ wtedy i tylko wtedy, gdy $k = 9m$. Co oznacza, że

$$b_n = -1,\ n \geqslant 13 \implies n = 144m + 13. \tag{11.30}$$

Rozważmy teraz ciąg $(d_p) = (b_{3p+1} \,(\mathrm{mod}\, 79))$. Nieco mniej żmudny (choć równie prosty) rachunek pokazuje, że

$$(d_p \,(\mathrm{mod}\, 79)): \quad (\mathbf{1},\ \mathbf{-3},\ \mathbf{7},\ \mathbf{-11},\ \boxed{\mathbf{-1}},\ \mathbf{14},\ \mathbf{17},\ \mathbf{-39},\ \mathbf{-20},\ \mathbf{17},\ \mathbf{-4},\ \mathbf{-37},\ \mathbf{-20}), \ldots .$$

Widzimy stąd, że ciąg $(d_p \,(\mathrm{mod}\, 79))$ jest ciągiem czysto-okresowym o okresie długości 13, a -1 występuje na piątym miejscu tego okresu. Wobec tego $d_p \equiv -1 \,(\mathrm{mod}\, 79)$ wtedy i tylko wtedy, gdy $p = 4 + 13q$. Co oznacza, że $b_n = -1,\ n \geqslant 13 \implies n = 39q + 13$. Ponieważ $144m + 13 = 39q + 13$ wtedy i tylko wtedy, gdy $48m = 13q$, czyli wtedy i tylko wtedy, gdy $m = 13r$, więc widzimy, że b_n (dla $n \geqslant 13$) może być równy -1 tylko gdy $n = 13(144r + 1)$.

Załóżmy więc, że istnieje taka liczba naturalna r, że $b_{13(144r+1)} = -1$. Wówczas, na mocy (11.29), $b_{144r+1}|(-1)$. Zatem $b_{144r+1} = -1$ (bo, jak wiemy, $b_{144r+1} \neq 1$ dla $r \geqslant 1$). To jest jednak sprzeczne z (11.30). □

S p o s ó b 2. Zauważmy przede wszystkim, że ciąg (b_n) jest ciągiem Lucas'*a* $(u(1,\ -2)_n)$, zobacz D9.3. To oznacza, że

$$b_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \tag{11.31}$$

gdzie $\alpha = \tau$, $\beta = \overline{\tau}$ spełniają warunki (11.25). Równości (9.19), po przyjęciu $n = 4$ i $n = 12$, dają:

$$\alpha^4 = -1 + 3\beta, \quad \beta^4 = -1 + 3\alpha, \quad \alpha^{12} = -1 - 45\beta, \quad \beta^{12} = -1 - 45\alpha. \tag{11.32}$$

Za pomocą tych równości udowodnimy dwie tożsamości

$$b_{4k+1} = (-1)^k - 6\sum_{j=2}^{k}\binom{k}{j}(-1)^{k-j}3^{j-1}b_{j-1}, \tag{11.33}$$

$$b_{12k+1} = (-1)^k + 90\sum_{j=2}^{k}\binom{k}{j}(-1)^{k-j}(-45)^{j-1}b_{j-1} \tag{11.34}$$

dla $k \geqslant 1$. Robi się to podobnie jak przy dowodzie tożsamości Cesàro w Z9.8:

$$\alpha^{12k+1} = (\alpha^{12})^k\alpha = (-1-45\beta)^k\alpha = (-1)^k\alpha + \sum_{j=1}^{k}\binom{k}{j}(-1)^{k-j}(-45\beta)^j\alpha =$$

$$= (-1)^k\alpha - 90\sum_{j=1}^{k}\binom{k}{j}(-45)^{j-1}\beta^{j-1}.$$

Ostatnia równość wynika z równości $\alpha\beta = 2$. Analogicznie:

$$\beta^{12k+1} = (-1)^k\beta - 90\sum_{j=1}^{k}\binom{k}{j}(-45)^{j-1}\alpha^{j-1}.$$

Odejmując ostatnie dwie równości stronami, dzieląc przez $\alpha-\beta$ i korzystając z (11.31) otrzymamy (11.34). Zauważmy, że składnik odpowiadający $j=1$ możemy opuścić, bo $b_0 = 0$. Podobnie dowodzimy równości (11.33).

Załóżmy teraz, że dla pewnego $s \geqslant 1$ zachodzi równość $b_{16s+13} = -1$ i połóżmy $k = 4s+3$ w równości (11.33). Wówczas

$$-1 = b_{16s+13} = b_{4k+1} = (-1)^{4s+3} - 6\sum_{j=2}^{4s+3}\binom{4s+3}{j}(-1)^{4s+3-j}3^{j-1}b_{j-1}.$$

Stąd

$$0 = \sum_{j=2}^{4s+3}\binom{4s+3}{j}(-1)^{j-1}3^{j-1}b_{j-1}.$$

Po podzieleniu przez 3 i wykorzystaniu równości $b_1 = b_2 = 1$ zapiszemy to w postaci

$$\binom{4s+3}{2} - 3\binom{4s+3}{3} = \sum_{j=4}^{4s+3}\binom{4s+3}{j}(-1)^{j-1}3^{j-2}b_{j-1},$$

czyli

$$(-2s)(4s+3)(4s+2) = \sum_{j=4}^{4s+3}\binom{4s+3}{j}(-1)^{j-1}3^{j-2}b_{j-1}.$$

Ta równość po podzieleniu przez $(4s+3)(4s+2)$ i wykorzystaniu prostych własności symbolów dwumiennych Newtona (zobacz tak zwane tożsamości pochłaniania, $\mathbb{KOM}$) daje

$$-2s = \sum_{j=4}^{4s+3} \binom{4s+1}{j-2} (-1)^{j-1} b_{j-1} \frac{3^{j-2}}{j(j-1)}.$$

Dzięki C2.47, z łatwością sprawdzamy, że wykładnik 3-adyczny sumy po prawej stronie jest $\geqslant 1$. To dowodzi, że $3|s$. Widzimy więc, że jeżeli $b_{16s+13} = -1$ przy pewnym $s \geqslant 1$, to $s = 3t$. Aby skończyć dowód musimy więc jeszcze udowodnić, że przy $t \geqslant 1$ n i e może zachodzić równość $b_{48t+13} = -1$. Załóżmy więc, nie wprost, że $b_{48t+13} = -1$ przy pewnym $t \geqslant 1$ i połóżmy $k = 4t+1$ w równości (11.34). Otrzymamy

$$-1 = b_{48t+13} = b_{12k+1} = (-1)^{4k+1} + 90 \sum_{j=2}^{4t+1} \binom{4t+1}{j} (-1)^{4t+1-j} (-45)^{j-1} b_{j-1}.$$

Stąd

$$0 = \sum_{j=2}^{4t+1} \binom{4t+1}{j} (-1)^{4t+1-j} (-45)^{j-1} b_{j-1}.$$

Po oczywistych uproszczeniach i podzieleniu przez 45 zapiszemy to w postaci równoważnej:

$$-\binom{4t+1}{2} = \sum_{j=3}^{4t+1} \binom{4t+1}{j} 45^{j-2} b_{j-1}.$$

Dzieląc obustronnie przez $4t(4t+1)/2$, podobnie jak przed chwilą, znajdujemy

$$-1 = 2 \sum_{j=3}^{4t+1} \binom{4t-1}{j-2} b_{j-1} \frac{45^{j-2}}{j(j-1)},$$

co jest niemożliwe, bo wykładnik 5-adyczny prawej strony jest $\geqslant 1$. □

Ćwiczenie 11.27 Wykorzystać podane w przykładach P1 i P2 z ustępu 9.5.4 wzory Eulera-Binet'*a* dla (znacznego) skrócenia czasu żmudnych rachunków (nie) wykonanych w sposobie 1 dowodu lematu L11.2.

Ćwiczenie 11.28 Podnieść pierwiastki $6 \pmod 8$ i $3 \pmod 8$ równania $x^2 - x + 2 = 0$ w $\mathbb{Z}/8$ do pierwiastków $(2^{13}-90) \pmod{2^{14}}$ i $(2^{13}+91) \pmod{2^{14}}$ tego samego równania w $\mathbb{Z}/2^{14}$. Napisać wzór Eulera-Binet'*a* dla redukcji ciągu (b_n) modulo 2^{14}. Spróbować wykorzystać ten wzór dla jeszcze jednego dowodu lematu L11.2.

Ćwiczenie 11.29 Wyznaczyć wszystkie liczby trójkątne, które są jednocześnie liczbami Mersenne'*a* $M_n = 2^n - 1$.

Ćwiczenie 11.30 Zbadać równanie $y^2 + 11 = 3^n$.

Ćwiczenie 11.31 Zbadać równanie $y^2 + 1 = 5^n$.

11.4 Równanie indyjskie

W całym paragrafie D oznacza liczbę naturalną nie będącą kwadratem. Równanie

$$x^2 - Dy^2 = 1 \tag{11.35}$$

będziemy nazywali **równaniem indyjskim**.

U w a g a. Euler omyłkowo nazwał równanie (11.35) **równaniem Pella** i pod tą nazwą funkcjonuje ono w literaturze (matematycznej), mimo że Pell w ogóle się nim nie zajmował.[2] Najuczciwszą nazwą dla tego równania byłaby nazwa równanie Brahmagupty-Bhaskary [znany z geometrii Brahmagupta (VII wiek!) tysiąc lat przed Bachetem podał dowód T2.12, umiał wyznaczyć wszystkie rozwiązania równania $x^2 - 92y^2 = 1$, stosując do tego celu tożsamość (8.1); późniejszy o pół tysiąclecia Bhaskara wzmocnił różne wyniki swojego poprzednika – rozwiązanie równania $x^2 - 61y^2 = 1$ jest jego zasługą].

Ćwiczenie 11.32 Uzasadnić następującą ***równość Bhaskary***

$$\sqrt{a \pm \sqrt{b}} = \sqrt{\frac{a + \sqrt{a^2 - b}}{2}} \pm \sqrt{\frac{a - \sqrt{a^2 - b}}{2}}.$$

11.4.1 Twierdzenie podstawowe

Udowodnimy tu twierdzenie Lagrange'a o istnieniu rozwiązań równania indyjskiego.

Zauważmy przede wszystkim, że jeżeli $D = d^2$ jest kwadratem, to lewa strona równania (11.35) rozkłada się na czynniki w $\mathbb{Z}$: $x^2 - Dy^2 = (x + dy)(x - dy)$. Analiza równania (11.35) w tym przypadku jest trywialna i sprowadza się do rozpatrzenia dwóch układów równań

$$\begin{cases} x + dy = 1 \\ x - dy = 1 \end{cases} \quad \text{lub} \quad \begin{cases} x + dy = -1 \\ x - dy = -1 \end{cases}$$

W dalszym ciągu będziemy więc zakładać, że D nie jest kwadratem. Niemniej rozkład lewej strony na czynniki będzie nadal bardzo użyteczny. Chodzi o rozkład $(x + y\sqrt{D})(x - y\sqrt{D})$ w pierścieniu kwadratowym $\mathbb{Z}[\tau_D]$. Jasne, że para (x, y) jest rozwiązaniem równania indyjskiego (11.35) wtedy i tylko wtedy, gdy norma elementu $x + y\sqrt{D} \in \mathbb{Z}[\tau_D]$ jest równa 1.

Twierdzenie 11.5 *Jeżeli $D > 1$ jest liczbą naturalną nie będącą kwadratem, to równanie indyjskie* (11.35) *ma nieskończenie wiele rozwiązań w liczbach całkowitych. Ponadto, istnieje taka liczba $\alpha = a_1 + b_1\sqrt{D}$, gdzie $a_1, b_1 \in \mathbb{N}$, że każde rozwiązanie równania* (11.35) *ma postać $(\pm a_n, \pm b_n)$, gdzie liczby całkowite a_n, b_n dostajemy z równości*

$$\alpha^n = a_n + b_n\sqrt{D}. \tag{11.36}$$

[2] Byłoby uczciwszym mówić w tym miejscu o równaniu Fermat'a, który prawdopodobnie znał jakąś ogólną metodę rozwiązywania (jakże inaczej mógłby wiedzieć, że najmniejszym nietrywialnym (tzn. takim, że $y \neq 0$) rozwiązaniem równania $x^2 - 61y^2 = 1$ jest para $(1\,766\,319\,049,\ 226\,153\,980)$?)

D O W Ó D. Istnienie nieskończenie wielu rozwiązań równania indyjskiego wywnioskować można natychmiast z równości (7.30), wybierając takie $k \in \mathbb{N}$, żeby $ks \equiv 0 \,(\mathrm{mod}\, 2)$. W ten sposób twierdzenia dowodził Lagrange. Poniżej przedstawiamy konkurencyjne rozumowanie Dirichlet'*a*. Zaczniemy od lematu:

LEMAT 11.3 *Istnieje liczba naturalna m, dla której istnieją takie dwie różne pary (h_1, k_1) i (h_2, k_2) liczb naturalnych względnie pierwszych, że $|h_1^2 - Dk_1^2| = |h_2^2 - Dk_2^2| = m$ oraz $h_1 \equiv h_2 \,(\mathrm{mod}\, m)$, $k_1 \equiv k_2 \,(\mathrm{mod}\, m)$.*

D o w ó d l e m a t u. Wiemy z T7.4, że istnieje n i e s k o ń c z e n i e w i e l e ułamków nieskracalnych $\frac{h}{k}$, dla których

$$\left|\frac{h}{k} - \sqrt{D}\right| < \frac{1}{2k^2}.$$

Dla każdego takiego ułamka mamy

$$\left|\frac{h}{k} + \sqrt{D}\right| = \left|\frac{h}{k} - \sqrt{D} + 2\sqrt{D}\right| \leqslant \left|\frac{h}{k} - \sqrt{D}\right| + 2\sqrt{D} < \frac{1}{2k^2} + 2\sqrt{D} \leqslant 1 + 2\sqrt{D}.$$

Oznaczmy $M = \frac{1}{2} + \sqrt{D}$. Wówczas, dla każdego rozważanego ułamka $\frac{h}{k}$ zachodzi

$$|h^2 - Dk^2| = k^2 \left|\frac{h}{k} - \sqrt{D}\right| \cdot \left|\frac{h}{k} + \sqrt{D}\right| < k^2 \cdot \frac{1}{2k^2} \cdot \left|\frac{h}{k} + \sqrt{D}\right| = \frac{1}{2}\left|\frac{h}{k} + \sqrt{D}\right| \leqslant M.$$

Stąd wynika, że istnieje taka liczba naturalna $m \leqslant M$, że dla nieskończenie wielu par (h, k) liczb naturalnych względnie pierwszych zachodzi równość $|h^2 - Dk^2| = m$. Rozważając teraz $m^2 + 1$ takich par i powołując się na zasadę szufladkową, widzimy, że znajdą się takie dwie r ó ż n e pary (h_1, k_1) i (h_2, k_2), które spełniają warunki lematu. □

Przechodzimy do *d o w o d u* twierdzenia. Weźmy pary (h_1, k_1) i (h_2, k_2), których istnienie zapewnia nasz lemat, i rozważmy liczby

$$x = \frac{h_1h_2 - Dk_1k_2}{m}, \quad y = \frac{-h_1k_2 + h_2k_1}{m}.$$

Twierdzimy, że zachodzi równość $|x^2 - Dy^2| = 1$, przy czym $x \in \mathbb{Z}$, $y \in \mathbb{Z}_{\neq 0}$. Sprawdzenie, że $x, y \in \mathbb{Z}$ jest natychmiastowe. Dla dowodu równości $|x^2 - Dy^2| = 1$ oznaczmy $\varphi = h_1 + k_1\sqrt{D}$, $\psi = h_2 + k_2\sqrt{D}$. Wówczas $|\mathbf{N}(\varphi)| = |\mathbf{N}(\psi)| = m$ i, jak łatwo sprawdzić, $\varphi \cdot \psi' = mx + my\sqrt{D}$. Korzystając z (10.2), mamy zatem

$$m^2 = |\mathbf{N}(\varphi)\mathbf{N}(\psi)| = |(\varphi\psi')(\varphi\psi')'| = |(mx + my\sqrt{D})(mx - my\sqrt{D})| = m^2|x^2 - Dy^2|.$$

Stąd $|x^2 - Dy^2| = 1$. Ponadto, $y \neq 0$, bo $h_1k_2 \neq h_2k_1$ (równość $h_1k_2 = h_2k_1$, wobec względnej pierwszości par (h_1, k_1), (h_2, k_2), dawałaby równość $h_1 = h_2$ i $k_1 = k_2$, co jest niemożliwe). Mamy więc $x^2 - Dy^2 = 1$ lub $x^2 - Dy^2 = -1$. W pierwszym przypadku para (x, y) jest n i e t r y w i a l n y m (to znaczy takim, że $y \neq 0$) rozwiązaniem równania (11.35). Jeżeli zaś $x^2 - Dy^2 = -1$, to, jak łatwo sprawdzić, para $(x^2 + Dy^2, 2xy)$ jest nietrywialnym rozwiązaniem równania (11.35). W każdym więc razie widzimy, że równanie indyjskie (11.35) m a r o z w i ą z a n i a n i e t r y w i a l n e.

Ze wszystkich nietrywialnych rozwiązań $(x,\, y)$, dla których $x > 1$, $y > 0$, wybierzmy teraz rozwiązanie z najmniejszym x. Oznaczmy to rozwiązanie $(a_1,\, b_1)$. Oznaczmy też

$$\alpha = a_1 + b_1\sqrt{D}, \quad \beta = a_1 - b_1\sqrt{D} \ \left(= \alpha' = \frac{1}{\alpha}\right).$$

Liczby α i β są (rzeczywistymi) liczbami dodatnimi, przy czym $\alpha > 1$, $\beta < 1$ i $\alpha\beta = 1$. Ponieważ $\alpha > 1$, więc ciąg (α^n) jest ciągiem rosnącym do nieskończoności.

Niech teraz $(u,\, v)$ będzie dowolnym takim rozwiązaniem równania (11.35), że $u,\, v \in \mathbb{N}$. Wówczas liczba $\varphi = u + v\sqrt{D}$ jest liczbą rzeczywistą większą od 1. Więc istnieje dokładnie jeden wykładnik $n \in \mathbb{N}$, dla którego zachodzą nierówności $\alpha^n \leqslant \varphi < \alpha^{n+1}$. Mnożąc je przez liczbę (dodatnią) β^n otrzymamy nierówności równoważne

$$1 \leqslant \varphi\beta^n < \alpha = a_1 + b_1\sqrt{D}.$$

Jeżeli teraz zapiszemy (jednoznacznie!) liczbę $\varphi\beta^n$ w postaci $a + b\sqrt{D}$, $a,\, b \in \mathbb{Z}$, to,

$$a^2 - Db^2 = \mathbf{N}(a + b\sqrt{D}) = \mathbf{N}(\varphi\beta^n) = \mathbf{N}(\varphi)\mathbf{N}(\beta)^n = 1,$$

patrz (10.2). Zatem para $(a,\, b)$ jest (dodatnim) rozwiązaniem równania (11.35). Jednocześnie, na mocy L10.3 z ustępu 10.4.1, $a < a_1$, co, wobec minimalności a_1, jest możliwe tylko gdy $a = 1$. Stąd wynika, że $1 = \varphi\beta^n$, czyli $\varphi = \alpha^n$ co dowodzi równości (11.36). □

Uwaga. Rozwiązanie $(a_1,\, b_1)$ równania (11.35) nazywa się **rozwiązaniem fundamentalnym**. Można udowodnić, że najefektywniejszą metodą otrzymywania rozwiązań fundamentalnych równania indyjskiego jest metoda wynikająca z równości (7.30). Mianowicie: *jeżeli długość s okresu w rozwinięciu* (7.29) *jest liczbą parzystą, to rozwiązaniem fundamentalnym jest para $(P_{s-1},\, Q_{s-1})$; jeżeli zaś s jest liczbą nieparzystą, to rozwiązaniem fundamentalnym jest para $(P_{2s-1},\, Q_{2s-1})$*. Trzecia i czwarta kolumna w tabelce z ustępu 7.3.1 pokazują rozwiązanie fundamentalne odpowiedniego równania indyjskiego (o ile w piątej kolumnie występuje $+1$; przypadek, gdy występuje tam -1 omówimy w ustępie o równaniu *anty*-indyjskim).

Równanie indyjskie pojawia się w różnych zadaniach. Oto trzy przykłady:

ZADANIE 11.11 Wyznaczyć wszystkie trójkąty o bokach, których długości są kolejnymi liczbami naturalnymi i polu będącym liczbą całkowitą.

Rozwiązanie. Niech $n-1$, n, $n+1$ będą długościami boków pewnego trójkąta ($n \in \mathbb{Z}_{\geqslant 3}$). Ponieważ *pół*-obwód takiego trójkąta wynosi $\frac{3n}{2}$, więc, na mocy wzoru Herona, pole dane jest przez

$$S = \sqrt{\left(\frac{3n}{2}\right)\left(\frac{3n}{2} - (n-1)\right)\left(\frac{3n}{2} - n\right)\left(\frac{3n}{2} - (n+1)\right)} = \frac{n}{4}\sqrt{3n^2 - 12}.$$

Aby S było liczbą całkowitą n musi być liczbą parzystą (gdy n jest liczbą nieparzystą, to $3n^2 - 12 \equiv 3 \pmod 4$, nie jest więc kwadratem). Połóżmy więc $n = 2x$. Wówczas mamy $S = x\sqrt{3x^2 - 3}$. Ćwiczenie C2.19 poucza nas, że w takim przypadku $3x^2 - 3$ jest kwadratem (liczby całkowitej). Oczywiście kwadratem liczby $\frac{S}{x}$ podzielnej przez 3. Oznaczając $y = \frac{S}{3x}$ znajdujemy równość $x^2 - 3y^2 = 1$. Rozwiązaniem fundamentalnym tego równania jest para $(2,\, 1)$. Widzimy więc, że najmniejszym poszukiwanym trójkątem jest trójkąt o bokach 3, 4, 5 i polu 6. Kolejnymi są: trójkąt 13, 14, 15 o polu 84 i trójkąt 51, 52, 53 o polu 1170. ◊

Ćwiczenie 11.33 Wyznaczyć wszystkie takie $n \in \mathbb{N}$, że $n(n+1)/3$ jest kwadratem.

Ćwiczenie 11.34 Rozwiązać równanie $(x+1)^3 - x^3 = y^2$ w liczbach całkowitych.

11.4.2 Interpretacje

Opowiemy tu o dwóch sposobach myślenia o równaniu indyjskim.

Związek z ciągami rekurencyjnymi

Niech, przy ustalonym $D > 1$ bezkwadratowym, para $(A, B) = (a_1, b_1)$ będzie rozwiązaniem fundamentalnym równania indyjskiego (11.35). Wynikająca z (11.36) równość

$$a_{n+1} + b_{n+1}\sqrt{D} = (A + B\sqrt{D})(a_n + b_n\sqrt{D})$$

po wymnożeniu i wykorzystaniu niewymierności $\sqrt{D}$, daje układ równości

$$\begin{cases} a_{n+1} = Aa_n + BDb_n, \\ b_{n+1} = Ba_n + Ab_n. \end{cases}$$

Z tego układu równości rekurencyjnych wnioskujemy, że oba ciągi (a_n) i (b_n) są elementami zbioru $\mathcal{R}ek(2A, -1)$, czyli że oba spełniają równanie rekurencyjne

$$x_{n+2} = 2Ax_{n+1} - x_n. \tag{11.37}$$

Istotnie,

$$\begin{aligned} a_{n+2} &= Aa_{n+1} + BDb_{n+1} = Aa_{n+1} + BD(Ba_n + Ab_n) = Aa_{n+1} + B^2Da_n + A \cdot BDb_n \\ &= Aa_{n+1} + B^2Da_n + A(a_{n+1} - Aa_n) = 2Aa_{n+1} - (A^2 - B^2D)a_n \\ &= 2Aa_{n+1} - a_n. \end{aligned}$$

Tak samo sprawdzamy, że $(b_n) \in \mathcal{R}ek(2A, -1)$. Warunkami początkowymi dla tych ciągów są: $a_0 = 1$, $a_1 = A$ oraz $b_0 = 0$, $b_1 = B$, odpowiednio. Zauważmy, że wyróżnik wielomianu charakterystycznego równania rekurencyjnego (11.37) jest równy $4B^2D$. Istotnie, $4A^2 - 4 = 4(A^2 - 1) = 4B^2D$.

ZADANIE 11.12 Wyznaczyć dwie najmniejsze wartości $s \in \mathbb{N}$, dla których liczby $7s+1$ i $42s+7$ są jednocześnie kwadratami liczb naturalnych.

Rozwiązanie. Załóżmy, że $42s + 7 = x^2$ i $7s + 1 = y^2$, $x, y > 0$. Wówczas

$$x^2 - 6y^2 = 1. \tag{11.38}$$

Co oznacza, że para (x, y) jest dodatnim rozwiązaniem równania indyjskiego (11.35) z $D = 6$. O tym równaniu wiemy, że ma rozwiązanie fundamentalne $(5, 2)$ odpowiadające liczbie $\alpha = 5 + 2\sqrt{6}$. Z twierdzenia T11.5 i opisanego związku z ciągami rekurencyjnymi, wnosimy, że $(x, y) = (a_n, b_n)$ dla pewnego n, gdzie ciągi (a_n) i (b_n) spełniają to samo równanie

rekurencyjne $x_{n+2} = 10x_{n+1} - x_n$, przy czym: $a_0 = 1$, $a_1 = 5$ oraz $b_0 = 0$, $b_1 = 2$. Musimy wyznaczyć takie dwa najmniejsze indeksy n, by $b_n^2 - 1 \equiv 0 \,(\mathrm{mod}\, 7)$. Dla takich n, wobec równości (11.38), mamy też $a_n^2 - 7 \equiv 0 \,(\mathrm{mod}\, 42)$ i

$$s = \frac{b_n^2 - 1}{7} = \frac{a_n^2 - 7}{42}$$

są poszukiwanymi wartościami s. Zredukujmy ciąg (b_n) modulo 7:

$$b_n \,(\mathrm{mod}\, 7): \quad \mathbf{0},\, \mathbf{2},\, \boxed{\mathbf{6}},\, \mathbf{2},\, \mathbf{0},\, \mathbf{5},\, \boxed{\mathbf{1}},\, \mathbf{5},\, \mathbf{0},\, \mathbf{2},\, \ldots\,.$$

Ciąg zredukowany jest okresowy, porównaj T9.7. Widzimy stąd, że pierwszymi dwoma indeksami n, dla których $b_n^2 \equiv 1 \,(\mathrm{mod}\, 7)$ są $n = 2$ i $n = 6$. Odpowiednie wartości s:

$$s = s_2 = \frac{b_2^2 - 1}{7} = 57, \quad s = s_6 = \frac{b_6^2 - 1}{7} = \frac{192060^2 - 1}{7} = 5\,269\,577\,657.$$

Tej drugiej wartości zapewne nie byłoby łatwo znaleźć metodą prób i błędów... . ◊

Interpretacja geometryczno-algebraiczna: Hiperbola z mnożeniem

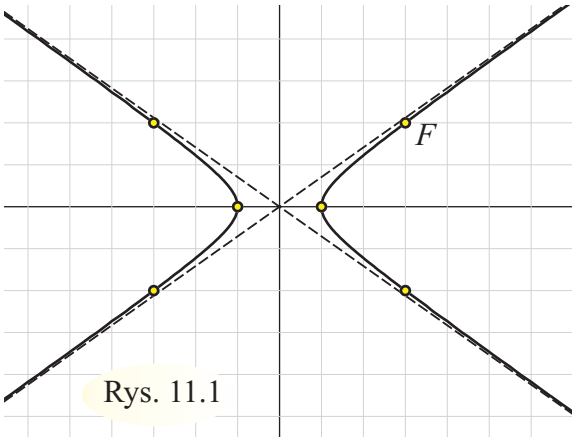
Równanie indyjskie $x^2 - Dy^2 = 1$ jest równaniem hiperboli $\mathcal{H}_D$ o asymptotach $x = \pm\sqrt{D}y$. Rozwiązania tego równania (w interpretacji geometrycznej) są punktami kratowymi, przez które przechodzi ta hiperbola. Jest rzeczą bardzo interesującą i niezwykłą, że taka hiperbola przechodzi przez nieskończenie wiele punktów kratowych.

Na rysunku 11.1 widzimy sześć punktów kratowych na hiperboli $\mathcal{H}_2$. Punkt $F = (3,\, 2)$ jest rozwiązaniem fundamentalnym równania

$$x^2 - 2y^2 = 1.$$

W zbiorze $\mathcal{H}_D$ określimy działanie $*$:

$$(x,\, y) * (u,\, v) = (xu + Dyv,\, xv + yu).$$



Rys. 11.1

Ćwiczenie 11.35 Udowodnić, że powyższa formuła zadaje działanie w zbiorze $\mathcal{H}_D$ i że działanie to jest łączne i przemienne, a punkt $(1,\, 0)$ jest elementem neutralnym.

Ćwiczenie 11.36 Udowodnić, że element $(x,\, y)' = (x,\, -y)$ jest elementem odwrotnym do elementu $(x,\, y)$. Wywnioskować stąd, że $(\mathcal{H}_D,\, *)$ jest grupą.

Ćwiczenie 11.37 Niech $\mathcal{H}_D^+ = \{(x,\, y) : x^2 - Dy^2 = 1,\, x > 0\}$ oznacza "prawą" gałąź hiperboli $\mathcal{H}_D$. Udowodnić, że $\mathcal{H}_D^+$ jest podgrupą w $(\mathcal{H}_D,\, *)$.

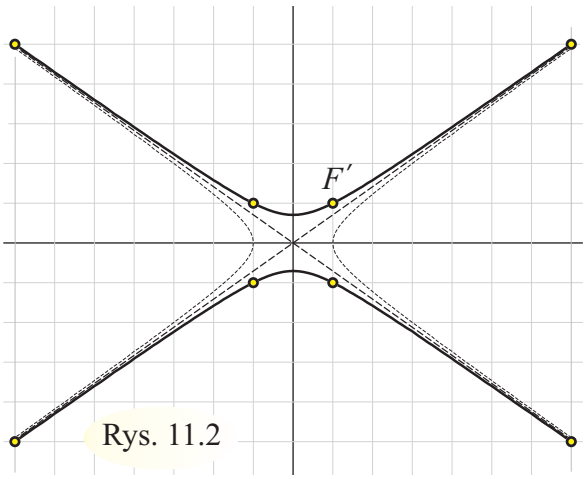
11.4.3 Równanie *anty*-indyjskie

Niech $D \in \mathbb{N}$ nie będzie kwadratem. Nieco żartobliwą nazwę **równanie anty-indyjskie**:

$$x^2 - Dy^2 = -1 \tag{11.39}$$

będziemy w dalszym ciągu traktować poważnie.

Na rysunku 11.2 mamy hiperbolę o równaniu $x^2 - 2y^2 = -1$ i osiem punktów kratowych na niej. Punkt $F' = (1, 1)$ jest generatorem.



Rys. 11.2

Ćwiczenie 11.38 Udowodnić, że jeżeli para (u_1, v_1) jest rozwiązaniem równania *anty*-indyjskiego (11.39), to para (u_n, v_n) wyznaczona z równości

$$(u_1 + v_1\sqrt{D})^n = u_n + v_n\sqrt{D}$$

jest, przy n parzystym, rozwiązaniem równania indyjskiego (11.35), a przy n nieparzystym, rozwiązaniem równania *anty*-indyjskiego (11.39). W tym sensie rozwiązania równania *anty*-indyjskiego są bardziej "fundamentalne" niż rozwiązania równania indyjskiego. Ich wadą jest to, że n i e z a w s z e i s t n i e j ą.

P r z y k ł a d 1. Ponieważ $(1 + \sqrt{2})^7 = 239 + 169\sqrt{2}$, a para $(1, 1)$ jest rozwiązaniem równania $x^2 - 2y^2 = -1$, więc i para $(239, 169)$ jest rozwiązaniem tego równania. ◊

P r z y k ł a d 2. Weźmy $D = 8$. Jasne, że $(3, 1)$ jest rozwiązaniem równania indyjskiego. Jest to rozwiązanie fundamentalne. Odpowiednie równanie *anty*-indyjskie nie ma rozwiązań. Istotnie, gdyby $x^2 - 8y^2 = -1$, to $x^2 \equiv -1 \pmod 4$, co jest niemożliwe. ◊

U w a g a. Można udowodnić, że równanie *anty*-indyjskie (11.39) ma rozwiązania wtedy i tylko wtedy, gdy liczba s (długość okresu) występująca w równości (7.29) jest nieparzysta. W takim przypadku rozwiązaniem fundamentalnym równania (11.39) jest para (P_{s-1}, Q_{s-1}). W tabelce z ustępu 7.3.1 zaznaczono ten przypadek znakiem -1 w piątej kolumnie. Ciekawym wyzwaniem dla młodego matematyka byłoby podanie arytmetycznej charakteryzacji tych liczb D, dla których s jest liczbą nieparzystą.

ZADANIE 11.13 Wyznaczyć wszystkie trójkąty prostokątne o długościach boków będących liczbami całkowitymi i takimi, że jedna przyprostokątna jest o 1 dłuższa od drugiej.

R o z w i ą z a n i e. Oznaczmy przez u długość krótszej przyprostokątnej, a przez y długość przeciwprostokątnej. Wówczas $u^2 + (u+1)^2 = y^2$ czyli $(2u+1)^2 - 2y^2 = -1$. Widzimy więc, że szukamy wszystkich rozwiązań (x, y) równania *anty*-indyjskiego

$$x^2 - 2y^2 = -1, \tag{11.40}$$

w których x jest nieparzyste (i > 1!). Ponieważ rozwiązaniem fundamentalnym równania (11.40) jest para $(1, 1)$, więc wszystkie rozwiązania (x_k, y_k) znajdujemy z równości

$$(1 + \sqrt{2})^{2k+1} = (1 + \sqrt{2})(3 + 2\sqrt{2})^k = x_k + y_k\sqrt{2}.$$

Jasne więc, że $x_{k+1} = 3x_k + 4y_k$. Zatem $x_{k+1} \equiv x_k \equiv \ldots \equiv x_1 \equiv 3 \,(\mathrm{mod}\, 2)$ jest liczbą nieparzystą dla każdego k. $\Diamond$

Ćwiczenie 11.39 Udowodnić, że istnieje nieskończenie wiele takich liczb naturalnych n, dla których $n^2+1|n!$. *Wskazówka.* Równanie $n^2-5k^2 = -1$ ma nieskończenie wiele rozwiązań.

11.4.4 Ogólne równanie indyjskie

Nie będziemy dowodzić żadnych twierdzeń na temat ogólnego równania indyjskiego (11.41). W jednym zadaniu pokażemy tylko przykładowy sposób postępowania z takimi równaniami.

Ogólnym równaniem indyjskim nazwiemy równanie

$$Px^2 - Qy^2 = R, \tag{11.41}$$

gdzie $P, Q \in \mathbb{N}$, są liczbami bezkwadratowymi, $R \in \mathbb{Z}$.

U w a g a 1. Oznaczmy $\mathrm{NWD}\,(P, Q) = d$. Wówczas, jeżeli $d \nmid R$, to równanie (11.41) na pewno n i e m a rozwiązań w liczbach całkowitych x, y. Jeżeli zaś $d|R$, to dzieląc obustronnie przez d, otrzymamy równanie r ó w n o w a ż n e $P'x^2 - Q'y^2 = R'$, gdzie P', Q' są względnie pierwsze. Możemy więc od początku zakładać, że w równaniu (11.38) współczynniki P, Q są względnie pierwsze.

U w a g a 2. Jedno konkretne rozwiązanie równania (11.41) powinniśmy znaleźć "na piechotę", czyli po prostu o d g a d n ą ć. Pewną pomocą mogą tu służyć wzory (2.12).

U w a g a 3. Załóżmy teraz, że $R = \pm 1$. Wówczas, jeżeli jeden ze współczynników P, Q jest równy 1, to mamy do czynienia z równaniem indyjskim lub *anty*-indyjskim. Niech więc $P, Q \neq 1$. W takiej sytuacji główną sztuczką podczas rozwiązywania naszego równania jest sprowadzanie lewej strony do **postaci normowej**:

$$Px^2 - Qy^2 = (x\sqrt{P} + y\sqrt{Q})(x\sqrt{P} - y\sqrt{Q}). \tag{11.42}$$

Ćwiczenie 11.40 Zakładamy, że P, Q są względnie pierwszymi liczbami naturalnymi bezkwadratowymi. Uzasadnić, że jeżeli $n \in \mathbb{N}$ jest wykładnikiem p a r z y s t y m, to dla dowolnych całkowitych a, b zachodzą równości:

$$(a\sqrt{P} + b\sqrt{Q})^n = A_n + B_n\sqrt{PQ},$$
$$(a\sqrt{P} - b\sqrt{Q})^n = A_n - B_n\sqrt{PQ},$$

przy pewnych całkowitych $A_n = A_n(a, b)$, $B_n = B_n(a, b)$. Jeżeli zaś $n \in \mathbb{N}$ jest wykładnikiem n i e p a r z y s t y m, to dla dowolnych całkowitych a, b zachodzą równości:

$$(a\sqrt{P} + b\sqrt{Q})^n = C_n\sqrt{P} + D_n\sqrt{Q},$$
$$(a\sqrt{P} - b\sqrt{Q})^n = C_n\sqrt{P} - D_n\sqrt{Q},$$

przy pewnych całkowitych $C_n = C_n(a, b)$, $D_n = D_n(a, b)$.

Powyższe uwagi i ćwiczenie można zobaczyć w działaniu w poniższym zadaniu:

ZADANIE 11.14 Udowodnić, że równanie $7x^2 - 3y^2 = 67$ ma nieskończenie wiele rozwiązań w liczbach całkowitych x, y.

Rozwiązanie. Zgodnie z U2, zgadujemy jedno rozwiązanie:

$$7 \cdot 5^2 - 3 \cdot 6^2 = (5\sqrt{7} + 6\sqrt{3})(5\sqrt{7} - 6\sqrt{3}) = 67.$$

Również równanie pomocnicze $7x^2 - 3y^2 = 1$ ma łatwe do odgadnięcia rozwiązanie:

$$7 \cdot 2^2 - 3 \cdot 3^2 = (2\sqrt{7} + 3\sqrt{3})(2\sqrt{7} - 3\sqrt{3}) = 1.$$

Korzystając z ćwiczenia C11.40, łatwo wykazać, że jeżeli, przy dowolnym $k \in \mathbb{N}$, przedstawimy liczbę

$$(5\sqrt{7} + 6\sqrt{3})(2\sqrt{7} + 3\sqrt{3})^{2k-1}$$

w postaci $U_k\sqrt{7} + V_k\sqrt{3}$, gdzie $U_k, V_k \in \mathbb{N}$, to para (U_k, V_k) jest rozwiązaniem równania $7x^2 - 3y^2 = 67$. Ponadto, $U_k \to \infty$. ◊

11.4.5 Kilka zadań

Proponujemy jeszcze kilka zadań "na" równanie indyjskie (lub podobne).

Ćwiczenie 11.41 Niech (a_n), (b_n) będą dwoma ciągami wyznaczonymi przez warunki $a_1 = 3$, $b_1 = 2$ i rekurencję

$$\begin{cases} a_{n+1} = 3a_n + 4b_n, \\ b_{n+1} = 2a_n + 3b_n. \end{cases}$$

Udowodnić, że dla każdego n zachodzi równość $a_n + 2b_n = \lfloor (a_n + b_n)\sqrt{2} \rfloor$.

Ćwiczenie 11.42 Wyznaczyć najmniejszą liczbę naturalną n, dla której liczby $19n+1$ i $95n + 1$ są kwadratami liczb całkowitych.

Ćwiczenie 11.43 Udowodnić, że równanie $x^2+y^2+z^2+2xyz = 1$ ma nieskończenie wiele rozwiązań w takich liczbach całkowitych x, y, z, że $|x|, |y|, |z| \geqslant 2011$.

Ćwiczenie 11.44 Istnieje nieskończenie wiele $n \in \mathbb{N}$ takich, że $3n+1$ i $n+1$ są kwadratami. Udowodnić, że jeżeli n_k jest k-tą taką liczbą, to $n_k n_{k+1} + 1$ również jest kwadratem.

Ćwiczenie 11.45 W urnie jest n kul białych i m kul czarnych. Prawdopodobieństwo, że dwie wyciągnięte losowo kule są tego samego koloru wynosi dokładnie $\frac{1}{2}$. Wyznaczyć możliwe wartości m, n.

Ćwiczenie 11.46 Wyznaczyć nieujemne m, n, dla których $\binom{n}{m} = \binom{n-1}{m+1}$.

Ćwiczenie 11.47 Wyznaczyć rozwiązania w liczbach całkowitych układu równań

$$\begin{cases} 2uv - xy = 16, \\ xv - uy = 12. \end{cases}$$

Wskazówka. Zauważyć, że $16^2 - 2 \cdot 12^2 = -32$.

Ćwiczenie 11.48 Czy średnia kwadratowa liczb $1, 2, \ldots, n$ może być liczbą całkowitą? *Wskazówka.* Zobacz C1.2.1.

Ćwiczenie 11.49 Rozwiązać w liczbach naturalnych $(1 + x^2)(1 + y^2) = 1 + z^2$.

Ćwiczenie 11.50 Wyznaczyć liczby naturalne a, b, dla których $ab|a^2 + b^2 + 1$.

Ćwiczenie 11.51 Trzywyrazowy ciąg arytmetyczny $(1, 8, 15)$ ma taką własność, że iloczyn każdych dwóch wyrazów jest postaci $x^2 - 1$. Wyznaczyć inne takie ciągi.

Ćwiczenie 11.52 Rozważmy **kongruencję indyjską** $x^2 - Dy^2 \equiv 1 \,(\mathrm{mod}\, m)$. Oznaczmy przez $\mathcal{I}(D, m)$ zbiór wszystkich rozwiązań takiej kongruencji (w $\mathbb{Z}/m \times \mathbb{Z}/m$). Wprowadzić strukturę grupową w zbiorze $\mathcal{I}(D, p)$. Czy grupa ta jest cykliczna? Udowodnić, że $|\mathcal{I}(D, p^n)| = p^{n-1}|\mathcal{I}(D, p)|$.

Ćwiczenie 11.53 Rozwiązać równanie $x^3 - 3y^3 = 1$ w liczbach całkowitych. *Wskazówka.* Zapisać to równanie w postaci $(x - 1)(x - \omega)(x - \omega^2) = -\omega\lambda^2 y^3$, zob. C10.75, i postępować według wzoru z ustępu 11.2.3 dla dowodu, że jedynym rozwiązaniem jest rozwiązanie trywialne $(x, y) = (1, 0)$.

11.5 Punkty wymierne na prostych i na stożkowych

W tym paragrafie zajmiemy się rozwiązaniami równań diofantycznych postaci $\varphi(x, y) = 0$, gdzie $\varphi(X, Y)$ jest wielomianem o współczynnikach wymiernych. Mnożąc obie strony tego równania przez wspólny mianownik wszystkich współczynników otrzymamy r ó w n o w a ż n e równanie o współczynnikach całkowitych. Odtąd zakładamy więc, że $\varphi(X, Y) \in \mathbb{Z}[X, Y]$. Jeżeli φ jest takim wielomianem, a $\mathcal{R}$ jest pierścieniem, to oznaczamy

$$\mathcal{N}(\varphi; \mathcal{R}) = \{(x, y) \in \mathcal{R} \times \mathcal{R} : \varphi(x, y) = 0\}.$$

W szczególności $\mathcal{N}(\varphi; \mathbb{Q})$ oznacza zbiór rozwiązań równania $\varphi(x, y) = 0$ w liczbach wymiernych, a $\mathcal{N}(\varphi; \mathbb{Z})$ zbiór rozwiązań tego równania w liczbach całkowitych.

Ćwiczenie 11.54 Niech $\varphi(X, Y) = X^2 + Y^2 - 1$. Opiszcie zbiory $\mathcal{N}(\varphi; \mathbb{R})$, $\mathcal{N}(\varphi; \mathbb{Q})$, $\mathcal{N}(\varphi; \mathbb{Z})$, $\mathcal{N}(\varphi; \mathbb{Z}/7)$, $\mathcal{N}(\varphi; \mathbb{Z}/8)$ i, jeżeli wystarczy wam wyobraźni, $\mathcal{N}(\varphi; \mathbb{C})$.

W dalszym ciągu ograniczymy się do badania wielomianów φ stopnia pierwszego, drugiego i (w paragrafie 11.6) trzeciego. Będziemy się zajmowali głównie rozwiązaniami w y m i e r n y m i.

Równania stopnia pierwszego

Przypadek $\deg\varphi = 1$ jest bardzo prosty.

Niech $\varphi(X, Y) = aX + bY + c \in \mathbb{Z}[X, Y]$ będzie wielomianem stopnia pierwszego o współczynnikach całkowitych. Równanie

$$\varphi(x, y) = ax + by + c = 0 \tag{11.43}$$

jest, jak to dobrze wiemy, r ó w n a n i e m p r o s t e j na płaszczyźnie. Zbiór $\mathcal{N}(\varphi; \mathbb{R})$ jest więc prostą. Jego podzbiór $\mathcal{N}(\varphi; \mathbb{Q})$ rozwiązań wymiernych jest, w tej interpretacji, zbiorem punktów o obu współrzędnych wymiernych, przez które ta prosta przechodzi.

ZADANIE 11.15 Opisać punkty wymierne na prostej o równaniu (11.43).

R o z w i ą z a n i e. Opis, o który nam chodzi jest tak zwanym **opisem parametrycznym**. Otrzymujemy go, w tym przypadku, bardzo prosto. Załóżmy, że (x_0, y_0) jest dowolnym punktem wymiernym leżącym na tej prostej. Taki punkt łatwo znaleźć. Gdy $b \neq 0$, to wystarczy wziąć $(x_0, y_0) = \left(0, -\frac{c}{b}\right)$. Wówczas

$$\begin{cases} x_\lambda = x_0 + b\lambda \\ y_\lambda = y_0 - a\lambda \end{cases} \tag{11.44}$$

jest, oczywiście, szukanym opisem parametrycznym zbioru (w s z y s t k i c h) punktów wymiernych na badanej prostej. To znaczy, że każdy punkt wymierny leżący na tej prostej jest postaci (x_λ, y_λ) dla pewnego $\lambda \in \mathbb{Q}$ i odwrotnie, równości (11.44) pozwalają każdej liczbie wymiernej λ przyporządkować punkt wymierny (x_λ, y_λ) na prostej. $\Diamond$

W T2.12 opisaliśmy zbiór $\mathcal{N}(\varphi; \mathbb{Z})$. Wiemy więc, że jest on niepusty wtedy i tylko wtedy, gdy $\mathrm{NWD}\,(a, b)|c$. Wzory (2.12) stanowią opis parametryczny tego zbioru.

Równania stopnia drugiego

Teraz zajmiemy się ogólnym równaniem stopnia drugiego dwóch zmiennych, ale będziemy poszukiwać r o z w i ą z a ń w y m i e r n y c h.

Niech dany będzie wielomian stopnia 2 dwóch zmiennych:

$$\varphi(X, Y) = aX^2 + bXY + cY^2 + dX + eY + f \in \mathbb{Z}[X, Y]. \tag{11.45}$$

Zbiór wszystkich rzeczywistych rozwiązań równania $\varphi(x, y) = 0$, czyli zbiór

$$\mathcal{N}(\varphi; \mathbb{R}) = \{(x, y) \in \mathbb{R}^2 : \varphi(x, y) = 0\}$$

jest krzywą na płaszczyźnie. Taka krzywa nazywa się **krzywą stożkową**. W zależności od współczynników $a, b, \ldots, f$ może to być **elipsa** (w szczególnym przypadku: okrąg), **parabola** lub **hiperbola**. Możemy też mieć do czynienia z przypadkami z d e g e n e r o w a n y m i: krzywa może być w istocie parą prostych lub jedną prostą. Czasami (na płaszczyźnie rzeczywistej) może to być zbiór jednopunktowy, a nawet zbiór pusty.

P r z y k ł a d 1. Jasne, że jeżeli wielomian φ rozkłada się na iloczyn wielomianów pierwszego stopnia: $\varphi(X, Y) = (aX + bY + c)(pX + qY + r)$, to krzywa $\mathcal{N}(\varphi; \mathbb{R})$ jest sumą teoriomnogościową prostych o równaniach $ax + by + c = 0$ i $px + qy + r = 0$. $\Diamond$

Ćwiczenie 11.55 Naszkicować krzywe $\mathcal{N}(\varphi;\mathbb{R})$ dla poniższych wielomianów $\varphi(X,Y)$:

1. $\varphi(X,Y)=X^2+2Y^2-2X+16Y+24$,
2. $\varphi(X,Y)=Y^2-3X-2Y-2$,
3. $\varphi(X,Y)=XY-2X+Y-5$,
4. $\varphi(X,Y)=2X^2+XY-Y^2+3Y-2$,
5. $\varphi(X,Y)=X^2+4XY+4Y^2+2X+4Y+1$,
6. $\varphi(X,Y)=X^2+Y^2-2X+4Y+5$,
7. $\varphi(X,Y)=2X^2-2XY+5Y^2+1$.

Ćwiczenie 11.56 Udowodnić, że na okręgu o równaniu $x^2+y^2=3$ nie leży ani jeden punkt wymierny. Ogólniej: jeżeli p jest liczbą pierwszą i $p\equiv 3\,(\mathrm{mod}\,4)$, to na okręgu o równaniu $x^2+y^2=p$ nie leży ani jeden punkt wymierny. A co gdy $p\equiv 1\,(\mathrm{mod}\,4)$?

Widzimy, że w przypadku niezdegenerowanych krzywych drugiego stopnia (stożkowych) sytuacja jest inna niż w przypadku krzywych pierwszego stopnia (czyli prostych). Tam, wymierność współczynników gwarantowała niepustość zbioru $\mathcal{N}(\varphi;\mathbb{Q})$, tu, n i e g w a r a n t u j e. Jednakże, gdy zbiór $\mathcal{N}(\varphi;\mathbb{Q})$ zawiera choćby jeden element, to zawiera ich nieskończenie wiele i, co więcej, można je (prawie) wszystkie opisać parametrycznie. Mówi o tym poniższe:

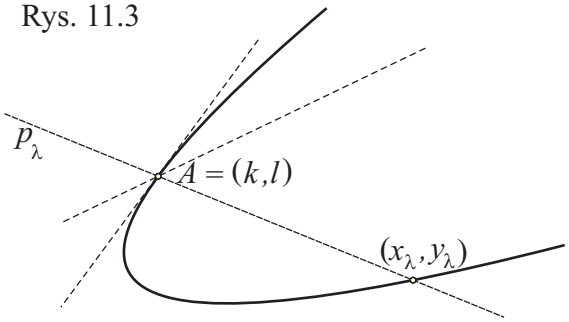
Twierdzenie 11.6 *Niech $\varphi(X,Y)\in\mathbb{Z}[X,Y]$ będzie takim wielomianem drugiego stopnia, że $\mathcal{N}(\varphi;\mathbb{R})$ jest stożkową niezdegenerowaną. Załóżmy, że zbiór $\mathcal{N}(\varphi;\mathbb{R})$ zawiera punkt w y m i e r n y (czyli że $\mathcal{N}(\varphi;\mathbb{Q})\neq\varnothing$). Wówczas zbiór ten zawiera nieskończenie wiele punktów wymiernych. Ponadto, istnieje parametryczny opis prawie całego zbioru $\mathcal{N}(\varphi;\mathbb{Q})$.*

D O W Ó D. Załóżmy, że $A=(k,l)$ jest punktem krzywej $\mathcal{N}(\varphi;\mathbb{R})$. Prowadzimy przez punkt A wszystkie proste. Każda taka prosta p_λ (z wyjątkiem prostej $x=k$) ma równanie postaci

$$y-l=\lambda(x-k),$$

gdzie $\lambda\in\mathbb{R}$ jest dowolnym parametrem. Wyznaczamy drugi punkt (x_λ,y_λ) przecięcia prostej p_λ z krzywą $\mathcal{N}(\varphi;\mathbb{R})$. To, oczywiście, oznacza, że wyznaczamy drugie, obok (k,l), rozwiązanie układu równań

Rys. 11.3



$$\begin{cases} ax^2+bxy+cy^2+dx+ey+f=0,\\ y-l=\lambda(x-k).\end{cases}$$

Podstawiając $y=\lambda(x-k)+l$ do pierwszego równania, otrzymamy równanie kwadratowe z parametrem λ (jeżeli, co zakładamy w dalszym ciągu, $a+b\lambda+c\lambda^2\neq 0$) o niewiadomej x:

$$\left[a+b\lambda+c\lambda^2\right]x^2+\left[d+bl+(2cl-bk+e)\lambda+2ck\lambda^2\right]x+c(l-k\lambda)^2+e(l-k\lambda)+f=0.$$

O tym równaniu wiemy, że ma ono pierwiastek równy k. Drugi pierwiastek x_λ wyznaczamy ze wzoru Viète'a:

$$k+x_\lambda=-\frac{d+bl+(-bk+2cl+e)\lambda+2ck\lambda^2}{a+b\lambda+c\lambda^2}.$$

Następnie wyznaczamy y_λ (z równości $y_\lambda = \lambda(x_\lambda - k) + l$). Dostaniemy ostatecznie:

$$\begin{cases} x_\lambda = \dfrac{-(ak + bl + d) - (2cl + e)\lambda + ck\lambda^2}{a + b\lambda + c\lambda^2}, \\ y_\lambda = \dfrac{al - (2ak + d)\lambda - (cl + bk + e)\lambda^2}{a + b\lambda + c\lambda^2}. \end{cases} \tag{11.46}$$

Zapamiętywanie wzorów (11.46) nie jest celowe – w każdym konkretnym przypadku wyprowadzamy odpowiednie wzory od początku, pamiętając jedynie sposób postępowania. Otrzymaliśmy w ten sposób **opis parametryczny** (prawie) wszystkich punktów krzywej $\mathcal{N}(\varphi; \mathbb{R})$:

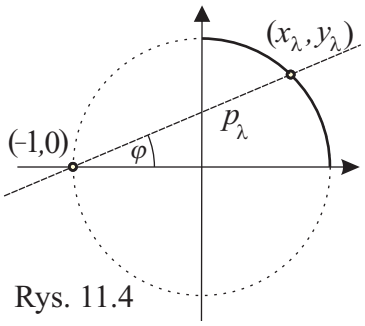
Gdy parametr λ przebiega zbiór $\mathbb{R}$, to punkt (x_λ, y_λ) przebiega wszystkie punkty krzywej $\mathcal{N}(\varphi; \mathbb{R})$, z ewentualnym wyjątkiem drugiego punktu przecięcia prostej $x = k$ z krzywą.

Dotychczas nie wykorzystywaliśmy wymierności punktu (k, l). Wobec tego, opis postaci (11.46) jest możliwy dla każdej stożkowej niezdegenerowanej przechodzącej przez znany punkt (k, l). My interesujemy się teraz elementami zbioru $\mathcal{N}(\varphi; \mathbb{Q})$ p u n k t ó w w y m i e r n y c h krzywej o równaniu $\varphi(x, y) = 0$. Załóżmy więc, że punkt $A = (k, l)$ ma obie współrzędne wymierne (i leży na krzywej $\mathcal{N}(\varphi; \mathbb{R})$). Wówczas wszystkie proste p_λ (przechodzące przez A) i mające w y m i e r n y współczynnik kierunkowy λ przecinają krzywą (po raz drugi) w punkcie (x_λ, y_λ) o o b u w s p ó ł r z ę d n y c h w y m i e r n y c h. I odwrotnie: jeżeli punkt $B = (c, d) \in \mathcal{N}(\varphi; \mathbb{Q})$ jest punktem wymiernym, to prosta AB ma wymierny współczynnik kierunkowy. Czytelnik łatwo uzasadni oba powyższe stwierdzenia. □

Ilustracją twierdzenia T11.6 jest (nasz) trzeci sposób wyznaczania trójek pitagorejskich:

ZADANIE 11.16 Wyznaczyć trójki pitagorejskie.

R o z w i ą z a n i e. Niech (a, b, c) będzie niezerową trójką pitagorejską. Wówczas punkt $(x, y) = (a/c, b/c)$ jest punktem wymiernym dodatniej ćwiartki okręgu o równaniu $x^2 + y^2 = 1$. Czyli jest drugim punktem przecięcia prostej p_λ o równaniu $y = \lambda(x + 1)$ z okręgiem jednostkowym, zobacz rysunek 11.4, gdzie widzimy, że $\lambda = \operatorname{tg}\varphi$ jest współczynnikiem kierunkowym. Jej drugi punkt przecięcia z okręgiem ma, jak łatwo sprawdzić, współrzędne



Rys. 11.4

$$x = x_\lambda = (1 - \lambda^2)/(1 + \lambda^2), \quad y = y_\lambda = (2\lambda)/(1 + \lambda^2).$$

Ponieważ $x = a/c$, $y = b/c$ więc otrzymamy stąd $\frac{a}{1-\lambda^2} = \frac{c}{1+\lambda^2} = \frac{b}{2\lambda}$. Oznaczając przez μ wspólną wartość tych trzech ułamków dostaniemy:

$$a = (1 - \lambda^2)\,\mu, \quad b = 2\lambda\mu, \quad c = (1 + \lambda^2)\,\mu.$$

Jeżeli $0 < \lambda < 1$ i $\mu > 0$ są liczbami wymiernymi, to powyższe wzory dają wszystkie dodatnie w y m i e r n e trójki pitagorejskie. Ponieważ interesują nas trójki pitagorejskie (liczb naturalnych), więc połóżmy $\lambda = t/s$ (ułamek nieskracalny), $t, s \in \mathbb{N}$. Wówczas dostajemy

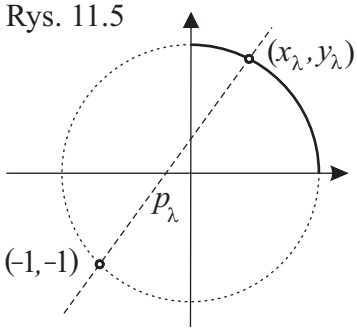
$$a = (s^2 - t^2)\mu', \quad b = 2st\mu', \quad c = (s^2 + t^2)\mu',$$

gdzie $\mu' = \mu/s^2$. Oznaczmy $d = \mathrm{NWD}\,(s^2-t^2,\, 2st,\, s^2+t^2)$. Wiemy, zobacz C11.57, że $d = 1$ lub $d = 2$. W przypadku $d = 1$ widać, że $s \not\equiv t \,(\mathrm{mod}\, 2)$, $\mu' \in \mathbb{N}$, więc dostajemy trójkę pierwotną, gdy $\mu' = 1$. W przypadku $d = 2$ widać, że $s \equiv t \equiv 1 \,(\mathrm{mod}\, 2)$ i wówczas, kładąc $u = (s+t)/2$, $v = (s-t)/2$, widzimy, że $(s^2-t^2)/2 = 2uv$, $st = u^2 - v^2$, $(s^2+t^2)/2 = u^2+v^2$, więc, przy $\mu' = 1/2$, dostajemy trójkę pierwotną jak w T2.20. ◊

Ćwiczenie 11.57 Uzasadnić, że jeżeli liczby całkowite s, t są względnie pierwsze, to największym wspólnym dzielnikiem liczb s^2-t^2, $2st$, s^2+t^2 jest 1 lub 2.

Taką samą technikę zastosujmy w kolejnym zadaniu:

Rys. 11.5



ZADANIE 11.17 Wyznaczyć wszystkie trójki kwadratów liczb wymiernych tworzące ciąg arytmetyczny.

Rozwiązanie. Szukamy (wszystkich) takich liczb wymiernych a, b, $c > 0$, dla których $c^2-a^2 = b^2-c^2$, czyli $a^2+b^2 = 2c^2$, więc równoważnie:

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 2,$$

co oznacza, że punkt $(a/c,\, b/c)$ jest punktem wymiernym na dodatniej części okręgu o równaniu $x^2+y^2 = 2$. Widzimy punkt wymierny $(-1,\, -1)$ leżący na tym okręgu. Wyznaczamy interesujące nas punkty wymierne zgodnie z wyłożoną techniką: Prosta p_λ przechodząca przez $(-1,\, -1)$ ma równanie $y = \lambda x + \lambda - 1$. Oznaczymy drugi punkt przecięcia tej prostej z okręgiem $x^2+y^2 = 2$ przez $(x_\lambda,\, y_\lambda)$. Punkt $(x_\lambda,\, y_\lambda)$ znajdujemy wyznaczając drugie, obok $(-1,\, -1)$, rozwiązanie układu równań

$$\begin{cases} x^2+y^2 = 2 \\ y = \lambda x + \lambda - 1 \end{cases} \tag{11.47}$$

Podstawiając $\lambda x + \lambda - 1$ w miejsce y w pierwszym z tych równań i porządkując, otrzymamy

$$(\lambda^2+1)x^2 + 2\lambda(\lambda-1)x + (\lambda-1)^2 - 2 = 0.$$

Wiemy, że to równanie kwadratowe względem x ma pierwiastek -1 (bo para $(-1,\, -1)$ jest rozwiązaniem układu (11.47)). Drugi pierwiastek x_λ, na mocy wzoru Viète'a, spełnia więc równość $(-1)\cdot x_\lambda = ((\lambda-1)^2-2)/(\lambda^2+1)$. Wobec tego

$$x_\lambda = \frac{-\lambda^2+2\lambda+1}{\lambda^2+1}, \quad y_\lambda = \frac{\lambda^2+2\lambda-1}{\lambda^2+1}.$$

Stąd, podobnie jak w rozwiązaniu Z11.16,

$$a = (-\lambda^2+2\lambda+1)\mu, \quad c = (\lambda^2+1)\mu, \quad b = (\lambda^2+2\lambda-1)\mu, \tag{11.48}$$

gdzie $\lambda \in (\sqrt{2}-1;\, \sqrt{2}+1)$, a μ jest dowolną liczbą wymierną (dodatnią). Zauważmy, że $\lambda = 1$ wyznacza stały ciąg arytmetyczny $a^2 = b^2 = c^2$. ◊

Ćwiczenie 11.58 Opisać wszystkie trójki a^2, b^2, c^2 kwadratów liczb całkowitych tworzące ciąg arytmetyczny.

Ćwiczenie 11.59 Wyznaczyć wszystkie rozwiązania równania $x^2 + 5y^2 = 6z^2$ w $\mathbb{Z}$.

Ćwiczenie 11.60 Udowodnić, że istnieje nieskończenie wiele parami niepodobnych trójkątów o bokach długości całkowitej i jednym z kątów o mierze 60°.

Powiemy jeszcze dwa słowa na temat momentu kluczowego: skąd wziąć jeden punkt wymierny w $\mathcal{N}(\varphi; \mathbb{R})$? Wiemy, że takiego punktu może w ogóle nie być (zobacz na przykład C2.66)! Gdy istnieją punkty wymierne, to czasami udaje się je wykryć. Kryterium, za pomocą którego można w skończonej liczbie kroków rozstrzygnąć czy takie punkty istnieją, pochodzi od Legendre'*a*:

TWIERDZENIE 11.7 (***Twierdzenie Legendre'a***) *Załóżmy, że $a, b, c \in \mathbb{Z}$ są parami względnie pierwszymi liczbami bezkwadratowymi różnych znaków. Wówczas równanie*

$$ax^2 + by^2 + cz^2 = 0$$

ma niezerowe rozwiązanie w liczbach całkowitych wtedy i tylko wtedy, gdy

$$(-ab)\mathbf{R}|c|, \quad (-ac)\mathbf{R}|b|, \quad (-bc)\mathbf{R}|a|. \qquad \blacktriangleright$$

Dowód implikacji ($\Longleftarrow$) jest dość trudny. Ale:

Ćwiczenie 11.61 Udowodnić implikację ($\Longrightarrow$) twierdzenia Legendre'*a*.

W poniższym przykładzie zobaczymy jak to działa.

Przykład 2. Rozważmy wielomian

$$\varphi(X, Y) = 23X^2 + 8XY + 17Y^2 - 48X - 54Y + 50.$$

Wykażemy, że zbiór $\mathcal{N}(\varphi; \mathbb{Q})$ jest pusty. Aby to zobaczyć przesuniemy najpierw układ współrzędnych tak, by w nowym układzie współrzędnych nasza krzywa miała równanie (drugiego stopnia, oczywiście) bez wyrazów stopnia pierwszego. Analitycznie oznacza to, że szukamy takich stałych α, β, dla których wielomian $\varphi(U + \alpha, V + \beta)$ zmiennych U, V nie ma wyrazów stopnia pierwszego. Wyznaczymy takie stałe w ogólnym przypadku (11.45). Mamy:

$$\varphi(U + \alpha, V + \beta) = \varphi(\alpha, \beta) + (d + 2a\alpha + b\beta)U + (e + b\alpha + 2c\beta)V + aU^2 + bUV + cV^2.$$

Wystarczy więc rozwiązać układ równań

$$\begin{cases} 2a\alpha + b\beta = -d, \\ b\alpha + 2c\beta = -e. \end{cases}$$

Ten układ ma rozwiązanie

$$\alpha = \frac{2cd - be}{\Delta}, \quad \beta = \frac{2ae - bd}{\Delta},$$

gdzie $\Delta = b^2 - 4ac$. Trzeba tu, oczywiście, mieć pewność, że $\Delta \neq 0$. W naszym przypadku mamy więc $\alpha = \frac{4}{5}$, $\beta = \frac{7}{5}$. Ponadto $\varphi\left(\frac{4}{5}, \frac{7}{5}\right) = -7$. Stąd widzimy, że $(x_0, y_0) \in \mathcal{N}(\varphi; \mathbb{Q})$ wtedy i tylko wtedy, gdy $\left(x_0 - \frac{4}{5}, y_0 - \frac{7}{5}\right) \in \mathcal{N}(\psi; \mathbb{Q})$, gdzie

$$\psi(X, Y) = 23X^2 + 8XY + 17Y^2 - 7.$$

Chcemy się teraz pozbyć wyrazu "mieszanego" $8XY$. W metrycznej geometrii analitycznej robi się to za pomocą stosownego obrotu. Jednakże, ponieważ po obrocie punkty wymierne zazwyczaj przestają być wymiernymi, a my chcemy mieć kontrolę nad wymiernością punktów, więc musimy się uciec do wymiernego przekształcenia liniowego (to znaczy zadanego przez macierz o wyrazach wymiernych). Robi się to przez standardową procedurę uzupełniania do p e ł n e g o k w a d r a t u:

$$23\psi(X, Y) = (23X + 4Y)^2 + 15 \cdot (5Y)^2 - 161.$$

Widzimy stąd, że jeżeli $(x_0, y_0) \in \mathcal{N}(\varphi; \mathbb{Q})$, to

$$\left(23\left(x_0 - \frac{4}{5}\right) + 4\left(y_0 - \frac{7}{5}\right), 5\left(y_0 - \frac{7}{5}\right)\right) = (23x_0 + 4y_0 - 24, 5y_0 - 7) \in \mathcal{N}(\chi; \mathbb{Q}),$$

gdzie $\chi(X, Y) = X^2 + 15Y^2 - 161$. Gdyby jednak punkt wymierny $(u/w, v/w)$ należał do $\mathcal{N}(\chi; \mathbb{Q})$, to mielibyśmy $u^2 + 15v^2 - 161w^2 = 0$. Ale, jak łatwo sprawdzić, $161\mathbf{N}15$, więc, na mocy T11.7, mamy sprzeczność. $\Diamond$

Ćwiczenie 11.62 Sprawdzić, że stożkowa $7x^2 + 22xy - 2y^2 + 2x + 16y - 9 = 0$ przechodzi przez nieskończenie wiele punktów wymiernych.

Przy okazji rozwiążemy interesujące zadanie z LXIV OM[3]:

ZADANIE 11.18 Załóżmy, że wielomian $f(X) \in \mathbb{Z}[X]$ wyznacza funkcję różnowartościową na $\mathbb{Q}$. Czy stąd wynika, że również funkcja wyznaczona przez $f(X)$ na $\mathbb{R}$ jest różnowartościowa?

R o z w i ą z a n i e. Mówiąc inaczej: czy jeżeli $f(x) \neq f(y)$ dla wszystkich $x \neq y \in \mathbb{Q}$, to $f(x) \neq f(y)$ dla wszystkich $x \neq y \in \mathbb{R}$? Odpowiedź: n i e. Niech $f(X)$ będzie wielomianem o współczynnikach całkowitych. Wówczas (zobacz dowód T3.1)

$$f(x) - f(y) = (x - y)H(x, y),$$

gdzie H jest wielomianem dwóch zmiennych o współczynnikach całkowitych. Załóżmy, że $f(x) - f(y) \neq 0$ dla wszystkich $x \neq y \in \mathbb{Q}$. Wobec powyższej równości oznacza to, że $H(x, y) \neq 0$ dla wszystkich takich par $(x, y) \in \mathbb{Q} \times \mathbb{Q}$, że $x \neq y$. Równoważnie: równanie diofantyczne $H(x, y) = 0$ nie ma rozwiązań wymiernych poza przekątną $x = y$. Jeżeli jednocześnie równanie $H(x, y) = 0$ będzie miało choćby jedno rozwiązanie $(x, y) \in \mathbb{R}^2$ z $x \neq y$, to będziemy mieli przykład wielomianu różnowartościowego na $\mathbb{Q}$, ale nieróżnowartościowego na $\mathbb{R}$. Wystarczy więc przyjrzeć się możliwym wielomianom $H(X, Y)$. Weźmy $f(X) = X^3 + aX$. Wówczas

$$f(x) - f(y) = x^3 + ax - y^3 - ay = (x - y)(x^2 + xy + y^2 + a).$$

[3]Konkurencyjne rozwiązanie wyczytać można z ćwiczenia C11.25

Czyli $H(X, Y) = X^2+XY+Y^2+a$. Załóżmy, że para $(u/w, v/w)$ jest rozwiązaniem równania $H(x, y) = 0$ w $\mathbb{Q}^2$. Wtedy $u^2 + uv + v^2 + aw^2 = 0$, skąd

$$(2u + v)^2 + 3v^2 + 4aw^2 = 4(u^2 + uv + v^2 + aw^2) = 0. \tag{11.49}$$

Wybierzmy teraz taką liczbę całkowitą ujemną a, by $(-4a)\mathbf{N}3$ (każde $a = -2 - 3n$, przy $n \in \mathbb{Z}_+$, jest dobre! – w rozwiązaniu firmowym przyjęto $a = -2$). Wtedy równanie (11.49) nie ma rozwiązań całkowitych. Więc na elipsie $H(x, y) = 0$ nie ma punktów wymiernych. Ale jest tam oczywiście "mnóstwo" punktów rzeczywistych! ♢

11.6 Krzywe sześcienne

W tym paragrafie powiemy parę słów na temat rozwiązywania w liczbach wymiernych (lub całkowitych) równań $\varphi(x, y) = 0$, gdzie wielomian $\varphi(X, Y) \in \mathbb{Q}[X, Y]$ ma stopień 3. Ogólny wielomian trzeciego stopnia dwóch zmiennych ma postać

$$\varphi(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + iY + j, \tag{11.50}$$

gdzie $a, b, \ldots, j$ są stałymi współczynnikami (wymiernymi) i $a^2 + b^2 + c^2 + d^2 > 0$.

11.6.1 Postać normalna. Przykłady

W przykładzie P2 z poprzedniego ustępu pokazaliśmy metodę redukcji ogólnego równania drugiego stopnia $\varphi(x, y) = 0$ do postaci prostszej $Au^2 + Bv^2 + C = 0$. Uzyskuje się to przez stosowne podstawienia afiniczne postaci $x = au+bv+p$, $y = cu+dv+q$. Również w przypadku sześciennym istnieją metody redukcji równań do prostszej postaci. Odpowiednie podstawienia są w tym przypadku przekształceniami rzutowymi, zobacz $\mathbb{GEO}$.

Nie będziemy tu pokazywać ogólnych metod takich redukcji. Tytułem przykładu rozważymy równanie Fermat'a przy $n = 3$:

P r z y k ł a d 1. Spróbujmy "wyzerować wyraz v^3" w równaniu $u^3 + v^3 = 1$. Załóżmy, że para $(u, v) \in \mathbb{Q} \times \mathbb{Q}$ jest rozwiązaniem tego równania. Wtedy $u + v \neq 0$. Połóżmy

$$u = \frac{v_1}{u_1}, \quad v = \frac{1 - v_1}{u_1} \quad \Longleftrightarrow \quad u_1 = \frac{1}{u + v}, \quad v_1 = \frac{u}{u + v}. \tag{11.51}$$

Wówczas $u^3 + v^3 = 1$ wtedy i tylko wtedy, gdy

$$1 - 3v_1 + 3v_1^2 = u_1^3 \quad \Leftrightarrow \quad 3\left(v_1 - \frac{1}{2}\right)^2 = u_1^3 - \frac{1}{4} \quad \Leftrightarrow \quad \left(9v_1 - \frac{9}{2}\right)^2 = (3u_1)^3 - \frac{27}{4}.$$

Możemy dokonać kolejnego podstawienia (tym razem afinicznego):

$$u_2 = 3u_1, \quad v_2 = 9v_1 - \frac{9}{2}. \tag{11.52}$$

Otrzymamy zależność $v_2^2 = u_2^3 - \frac{27}{4}$. Aby uzyskać (równoważne) równanie o współczynnikach całkowitych mnożymy obustronnie przez $64 = 2^6$. Kładąc wtedy $x = 4u_2$, $y = 8v_2$ otrzymamy:

$$y^2 = x^3 - 432. \tag{11.53}$$

Podstawienia (11.52) i (11.51) pozwalają napisać:

$$x = \frac{12}{u+v}, \;\; y = 36\,\frac{u-v}{u+v} \quad\Longleftrightarrow\quad u = \frac{36+y}{6x}, \;\; v = \frac{36-y}{6x}. \tag{11.54}$$

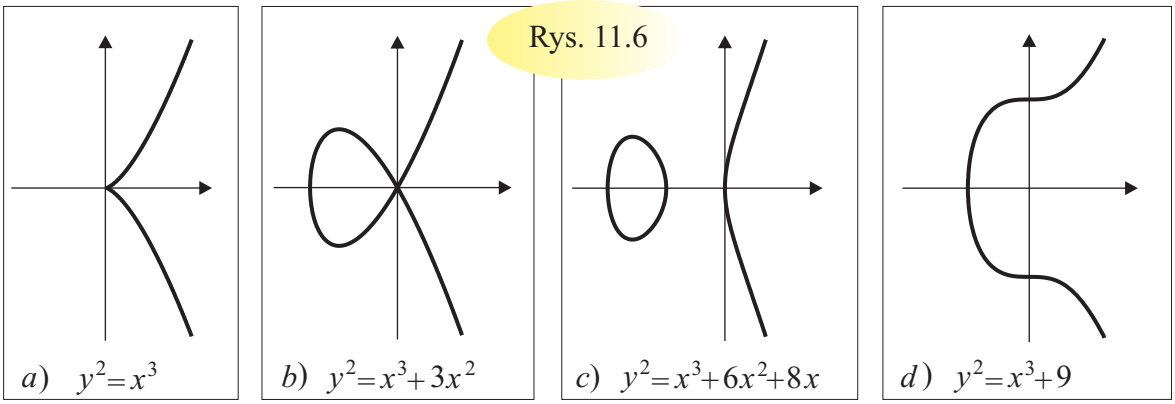
Podsumowując możemy powiedzieć: $(u,\, v)$ jest rozwiązaniem równania $u^3+v^3=1$ wtedy i tylko wtedy, gdy para $(12/(u+v),\, 36(u-v)/(u+v))$ jest rozwiązaniem równania $y^2 = x^3-432$. I odwrotnie: para $(x,\, y)$ jest rozwiązaniem równania $y^2 = x^3 - 432$ wtedy i tylko wtedy, gdy para $((36+y)/6x,\, (36-y)/6x)$ jest rozwiązaniem równania $u^3+v^3 = 1$. Co więcej, przekształcenia (11.54) mają własność **biwymierności**: $(x,\, y) \in \mathbb{Q}\times\mathbb{Q}$ wtedy i tylko wtedy, gdy $(u,\, v) \in \mathbb{Q}\times\mathbb{Q}$.

Po rozwiązaniu ćwiczenia C11.25 wiemy, że jedynymi wymiernymi rozwiązaniami równania $u^3+v^3=1$ są pary $(1,\, 0)$ i $(0,\, 1)$. Wobec tego, *jedynymi wymiernymi rozwiązaniami równania Bachet'a* (11.53) *są pary* $(12,\, 36)$ *i* $(12,\, -36)$. ◊

Postać (11.53) równania $x^3+y^3=1$ jest przykładem tak zwanej postaci normalnej. Ogólniej: mówimy, że równanie sześcienne

$$C \;:\; y^2 = ax^3+bx^2+cx+d \tag{11.55}$$

jest (binarnym) równaniem sześciennym w **postaci normalnej**. Zbiór rozwiązań takiego równania w liczbach całkowitych (odpowiednio: wymiernych, rzeczywistych czy zespolonych) będziemy, zgodnie z tradycją, oznaczać symbolem $C(\mathbb{Z})$ (odpowiednio: $C(\mathbb{Q})$, $C(\mathbb{R})$ czy $C(\mathbb{C})$). Zbiór ten nazywamy zbiorem **punktów całkowitych** (odpowiednio: **punktów wymiernych**, **punktów rzeczywistych** czy **punktów zespolonych**) krzywej C.

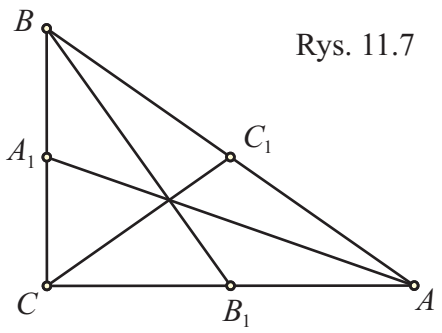


Rys. 11.6

Na rysunku 11.6 pokazujemy przykładowe kształty zbiorów punktów rzeczywistych krzywych o równaniach postaci (11.55). Krzywe wyobrażone na rysunkach 11.6*a*) i 11.6*b*) są krzywymi osobliwymi, pozostałe dwie są nieosobliwe.

Pokażemy kilka przykładów zadań teorioliczbowych lub geometryczno-teorioliczbowych, które prowadzą do równań diofantycznych postaci (11.55).

P r z y k ł a d 2. ***Pytanie Eulera***: *Czy istnieje trójkąt prostokątny o bokach i środkowych długości wymiernej?* Niech oznaczenia będą standardowe (zobacz $\mathbb{GEO}$). Jak wiemy z $\mathbb{GEO}$ WT2.26 (lub z twierdzenia Pitagorasa w $\triangle AA_1C$) zachodzi równość $4m_a^2 = a^2 + 4b^2$. Połóżmy



Rys. 11.7

$$x = \frac{a^2}{b^2}, \quad y = \frac{2acm_a}{b^3}. \tag{11.56}$$

Wówczas

$$y^2 = \left(\frac{2acm_a}{b^3}\right)^2 = \frac{a^2}{b^2} \cdot \frac{a^2+b^2}{b^2} \cdot \frac{a^2+4b^2}{b^2} = x(x+1)(x+4).$$

Widzimy stąd, że każdy trójkąt prostokątny o bokach i środkowych długości wymiernej wyznacza (za pomocą równości (11.56)) parę (x, y) liczb wymiernych będącą rozwiązaniem równania $y^2 = x^3 + 5x^2 + 4x$. Przyglądając się bliżej krzywej

$$C : y^2 = x^3 + 5x^2 + 4x \tag{11.57}$$

można udowodnić, zobacz na przykład [**4**], że zbiór $C(\mathbb{Q})$ jest zbiorem siedmioelementowym: $\{(-4, 0), (-1, 0), (0, 0), (-2, 2), (-2, -2), (2, 6), (2, -6)\}$. Jasne, że żaden z tych elementów nie odpowiada trójkątowi prostokątnemu o bokach wymiernych. Wobec tego odpowiedź na postawione pytanie Eulera jest n e g a t y w n a. ◊

P r z y k ł a d 3. ***Pytanie Fermat'a***: *Czy istnieją czterowyrazowe niestałe ciągi arytmetyczne o wyrazach będących kwadratami liczb wymiernych?* Załóżmy, że a^2, c^2, b^2, d^2 jest takim ciągiem. Wówczas, zobacz (11.48),

$$a = (-\lambda^2 + 2\lambda + 1)\mu, \quad c = (\lambda^2 + 1)\mu, \quad b = (\lambda^2 + 2\lambda - 1)\mu,$$

dla pewnych $\lambda, \mu \in \mathbb{Q}$. Oraz $d^2 = 2b^2 - c^2$. Zatem

$$(d/\mu)^2 = 2(-\lambda^2 + 2\lambda - 1)^2 - (\lambda^2 + 1)^2.$$

Oznaczmy $y_1 = d/\mu$ i (ze względów "estetycznych") $x_1 = \lambda$. Mamy więc zależność:

$$y_1^2 = x_1^4 + 8x_1^3 + 2x_1^2 - 8x_1 + 1. \tag{11.58}$$

Otrzymaliśmy więc równanie $y_1^2 = f(x_1)$, które jest "prawie postaci" (11.55). Różnica polega na tym, że nasz wielomian $f(X)$ jest stopnia 4, a chcemy mieć wielomian stopnia 3. Aby to osiągnąć postępujemy następująco: Załóżmy, że (x_1, y_1) jest rozwiązaniem równania (11.58). Oznaczmy $x_2 = y_1 - x_1^2 - 4x_1$. Wówczas x_2 jest liczbą w y m i e r n ą i zachodzi równość $y_1 = x_2 + x_1^2 + 4x_1$. Stąd i z równości (11.58) mamy

$$x_1^4 + 8x_1^3 + 2x_1^2 - 8x_1 + 1 = y_1^2 = x_2^2 + x_1^4 + 16x_1^2 + 2x_1^2x_2 + 8x_1x_2 + 8x_1^3,$$

czyli $2x_1^2 - 8x_1 + 1 = x_2^2 + 16x_1^2 + 2x_1^2x_2 + 8x_1x_2$. Widzimy więc, że liczba $x_1 \in \mathbb{Q}$ spełnia równanie o współczynnikach wymiernych:

$$2(7 + x_2)x_1^2 + 8(1 + x_2)x_1 + x_2^2 - 1 = 0. \tag{11.59}$$

Rozważamy teraz dwa przypadki: (1) $x_2 = -7$, albo (2) $x_2 \neq -7$. W pierwszym przypadku równość (11.59) daje $x_1 = 1$, czyli $\lambda = 1$, co, jak wiemy, prowadzi do s t a ł e g o ciągu arytmetycznego.

Załóżmy więc, że $x_2 \neq -7$. Wówczas x_1 jest wymiernym pierwiastkiem równania kwadratowego (11.59) o współczynnikach wymiernych i wyróżniku równym

$$\Delta = 64(1 + x_2)^2 - 8(7 + x_2)(x_2^2 - 1).$$

Wiadomo (udowodnić to!), że równanie kwadratowe o współczynnikach wymiernych ma pierwiastki wymierne wtedy i tylko wtedy, gdy jego wyróżnik jest kwadratem liczby wymiernej. Czyli wtedy i tylko wtedy, gdy równanie $y_2^2 = \Delta$ ma rozwiązania wymierne. W naszym przypadku oznacza to, że równanie

$$y_2^2 = -8x_2^3 + 8x_2^2 + 136x_2 + 120$$

ma rozwiązania wymierne. Otrzymaliśmy więc postać (11.55) równania sześciennego. Możemy jeszcze ją nieco zmodyfikować. Ponieważ prawa strona rozkłada się na czynniki

$$-8(x_2 + 1)(x_2 + 3)(x_2 - 5) = 64\left(-\tfrac{x_2}{2} - \tfrac{1}{2}\right)\left(-\tfrac{x_2}{2} - \tfrac{3}{2}\right)\left(-\tfrac{x_2}{2} + \tfrac{5}{2}\right),$$

więc, kładąc $y = \frac{y_2}{8}$ i $x = -\frac{x_2}{2} - \frac{3}{2}$, znajdujemy $y^2 = x(x + 1)(x + 4)$, czyli (11.57). $\Diamond$

Ćwiczenie 11.63 Znając wszystkie wymierne punkty (na) krzywej (11.57) (zobacz P2) udowodnić, że nie istnieją niestałe ciągi arytmetyczne o wyrazach będących kwadratami liczb wymiernych.

P r z y k ł a d 4. Pytanie: *Czy istnieją trójkąty prostokątne o bokach długości wymiernej i polu będącym liczbą całkowitą?* Załóżmy, że a, b i c są długościami przyprostokątnych i przeciwprostokątnej takiego trójkąta, a n jest jego polem. To oznacza, że trójka (a, b, c) jest elementem zbioru

$$A_n = \{(a, b, c) \in \mathbb{Q}^3 \,:\, ab = 2n,\ a^2 + b^2 = c^2\}. \tag{11.60}$$

Określimy na zbiorze A_n funkcję φ przyjmującą wartości w $\mathbb{Q} \times \mathbb{Q}$:

$$\varphi(a, b, c) = \left(\frac{-nb}{a + c},\ \frac{2n^2}{a + c}\right) =: (x, y). \tag{11.61}$$

Łatwo sprawdzić, że tak określona para (x, y) liczb wymiernych spełnia równanie

$$E_n \,:\, y^2 = x^3 - n^2x, \tag{11.62}$$

zobacz C11.64. Wobec tego każdy trójkąt prostokątny o bokach długości wymiernej i polu równym n wyznacza punkt wymierny o dodatniej rzędnej (na) krzywej E_n. $\Diamond$

Ćwiczenie 11.64 Sprawdzić, że jeżeli $(a, b, c) \in A_n$, $(x, y) = \varphi(a, b, c)$ jest parą określoną przez (11.61), to punkt (x, y) należy do $E_n(\mathbb{Q})$, czyli jest punktem wymiernym krzywej danej przez równanie (11.62).

Ćwiczenie 11.65 Niech $n \in \mathbb{N}$ i niech $T_n := E_n(\mathbb{Q}) \setminus \{(0,\,0),\,(n,\,0),\,(-n,\,0)\}$. Udowodnić, że funkcja $\psi : T_n \longrightarrow \mathbb{Q}^3$ dana wzorem

$$\psi(x,\,y) = \left(\frac{n^2 - x^2}{y},\ \frac{-2nx}{y},\ \frac{n^2 + x^2}{y}\right)$$

przyjmuje wartości w zbiorze A_n i jest funkcją odwrotną funkcji φ zadanej przez (11.61). Czyli, że $\varphi \circ \psi = \mathbf{Id}$ i $\psi \circ \varphi = \mathbf{Id}$.

Liczbę naturalną n będącą polem trójkąta prostokątnego o bokach długości wymiernej nazywa się **liczbą kongruentną**. Ćwiczenie C11.65 poucza nas, że liczba naturalna n jest liczbą kongruentną wtedy i tylko wtedy, gdy krzywa E_n ma nietrywialne (to znaczy o niezerowej rzędnej) punkty wymierne. Oczywiście $n = 6$ jest liczbą kongruentną, zobacz najprostszy trójkąt pitagorejski $(3,\,4,\,5)$.

Ćwiczenie 11.66 Rozważyć trójkąt o bokach długości $3/2$, $20/3$ i $41/6$. Uzasadnić, że $n = 5$ jest liczbą kongruentną. Jaki punkt wymierny na krzywej E_5 odpowiada wskazanemu trójkątowi?

Ćwiczenie 11.67 Punkt $(41^2/7^2,\,29520/7^3)$ leży na krzywej E_{31}. Sprawdzić. Wyznaczyć trójkąt prostokątny wymierny o polu równym 31.

Ćwiczenie 11.68 Udowodnić, że żaden kwadrat nie jest liczbą kongruentną.

W dwóch poniższych ćwiczeniach zobaczymy jeszcze dwa pytania prowadzące do badania zbioru punktów wymiernych na krzywych sześciennych:

Ćwiczenie 11.69 Chcemy odpowiedzieć na pytanie: *Czy iloczyn kolejnych dwóch liczb całkowitych może być równy iloczynowi kolejnych czterech liczb całkowitych?* Do jakiego równania postaci (11.55) prowadzi nas próba odpowiedzi na to pytanie?

Ćwiczenie 11.70 Chcemy odpowiedzieć na pytanie: *Czy trzy sześciany liczb naturalnych mogą tworzyć niestały ciąg arytmetyczny?* Do jakiego równania postaci (11.55) prowadzi nas próba odpowiedzi na to pytanie?

11.6.2 Krzywe eliptyczne

Krzywe sześcienne o równaniu (11.55) dzielą się na dwie kategorie: krzywe eliptyczne i krzywe osobliwe. Możliwe kształty krzywych osobliwych zobaczyć można na rysunkach 11.6*a* i 11.6*b*, zaś możliwe kształty krzywych eliptycznych, na rysunkach 11.6*c* i 11.6*d*.

Definicja 11.1 Krzywą C o równaniu (11.55), gdzie $a,\,b,\,c,\,d \in \mathbb{Z}$, $a \neq 0$, oraz wielomian $aX^3 + bX^2 + cX + d$ n i e ma pierwiastków wielokrotnych, nazywamy **krzywą eliptyczną**. Gdy wielomian $aX^3 + bX^2 + cX + d$ ma pierwiastek wielokrotny, krzywą (11.55) nazywamy **osobliwą**.

Problem wyznaczania punktów wymiernych na krzywej (11.55), dla której wielomian $aX^3 + bX^2 + cX + d$ ma wymierny pierwiastek wielokrotny, jest łatwo rozwiązywalny:

Ćwiczenie 11.71 Załóżmy, że wielomian trzeciego stopnia $f(X) \in \mathbb{Q}[X]$ ma wymierny pierwiastek podwójny lub potrójny. Opisać wszystkie punkty wymierne na krzywej $C : y^2 = f(x)$. *Wskazówka.* Jeżeli x_0 jest pierwiastkiem wielokrotnym wielomianu $f(X)$, to rozważmy wszystkie proste przechodzące przez punkt $(x_0, 0)$ i znajdźmy drugi punkt przecięcia takich prostych z krzywą C.

Jasne, że równanie (11.55) można zapisać w postaci $(ay)^2 = (ax)^3 + a^2bx^2 + a^2cx + a^2d$. Badanie punktów wymiernych krzywej $C : y^2 = ax^3+bx^2+cx+d$ jest więc równoważne badaniu punktów wymiernych krzywej $C_1 : y_1^2 = x_1^3 + b_1x_1^2 + c_1x_1 + d_1$. Podstawiając $x_1 = x_2 - b_1/3$, tak jak w ustępie 3.3.4, dostajemy postać zredukowaną $y_1^2 = x_2^3 + Ax_2 + B$. W dalszym ciągu będziemy więc mówić o krzywej eliptycznej

$$E \,:\, y^2 = x^3 + Ax + B. \tag{11.63}$$

Przypomnijmy, zobacz (3.50), że liczbę $\Delta = (27)^{-1}(27B^2 + 4A^3)$ nazywamy **wyróżnikiem** trójmianu sześciennego $X^3 + AX + B$.

ZADANIE 11.19 Udowodnić, że warunek $\Delta \neq 0$ jest równoważny warunkowi, że wielomian $X^3 + AX + B$ nie ma pierwiastków wielokrotnych.

R o z w i ą z a n i e. Teza wynika natychmiast z tożsamości

$$27\Delta = (X^3 + AX + B)(27B - 18AX) + (3X^2 + A)(4A^2 - 9BX + 6AX^2).$$

Tożsamość ta jest wynikiem zastosowania algorytmu Euklidesa do wielomianu $X^3 + AX + B$ i jego pochodnej $3X^2 + A$. Zobacz też C6.7. ◊

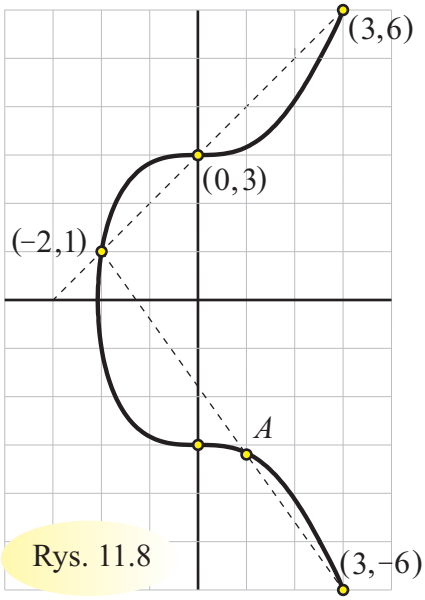
Na rysunkach 11.6*c* i 11.6*d* widzimy przybliżone kształty (zbioru punktów rzeczywistych) krzywych eliptycznych. Rysunek 11.6*c* dotyczy przypadku, gdy wielomian $f(X) = X^3+AX+B$ ma trzy różne pierwiastki rzeczywiste (to zachodzi, gdy $\Delta > 0$), rysunek 11.6*d*, przypadku, gdy $f(X)$ ma tylko jeden pierwiastek rzeczywisty (to zachodzi, gdy $\Delta < 0$).

Niestety, w przeciwieństwie do przypadku krzywych stopnia drugiego, czy (niektórych) krzywych osobliwych stopnia trzeciego, n i e d y s p o n u j e m y żadną metodą łatwej (to znaczy a l g e b r a i c z n e j) parametryzacji krzywej $E(\mathbb{R})$ (ani jej zbioru punktów wymiernych $E(\mathbb{Q})$). Ale już u Diofantosa znaleźć można zaczątki metody znajdowania nowych punktów krzywej, gdy znamy już pewne takie punkty. O tej metodzie powiemy w następnym ustępie.

11.6.3 Metoda siecznych-stycznych

Omówioną poniżej metodę wyznaczania nowych punktów krzywej $\varphi(x, y) = 0$, gdzie wielomian $\varphi(X, Y)$ jest postaci (11.50), gdy znamy już pewne jej punkty, wymyślono już w starożytności. Metodę tę nazywamy **metodą siecznych-stycznych**. Jej działanie pokażemy w zadaniach. Zobaczymy najpierw jak działa metoda siecznych.

ZADANIE 11.20 Wyznaczyć dziesięć rozwiązań równania $y^2 = x^3 + 9$ w liczbach całkowitych. Wyznaczyć jeszcze parę rozwiązań wymiernych.



Rys. 11.8

Rozwiązanie. Kilka rozwiązań łatwo odgadnąć. Na przykład $(0, \pm 3)$, $(3, \pm 6)$. Mając te cztery punkty na krzywej o równaniu $x^3 - y^2 + 9 = 0$ możemy spróbować znaleźć inne punkty na tej krzywej. Wybieramy punkty $(0, 3)$ i $(3, 6)$ i prowadzimy przez nie prostą. Prosta przechodząca przez te punkty ma równanie $y = x + 3$, jej trzeci punkt przecięcia z krzywą ma odciętą będącą trzecim (obok $x = 0$ i $x = 3$) pierwiastkiem równania $(x + 3)^2 = x^3 + 9$. Czyli trzecim pierwiastkiem równania

$$x^3 - x^2 - 6x = 0.$$

Na mocy wzoru Viète'a mamy więc $0 + 3 + x = 1$, skąd $x = -2$. Zatem $y = -2 + 3 = 1$. Znaleźliśmy więc nowe dwa punkty całkowite $(-2, 1)$, i $(-2, -1)$ na naszej krzywej. Drugi punkt otrzymujemy dzięki symetrii krzywej względem osi Ox.

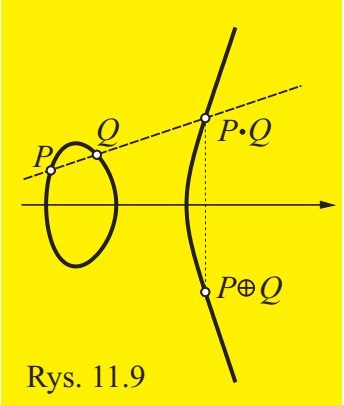
Zróbmy taką sztuczkę jeszcze raz, tym razem startując od punktów $(0, -3)$ i $(3, 6)$. Prosta przechodząca przez te punkty ma równanie $y = 3x - 3$, jej trzeci punkt przecięcia z krzywą ma odciętą będącą trzecim (obok $x = 0$ i $x = 3$) pierwiastkiem równania $(3x - 3)^2 = x^3 + 9$. Czyli trzecim pierwiastkiem równania $x^3 - 9x^2 + 18x = 0$. Na mocy wzoru Viète'a mamy więc $0 + 3 + x = 9$, skąd $x = 6$. Zatem $y = 3 \cdot 6 - 3 = 15$. W ten sposób znajdujemy kolejne dwa punkty całkowite na badanej krzywej: $(6, 15)$ i $(6, -15)$. Stosując sztuczkę do punktów $(3, -6)$ i $(6, 15)$ znajdujemy "niebanalne" rozwiązania

$$(40, 253), \quad (40, -253).$$

Dotychczas mieliśmy szczęście: znajdowaliśmy rozwiązania całkowite. Tak jednak zdarza się raczej wyjątkowo. Zastosujmy naszą sztuczkę do punktów $P = (-2, 1)$ i $Q = (3, -6)$. Prosta l_{PQ} ma równanie $y = -\frac{7}{5}x - \frac{9}{5}$. Stąd, podobnie jak wyżej, znajdujemy trzeci punkt przecięcia tej prostej z krzywą $E(\mathbb{R})$: $A = (\frac{24}{25}, -\frac{393}{125})$. Tym razem wyznaczyliśmy wymierny punkt naszej krzywej. Czytelnik zechce samodzielnie zastosować sztuczkę startując od punktów $(6, 15)$ i $(40, 253)$. ◊

Na rysunku 11.9 pokazujemy metodę siecznych. [Znaczenie punktu $P \oplus Q$ będzie wyjaśnione później.] Jeżeli punkty P, Q leżą na krzywej, to trzeci punkt przecięcia prostej l_{PQ} z tą krzywą oznaczamy $P \cdot Q$. Zastosowaną w powyższym rozwiązaniu **metodę siecznych** opisujemy tak:

prowadzimy prostą przez dwa dane punkty na badanej krzywej i wyznaczamy trzeci punkt przecięcia tej prostej z krzywą.



Rys. 11.9

Ćwiczenie 11.72 Udowodnić, że jeżeli punkty wymierne P, Q leżą na krzywej o równaniu $\varphi(x, y) = 0$, gdzie $\varphi(X, Y)$ jest postaci (11.50), to punkt $P \cdot Q$ (jeżeli istnieje) jest punktem wymiernym.

Gdy dysponujemy tylko jednym punktem na krzywej i nie możemy zastosować metody siecznych, nie traćmy nadziei. Gdy dwa punkty, przez które prowadzimy sieczną, pokrywają się, słusznym jest uważać, że odpowiednia prosta sieczna staje się prostą s t y c z n ą. Z rachunku różniczkowego wiemy, że równanie prostej stycznej do krzywej o równaniu $\varphi(x, y) = 0$ w punkcie (x_0, y_0) leżącym na tej krzywej ma postać:

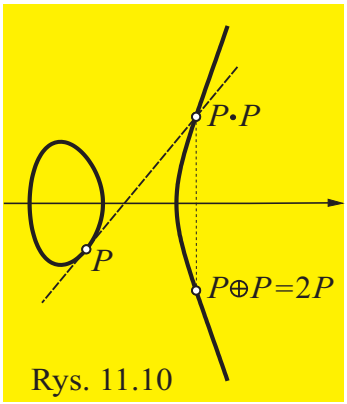
$$\varphi'_x(x_0, y_0) \cdot (x - x_0) + \varphi'_y(x_0, y_0) \cdot (y - y_0) = 0, \tag{11.64}$$

gdzie $\varphi'_x(x_0, y_0)$ oznacza wartość pochodnej (cząstkowej) wielomianu φ jako wielomianu zmiennej x (przy ustalonym $y = y_0$) w punkcie x_0. Oczywiście $\varphi'_y(x_0, y_0)$ oznacza wartość pochodnej (cząstkowej) wielomianu φ jako wielomianu zmiennej y (przy ustalonym $x = x_0$) w punkcie y_0. Należy podkreślić, że równanie (11.64) jest równaniem prostej wtedy i tylko wtedy, gdy co najmniej jedna z liczb φ'_x, φ'_y jest r ó ż n a od 0. Punkt $P = (x_0, y_0)$, w którym obie pochodne $\varphi'_x(x_0, y_0)$, $\varphi'_y(x_0, y_0)$ są równe 0 nazywa się **punktem osobliwym** krzywej $\varphi(x, y) = 0$. Punkt $(0, 0)$ jest punktem osobliwym zarówno krzywej z rysunku 11.6*a* jak i krzywej z rysunku 11.6*b*.

Ćwiczenie 11.73 Udowodnić, że krzywa o równaniu (11.55) m a punkty osobliwe wtedy i tylko wtedy, gdy wielomian $aX^3 + bX^2 + cX + d$ ma pierwiastki wielokrotne.

Na rysunku 11.10 pokazujemy metodę stycznych. Jeżeli P jest punktem krzywej, to "trzeci" punkt przecięcia prostej stycznej l_P z tą krzywą oznaczamy $P \cdot P$. **Metodę stycznych** opisujemy tak:

prowadzimy prostą styczną w danym punkcie badanej krzywej i wyznaczamy "trzeci" punkt przecięcia tej prostej z krzywą.



Rys. 11.10

Ćwiczenie 11.74 Wykaż, że jeśli P jest punktem wymiernym krzywej o równaniu $\varphi(x, y) = 0$, gdzie φ jest postaci (11.50), to punkt $P \cdot P$, jeśli istnieje, jest punktem wymiernym.

ZADANIE 11.21 Wiemy z Z10.8, że równanie $y^2 = x^3 - 2$ ma tylko dwa rozwiązania w liczbach całkowitych: $(3, \pm 5)$. Wyznaczyć kilka innych punktów wymiernych (na) krzywej eliptycznej Bachet'a $B_{(-2)} : y^2 = x^3 - 2$.

R o z w i ą z a n i e. Mamy znaleźć różne od $(3, \pm 5)$ punkty zbioru $B_{(-2)}(\mathbb{Q})$. Rozważmy prostą styczną do naszej krzywej w punkcie $P = (3, 5)$. Z (11.64) wiemy, że ma ona równanie

$$27(x - 3) - 10(y - 5) = 0. \tag{11.65}$$

Jej punkty przecięcia z naszą krzywą mają więc odcięte będące pierwiastkami równania

$$x^3 - \frac{729}{100}x^2 + \frac{837}{50}x - \frac{1161}{100} = 0. \tag{11.66}$$

Ponieważ punkt $(3,\,5)$ jest podwójnym punktem przecięcia prostej (11.65) z badaną krzywą, więc równanie (11.66) ma (co zresztą łatwo(?) sprawdzić bezpośrednio) pierwiastek podwójny $x_1 = x_2 = 3$. Trzeci pierwiastek (czyli odciętą poszukiwanego trzeciego punktu przecięcia) znajdujemy za pomocą jednego z dwóch wzorów Viète'a:

$$x_1 + x_2 + x_3 = \frac{729}{100} \quad \text{lub} \quad x_1x_2x_3 = \frac{1161}{100}.$$

Dostajemy $x_3 = \frac{129}{100}$. Rzędną y_3 wyznaczamy z równania stycznej (11.65): $y_3 = \frac{383}{1000}$. Znaleźliśmy więc nowy punkt wymierny $Q = (\frac{129}{100},\, \frac{383}{1000})$ na badanej krzywej. Powyższą sztuczkę możemy teraz zastosować do punktu Q. $\Diamond$

Ćwiczenie 11.75 Zrobić to.

Ćwiczenie 11.76 Zastosować metodę stycznych do znanych punktów wymiernych na krzywej Bachet'a $B_{(-432)}$: $y^2 = x^3 - 432$, zobacz 11.6.1 P1.

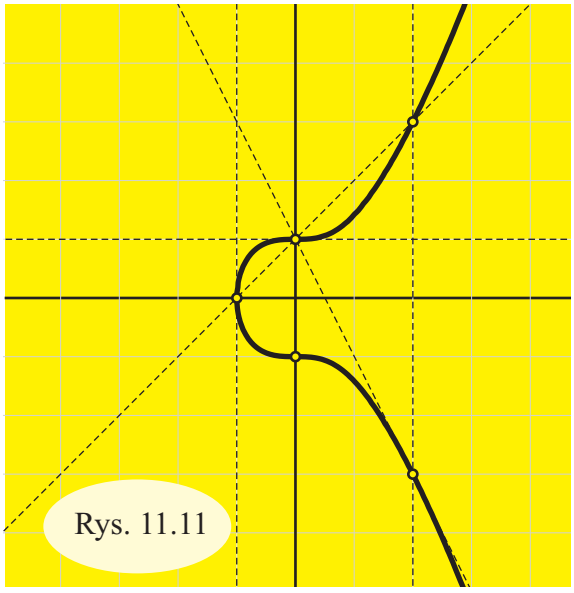
Ćwiczenie 11.77 Wyznaczyć rozwiązanie $(49,\,840)$ równania $y^2 = 6x^3 - 6x$ znając oczywiste rozwiązania $(\pm1,\,0)$, $(0,\,0)$ i $(2,\,\pm6)$.

11.6.4 Równania $y^2 = x^3 + 1$ i $y^2 = x^3 - 1$

Rozważymy teraz kolejne równanie Bachet'a:

$$B_{(1)}:\ y^2 = x^3 + 1. \tag{11.67}$$

Na rysunku 11.11 mamy krzywą o równaniu (11.67) i pięć oczywistych punktów całkowitych. Są to $(-1,\,0)$, $(0,\,\pm1)$ i $(2,\,\pm3)$. Również rozwiązanie poniższego ćwiczenia łatwo dostrzec na tym rysunku:


Rys. 11.11

Ćwiczenie 11.78 Zastosować metodę siecznych-stycznych do równania $y^2 = x^3 + 1$. Czy dostajemy w ten sposób jakieś nowe rozwiązania w liczbach wymiernych?

Ustęp ten poświęcimy na wyjaśnienie braku sukcesu w powyższym ćwiczeniu. Dowiedziemy mianowicie (za pomocą nieco zmodyfikowanego rozumowania Eulera), że na krzywej (11.67) nie ma więcej punktów wymiernych.

W trakcie dowodu twierdzenia T11.8 będziemy korzystać z najprostszych własności pierścienia Eisensteina. W szczególności z tezy poniższego lematu:

LEMAT 11.4 *Jeżeli $\alpha \in \mathbb{Z}[\omega]$ jest takim elementem pierścienia Eisensteina, że $\mathbf{N}(\alpha)$ jest kwadratem (w $\mathbb{Z}$), to $\alpha = k\beta^2$ dla pewnego $k \in \mathbb{Z}$ i pewnego $\beta \in \mathbb{Z}[\omega]$.*

D O W Ó D. Teza wynika łatwo z jednoznaczności rozkładu w $\mathbb{Z}[\omega]$ i faktu, że każda jedność w $\mathbb{Z}[\omega]$ jest kwadratem lub *minus* kwadratem. Istotnie, każda jedność jest potęgą parzystą $\tau^{2k} = (\tau^k)^2$ lub potęgą nieparzystą $\tau^{2k+1} = \tau^3\tau^{2k-2} = -(\tau^{k-1})^2$. [Używamy tu oznaczeń z ustępu 10.2.8.] Niech

$$\alpha = \varepsilon \cdot q_1 q_2 \cdot \ldots \cdot q_r \cdot \lambda^d \cdot \pi_1^{e_1}\pi_2^{e_2} \cdot \ldots \cdot \pi_s^{e_s}$$

będzie rozkładem α na czynniki nierozkładalne w $\mathbb{Z}[\omega]$. Tu ε jest jednością, q_i oznaczają liczby pierwsze $\equiv 2 \pmod 3$, a π_j oznaczają elementy pierwsze leżące nad liczbami pierwszymi $p_j \equiv 1 \pmod 3$. Wówczas $\mathbf{N}(\alpha) = q_1^2 q_2^2 \cdot \ldots \cdot q_r^2 \cdot 3^d \cdot p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$. Ponieważ $\mathbf{N}(\alpha)$ jest kwadratem, więc widzimy, że wykładniki d i $e_1, e_2, \ldots, e_s$ są parzyste. Wystarczy więc położyć $\beta = \eta \cdot 3^{d/2}\pi_1^{e_1/2}\pi_2^{e_2/2} \cdot \ldots \cdot \pi_s^{e_s/2}$, gdzie $\eta^2 = \pm\varepsilon$ i $k = \pm q_1 q_2 \cdot \ldots \cdot q_r$. □

TWIERDZENIE 11.8 *Równanie* (11.67) *ma dokładnie pięć rozwiązań w liczbach wymiernych. Są to* $(-1, 0)$, $(0, \pm 1)$, $(2, \pm 3)$.

D O W Ó D. Załóżmy, że $\frac{m}{n}$, $m, n \in \mathbb{Z}$, jest takim ułamkiem, że para (x, y), $x = \frac{m}{n}$ jest wymiernym rozwiązaniem równania (11.67) przy pewnym $y \in \mathbb{Q}$. Wówczas, po pomnożeniu przez n^4, dostajemy

$$(n^2 y)^2 = n(m+n)[m^2 - mn + n^2]. \tag{11.68}$$

Oznaczmy przez $E(m, n)$ prawą stronę powyższej równości. Równość (11.68) będziemy zapisywać w postaci $E(m, n) = \square$, zaznaczając w ten sposób, że wartość *formy Eulera* $E(m, n)$ jest kwadratem (liczby całkowitej). Jasne, że $E(-m, -n) = E(m, n)$. Zatem każda para $(m, n) \in \mathbb{Z} \times \mathbb{Z}_{\neq 0}$, dla której $E(m, n) = \square = d^2$ wyznacza rozwiązania $\left(\frac{m}{n}, \pm\frac{d}{n^2}\right)$ równania (11.67). Zauważmy, że rozwiązania $(-1, 0)$, $(0, \pm 1)$, $(2, \pm 3)$ pochodzą od par (m, n) należących do zbioru

$$\Omega_0 = \{(1, -1), (-1, 1), (0, 1), (0, -1), (2, 1), (-2, -1)\}.$$

Odpowiednie wartości formy Eulera to $E(\pm 1, \mp 1) = 0$, $E(0, \pm 1) = 1$, $E(\pm 2, \pm 1) = 9$. Oznaczmy

$$\Omega_\square = \{(m, n) \in \mathbb{Z} \times \mathbb{Z}_{\neq 0} : \mathrm{NWD}\,(m, n) = 1 \text{ oraz } E(m, n) = \square\}.$$

Wiemy, że $\Omega_0 \subseteq \Omega_\square$. Udowodnimy, za pomocą d e s a n t u wymyślonego przez Eulera, że w istocie *zachodzi równość* $\Omega_0 = \Omega_\square$. To zakończy dowód twierdzenia.

Załóżmy nie wprost, że istnieje $(m, n) \in \Omega_\square \setminus \Omega_0$. Desant Eulera polega na wskazaniu pary $(m_1, n_1) \in \Omega_\square \setminus \Omega_0$, dla której $E(m_1, n_1) < E(m, n)$. Czytelnik oczywiście widzi, że to prowadzi do sprzeczności. Konstrukcję pary (m_1, n_1) przeprowadzamy różnie dla dwóch przypadków: (1) $m + n \equiv 0 \pmod 3$ i (2) $m + n \not\equiv 0 \pmod 3$.

W przypadku (1) połóżmy $3n_1 = m + n$ i $m_1 = n - n_1$. Wówczas, jak łatwo sprawdzić,

$$E(m, n) = 9\,E(m_1, n_1).$$

Jasne, że stąd wynika: $E(m_1, n_1) = \square$, $\mathrm{NWD}\,(m_1, n_1) = 1$ i $E(m_1, n_1) < E(m, n)$.

W przypadku (2) konstrukcja pary (m_1, n_1) jest trudniejsza. Zaczynamy od uwagi, że czynniki n, $m+n$ i m^2-mn+n^2 formy Eulera są w tym przypadku parami względnie pierwsze, zobacz C11.79, i dodatnie, więc, na mocy *triku*, każdy z nich jest kwadratem:

$$n=a^2, \quad m+n=b^2, \quad m^2-mn+n^2=c^2. \tag{11.69}$$

Ostatnia z tych równości mówi, że norma $\mathbf{N}(m+n\omega)$ jest kwadratem (liczby całkowitej). Wobec tego, na mocy L11.4 możemy zapisać równość $m+n\omega=k(s+t\omega)^2$. Stąd

$$m=k(s^2-t^2), \quad n=k(2st-t^2).$$

Ponieważ $\mathrm{NWD}\,(m,\,n)=1$, więc $k=\pm 1$. Jednocześnie

$$1\equiv b^2=m+n=k[(s+t)^2-3t^2]\equiv k(s+t)^2\equiv k\,(\mathrm{mod}\,3).$$

Zatem $k=1$, więc

$$m=s^2-t^2, \quad n=2st-t^2. \tag{11.70}$$

Uzyskaną równość $b^2=(s+t)^2-3t^2$ zapisujemy w postaci

$$(s+t)^2=b^2+3t^2=\mathbf{N}(b+t\sqrt{-3}).$$

Ponadto, skoro norma liczby $b+t\sqrt{-3}\in\mathbb{Z}[\,\omega\,]$ jest kwadratem, więc, znów na mocy L11.4, $b+t\sqrt{-3}=l\beta^2$ dla pewnych $l\in\mathbb{Z}$ i $\beta=\frac{1}{2}(u+v\sqrt{-3})\in\mathbb{Z}[\,\omega\,]$. Stąd

$$b=l\left(\frac{u^2-3v^2}{4}\right), \quad t=l\cdot\frac{uv}{2}. \tag{11.71}$$

Zatem

$$(s+t)^2=b^2+3t^2=l^2\left(\frac{u^2-3v^2}{4}\right)^2+3l^2\left(\frac{uv}{2}\right)^2=l^2\left(\frac{u^2+3v^2}{4}\right)^2.$$

Wobec tego

$$\text{(a)}\quad s+t=l\left(\frac{u^2+3v^2}{4}\right)\quad\text{lub}\quad\text{(b)}\quad s+t=(-l)\left(\frac{u^2+3v^2}{4}\right). \tag{11.72}$$

W przypadku (a) mamy

$$\begin{aligned}E(u-v,\,v)=&v(u-v+v)[(u-v)^2-(u-v)v+v^2]=uv[u^2+3v^2-3uv]\\=&\frac{2t}{l}\left[\frac{4(s+t)}{l}-\frac{6t}{l}\right]=\frac{2t}{l^2}(4s-2t)=\frac{4t}{l^2}\cdot\frac{n}{t}=\left(\frac{2a}{l}\right)^2,\end{aligned}$$

gdzie trzecia równość wynika z drugiej równości (11.71) i pierwszej równości (11.72), piąta równość wynika z drugiej równości (11.70), a ostatnia równość wynika z pierwszej równości (11.69). W przypadku (11.72)(b) mamy, jak łatwo sprawdzić,

$$E(u+v,\,-v)=\left(\frac{2a}{l}\right)^2.$$

Oznaczmy $d = \mathrm{NWD}\,(u, v)$. Wówczas, kładąc $m_1 = (u - v)/d$, $n_1 = v/d$ w przypadku (11.72)(a), i $m_1 = (u + v)/d$, $n_1 = (-v)/d$ w przypadku (11.72)(b), dostajemy równość

$$E(m_1, n_1) = \left(\frac{2a}{d^2 l}\right)^2 = \square.$$

Trzeba jeszcze sprawdzić, że $E(m_1, n_1) < E(m, n) = a^2b^2c^2$. Zostawiamy to Czytelnikowi. $\square$

Ćwiczenie 11.79 Udowodnić, że jeżeli $\mathrm{NWD}\,(m, n) = 1$ i $m+n \not\equiv 0 \,(\mathrm{mod}\, 3)$, to czynniki iloczynu (11.68) są parami względnie pierwsze.

Ćwiczenie 11.80 Rozważyć formę $E'(m, n) := E(m, -n)$ i udowodnić, że na krzywej $B_{(-1)} : y^2 = x^3 - 1$ leży tylko jeden punkt wymierny $(1, 0)$.

11.6.5 Dodawanie punktów krzywej eliptycznej

Okazuje się, że w zbiorze $E(\mathbb{C})$ punktów zespolonych krzywej eliptycznej, uzupełnionym o jeden d o d a t k o w y punkt, można wprowadzić działanie **dodawania** $\oplus$, względem którego zbiór ten staje się g r u p ą a b e l o w ą. Dodawanie $\oplus$ definiujemy za pomocą opisanej w ustępie 11.6.3 metody siecznych-stycznych. Również podzbiory $E(\mathbb{R})$ i $E(\mathbb{Q})$ punktów rzeczywistych i wymiernych są grupami względem działania $\oplus$.

Opiszemy teraz rzeczone działanie dodawania punktów. Będziemy to robić w zbiorze $E(\mathbb{R})$ punktów rzeczywistych krzywej E zadanej przez równanie (11.63). (Robimy tak dla wygody Czytelnika, którego nie chcemy przerażać **zespoloną płaszczyzną rzutową**. Formalnie rzecz ujmując wszystko jest również prawdą dla punktów zespolonych.)

Wprowadzimy parę oznaczeń.

1. Odciętą punktu P oznaczamy przez $x(P)$, a rzędną przez $y(P)$;

2. Dla danego punktu $P \in \mathbb{R}^2$ przez P' oznaczymy punkt, którego współrzędnymi są

$$x(P') = x(P), \quad y(P') = -y(P)$$

(P' jest więc odbiciem punktu P w osi Ox);

3. Dla danych dwóch punktów $P, Q \in E(\mathbb{R})$ symbolem $P \cdot Q$ oznaczamy trzeci punkt przecięcia prostej l_{PQ} z krzywą $E(\mathbb{R})$;

4. Przez O oznaczymy **punkt idealny**, w którym przecinają się wszystkie proste pionowe $x = s$. Znający podstawy geometrii płaszczyzny rzutowej wiedzą, że O jest kierunkiem osi Oy. Ponieważ nasza krzywa jest coraz bardziej "pionowa", więc naturalnym jest uważać, że przechodzi ona przez punkt O. Uznajemy, że punkt O jest punktem całkowitym, w szczególności, wymiernym. Ponadto kładziemy

$$O' = O;$$

5. Definiujemy **sumę** $P \oplus Q$ punktów $P, Q \in E(\mathbb{R})$ wzorem (zobacz rysunki 11.9 i 11.10)

$$\boxed{P \oplus Q = (P \cdot Q)'.}$$

Jasne, że jeżeli $P \in E(\mathbb{R})$, to $P' \in E(\mathbb{R})$. Jasnym też być powinno, że $O \cdot P = P'$.

Ćwiczenie 11.81 Przekonać się, że punkt O jest elementem neutralnym dodawania $\oplus$. Nazywamy go więc **zerem**. Przekonać się również, że dla dowolnego punktu P zachodzi równość $P \oplus P' = O$. Zatem, P' jest elementem przeciwnym do P.

Regułę tworzenia sumy punktów na krzywej (11.63) można streścić następująco:

***suma trzech punktów, w których prosta przecina krzywą wynosi* 0.**

Wyprowadzimy teraz wzory na odciętą $x(P_1 \oplus P_2)$ i rzędną $y(P_1 \oplus P_2)$ sumy dwóch punktów na krzywej eliptycznej. Możliwe są cztery przypadki położenia punktów P_1, P_2:

1. Jeżeli $P_1 \neq P_2 \in E(\mathbb{R})$ są dwoma punktami mającymi tę samą odciętą, to, oczywiście, uważamy, że $P_1 \cdot P_2 = O$. Wobec tego, w tym przypadku mamy

$$P_1 \oplus P_2 = O' = O.$$

2. Niech $P_1 = (k_1, l_1)$, $P_2 = (k_2, l_2) \in E(\mathbb{R})$, $x(P_1) \neq x(P_2)$, będą punktami krzywej (11.63). Poprowadźmy przez te punkty prostą $l_{P_1P_2}$. Jej równanie, jak wiadomo, ma postać

$$y = \lambda(x - k_1) + l_1, \quad \text{gdzie} \quad \lambda = \frac{l_2 - l_1}{k_2 - k_1}.$$

Oznaczmy przez (k_3, l_3) trzeci punkt przecięcia tej prostej z krzywą $E(\mathbb{R})$. Aby wyznaczyć k_3 znajdujemy trzeci, obok k_1 i k_2 pierwiastek równania

$$x^3 - (\lambda x + l_1 - \lambda k_1)^2 + Ax + B = 0.$$

Dzięki wzorowi Viète'a mamy $k_1 + k_2 + k_3 = \lambda^2$. Wobec tego

$$\begin{cases} x(P_1 \oplus P_2) = \lambda^2 - x(P_1) - x(P_2), \\ y(P_1 \oplus P_2) = \lambda\,(x(P_1) - x(P_1 \oplus P_2)) - y(P_1). \end{cases} \tag{11.73}$$

Jasne, że $y(P_1 \oplus P_2) = -l_3$ wyznaczamy z równości $l_3 = \lambda(k_3 - k_1) + l_1$. Zauważmy, że może się zdarzyć, że $P_1 \cdot P_2 = P_2$ (lub $P_1 \cdot P_2 = P_1$). W takiej sytuacji prosta $l_{P_1P_2}$ jest styczna do krzywej w punkcie P_2 (lub P_1).

3. Niech teraz $P_1 = P_2 = P = (k, l)$ i $y(P) \neq 0$. Ponieważ jest intuicyjnie jasne, że prosta sieczna l_{PQ}, dla ustalonego punktu $P \in E(\mathbb{R})$ i zmiennego, zbieżnego do P, punktu $Q \in E(\mathbb{R})$, jest zbieżna do prostej l_P stycznej do krzywej E w punkcie P, więc wyznaczymy trzeci punkt przecięcia stycznej l_P z krzywą. Znający pochodne z łatwością sprawdzą, że prosta l_P ma równanie

$$y = \lambda(x - k) + l, \quad \text{gdzie} \quad \lambda = \frac{3k^2 + A}{2l}.$$

Wobec tego, podobnie jak wyżej (korzystając ze wzoru Viète'a), znajdujemy

$$\begin{cases} x(P \oplus P) = \lambda^2 - 2x(P) \\ y(P \oplus P) = \lambda(x(P) - x(P \oplus P)) - y(P). \end{cases} \tag{11.74}$$

4. Gdy $P_1 = P_2 = P$ i $y(P) = 0$, to kładziemy

$$P_1 \oplus P_2 = O,$$

bo prosta styczna jest "pionowa".

Formuły (11.73) pochodzą w zasadzie od Diofantosa (w zupełnie innej notacji, oczywiście), a Bachet de Méziriac wykrył ***formuły duplikacji*** (11.74) na długo przed powstaniem teorii krzywych eliptycznych.

Interpretacja tych wzorów w ramach teorii grup jest zasługą Poincaré'*go*, który zdefiniował dodawanie punktów na krzywej eliptycznej i udowodnił poniższe ważne:

TWIERDZENIE 11.9 (***Twierdzenie Poincaré'go***) *Zbiór* $E(\mathbb{R}) \cup \{O\}$ *z działaniem* $\oplus$ *jest grupą abelową. Jeżeli* A, B *w równaniu* (11.63) *są liczbami wymiernymi, to* $E(\mathbb{Q}) \cup \{O\}$ *z działaniem* $\oplus$ *jest grupą abelową (podgrupą grupy* $(E(\mathbb{R}) \cup \{O\}, \oplus)$*).* □

Jedynie trudnym momentem w dowodzie tego twierdzenia jest dowód, że wprowadzone działanie dodawania punktów jest d z i a ł a n i e m ł ą c z n y m.

U w a g a. Zauważmy na koniec, że jeżeli A, B w równaniu (11.63) są liczbami całkowitymi i dane jest dowolne ciało $\mathbb{K}$, to można rozważać zbiór $\mathbb{K}$-**punktów** krzywej E (czyli zbiór takich rozwiązań (x, y) równania (11.63), że $x, y \in \mathbb{K}$). Jasne, że zbiór $\mathbb{K}$-punktów krzywej E oznaczamy symbolem $E(\mathbb{K})$.

Możemy, w szczególności, za $\mathbb{K}$ wybrać któreś ze znanych nam ciał skończonych. Na przykład, gdy $\mathbb{K} = \mathbb{Z}/p$ dla danej liczby pierwszej $p \neq 2, 3$, to wzory (11.73) i (11.74) definiujące działanie dodawania $\oplus$ zachowują swoją moc. W ten sposób powstaje grupa $E(\mathbb{Z}/p) \cup \{O\}$. Grupy $E(\mathbb{Z}/p) \cup \{O\}$ i, ogólniej, $E(\mathbb{F}_{p^n}) \cup \{O\}$, mają zastosowanie w kryptografii, zobacz na przykład [**3**] i [**18**].

Ćwiczenie 11.82 Napisać tabelkę grupy $(E(\mathbb{Z}/7) \cup \{O\}, \oplus)$ dla krzywej

$$E : y^2 = x^3 + 5x + 4.$$

Rozdział 12

Kilka wiadomości dodatkowych

M^r Jacq. Bernoulli [...] *avouë, que malgré toutes les peines,*
qu'il s'etoit données, il n'avoit pû venir à bout, de sorte que [...]
grands Maîtres dans cette matière, ont été extrêmement surpris,
quand je leur annonçois que j'avois trouvé la somme de cette serie [...]
(Leonhard Euler)

Opowiemy tu o paru jeszcze, występujących w matematyce olimpijskiej, tematach, więcej lub mniej związanych z teorią liczb.

12.1 Część całkowita i ułamkowa liczby rzeczywistej

Pokażemy tu parę zadań dotyczącej części całkowitej i części ułamkowej liczb rzeczywistych.

12.1.1 Podstawowe własności

Każdą liczbę rzeczywistą x przedstawiamy jednoznacznie w postaci sumy pewnej liczby całkowitej i pewnej nieujemnej liczby rzeczywistej mniejszej niż 1. Mówimy odpowiednio o części całkowitej i części ułamkowej liczby x.

Definicja 12.1 **Część całkowita** liczby $x \in \mathbb{R}$ to jedyna taka liczba całkowita $\lfloor x \rfloor$, że

$$\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1.$$

Część całkowitą liczby x nazywa się (ostatnio) również **podłogą liczby** x. **Częścią ułamkową** liczby x nazywamy "naddatek" $x - \lfloor x \rfloor$. Oznaczamy ją $\{x\}$.

Jasne jest, że dla dowolnej liczby rzeczywistej x, przedstawienie jej w postaci

$$x = n + \alpha,$$

gdzie $n \in \mathbb{Z}$ oraz $\alpha \in [\,0;\,1\,)$, jest jednoznaczne. Tu, oczywiście, $n = \lfloor x \rfloor$, $\alpha = \{x\}$.

Elementarne własności tych pojęć zebrane są w poniższym ćwiczeniu:

Ćwiczenie 12.1 Udowodnić, że dla dowolnych liczb rzeczywistych x, x_1, x_2, …, x_m:

1. $x - 1 < \lfloor x \rfloor \leqslant x$,

2. $x \in \mathbb{Z} \iff x = \lfloor x \rfloor \iff \{x\} = 0$,

3. dla $x > 0$, do przedziału $[\,1;\, x\,]$ należy dokładnie $\left\lfloor \frac{x}{m} \right\rfloor$ wielokrotności liczby $m \in \mathbb{N}$,

4. $\lfloor n + x \rfloor = n + \lfloor x \rfloor$ dla dowolnego $n \in \mathbb{Z}$,

5. $\lfloor x_1 + x_2 + \ldots + x_m \rfloor - \lfloor x_1 \rfloor - \lfloor x_2 \rfloor - \ldots - \lfloor x_m \rfloor \in \{0, 1, \ldots, m-1\}$,

6. $\left\lfloor \dfrac{\lfloor x \rfloor}{b} \right\rfloor = \left\lfloor \dfrac{x}{b} \right\rfloor$ dla $b \in \mathbb{N}$.

Oto jeszcze kilka ćwiczeń z częścią całkowitą liczb rzeczywistych:

Ćwiczenie 12.2 Udowodnić, że dla dowolnej liczby rzeczywistej x i dowolnej liczby naturalnej n zachodzi ***tożsamość Hermite'a***

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \ldots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor .$$

Ćwiczenie 12.3 Udowodnić, że dla każdej liczby naturalnej n zachodzi równość

$$\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{8} \right\rfloor + \ldots + \left\lfloor \frac{n+2^k}{2^{k+1}} \right\rfloor + \ldots = n.$$

Ćwiczenie 12.4 Udowodnić, że dla dowolnej liczby naturalnej n zachodzi równość

$$\lfloor \sqrt{n+1} + \sqrt{n} \rfloor = \lfloor \sqrt{4n+2} \rfloor.$$

Ćwiczenie 12.5 Udowodnić, że dla dowolnej liczby naturalnej n liczba

$$\lfloor (5 + \sqrt{19})^n \rfloor$$

jest nieparzysta. *Wskazówka.* $(5 - \sqrt{19})^n < 1$ dla każdego $n > 1$.

Ćwiczenie 12.6 Udowodnić, że dla dowolnej liczby naturalnej n zachodzi równość

$$\left\lfloor \sqrt{n} \right\rfloor + \left\lfloor \sqrt[3]{n} \right\rfloor + \left\lfloor \sqrt[4]{n} \right\rfloor + \ldots + \left\lfloor \sqrt[n]{n} \right\rfloor = \lfloor \log_2 n \rfloor + \lfloor \log_3 n \rfloor + \lfloor \log_4 n \rfloor + \ldots + \lfloor \log_n n \rfloor .$$

Ćwiczenie 12.7 Udowodnić, że równanie

$$\lfloor x \rfloor + \lfloor 2x \rfloor + \lfloor 4x \rfloor + \lfloor 8x \rfloor + \lfloor 16x \rfloor + \lfloor 32x \rfloor = m,$$

przy $m = 2010$ ma nieskończenie wiele rozwiązań, a przy $m = 2011$ nie ma rozwiązań w liczbach rzeczywistych x.

Ćwiczenie 12.8 Udowodnić, że dla dowolnych względnie pierwszych liczb naturalnych a, b zachodzi równość

$$\sum_{k=1}^{a-1} \left\lfloor \frac{kb}{a} \right\rfloor = \frac{(a-1)(b-1)}{2}.$$

12.1.2 Twierdzenie Beatty'*ego*

Interesującą własność części całkowitej znajdujemy w twierdzeniu Beatty'*ego*-Banga.

Dla danej liczby rzeczywistej γ połóżmy

$$S_\gamma = \{\lfloor n\gamma \rfloor : n \in \mathbb{N}\}.$$

Zbiór S_γ nazywa się czasami **spektrum** liczby rzeczywistej γ.

Przy tym oznaczeniu mamy:

TWIERDZENIE 12.1 (***Beatty, Bang***) *Niech α i β będą dwiema ściśle dodatnimi liczbami rzeczywistymi. Wówczas zbiory S_α, S_β stanowią rozbicie zbioru $\mathbb{N}$ liczb naturalnych (to znaczy $S_\alpha \cup S_\beta = \mathbb{N}$ i $S_\alpha \cap S_\beta = \varnothing$) wtedy i tylko wtedy, gdy α i β są liczbami niewymiernymi spełniającymi warunek $\frac{1}{\alpha} + \frac{1}{\beta} = 1$.*

D O W Ó D. Zauważmy przede wszystkim, że $m \in S_\gamma$ wtedy i tylko wtedy, gdy istnieje takie $k \in \mathbb{N}$, że

$$\frac{m}{\gamma} \leqslant k < \frac{m}{\gamma} + \frac{1}{\gamma}, \tag{12.1}$$

przy czym, gdy γ jest liczbą niewymierną, to obie nierówności są ścisłe.

($\Longleftarrow$) Załóżmy, że dla $\alpha \notin \mathbb{Q}$, $\beta \notin \mathbb{Q}$ zachodzi równość $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ i załóżmy, nie wprost, że $m \in S_\alpha \cap S_\beta$. Wówczas, na mocy (12.1),

$$\frac{m}{\alpha} < k < \frac{m}{\alpha} + \frac{1}{\alpha} \quad \text{oraz} \quad \frac{m}{\beta} < l < \frac{m}{\beta} + \frac{1}{\beta}$$

dla pewnych naturalnych k, l. Dodając te nierówności stronami i korzystając z równości $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ dostajemy

$$m < k + l < m + 1,$$

co jest niemożliwe. Ta sprzeczność dowodzi, że $S_\alpha \cap S_\beta = \varnothing$.

Pokażemy teraz, że $S_\alpha \cup S_\beta = \mathbb{N}$. Załóżmy, nie wprost, że liczba naturalna m nie należy ani do S_α ani do S_β. To, na mocy (12.1), oznacza, że ani w przedziale $\left(\frac{m}{\alpha}; \frac{m}{\alpha} + \frac{1}{\alpha}\right)$, ani w przedziale $\left(\frac{m}{\beta}; \frac{m}{\beta} + \frac{1}{\beta}\right)$ nie ma ż a d n e j liczby naturalnej. Jednocześnie, dłuższe przedziały $\left(\frac{m}{\alpha}; \frac{m}{\alpha} + 1\right)$ i $\left(\frac{m}{\beta}; \frac{m}{\beta} + 1\right)$, z których każdy ma długość 1 i końce niewymierne, zawierają liczby całkowite. Istnieją więc $s, t \in \mathbb{N}$ należące do prawych części tych przedziałów:

$$\frac{m}{\alpha} + \frac{1}{\alpha} < s < \frac{m}{\alpha} + 1, \qquad \frac{m}{\beta} + \frac{1}{\beta} < t < \frac{m}{\alpha} + 1.$$

Dodając te nierówności stronami dostajemy

$$m + 1 < s + t < m + 2,$$

co jest niemożliwe. Ta sprzeczność dowodzi, że $S_\alpha \cup S_\beta = \mathbb{N}$.

($\Longrightarrow$) Odwrotnie, załóżmy, że zbiory S_α, S_β stanowią rozbicie zbioru $\mathbb{N}$. Ustalmy liczbę naturalną k i rozważmy zbiór $A_k = \{1, 2, \ldots, k\}$. Wówczas, jak łatwo sprawdzić,

$$|A_k \cap S_\alpha| = \left\lfloor \frac{k}{\alpha} \right\rfloor, \quad |A_k \cap S_\beta| = \left\lfloor \frac{k}{\beta} \right\rfloor.$$

Ale, $A_k \cap S_\alpha$ i $A_k \cap S_\beta$ są rozłączne, więc

$$\left\lfloor \frac{k}{\alpha} \right\rfloor + \left\lfloor \frac{k}{\beta} \right\rfloor = k. \tag{12.2}$$

Oznaczmy $\frac{1}{\alpha} + \frac{1}{\beta} = 1 + \varepsilon$. Wówczas, korzystając z C12.1.3, mamy dzięki (12.2),

$$k \leqslant \lfloor k(1+\varepsilon) \rfloor = k + \lfloor k\varepsilon \rfloor \leqslant k+1,$$

czyli $0 \leqslant \lfloor k\varepsilon \rfloor \leqslant 1$ dla każdego $k \in \mathbb{N}$. Jasne, że stąd $\varepsilon = 0$. Trzeba jeszcze wykazać, że α (i β) są niewymierne. To jest proste ćwiczenie, zobacz C12.9. □

Ćwiczenie 12.9 Udowodnić, że jeżeli $\alpha \in \mathbb{Q}_{>0}$ i $1/\alpha + 1/\beta = 1$, to $S_\alpha \cap S_\beta \neq \varnothing$.

ZADANIE 12.1 Załóżmy, że "odsiewamy" liczby naturalne następująco: wybieramy $a_1 = 1$ i odrzucamy $a_1 + 1 = 2$. Następnie wybieramy następną liczbę $a_2 = 3$ i odrzucamy $a_2 + 2 = 5$. Następną osiągalną (to znaczy nie wybraną i nie odrzuconą) liczbą jest $a_3 = 4$, więc odrzucamy $a_3 + 3 = 7$. I tak dalej. Widzimy, że wybranymi początkowymi liczbami są 1, 3, 4, 6, 8, 9, 11, 12, 14, ... Znaleźć formułę wyrażającą a_n.

Rozwiązanie. Zauważmy, że szukamy takiego ciągu (a_n), że ciągi (a_n) i (a_n+n) tworzą rozbicie zbioru $\mathbb{N}$. Z twierdzenia Beatty'*ego*-Banga wiemy, że ciągi $\lfloor \tau n \rfloor$ i $\lfloor \tau n \rfloor + n = \lfloor (\tau+1)n \rfloor$ tworzą rozbicie $\mathbb{N}$, gdy $\frac{1}{\tau} + \frac{1}{\tau+1} = 1$. Ale wówczas τ jest złotą liczbą $\tau = (1+\sqrt{5})/2$. Zatem $a_n = \lfloor \tau n \rfloor$. ◊

12.1.3 Zadania z częścią ułamkową

Pokażemy parę twierdzeń o części ułamkowej liczb rzeczywistych.

ZADANIE 12.2 Udowodnić, że istnieje nieskończenie wiele liczb naturalnych n, dla których zachodzi nierówność podwójna

$$\frac{1}{2n\sqrt{2}} < \{n\sqrt{2}\} < \frac{1+\varepsilon}{2n\sqrt{2}},$$

gdzie $\varepsilon > 0$ jest ustaloną liczbą rzeczywistą. Ponadto, nierówność lewa zachodzi dla wszystkich liczb naturalnych n.

Rozwiązanie. Udowodnimy najpierw lewą nierówność. Dla danej liczby $n \in \mathbb{N}$ oznaczmy $m = \lfloor n\sqrt{2} \rfloor$. Wówczas $m < n\sqrt{2}$. Równość nie może zachodzić, bo $\sqrt{2}$ jest liczbą niewymierną. Zatem

$$1 \leqslant 2n^2 - m^2 = (n\sqrt{2} - m)(n\sqrt{2} + m) = \{n\sqrt{2}\}(n\sqrt{2} + m) < \{n\sqrt{2}\} \cdot 2n\sqrt{2}.$$

To dowodzi nierówności lewej.

Niech teraz $(m_s, n_s)_{s \geqslant 0}$ będzie ciągiem dodatnich rozwiązań równania *anty*-indyjskiego

$$m^2 - 2n^2 = -1.$$

(Wiemy z ustępu 11.4.4, że liczby m_s, n_s otrzymuje się z równości

$$(1 + \sqrt{2})^{2s+1} = m_s + n_s\sqrt{2}, \quad s = 0, 1, 2, \ldots .)$$

Ponieważ ciąg (n_s) rośnie (szybko!) do nieskończoności, więc dla danej liczby $\varepsilon > 0$, nierówność

$$n_s > \left(1 + \frac{1}{\varepsilon}\right) \cdot \frac{1}{2\sqrt{2}}$$

zachodzi dla wszystkich $s \geqslant s_\varepsilon$. Łatwo stąd wywnioskować, że dla $n = n_s$, przy $s \geqslant s_\varepsilon$, zachodzi nierówność prawa. $\Diamond$.

Pokażemy teraz, że jeżeli α jest liczbą niewymierną, to części ułamkowe liczb $n\alpha$, $n \in \mathbb{N}$, leżą **gęsto** w przedziale $[\,0;\,1\,]$.

ZADANIE 12.3 Udowodnić, że jeżeli $\alpha \in \mathbb{R}$ jest liczbą niewymierną, to dla dowolnych liczb $0 \leqslant s < t \leqslant 1$ istnieje taka liczba naturalna n, że

$$s \leqslant \{n\alpha\} \leqslant t.$$

Rozwiązanie. Oznaczmy $\varepsilon = t - s$. Korzystając z T7.4 znajdujemy taką liczbę $k \in \mathbb{N}$, by były spełnione nierówności

$$|k\alpha - h| < \frac{1}{2k} \quad \text{oraz} \quad \frac{1}{2k} < \varepsilon \tag{12.3}$$

przy pewnym $h \in \mathbb{Z}$. Stąd $k\alpha = h + \delta$, gdzie $|\delta| < \varepsilon$.

Jeżeli $\delta > 0$, to wybierzmy liczbę naturalną l spełniającą nierówności

$$\frac{s}{\delta} < l < \frac{t}{\delta}$$

(taki wybór jest możliwy, bo $\frac{t}{\delta} - \frac{s}{\delta} > 1$) i kładziemy $n = lk$. Wówczas $n\alpha = lh + l\delta$, skąd $\{n\alpha\} = l\delta \in [\,s;\,t\,]$. Jeżeli zaś $\delta < 0$, to wybierzmy $l \in \mathbb{N}$, dla której

$$\frac{1 - t}{-\delta} < l < \frac{1 - s}{-\delta}$$

i połóżmy $n = lk$. Wówczas, jak łatwo sprawdzić, $\{n\alpha\} = 1 + l\delta \in [\,s;\,t\,]$. $\Diamond$

Ćwiczenie 12.10 Udowodnić, że do przedziału $[\,s;\,t\,]$ należy w istocie nieskończenie wiele (każda inna) liczb $\{n\alpha\}$.

Ćwiczenie 12.11 Niech $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Udowodnić, że w zbiorze $S_\alpha = \{\lfloor n\alpha \rfloor : n \in \mathbb{N}\}$ da się wskazać 2015 liczb będących wyrazami ciągu arytmetycznego. Czy istnieją niestałe nieskończone ciągi arytmetyczne o wyrazach ze zbioru S_α?

Okazuje się, że jeżeli α jest liczbą niewymierną, to części ułamkowe liczb $n\alpha$, dla $n \in \mathbb{N}$, są równomiernie rozłożone w odcinku $[\,0;\,1\,]$. Mówi o tym poniższe, udowodnione przez Bohla, Sierpińskiego i Weyla (niezależnie w latach 1909-1910):

Twierdzenie 12.2 (***twierdzenie o ekwipartycji***) *Jeżeli α jest liczbą niewymierną, to ciąg części ułamkowych $\{n\alpha\}$ jest jednostajnie rozłożony w przedziale $[\,0;\,1\,]$. To oznacza, że dla dowolnych $0 \leqslant s < t \leqslant 1$ zachodzi równość*

$$\lim_{n\to\infty} \frac{|\{k \in \mathbb{N} : 1 \leqslant k \leqslant n,\ s \leqslant \{k\alpha\} \leqslant t\}|}{n} = t - s. \quad \square$$

12.2 Zapis pozycyjny liczb

Jak wiadomo, od czasów "arabskich" liczby naturalne (a potem również wymierne dodatnie i rzeczywiste dodatnie) zapisujemy w tak zwanym **systemie pozycyjnym** o danej **podstawie**. Podstawą jest w początkowych stadiach studiów matematycznych liczba 10, potem 2 i wreszcie dowolna, większa od 1, liczba naturalna m.

Ustalamy liczbę naturalną $m > 1$. Elementy zbioru

$$\mathcal{C}_m = \{0,\, 1,\, 2,\, \ldots,\, m-1\} \tag{12.4}$$

nazywamy **cyframi** m-kowymi.

12.2.1 Zapis pozycyjny liczb naturalnych

Zapis pozycyjny liczb naturalnych w systemie o podstawie m znany jest od szkoły podstawowej (przynajmniej dla $m = 10$ i $m = 2$).

Mianowicie, dla danej liczby naturalnej N tworzymy ciąg cyfr m-kowych $a_0(N)$, $a_1(N)$, $a_2(N)$, $\ldots$, następująco: $a_k = a_k(N) \in \mathcal{C}_m$ jest jedyną taką cyfrą, że

$$a_0 + a_1 m + a_2 m^2 + \ldots + a_k m^k \equiv N \,(\mathrm{mod}\, m^{k+1}) \tag{12.5}$$

dla $k = 0,\, 1,\, 2,\, \ldots$.

Ćwiczenie 12.12 Uzasadnić, że kongruencje (12.5) wyznaczają jednoznacznie ciąg (a_k) cyfr m-kowych liczby naturalnej N.

Ćwiczenie 12.13 Udowodnić, że dla dowolnych $N \in \mathbb{N}$ i $k \in \mathbb{Z}_{\geqslant 0}$ zachodzi równość

$$a_k(N) = \left\lfloor \frac{N}{m^k} \right\rfloor - m \left\lfloor \frac{N}{m^{k+1}} \right\rfloor . \tag{12.6}$$

Ćwiczenie 12.14 Udowodnić, że jeżeli N jest liczbą naturalną, to wyrazy ciągu $(a_k(N))$ są równe zero od pewnego miejsca i zachodzi równość

$$N = \sum_{k \geqslant 0} a_k(N) m^k. \tag{12.7}$$

ZADANIE 12.4 Dana jest liczba naturalna $n \neq 0$. Udowodnić, że pewna wielokrotność qn, $q \in \mathbb{N}$, liczby n ma w zapisie dziesiętnym wyłącznie cyfry 0 i 1.

Rozwiązanie. Rozwiązanie jest prostym zastosowaniem zasady szufladkowej. Rozważmy ciąg 1, 11, 111, 1111, ... Jeżeli weźmiemy $n+1$ początkowych wyrazów tego ciągu, to wśród nich znajdą się dwa dające tę samą resztę z dzielenia przez n. Jasne, że jeżeli odejmiemy mniejszy z nich od większego, to różnica spełnia postawione żądania. ◊

ZADANIE 12.5 Udowodnić, że istnieje nieskończenie wiele potęg 2, w zapisie dziesiętnym których występuje cyfra 7.

Rozwiązanie. Udowodnimy nieco więcej: istnieje nieskończenie wiele potęg 2, których zapis dziesiętny zaczyna się od cyfry 7. Wiemy z C12.11, że istnieje nieskończenie wiele takich liczb naturalnych n, że $\log 7 \leqslant \{n \log 2\} < \log 8$. [Używamy tu logarytmu dziesiętnego.] Dodając $\lfloor n \log 2 \rfloor$ dostajemy $\lfloor n \log 2 \rfloor + \log 7 \leqslant n \log 2 < \lfloor n \log 2 \rfloor + \log 8$, czyli

$$7 \cdot 10^k \leqslant 2^n < 8 \cdot 10^k,$$

dla nieskończenie wielu n ($k = \lfloor n \log 2 \rfloor$). Ta nierówność, oczywiście, pokazuje, że w zapisie dziesiętnym liczby 2^n na pierwszym (od lewej strony) miejscu występuje cyfra 7. ◊

Uwaga. Tak samo, oczywiście, dowodzimy, że cyfra $a \in \{1, 2, \ldots, 9\}$ jest pierwszą cyfrą liczby 2^n, gdy część ułamkowa $\{n \log 2\}$ leży w przedziale $[\log a, \log(a+1)[$. Warto to porównać z twierdzeniem T12.2. Otrzymamy interesujący wniosek heurystyczny: *"prawdopodobieństwo", że liczba 2^n zaczyna się cyfrą a wynosi* $\log(a+1) - \log a = \log\left(1 + \frac{1}{a}\right)$. W szczególności, potęgi dwójki "chętniej" zaczynają się od cyfry 1 niż od cyfry 2, itd.

Ćwiczenie 12.15 Udowodnić, że każda liczba naturalna ma wielokrotność, w zapisie m-kowym której występuje każda z cyfr $0, 1, \ldots, m-1$.

Ćwiczenie 12.16 Udowodnić, że nie istnieje taka liczba naturalna, która zmniejsza się 35-krotnie, gdy zetrzemy jej początkową cyfrę (w zapisie dziesiętnym).

Ćwiczenie 12.17 n-cyfrowa liczba naturalna jest równa średniej arytmetycznej $n!$ liczb uzyskanych z niej przez możliwe permutacje jej cyfr. Wyznaczyć wszystkie liczby o tej własności.

Ćwiczenie 12.18 Niech $a_0 + a_1 p + a_2 p^2 + \ldots + a_k p^k$ będzie zapisem liczby naturalnej n w systemie p-kowym, gdzie p jest liczbą pierwszą. Udowodnić, że

$$v_p(n!) = \frac{n - a_0 - a_1 - a_2 - \ldots - a_k}{p-1}.$$

Ćwiczenie 12.19 Udowodnić, że istnieje nieskończenie wiele potęg 2008, w zapisie dziesiętnym których występują kolejno cyfry 2, 0, 0, 9.

12.2.2 Zapis pozycyjny liczb rzeczywistych

W szkole utożsamiamy **liczbę rzeczywistą** z punktem osi liczbowej. Nazwiemy to **interpretacją geometryczną** liczb rzeczywistych. Istnieje, i również jest używana w matematyce szkolnej, **interpretacja arytmetyczna** liczb rzeczywistych d o d a t n i c h. W tej interpretacji utożsamia się dodatnią liczbę rzeczywistą α z jej zapisem pozycyjnym (zazwyczaj dziesiętnym), czyli z takim ciągiem $(a_k)_{k\leqslant n}$ cyfr, że

$$\alpha = \sum_{k\leqslant n} a_k 10^k = a_n 10^n + a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \ldots .$$

Uogólnimy i nieco uściślimy taki sposób myślenia o liczbach rzeczywistych. K o n s t r u k c j a liczb rzeczywistych przedstawiona jest na przykład w [**10**] lub w $\mathbb{RIN}$.

Ustalmy liczbę naturalną $m > 1$. Opowiemy najpierw o zapisie pozycyjnym liczb $\alpha \in \mathbb{R}_{>0}$. Dla danej liczby $k \in \mathbb{N}$ przybliżamy (od dołu) liczbę α za pomocą największej całkowitej wielokrotności liczby m^{-k}. To znaczy, wyznaczamy n a j w i ę k s z ą liczbę całkowitą A_k, dla której $A_k m^{-k} \leqslant \alpha$. Wówczas

$$A_k m^{-k} \leqslant \alpha < (A_k + 1)m^{-k},$$

skąd widzimy, że A_k jest częścią całkowitą liczby $m^k\alpha$. Połóżmy więc, dla dowolnego $k \in \mathbb{N}$,

$$R_k(\alpha) = \frac{\lfloor m^k\alpha \rfloor}{m^k} = A_k m^{-k}. \tag{12.8}$$

Liczbę $R_k(\alpha)$ nazywamy k-tym **reduktem** liczby α przy podstawie m.

Ćwiczenie 12.20 Wykorzystać nierówności $0 \leqslant \alpha - R_k(\alpha) < m^{-k}$ do dowodu faktu, że ciąg $(R_k(\alpha))_k$ reduktów liczby rzeczywistej $\alpha \geqslant 0$ jest zbieżny do α.

Zapiszmy teraz redukt $R_k = R_k(\alpha)$ w postaci s u m y t e l e s k o p o w e j:

$$\frac{\lfloor m^k\alpha \rfloor}{m^k} = \frac{\lfloor m^k\alpha \rfloor - m\lfloor m^{k-1}\alpha \rfloor}{m^k} + \frac{\lfloor m^{k-1}\alpha \rfloor - m\lfloor m^{k-2}\alpha \rfloor}{m^{k-1}} + \ldots + \frac{\lfloor m\alpha \rfloor - m\lfloor \alpha \rfloor}{m} + \lfloor \alpha \rfloor.$$

Dla skrótu połóżmy

$$a_{-l} = a_{-l}(\alpha) = \lfloor m^l\alpha \rfloor - m\lfloor m^{l-1}\alpha \rfloor \tag{12.9}$$

dla $l = 1, 2, 3, \ldots$. Wówczas powyższe przedstawienie k-tego reduktu zapisuje się następująco:

$$R_k(\alpha) = \lfloor \alpha \rfloor + \frac{a_{-1}}{m} + \frac{a_{-2}}{m^2} + \ldots + \frac{a_{-k}}{m^k}. \tag{12.10}$$

Liczbę $a_{-l}(\alpha)$ nazywamy l-tą **cyfrą po przecinku** (w zapisie liczby α przy podstawie m).

Ćwiczenie 12.21 Udowodnić, że $a_{-l}(\alpha)$ są cyframi m-kowymi.

Zapiszmy teraz część całkowitą $\lfloor \alpha \rfloor$ liczby α w systemie pozycyjnym przy podstawie m:

$$\lfloor \alpha \rfloor = a_0 + a_1 m + \ldots + a_n m^n.$$

Ćwiczenie 12.22 Udowodnić, że w takim przypadku zachodzą równości

$$a_j = \left\lfloor \frac{\alpha}{m^j} \right\rfloor - m \left\lfloor \frac{\alpha}{m^{j-1}} \right\rfloor = a_j(\lfloor \alpha \rfloor).$$

Ćwiczenia C12.20, C12.21 i C12.22 pozwalają więc dla dowolnej nieujemnej liczby rzeczywistej α napisać równość

$$\alpha = \sum_{k \geqslant -n} a_{-k}(\alpha) m^{-k}, \tag{12.11}$$

gdzie $a_{-k}(\alpha) = \lfloor m^k \alpha \rfloor - m \lfloor m^{k-1} \alpha \rfloor$, dla $k \in \mathbb{Z}$, są cyframi m-kowymi.

Zapis (12.11) nazywamy **zapisem pozycyjnym liczby rzeczywistej** $\alpha \geqslant 0$ (w systemie) przy podstawie m. "Numerycznie" zapisujemy tę równość następująco:

$$\alpha = \lfloor \alpha \rfloor + (0,\, a_{-1} a_{-2} a_{-3} \ldots)_m. \tag{12.12}$$

Dla danej liczby $\alpha > 0$ i danej liczby $n \in \mathbb{N}$ połóżmy

$$\alpha_n = m^n \left(\alpha - R_n(\alpha)\right) = m^n \alpha - \lfloor m^n \alpha \rfloor. \tag{12.13}$$

Ćwiczenie 12.23 Sprawdzić, że dla $k \in \mathbb{N}$ zachodzi równość $a_{-k}(\alpha) = \lfloor m \alpha_k \rfloor$.

Ćwiczenie 12.24 Udowodnić, że ciąg cyfr $(a_{-n}(\alpha))_{n \in \mathbb{N}}$ jest okresowy (od pewnego miejsca) wtedy i tylko wtedy, gdy istnieją takie liczby naturalne $k < l$, że $\alpha_k = \alpha_l$.

Najważniejszym twierdzeniem dotyczącym zapisu pozycyjnego liczb rzeczywistych dodatnich jest poniższe:

TWIERDZENIE 12.3 *Liczba rzeczywista dodatnia ma okresowy (od pewnego miejsca) zapis pozycyjny przy podstawie m wtedy i tylko wtedy, gdy jest liczbą wymierną.*

D O W Ó D. ($\Longleftarrow$) Niech $\alpha = \frac{u}{w}$ będzie dodatnią liczbą wymierną. Nie zmniejszając ogólności rozważań możemy założyć, że $0 < u < w$. Wówczas $\alpha_k = m^k u/w - \lfloor m^k u/w \rfloor$. Wykonajmy dzielenie $m^k u$ przez w z resztą:

$$m^k u = q_k w + r_k, \quad 0 \leqslant r_k < w. \tag{12.14}$$

Możemy więc zapisać

$$\alpha_k = \frac{m^k u}{w} - \left\lfloor \frac{m^k u}{w} \right\rfloor = q_k + \frac{r_k}{w} - \left\lfloor q_k + \frac{r_k}{w} \right\rfloor = \frac{r_k}{w}. \tag{12.15}$$

Ponieważ reszty r_k, dla $k = 1, 2, \ldots$, przyjmują tylko wartości ze zbioru $\{0, 1, \ldots, w-1\}$, więc w ciągu $r_1, r_2, \ldots, r_{w+1}$ znajdą się dwa r ó w n e wyrazy. Zatem $\alpha_k = \alpha_l$ dla pewnych $1 \leqslant k < l \leqslant w+1$. Na mocy C12.24 widzimy więc, że ciąg $(a_{-n}(u/w))$ cyfr m-kowych liczby $\frac{u}{w}$ jest okresowy o okresie długości n i e w i ę k s z e j niż w.

($\Longrightarrow$) Dowód w tę stronę jest prostym wykorzystaniem wzoru na sumę wyrazów ciągu geometrycznego. Załóżmy, że

$$\alpha = \lfloor \alpha \rfloor + (0,\, a_{-1}a_{-2}\ldots a_{-n}\overline{c_1c_2\ldots c_k})_m. \tag{12.16}$$

Patrz (12.12). Oznaczmy

$$A = \frac{c_1}{m} + \frac{c_2}{m^2} + \ldots + \frac{c_k}{m^k}.$$

Przy tym oznaczeniu, równość (12.11) pisze się następująco:

$$\alpha = \lfloor \alpha \rfloor + \frac{a_{-1}}{m} + \ldots + \frac{a_{-n}}{m^n} + \frac{1}{m^n}\left(A + \frac{A}{m^k} + \frac{A}{m^{2k}} + \frac{A}{m^{3k}} + \ldots\right).$$

Ponieważ wyrażenie w nawiasie równe jest $A\left(1-\frac{1}{m^k}\right)^{-1}$, więc widzimy, że $\alpha \in \mathbb{Q}$. □

Korzystając z (12.14) i (12.15) łatwo rozwiążemy dwa ćwiczenia.

Ćwiczenie 12.25 Udowodnić, że przedstawienie liczby $\alpha \in \mathbb{Q}_{>0} \setminus \mathbb{N}$ w systemie pozycyjnym przy podstawie m jest s k o ń c z o n e (to znaczy, że cyfry a_{-n} są równe zero od pewnego miejsca) wtedy i tylko wtedy, gdy zachodzi równość $\alpha = \frac{a}{b}$, gdzie mianownik b dzieli się przez takie i tylko takie liczby pierwsze p, dla których $v_p(m) > 0$.

Ćwiczenie 12.26 Udowodnić, że zapis m-kowy liczby wymiernej $\frac{1}{p}$, gdzie p jest liczbą pierwszą, jest czysto-okresowy o okresie długości $p-1$ wtedy i tylko wtedy, gdy $m \pmod p$ jest pierwiastkiem pierwotnym modulo p. Zobacz też C5.52.

12.3 Ułamki egipskie

Starożytni egipcjanie używali w zasadzie tylko najprostszych ułamków. Ułamków postaci $1/n$, gdzie $n \in \mathbb{N}$. Będziemy je wobec tego nazywać **ułamkami egipskimi**.[1]

12.3.1 Skończone sumy ułamków egipskich

Sumy ułamków egipskich są, oczywiście, liczbami wymiernymi dodatnimi. Zajmiemy się pytaniem odwrotnym: czy każda liczba wymierna dodatnia jest sumą ułamków egipskich? Odpowiedź na tak postawione pytanie jest trywialna: t a k. Bowiem $m/n = 1/n + 1/n + \ldots + 1/n$. Utrudnimy więc pytanie: *czy każda liczba wymierna dodatnia* $\alpha = m/n$ *da się zapisać w postaci*

$$\alpha = \frac{1}{k_1} + \frac{1}{k_2} + \ldots + \frac{1}{k_s}, \qquad \text{gdzie } k_1 < k_2 < \ldots < k_s? \tag{12.17}$$

[1] Nazywa sie je również *ułamkami prostymi*. Zobacz **[17]** gdzie znaleźć można dużo więcej informacji na temat sum ułamków egipskich.

Sumy dwóch ułamków egipskich

Zaczniemy od rozkładów liczb wymiernych (dodatnich) na sumy d w ó c h ułamków egipskich.

Ćwiczenie 12.27 Udowodnić twierdzenie A. Schinzla: *Liczba wymierna* $m/n > 0$ *(dana w postaci nieskracalnej) jest sumą dwóch ułamków egipskich wtedy i tylko wtedy, gdy mianownik* n *ma takie względnie pierwsze dzielniki* a, b, *że* $m|a+b$.

Ćwiczenie 12.28 Udowodnić, że na to żeby liczba wymierna $m/n > 0$ (dana w postaci nieskracalnej) była sumą dwóch ułamków egipskich o względnie pierwszych mianownikach, potrzeba i wystarcza, aby liczba $m^2 - 4n$ była kwadratem (liczby całkowitej).

Ćwiczenie 12.29 Udowodnić, że istnieje nieskończenie wiele liczb naturalnych n, dla których liczba wymierna $3/n$ n i e jest sumą dwóch ułamków egipskich.

Hipoteza Erdősa-Strausa

W związku z rozkładami liczb wymiernych dodatnich na sumy ułamków egipskich mamy wiele nierozstrzygniętych pytań. Odsyłając zainteresowanego Czytelnika do literatury, wspomnimy tu tylko o ***hipotezie Erdősa-Strausa***: *Dla dowolnej liczby naturalnej* n *liczba* $4/n$ *da się zapisać w postaci sumy trzech ułamków egipskich*, innymi słowy, *równanie*

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

ma rozwiązania w liczbach n a t u r a l n y c h x, y, z *dla każdego* $n \in \mathbb{N}$. Hipoteza ta została sprawdzona dla wszystkich $n \in [\,2;\, 10^{14}\,] \cap \mathbb{N}$.

Ćwiczenie 12.30 Sprawdzić hipotezę Erdősa-Strausa dla $n = 2, \ldots, 20$.

Rozkłady jedynki

Przedstawienie liczby 1 w postaci sumy r ó ż n y c h ułamków egipskich nazwiemy **rozkładem jedynki**. Każdy zna najprostszy rozkład jedynki (jedyny na trzy składniki, zobacz Z11.1):

$$1 = \tfrac{1}{2} + \tfrac{1}{3} + \tfrac{1}{6}. \tag{12.18}$$

Łatwo podać rozkłady jedynki na sumy parzystych (to znaczy o parzystych mianownikach) ułamków egipskich. Serię prostych przykładów widzimy poniżej:

$$1 = \tfrac{1}{2} + \tfrac{1}{4} + \ldots + \tfrac{1}{2^n} + \tfrac{1}{2^{n+1}} + \tfrac{1}{3\cdot 2^n} + \tfrac{1}{6\cdot 2^n}. \tag{12.19}$$

[Suma pierwszych n wyrazów jest równa $1 - \frac{1}{2^n}$, pozostałe trzy składniki powstają przez pomnożenie obu stron równości (12.18) przez $\frac{1}{2^n}$.]

Jeżeli znajdziemy liczbę naturalną N i takie jej r ó ż n e dzielniki $1 \leqslant d_1 < d_2 < \ldots < d_s$, że $N = d_1 + d_2 + \ldots + d_s$, to dzieląc tę równość przez N znajdujemy rozkład jedynki:

$$1 = \tfrac{1}{k_1} + \tfrac{1}{k_2} + \ldots + \tfrac{1}{k_s},$$

gdzie $N = d_{s-j}k_{j+1}$ dla $j = 0, \ldots, s-1$. W ten sposób z sumy $6 = 1 + 2 + 3$ powstaje rozkład (12.18). Wszystkie inne liczby doskonałe dostarczają podobnych przykładów.

Ćwiczenie 12.31 Uzasadnić, że n i e istnieje rozkład jedynki na sumę dwóch, ani trzech, ani czterech, ani pięciu, ani sześciu różnych nieparzystych (o nieparzystych mianownikach) ułamków egipskich.

Istnieją takie liczby n i e p a r z y s t e, które są sumami swoich różnych dzielników. Każda taka liczba dostarcza więc przykładu rozkładu jedynki na sumę nieparzystych ułamków egipskich.

P r z y k ł a d 1. Niech $N = 3465 = 3^2 \cdot 5 \cdot 7 \cdot 11$. Mamy $3465 = 1155 + 693 + 495 + 385 + 315 + 231 + 99 + 77 + 15$, skąd dostajemy dziewięciowyrazowy nieparzysty rozkład jedynki:

$$1 = \tfrac{1}{3} + \tfrac{1}{5} + \tfrac{1}{7} + \tfrac{1}{9} + \tfrac{1}{11} + \tfrac{1}{15} + \tfrac{1}{35} + \tfrac{1}{45} + \tfrac{1}{231}. \quad \Diamond$$

P r z y k ł a d 2. Interesującą własność ma liczba $945 = 3^3 \cdot 5 \cdot 7$. Oto zbiór jej dodatnich dzielników:

$$D_+(945) = \{1, 3, 5, 7, 9, 15, 21, 27, 35, 45, 63, 105, 135, 189, 315, 945\}.$$

Można udowodnić, że nie tylko sama liczba 945, ale wszystkie liczby naturalne z przedziału $[\,1;\, \sigma(945)\,]$, z wyjątkiem 2 i 1918, są sumami różnych elementów zbioru $D_+(945)$. W szczególności $945 = 315 + 189 + 135 + 105 + 63 + 45 + 35 + 27 + 21 + 9 + 1$. Stąd dostajemy jedenastowyrazowy nieparzysty rozkład jedynki:

$$1 = \tfrac{1}{3} + \tfrac{1}{5} + \tfrac{1}{7} + \tfrac{1}{9} + \tfrac{1}{15} + \tfrac{1}{21} + \tfrac{1}{27} + \tfrac{1}{35} + \tfrac{1}{45} + \tfrac{1}{105} + \tfrac{1}{945} \quad \Diamond$$

Ćwiczenie 12.32 Udowodnić, że każda liczba naturalna $m \in [\,1920\,] \setminus \{2,\, 1918\}$ jest sumą r ó ż n y c h elementów zbioru $D_+(945)$.

Ćwiczenie 12.33 Udowodnić, że istnieją rozkłady jedynki na sumę nieparzystych (i różnych) ułamków egipskich mające dowolną nieparzystą i większą niż 7 liczbę składników. *Wskazówka.* Można wykorzystać rozkład $1/3 = 1/5 + 1/9 + 1/45$.

Ćwiczenie 12.34 Udowodnić, że żadna liczba naturalna $\geqslant 2$ nie da się zapisać w postaci sumy różnych kwadratowych ułamków egipskich (tzn. ułamków postaci $1/k^2$).

Ćwiczenie 12.35 Udowodnić, że żadna liczba naturalna nie jest sumą różnych ułamków egipskich o mianownikach będących liczbami pierwszymi.

Algorytm Fibonacci'*ego*

Fibonacci pokazał prosty algorytm pozwalający uzyskiwać przedstawienia postaci (12.17) dla dodatnich liczb wymiernych m/n niewiększych od 1 (tzw. ułamków właściwych). Niech mianowicie m/n będzie ułamkiem właściwym nieegipskim danym w postaci nieskracalnej, to znaczy, że $2 \leqslant m \leqslant n$ i $\mathrm{NWD}\,(m,\, n) = 1$. Niech k_1 będzie jedyną taką liczbą naturalną, że

$$\frac{1}{k_1} < \frac{m}{n} < \frac{1}{k_1 - 1}. \tag{12.20}$$

Łatwo widzieć, że jeżeli $m \geqslant 2$, to takie k_1 istnieje (oczywiście $k_1 = \lceil \frac{n}{m} \rceil$, gdzie $\lceil x \rceil$ oznacza najmniejszą liczbę całkowitą większą bądź równą x, jest to tak zwany **sufit** liczby $x \in \mathbb{R}$).

Wówczas $\frac{m}{n} - \frac{1}{k_1} = \frac{k_1 m - n}{k_1 n} =: \frac{m'}{n'} = \frac{m_1}{n_1}$, gdzie $\frac{m_1}{n_1}$ jest postacią nieskracalną ułamka $\frac{m'}{n'}$. W ten sposób otrzymujemy przedstawienie

$$\frac{m}{n} = \frac{1}{k_1} + \frac{m_1}{n_1},$$

Ćwiczenie 12.36 Udowodnić, że wówczas $m_1 \leqslant m' < m$ oraz że, jeżeli $m_1 \geqslant 2$, to $k_2 := \lceil \frac{n_1}{m_1} \rceil > k_1$.

Stąd wynika, że sztuczkę polegającą na odejmowaniu największego ułamka egipskiego mniejszego niż dana liczba wymierna z przedziału $(0; 1)$ możemy powtarzać aż do momentu, gdy dostaniemy licznik $m_s = 1$. Opisaną tym sposobem procedurę nazwiemy ***algorytmem Fibonacci'ego*** lub ***algorytmem zachłannym*** (ang. *greedy*). Jego "zachłanność" przejawia się w tym, że prowadzi on zazwyczaj do dużych mianowników k_i.

P r z y k ł a d 3. Stosując algorytm Fibonacci'*ego* do liczby $\frac{59}{120}$ dostajemy rozkład

$$\frac{59}{120} = \frac{1}{3} + \frac{1}{7} + \frac{1}{65} + \frac{1}{10920}.$$

Tymczasem $\frac{59}{120} = \frac{1}{5} + \frac{1}{6} + \frac{1}{8}$. ◊

Dzięki algorytmowi Fibonacci'*ego* możemy udowodnić twierdzenie:

TWIERDZENIE 12.4 *Każda liczba wymierna dodatnia może być zapisana w postaci sumy r ó ż n y c h ułamków egipskich (i to na nieskończenie wiele sposobów).*

D O W Ó D. Niech $\alpha \in \mathbb{Q}_{>0}$. Pokażemy najpierw i s t n i e n i e rozkładu postaci (12.17). Jeżeli $\alpha \leqslant 1$, to już wiemy. Załóżmy więc, że $\alpha > 1$. Korzystając z twierdzenia T12.5 znajdziemy taką liczbę naturalną n, że $h_{n-1} \leqslant \alpha < h_n$. Jeżeli $\alpha = h_{n-1}$, to koniec. Załóżmy więc, że $h_{n-1} < \alpha < h_n$ i rozważmy dodatnią liczbę wymierną $\beta = \alpha - h_{n-1}$. Ponieważ $\beta < h_n - h_{n-1} = \frac{1}{n} < 1$, więc stosując do β algorytm Fibonacci'*ego* znajdujemy rozkład $\beta = \frac{1}{k_1} + \cdots + \frac{1}{k_s}$, gdzie $\frac{1}{k_1} < \beta < \frac{1}{n}$. Ostatecznie

$$\alpha = h_{n-1} + \beta = \tfrac{1}{1} + \ldots + \tfrac{1}{n-1} + \tfrac{1}{k_1} + \ldots + \tfrac{1}{k_s}$$

i $1 < 2 < \ldots < n-1 < k_1 < \ldots < k_s$. Mamy więc szukany rozkład.

Chcemy jeszcze udowodnić, że różnych takich rozkładów danej liczby $\alpha \in \mathbb{Q}_{>0}$ jest dowolnie wiele. W tym celu pokażemy metodę, która dla danego rozkładu (12.17) pozwala wskazać rozkład liczby α o istotnie większych mianownikach. Weźmy mianowicie dowolną liczbę naturalną $N > k_s$ i dowolny rozkład

$$N\alpha = \tfrac{1}{l_1} + \tfrac{1}{l_2} + \ldots + \tfrac{1}{l_t}$$

spełniający warunek $l_1 < l_2 < \ldots < l_t$. Dzieląc tę równość obustronnie przez N znajdujemy rozkład liczby α

$$\alpha = \tfrac{1}{Nl_1} + \tfrac{1}{Nl_2} + \ldots + \tfrac{1}{Nl_t},$$

dla którego $k_s < N \leqslant Nl_1 < Nl_2 < \ldots < Nl_t$. To kończy dowód. □

Zachęcamy Czytelnika do przeczytania książki Wacława Sierpińskiego [**17**], gdzie między innymi znaleźć można dowód twierdzenia, że *każda dodatnia liczba wymierna o nieparzystym mianowniku jest sumą r ó ż n y c h nieparzystych ułamków egipskich.*

12.3.2 Szeregi harmoniczne

Pokażemy teraz, że "sumą" wszystkich ułamków egipskich jest "nieskończoność". To znaczy, że ciąg (h_n), którego n-ty wyraz równy jest sumie $\sum_{k=1}^{n} 1/k$, jest ciągiem rosnącym do nieskończoności (ma dowolnie duże wyrazy). Z tego faktu korzystaliśmy już w dowodzie T12.4. Pokażemy jeszcze parę jego zastosowań w teorii liczb. Ustęp zakończymy pięknym rozwiązaniem tak zwanego problemu bazylejskiego.

Wygodnie jest badać ogólniejsze sumy postaci

$$h_n(s) := 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots + \frac{1}{n^s}, \tag{12.21}$$

gdzie $s \in \mathbb{R}$. Zamiast $h_n(1)$ piszemy po prostu h_n. Jasne, że ciąg $(h_n(s))_{n\geqslant 1}$ jest ciągiem ściśle rosnącym. Może być ograniczony (na przykład $h_n(2) \leqslant 2$ dla każdego $n \in \mathbb{N}$, zobacz C1.4), albo nieograniczony (na przykład $h_n(0) \geqslant n$ dla każdego $n \in \mathbb{N}$).

TWIERDZENIE 12.5 *Jeżeli $s > 1$, to ciąg $(h_n(s))_{n\geqslant 1}$ jest ciągiem ograniczonym, jeżeli zaś $s \leqslant 1$, to ciąg $(h_n(s)_{n\geqslant 1}$ jest ciągiem nieograniczonym (rosnącym do nieskończoności).*

DOWÓD. Zaczniemy od przypadku $s = 1$. Niech $n = 2^k$. Zapiszmy liczbę $h_n = h_n(1)$ następująco:

$$h_n = 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \ldots + \left(\frac{1}{2^{k-1}+1} + \frac{1}{2^{k-1}+2} + \ldots + \frac{1}{2^k}\right).$$

Ponieważ, jak łatwo widzieć, suma liczb w każdym ze wskazanych nawiasów jest $> \frac{1}{2}$, więc mamy oszacowanie $h_{2^k} \geqslant 1 + \frac{k}{2}$ dla każdego $k \in \mathbb{N}$. Jeżeli dla danej liczby M wybierzemy dowolną liczbę naturalną k spełniającą warunek $k \geqslant 2(M-1)$, to, jak widać z tego oszacowania, $h_{2^k} \geqslant M$. To znaczy, że liczby h_n są dowolnie duże (dla dostatecznie dużych n). [Inaczej mówiąc: jeżeli startujemy z punktu 0 na osi liczbowej i kroczymy "w prawo" przy czym tak, że nasz k-ty krok ma długość równą $\frac{1}{k}$, to możemy zajść dowolnie daleko.]

Jeżeli teraz $s \leqslant 1$, to dla każdego $k \in \mathbb{N}$ mamy nierówność $k^s \leqslant k$, więc

$$h_n(s) = \sum_{k=1}^{n} \frac{1}{k^s} \geqslant \sum_{k=1}^{n} \frac{1}{k} = h_n.$$

Ponieważ ciąg (h_n) jest ciągiem rosnącym do $+\infty$, więc, mający większe wyrazy, ciąg $(h_n(s))$ tym bardziej rośnie do $+\infty$.

Załóżmy teraz, że $s > 1$. Połóżmy $s = 1 + t$, gdzie $t > 0$. Wówczas, dla $n = 2^k - 1$

$$h_n(s) = (1) + \left(\frac{1}{2^s} + \frac{1}{3^s}\right) + \left(\frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s}\right) + \ldots + \left(\frac{1}{(2^{k-1})^s} + \ldots + \frac{1}{(2^k-1)^s}\right).$$

Widzimy, że liczba $h_n(s)$ jest (przy $n = 2^k - 1$) sumą k składników (w nawiasach), z których l-ty jest sumą 2^{l-1} składników mniejszych bądź równych 2^{ls}. Wobec tego

$$h_n(s) \leqslant 1 + \frac{2}{2^s} + \frac{4}{4^s} + \ldots + \frac{2^{k-1}}{(2^{k-1})^s} = 1 + \frac{1}{2^t} + \frac{1}{4^t} + \ldots + \frac{1}{(2^{k-1})^t}.$$

Z prawej strony widzimy tu sumę skończonej liczby wyrazów ciągu geometrycznego o ilorazie 2^{-t}. Więc suma ta jest $<$ niż suma wszystkich wyrazów takiego ciągu:

$$h_n(s) < \frac{1}{1-2^{-t}} = \frac{2^t}{2^t-1} = \frac{2^{s-1}}{2^{s-1}-1}. \tag{12.22}$$

[Zauważmy, że przy $s=2$ otrzymaliśmy to samo szacowanie co w C1.4.] Stąd natychmiast dostajemy ograniczoność ciągu $(h_n(s))_{n\geqslant 1}$. □

Ćwiczenie 12.37 Czy możecie uzasadnić nieograniczoność ciągu (h_n) za pomocą poniższych napisów

$$\sum_{k=1}^{\infty}\frac{1}{k} = \sum_{l=0}^{\infty}\left(\frac{1}{2l+1}+\frac{1}{2l+2}\right) > \sum_{l=0}^{\infty}\left(\frac{1}{2l+2}+\frac{1}{2l+2}\right) = \sum_{l=0}^{\infty}\frac{1}{l+1} = \sum_{k=1}^{\infty}\frac{1}{k}?$$

Należy przy tym zwrócić uwagę na dwie okoliczności: (1) zarówno wszystkie trzy występujące tu znaki równości jak i znak nierówności wymagają zrozumienia i uzasadnienia, (2) powstały w ten sposób dowód rozbieżności ciągu (h_n) do nieskończoności, w przeciwieństwie do pokazanego w dowodzie twierdzenia, nie daje wyobrażenia o szybkości tej rozbieżności.

Dla $s>1$ oznaczamy przez $\zeta(s)$ najmniejsze ograniczenie (górne) ciągu $(h_n(s))$. To znaczy, że $h_n(s)<\zeta(s)$ dla każdego n, ale nierówność $h_n(s)<\zeta(s)-\varepsilon$ może (przy $\varepsilon>0$) zachodzić dla skończonej tylko liczby indeksów n. Zapisujemy to tak:

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \lim_{n\to\infty} h_n(s).$$

Pokażemy teraz (mało teorioliczbowe, dlaczego?) zastosowanie rozbieżności ciągu (h_n):

ZADANIE 12.6 Dana jest (ustalona) liczba naturalna a. Udowodnić, że w zapisie dziesiętnym pewnej jej wielokrotności występują wszystkie cyfry $0, 1, \ldots, 9$.

Rozwiązanie. Dla danej cyfry $l\in\{0,1,\ldots,9\}$ oznaczmy przez C_l zbiór tych wszystkich liczb naturalnych, w zapisie dziesiętnym których nie występuje cyfra l. Gdy $l\neq 0$, to liczb s-cyfrowych w zbiorze C_l jest $8\cdot 9^{s-1}$ i każda z nich jest $\geqslant 10^{s-1}$. Zatem suma odwrotności wszystkich, mających mniej niż N cyfr, liczb należących do C_l spełnia nierówność

$$\sum_{k\in C_l,\,1\leqslant k<10^N}\frac{1}{k} \leqslant 8+\frac{8\cdot 9}{10}+\frac{8\cdot 9^2}{10^2}+\ldots+\frac{8\cdot 9^N}{10^N} = 80(1-(0,9)^{N+1}) < 80.$$

Wobec tego $\sum_{k\in C_l}\frac{1}{k}<80$ dla każdego $l=1,\ldots,9$. Przy $l=0$ dostajemy analogicznie $\sum_{k\in C_0}\frac{1}{k}<90$.

Załóżmy teraz nie wprost, że wszystkie wielokrotności ka liczby a należą do sumy $C=C_0\cup C_1\cup\ldots\cup C_9$ (to znaczy, że żadna wielokrotność ka nie jest dobra). Wtedy

$$\sum_{k\geqslant 1}\frac{1}{ka} = \sum_{k\in C}\frac{1}{ka} < \sum_{r\in C_0}\frac{1}{r}+\sum_{l=1}^{9}\sum_{r\in C_l}\frac{1}{r} < 90+9\cdot 80.$$

Dostaliśmy sprzeczność z rozbieżnością ciągu (h_n/a). Czytelnik z pewnością potrafi dostrzec i naprawić pozostawione tu rozmyślnie luki matematyczne. ◊

Ćwiczenie 12.38 Ciąg (a_n) ma wyrazy całkowite i jest ściśle rosnący. Załóżmy ponadto, że $|a_n| \leqslant 2016^{2017}n$ dla wszystkich n większych niż 2018^{2019}. Wykazać, że istnieje co najmniej 2020^{2021} takich indeksów $n \in \mathbb{N}$, że a_n jest liczbą naturalną, w zapisie dziesiętnym której występuje 2022^{2023} cyfr równych 7 pod rząd.

Pokażemy teraz zapowiadany nowy dowód twierdzenia Schura T5.3. Ten dowód ma się tak do pokazanego w ustępie 5.1.3, jak nasz CZWARTY DOWÓD TE ma się do naszego PIERWSZEGO DOWODU TE, zobacz ustęp 2.3.2.

D O W Ó D. Niech $f(X) \in \mathbb{Z}[X]$, $\deg f(X) = n \geq 1$. Chcemy wykazać, że kongruencja

$$f(x) \equiv 0 \,(\mathrm{mod}\, p) \tag{12.23}$$

ma rozwiązania w liczbach naturalnych dla n i e s k o ń c z e n i e wielu liczb pierwszych p. Jasne, że jeżeli wielomian $f(X)$ ma pierwiastek całkowity, na przykład $f(u) = 0$, to dla d o w o l n e j liczby pierwszej p i dostatecznie dużych $t \in \mathbb{N}$, liczba $u+tp$ jest naturalnym (należącym do $\mathbb{N}$) pierwiastkiem kongruencji (12.23). Załóżmy więc, że $f(X)$ nie ma pierwiastków całkowitych. W szczególności $f(k) \neq 0$ dla wszystkich $k \in \mathbb{N}$. Załóżmy też, nie wprost, że kongruencje $f(x) \equiv 0 \,(\mathrm{mod}\, p)$ mają rozwiązania w y ł ą c z n i e dla $p \in \{p_1, p_2, \ldots, p_r\}$. To, oczywiście, znaczy, że dla dowolnego $k \in \mathbb{N}$ liczba naturalna(!) $|f(k)|$ dzieli się tylko przez liczby pierwsze ze zbioru $\{p_1, \ldots, p_r\}$. Czyli zachodzi równość

$$|f(k)| = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r} \tag{12.24}$$

dla pewnych (zależnych od k) wykładników $e_1, \ldots, e_r$. Stąd

$$\sum_{k\geqslant 1} \frac{1}{|f(k)|^s} \leqslant 2n \sum_{e_1,\ldots,e_r \geqslant 0} \frac{1}{p_1^{e_1 s} \cdot \ldots \cdot p_r^{e_r s}} = 2n \prod_{j=1}^{r} \left(1 + \frac{1}{p_j^s} + \frac{1}{p_j^{2s}} + \frac{1}{p_j^{3s}} + \ldots\right).$$

Nierówność jest jasna, ponieważ dana liczba stojąca z prawej strony (12.24) może być wartością $|f(k)|$ dla co najwyżej $2n$ wartości k. Korzystając ze wzoru na sumę wyrazów ciągu geometrycznego, mamy więc dla dowolnego $s > 0$:

$$\sum_{k\geqslant 1} \frac{1}{|f(k)|^s} \leqslant 2n \prod_{j=1}^{r} \frac{p_j^s}{p_j^s - 1}. \tag{12.25}$$

Z drugiej strony, ponieważ $|f(x)| \leqslant x^{n+1}$ dla wszystkich $x \geqslant M$ (gdzie $M \geqslant 1$), więc

$$\sum_{k\geqslant M} \frac{1}{k} \leqslant \sum_{k\geqslant M} \frac{1}{|f(k)|^s} \leqslant \sum_{k\geqslant 1} \frac{1}{|f(k)|^s},$$

dla dowolnego $0 < s < 1/(n+1)$. To jest sprzeczne z nierównością (12.25). □

Dla ułatwienia wysłowień przyjmijmy definicję:

Definicja 12.2 Mówimy, że podzbiór $\mathcal{D} \subseteq \mathbb{N}$ jest **szczupły**, gdy istnieje taka stała M, że $\sum_{k\in\mathcal{D}} \frac{1}{k} \leqslant M$. W przypadku przeciwnym mówimy, że $\mathcal{D}$ jest zbiorem **obszernym**.

ZADANIE 12.7 Dowieść, że zbiór liczb bezkwadratowych jest zbiorem o b s z e r n y m.

R o z w i ą z a n i e. Załóżmy nie wprost, że zbiór $\mathcal{B}$ liczb naturalnych bezkwadratowych jest szczupły, czyli że $\sum_{k\in\mathcal{B}} \frac{1}{k} \leqslant M$ dla pewnej stałej M. Wówczas, zobacz C2.36,

$$\sum_{k\in\mathbb{N}} \frac{1}{k} = \sum_{a\in\mathbb{N}} \sum_{k\in\mathcal{B}} \frac{1}{a^2 k} = \sum_{a\in\mathbb{N}} \left(\frac{1}{a^2} \sum_{k\in\mathcal{B}} \frac{1}{k} \right) \leqslant \sum_{a\in\mathbb{N}} \frac{M}{a^2} = M\zeta(2) < \infty.$$

Uzyskana sprzeczność kończy rozwiązanie. ◊

TWIERDZENIE 12.6 (***Euler***) *Zbiór* $\mathbb{P}$ *liczb pierwszych jest zbiorem o b s z e r n y m.*

D O W Ó D. (I. Niven) Oznaczmy przez $\mathcal{B}_x$ zbiór wszystkich takich liczb naturalnych bezkwadratowych, które dzielą się tylko przez liczby pierwsze $\leqslant x$. Wówczas, zakładając nie wprost, że $\sum_{p\in\mathbb{P}} \frac{1}{p} \leqslant M$, dostajemy

$$\sum_{k\in\mathcal{B}_x} \frac{1}{k} = \prod_{p\leqslant x} \left(1 + \frac{1}{p}\right) < \prod_{p\leqslant x} e^{1/p} = \exp \sum_{p\leqslant x} \frac{1}{p} \leqslant e^M.$$

Korzystamy tu z nierówności $1 + x < e^x =: \exp x$ prawdziwej dla $x > 0$. Ponieważ, zgodnie z Z12.7, $\lim_{x\to\infty} \sum_{k\in\mathcal{B}_x} \frac{1}{k} = \infty$, więc mamy sprzeczność. □

U w a g a 1. Zbiór obszerny jest zbiorem nieskończonym. To jest oczywiste. Dzięki T12.6 widzimy więc (po raz kolejny!), że $\mathrm{card}(\mathbb{P}) = \infty$.

U w a g a 2. Nie wiemy czy zbiór $\mathbb{P}_{\mathrm{twin}}$ liczb pierwszych bliźniaczych (zobacz 2.3.3 P1) jest nieskończony. Wiemy, że *jest on zbiorem szczupłym*. Udowodnił to Viggo Brun (1919). Zatem

$$\sum_{p\in\mathbb{P}_{\mathrm{twin}}} \frac{1}{p} < M \tag{12.26}$$

dla pewnej stałej M. Udowodniono później, że można przyjąć $M = 1,71$, zobacz [**6**].

U w a g a 3. *Zbiór kwadratów jest szczupły*. Można zapytać o w a r t o ś ć $\zeta(2)$ (pytanie znane jako ***problem bazylejski***). Ustęp zakończymy pięknym rozwiązaniem tego problemu:

TWIERDZENIE 12.7 (***Euler* – 1735**) *Zachodzi równość* $\boxed{\zeta(2) = \pi^2/6.}$

D O W Ó D. (1) Pokażemy najpierw "trygonometryczne" przybliżenie liczb $h_n(2)$. Wystartujemy od znanej nierówności $\sin x < x < \mathrm{tg}\, x$ prawdziwej dla wszystkich $x \in (0; \frac{\pi}{2})$. Prosty dowód znaleźć można w każdym podręczniku analizy matematycznej, również w $\mathbb{RIN}$. Nierówność tę zapiszemy w r ó w n o w a ż n e j postaci

$$\mathrm{ctg}^2 x < \frac{1}{x^2} < 1 + \mathrm{ctg}^2 x.$$

Kładąc tu kolejno $x = x_k = \frac{k\pi}{2n+1}$ (dla $k = 1, 2, \ldots, n$) i dodając stronami, dostajemy

$$\sum_{k=1}^{n} \left(\mathrm{ctg}\, \frac{k\pi}{2n+1} \right)^2 < \frac{(2n+1)^2}{\pi^2} \sum_{k=1}^{n} \frac{1}{k^2} < n + \sum_{k=1}^{n} \left(\mathrm{ctg}\, \frac{k\pi}{2n+1} \right)^2. \tag{12.27}$$

(2) Obliczymy występującą po obu stronach powyższych nierówności sumę $\sum_{k=1}^{n} \operatorname{ctg}^2 x_k$. W tym celu pokażemy wielomian, którego pierwiastkami są liczby $\operatorname{ctg}^2 x_k$ i zastosujemy wzór Viète'*a* (na sumę pierwiastków wielomianu).

Tym wielomianem jest wielomian

$$Q_n(X) = \binom{2n+1}{1} X^n - \binom{2n+1}{3} X^{n-1} + \binom{2n+1}{5} X^{n-2} - \ldots .$$

Aby to zobaczyć przekształcimy wzór de Moivre'*a*: $(\sin\varphi)^m(\operatorname{ctg}\varphi + i)^m = \cos m\varphi + i \sin m\varphi$. Następnie, kładąc $m = 2n+1$, zastosujemy wzór dwumienny (1.7) i porównamy części urojone:

$$\frac{\sin(2n+1)\varphi}{(\sin\varphi)^{2n+1}} = \binom{2n+1}{1} (\operatorname{ctg}^2\varphi)^n - \binom{2n+1}{3} (\operatorname{ctg}^2\varphi)^{n-1} + \binom{2n+1}{5} (\operatorname{ctg}^2\varphi)^{n-2} - \ldots .$$

Stąd widzimy, że każda z n (różnych!) liczb $\operatorname{ctg}^2 x_k$, dla $k = 1, 2, \ldots, n$, jest pierwiastkiem wielomianu n-tego stopnia $Q_n(X)$. Wobec tego i wzoru Viète'*a*:

$$\sum_{k=1}^{n} \operatorname{ctg}^2 x_k = \frac{\binom{2n+1}{3}}{\binom{2n+1}{1}} = \frac{n(2n-1)}{3}. \tag{12.28}$$

(3) Udowodniona równość (12.28) pozwala przekształcić nierówności (12.27):

$$\frac{n(2n-1)}{3(2n+1)^2} \cdot \pi^2 \;<\; h_n(2) \;<\; \frac{3n+n(2n-1)}{3(2n+1)^2} \cdot \pi^2.$$

Twierdzenie o trzech ciągach kończy rozumowanie. □

U w a g a 4. Euler udowodnił więcej: $\zeta(2m) = \dfrac{(-1)^{m-1} B_{2m}}{2 \cdot (2m)!} (2\pi)^{2m}$ dla każdego $m \in \mathbb{N}$. B_{2m} oznacza tu liczbę Bernoulli'*ego*. N i e znamy podobnych wyrażeń dla $\zeta(2m+1)$.

Ćwiczenie. Udowodnić, że $\sum_{k\in\mathbb{N}} (2k-1)^{-2} = \pi^2/8$.

12.3.3 Liczby harmoniczne. Twierdzenie Wolstenholme'*a*

Sumę $h_n = h_n(1)$ nazwiemy n-tą **liczbą harmoniczną**. Mamy więc

$$h_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} = \frac{A(n)}{B(n)}. \tag{12.29}$$

Umawiamy się w takiej sytuacji, że ułamek $\frac{A(n)}{B(n)}$ jest nieskracalny, tzn. że $A(n) \perp B(n)$.

ZADANIE 12.8 Udowodnić, że $h_n \notin \mathbb{N}$ dla $n > 1$.

R o z w i ą z a n i e. Niech k oznacza taki wykładnik, że $2^k \leqslant n < 2^{k+1}$. Niech m będzie najmniejszą wspólną wielokrotnością wszystkich liczb $1, 2, \ldots, n$ z w y j ą t k i e m 2^k. Wtedy $m\,h_n = m + \frac{m}{2} + \ldots + \frac{m}{n}$. Jasne, że wszystkie, z w y j ą t k i e m $m/2^k$, składniki po prawej stronie tej równości są liczbami całkowitymi. Gdyby więc h_n było liczbą całkowitą, to mielibyśmy sprzeczność. ◊

Ćwiczenie 12.39 Udowodnić, że $B(n) > \frac{n}{2}$ dla każdego $n \in \mathbb{N}$. *Wskazówka.* Jeżeli k jest takie jak w rozwiązaniu zadania Z12.8, to 2^k jest dzielnikiem $B(n)$, więc $n/2 < 2^k \leqslant B(n)$.

Ćwiczenie 12.40 Czy różnica $h_n - h_m$ może być liczbą całkowitą?

Ćwiczenie 12.41 Niech $a_1, a_2, \ldots, a_n$, przy $n \geqslant 2$, będą niezerowymi liczbami całkowitymi. Załóżmy, że istnieje taka liczba pierwsza p, że

$$v_p(a_i) > \max_{j \neq i} \{v_p(a_j)\}$$

dla pewnego $i \in [\,n\,]$. Udowodnić, że liczba $1/a_1 + 1/a_2 + \ldots + 1/a_n$ nie jest liczbą całkowitą.

Interesują nas arytmetyczne własności liczników liczb harmonicznych (i podobnych do nich). Dla wygodniejszego zapisywania takich własności u m a w i a m y się, że jeżeli w jest liczbą wymierną, to napis $w \equiv 0 \,(\mathrm{mod}\, m)$ oznacza, że $m|a$, gdzie $\frac{a}{b}$ jest ułamkiem nieskracalnym równym w. [Poprawność tej umowy wynika z C2.18.] Czytelnik s p r a w d z i, że jeżeli dla liczb wymiernych w, u zachodzi $w \equiv 0 \,(\mathrm{mod}\, m)$ i $u \equiv 0 \,(\mathrm{mod}\, m)$, to $w + u \equiv 0 \,(\mathrm{mod}\, m)$.

LEMAT 12.1 *Ustalmy $m \in \mathbb{N}$. Dane są liczby $a_j, b_j \in \mathbb{Z}_{\neq 0}$, przy czym $b_j \perp m$ dla każdego $j = 1, 2, \ldots, s$. Wówczas*

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} + \ldots + \frac{a_s}{b_s} \equiv 0 \,(\mathrm{mod}\, m) \tag{12.30}$$

wtedy i tylko wtedy, gdy

$$a_1 b_1^{-1} + a_2 b_2^{-1} + \ldots + a_n b_n^{-1} \equiv 0 \,(\mathrm{mod}\, m),$$

gdzie b_j^{-1} oznacza odwrotność b_j modulo m.

D O W Ó D. Zapiszmy sumę z lewej strony (12.30) w postaci ułamka nieskracalnego

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} + \ldots + \frac{a_s}{b_s} = \frac{A}{B}.$$

Równość ta może być zapisana w postaci

$$A b_1 b_2 \cdot \ldots \cdot b_s = B(a_1 b_2 b_3 \cdot \ldots \cdot b_s + b_1 a_2 b_3 \cdot \ldots \cdot b_s + \ldots + b_1 b_2 \cdot \ldots \cdot a_s).$$

Stąd, wobec względnej pierwszości $A \perp B$, $b_j \perp m$ i ZTA, widzimy, że

$$A \equiv 0 \,(\mathrm{mod}\, m) \Longleftrightarrow a_1 b_2 b_3 \cdot \ldots \cdot b_s + b_1 a_2 b_3 \cdot \ldots \cdot b_s + \ldots + b_1 b_2 \cdot \ldots \cdot a_s \equiv 0 \,(\mathrm{mod}\, m).$$

Wystarczy teraz pomnożyć obie strony drugiej z tych kongruencji przez odwracalny $(\mathrm{mod}\, m)$ iloczyn $b_1^{-1} b_2^{-1} \cdot \ldots \cdot b_s^{-1}$. □

Ćwiczenie 12.42 Niech $\{r_1, r_2, \ldots, r_{p-1}\}$, gdzie $p \in \mathbb{P}_{\geqslant 3}$, będzie dowolnym zredukowanym układem reszt modulo p. Udowodnić, że

$$\frac{1}{r_1} + \frac{1}{r_2} + \ldots + \frac{1}{r_{p-1}} \equiv 0 \,(\mathrm{mod}\, p).$$

Z ćwiczenia C12.42 widzimy, że $h_{p-1} \equiv 0 \,(\mathrm{mod}\, p)$ dla dowolnej liczby pierwszej $p \geqslant 3$. Okazuje się, że dla $p \geqslant 5$ można udowodnić więcej:

TWIERDZENIE 12.8 (***Twierdzenie Wolstenholme'a* – 1862**) *Jeżeli $p \geqslant 5$ jest liczbą pierwszą, to zachodzi kongruencja:*

$$\boxed{1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} \equiv 0 \,(\mathrm{mod}\, p^2).}$$

D O W Ó D. Grupując składniki sumy h_{p-1} w pary, otrzymamy:

$$h_{p-1} = \sum_{k=1}^{s} \left(\frac{1}{k} + \frac{1}{p-k} \right) = p \left(\frac{1}{1 \cdot (p-1)} + \frac{1}{2 \cdot (p-2)} + \ldots + \frac{1}{s \cdot (s+1)} \right),$$

gdzie $s = \frac{p-1}{2}$. Wszystkie mianowniki $k(p-k)$ występujących tu ułamków są niezerowymi *minus kwadratami* modulo p: $k(p-k) \equiv -k^2 \,(\mathrm{mod}\, p)$. Ich odwrotnościami modulo p są więc również *minus kwadraty* modulo p. Ponieważ jest ich s, czyli tyle ile występuje niezerowych *minus kwadratów* modulo p, więc te odwrotności $(k(p-k))^{\sim}$, $k = 1, 2, \ldots, s$, stanowią permutację ciągu $(-1^2) \,(\mathrm{mod}\, p)$, $(-2^2) \,(\mathrm{mod}\, p)$, $\ldots$, $(-s^2) \,(\mathrm{mod}\, p)$ niezerowych *minus kwadratów* modulo p. Z drugiej strony

$$\frac{p(p-1)(2p-1)}{6} = \sum_{j=1}^{p-1} j^2 = \sum_{j=1}^{s} j^2 + \sum_{j=1}^{s} (p-j)^2 \equiv 2 \sum_{j=1}^{s} j^2 \,(\mathrm{mod}\, p).$$

Zatem (pamiętamy, że $p > 3$)

$$\sum_{k=1}^{s} (k(p-k))^{\sim} \equiv \sum_{k=1}^{s} (-k^2)^{\sim} \equiv -\sum_{j=1}^{s} j^2 \equiv -2^{-1} \cdot \frac{p(p-1)(2p-1)}{6} \equiv 0 \,(\mathrm{mod}\, p).$$

To, na mocy L12.1, kończy rozwiązanie. □

U w a g a. W trakcie dowodu T12.8 pokazaliśmy, że dla każdej liczby pierwszej $p \geqslant 5$

$$\boxed{1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{(p-1)^2} \equiv 0 \,(\mathrm{mod}\, p).} \tag{12.31}$$

Na tę kongruencję również zwrócił uwagę Wolstenholme.

12.4 Współczynniki dwumienne

Ustęp ten poświęcamy kilku teorioliczbowym aspektom współczynników dwumiennych.

12.4.1 Wielomiany Newtona

Określone niżej wielomiany nazwaliśmy (tu) nazwiskiem Newtona. Wielomiany Newtona przyjmują tylko wartości całkowite dla całkowitych wartości argumentu.

Definicja 12.3 Niech m będzie liczbą naturalną. Wielomian m-tego stopnia

$$N_m(X) = \frac{1}{m!}X(X-1)\cdot\ \ldots\ \cdot(X-m+1)$$

nazwiemy m-tym **wielomianem Newtona**. Kładziemy też $N_0(X) = 1$.

Wielomiany Newtona mają współczynniki wymierne, na przykład

$$N_1(X) = X, \quad N_2(X) = \tfrac{1}{2}X^2 - \tfrac{1}{2}X, \quad N_3(X) = \tfrac{1}{6}X^3 - \tfrac{1}{2}X^2 + \tfrac{1}{3}X.$$

Mają jednak pewną sympatyczną własność, mianowicie, przyjmują wartości c a ł k o w i t e dla wszystkich całkowitych wartości argumentu:

Ćwiczenie 12.43 Udowodnić, że jeżeli $a \in \mathbb{Z}$, to $N_m(a) \in \mathbb{Z}$.

W istocie wielomiany Newtona są w pewnym sensie jedynymi wielomianami przyjmującymi tylko wartości całkowite dla całkowitych wartości argumentu. Dokładniej:

Ćwiczenie 12.44 Udowodnić, że jeżeli wielomian $f(X) \in \mathbb{R}[X]$ stopnia n przyjmuje wartości całkowite dla każdej całkowitej wartości argumentu, to istnieją takie liczby całkowite $a_0, a_1, \ldots, a_n$, że $f(X) = a_0N_0(X) + a_1N_1(X) + a_2N_2(X) + \ldots + a_nN_n(X)$. Ponadto, liczby $a_0, a_1, \ldots, a_n$ są wyznaczone jednoznacznie.

12.4.2 Twierdzenie Lucas'*a*

Wartość $N_k(n)$ dla $0 \leqslant k \leqslant n$, oznaczana $\binom{n}{k}$, nazywa się **współczynnikiem** (**symbolem**) **dwumiennym** (Newtona). Jasne, że $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, zobacz $\mathbb{KOM}$. Głównym wynikiem tego ustępu jest twierdzenie Lucas'*a* dające resztę z dzielenia współczynnika dwumiennego przez daną liczbę pierwszą p w terminach cyfr p-kowych jego licznika i mianownika.

TWIERDZENIE 12.9 (***Twierdzenie Lucas'a***) *Niech p będzie liczbą pierwszą. Niech*

$$\begin{cases} n = a_0 + a_1p + a_2p^2 + \ \ldots\ + a_rp^r, \\ k = b_0 + b_1p + b_2p^2 + \ \ldots\ + b_rp^r \end{cases}$$

będą przedstawieniami liczb całkowitych nieujemnych k, n w systemie pozycyjnym przy podstawie p. Wówczas zachodzi kongruencja:

$$\binom{n}{k} \equiv \binom{a_r}{b_r}\cdot\binom{a_{r-1}}{b_{r-1}}\cdot\ \ldots\ \cdot\binom{a_0}{b_0} \pmod{p}. \tag{12.32}$$

D O W Ó D. Zauważmy najpierw, że na mocy wzoru dwumiennego (1.7) i C2.50,

$$(1+X)^{p^s} \equiv 1 + X^{p^s} \,(\mathrm{mod}\, p).$$

Oznaczenie $F(X) \equiv G(X) \,(\mathrm{mod}\, p)$ wprowadziliśmy w ustępie 5.4.4. Stąd

$$(1+X)^n \equiv (1+X)^{a_0}(1+X^p)^{a_1} \cdot \ldots \cdot (1+X^{p^r})^{a_r} \,(\mathrm{mod}\, p).$$

Zatem, znowu dzięki dwumianowi Newtona,

$$(1+X)^n \equiv \left(\sum_{j_0=0}^{a_0} \binom{a_0}{j_0} X^{j_0}\right)\left(\sum_{j_1=0}^{a_1} \binom{a_1}{j_1} X^{pj_1}\right) \cdot \ldots \cdot \left(\sum_{j_r=0}^{a_r} \binom{a_r}{j_r} X^{p^r j_r}\right) \,(\mathrm{mod}\, p).$$

Ponieważ k ma jednoznaczne przedstawienie w systemie pozycyjnym przy podstawie p, więc współczynnik przy X^k w ostatnim iloczynie równy jest $\binom{a_r}{b_r} \cdot \binom{a_{r-1}}{b_{r-1}} \cdot \ldots \cdot \binom{a_0}{b_0}$. Porównując współczynniki po obu stronach ostatniej kongruencji otrzymujemy (12.32). □

Ćwiczenie 12.45 Udowodnić, że wszystkie wyrazy n-tego wiersza trójkąta Pascala są liczbami nieparzystymi wtedy i tylko wtedy, gdy n jest postaci $2^k - 1$.

ZADANIE 12.9 Niech p będzie liczbą pierwszą, $s \in \mathbb{N}$. Udowodnić, że

$$\binom{p^s}{p} \equiv p^{s-1} \,(\mathrm{mod}\, p^s).$$

R o z w i ą z a n i e. Z oczywistej równości $p\binom{p^s}{p} = p^s\binom{p^s-1}{p-1}$ mamy

$$\binom{p^s}{p} = p^{s-1}\binom{p^s-1}{p-1}. \tag{12.33}$$

W zapisie liczby $k = p-1$ przy podstawie p mamy $b_0 = p-1$ oraz $b_i = 0$ dla $i > 0$. W zapisie liczby $n = p^s - 1$ cyfry $a_0 = a_1 = \ldots = a_{s-1} = p-1$ i $a_i = 0$ dla $i \geqslant s$. Stąd, na podstawie formuły Lucas'*a*,

$$\binom{p^s-1}{p-1} \equiv \left(\binom{p-1}{0}\right)^{s-1} \cdot \binom{p-1}{p-1} \equiv 1 \,(\mathrm{mod}\, p).$$

To, dzięki (12.33), pozwala skończyć rozwiązanie (zróbcie to!). ◊

Ćwiczenie 12.46 Udowodnić, że jeżeli p jest liczbą pierwszą, to dla $0 \leqslant r \leqslant p-1$ zachodzi kongruencja:

$$\binom{p-1}{r} \equiv (-1)^r \,(\mathrm{mod}\, p). \tag{12.34}$$

Wyprowadzić stąd ***uproszczony wzór dwumienny modulo*** p:

$$(x-y)^{p-1} \equiv \sum_{r=0}^{p-1} x^r y^{p-1-r} \,(\mathrm{mod}\, p),$$

dla dowolnych liczb całkowitych x, y.

12.4.3 Twierdzenie Wolstenholme'*a*-Glaishera

Jeżeli p jest liczbą pierwszą, to natychmiastowym wnioskiem z twierdzenia Lucas'*a* jest kongruencja $\binom{np}{mp} \equiv \binom{n}{m} \pmod p$ dla dowolnych liczb naturalnych $m \leqslant n$. W tym ustępie udowodnimy, że taka kongruencja zachodzi modulo p^3.

Teza poniższego zadania jest przypadkiem szczególnym i jednocześnie ważnym krokiem w dowodzie twierdzenia ogólnego.

ZADANIE 12.10 Udowodnić, że dla każdej liczby pierwszej $p \geqslant 5$,

$$\binom{2p}{p} \equiv 2 \pmod{p^3}. \tag{12.35}$$

R o z w i ą z a n i e. Zauważmy najpierw, że kongruencja $\binom{2p}{p} \equiv 2 \pmod p$ wynika natychmiast z twierdzenia Lucas'*a*. Mocniejszą kongruencję $\binom{2p}{p} \equiv 2 \pmod{p^2}$ łatwo udowodnić korzystając z równości

$$\binom{2p}{p} = \binom{p}{0}^2 + \binom{p}{1}^2 + \ldots + \binom{p}{p}^2, \tag{12.36}$$

(patrz tożsamość Cauchy'*ego*-Vandermonde'*a* w 3.1 P1 dla $m = n = r = p$) i ćwiczenia C2.50. My chcemy dostać więcej. Robimy to tak: Równość (12.36) można przepisać do postaci

$$\binom{2p}{p} - 2 = \sum_{k=1}^{p-1} \left(\frac{p}{k}\binom{p-1}{k-1}\right)^2 = p^2 \sum_{k=1}^{p-1} \left(\frac{1}{k}\binom{p-1}{k-1}\right)^2.$$

Korzystaliśmy tu z oczywistej ***tożsamości pochłaniania*** $\frac{a}{b}\binom{a-1}{b-1} = \binom{a}{b}$, zobacz też $\mathbb{KOM}$. Dla zakończenia rozwiązania musimy więc wykazać, że

$$\sum_{k=1}^{p-1} \frac{1}{k^2}\binom{p-1}{k-1}^2 \equiv 0 \pmod p.$$

Lub, korzystając z (12.34) i lematu L12.1, że

$$\sum_{k=1}^{p-1} (k^2)^{-1}(-1)^{2(k-1)} \equiv 0 \pmod p,$$

a to jest znaną nam kongruencją Wolstenholme'*a* (12.31). Rozwiązanie jest skończone. ◊

Ćwiczenie 12.47 Uzasadnić, że $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$ dla każdej liczby pierwszej $p \geqslant 5$.

Udowodnimy teraz piękne uogólnienie kongruencji (12.35). Dowód będzie polegał na sprytnej kombinatorycznej redukcji do przypadku szczególnego. Jednym z elementów tej redukcji jest kombinatoryczna interpretacja liczby $\binom{2n}{n} - 2$:

Ćwiczenie 12.48 Dany jest zbiór $A = A_1 \sqcup A_2$ przedstawiony w postaci sumy rozłącznej dwóch podzbiorów n-elementowych. Udowodnić, że liczba takich n-elementowych podzbiorów zbioru A, które zawierają co najmniej jeden element z podzbioru A_1 i co najmniej jeden element z podzbioru A_2, wynosi $\binom{2n}{n} - 2$. *Wskazówka.* Zobacz kombinatoryczny dowód tożsamości Cauchy'*ego*-Vandermonde'*a* w $\mathbb{KOM}$.

TWIERDZENIE 12.10 (***Twierdzenie Glaishera***) *Dla dowolnych liczb całkowitych* $0 \leqslant m \leqslant n$ *i dowolnej liczby pierwszej* $p \geqslant 5$ *zachodzi kongruencja*

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3}. \tag{12.37}$$

D O W Ó D. Niech $A = A_1 \sqcup A_2 \sqcup \ldots \sqcup A_n$ będzie zbiorem np-elementowym przedstawionym w postaci sumy n rozłącznych podzbiorów $A_j = \{a_0^{(j)}, a_1^{(j)}, \ldots, a_{p-1}^{(j)}\}$. Jeżeli $B = \{a_{i_1}^{(j)}, a_{i_2}^{(j)}, \ldots, a_{i_s}^{(j)}\}$ jest dowolnym niepustym podzbiorem zbioru A_j, to dla dowolnego $k \in \mathbb{Z}/p$ kładziemy

$$k + B := \{a_{k+i_1}^{(j)}, a_{k+i_2}^{(j)}, \ldots, a_{k+i_s}^{(j)}\}.$$

To oznacza, że, po utożsamieniu (za pomocą dolnych indeksów) elementów zbioru A_j z elementami grupy $\mathbb{Z}/p$, dodajemy k do wszystkich elementów zbioru B. Każdy podzbiór $X \subseteq A$ wyznacza i jest (jednoznacznie) wyznaczony przez ciąg

$$X_1 := X \cap A_1,\ X_2 := X \cap A_2,\ \ldots,\ X_n := X \cap A_n$$

przekrojów z kolejnymi zbiorami A_j. Dwa podzbiory $X, Y \subseteq A$ nazwiemy *równoważnymi*, $X \sim Y$, gdy istnieje taki ciąg $\kappa = (k_1, k_2, \ldots, k_n) \in (\mathbb{Z}/p)^n$, że $\kappa + X = Y$, przy czym

$$\kappa + X = (k_1 + X_1) \sqcup (k_2 + X_2) \sqcup \ldots \sqcup (k_n + X_n).$$

Umawiamy się oczywiście, że jeżeli $B \subseteq A_j$ jest pustym podzbiorem zbioru A_j, to $k + B$ jest również pustym podzbiorem zbioru A_j. Liczba $\binom{np}{mp}$ oznacza moc rodziny wszystkich podzbiorów mp-elementowych zbioru A. Wszystkie zbiory $X \in \mathcal{P}_{mp}(A)$ podzielimy na typy: Taki zbiór X jest typu r, gdy wśród zbiorów $X_1, X_2, \ldots, X_n$ jest dokładnie r właściwych (podzbiór $B \subseteq A_i$ nazywamy tu *właściwym*, gdy jest niepusty i nie równy A_i). Po tych ustaleniach Czytelnik udowodni poniższe fakty:

F a k t 1: *Jeżeli* $X \in \mathcal{P}_{mp}(A)$ *jest podzbiorem typu* r, *to w klasie abstrakcji* $[X]_\sim$ *jest dokładnie* p^r *elementów.*

F a k t 2: *Podzbiorów* $X \in \mathcal{P}_{mp}(A)$ *typu* 0 *jest dokładnie* $\binom{n}{m}$.

F a k t 3: *Żaden podzbiór* $X \in \mathcal{P}_{mp}(A)$ *n i e jest typu* 1.

F a k t 4: *Podzbiorów* $X \in \mathcal{P}_{mp}(A)$ *typu* 2 *jest*

$$\binom{n}{2}\binom{n-2}{m-1} \cdot \left[\binom{2p}{p} - 2\right].$$

[W dowodzie F a k t u 4 korzystamy z C12.48.] Z tych czterech faktów dostajemy równość:

$$\binom{np}{mp} = \binom{n}{m} + \binom{n}{2}\binom{n-2}{m-1} \cdot \left[\binom{2p}{p} - 2\right] + p^3 \cdot \text{coś}, \tag{12.38}$$

z której, dzięki (12.35), natychmiast dostajemy kongruencję (12.37). □

* * * ∞ ∞ ∞ * * *

Na zakończenie proponujemy ćwiczenie-problem:

Ćwiczenie 12.49 Załóżmy, że dany jest NWD-ciąg $\boldsymbol{a} = (a_n)$ o wyrazach należących do $\mathbb{N}$ (por. C2.76, T9.1 czy C9.25). Definiujemy ciąg $(A_n)_{n\geqslant 0}$: $A_0 = 1$ i $A_n = a_1 a_2 \cdot \ldots \cdot a_n$ dla $n \in \mathbb{N}$. Definiujemy wreszcie

$$\binom{n}{k}_{\boldsymbol{a}} := \frac{A_n}{A_k\, A_{n-k}}. \tag{12.39}$$

Udowodnić, że liczby $\binom{n}{k}_{\boldsymbol{a}}$ są liczbami całkowitymi. Udowodnić jak najwięcej własności tak określonych **$\boldsymbol{a}$-współczynników dwumiennych**. *Uwaga.* Gdy $\boldsymbol{a} = (f_n)$ jest ciągiem liczb Fibonacci'*ego*, liczby (12.39) nazywamy **współczynnikami dwumiennymi Fibonacci'*ego*** i oznaczamy $\binom{n}{k}_{\mathrm{Fib}}$. Gdy zaś $\boldsymbol{a} = (q^n - 1)_{n\geqslant 1}$, przy $q \in \mathbb{N}_{\geqslant 2}$, liczby (12.39) nazywamy **q-współczynnikami dwumiennymi** (oznaczenie $\binom{n}{k}_q$).

12.5 Rozmieszczenie liczb pierwszych

Wiemy, że liczb pierwszych jest nieskończenie wiele. Przytoczymy teraz cztery twierdzenia mówiące trochę więcej o rozmieszczeniu liczb pierwszych na osi liczbowej. Dla danej liczby rzeczywistej $x > 0$ przez $\pi(x)$ oznaczamy liczbę liczb pierwszych mniejszych lub równych x. Tak określona funkcja π jest jedną z trudniej "badalnych" funkcji w całej matematyce. Twierdzenie Euklidesa z ustępu 2.3.2 jest równoważne z faktem, że $\pi(x)$ rośnie do nieskończoności, gdy $x \longrightarrow \infty$. Nierówność (2.20) pokazuje, że $\pi(x)$ rośnie co najmniej tak szybko jak logarytm (pomnożony przez stałą $\frac{1}{2\log 2}$). W tym paragrafie udowodnimy twierdzenie Czebyszewa, z którego między innymi wynika, że w rzeczywistości funkcja $\pi(x)$ rośnie do nieskończoności zdecydowanie szybciej.

12.5.1 Dwa twierdzenia Czebyszewa

Ten ustęp poświęcamy na dowód dwóch twierdzeń Czebyszewa. W ich dowodzie wykorzystamy kilka prostych własności arytmetyczno-wielkościowych liczb $\binom{n}{k}$.

Będziemy oznaczać przez $v_p(n,k)$ wykładnik p-adyczny liczby $\binom{n}{k}$. Jasne, że $v_p(n,k) = v_p(n!) - v_p(k!) - v_p((n-k)!)$, więc, na mocy formuły Legendre'*a* z T2.17,

$$v_p(n,k) = \sum_{e=1}^{\infty} \left(\left\lfloor \frac{n}{p^e} \right\rfloor - \left\lfloor \frac{k}{p^e} \right\rfloor - \left\lfloor \frac{n-k}{p^e} \right\rfloor \right). \tag{12.40}$$

ZADANIE 12.11 Dowieść, że jeżeli p jest liczbą pierwszą, a $1 \leqslant k \leqslant p^s - 1$, to $p \mid \binom{p^s}{k}$.

Rozwiązanie. Połóżmy $n = p^s$ w (12.40). Wiemy, że dla dowolnych $x, y \in \mathbb{R}$ liczba $\lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor$ jest równa 0 lub 1, zobacz C12.1.5. Więc wszystkie składniki sumy (12.40) są $\geqslant 0$, a składnik s-ty jest równy $1 - 0 - 0 = 1$. Stąd $v_p(p^s, k) \geqslant 1$. ◊

ZADANIE 12.12 Dowieść, że jeżeli $\binom{n}{k} = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ jest kanonicznym rozkładem na czynniki pierwsze, to dla każdego $i = 1, \ldots, s$ zachodzi nierówność $p_i^{e_i} \leqslant n$.

Rozwiązanie. Niech, dla danego i, liczba całkowita r będzie (jednoznacznie) wyznaczona z nierówności $p_i^r \leqslant n < p_i^{r+1}$. Kładąc w (12.40) $p = p_i$ widzimy, tak jak wyżej, że $e_i = v_{p_i}(n,k)$ jest sumą r liczb równych 1 lub 0. Stąd $e_i \leqslant r$, więc $p_i^{e_i} \leqslant p_i^r \leqslant n$. ◊

ZADANIE 12.13 Dowieść, że dla dowolnych $0 \leqslant k \leqslant n$ zachodzi nierówność $\binom{n}{k} \leqslant 2^n$.

Rozwiązanie. Wynika z równości $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, zobacz $\mathbb{KOM}$. $\Diamond$

ZADANIE 12.14 Dowieść, że dla dowolnego $n \in \mathbb{N}$ zachodzi nierówność $\binom{2n+1}{n} < 4^n$.

Rozwiązanie. Wynika z faktu, że r ó w n e liczby $\binom{2n+1}{n}$ i $\binom{2n+1}{n+1}$ są składnikami, równej 2^{2n+1}, sumy $\sum_{k=0}^{2n+1} \binom{2n+1}{k}$. $\Diamond$

ZADANIE 12.15 Dowieść, że dla dowolnego $n \in \mathbb{N}$ zachodzi nierówność $\binom{2n}{n} \geqslant 4^n/2n$.

Rozwiązanie. Wiadomo, zobacz na przykład $\mathbb{KOM}$ C1.26, że $\binom{2n}{n}$ jest największym ze wszystkich współczynników dwumiennych występujących w $2n$-tym wierszu trójkąta Pascala. Po odjęciu dwóch skrajnych jedynek ($\binom{2n}{0} = \binom{2n}{2n} = 1$), mamy więc

$$\frac{2^{2n} - 2}{2n - 1} \leqslant \binom{2n}{n},$$

bo średnia arytmetyczna jest niewiększa niż maksimum. Wystarczy więc udowodnić, że lewa strona powyższej nierówności jest $\geqslant 4^n/2n$, co jest natychmiastowe. $\Diamond$

Udowodnimy metodą Erdősa następujący lemat:

LEMAT 12.2 *Iloczyn wszystkich liczb pierwszych niewiększych niż dana liczba $x \geqslant 2$ jest mniejszy niż 4^x. To znaczy,*

$$\prod_{p \leqslant x} p < 4^x.$$

D O W Ó D. Oznaczmy przez $P(n)$ iloczyn wszystkich liczb pierwszych niewiększych niż $n \geqslant 2$. Dowodzimy przez indukcję względem $n \geqslant 2$ mocniejszej tezy, że $P(n) \leqslant 4^{n-1}$. Baza indukcji jest oczywista. Załóżmy więc, że $P(k) \leqslant 4^{k-1}$ dla wszystkich $2 \leqslant k \leqslant n-1$ i rozważmy iloczyn $P(n)$. Zachodzi jedna z możliwości: albo $n = 2k$, i wtedy $P(n) = P(n-1) \leqslant 4^{n-2} \leqslant 4^{n-1}$, albo $n = 2k+1$. W tym przypadku zapiszmy:

$$P(n) = P(2k+1) = P(k+1) \cdot p_1 p_2 \cdot \ldots \cdot p_s, \tag{12.41}$$

gdzie przez $p_1, \ldots, p_s$ oznaczyliśmy wszystkie liczby pierwsze z przedziału $(k+1;\, 2k+1]$. Zauważmy, że wszystkie te liczby dzielą licznik ułamka $\frac{(2k+1)!}{k!(k+1)!}$ ale nie(!) dzielą mianownika tego ułamka. Wobec tego $p_1 p_2 \cdot \ldots \cdot p_s | \binom{2k+1}{k}$, skąd $p_1 p_2 \cdot \ldots \cdot p_s \leqslant \binom{2k+1}{k}$. Równość (12.41) i założenie indukcyjne $P(k+1) \leqslant 4^k$ dają więc

$$P(n) \leqslant 4^k \cdot \binom{2k+1}{k} \leqslant 4^k \cdot 4^k = 4^{2k} = 4^{n-1}.$$

[Druga nierówność wynika z Z12.14.] To kończy dowód. $\square$

Fizyk francuski Joseph Bertrand, przeglądając tablice liczb pierwszych, wysunął przypuszczenie, że w każdym przedziale $(n;\, 2n\,]$, $n \in \mathbb{N}$, znajdzie się co najmniej jedna liczba pierwsza. Matematyk rosyjski Pafnucy Czebyszew udowodnił, że przypuszczenie Bertrand'*a* jest prawdą. Udowodnimy teraz to twierdzenie Czebyszewa.

TWIERDZENIE 12.11 (***Postulat Bertrand'a***) *Dla każdej liczby naturalnej $n > 1$ istnieje (co najmniej jedna) taka liczba pierwsza p, że $n < p \leqslant 2n$.*

D O W Ó D. Załóżmy, nie wprost, że n jest taką liczbą naturalną, że w przedziale $(\,n;\,2n\,]$ nie(!) ma ani jednej liczby pierwszej. Niech

$$\binom{2n}{n} = (p_1^{e_1} \cdot \ldots \cdot p_s^{e_s})(p_{s+1}^{e_{s+1}} \cdot \ldots \cdot p_{s+t}^{e_{s+t}}) \tag{12.42}$$

będzie kanonicznym rozkładem współczynnika $\binom{2n}{n}$ na czynniki pierwsze. Liczby pierwsze p_i występujące w tym rozkładzie podzieliliśmy na dwie grupy. Do pierwszej grupy należą wszystkie(!) liczby pierwsze z przedziału $(\,1;\,\sqrt{2n}\,]$, do drugiej wszystkie(!) liczby pierwsze z przedziału $(\,\sqrt{2n};\,\frac{2}{3}n\,]$. Łatwo widzieć, że innych liczb pierwszych w rozkładzie współczynnika $\binom{2n}{n}$ na czynniki pierwsze nie ma. Rzeczywiście: każda liczba pierwsza dzieląca $\binom{2n}{n}$ dzieli licznik $(2n)!$, więc jest dzielnikiem któregoś z czynników tej silni, więc jest $\leqslant 2n$, czyli, zgodnie z założeniem nie wprost, $\leqslant n$. Ponadto, jeżeli $p \in (\frac{2}{3}n;\,n]$ jest dzielnikiem pierwszym licznika $(2n)!$ ułamka $\binom{2n}{n} = \frac{(2n)!}{n!\,n!}$, to dzieli go w potędze drugiej (w silni $(2n)!$ występują tylko wielokrotności p i $2p$ liczby p, bo $3p > 2n$), a w mianowniku $n! \cdot n!$ mamy dwa czynniki p.

Z zadania Z12.12 wiemy, że $p_i^{e_i} \leqslant 2n$ dla każdego $i = 1,\,2,\,\ldots,\,s+t$. Jednocześnie

$$(\sqrt{2n})^{e_i} < p_i^{e_i} \leqslant 2n$$

dla $i = s+1,\,\ldots,\,s+t$, bowiem $\sqrt{2n} < p_i$ dla tych i. Stąd wynika, że $e_i \leqslant 1$ dla każdego $i = s+1,\,\ldots,\,s+t$. Biorąc to pod uwagę widzimy, że równość (12.42) ma postać $\binom{2n}{n} = (p_1^{e_1} \cdot \ldots \cdot p_s^{e_s})(p_{s+1} \cdot \ldots \cdot p_{s+t})$ i każdy z początkowych s czynników $p_i^{e_i}$ jest $\leqslant 2n$. Mamy więc

$$\binom{2n}{n} \leqslant (2n)^s \cdot (p_{s+1}p_{s+2} \cdot \ldots \cdot p_{s+t}) \leqslant (2n)^{\sqrt{2n}} \cdot \prod_{p \leqslant \frac{2}{3}n} p \leqslant (2n)^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n}.$$

Druga z tych nierówności wynika z faktu, że $s = \pi(\sqrt{2n}) \leqslant \sqrt{2n}$ (jasne, że $\pi(x) \leqslant x$ dla każdego $x > 0$) i z faktu, że wszystkie liczby pierwsze p_{s+j} są $\leqslant \frac{2}{3}n$. Trzecia zaś z lematu L12.2. Korzystając teraz z Z12.15 otrzymujemy nierówność

$$4^n \leqslant (2n)^{1+\sqrt{2n}} \cdot 4^{\frac{2}{3}n}, \quad \text{równoważnie} \quad 4^{\frac{1}{3}n} \leqslant (2n)^{1+\sqrt{2n}}.$$

W ćwiczeniu C12.50 proponujemy Czytelnikowi sprawdzenie, że nierówność ta nie zachodzi dla $n \geqslant 4000$. Wobec tego: jeżeli w przedziale $(\,n;\,2n\,]$ nie ma liczb pierwszych, to $n < 4000$. Ale to jest sprzeczne z obserwacją, że ciąg

$$2,\,3,\,5,\,7,\,13,\,23,\,43,\,83,\,163,\,317,\,631,\,1259,\,2003,\,4001$$

składa się z liczb pierwszych i że każdy przedział $(\,n;\,2n\,]$, dla $n < 4000$, zawiera co najmniej jeden wyraz tego ciągu. Uzyskana sprzeczność kończy dowód. □

Ćwiczenie 12.50 Udowodnić, że jeżeli $4^{\frac{1}{3}n} \leqslant (2n)^{1+\sqrt{2n}}$, to $n < 4000$.

Ćwiczenie 12.51 Udowodnić, że jeżeli $n! = m^k$ dla $k,\,m,\,n \in \mathbb{N}$, to $n = 1$ lub $k = 1$.

Ćwiczenie 12.52 Liczbę naturalną $n \geqslant 2$ nazwiemy *miłą*, gdy jest równa sumie wszystkich liczb pierwszych $p < n$. Udowodnić, że jedyną liczbą miłą jest 5.

Ćwiczenie 12.53 Udowodnić, że dla każdego $n \in \mathbb{N}$ istnieje takie rozbicie

$$\{1, 2, \ldots, 2n\} = \{x_1, y_1\} \sqcup \{x_2, y_2\} \sqcup \ldots \sqcup \{x_n, y_n\},$$

że każda liczba $x_i + y_i$ jest liczbą pierwszą.

Przyglądając się wnikliwie tablicom liczb pierwszych (oczywiście znacznie obszerniejszym niż zamieszczona w naszym skrypcie) można zauważyć, że gęstość zbioru liczb pierwszych w zbiorze liczb naturalnych w otoczeniu liczby naturalnej n wynosi około $\frac{1}{\log n}$. To oznacza, że jeżeli k jest dużo mniejszą liczbą naturalną niż n (zapisujemy to: $k \ll n$), to prawdopodobieństwo znalezienia liczby pierwszej w przedziale $[\,n-k;\, n+k\,]$ wynosi w przybliżeniu $\frac{1}{\log n}$ (log oznacza tu i dalej logarytm naturalny). Obserwacja ta sugeruje, że funkcja π powinna w "otoczeniu nieskończoności" zachowywać się podobnie do funkcji $\frac{x}{\log x}$. Poniższe twierdzenie Czebyszewa zdaje się do pewnego stopnia potwierdzać takie przypuszczenie:

TWIERDZENIE 12.12 (***Czebyszew***) *Istnieją takie stałe* $0 < C < 1 < D$, *że*

$$\boxed{C\,\frac{n}{\log n} < \pi(n) < D\,\frac{n}{\log n}} \tag{12.43}$$

dla wszystkich $n \in \mathbb{N}_{\geqslant 2}$.

D O W Ó D. W rozwiązaniu Z4.C1 udowodniliśmy, że stała $D = 6\log 2$ jest dobra. Wskażemy więc teraz stałą C. Ustalmy $n \in \mathbb{N}_{\geqslant 2}$ i weźmy dowolne $k \leqslant n$. Niech $\binom{n}{k} = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ będzie kanonicznym rozkładem na czynniki pierwsze. Wówczas, jak wiemy z Z12.12, $p_i^{e_i} \leqslant n$ dla każdego i. Zatem

$$\binom{n}{k} = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_s^{e_s} \leqslant n^s \leqslant n^{\pi(n)}, \tag{12.44}$$

bo wszystkie liczby pierwsze $p_1, p_2, \ldots, p_s$, jako dzielniki licznika $n!$ ułamka $\frac{n!}{k!(n-k)!}$, są niewiększe niż n, więc ich ilość s jest niewiększa niż $\pi(n)$. Dodając stronami nierówności (12.44) dla wszystkich $k = 0, 1, \ldots, n$, dostajemy

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \leqslant (n+1)n^{\pi(n)}.$$

Stąd, po zlogarytmowaniu, dostajemy nierówność $\frac{n\log 2 - \log(n+1)}{\log n} \leqslant \pi(n)$ dla każdego $n \in \mathbb{N}_{\geqslant 2}$. Czytelnik zechce uzasadnić, że licznik wyrażenia z lewej strony jest większy niż $n\log\frac{2}{\sqrt{3}}$ i, w ten sposób, uzasadnić, że stała $C = \log\frac{2}{\sqrt{3}}$ jest dobra. □

Ćwiczenie 12.54 Uzasadnić, że ciąg $(a_n)_{n\geqslant 2}$ dany wzorem $a_n = \frac{\log(n+1)}{n}$ jest ciągiem malejącym zbieżnym do zera. Wywnioskować stąd, że dla dostatecznie dużych n stałą C z nierówności (12.43) można wybrać równą $2/3$.

U w a g a. Wykazując więcej skrupulatności w takich jak wyżej (i podobnych) szacowaniach, Czebyszew udowodnił, że dla dostatecznie dużych n zachodzi nierówność podwójna:

$$0,92129\,\frac{n}{\log n} < \pi(n) < 1,10555\,\frac{n}{\log n}.$$

Ćwiczenie 12.55 W kryptografii używa się d u ż y c h (to znaczy wielocyfrowych) liczb pierwszych. Czy da się każdemu człowiekowi na Ziemi (dla uproszczenia przyjmijmy, że jest nas 10 miliardów) "przydzielić" milion liczb pierwszych 200-cyfrowych tak, by każdy człowiek dostał inne liczby?

12.5.2 Twierdzenie o liczbach pierwszych

Okazuje się, że zachodzi mocniejsze, tak zwane ***Twierdzenie o Liczbach Pierwszych***:

TWIERDZENIE 12.13 (**PNT**) *Zachodzi następująca równość asymptotyczna*

$$\pi(x) \sim \frac{x}{\log x}\,.$$

To oznacza, że i s t n i e j e (i jest równa 1) granica ilorazu $\pi(x)/\frac{x}{\log x}$ *przy* $x \to \infty$, *tzn.,*

$$\boxed{\boxed{\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.}} \quad \square \tag{12.45}$$

To piękne twierdzenie udowodnili niezależnie od siebie w roku **1896** Jacques Hadamard i Charles de la Vallée Poussin.

Ćwiczenie 12.56 Udowodnić, że istnieje taka liczba B, że jeżeli $x \geqslant B$, to w przedziale $[x;\, \frac{3}{2}x]$ znajdzie się co najmniej 2013 liczb pierwszych.

Charles de la Vallée Poussin udowodnił również poniższe wzmocnienie twierdzenia T5.19:

TWIERDZENIE 12.14 *Dla danych liczb naturalnych względnie pierwszych* a, r, *oznaczmy przez* $\pi_{a,r}(x)$ *liczbę liczb pierwszych niewiększych niż* $x \in \mathbb{R}_{>0}$ *będących wyrazami ciągu arytmetycznego* a, $a+r$, $a+2r$, $a+3r$, $\ldots$. *Wówczas*

$$\boxed{\boxed{\lim_{x\to\infty} \frac{\pi_{a,r}(x)\log x}{x} = \frac{1}{\varphi(r)}.}} \quad \square \tag{12.46}$$

To oznacza, że jeżeli $\{a_1,\, a_2,\, \ldots,\, a_{\varphi(r)}\}$ jest zredukowanym układem reszt modulo r, to w każdym z ciągów arytmetycznych $(a_1+rn)_{n\in\mathbb{Z}}$, $(a_2+rn)_{n\in\mathbb{Z}}$, $\ldots$, $(a_{\varphi(r)}+rn)_{n\in\mathbb{Z}}$ leży nieskończenie wiele i "mniej więcej" tyle samo liczb pierwszych. We wszystkich pozostałych ciągach arytmetycznych o różnicy r leży łącznie skończenie wiele liczb pierwszych.

Literatura

[**0**] Aigner M., Ziegler G. M. *Dowody z Księgi*, PWN, Warszawa 2004.

[**1**] Courant R., Robbins H. *Co to jest matematyka*, PWN, Warszawa 1967.

[**2**] Ireland K., Rosen M. *A Classical Introduction to Modern Number Theory*, Springer.

[**3**] Koblitz N. *Wykład z teorii liczb i kryptografii*, WN-T, Warszawa 1995.

[**4**] Kurlyandchik L. *Złote rybki w oceanie matematyki*, "Tutor", Toruń 2005.

[**5**] Mostowski A., Stark M. *Elementy algebry wyższej*, PWN, Warszawa 1968.

[**6**] Narkiewicz W. *Elementy algebraicznej teorii liczb*, PZWS, Warszawa 1972.

[**7**] Narkiewicz W. *Teoria liczb*, PWN, Warszawa 2003.

[**8**] Rademacher H., Toeplitz O. *O liczbach i figurach*, PWN, Warszawa 1956.

[**9**] Ribenboim P. *Wielkie twierdzenie Fermata dla laików*, WN-T, Warszawa 2001.

[**10**] Sierpiński W. *Arytmetyka teoretyczna*, PWN, Warszawa 1968.

[**11**] Sierpiński W. *Wstęp do teorii liczb*, WSiP, Warszawa 1987.

[**12**] Sierpiński W. *250 zadań z elementarnej teorii liczb*, WSiP, Warszawa 1987.

[**13**] Sierpiński W. *Elementary Theory of Numbers*, PWN, Warszawa 1964.

[**14**] Sierpiński W. *Trójkąty pitagorejskie*, PWN, Warszawa 1954.

[**15**] Sierpiński W. *O rozwiązywaniu równań w liczbach całkowitych*, Warszawa 1956.

[**16**] Sierpiński W. *Liczby trójkątne*, PZWS, Warszawa 1962.

[**17**] Sierpiński W. *O rozkładach liczb wymiernych na ułamki proste*, PWN 1957.

[**18**] Song Y. Yan *Teoria liczb w informatyce*, PWN, Warszawa 2006.

[**19**] Winogradow I. *Elementy teorii liczb*, PWN, Warszawa 1954.

[**20**] Wowk C., Szkibiel G. *Zadania z arytmetyki szkolnej i teorii liczb*, Szczecin 1999.

Indeks

***A**lgebra*, 6
algebra parzystości, 175
algebraiczna teoria liczb, 287
algorytm, 26
— dzielenia z resztą wielomianów, 69
— Euklidesa, 26, 84, 330
— — w pierścieniu normowo-euklidesowym, 341
— Fibonacci'*ego* (zachłanny), 424
analityczna teoria liczb, 162
analiza matematyczna, 75
argument liczby zespolonej, 13
arytmetyczna przestrzeń wektorowa nad ciałem, 240
***a**-współczynnik* dwumienny, 436

***B**aza* indukcji, 3
— definicji indukcyjnej, 5
— przestrzeni liniowej, 123
— — $\mathcal{R}ek(P, Q)$, 310
bikwadrat, 50, 373
binarna forma kwadratowa, 288
biwymierność przekształcenia, 399

***C**echy* podzielności, 159
ciało, 11
— algebraicznie domknięte, 92
— charakterystyki dwa, 77
— $\mathbb{F}_p(=\mathbb{Z}/p)$, 178
— $\mathbb{F}_{p^2}$, 319
— kwadratowe $\mathbb{Q}(\sqrt{D})$, 325
— kwaternionów (Hamiltona), 296
— liczb algebraicznych $\mathbb{A}$, 235
— — rzeczywistych $\mathbb{R}$, 10
— — wymiernych $\mathbb{Q}$, 10
— — zespolonych $\mathbb{C}$, 13
ciąg czysto-okresowy, 198, 265
— Farey'*a*, 251
— Fermat'*a*, 311
— Fibonacci'*ego* klasyczny, 301
— Lucas'*a*, 310
— — klasyczny, 311
— — stowarzyszony, 310
— —, formuły konwersji, 312
— —, tożsamość kwadratowa, 312
— —, uogólnione tożsamości Cesàro, 312
— —, wzór Cassini'*ego*, 312
— Mersenne'*a*, 311
Combinatorial Nullstellensatz, CN, 241
cyfra m-kowa, 417
— po przecinku l-ta, 419
część całkowita liczby rzeczywistej, 412
— rzeczywista liczby zespolonej, 12
— ułamkowa liczby rzeczywistej, 412
— urojona liczby zespolonej, 12
czwórka Catalan'*a*, 58
czynnik kwadratowy wielomianu, 96
— liniowy wielomianu, 96

***D**esant* nieskończony, 80, 125, 160, 274, 366
diagonalizacja macierzy, 314
dodawanie, 8
— liczb całkowitych, 7
— liczb zespolonych, 11
— modulo m, 176
— punktów krzywej eliptycznej, 409
— — płaszczyzny, 277
— w ciele $\mathbb{F}_p(\iota)$, 317
— — grupie addytywnej, 8
— — pierścieniu, 9
— wielomianów jednej zmiennej, 64
dyskretna własność Darboux, 243
działanie dwuargumentowe, 6
— — łączne, przemienne, 7
— rozdzielne względem działania, 7
— składania, 7
dziedzina całkowitości, 11, 354
— ideałów głównych, dig, 21, 83, 341, 366
— z jednoznacznością rozkładu, 347, 358
dzielenie liczb zespolonych, 12
— z resztą liczb całkowitych, 20
— — — — — Gaussa, 327
— — — wielomianów, 68
dzielnik, 18, 82, 328, 340, 355
— pierwotny (wyrazu ciągu), 192

— właściwy, 31
— zera w pierścieniu, 11
dziewiątkowy test poprawności mnożenia, 159

***E**lement* neutralny działania, 8
— nierozkładalny, 357
— — pierścienia kwadratowego, 343
— nieskończonego rzędu (w grupie), 184
— odwrotny w grupie, 8
— odwracalny w pierścieniu, 11
— pierwszy, 358
— — pierścienia kwadratowego, 343
— przeciwny w grupie addytywnej, 8
— (punkt) przeciwny w płaszczyźnie, 277
— rzędu nieskończonego w grupie, 184
— zerowy pierścienia, 9
elementy komutujące w grupie, 185
— stowarzyszone w pierścieniu, 341
— względnie pierwsze, 341, 357
elipsa, 392

***F**igura* centralnie symetryczna, 280
— wypukła, 280
"filozofia" Viète'*a*, 78
forma kwadratowa binarna, 288
— — dodatnio-określona, 291
— — — — zredukowana, 292
— — kanoniczna, 344
— — nieokreślona, 291
— — określona, 291
formalny szereg potęgowy, 308
formuła Legendre'*a*, 37
— Waringa, 230
formuły duplikacji, 411
— konwersji dla ciągów Lucas'*a*, 312
formy kwadratowe równoważne, 288
funkcja arytmetyczna, 143
— — multyplikatywna, 143
— — μ-Möbiusa, 148
— — σ, 145
— — silnie multyplikatywna, 154
— — τ, 144
— — φ-Eulera, 146
— charakterystyczna, 246
— ciągła, 76
— kwadratowa, 75
— różniczkowalna, 225
— symetryczna, 78
— tworząca (ciągu), 231, 309
— wielomianowa, 72
— wymierna jednej zmiennej, 106
— — prosta, 107

***G**enerator* grupy cyklicznej, 196, 320
— ideału, 20
geometria algebraiczna, 241
granica, 225
grupa, 8
— abelowa (= komutatywna, = przemienna), 8
— bijekcji, 9
— cykliczna, 195, 320
— jedności pierścienia, 11
— — pierścienia wielomianów, 81
— multyplikatywna ciała, 320
— pierwiastków z jedynki stopnia n, 15
— symetryczna, 9
— typu addytywnego, 8
— warstw odwracalnych modulo m, 177
grupy izomorficzne, 320

***H**iperbola*, 392
— z mnożeniem, 387
hipoteza Erdősa-Strausa, 422
— Goldbacha, 33

***I**deał*, 20, 83, 329, 341, 356
— generowany przez dwa elementy, 21, 83, 341
— główny, 20, 82, 328, 340, 355
— zerowy, 20
iloczyn prosty (pod)grup, 199
— teoriomnogościowy, 7
— punktu płaszczyzny przez liczbę, 277
iloraz (niepełny), 20, 69, 327
indeks przy podstawie g, 201
indukcja wsteczna, 52
interpretacja piechura liczb Fibonacci'*ego*, 304
inwolucja, 298

***J**ednokładność*, 14
jednomian, 109
jednorodny składnik wielomianu, 110
jedność pierścienia, 11
— trywialna, 361
— fundamentalna, 362
jedynka pierścienia, 9

***K**anoniczne* rozwinięcie liczby rzeczywistej na ułamek łańcuchowy, 253
kanoniczny rozkład na czynniki pierwsze, 36
klasa reszt modulo m, 176
kombinacja liniowa liczb, 21
— — punktów (wektorów), 277

komutujące elementy grupy, 185
kongruencja indyjska, 391
— modulo (według modułu) m, 157
— — μ, 351
— stopnia pierwszego (liniowa), 162
kontynuanta, 256
$\mathbb{K}$-punkty krzywej, 411
krata (podgrupa punktów płaszczyzny), 277
— Eisensteina, 277
— — uogólnione, 91
— Gaussa, 326
krok indukcyjny, 4
— — definicji indukcyjnej, 5
kryterium Eisensteina, 90
— — uogólnione, 91
— Eulera, 204
— Gaussa, 206
— Korselta, 202
krzywa eliptyczna, 403
— stożkowa, 392
— — zdegenerowana, 392
— sześcienna, 398
— — osobliwa, 402
kwadrat w grupie, 203
kwadratura koła, 238
kwaterniony, 294

***L**emat* Gaussa (kryterium Gaussa), 206
— — o wielomianach pierwotnych, 87
— Hensela, 220
— Lagrange'*a*, 290
— o zwiększaniu wykładnika, LZW, 39
liczba algebraiczna (całkowita), 232
— całkowita, 1
— — bezkwadratowa, 34
— — Eisensteina, 351
— — Gaussa, 326
— — p-adyczna, 222
— Carmichaela, 202
— Catalan'*a*, 45
— czysto urojona, 12
— doskonała, 145
— Fermat'*a*, 23
— f-wyróżniona, 161
— Frobeniusa, 30
— harmoniczna (n-ta), 428
— kongruentna, 402
— naturalna, 1
— nierozkładalna Gaussa, 331
— Mersenne'*a*, 35
— Nováka, 46
— odwracalna modulo m, 163
— pierwsza, 31
— — Fermat'*a*, 36
— — Gaussa, 331
— — — leżąca nad p, 336
— — Mersenne'*a*, 35
— — Sophie Germain, 215
— — wymierna, 335
— przedstawialna przez formę kwadratową, 288
— — właściwie przez formę kwadratową, 288
— przestępna, 232
— rozwiązań kongruencji, 161
— rzeczywista, 419
— —, interpretacja arytmetyczna, 419
— —, — geometryczna, 419
— —, zapis pozycyjny, 420
— sprzężona liczby zespolonej, 12
— — niewymierności kwadratowej, 264, 325
— zespolona, 11
— złota, 259
— złożona, 31
liczby Bernoulli'*ego*, 249
— pierwsze bliźniacze, 35
— rzeczywiste równoważne, 262
— stowarzyszone w $\mathbb{Z}[i]$, 328
— trójkątne, 46, 297
— względnie pierwsze, 23, 329
— złote, 259
lokalizacja w liczbie pierwszej, 181
logarytm dyskretny, 201

***M**acierz* odwzorowania liniowego płaszczyzny, 313
— jednostkowa, odwrotna, 261
małe twierdzenie Fermat'*a*, 166
— — — w ciele $\mathbb{F}_{p^2}$, 320
medianta dwóch ułamków, 252
metoda desantu (nieskończonego), 80, 125
— Eulera dowodu WTF(3), 375
— siecznych, 404
— siecznych-stycznych, 403
— stycznych, 405
— zstępowania, 366
metryka w $\mathbb{Z}_p$, 223
mianowniki ułamka łańcuchowego, 253
miejsce zerowe wielomianu, 66
mnożenie liczb całkowitych, 7
— — zespolonych, 11

— macierzy, 314
— modulo m, 176
— w ciele $\mathbb{F}_p(\iota)$, 317
— — pierścieniu, 9
— wielomianów jednej zmiennej, 64
moduł, 157
— liczby zespolonej, 12
MTF, 166
multiwykładnik, 230
multyplikatywność normy w ciałach kwadratowych, 325

N*adpierścień*, 325
najmniejsza wspólna wielokrotność, 25
największy wspólny dzielnik, 22, 83, 329, 341, 357
niereszta kwadratowa modulo m, 203
nierówność Bonse 47
— Schwarza, 76
— trójkąta w $\mathbb{C}$, 12
— — — płaszczyźnie, 277
— — — $\mathbb{Z}_p$ (ultrametryczna), 223
niewymierność kwadratowa, 233, 263
— — zredukowana, 265
— liczby $\sqrt{2}$, 2, 366
nitka p-adyczna, 222
norma niewymierności kwadratowej, 325
nośnik liczby całkowitej, 54
Nullstellensatz, 240
NWD-ciąg, 53

O*brót* płaszczyzny, 14
odwrotność elementu w grupie, 8
— — pierścienia, 11
— (liczby) modulo m, 163
— liczby zespolonej, 12
odwzorowanie liniowe płaszczyzny, 313
ogon ciągu, 263
ogólne równanie indyjskie, 389
— — —, postać normowa, 389
opis parametryczny, 392, 394
oś liczbowa, 11
— rzeczywista, urojona 12

P*arabola*, 392
pełny wielomian symetryczny jednorodny danego stopnia, 231
permutacja, 9
pierścień Dedekinda, 352
— Eisensteina $\mathbb{Z}[\tau_{-3}]$, 351
— Eulera $\mathbb{Z}[\tau_{-2}]$, 349
— formalnych szeregów potęgowych, 308
— ilorazowy, 325
— klas reszt (liczb całkowitych) modulo m, 177
— kwadratowy (rzeczywisty lub urojony), 336
— — (normowo-) euklidesowy, 338
— — — typu (± 1), 364
— liczb algebraicznych całkowitych $\mathbb{I}$, 234
— — całkowitych, 10
— — — Gaussa $\mathbb{Z}[\,i\,]$, 326
— — rzeczywistych, 10
— — wymiernych, 10
— noetherowski, 359
— przemienny z jedynką, 9
— wielomianów jednej zmiennej, 64
— — wielu zmiennych, 109
pierwiastek arytmetyczny, 325
— kongruencji wielomianowej, 179
— kwadratowy, 73
— pierwotny modulo m, 195
— podwójny trójmianu kwadratowego, 73
— redukcji wielomianu modulo m, 179
— wielokrotny (k-krotny) wielomianu, 227
— wielomianu, 66
pierwiastki charakterystyczne, 301
— n-tego stopnia z liczby zespolonej, 15
pierwotna trójka pitagorejska, 43
pochodna, 225
— druga, k-ta, 225
— wielomianu, 225
podłoga liczby rzeczywistej, 412
podgrupa, 183
— dyskretna płaszczyzny, 278
— generowana przez (dany) element, 183
podkrata, 326
podniesienie rozwiązania, 218
podstawa systemu pozycyjnego, 417
podzbiór induktywny zbioru $\mathbb{N}$, 3
— multyplikatywny (multyplikatywnie zamknięty) w $\mathbb{Z}$, 111
— zamknięty względem działania, 183
postać kanoniczna trójmianu kwadratowego, 73
— normalna równania sześciennego, 399
— normowa ogólnego równania indyjskiego, 389
— trygonometryczna liczby zespolonej, 13
— zredukowana równania sześciennego, 99
postulat Bertrand'*a*, 438
potęga elementu grupy, 183
— malejąca 51
— właściwa liczby całkowitej, 47

prawo najlepszego przybliżenia, 258
— skracania, 159, 326, 355
— wzajemności reszt kwadratowych, 208
— — — — , II uzupełnienie, 207
— — — — , I uzupełnienie, 205
problem bazylejski, 428
— Catalan'*a*, 58
— Frobeniusa, 30
przedłużenie ciągu na $\mathbb{Z}$, 316
przedstawienie liczby przez formę, 288
— właściwe liczby przez formę, 288
przekrój zbiorów, 7
pseudomianowniki, 253
punkt idealny, 409
— osobliwy krzywej, 405
— wymierny płaszczyzny, 44, 278
— — (całkowity, rzeczywisty, zespolony) krzywej, 399
punkty stałe odwzorowania, 299
PWRK (prawo wzajemności reszt kwadratowych), 208
pytanie Eulera, 400
— Fermat'*a*, 400

q-współczynnik dwumienny, 436

***R**edukcja* ciągu modulo m, 321
— wielomianu modulo m, 179
redukt liczby $\in \mathbb{R}$ przy danej podstawie, 419
— ułamka łańcuchowego, 256
reguła Eulera, 256
relacja kongruencji modulo m, 157
— podzielności w pierścieniu $\mathbb{Z}$, 19
— —- — — wielomianów, 82
— — — dziedzinach całkowitości, 355
— stowarzyszenia, 356
— — w $\mathbb{K}[X]$, 82
— zgodna z dodawaniem, 158, 351
— — — — wielomianów, 179
— — — mnożeniem, 158
reszta kwadratowa modulo m, 203
— z dzielenia, 20, 69, 327
— — — w pierścieniu wielomianów, 69
rozdzielność działań, 7
rozkład jedynki, 422
rozwiązania kongruencji wielomianowej, 161
— — — równoważne modulo m, 161
rozwiązanie fundamentalne równania indyjskiego, 385
równanie anty-indyjskie, 388
— Bachet'*a*, 370
— diofantyczne, 160
— indyjskie (Pella), 383
— — ogólne, 389
— Pitagorasa, 43, 333, 394
— Ramanujana, 378
— rekurencyjne liniowe, 301
— rozwiązujące równania szaściennego, 99
— trzykwadratowe, 99
równoległobok podstawowy kraty, 278
równość Bézout'*a*, 66
równość Bhaskary, 383
— pochłaniania, 122
— Ramanujana, 378
równoważność form kwadratowych, 288
— liczb (rzeczywistych), 262
— nitek p-adycznych, 222
rząd elementu grupy, 184

***S**ito* Eratostenesa, 32
składanie (bijekcji), 7
składnik jednorodny stopnia k, 110
skoki Viète'*a*, 79
spektrum liczby rzeczywistej, 414
splot Dirichlet'*a*, 147
sprzęganie w ciele $\mathbb{F}_p(\iota)$, 318
sprzężona liczba zespolona, 12
— niewymierność kwadratowa, 264
stała Minkowskiego, 287
standardowy zredukowany układ reszt, 164
— zupełny układ reszt, 20, 164
stopień dolny szeregu potęgowego, 308
— jednomianu, 109
— liczby algebraicznej, 232
— wielomianu jednej zmiennej, 65
— — wielu zmiennych, 109
stowarzyszenia relacja w dziedzinach całkowitości, 356
struktura algebraiczna, 6
sufit liczby rzeczywistej, 423
suma teoriomnogościowa, 7
superpozycja wielomianów, 66
symbol dwumienny (Newtona), 432
— Legendre'*a*, 204
system pozycyjny, 417
szereg harmoniczny, 425
— Neumanna, 308
— potęgowy (formalny), 308
sześcian, 50

***T**echnika* skoków Viète'*a*, 79
teoria form modularnych, 287
TFE, dowód pierwszy, 273
— — drugi, 274
— — trzeci, 282
— — czwarty, 292
— — piąty, 299
— — szósty, 332
theorema fundamentale (aureum), 208
tożsamość algebraiczna, 110
— Brahmagupty, Fibonacci'*ego*, 271
— Cauchy'*ego*-Vandermonde'*a*, 65
— Cesàro, 303
— — uogólniona, 312
— Eulera, 294
— Hermite'*a*, 413
— kwadratowa dla ciągów Lucas'*a*, 312
— "nieśmiertelna", 10
— —, "nieskończone" uogólnienie, 308
— pochłaniania, 434
— Sophie Germain, 110
translacja, 13
trik w $\mathbb{N}$, 42
— w $\mathbb{Z}[\,i\,]$, 333
— w dziedzinie z jednoznacznością rozkładu, 369
trójka pitagorejska, 43
— —, pierwotna, 43
trójkąt pitagorejski, 43
— Tartaglia'*i*, 100
trójmian kwadratowy, 73
— minimalny (niewymierności kwadratowej), 264
twierdzenie Brahmagupty-Bachet'*a*, 28
— Beatty'*ego*-Banga, 414
— Bézout'*a*, 67
— Catalan'*a*, 45
— Cauchy'*ego*-Davenporta, 245
— Cauchy'*ego*-Farey'*a*, 252
— Chevalley'*a*-Warninga, 246, 247
— chińskie o resztach, CTR, 169
— — — — uogólnione, 173
— Czebyszewa, 438, 439
— Dirichlet'*a* o aproksymacji, 251
— — o liczbach pierwszych w ciągach arytmetycznych, 189
— Erdősa-Ginzburga-Ziva, 244
— Euklidesa, TE, 33
— — o liczbach doskonałych, 145
— Eulera, 165
— — o czterech liczbach, 370
— — — funkcji $\pi(n)$, 150
— — — liczbach doskonałych, 145
— — — wartości $\zeta(2)$, 428
— Fermat'*a*-Eulera, TFE, 273
— Fermat'*a*, małe, MTF, 166
— —, wielkie, WTF, 372
— Galois'*a*, 267
— Gaussa o φ-funkcji, 146
— — — istnieniu NWD wielomianów, 84
— Gaussa-Bézout'*a*, 24
— Gaussa-Legendre'*a*, 296
— Glaishera, 435
— Goldbacha, 23
— Hurwitza, 259
— kombinatoryczne o zerach, CN, 241
— Lagrange'*a* o czterech kwadratach, 294
— — — liczbach pierwszych postaci $x^2 + 2y^2$, 283
— — — pierwiastkach wielomianu, 70
— — — równaniu indyjskim, 383
— — — rzędzie podgrupy, 184
— — — ułamku łańcuchowym niewymierności kwadratowej, 268
— — — — — liczby $\sqrt{D}$, 268
— — — wartości średniej, 226
— — — wielomianie interpolacyjnym, 105
— Legendre'*a*, 37, 396
— Lindemanna, 238
— Liouville'*a*, 238
— Lucas'*a*, 432
— Minkowskiego o figurze wypukłej, 280
— Möbiusa o odwracaniu (I i II), 149 i 150
— Newtona o wielomianach symetrycznych, 229
— o aproksymacji diofantycznej, 252
— — ekwipartycji, 417
— — istnieniu pierwiastków pierwotnych $(\mathrm{mod}\, m)$, 198
— — jednoznaczności dla funkcji wymiernych, 108
— — — (zapisu wielomianu), 71
— — — rozkładu w dig'*ach*, 359
— — — — — $\mathbb{K}[X]$, 86
— — — — — $\mathbb{N}$, 32
— — — — — $\mathbb{Z}[\,i\,]$, 332
— — — — — $\mathbb{Z}[X]$, 88
— — kongruencji liniowej, 162
— — liczbach pierwszych, PNT, 441
— — partyzantach, 282
— — strażakach, 96
— Picka, 252

— Poincaré'*go*, 411
— Rolle'*a*, 225
— Schinzla, 422
— Schura, 162
— Sophie Germain, 374
— Sylvestera, 29
— Thue'*go*, 281
— de la Vallée Poussin'*a*, 441
— Wilsona, 167
— Wolstenholme'*a*, 431
— zasadnicze algebry, 92
— — arytmetyki, ZTA, 24
— Zsigmondy'*ego*, 192

***U**kład* Eisensteina, Gaussa, 206
— kongruencji liniowych, 174
— zredukowany reszt modulo m, 164
— zupełny reszt modulo m, 164
ułamek egipski, 421
— łańcuchowy, kanoniczne rozwinięcie na, 253
— nieskracalny, 25
— prosty, 107
uogólnienie tożsamości nieśmiertelnej, 308
uogólnione twierdzenie chińskie o resztach, 173
uproszczony wzór dwumienny (mod p), 433
uzupełnienie I prawa wzajemności, 205
— II prawa wzajemności, 207

***W**arstwa* liczby a modulo m, 176
wartość funkcji wymiernej, 108
— średnia funkcji $r(n)$, 276
— ułamka łańcuchowego, 257
— wielomianu, 66
— — $f(X) \in \mathbb{Z}[X]$ dla argumentu $\alpha \in \mathbb{Z}_p$, 222
warunek bazowy indukcji, 3
— jednorodności danego stopnia, 110
warunki początkowe, 301
wektor, 240
Wielkie Twierdzenie Fermat'*a*, WTF, 372
— — —, przypadek I, 374
— — —, przypadek II, 374
wielokrotność, 18, 328, 340, 355
— w pierścieniu wielomianów, 82
— elementu grupy addytywnej, 183
wielomian Bernoulli'*ego*, 248
— "broszkowy", 243
— charakterystyczny, 301
— cyklotomiczny, 98
— — jednorodny, 191
— Czebyszewa, 306
— dwóch zmiennych, 108
— interpolacyjny Lagrange'*a*, 105
— jednej zmiennej, 64
— minimalny liczby algebraicznej, 232
— n zmiennych, 109
— Newtona, 432
— nierozkładalny, 85
— palindromiczny, 104
— Petersena grafu prostego, 243
— pierwotny, 87
— Polya'*i*, 115
— stały, 64
— symetryczny (elemetarny), 228
— — pełny jednorodny stopnia k, 110
— — elementarny, 228
— unormowany, 69
— zerowy, 64
wielomiany stowarzyszone, 82
— względnie pierwsze, 84
własność Darboux (funkcji ciągłych), 75
— — dyskretna, 243
— nieparzystej podzielności (ciągu), 53
— podzielności (ciągu), 53
wspólne dzielniki (zbiór owych), 19
współczynnik dwumienny, 432
— — Fibonacci'*ego*, 436
— wielomianu, 64
— — wiodący, 65
współrzędne biegunowe, 13
wstępujący łańcuch ideałów, 359
wykładnik p-adyczny, 36
wynik działania, 6
wyraz wolny wielomianu, 64
wyróżnik, 230
— binarnej formy kwadratowej, 288
— kraty, 278
— niewymierności kwadratowej, 264
— równania sześciennego, 99
— trójmianu kwadratowego, 73
— — sześciennego, 403
wyznacznik macierzy (odwzorowania liniowego) 315
— Vandermonde'*a* 51
wzory Eulera-Binet'*a*, 306
— — — na wielomiany Czebyszewa, 307
— Viète'*a*, 77, 101
wzór Binet'*a*, 302
— dwumienny, 10
— —, uproszczony modulo p, 433
— Cassini'*ego* 304

— — uogólniony, 316
— de Moivre'*a*, 14
— Legendre'*a*, 37
— Maclaurina, Taylora, 226

***Z**adanie* Fermat'*a*, 373
— Halmosa, 5
— o broszkach, 242
— — długiej igle, 171
— — trójkątach Napoleona, 17
— — woźnym matematyku, 144
— — zakopanym skarbie, 16
— — znudzonych uczniach, 144
zagadka Erdösa, 23
zapis pozycyjny liczb naturalnych, 417
— — — rzeczywistych, 420
zasada indukcji (matematycznej), 3
— maksimum, 2
— minimum, 1
— odejmowania proporcji stronami, 2
— podstawowa, 19
— równoległoboku dodawania wektorów, 13
— skwantowania (liczb całkowitych), 2
— szufladkowa, 250
zasadnicze twierdzenie algebry, 92
— — arytmetyki, ZTA, 24
— — — w pierścieniu Gaussa, 329
— — — — — wielomianów, 84
zawartość wielomianu z $\mathbb{Q}[X]$, 87
zbiór liczb algebraicznych $\mathbb{A}$, 232
— — — całkowitych $\mathbb{I}$, 232
— — całkowitych $\mathbb{Z}$, 1
— — naturalnych $\mathbb{N}$, 1
— — zespolonych $\mathbb{C}$, 11
— multyplikatywnie zamknięty, 271
— obszerny/szczupły (liczb naturalnych), 427
— wspólnych dzielników, 19
zero grupy addytywnej, 8
— pierścienia, 9
— wielomianu, 66
zespolona płaszczyzna rzutowa, 409
złożenie wielomianów, 66
zredukowana niewymierność kwadratowa, 265
zredukowany układ reszt modulo m, 164
— standardowy układ reszt modulo m, 164
ZTA (Zasadnicze Twierzenie Arytmetyki), 24
zupełność pierścienia $\mathbb{Z}_p$, 223
zupełny układ reszt modulo m, 164
— standardowy układ reszt modulo m, 20, 164
zwartość pierścienia $\mathbb{Z}_p$, 223

Kilka oznaczeń

F_n liczba Fermat'*a*, 23
M_n liczba Mersenne'*a*, 35
$\mathbb{P}$ zbiór liczb pierwszych, 31
(α) ideał główny generowany przez α, 20, 355
$v_p(c)$ wykładnik p-adyczny liczby $c \in \mathbb{Z}$, 36
$\mathrm{Supp}(a)$ nośnik liczby całkowitej a, 54
$\mathcal{R}[X]$ pierścień wielomianów jednej zmiennej X o współczynnikach w pierścieniu $\mathcal{R}$, 64
$\Phi_n(X)$ n-ty wielomian cyklotomiczny, 98
$\sigma_k(X_1, \ldots, X_n)$ k-ty elementarny wielomian symetryczny zmiennych $X_1, \ldots, X_n$, 228
$\tau(n)$ liczba dzielników liczby $n \in \mathbb{N}$, 144
$\sigma(n)$ suma dzielników liczby $n \in \mathbb{N}$, 145
$\varphi(n)$ wartość funkcji Eulera, 146
$\mu(n)$ wartość funkcji Möbiusa, 148
$f * g$ splot Dirichlet'*a*, 148
$a \equiv b \,(\mathrm{mod}\, m)$ kongruencja modulo m, 157
$\mathbb{Z}/m$ pierścień klas reszt modulo m, 176
$(\mathbb{Z}/m)^*$ grupa jedności pierścienia $\mathbb{Z}/m$, 177
$\mathbb{F}_p = \mathbb{Z}/p$ ciało klas reszt modulo p, 178
$\mathcal{N}(h;\, m)$ zbiór rozwiązań (parami nierównoważnych) kongruencji $h(x) \equiv 0 \,(\mathrm{mod}\, m)$, 161
$N(h;\, m)$ moc zbioru $\mathcal{N}(h;\, m)$, 161
(α) podgrupa cykliczna generowana przez element α danej grupy, 183
$\mathrm{rz}(\alpha)$ rząd elementu α danej grupy, 184
$\mathrm{rz}_p(a)$ rząd $a \,(\mathrm{mod}\, p)$ w grupie $(\mathbb{Z}/p)^*$, 187
$\mathrm{ind}_g(a)$ indeks $a \,(\mathrm{mod}\, m)$ przy podstawie g, 202
$a\mathbf{R}m$, $a\mathbf{N}m$ a jest resztą, nieresztą kwadratową modulo m, 203
$\left(\frac{a}{p}\right) = (a|p)$ symbol Legendre'*a* (a *po* p), 204
$\mathbb{Q}(\sqrt{D})$ ciało kwadratowe, 325
α' sprzężenie elementu α danego ciała kwadratowego, 325
$\mathbf{N}(\alpha)$ norma w ciele kwadratowym, 325
$\mathbb{Z}[\tau_D]$ pierścień kwadratowy, 336