Matematyka Dyskretna
Wykład 2.
Arytmetyka liczb całkowitych.

Czesław Bagiński
c.baginski@pb.edu.pl

Wydział Informatyki
Politechnika Białostocka

Literatura podstawowa:

1. Victor Bryant, Aspekty kombinatoryki, Wydawnictwo Naukowo-Techniczne, Warszawa 1997.
2. Ronald L. Graham, Donald E. Knuth, Oren Patashnik, Matematyka konkretna, Wydawnictwo Naukowe PWN, Warszawa 1998.
3. Donald E. Knuth, Sztuka programowania, t. 1-3, Wydawnictwo Naukowo-Techniczne, Warszawa 2003.
4. Witold Lipski, Kombinatoryka dla programistów, Wydawnictwo Naukowo-Techniczne, Warszawa 1982.
5. Kenneth A. Ross, Charles R.B. Wright, Matematyka dyskretna, Wydawnictwo Naukowe PWN, Warszawa 2001.
6. Robin J. Wilson, Wstęp do teorii grafów, Wydawnictwo Naukowe PWN, Warszawa 1998.
7. Harry Lewis, Rachel Zax, Matematyka dyskretna; Niezbędnik dla informatyków, Wydawnictwo Naukowe PWN, Warszawa 2021.

Plan wykładu

1. Wstęp
2. Systemy pozycyjne.
3. Liczby pierwsze.
4. Zasadnicze twierdzenie arytmetyki liczb całkowitych.
5. Największy wspólny dzielnik, najmniejsza wspólna wielokrotność.
6. Algorytm Euklidesa, Rozszerzony Algorytm Euklidesa.
7. Arytmetyka modularna.

Teoria Liczb - kilka słów historii

Teoria Liczb – jeden z najstarszych działów matematyki, zajmujący się opisem własności liczb (zwłaszcza naturalnych).
Wkład w badania objęte tym działem mają między innymi:

- Pitagoras (580-520 pne)
  Trójki pitagorejskie, liczby doskonałe, niewymierność
- Euklides (325-265 pne)
  Zasadnicze twierdzenie arytmetyki, nieskończoność zbioru liczb pierwszych
- Eratostenes (276-197 pne)
  Sito Eratostenesa – jak rozmieszczone są liczby pierwsze
- Diofantos (200-284 ne)
  Równanie Pitagorasa
- Pierre de Fermat (1601-1665)

Słynne twierdzenia

Wielkie Twierdzenie Fermata (1637). *Dla dowolnej liczby naturalnej $n \geqslant 3$ nie istnieją liczby naturalne x, y, z takie, że*

$$x^n + y^n = z^n. \tag{1}$$

Twierdzenie Fermata udowodnił A. Wiles w 1995 r.

Hipoteza Catalana (1844). Nie istnieją liczby naturalne x, m, y, n takie, że

$$x^m - y^n = 1$$

poza przypadkiem ujętym w równości

$$3^2 - 2^3 = 1.$$

Hipotezę Catalana udowodnił Preda Mihăilescu w 2002 r.

Przykładowe problemy

Hipoteza Goldbacha. *Każda liczba parzysta większa od 2 jest sumą dwóch liczb pierwszych.*

Liczby Fermata. *Czy istnieje liczba pierwsza postaci* $F_n = 2^{2^n} + 1$ *dla* $n > 5$*?*

Bliźniacze liczby pierwsze. *Czy zbiór par bliźniaczych liczb pierwszych jest skończony?*

Liczby doskonałe. *Czy istnieją nieparzyste liczby doskonałe*

Definicja

Mówimy że liczba całkowita a jest *dzielnikiem* liczby całkowitej b (lub że a dzieli b) i piszemy $a|b$, jeśli istnieje liczba całkowita c, taka że $b = ac$.

Lemat

Niech a i b będą dowolnymi liczbami całkowitymi, $b > 0$. Wówczas istnieją liczby całkowite q i r takie, że

$$a = bq + r, \quad \textit{gdzie} \;\; 0 \leq r < b.$$

Indukcja zupełna względem $|a|$.
Baza: Jeśli $0 \leq a < b$, to przyjmujemy $q = 0$, $r = a$ i mamy

$$a = 0 \cdot b + a.$$

Założenie indukcyjne: Teza twierdzenia jest prawdziwa dla wszystkich liczb $a_1 < a$, tzn. jeśli $a_1 < a$, to istnieją $q_1, r_1 \in \mathbb{Z}$ takie, że

$$a_1 = q_1 b + r_1, \quad 0 \leq r_1 < b.$$

Teza indukcyjna: Teza twierdzenia jest prawdziwa dla a.

Dowód: Na mocy pierwszego kroku możemy przyjąć, że $a \geq b$. Ponieważ $0 \leq a - b < a$, więc z założenia indukcyjnego istnieją $q_1, r_1 \in \mathbb{Z}$, $0 \leq r_1 < b$, że

$$a - b = q_1 b + r_1$$

Stąd

$$a = b + q_1 b + r_1 = (q_1 + 1)b + r_1.$$

Wystarczy więc przyjąć $q = q_1 + 1$, $r = r_1$. To kończy dowód tezy indukcyjnej, zatem na mocy zasady indukcji zupełnej twierdzenie jest prawdziwe dla każdej pary liczb całkowitych $0 \leq a$, $0 < b$.

Definicja

Niech b będzie liczbą całkowitą większą od 1. Klasycznym systemem pozycyjnym o podstawie b nazywamy sposób zapisu liczb rzeczywistych nieujemnych w postaci

$$(a_n\, a_{n-1}\, \ldots\, a_3\, a_2\, a_1\, a_0,\ a_{-1}\, a_{-2}\, \ldots)_b, \tag{2}$$

gdzie $a_i \in \{0, 1, 2, \ldots, b-1\}$. Zapis taki oznacza liczbę

$$a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \cdots + a_3 \cdot b^3 + a_2 \cdot b^2 + a_1 \cdot b + a_0 + \\ + a_{-1} \cdot \frac{1}{b} + a_{-2} \cdot \frac{1}{b^2} + \cdots\ , \tag{3}$$

Liczby 0, 1, . . . , $b - 1$ nazywamy cyframi systemu o podstawie b.
Pełnią one dwojaką rolę:

- liczb
- znaków graficznych.

Przecinek występujący w zapisie oddziela część całkowitą liczby od jej części ułamkowej. Jeżeli część ułamkowa jest równa zeru, można w tym zapisie zrezygnować z przecinka i cyfr (równych 0) po jego prawej stronie.

Twierdzenie

Niech b będzie liczbą całkowitą, $b > 1$. Każdą liczbę całkowitą $a > 0$ można w sposób jednoznaczny zapisać w klasycznym systemie o podstawie b, tzn. w postaci:

$$(a_n\, a_{n-1}\, \dots\, a_3\, a_2\, a_1\, a_0)_b = \\ = a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \cdots + a_3 \cdot b^3 + a_2 \cdot b^2 + a_1 \cdot b + a_0,$$

gdzie $a_n > 0$.

Przykład

Jeśli włączymy w zapis część ułamkową, to przestaje on być jednoznaczny. Wystarczy zauważyć, że

$$\begin{aligned} \frac{b-1}{b} + \frac{b-1}{b^2} + \frac{b-1}{b^3} + \cdots &= \frac{b-1}{b}\left(1 + \frac{1}{b} + \frac{1}{b^2} + \cdots\right) = \\ &= \frac{b-1}{b}\left(\frac{1}{1-\frac{1}{b}}\right) = 1. \end{aligned}$$

Zatem $(0, b-1\, b-1\, b-1\, \ldots)_b = (1, 0\,0\,0\, \ldots)_b$.

Przykład

podstawa	nazwa systemu	cyfry
10	dziesiętny	$0,\ 1,\ 2,\ 3, \ldots,\ 8,\ 9$
2	dwójkowy (binarny)	$0,\ 1$
8	ósemkowy (oktonalny)	$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7$
16	szesnastkowy (hexadecymalny)	$0,\ 1,\ 2, \ldots, 9,\ A,\ B,\ C,\ D,\ E,\ F$
60	sześćdziesiętny	$0,\ 1,\ \ldots,\ 59$

Definicja

Liczbę naturalną p nazywamy *liczbą pierwszą*, jeżeli ma ona dokładnie dwa różne dzielniki naturalne. W myśl tego określenia, liczba 1 nie jest liczbą pierwszą, bo ma tylko jeden taki dzielnik.

Lemat

Każdą liczbę naturalną większą od 1*, która nie jest liczbą pierwszą, można rozło.zyć na iloczyn liczb pierwszych. W szczególności więc, każda liczba naturalna większa od* 1 *dzieli się przez pewną liczbę pierwszą.*

Twierdzenie Euklidesa

Istnieje nieskończenie wiele liczb pierwszych

Dowód

Przypuśćmy, że jest inaczej, tzn. ilość liczb pierwszych jest skńczona. Niech

$$\Pi = \{p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_6 = 11,\ p_7,\ \ldots,\ p_n\}$$

będzie zbiorem wszystkich liczb pierwszych. Rozważmy dwie liczby

$$M = p_1 \cdot p_2 \cdot \ldots \cdot p_n \quad \text{i} \quad N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 = M + 1.$$

Każda liczba naturalna dzieli się przez przynajmniej jedną liczbę pierwszą, liczba N również. Niech

$$p_i \mid N.$$

Ponieważ $p_i \mid M$ i $p_i \mid (M+1)$, więc $p_i \mid (M+1) - M$, czyli $p_i \mid 1$, co jest niemożliwe.

Największe znane liczby pierwsze

Największa znana obecnie liczba pierwsza to 51. liczba pierwsza Mersenne'a:

$$2^{82\,589\,933} - 1$$

i liczy sobie

$$24\,862\,048$$

cyfr w zapisie dziesiętnym. Odkryto ją w 2018 roku.
Dziewięć największych znanych liczb pierwszych, to liczby pierwsze Mersenne'a

Twierdzenie

Szereg harmoniczny, tzn. szereg odwrotności liczb naturalnych

$$\sum_{n\in\mathbb{N}} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \cdots$$

jest rozbieżny.

Twierdzenie

Szereg odwrotności liczb pierwszych

$$\sum_{p\in\Pi} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} \cdots$$

jest rozbieżny.

Przedziały bez liczb pierwszych

Dla dowolnej liczby naturalnej n istnieje ciąg kolejnych liczb naturalnych, z których żadna nie jest liczbą pierwszą.

Dowód

Liczby od $(n+1)!+2$, do $(n+1)!+(n+1)$ są złożone, bo $2 \mid ((n+1)!+2)$, $3 \mid ((n+1)!+3)$, $\ldots$, $(n+1) \mid ((n+1)!+(n+1))$.

Bliźniacze liczby pierwsze

Liczby pierwsze p i q nazywamy bliźniaczymi, jeśli $|p-q|=2$. Nie wiadomo, czy liczba bliźniaczych liczb pierwszych jest skończona.

Wielomiany

Nie istnieje wielomian jednej zmiennej, którego wartości są wyłącznie liczbami pierwszymi.

Różne wielomiany

L. Euler: *Dla liczby naturalnej* $q \in \{2, 3, 5, 11, 17\}$ *wielomian*

$$x^2 + x + q$$

przyjmuje wartości będące liczbami pierwszymi dla $x \in \{1, 2, \dots, q-2\}$

Liczby pierwsze Fermata (K. F. Gaussa)

Fermat: Dla każdego $k \geqslant 0$ liczba

$$F_k = 2^{2^k} + 1$$

jest pierwsza.

$F_0 = 2^{2^0} + 1 = 3$, $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$,
$F_3 = 2^{2^3} + 1 = 257$, $F_4 = 2^{2^4} + 1 = 65\,537$
L. Euler: $F_5 = 2^{2^5} + 1 = 641 \cdot 6\,700\,417$
F. Laundry: $F_6 = 274\,177 \cdot 67\,280\,421\,310\,721$ (1880, miał wtedy 82 lata)
$F_9 = 2^{512} + 1 =$
$= 2\,424\,833 \times$
$\times 7\,455\,602\,825\,647\,884\,208\,337\,395\,736\,200\,454\,918\,783\,366\,342\,657 \times$
$\times 741\,640\,062\,627\,530\,801\,524\,787\,141\,901\,937\,474\,059\,940\,781\,097$
$519\,023\,905\,821\,316\,144\,415\,759\,504\,705\,008\,092\,818\,711\,693\,940\,737$
Pełne rozkłady znane są tylko dla liczb od F_k, gdy $k \leqslant 11$.

Liczby pierwsze Mersenne'a

Liczbą pierwszą Mersenne'a nazywamy liczbę pierwszą postaci

pt
$$M_p = 2^p - 1,$$

gdzie p jest liczbą pierwszą.

Liczby

$$M_2 = 3,\ M_3 = 7,\ M_5 = 31,\ M_7 = 127,\ M_{13},\ M_{17},\ M_{19}, \ldots$$

są pierwsze, a liczby

$$M_{11} = 23 \times 89,\ M_{23} = 47 \times 178\,481,\ M_{67} = 193\,707\,721 \times 761\,838\,257\,287,$$

$$M_{83} = 167 \times 57\,912\,614\,113\,275\,649\,087\,721, \ldots$$

są złożone.

Prawdopodobieństwo wylosowania liczby pierwszej

Jeśli $N < 2^{1000}$, to prawdopodobieństwo p wylosowania liczby pierwszej w jednym losowaniu mieści się w przedziale:

$$\frac{1}{1000 \cdot \ln 2} < p < \ln 4 \cdot \frac{1}{1000 \ln 2}$$

$\ln 2 = 0,69315, \quad \ln 4 = 1,38629.$

$$\frac{1}{348,57} < p < \frac{1,38629}{348,57}.$$

(uwzględniając tylko liczby nieparzyste).

Zasadnicze Twierdzenie Arytmetyki

Każdą liczbę całkowitą a różną od zera można w sposób jednoznaczny przedstawić w postaci:

$$a = (-1)^{\alpha} p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = (-1)^{\alpha} \prod_{i=1}^{k} p_i^{a_i},$$

gdzie $\alpha \in \{0,1\}$, $p_1 < p_2 < \cdots < p_k$ są liczbami pierwszymi, $a_i \in \mathbb{N}$ dla $i = 1, 2 \ldots, k$.

5. Największy wspólny dzielnik, najmniejsza wspólna wielokrotna

Definicja

Największym wspólnym dzielnikiem liczb a i b nazywamy największą liczbę naturalną $NWD(a, b) = d$, taką że d jest dzielnikiem a, d jest dzielnikiem b i dzieli się przez każdy wspólny dzielnik tych liczb. Największy wspólny dzielnik liczb a i b oznaczamy symbolem $NWD(a, b)$. Przyjmujemy, że $NWD(0, b) = b$. Liczby całkowite a i b nazywamy *względnie pierwszymi* jeśli ich największy wspólny dzielnik jest równy 1.

Definicja

Najmniejszą wspólną wielokrotną liczb a i b nazywamy najmniejszą liczbę naturalną e, taką że a jest dzielnikiem e, b jest dzielnikiem e i e jest dzielnikiem każdej liczby, która się dzieli jednocześnie przez a i b. Najmniejszą wspólną wielokrotność a i b oznaczamy symbolem $NWW(a, b)$.

5. Największy wspólny dzielnik, najmniejsza wspólna wielokrotna

Twierdzenie

Niech a i b będą ustalonymi liczbami całkowitymi różnymi od zera:

$$a = (-1)^{\eta} p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad b = (-1)^{\epsilon} p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

Wówczas

$$NWD(a, b) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}, \quad NWW(a, b) = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k},$$

gdzie $c_i = min\{a_i, b_1\}$, $d_i = max\{a_i, b_i\}$ *dla* $i = 1, 2, \ldots, k$.

Wniosek

Niech a i b będą ustalonymi liczbami całkowitymi różnymi od zera. Wówczas

$$NWD(a, b) \cdot NWW(a, b) = |a \cdot b|.$$

Algorytm Euklidesa

Niech a i b będą dowolnymi liczbami całkowitymi dodatnimi. Dla $n = 1, 2, \ldots$ definiujemy kolejne wyrazy ciągów a_n, b_n, q_n i r_n przyjmując:

$$\begin{array}{llll}
a_1 = a, & b_1 = b, & q_1 = \lfloor a_1/b_1 \rfloor, & r_1 = a_1 - b_1 q, \\
a_2 = b_1, & b_2 = r_1, & q_2 = \lfloor a_2/b_2 \rfloor, & r_2 = a_2 - b_2 q \\
\ldots & & & \\
a_n = b_{n-1}, & b_n = r_{n-1}, & q_n = \lfloor a_n/b_n \rfloor, & r_n = a_n - b_n q
\end{array}$$

Wyrazy ciągu $\{r_n\}$ są nieujemne oraz $r_1 > r_2 > r_3 > \cdots$, o ile są dodatnie. Zatem, istnieje takie n, że $r_n \neq 0$ i $r_{n+1} = 0$. Wówczas $NWD(a, b) = r_n$.

Rozszerzony Algorytm Euklidesa

Definiujemy ciągi $\{x_n\}$, $\{y_n\}$, $\{a_n\}$, $\{b_n\}$, $\{q_n\}$, $\{r_n\}$, przy tym dla $n \geqslant 1$ cztery ostatnie są takie, jak w opisanym wyżej algorytmie Euklidesa:

x	y	a	b	q	r
$x_0 = 1$	$y_0 = 0$	—	$b_0 = a$		b
$x_1 = 0$	$y_1 = 1$	$a_1 = b_0$	$b_1 = r_0$	$q_1 = \lfloor a_1/b_1 \rfloor$	$r_1 = a_1 - b_1 q_1$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots\dots$
$x_n = x_{n-2} - x_{n-1} q_{n-1}$	$y_n = y_{n-2} - y_{n-1} q_{n-1}$	$a_n = b_{n-1}$	$b_n = r_{n-1}$	$q_n = \lfloor a_n/b_n \rfloor$	$r_n = a_n - b_n q_n$

Dla dowolnej liczby naturalnej n

$$x_n a + y_n b = r_{n-1}.$$

W szczególności, jeśli $r_n = 0$ i $r_{n-1} \neq 0$, to

$$x_n a + y_n b = NWD(a, b).$$

Liniowe równanie diofantyczne.

Niech k, m, n będą ustalonymi liczbami całkowitymi. Wówczas równanie

$$mx + ny = k \tag{4}$$

ma rozwiązanie wtedy i tylko wtedy, gdy $d \mid k$, gdzie $d = NWD(m, n)$. Jeśli para liczb całkowitych (x_0, y_0) jest pewnym rozwiązaniem tego równania, to wszystkie rozwiązania dane są wzorami:

$$x = x_0 + \frac{n}{d} \cdot t, \quad y = y_0 - \frac{m}{d} \cdot t, \quad t \in \mathbb{Z}.$$

Rzeczywiście, jeśli $mx_0 + ny_0 = k$, to

$$m(x_0 + \frac{n}{d}t) + n(y_0 - \frac{m}{d}t) = mx_0 + ny_0 + \frac{mn}{d}t - \frac{mn}{d}t = k$$

Jeżeli $NWD(m, n) = 1$ to dla dowolnej liczby całkowitej k równanie (4) ma nieskonczenie wiele rozwiązań. Wszystkie te rozwiązania można uzyskać z jednego rozwiązania (x_0, y_0) z wykorzystaniem wzorów $x = x_0 + nt, \quad y = y_0 - mt, \quad t \in \mathbb{Z}$

Przykład

Rozwiąż równanie 3524574x+832048y=123456,