Notatki z Algorytmicznej Teorii Liczb

Jakub Pawlewicz

7 stycznia 2010

1 Liczby pierwsze

Podstawowy fakt udowodniony dawno temu przez Euklidesa brzmi.

Twierdzenie 1.1. *Liczb pierwszych jest nieskończenie wiele.*

Poniżej przedstawiamy dowód edukacyjny, który różni się od oryginalnego dowodu Euklidesa.

Dowód. Skorzystamy ze znanej równości:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \tag{1.1}$$

Prawa strona równości (1.1) jest liczbą niewymierną. Z drugiej strony mamy:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \prod_{p \text{ pierwsza}} \frac{1}{1 - \frac{1}{p^2}} \tag{1.2}$$

Zatem jeśli mamy skończenie wiele liczb pierwszych to prawa strona (1.2) jest liczbą wymierną — sprzeczność. □

Skąd się biorą takie równości jak (1.2)? Dla dowolnej funkcji f takiej, że $f(xy) = f(x)f(y)$, można ogólnie napisać

$$\sum_{n=1}^{\infty} f(n) = \prod_{p \text{ pierwsza}} \frac{1}{1 - f(p)}.$$

Bierze się to stąd, że

$$\begin{aligned}
\prod_{p \text{ pierwsza}} \frac{1}{1 - f(p)} &= \prod_{p \text{ pierwsza}} \sum_{i=0}^{\infty} \big(f(p)\big)^i \\
&= \sum_{\substack{0 \le i_1, i_2, \ldots \\ \lim_{k\to\infty} i_k = 0}} \prod_{k=1}^{\infty} \big(f(p_k)\big)^{i_k} = \sum_{\substack{0 \le i_1, i_2, \ldots \\ \lim_{k\to\infty} i_k = 0}} f\left(\prod_{k=1}^{\infty} p_k^{i_k}\right) = (*)
\end{aligned}$$

Z jednoznaczności rozkładu liczb naturalnych otrzymujemy, że

$$(*) = \sum_{n=1}^{\infty} f(n).$$

2 Ciała skończone

Ciała skończone mają zastosowanie w wielu dziedzinach takich jak kryptografia, czy teoria kodów.

Jak tworzyć ciała skończone $GF(p^n)$? Dla $n = 1$ bierzemy $\mathbb{Z}_p$.

Fakt 2.1. *$\mathbb{Z}_p$ jest ciałem.*

Dowód. Łatwo jest wykazać, że $\mathbb{Z}_p$ jest pierścieniem. Jedyną trudność sprawia wykazanie istnienia elementu odwrotnego. Niech $a \neq 0$.

Ponieważ a jest względnie pierwsze z p, więc z algorytmu Euklidesa wynika, że istnieją takie liczby $x, y \in \mathbb{Z}$, że $ax + py = 1$, skąd $ax \equiv 1 \pmod{p}$. Zatem x jest odwrotnością a w $\mathbb{Z}_p$.

Możemy udowodnić istnienie odwrotności bez wykorzystywania algorytmu Euklidesa. Rozważmy liczby

$$1a, 2a, \ldots, (p-1)a. \tag{2.1}$$

Jeśli $ai \equiv aj \pmod{p}$, to $p \mid a(i-j) \Rightarrow p \mid i-j \Leftrightarrow i \equiv j \pmod{p}$, zatem wszystkie liczby (2.1) są różne modulo p i dają cały zbiór $\{1, \ldots, p-1\}$. Tak więc będzie co najmniej jedna taka liczba x, że $ax \equiv 1 \pmod{p}$. $\square$

W przypadku gdy $n > 1$ postępujemy następująco.

Bierzemy wielomian f nad $\mathbb{Z}_p$ stopnia n, który jest nierozkładalny, wtedy

$$GF(p^n) = \mathbb{Z}_p[X]/_{\equiv_f},$$

Gdzie $\equiv_f$ oznacza przystawanie dwóch wielomianów modulo f, tzn. $g \equiv_f h \Leftrightarrow f \mid (g-h)$. Ciało takie zwykle reprezentujemy wszystkimi wielomianami stopnia mniejszego od n.

Przykład 2.2. $GF(4)$. Znajdźmy wielomian stopnia 2 nierozkładalny nad $\mathbb{Z}_2$, wykluczając wszystkie rozkładalne wielomiany.

$$\begin{aligned} x \cdot x &= x^2, \\ x \cdot (x+1) &= x^2 + x, \\ (x+1)(x+1) &= x^2 + 2x + 1 = x^2 + 1. \end{aligned}$$

Zatem jedynym nierozkładalnym wielomianem stopnia 2 nad $\mathbb{Z}_2$ jest $x^2 + x + 1$. Elementami tego ciała są $0, 1, x, x+1$. Operacje mnożenia i dodawania wykonujemy jak na zwykłych wielomianach z tym, że x^2 utożsamiamy z $-x-1 = x+1$, np.

$$x(x+1) = x^2 + x = x + 1 + x = 1.$$

W ten sposób tworzymy tabelkę działań dla $+$ i $\cdot$:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

3 Rozszerzony algorytm Euklidesa, a algorytm binarny

Liczymy NWD liczb 644 i 490:

$$\begin{aligned} 644 &= 1 \cdot 490 + 154 \\ 490 &= 3 \cdot 154 + 28 \\ 154 &= 5 \cdot 28 \quad + 14 \\ 28 &= 2 \cdot 14 \end{aligned}$$

oraz kombinację liniową:

$$\begin{aligned} 14 = 154 - 5 \cdot 28 = 154 - 5 \cdot (490 - 3 \cdot 154) &= -5 \cdot 490 + 16 \cdot 154 \\ &= -5 \cdot 490 + 16(644 - 1 \cdot 490) = 16 \cdot 644 - 21 \cdot 490. \end{aligned}$$

Teraz jeszcze raz liczymy $\mathrm{NWD}(644, 490)$ algorytmem binarnym. Wpierw wyciągamy 2 i zostaje nam policzyć $\mathrm{NWD}(322, 245)$.

$$\begin{aligned} 322/2 &= 161 & 245 - 161 &= 84 \\ 84/2^2 &= 21 & 161 - 21 &= 140 \\ 140/2^2 &= 35 & 35 - 21 &= 14 \\ 14/2 &= 7 & 21 - 7 &= 14 \\ 14/2 &= 7 & 7 - 7 &= 0 \end{aligned}$$

Pytanie: jak możemy teraz wyciągnąć kombinację liniową?

Żeby znaleźć odpowiedź zobaczmy jak wygląda rozszerzony algorytm Euklidesa. Dla liczb $a \geq b$ konstruujemy ciąg reszt $r_0 = a, r_1 = b, r_2, \ldots, r_n = \mathrm{NWD}(a, b), r_{n+1} = 0$. Dla każdej reszty r_i znajdujemy ponadto liczby t_i i s_i takie, że

$$t_i a + s_i b = r_i. \tag{3.1}$$

Na końcu otrzymujemy $t_n a + s_n b = \mathrm{NWD}(a, b)$.

Tak naprawdę w rozszerzonym algorytmie Euklidesa operujemy na trójkach liczb. Oznaczmy $K(a, b) = \{(r, t, s) \in \mathbb{Z}^3 \mid ta + sb = r\}$.

Fakt 3.1. *Zachodzą następujące własności trójek $K(a, b)$:*

(i) $(a, 1, 0) \in K(a, b)$,

(ii) $(b, 0, 1) \in K(a, b)$,

(iii) $(r, t, s), (r', t', s') \in K(a, b) \Rightarrow (r + r', t + t', s + s') \in K(a, b)$,

(iv) $(r, t, s) \in K(a, b) \Leftrightarrow (kr, kt, ks) \in K(a, b)$, *przy* $\Leftarrow$ *jest* $k \neq 0$,

	i	q_i	r_i	t_i	s_i
	0		644	1	0
	1		490	0	1
$644 = 1 \cdot 490 + 154$	2	1	154	$1 - 1 \cdot 0 = 1$	$0 - 1 \cdot 1 = -1$
$490 = 3 \cdot 154 + 28$	3	3	28	$0 - 3 \cdot 1 = -3$	$1 - 3 \cdot (-1) = 4$
$154 = 5 \cdot 28 + 14$	4	5	14	$1 - 5 \cdot (-3) = 16$	$-1 - 5 \cdot 4 = -21$
$28 = 2 \cdot 14$	5	2	0		

Tablica 1: Przebieg rozszerzonego Euklidesa dla 644 i 490.

(v) $(r, t, s) \in K(a, b) \Rightarrow (r, t \mp b, s \pm a) \in K(a, b)$.

Z $r_{i-2} = q_{i-1}r_{i-1} + r_i$ mamy $r_i = r_{i-2} - q_{i-1}r_{i-1}$, więc z własności (iii) i (iv) dostajemy, że jeśli $(r_{i-2}, t_{i-2}, s_{i-2}), (r_{i-1}, t_{i-1}, s_{i-1}) \in K(a, b)$, to

$$(r_{i-2} - q_{i-1}r_{i-1}, t_{i-2} - q_{i-1}t_{i-1}, s_{i-2} - q_{i-1}s_{i-1}) \in K(a, b).$$

Przyjmując $t_i = t_{i-2} - q_{i-1}t_{i-1}$ i $s_i = s_{i-2} - q_{i-1}s_{i-1}$ mamy $(r_i, t_i, s_i) \in K(a, b)$. Stosując te wzory w tablicy 1 zbudowaliśmy od przodu kombinację liniową

$$16 \cdot 644 - 21 \cdot 490 = 14.$$

Pokaże jak w podobny sposób uzyskiwać kombinację liniową w algorytmie binarnym.

Fakt 3.2. *Niech* $(r, t, s) \in K(a, b)$ *i* $2 \mid r$. *Jeśli* $2 \nmid a$, *a* $2 \mid s$, *to* $2 \mid t$.

Dowód. $2 \mid r - sb = at$, ponieważ $2 \nmid a$, więc $2 \mid t$. $\square$

Daje to następujący rozszerzony algorytm binarny. Wpierw dzielimy liczby a i b tak długo aż jedna z nich będzie nieparzysta. Niech $a = ea'$ i $b = eb'$, gdzie e jest potęgą dwójki. a' lub b' jest nieparzyste. Jeśli wyliczymy, że $d' = \mathrm{NWD}(a', b')$ oraz znajdziemy kombinację $t'a' + s'b' = d'$, to $\mathrm{NWD}(a, b) = d = ed'$ oraz $t'a + s'b = t'ea' + s'eb' = ed' = d$. Wystarczy zatem umieć liczyć NWD i kombinację liniową w przypadku, gdy jedna z liczb a i b jest nieparzysta.

W dalszej części założymy zatem, że $2 \nmid a$. Trójki $K(a, b)$ możemy odejmować. Chcielibyśmy trójkę (r, t, s) móc podzielić przez 2, jeśli $2 \mid r$. Jeśli $2 \mid s$, to z faktu 3.2 także $2 \mid t$ i na podstawie własności (iv) mamy $(r/2, t/2, s/2) \in K(a, b)$. Jeśli $2 \nmid s$, to $2 \mid s \pm a$, bo $2 \nmid a$. Zatem, aby uczynić s parzystym, zaburzamy je używając własności (v) i otrzymujemy trójkę $(r, t \mp a, s \pm a)$, którą możemy już podzielić przez 2. Pytanie jest, czy dodawać, czy odejmować, przy zaburzaniu? Generalnie nie ma to znaczenia, ale możemy trzymać wartość bezwzględną s jak najmniejszą, czyli dodawać a, gdy $s \geq 0$ i odejmować a, gdy $s < 0$.

W tablicy 2 otrzymaliśmy kombinację liniową $25 \cdot 245 - 19 \cdot 322 = 7$, skąd $25 \cdot 490 - 19 \cdot 644 = 14$.

Jeśli chcemy tylko znaleźć takie t, że $ts \equiv \mathrm{NWD}(a, b) \pmod{b}$, to w przypadku rozszerzonego algorytmu Euklidesa nie musimy pamiętać w ogóle wartości s. Taka optymalizacja nie jest możliwa w przypadku rozszerzonego algorytmu binarnego.

r	t	s
245	1	0
322	0	1
322	$0+322=322$	$1-245=-244$
$322/2=161$	$322/2=161$	$-244/2=-122$
$245-161=84$	$1-161=-160$	$0-(-122)=122$
$84/2=42$	$-160/2=-80$	$122/2=61$
42	$-80+322=242$	$61-245=-184$
$42/2=21$	$242/2=121$	$-184/2=-92$
$161-21=140$	$161-121=40$	$-122-(-92)=-30$
$140/2=70$	$40/2=20$	$-30/2=-15$
70	$20-322=-302$	$-15+245=230$
$70/2=35$	$-302/2=-151$	$230/2=115$
$35-21=14$	$-151-121=-272$	$115-(-92)=207$
14	$-272+322=50$	$207-245=-38$
$14/2=7$	$50/2=25$	$-38/2=-19$
$21-7=14$	$121-25=96$	$-92-(-19)=-73$
14	$96-322=-226$	$-73+245=172$
$14/2=7$	$-226/2=-113$	$172/2=86$
$7-7=0$		

Tablica 2: Przebieg rozszerzonego algorytmu binarnego dla 245 i 322.

4 Równania diofantyczne

Przykład 4.1.

$$12x + 8y = 6$$

Nie ma rozwiązań, bo $\mathrm{NWD}(12, 8) = 4 \nmid 6$.

Przykład 4.2.

$$12x + 21y = 27 \tag{4.1}$$

Ma rozwiązania, bo $\mathrm{NWD}(12, 21) = 3 \mid 27$. Liczymy NWD:

$$\begin{aligned} 21 &= 1 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 \quad + 3 \\ 9 &= 3 \cdot 3 \end{aligned}$$

oraz kombinację liniową:

$$3 = 12 - 1 \cdot 9 = 12 - (21 - 1 \cdot 12) = 12 \cdot 2 + 21 \cdot (-1),$$

skąd mamy

$$12 \cdot 2 + 21 \cdot (-1) = 3,$$

przemnażające obie strony przez 9 otrzymujemy

$$12 \cdot 18 + 21 \cdot (-9) = 27. \tag{4.2}$$

Odejmując równania (4.1) i (4.2) stronami otrzymujemy

$$12(x - 18) + 21(y + 9) = 0.$$

Dzielimy przez NWD$(12, 21) = 3$ i mamy

$$4(x - 18) + 7(y + 9) = 0. \tag{4.3}$$

Wszystkie rozwiązania równania postaci $a'x' = b'y'$, gdzie NWD$(a', b') = 1$ są postaci $x' = b't, y' = a't$ dla dowolnego całkowitego t. Zatem wszystkie rozwiązania (4.3) są postaci: $x - 18 = 7t, y + 9 = -4t$, skąd rozwiązanie ogólne $x = 18 + 7t, y = -9 - 4t$.

Metoda znajdowania rozwiązań równań diofantycznych stosuje się także do np. równań diofantycznych na wielomianach.

Ćwiczenie 4.3. Rozwiązać następujące równania diofantyczne:

$$\begin{aligned} 27x - 13y &= 17 \\ 21x + 35y &= 63 \\ 118x - 96y &= 38 \end{aligned}$$

5 Algorytm Euklidesa dla wielomianów

5.1 Dzielenie z resztą

Dla każdych dwóch wielomianów $a, b \in \mathbb{K}[X]$ istnieją wielomiany $q, r \in \mathbb{K}[X]$ takie, że

$$a = qb + r, \qquad \deg r < \deg b.$$

Dzielenie to wykonujemy podobnie jak dzielenie pisemne, z tym że podstawą nie jest 10 tylko X.

Przykład 5.1. Dzielenie wielomianów $x^4 - x^3 + x^2 - x + 1$ i $x^2 + x + 1$ w $\mathbb{Q}[X]$.

		x^2	$-2x$	2	
x^4	$-x^3$	x^2	$-x$	1	$: x^2 + x + 1$
x^4	x^3	x^2			
	$-2x^3$		$-x$		
	$-2x^3$	$-2x^2$	$-2x$		
		$2x^2$	x	1	
		$2x^2$	$2x$	2	
			$-x$	-1	

skąd $x^4 - x^3 + x^2 - x + 1 = (x^2 - 2x + 2)(x^2 + x + 1) + (-x - 1)$.

5.2 NWD

Do liczenia NWD używamy algorytmu Euklidesa zupełnie analogicznie jak dla liczba naturalnych, z tymże używamy dzielenia z resztą dla wielomianów.

Przykład 5.2. Policzmy NWD(a, b), gdzie $a = x^4 - 4x^3 + 6x^2 - 4x + 1 = r_0$ i $b = x^3 - x^2 + x - 1 = r_1$. Mamy:

$$\begin{aligned} r_0 &= (x - 3) \cdot r_1 + r_2, & r_2 &= 2x^2 - 2, \\ r_1 &= \left(\frac{1}{2}x - \frac{1}{2}\right) \cdot r_2 + r_3, & r_3 &= 2x - 2, \\ r_2 &= (x + 1) \cdot r_3. \end{aligned}$$

Zatem NWD$(a, b) = 2x - 2$, czyli NWD$(a, b) = x - 1$.

5.3 Kombinacja liniowa

Analogicznie jak dla liczb całkowitych możemy znajdować kombinację liniową $au + bv = \mathrm{NWD}(a, b)$ przy czym a, b, u, v są wielomianami.

Przykład 5.3. Niech a i b jak w przykładzie 5.2. Mamy

$$\begin{aligned}\mathrm{NWD}(a,b) = r_3 = r_1 - \left(\frac{1}{2}x - \frac{1}{2}\right) \cdot r_2 = r_1 - \left(\frac{1}{2}x - \frac{1}{2}\right) \cdot \big(r_0 - (x-3) \cdot r_1\big) \\ = \left(1 + \left(\frac{1}{2}x - \frac{1}{2}\right) \cdot (x-3)\right) \cdot r_1 - \left(\frac{1}{2}x - \frac{1}{2}\right) \cdot r_0 \\ = \left(\frac{1}{2}x^2 - 2x + \frac{5}{2}\right) \cdot b - \left(\frac{1}{2}x - \frac{1}{2}\right) \cdot a.\end{aligned}$$

6 Układ równań liniowych

Przykład 6.1.

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 3 \pmod 7 \\ x \equiv 7 \pmod{11} \end{cases} \tag{6.1}$$

Rozwiązanie budujemy z trzech części:

$$x = A + B + C,$$

gdzie

$$\begin{cases} A \equiv 2 \pmod 6 \\ A \equiv 0 \pmod 7 \\ A \equiv 0 \pmod{11} \end{cases} \qquad \begin{cases} B \equiv 0 \pmod 6 \\ B \equiv 3 \pmod 7 \\ B \equiv 0 \pmod{11} \end{cases} \qquad \begin{cases} C \equiv 0 \pmod 6 \\ C \equiv 0 \pmod 7 \\ C \equiv 7 \pmod{11} \end{cases}$$

Przyjmujemy

$$A = 7 \cdot 11 \cdot a \cdot 2 \qquad B = 6 \cdot 11 \cdot b \cdot 3 \qquad C = 6 \cdot 7 \cdot c \cdot 7,$$

gdzie a, b, c dobieramy tak, aby

$$7 \cdot 11 \cdot a \equiv 1 \pmod 6 \quad 6 \cdot 11 \cdot b \equiv 1 \pmod 7 \quad 6 \cdot 7 \cdot c \equiv 1 \pmod{11}.$$

Liczymy

$$5 \cdot a \equiv 1 \pmod 6 \qquad 3 \cdot b \equiv 1 \pmod 7 \qquad 9 \cdot c \equiv 1 \pmod{11}$$

W pierwszym odwrotnością -1 jest -1, czyli $a = 5$. W drugim $3 \cdot 2 \equiv -1$ zatem $3 \cdot (-2) \equiv 1$, skąd $b \equiv -2 = 5$. W trzecim zastosujemy Euklidesa. $11 = 9 + 2$, $9 = 2 \cdot 4 + 1$, $1 = 9 - 2 \cdot 4 = 9 - (11 - 9) \cdot 4 = 9 \cdot 5 - 11 \cdot 4$, czyli $c = 5$. Ostatecznie mamy rozwiązanie (6.1):

$$x = 7 \cdot 11 \cdot 5 \cdot 2 + 6 \cdot 11 \cdot 5 \cdot 3 + 6 \cdot 7 \cdot 5 \cdot 7 = 3230 \equiv 458 \pmod{462}.$$

7 Kongruencje liniowe - ćwiczenia

Ćwiczenie 7.1. Udowodnić, że liczb pierwszych postaci $4m+3$ jest nieskończenie wiele.

Rozwiązanie. Załóżmy, że $p_1, \ldots, p_k$ są wszystkimi liczbami pierwszymi postaci $4m + 3$. Weźmy liczbę $q = 4p_1 \cdots p_k + 3$. Nie jest ona podzielna przez żadną z liczb $p_1, \ldots, p_k$, nie jest też podzielna przez 2, a zatem jest podzielna tylko przez liczby pierwsze postaci $4m + 1$, ale iloczyn takich liczb pierwszych też jest tej postaci, a q nie jest — sprzeczność. □

Ćwiczenie 7.2. Udowodnić, że liczb pierwszych postaci $6m+5$ jest nieskończenie wiele.

Ćwiczenie 7.3. Udowodnić, że istnieje nieskończenie wiele liczb złożonych postaci $a_n x^n + \cdots + a_1 x + a_0$, gdzie $n \geq 1$ i $a_n \neq 0$.

Rozwiązanie.

$$f(c) \mid f\big(c + f(c)t\big) \text{ dla dowolnego } t.$$

□

Ćwiczenie 7.4 (Turnieje). Załóżmy, że liczba drużyn n jest parzysta. Turniejem nazywamy takie rozgrywki, które

- składają się z $n - 1$ kolejek,
- w każdej kolejce każda drużyna rozgrywa dokładnie jeden mecz,
- każda para drużyn rozegra jeden mecz w turnieju.

W meczu grają dwie drużyny przy czym jedna gra u siebie, a druga gra na wyjeździe. Skonstruuj taki turniej, aby liczba sytuacji, takich, że jakaś drużyna w dwóch kolejkach pod rząd gra u siebie, albo w dwóch kolejkach pod rząd gra na wyjeździe była minimalna.

$$ax \equiv b \pmod{n} \tag{7.1}$$

Ćwiczenie 7.5. Kiedy kongruencja (7.1) ma rozwiązanie? Ile ma rozwiązań?

Rozwiązanie. Rozwiązanie jest wtw., gdy istnieje y, że $ny = ax - b$, czyli wtedy, gdy następujące rozwiązanie diofantyczne ma rozwiązanie:

$$ax - ny = b, \tag{7.2}$$

czyli wtedy, gdy $d = \mathrm{NWD}(a, n) \mid b$.

Ile jest rozwiązań (7.1) jak $d \mid b$? Niech $a = a'd, n = n'd, b = b'd$. Niech x_0, y_0 będzie rozwiązaniem

$$a'x_0 - n'y_0 = b',$$

wtedy wszystkie rozwiązania (7.2) są postaci $x = x_0 + n't, y = y_0 + a't$.

Ile jest różnych liczb postaci $x_0 + n't$ modulo n? Ponieważ $n = n'd$, więc takich liczb jest d. Zatem (7.1) ma d rozwiązań. □

8 Reszty kwadratowe

8.1 Reszty kwadratowe

Definicja 8.1. Liczbę a, $NWD(a,p) = 1$ nazywamy resztą kwadratową modulo p, jeśli istnieje x, że
$$x^2 \equiv a \pmod{p}.$$

Ile jest reszt kwadratowych modulo p?

Fakt 8.2. *Reszt kwadratowych modulo liczba pierwsza p jest $\frac{p-1}{2}$.*

Dowód. Zbiór wszystkich reszt kwadratowych to:
$$P = \{1^2, 2^2, \ldots, (p-1)^2\} = \left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\},$$
gdyż dla $\frac{p-1}{2} < i \leq p-1$ jest $i^2 \equiv (p-i)^2 \pmod{p}$ i $p - i \leq \frac{p-1}{2}$. Pokażemy, że wszystkie liczby w zbiorze P są różne. Niech $i, j \in \left\{1, \ldots, \frac{p-1}{2}\right\}$ oraz $i^2 \equiv j^2 \pmod{p}$. Wtedy $p \mid i^2 - j^2$, czyli $p \mid (i-j)(i+j)$. Ponieważ $0 < i + j \leq \frac{p-1}{2} + \frac{p-1}{2} = p - 1$, więc $p \nmid i + j$, zatem $p \mid i - j$, czyli $i \equiv j \pmod{p}$, skąd $i = j$. □

Wniosek 8.3. *Niereszt kwadratowych modulo p jest $\frac{p-1}{2}$.*

8.2 Symbol Legendre

Definicja 8.4. Dla nieparzystej liczby pierwszej p symbolem Legendre $\left(\frac{a}{p}\right)$ nazywamy:
$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{jeśli } a \text{ jest resztą kwadratową modulo } p \\ -1 & \text{jeśli } a \text{ jest nieresztą kwadratową modulo } p \\ 0 & \text{jeśli } p \mid a \end{cases}$$

Twierdzenie 8.5 (Kryterium Eulera)**.**
$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Dowód. Jeśli $p \mid a$, to $a \equiv 0 \pmod{p}$ i wtedy $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$. Zatem niech $\mathrm{NWD}(a,p) = 1$. Z małego twierdzenia Fermata mamy:
$$a^{p-1} \equiv 1 \pmod{p},$$
skąd
$$p \mid a^{p-1} - 1,$$
$$p \mid \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right).$$

Zauważmy, że p nie może jednocześnie dzielić $a^{\frac{p-1}{2}} - 1$ i $a^{\frac{p-1}{2}} + 1$, gdyż w przeciwnym razie $p \mid 2$. Zatem zachodzi dokładnie jedna z możliwości:
$$p \mid a^{\frac{p-1}{2}} - 1 \qquad \text{albo} \qquad p \mid a^{\frac{p-1}{2}} + 1,$$

czyli

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p \qquad \text{albo} \qquad a^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Jeśli $\left(\frac{a}{p}\right) = 1$, to istnieje b, że $a \equiv b^2 \pmod p$, skąd

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod p.$$

Równanie

$$x^{\frac{p-1}{2}} \equiv 1 \pmod p$$

ma co najwyżej $\frac{p-1}{2}$ rozwiązań, a ponieważ spełniają je wszystkie reszty kwadratowe i jest ich $\frac{p-1}{2}$, więc tego równania nie może spełniać niereszta kwadratowa. Zatem jeśli $\left(\frac{a}{p}\right) = -1$, to $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Możemy też udowodnić w inny sposób to, że jeśli $\left(\frac{a}{p}\right) = -1$, to $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. Zauważmy, że jeśli $cd \equiv a \pmod p$, to $c \neq d$, bo a jest nieresztą kwadratową. Zatem mamy

$$a^{\frac{p-1}{2}} = \prod_{\substack{\{c,d\} \in \{1,\ldots,p-1\} \\ cd \equiv a \pmod p}} cd = (p-1)! \equiv -1 \pmod p$$

z twierdzenia Wilsona. □

Twierdzenie 8.6 (Własności symbolu Legendre)**.** *Dla nieparzystych liczb pierwszych p i q oraz całkowitych a i b zachodzi:*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ dla } a \equiv b \pmod p, \tag{8.1}$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \tag{8.2}$$

$$\left(\frac{a^2}{p}\right) = 1, \tag{8.3}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases} \tag{8.4}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases} \tag{8.5}$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} 1 & p \equiv 1 \text{ lub } q \equiv 1 \pmod 4 \\ -1 & p \equiv q \equiv 3 \pmod 4 \end{cases} \tag{8.6}$$

Własność (8.6) *nazywana jest prawem wzajemności i może być zapisana jako:*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & p \equiv 1 \text{ lub } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & p \equiv q \equiv 3 \pmod 4 \end{cases}$$

8.3 Symbol Jacobiego

Definicja 8.7. Dla nieparzystej liczby $n > 2$ o rozkładzie na czynniki $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ symbolem Jacobiego nazywamy liczbę

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Przy takiej definicji, jeśli n jest pierwsze, to $\left(\frac{a}{n}\right)$ jest symbolem Legendre.

Twierdzenie 8.8 (Własności symbolu Jacobiego)**.** *Dla nieparzystych liczb pierwszych n i m oraz całkowitych a i b zachodzi:*

$$\left(\frac{a}{n}\right) \in \{0, 1, -1\} \tag{8.7}$$

$$\left(\frac{a}{n}\right) = 0 \textit{ jeśli } \mathrm{NWD}(a, n) \neq 1 \tag{8.8}$$

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) \textit{ dla } a \equiv b \pmod n, \tag{8.9}$$

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right), \tag{8.10}$$

$$\left(\frac{a^2}{n}\right) = 1, \tag{8.11}$$

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & n \equiv 1 \pmod 4 \\ -1 & n \equiv 3 \pmod 4 \end{cases} \tag{8.12}$$

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & n \equiv \pm 1 \pmod 8 \\ -1 & n \equiv \pm 3 \pmod 8 \end{cases} \tag{8.13}$$

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}} = \begin{cases} 1 & n \equiv 1 \textit{ lub } m \equiv 1 \pmod 4 \\ -1 & n \equiv m \equiv 3 \pmod 4 \end{cases} \tag{8.14}$$

Jaki jest związek między symbolem Jacobiego, a resztami kwadratowymi modulo n? Tzn. co nam mówi $\left(\frac{a}{n}\right)$ o rozwiązywalności równania $x^2 \equiv a \pmod n$?

Jeśli a jest resztą kwadratową modulo n, to jest też resztą kwadratową modulo dowolny dzielnik n, więc wtedy $\left(\frac{a}{n}\right) = 1$. Zatem jeśli $\left(\frac{a}{n}\right) = -1$, to a jest nieresztą kwadratową modulo n.

Odwrotne implikacje nie są prawdziwe, bo istnieją a i n takie, że $\left(\frac{a}{n}\right) = 1$ i a jest nieresztą kwadratową modulo n. Przykładem jest $a = 2$ i $n = 15$. Wtedy

$$\left(\frac{2}{15}\right) \stackrel{(8.13)}{=} 1,$$

ale wszystkie reszty kwadratowe to:

i	1	2	3	4	5	6	7
i^2	1	4	9	1	10	6	4

Przykład 8.9. Sprawdzić, czy równanie $x^2 \equiv 127 \pmod{307}$ ma rozwiązanie. 307 jest pierwsza, więc liczymy symbol Legendre przy użyciu symbolu Jacobiego:

$$\left(\frac{127}{307}\right) \overset{(8.14)}{=} -\left(\frac{307}{127}\right) \overset{(8.9)}{=} -\left(\frac{53}{127}\right) \overset{(8.14)}{=} -\left(\frac{127}{53}\right) \overset{(8.9)}{=} -\left(\frac{21}{53}\right)$$
$$\overset{(8.14)}{=} -\left(\frac{53}{21}\right) \overset{(8.9)}{=} -\left(\frac{11}{21}\right) \overset{(8.14)}{=} -\left(\frac{21}{11}\right) \overset{(8.9)}{=} -\left(\frac{-1}{11}\right) \overset{(8.12)}{=} -(-1) = 1.$$

Zatem 127 jest resztą kwadratową i równanie ma rozwiązanie.

Przykład 8.10. Sprawdzić, czy równanie $x^2 \equiv 217 \pmod{313}$ ma rozwiązanie. 313 jest pierwsza, więc podobnie jak poprzednio liczymy symbol Legendre przy użyciu symbolu Jacobiego:

$$\left(\frac{217}{313}\right) \overset{(8.14)}{=} \left(\frac{313}{217}\right) \overset{(8.9)}{=} \left(\frac{96}{217}\right) = \left(\frac{2^5 \cdot 3}{217}\right) \overset{(8.10)\text{ i }(8.11)}{=} \left(\frac{2}{217}\right)\left(\frac{3}{217}\right)$$
$$\overset{(8.13)\text{ i }(8.14)}{=} 1 \cdot \left(\frac{217}{3}\right) \overset{(8.9)}{=} \left(\frac{1}{3}\right) = 1.$$

Zatem znowu dane równanie ma rozwiązanie.

Przykład 8.11. Sprawdzić, czy równanie $x^2 \equiv 127 \pmod{313}$ ma rozwiązanie.

$$\left(\frac{127}{313}\right) \overset{(8.14)}{=} \left(\frac{313}{127}\right) \overset{(8.9)}{=} \left(\frac{59}{127}\right) \overset{(8.14)}{=} -\left(\frac{127}{59}\right) \overset{(8.9)}{=} -\left(\frac{9}{59}\right) \overset{(8.11)}{=} -1$$

Tym razem dane równanie nie ma rozwiązania.

8.4 Dowód własności symbolu Legendre

Wszystkie własności oprócz (8.5) i (8.6) wynikają bezpośrednio z kryterium Eulera. Do udowodnienia tych dwóch własności będzie potrzebny lemat Gaussa.

Twierdzenie 8.12 (Lemat Gaussa)**.**

$$\begin{aligned} S &= \left\{1, 2, \ldots, \frac{p-1}{2}\right\}, \\ aS &= \{ai \mid i \in S\} = \left\{1a, 2a, \ldots, \frac{p-1}{2}a\right\}, \\ U &= aS \setminus S, \end{aligned}$$

przy czym wszystkie operacje wykonujemy modulo p. Wtedy

$$\left(\frac{a}{p}\right) = (-1)^{|U|}.$$

Dowód. Niech liczby $r_i \in S$ i $\epsilon_i \in \{-1, 1\}$ dla $i \in S$ będą jednoznacznie wyznaczone przez:

$$ai \equiv \epsilon_i r_i \pmod{p}. \tag{8.15}$$

Załóżmy, że $r_i = r_j$ dla pewnych $i, j \in S$, wtedy

$$ai\epsilon_j r_j \equiv aj\epsilon_i r_i \pmod{p},$$

skąd

$$i\epsilon_j \equiv j\epsilon_i \pmod p,$$

zatem

$$i \equiv \pm j \pmod p.$$

$i \equiv -j \pmod p$ jest niemożliwe, bo $1 \leq i+j \leq \frac{p-1}{2} + \frac{p-1}{2} = p-1$, więc $p \not| \, i+j$. Pozostaje zatem $i = j$. Pokazaliśmy zatem, że

$$\{r_i \mid i \in S\} = S, \tag{8.16}$$

skąd

$$\prod_{i \in S} ai \overset{(8.15)}{\equiv} \prod_{i \in S} \epsilon_i r_i \overset{(8.16)}{\equiv} \prod_{i \in S} \epsilon_i \prod_{i \in S} i \pmod p.$$

Dzieląc obie strony przez $\prod_{i \in S} i$ otrzymujemy

$$\prod_{i \in S} a \equiv \prod_{i \in S} \epsilon_i \pmod p.$$

Z kryterium Eulera mamy

$$\prod_{i \in S} a = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p,$$

skąd ostatecznie

$$\left(\frac{a}{p}\right) = \prod_{i \in S} \epsilon_i. \tag{8.17}$$

Teraz wystarczy zauważyć, że w iloczynie $\prod_{i \in S} \epsilon_i$ liczba -1 występuje tyle razy ile jest elementów U. Wynika to stąd, że jeśli $ai \in S$, to $\epsilon_i = 1$, a jeśli $ai \notin S$, to $\epsilon_i = -1$. □

Uwaga 8.13. Twierdzenie 8.12 możemy uogólnić, biorąc za S dowolny zbiór taki, że dla każdego $x \not\equiv 0 \pmod p$ istnieje dokładnie jeden element $y \in S$, że $x \equiv \pm y \pmod p$ co możemy zapisać jako $x^2 \equiv y^2 \pmod p$.

Zbadajmy parzystość liczby $\left\lfloor \frac{2ai}{p} \right\rfloor$. Z (8.15) wiemy, że istnieje całkowita liczba t taka, że

$$ai = tp + \epsilon_i r_i,$$

skąd

$$2ai = 2t \cdot p + \epsilon_i \cdot 2r_i.$$

Zauważmy, że $1 \leq 2r_i \leq p-1$, zatem

$$\left\lfloor \frac{2ai}{p} \right\rfloor = \begin{cases} 2t & \text{jeśli } \epsilon_i = 1 \\ 2t-1 & \text{jeśli } \epsilon_i = -1 \end{cases}$$

skąd

$$(-1)^{\left\lfloor \frac{2ai}{p} \right\rfloor} = \epsilon_i.$$

Z równości (8.17) mamy zatem

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i \in S} \left\lfloor \frac{2ai}{p} \right\rfloor} \tag{8.18}$$

Załóżmy, że a jest nieparzyste, wtedy $a+p$ będzie parzyste. Korzystając z tego przekształcamy:

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\cdot\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) \overset{(8.18)}{=} (-1)^{\sum_{i\in S}\left\lfloor\frac{(a+p)i}{p}\right\rfloor}$$
$$= (-1)^{\sum_{i\in S}\left\lfloor\frac{ai}{p}\right\rfloor + \sum_{i\in S} i} = (-1)^{\sum_{i\in S}\left\lfloor\frac{ai}{p}\right\rfloor + \frac{p^2-1}{8}} \tag{8.19}$$

Wstawiając do tego równania $a = 1$ otrzymujemy

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \tag{8.20}$$

co dowodzi własności (8.13).

Przejdźmy do dowodu własności (8.14). Na podstawie równości (8.19) i (8.20) łatwo otrzymujemy następujący lemat.

Lemat 8.14. *Dla nieparzystego a zachodzi:*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i\in S}\left\lfloor\frac{ai}{p}\right\rfloor} \tag{8.21}$$

Dowód. Dzieląc równości (8.19) i (8.20) i korzystając z tego, że

$$\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right)$$

otrzymujemy żądaną równość. □

Niech teraz p i q będą nieparzystymi liczbami pierwszymi. Niech R oznacza zbiór punktów

$$R = \left\{(x,y) \mid x \in \left\{1,\ldots,\frac{p-1}{2}\right\}, y \in \left\{1,\ldots,\frac{q-1}{2}\right\}\right\}$$

Podzielimy ten zbiór na dwa mniejsze prostą $py = qx$ (rysunek 8.4). Definiujemy zbiory R_1 i R_2:

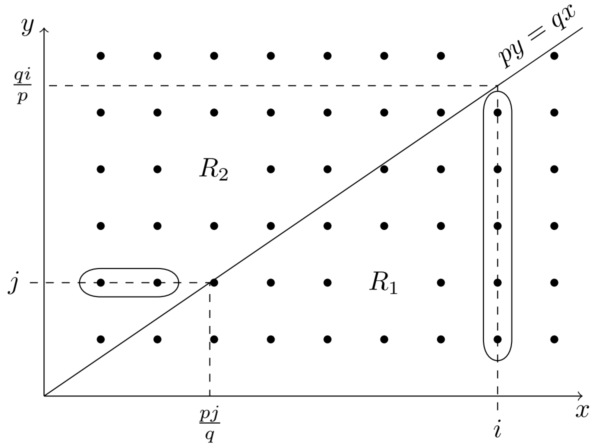
$$R_1 = \{(x,y) \in R \mid py < qx\}$$
$$R_2 = \{(x,y) \in R \mid py > qx\}$$

Zbiory R_1 i R_2 w sumie dają zbiór R, gdyż równanie $py = qx$ nie ma rozwiązań dla $1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}$. Zatem

$$|R_1| + |R_2| = |R|. \tag{8.22}$$

Policzymy liczbę elementów zbioru R_1. Ustalmy $i = 1,\ldots,\frac{p-1}{2}$. Ile jest takich y, że $(i,y) \in R_1$? Z definicji R_1 wynika, że musi być $y < \frac{qi}{p}$, więc takich y jest dokładnie $\left\lfloor\frac{qi}{p}\right\rfloor$. Mamy zatem

$$|R_1| = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor\frac{qi}{p}\right\rfloor \tag{8.23}$$



Rysunek 1: Zbiory R_1 i R_2

Analogicznie liczymy liczbę elementów zbioru R_2. Ustalamy $j = 1, \ldots, \frac{q-1}{2}$. Z definicji R_2 mamy $x < \frac{pj}{q}$, więc jest dokładnie $\left\lfloor \frac{qi}{p} \right\rfloor$ takich x, że $(x, j) \in R_2$, skąd

$$|R_2| = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor \tag{8.24}$$

Z drugiej strony mamy oczywistą równość

$$|R| = \frac{p-1}{2} \cdot \frac{q-1}{2} \tag{8.25}$$

Wstawiając (8.23), (8.24) i (8.25) do równania (8.22) otrzymujemy

$$\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

skąd

$$(-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor} (-1)^{\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Korzystając dwukrotnie z lematu 8.14 ostatecznie otrzymujemy

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

co kończy dowód własności (8.14)

8.5 Dowód własności symbolu Jacobiego

W celu udowodnienia własności symbolu Jacobiego zauważmy, że definicję 8.7 można napisać inaczej.

Mianowicie jeśli n jest nieparzysta z rozkładem na liczby pierwsze (niekoniecznie różne) $n = p_1 \cdots p_k$, to

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right)$$

Większość własności wynika wprost z definicji i własności symbolu Legendre. Jedynie własności (8.12), (8.13) i (8.14) wymagają dowodu. Dowody tych własności sprowadzają się do następującego lematu.

Lemat 8.15. *Niech n będzie nieparzysta z rozkładem na niekoniecznie różne czynniki pierwsze $n = p_1 \cdots p_k$. Wtedy zachodzi:*

$$\frac{n-1}{2} \equiv \sum_{i=1}^{k} \frac{p_i - 1}{2} \pmod 2 \tag{8.26}$$

$$\frac{n^2-1}{8} \equiv \sum_{i=1}^{k} \frac{p_i^2 - 1}{8} \pmod 2 \tag{8.27}$$

Dowód. Indukcja po k.

1. Dla $k = 1$ mamy po prostu równości.
2. Niech $m = np_{k+1}$, gdzie $m = p_1 \cdots p_k$. Mamy

$$\begin{aligned}\frac{m-1}{2} = \frac{np_{k+1}-1}{2} &= \frac{\left(1+2\frac{n-1}{2}\right)\left(1+2\frac{p_{k+1}-1}{2}\right)-1}{2}\\ &= \frac{2\frac{n-1}{2}+2\frac{p_{k+1}-1}{2}+4\frac{n-1}{2}\cdot\frac{p_{k+1}-1}{2}}{2} \equiv \frac{n-1}{2}+\frac{p_{k+1}-1}{2}\\ &\overset{(8.26)}{\equiv} \sum_{i=1}^{k+1}\frac{p_i-1}{2} \pmod 2\end{aligned}$$

oraz

$$\begin{aligned}\frac{m^2-1}{8} = \frac{n^2p_{k+1}^2-1}{8} &= \frac{\left(1+8\frac{n^2-1}{8}\right)\left(1+8\frac{p_{k+1}^2-1}{8}\right)-1}{8}\\ &= \frac{8\frac{n^2-1}{8}+8\frac{p_{k+1}^2-1}{8}+64\frac{n^2-1}{8}\cdot\frac{p_{k+1}^2-1}{8}}{8} \equiv \frac{n^2-1}{8}+\frac{p_{k+1}^2-1}{8}\\ &\overset{(8.27)}{\equiv} \sum_{i=1}^{k+1}\frac{p_i^2-1}{8} \pmod 2\end{aligned}$$

□

Niech teraz n i m będą nieparzyste o rozkładach na niekoniecznie różne czynniki pierwsze $n = p_1 \cdots p_k$ i $m = q_1 \cdots q_l$. Przekształcamy.

$$\left(\frac{-1}{n}\right) = \prod_{i=1}^{k}\left(\frac{-1}{p_i}\right) = \prod_{i=1}^{k}(-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^{k}\frac{p_i-1}{2}} \overset{(8.26)}{=} (-1)^{\frac{n-1}{2}},$$

co dowodzi własności (8.12).

$$\left(\frac{2}{n}\right) = \prod_{i=1}^{k}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{k}(-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_{i=1}^{k}\frac{p_i^2-1}{8}} \overset{(8.27)}{=} (-1)^{\frac{n^2-1}{8}},$$

co dowodzi własności (8.13).

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}$$
$$= (-1)^{\sum_{i=1}^{k}\frac{p_i-1}{2}\sum_{j=1}^{l}\frac{q_j-1}{2}} \overset{(8.26)}{=} (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}},$$

co dowodzi własności (8.14).

8.6 Ćwiczenia na reszty kwadratowe

Ćwiczenie 8.16. Rozwiązać równanie

$$x^2 + 1 \equiv 0 \pmod{p}. \tag{8.28}$$

Rozwiązanie. Sprawdzamy, czy (8.28) ma rozwiązanie, czyli, czy -1 jest resztą kwadratową modulo p. Z własności (8.4) wiemy, że

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p = 4m+1 \\ -1 & p = 4m+3 \end{cases}$$

Zatem (8.28) ma rozwiązanie tylko wtedy, gdy $p = 4m+1$. Z twierdzenia Wilsona mamy

$$(p-1)! \equiv -1 \pmod{p},$$

ale

$$(p-1)! = 1\cdot\dots\cdot(2m)\cdot(2m+1)\cdot\dots\cdot(4m) \equiv 1\cdot\dots\cdot(2m)\cdot(-2m)\cdot\dots\cdot(-1) = \big((2m)!\big)^2$$

Zatem rozwiązaniem (8.28) jest $x = \pm(2m)!$. □

Ćwiczenie 8.17. Wykazać, że liczb pierwszych postaci $4m+1$ jest nieskończenie wiele.

Rozwiązanie. Niech $p_1, \dots, p_k$ będą wszystkimi liczbami pierwszymi postaci $4m+1$. Niech p będzie dzielnikiem pierwszym liczby $(2p_1\cdots p_k)^2+1$. Oczywiście $p \neq p_1, \dots, p_k$. Zauważmy, że

$$(2p_1\cdots p_k)^2 \equiv -1 \pmod{p},$$

czyli -1 jest resztą kwadratową modulo p, a zatem $p \equiv 1 \pmod{4}$. Zatem p jest inną liczbą pierwszą postaci $4m+1$ — sprzeczność. □

Ćwiczenie 8.18. Wykazać, że liczb pierwszych postaci $6m+1$ jest nieskończenie wiele.

Wskazówka. $x^2 + 3 \equiv 0 \pmod{p}$ ma rozwiązanie wtw., gdy $p = 6m+1$. □

Ćwiczenie 8.19. Kiedy równanie

$$x^2 + 2 \equiv 0 \pmod{p}. \tag{8.29}$$

ma rozwiązanie?

Rozwiązanie. Liczymy

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1,3 \pmod{8} \\ -1 & p \equiv 5,7 \pmod{8} \end{cases}$$

Zatem (8.29) ma rozwiązanie gdy $p \equiv 1, 3 \pmod{8}$. □

9 Pseudopierwszość i testy pierwszości

9.1 Pseudopierwszość Eulera

Definicja 9.1. Nieparzystą liczbę n nazywamy liczbą pseudopierwszą Eulera przy podstawie a, $\mathrm{NWD}(a, n) = 1$, jeśli

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}. \tag{9.1}$$

W skrócie będziemy pisać, że n jest pp. Eulera przy podstawie a.

Jeśli n jest liczbą pierwszą, to (9.1) jest spełnione z kryterium Eulera.

Fakt 9.2. *Jeśli n jest liczbą złożoną, to wśród liczb z $\mathbb{Z}_n^*$ jest co najmniej połowa podstaw, przy których n nie jest pp. Eulera.*

Dowód. Dowód przebiega w czterech krokach.

1. Jeśli n jest pp. Eulera przy podstawie a i nie jest pp. Eulera przy podstawie b, to n nie jest pp. Eulera przy podstawie ab:

$$(ab)^{\frac{n-1}{2}} = a^{\frac{n-1}{2}} b^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) b^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right) \pmod{n}$$

2. Jeśli istnieje podstawa $b \in \mathbb{Z}_n^*$ przy której n nie jest pp. Eulera, to wtedy podstaw z $\mathbb{Z}_n^*$, przy których n nie jest pp. Eulera jest co najmniej tyle ile podstaw, przy których n jest pp. Eulera. Wystarczy zauważyć, że funkcja $f(a) = ab$ jest 1–1 w $\mathbb{Z}_n^*$, i dla podstawy przy której n jest pp. Eulera daje podstawę, przy której n jest nie jest pp. Eulera.

   W dalszej części udowodnimy, że takie b istnieje.

3. Istnieje liczba pierwsza p, że $p^2 \mid n$. Wtedy $n = p^2 t$ dla pewnego t. Przyjmujemy $b = pt + 1$. Mamy $\mathrm{NWD}(b, n) = 1$, bo $tn - (pt - 1)b = tp^2 t - (pt - 1)(pt + 1) = 1$. Dalej

$$\left(\frac{b}{n}\right) = \left(\frac{pt+1}{p^2 t}\right) = \left(\frac{pt+1}{p}\right)^2 \left(\frac{pt+1}{t}\right) = 1 \cdot 1 = 1$$

   Zastanówmy się dla jakich i jest $b^i \equiv 1 \pmod{n}$, czyli kiedy $n \mid b^i - 1$.

$$b^i - 1 = (1 + pt)^i - 1 = pt\big(1 + (1 + pt) + \cdots + (1 + pt)^{i-1}\big)$$

Zatem $p^2 t \mid b^i - 1$ jeśli $p \mid 1 + (1+pt) + \cdots + (1+pt)^{i-1}$, ale

$$1 + (1+pt) + \cdots + (1+pt)^{i-1} \equiv \underbrace{1 + 1 + \cdots + 1}_{i} \equiv i \pmod p$$

Mamy zatem, że $n \mid b^i - 1$, jeśli $p \mid i$. Wiemy też, że $p \nmid \frac{n-1}{2}$, zatem

$$b^{\frac{n-1}{2}} \not\equiv 1 \pmod n$$

4. n rozkłada się na iloczyn różnych liczb pierwszych. Niech $n = p_1 \cdots p_k \cdot p$. Niech b' będzie nieresztą kwadratową modulo p. Z chińskiego twierdzenia o resztach b bierzemy tak, aby

$$\begin{cases} b \equiv 1 \pmod{p_1} \\ \quad \cdots \\ b \equiv 1 \pmod{p_k} \\ b \equiv b' \pmod p \end{cases}$$

skąd

$$\left(\frac{b}{p_1}\right) = \cdots = \left(\frac{b}{p_k}\right) = 1$$

oraz

$$\left(\frac{b}{p}\right) = \left(\frac{b'}{p}\right) = -1,$$

zatem

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right) \cdots \left(\frac{b}{p_k}\right) \left(\frac{b}{p}\right) = -1$$

Z drugiej strony nie może być

$$b^{\frac{n-1}{2}} \equiv -1 \pmod n,$$

gdyż w przeciwnym razie było by

$$b^{\frac{n-1}{2}} \equiv -1 \pmod{p_1 \cdots p_k},$$

a z definicji b wiemy, że

$$b^{\frac{n-1}{2}} \equiv 1 \pmod{p_1 \cdots p_k}.$$

□

9.2 Test Solovaya–Strassena

Niech n będzie nieparzystą liczbą złożoną. Z faktu 9.2 wiemy, że jeśli wybierzemy losowo a i okaże się, że $\mathrm{NWD}(a,n) = 1$, to wtedy z prawdopodobieństwem co najmniej $\frac{1}{2}$, n nie jest pp. przy podstawie a, czyli nie jest pierwsza. Wylosowanie podstawy a takiej, że n jest pp. Eulera przy podstawie a może się zdarzyć z prawdopodobieństwem co najwyżej $\frac{1}{2}$. Jeśli powtórzymy losowanie podstawy k razy i za każdym razem otrzymamy, że n jest pp. Eulera, to prawdopodobieństwo tego zdarzenia wynosi co najwyżej $\frac{1}{2^k}$, co oznacza, że n jest pierwsza z prawdopodobieństwem co najmniej $1 - \frac{1}{2^k}$.

9.3 Silna pseudopierwszość

Pojęcie silnej pseudopierwszości wywodzi się z dwóch własności. Z małego twierdzenia Fermata $a^{p-1} \equiv 1 \pmod p$ oraz z tego, że równanie $x^2 \equiv 1 \pmod p$ ma dwa rozwiązania, mianowicie $x = 1$ i $x = -1$.

Niech n będzie nieparzysta oraz a takie, że $\mathrm{NWD}(a, n) = 1$. Wtedy możemy postępować tak jak na rysunku 2.

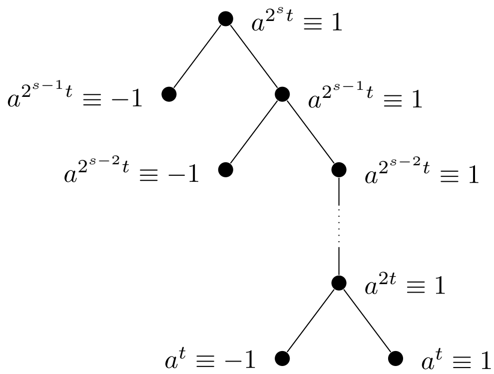
$r \leftarrow n - 1$
jeśli $a^r \not\equiv 1 \pmod n$ **to NIE**
dopóki $2 \mid r \wedge a^r \equiv 1 \pmod n$ **rób** $r \leftarrow r/2$
Teraz jeśli jeszcze $2 \mid r$ *(czyli* $a^r \not\equiv 1$*), to powinno być* $a^r \equiv -1$*, a jeśli już* $2 \not| r$*, to powinno być* $a^r \equiv \pm 1$*.*
jeśli $a^r \not\equiv \pm 1 \pmod n$ **to TAK wpp NIE**

Rysunek 2: Sprawdzanie, czy n jest silnie pp. przy podstawie a

Prowadzi to do następującej definicji.

Definicja 9.3. Niech n będzie liczbą nieparzystą i niech $n - 1 = 2^s t$, gdzie $2 \not| t$. Liczbę n nazywamy silnie pseudopierwszą przy podstawie a, $\mathrm{NWD}(a, n) = 1$, jeżeli

$$a^t \equiv 1 \pmod n \quad \text{lub} \quad a^{2^i t} \equiv -1 \pmod n \text{ dla pewnego } i = 0, 1, \ldots, s - 1.$$



Rysunek 3: Definicja silnej pseudopierwszości

Definicja jest zilustrowana na rysunku 3. Zauważmy, że jeśli $a^{2^i t} \equiv \pm 1 \pmod n$, to dla wszystkich $i < j \leq s$ jest $a^{2^j t} \equiv 1 \pmod n$. Sugeruje to sprawdzanie silnej pp. "od dołu". Odpowiedni algorytm przedstawiony jest na rysunku 4.

Fakt 9.4. *Jeśli n jest liczbą złożoną, to jest ponad $\frac{3}{4}$ podstaw, przy których n nie silnie pp.*

W rzeczywistości jeśli n jest złożona, to tych podstaw jest dużo więcej.

Przykład 9.5. Jeśli n jest liczbą złożoną mniejszą od 1373563, to n nie jest silnie pp. dla jednej z podstaw 2 lub 3. Korzystając z tego sprawdzimy, czy liczby 36493 i 25769 są pierwsze.

$x \leftarrow a^t \bmod n$
jeśli $a^r \equiv \pm 1 \pmod{n}$ **to TAK**
dla $i = 1, \ldots, s-1$ **rób** $\quad \{\ x \not\equiv \pm 1\ \}$
$\quad x \leftarrow x^2 \bmod n \qquad \{\ x \equiv a^{2^i t}\ \}$
$\quad$ **jeśli** $x \equiv 1 \pmod{n}$ **to NIE**
$\quad$ **jeśli** $x \equiv -1 \pmod{n}$ **to TAK**
NIE

Rysunek 4: Sprawdzanie "od dołu", czy n jest silnie pp. przy podstawie a

Mamy $36493 - 1 = 2^2 \cdot 9123$, liczymy $2^{9123} \equiv 11667$, dalej $2^{2 \cdot 9123} \equiv 11667^2 \equiv -1$, zatem 36493 jest silnie pp. przy podstawie 2. Dalej $3^{9123} \equiv 1$, zatem 36493 jest silnie pp. przy podstawie 3, a więc jest pierwsza.

Mamy $25769 - 1 = 2^3 \cdot 3221$, liczymy $2^{3221} \equiv 2665$, dalej $2^{2 \cdot 3221} \equiv 2665^2 \equiv 15750$, dalej $2^{2^2 \cdot 3221} \equiv 15750^2 \equiv 10106$, zatem 25769 nie jest silnie pp. przy podstawie 2, więc jest złożona.

9.4 Zależności między pojęciami pseudopierwszości

Pierwsza oczywista zależność, to: jeśli n jest pp. Eulera przy podstawie a, to jest pp. przy podstawie a. Przypomnijmy, że n jest pp. przy podstawie a, jeśli $a^{n-1} \equiv 1 \pmod{n}$. Druga zależność znaczniej mniej oczywista, której nie będę dowodził jest taka: jeśli n jest silnie pp. przy podstawie a, to n jest pp. Eulera przy podstawie a. Udowodnimy za to inną zależność.

Fakt 9.6. *Niech $n \equiv 3 \pmod{4}$, wtedy n jest silnie pp. przy podstawie a wtedy i tylko wtedy, gdy n jest pp. Eulera przy podstawie a.*

Dowód. Mamy $s = 1$, $t = \frac{n-1}{2}$, $2 \nmid t$ i $n - 1 = 2^s t$.

$\Leftarrow$ Z założenia $a^t \equiv \left(\frac{a}{n}\right) = \pm 1 \pmod{n}$, co z oznacza, że n jest silnie pp. przy podstawie a.

$\Rightarrow$ Z założenia wiemy, że $a^t \equiv \pm 1$, a ponieważ $n \equiv 3 \pmod{4}$, więc $\left(\frac{-1}{n}\right) = -1$, zatem możemy napisać $\left(\frac{\pm 1}{n}\right) = \pm 1$ lub nawet

$$\left(\frac{a^t}{n}\right) \equiv a^t \pmod{n} \tag{9.2}$$

Przekształcamy lewą stronę:

$$\left(\frac{a^t}{n}\right) = \left(\frac{a^{\frac{n-1}{2}}}{n}\right) = \left(\frac{a \cdot a^{\frac{n-3}{2}}}{n}\right) \overset{(8.10)}{=} \left(\frac{a}{n}\right)\left(\frac{a^{\frac{n-3}{4}}}{n}\right)^2 = \left(\frac{a}{n}\right)$$

Wstawiając to do (9.2) i rozpisując t otrzymujemy

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}.$$

□

10 Rzędy

Definicja 10.1. Rząd liczby a modulo n, $a \in \mathbb{Z}_n^*$ ($\mathrm{NWD}(a, n) = 1$) definiujemy wzorem:

$$\mathrm{ord}_n\, a = \min\{m \geq 1 \,|\, a^m \equiv 1 \pmod{n}\}$$

Używając języka teorii grup $\mathrm{ord}_n\, a$ możemy określić inaczej. Biorąc z podstawę grupę multiplikatywną modulo n ($\mathbb{Z}_n^*$) możemy powiedzieć, że rząd a wynosi tyle co moc grupy generowanej przez a:

$$\mathrm{ord}\, a = |\langle a \rangle|$$

Oczywiście podstawą tak naprawdę nie musi być $\mathbb{Z}_n^*$, ale dowolna grupa. Czasami mogą być interesujące grupy multiplikatywne $GF(p^n)$. Z twierdzenia Lagrange'a (o mocy podgrupy) otrzymujemy fakt.

Fakt 10.2. *Dla $a \in G$ mamy*

$$\mathrm{ord}\, a \,\big|\, |G|$$

Wniosek 10.3. *Dla $a \in \mathbb{Z}_n^*$ mamy*

$$\mathrm{ord}_n\, a \,|\, \varphi(n)$$

Ponadto możemy wskazać parę interesujących własności jeśli element grupy podniesiony do pewnej potęgi, daje 1.

Fakt 10.4. *Niech $a \in G$. Niech $a^i = a^j = 1$. Wtedy*

$$a^{\mathrm{NWD}(i,j)} = 1$$

Dowód. Wiemy, że istnieją takie x i y całkowite, że $ix + jy = \mathrm{NWD}(i, j)$, skąd

$$a^{\mathrm{NWD}(i,j)} = a^{ix+jy} = \left(a^i\right)^x \left(a^j\right)^y = 1$$

□

Wniosek 10.5. *Niech $a \in G$, wtedy*

$$a^m = 1 \qquad \Leftrightarrow \qquad \mathrm{ord}\, a \,|\, m$$

Dowód. $\Leftarrow$ Oczywiste.

$\Rightarrow$ Wiemy, że $a^m = 1$ i $a^{\mathrm{ord}\, a} = 1$, więc z faktu 10.4 mamy $a^d = 1$, gdzie $d = \mathrm{NWD}(m, \mathrm{ord}\, a)$. Oczywiście musi być $d \geq \mathrm{ord}\, a$, ale z definicji d mamy $d \,|\, \mathrm{ord}\, a$, więc $d = \mathrm{ord}\, a$. Ponieważ $d \,|\, m$, więc $\mathrm{ord}\, a \,|\, m$.

□

Wstawiając $m = i - j$ we wniosku 10.5 otrzymujemy:

Wniosek 10.6. $a^i = a^j \quad \Leftrightarrow \quad i \equiv j \pmod{\mathrm{ord}\, a}$.

Ponadto mamy też wnioski:

Wniosek 10.7. *Dla $a \in G$ mamy $a^{|G|} = 1$.*

Wniosek 10.8 (Twierdzenia Eulera)**.** $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Przykład 10.9. Jaki jest rząd 3 module 41? Liczymy: $3^1 = 3, 3^2 = 9, 3^3 = 27, 3^4 = 81 = 82 - 1 \equiv -1, 3^5 = -3, 3^6 = -9, 3^7 = -72, 3^8 = 1$, zatem $\operatorname{ord}_{41} 3 = 8$.

Ćwiczenie 10.10. Znaleźć $\operatorname{ord}_{127} 5$.

Rozwiązanie. Metoda wyliczania kolejnych potęg okaże się tu bardzo pracochłonna. Będziemy, więc korzystać z wniosku 10.5.

Po pierwsze $\operatorname{ord} 5 \mid 127 - 1 = 126 = 2 \cdot 3^2 \cdot 7$, więc $\operatorname{ord} 5$ jest postaci $2^\alpha 3^\beta 7^\gamma$, gdzie $\alpha = 0, 1; \beta = 0, 1, 2; \gamma = 0, 1$.

Policzmy np. $5^{3^2 \cdot 7} \equiv -1$, skąd $\operatorname{ord} 5 \nmid 3^2 \cdot 7$. Zatem $\alpha \neq 0$, czyli $\alpha = 1$, gdyż w p.p. $\operatorname{ord} 5 \mid 3^2 \cdot 7$.

Teraz liczymy $5^{2 \cdot 3 \cdot 7} \equiv 1$, skąd $\operatorname{ord} 5 \mid 2 \cdot 3 \cdot 7$, czyli $\beta \leq 1$. No to liczymy $5^{2 \cdot 7} \equiv 19$, skąd $\operatorname{ord} 5 \nmid 2 \cdot 7$, czyli $\beta = 1$.

Teraz liczymy $5^{2 \cdot 3} \equiv 4$, skąd $\operatorname{ord} 5 \nmid 2 \cdot 3$, czyli $\gamma = 1$.

Ostatecznie otrzymujemy $\operatorname{ord}_{127} 5 = 2 \cdot 3 \cdot 7 = 42$. □

Metodę z przykładu możemy sformalizować.

Fakt 10.11. *Jeżeli* $m \geq 1$ *będzie taka, że*

1. $a^m = 1$, *oraz*
2. *dla każdej liczby pierwszej* $p \mid m$ *jest*
$$a^{\frac{m}{p}} \neq 1,$$

to $\operatorname{ord} a = m$.

Dowód. Ponieważ $a^m = 1$, więc $\operatorname{ord} a \mid m$. Jeżeli byłoby $\operatorname{ord} a < m$, to istniała by liczba pierwsza, że $\operatorname{ord} a \mid \frac{m}{p}$, skąd $a^{\frac{m}{p}} = 1$, a to jest niemożliwe. □

Przy okazji możemy udowodnić prosty test na sprawdzanie, czy liczba jest pierwsza.

Twierdzenie 10.12. *Niech* $n > 1$. *Jeśli dla każdego dzielnika pierwszego* q *liczby* $n - 1$ *istnieje* a *takie, że*

$$a^{n-1} \equiv 1 \pmod{n}, \tag{10.1}$$
$$a^{(n-1)/q} \not\equiv 1 \pmod{n}, \tag{10.2}$$

to n *jest pierwsza.*

Dowód. Z faktu 10.11 wynika, że $\operatorname{ord} a = n - 1$. Skąd $\varphi(n) \geq n - 1$, czyli musi być $\varphi(n) = n - 1$, zatem n jest pierwsza. □

Wracając do faktu 10.11, jak z niego zrobić algorytm na wyliczanie rzędu a? Zakładając, że moc grupy potrafimy rozłożyć na czynniki, mamy medotą na liczenie $\operatorname{ord} a$, przedstawioną w poniższym fakcie.

Fakt 10.13. *Niech* $a \in G$ *i* $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. *Niech dla każdego* $i = 1, \ldots, k$, $\beta_i \geq 0$ *będzie najmniejszą liczbą taką, że*

$$a^{p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} \cdot p_i^{\beta_i} \cdot p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k}} = 1,$$

wtedy

$$\operatorname{ord} a = p_1^{\beta_1} \cdots p_k^{\beta_k}$$

Ćwiczenie 10.14. Pokaż, że jeśli $p \mid a^n - 1$, p – pierwsza, to zachodzi jeden z warunków

(i) $p \mid a^d - 1$, dla pewnego $d < n$ i $d \mid n$,

(ii) $p \equiv 1 \pmod{n}$.

Ponadto, jeśli $p > 2$ i n nieparzyste, to warunek (ii) ma postać $p \equiv 1 \pmod{2n}$.

Rozwiązanie. Mamy $a^n \equiv 1 \pmod{p}$ oraz $a^{p-1} \equiv 1 \pmod{p}$. Z faktu 10.4 mamy $a^d \equiv 1 \pmod{p}$, dla $d = \mathrm{NWD}(n, p-1)$. Jeżeli $d < n$, to zachodzi (i). Jeżeli $d = n$, to $n \mid p - 1$, czyli (ii). Ponadto, jeżeli $p > 2$ i n nieparzyste, to $2n \mid p - 1$. □

Ćwiczenie 10.15. Niech $a > 1$ oraz p pierwsza nieparzysta. Pokaż, że dla każdego nieparzystego dzielnika q liczby $a^p - 1$ jest $q \mid a - 1$ albo q jest postaci $2pk + 1$. Ponadto, jeśli $q \nmid a - 1$, wylicz $\left(\frac{a}{q}\right)$.

Rozwiązanie. Mamy $a^p \equiv 1 \pmod{q}$. $\mathrm{ord}_q a = 1, p$. Jeśli $\mathrm{ord}_q a = 1$, to $q \mid a-1$. Niech $\mathrm{ord}_q a = p$. Mamy $a^{q-1} \equiv 1 \pmod{q}$, zatem $p \mid q - 1$. Zatem $q = 2pk + 1$ dla pewnego k. Liczymy

$$\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} = a^{pk} = (a^p)^k \equiv 1^k = 1 \pmod{q}.$$

□

Zauważmy, że z powyższego ćwiczenia mamy następujący wniosek o dzielnikach liczb Mersenne'a.

Wniosek 10.16. *Dzielnik pierwszy q liczby $M_p = 2^p - 1$ jest postaci $2pk + 1$ oraz $q \equiv 1, 7 \pmod{8}$.*

Ćwiczenie 10.17. Niech $a > 1$ oraz p pierwsza. Pokaż, że dla każdego nieparzystego dzielnika q liczby $a^p + 1$ jest $q \mid a + 1$ albo q jest postaci $2pk + 1$. Ponadto, jeśli $q \nmid a + 1$, wylicz $\left(\frac{a}{q}\right)$.

Rozwiązanie. Mamy $a^p \equiv -1 \pmod{q}$, czyli $a^{2p} \equiv 1 \pmod{q}$. $\mathrm{ord}_q a = 1, 2, p, 2p$. Jeśli $\mathrm{ord}_q a \neq 1, p$, bo w p.p. $a^p \equiv 1 \pmod{q}$. Zatem $\mathrm{ord}_q a = 2, 2p$. Jeśli $\mathrm{ord}_q a = 2$, to $q \mid a^2 - 1$, ponadto $q \nmid a - 1$, więc $q \mid a + 1$. Niech $\mathrm{ord}_q a = 2p$. Mamy $a^{q-1} \equiv 1 \pmod{q}$, zatem $2p \mid q - 1$. Zatem $q = 2pk + 1$ dla pewnego k. Liczymy

$$\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} = a^{pk} = (a^p)^k \equiv (-1)^k = (-1)^{\frac{q}{2p}} \pmod{q}.$$

□

Pokazaliśmy postać dzielników liczb Mersenne'a, a teraz pokażemy postać dzielników liczb Fermata.

Fakt 10.18. *Dzielnik pierwszy q liczby Fermata $F_n = 2^{2^n} + 1$ ma postać $q = 2^{n+2}k + 1$ dla $n \geq 2$.*

Dowód. Jeśli $q \mid 2^{2^n}+1$, to

$$2^{2^n} \equiv -1 \pmod q \qquad\qquad 2^{2^{n+1}} \equiv 1 \pmod q$$

Zatem $\operatorname{ord}_q 2 \nmid 2^n$ i $\operatorname{ord}_q 2 \mid 2^{n+1}$, zatem $\operatorname{ord}_q 2 = 2^{n+1}$. Ponadto oczywiście $2^{q-1} \equiv 1 \pmod q$, skąd $2^{n+1} \mid q-1$, więc wiemy, że $q = 2^{n+1}l+1$ dla pewnego l. Ponieważ $q \equiv 1 \pmod 8$, więc $\left(\frac{2}{q}\right) = 1$, skąd

$$2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) = 1 \pmod q$$

Zatem $\operatorname{ord}_q 2 \mid \frac{q-1}{2}$, czyli $2^{n+1} \mid \frac{q-1}{2}$, więc dla pewnego k zachodzi $q = 2^{n+2}k+1$. □

Z ćwiczenia 10.15 możemy wywnioskować następujący fakt.

Fakt 10.19. *Niech $p > 2$ pierwsza. Liczb pierwszych postaci $2pk+1$ jest nieskończenie wiele.*

Dowód. Załóżmy, że liczby $p_1, \ldots, p_n$ są wszystkimi liczbami pierwszymi postaci $2pk+1$. Oznaczmy $a = p_1 \cdots p_n$. Weźmy pod uwagę liczbę $a^p - 1$. Niech $q \mid a^p - 1$, q – pierwsza. Z ćwiczenia 10.15 wiemy, że albo $q \mid a-1$, albo q jest postaci $2pk+1$. To drugie jest niemożliwe, gdyż $p_i \nmid a^p - 1$.

Zatem dla dowolnego dzielnika pierwszego q liczby a^p-1 zachodzi $a \equiv 1 \pmod q$. $a^p - 1$ możemy przedstawić jako iloczyn $(a-1)(1+a+\cdots+a^{p-1})$. Zastanówmy się jakie są dzielniki pierwsze $1+a+\cdots+a^{p-1}$. Jeśli $q \mid 1+a+\cdots+a^{p-1}$, to oczywiście $a \equiv 1 \pmod q$, bo $q \mid a^p-1$ zatem

$$1+a+\cdots+a^{p-1} \equiv \underbrace{1+1+\cdots+1}_{p} = p \pmod q,$$

zatem $q \mid p$, czyli $q = p$. Zatem jedyny dzielnik pierwszy $1+a+\cdots+a^{p-1}$ to p, więc $1+a+\cdots+a^{p-1} = p^s$ dla pewnego s. Ponieważ $1+a+\cdots+a^{p-1} > p$, więc $s \geq 2$.

Zatem $1+a+\cdots+a^{p-1} \equiv 0 \pmod{p^2}$. Z drugiej strony $a = 2pk+1$, gdyż jest iloczynem liczb postaci $2pk+1$, skąd

$$a^i \equiv 1 + 2pki \pmod{p^2},$$

czyli

$$1+a+\cdots+a^{p-1} \equiv p + 2pk\big(1+\cdots+(p-1)\big) = p + 2pk\frac{p(p-1)}{2} \equiv p \pmod{p^2},$$

a to jest sprzeczność.

W dowodzie korzystaliśmy z tego, że istnieje co najmniej jedna liczba pierwsza postaci $2pk+1$. To jednak wynika z tego, że wszystkie dzielniki pierwsze liczby 2^p-1 muszą być właśnie tej postaci.. □

Parę innych faktów na rzędy.

Fakt 10.20. *Niech $a \in G$ oraz $s \geq 1$, wtedy*

$$\operatorname{ord} a^s = \frac{\operatorname{ord} a}{\operatorname{NWD}(\operatorname{ord} a, s)}.$$

Dowód. Oznaczmy $m = \operatorname{ord} a$, $d = \mathrm{NWD}(m, s)$, $m = m'd$ i $s = s'd$. Wtedy $\mathrm{NWD}(m', s') = 1$. Mamy

$$(a^s)^{m'} = a^{ds'm'} = a^{ms'} = (a^m)^{s'} = 1,$$

skąd

$$\operatorname{ord} a^s \,|\, m'. \tag{10.3}$$

Z drugiej strony mamy

$$1 = (a^s)^{\operatorname{ord} a^s} = a^{s \operatorname{ord} a^s},$$

skąd

$$\operatorname{ord} a \,|\, s \operatorname{ord} a^s \Leftrightarrow m \,|\, s \operatorname{ord} a^s \Leftrightarrow m'd \,|\, s'd \operatorname{ord} a^s \Leftrightarrow m' \,|\, s' \operatorname{ord} a^s,$$

ale $\mathrm{NWD}(m', s') = 1$, więc

$$m' \,|\, \operatorname{ord} a^s. \tag{10.4}$$

Z (10.3) i (10.4) ostatecznie mamy $\operatorname{ord} a^s = m'$, a to jest teza. □

Wniosek 10.21. *Niech $a \in G$. Jeżeli $s \,|\, \operatorname{ord} a$, $s \geq 1$, to*

$$\operatorname{ord} a^s = \frac{\operatorname{ord} a}{s}.$$

Fakt 10.22. *Niech G będzie grupą przemienną i $a, b \in G$. Jeżeli* $\mathrm{NWD}(\operatorname{ord} a, \operatorname{ord} b) = 1$, *to* $\operatorname{ord} ab = \operatorname{ord} a \operatorname{ord} b$.

Dowód. Oznaczmy $m = \operatorname{ord} a$ i $n = \operatorname{ord} b$. Zauważmy, że $(ab)^{mn} = 1$, zatem $\operatorname{ord} ab \,|\, mn$. $\operatorname{ord} ab$ będzie postaci $m'n'$, gdzie $m' \,|\, m$ i $n' \,|\, n$. Liczymy:

$$1 = (ab)^{\frac{n}{n'} \operatorname{ord} ab} = (ab)^{m'n} = a^{m'n}(b^n)^{m'} = a^{m'n},$$

skąd otrzymujemy, że $\operatorname{ord} a \,|\, m'n$, czyli $m \,|\, m'n$, a ponieważ $\mathrm{NWD}(m, n) = 1$, więc $m \,|\, m'$, czyli $m' = m$. Analogicznie otrzymujemy, że $n' = n$, zatem ostatecznie $\operatorname{ord} ab = mn$. □

Fakt 10.23. *W grupie przemiennej G dla dowolnych $a, b \in G$ istnieje $c \in G$, że* $\operatorname{ord} c = \mathrm{NWW}(\operatorname{ord} a, \operatorname{ord} b)$.

Dowód. Oznaczmy $m = \operatorname{ord} a$ i $n = \operatorname{ord} b$. Z wniosku 10.21 wynika, że umiemy utworzyć elementy, których rząd jest dowolnym dzielnikiem m lub n. Zatem, aby użyć faktu 10.22, należy znaleźć takie $m' \,|\, m$ i $n' \,|\, n$, że $\mathrm{NWD}(m', n') = 1$ i $m'n' = \mathrm{NWW}(m, n)$.

Niech $p_1, \ldots, p_k$ będą wszystkimi liczbami pierwszymi występującymi w rozkładach m i n, wtedy niech

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$
$$n = p_1^{\beta_1} \cdots p_k^{\beta_k}.$$

Liczby m' i n' budujemy następująco. Dla każdej liczby pierwszej p_i porównujemy α_i z β_i. Jeżeli $\alpha_i > \beta_i$, to do rozkładu m' dodajemy $p_i^{\alpha_i}$, a jeżeli $\alpha_i \leq \beta_i$, to $p_i^{\beta_i}$ dodajemy do rozkładu n'. Wtedy $\mathrm{NWD}(m', n') = 1$, gdyż w rozkładach m' i n' są różne liczby pierwsze oraz

$$m'n' = p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)} = \mathrm{NWW}(m, n).$$

Mając m' i n' o rządanych własnościach bierzemy:

$$c = a^{m/m'} b^{n/n'}.$$

Z wniosku 10.21 wynika, że $\operatorname{ord} a^{m/m'} = m'$ i $\operatorname{ord} b^{n/n'} = n'$, a z faktu 10.22 wynika, że $\operatorname{ord} c = m'n' = \mathrm{NWW}(m, n)$. $\square$

Ćwiczenie 10.24. W dowodzie faktu 10.23 mieliśmy sytuacje, że $\mathrm{NWW}(m, n)$ staraliśmy się rozbić na iloczyn liczb względnie pierwszych tak, aby jedna dzieliła m, a druga n. W tym celu rozłożyliśmy na czynniki m i n. Jak zrobić to bez znajdowania rozkładu m i n na czynniki?

Tzn. podać efektywny algorytm, który dla danych m i n znajdzie liczby m' i n', takie, że

$$\mathrm{NWW}(m, n) = m'n' \qquad m' \mid m \qquad n' \mid n \qquad \mathrm{NWD}(m', n') = 1.$$

11 Pierwiastki pierwotne

Definicja 11.1. Generatorem grupy nazywamy taki element $a \in G$, że $\operatorname{ord} a = |G|$. W grupach multiplikatywnych $\mathbb{Z}_n^*$, taki element nazywamy pierwiastkiem pierwotnym modulo n.

Przykład 11.2. Znajdziemy pierwiastek pierwotny modulo 127. Wiemy, że $\operatorname{ord}_{127} 5 = 42 = 2 \cdot 3 \cdot 7$.

Wystarczy znaleźć taką liczbę a, że $3^2 \mid \operatorname{ord}_{127} a$. Dlaczego? Oznaczmy $\operatorname{ord}_{127} a = m = 3^2 k$. Ponieważ $m \mid 2 \cdot 3^2 \cdot 7$, więc $k \mid 2 \cdot 7$. Skąd $k = \mathrm{NWD}(k, 2 \cdot 7) = \mathrm{NWD}(3^2 k, 2 \cdot 7) = \mathrm{NWD}(m, 2 \cdot 7)$. Teraz na podstawie faktu 10.20 mamy

$$\operatorname{ord}_{127} a^{2 \cdot 7} = \frac{\operatorname{ord}_{127} a}{\mathrm{NWD}(\operatorname{ord}_{127} a, 2 \cdot 7)} = \frac{m}{\mathrm{NWD}(m, 2 \cdot 7)} = \frac{3^2 k}{k} = 3^2.$$

W ten sposób otrzymamy liczbę $b = a^{2 \cdot 7}$, dla której $\operatorname{ord}_{127} b = 3^2$. Z wniosku 10.21 wiemy, że $\operatorname{ord}_{127} 5^3 = 2 \cdot 7$, zatem z faktu 10.22 mamy $\operatorname{ord}_{127} 5^3 b = \operatorname{ord} 5^3 \operatorname{ord} b = 2 \cdot 7 \cdot 3^2 = 126$, czyli $5^3 b$ będzie pierwiastkiem pierwotnym modulo 127.

Zatem trzeba znaleźć a, że $3^2 \mid \operatorname{ord}_{127} a$, czyli innymi słowy takie a, że $a^{2 \cdot 3 \cdot 7} \not\equiv 1$. Dla $a = 2$ mamy $2^7 \equiv 1$, źle. Dla $a = 3$ mamy $3^{2 \cdot 3 \cdot 7} \equiv 107 \not\equiv 1$, dobrze. Zatem pierwiastkiem pierwotnym modulo 127 jest $5^3 \cdot 3^{2 \cdot 7} \equiv 83$.

Fakt 11.3. *Niech $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ oraz niech $a_1, \ldots, a_k$ będą elementami G (niekoniecznie różnymi) takimi, że*

$$a_i^{\frac{|G|}{p_i}} \neq 1 \quad \text{dla } i = 1, \ldots, k, \tag{11.1}$$

wtedy element

$$a_1^{\frac{|G|}{p_1^{\alpha_1}}} \cdots a_k^{\frac{|G|}{p_k^{\alpha_k}}} \tag{11.2}$$

jest generatorem grupy G.

Dowód. Warunek (11.1) mówi, że $\operatorname{ord} a_i \nmid \frac{|G|}{p_i}$, ale ponieważ zachodzi również $\operatorname{ord} a_i \mid |G|$, więc musi być

$$p_i^{\alpha_i} \mid \operatorname{ord} a_i.$$

Z faktu 10.20 wynika, że

$$\operatorname{ord} a_i^{\frac{|G|}{p_i^{\alpha_i}}} = p_i^{\alpha_i}.$$

Z kolei z faktu 10.22 wynika, że rząd iloczynu (11.2) jest iloczynem rzędów, czyli wynosi on $p_1^{\alpha_1} \cdots p_k^{\alpha_k} = |G|$, więc jest generatorem. □

Twierdzenie 11.4. *Grupa multiplikatywna dowolnego ciała skończonego jest cykliczna, tzn. istnieje generator.*

Dowód. Rozważmy ciało $GF(q)$. Załóżmy, że nie istnieje generator $GF(q)^*$. Niech a będzie elementem o maksymalnym rzędzie.

Pokażemy, że dla dowolnego $b \in GF(q)^*$ jest $\operatorname{ord} b \mid m$. Niech $\operatorname{ord} b = n$. Z faktu 10.23 wiemy, że istnieje c, że $\operatorname{ord} c = \mathrm{NWW}(m, n)$. Ponieważ m jest maksymalnym rzędem, więc $\mathrm{NWW}(m, n) \leq m$, skąd $\mathrm{NWW}(m, n) = m$, a zatem $n \mid m$.

Ponieważ dla każdego $b \in GF(q)^*$ jest $\operatorname{ord} b \mid m$, więc wszystkie elementy $GF(q)^*$ spełniają równanie $x^m - 1 = 0$. Ponieważ w $GF(q)^*$ jest $q-1$ różnych elementów, to z lematu 11.5 wynika, że $\deg(x^m - 1) \geq q - 1$, czyli $m \geq q - 1$. Z drugiej strony rząd elementu nie jest większy niż moc grupy, więc $\operatorname{ord} a = q - 1$. □

Lemat 11.5. *Stopień niezerowego wielomianu nad ciałem, który ma n różnych pierwiastków, wynosi co najmniej n.*

Dowód. Indukcja po n.

1. Dla $n = 0$ każdy niezerowy wielomian ma stopień co najmniej 0.

2. Załóżmy, że $P(x) = \sum_{i=0}^{k} a_i x^i$ ma pierwiastki $x_1, \ldots, x_n$. Wtedy

$$\begin{aligned} P(x) = P(x) - P(x_n) &= \sum_{i=1}^{k} a_i (x^i - x_n^i) \\ &= (x - x_n) \sum_{i=1}^{k} a_i (x^{i-1} + x^{i-2} x_n + \cdots + x_n^{i-1}), \end{aligned}$$

zatem istnieje wielomian $Q(x)$ taki, że $P(x) = (x - x_n) Q(x)$. Zauważmy, że $x_1, \ldots, x_{n-1}$ są pierwiastkami $Q(x)$. Otóż dla $i = 1, \ldots, n-1$ wiemy, że $P(x_i) = 0$, zatem $(x_i - x_n) Q(x_i) = 0$, ponieważ $x_i - x_n \neq 0$, więc dzieląc obie strony przez $x_i - x_n$ (korzystamy, że wielomian jest nad ciałem) otrzymujemy, że $Q(x_i) = 0$. Z założenia indukcyjnego $\deg Q(x) \geq n - 1$, skąd $\deg P(x) = \deg(x - x_n) Q(x) \geq n$.

□

Ćwiczenie 11.6. Znaleźć pierwiastek pierwotny modulo liczba pierwsza postaci $2^N + 1$.

Rozwiązanie. Oznaczmy $p = 2^N + 1$. Szukamy g takiego, że $\operatorname{ord}_{2^N+1} g = 2^N$. czyli musi być

$$g^{2^N} \equiv 1 \pmod{p} \quad \text{i} \quad g^{2^{N-1}} \not\equiv 1 \pmod{p},$$

skąd wynika, że musi być

$$g^{2^{N-1}} \equiv -1 \pmod{p} \Leftrightarrow \left(\frac{g}{2^N+1}\right) = -1.$$

Dla $N \geq 2$ z prawa wzajemności dostajemy

$$\left(\frac{g}{2^N+1}\right) = \left(\frac{2^N+1}{g}\right).$$

Zatem wystarczy na przykład znaleźć g, że $2^N \equiv -2 \pmod{g}$ i $g \equiv 3 \pmod{4}$. Na przykład weźmy $g \equiv 3$.

Wtedy $2^N \equiv 1, 2 \pmod{3}$, ale nie może być $2^N \equiv 2 \pmod{3}$, bo wtedy $2^N + 1$ nie była by pierwsza, a zatem $2^N \equiv 1 \pmod{3}$, czyli $2^N + 1 \equiv -1 \pmod{3}$, więc

$$\left(\frac{3}{2^N+1}\right) = -1.$$

□

Co można powiedzieć o N, jeżeli wiemy, że $2^N + 1$ jest pierwsza? Skorzystajmy z wzroru:

$$a^k + b^k = (a+b)(a^{k-1}b^0 - a^{k-1}b + a^{k-2}b^2 - \ldots + a^0 b^{k-1}),$$

który zachodzi dla k nieparzystego. Wynika z niego, że jeśli N da się przedstawić w postaci kt, gdzie k jest nieparzyte, to wtedy $2^N + 1$ ma dzielnik $2^t + 1$, bo

$$2^N + 1 = 2^{kt} + 1 = (2^t)^k + 1^k = (2^t + 1)(\ldots).$$

Zatem, aby $2^N + 1$ pierwsza, to N nie może mieć nieparzystych dzielników, a zatem musi być postaci $N = 2^n$.

Z powyższego ćwiczenia otrzymujemy następujący wniosek.

Wniosek 11.7 (Test Pepina)**.** *Liczba Fermata $F_n = 2^{2^n} + 1$ dla $n > 1$ jest pierwsza wtedy i tylko wtedy, gdy*

$$3^{\frac{F_n - 1}{2}} = 3^{2^{(2^n - 1)}} \equiv -1 \pmod{F_n}. \tag{11.3}$$

Dokładniej z ćwiczenia 11.6 wynika implikacja w jedną stronę. Mianowicie, jeśli F_n jest pierwsza, to musi zachodzić (11.3). Implikacja w drugą stronę wynika z twierdzenia 10.12.

Ćwiczenie 11.8. Pierwiastkiem pierwotnym modulo liczba pierwsza postaci $2p+1$, gdzie p jest pierwsza, jest $\begin{cases} 2 & p \equiv 1 \pmod{4} \\ -2 & p \equiv 3 \pmod{4} \end{cases}$.

Rozwiązanie. Kiedy $\operatorname{ord}_{2p+1} g = 2p$? Wtedy, gdy $g^2 \not\equiv 1 \pmod{2p+1}$ i $g^p \not\equiv 1 \pmod{2p+1}$. Druga kongruencja oznacza, że

$$g^p \equiv -1 \pmod{2p+1} \Leftrightarrow \left(\frac{g}{2p+1}\right) = -1$$

Wystarczy sprawdzić, że ta równość zachodzi w obu przypadkach. □

Ćwiczenie 11.9. Znaleźć wszystkie liczby pierwsze postaci $2^n p + 1$ dla $n \geq 1$ i $p > \frac{3^{2^{n-1}}}{2^n}$, modulo które 3 nie jest pierwiastkiem pierwotnym.

Rozwiązanie. Będziemy badać kiedy 3 jest p.p. modulo $2^n p+1$. Trzeba sprawdzić, że

$$3^{2^n} \not\equiv 1 \pmod{2^n p+1} \quad \text{i} \quad 3^{2^{n-1}p} \not\equiv 1 \pmod{2^n p+1}.$$

Jeśli było by $3^{2^n} \equiv 1$, to $3^{2^{n-1}} \equiv \pm 1$, a to jest niemożliwe, gdyż

$$1 < 3^{2^{n-1}} = \frac{3^{2^{n-1}}}{2^n} \cdot 2^n < 2^n p.$$

Druga kongruencja do sprawdzenia, to $3^{2^{n-1}p} \equiv -1 \pmod{2^n p+1}$, czyli trzeba pokazać, że $\left(\frac{3}{2^n p+1}\right) = -1$. Mamy z prawa wzajemności

$$\left(\frac{3}{2^n p+1}\right) = \left(\frac{2^n p+1}{3}\right) \equiv 2^n p+1 \pmod 3.$$

W przypadku, gdy $p = 3$ otrzymamy, że $n < 3$. Dla $n = 2$ otrzymamy, że 3 wyjątkowo nie jest pierwiastkiem pierwotnym modulo $13 = 2^2 \cdot 3 + 1$, bo $3^3 \equiv 1 \pmod{13}$. Dla $p \neq 3$ mamy, że $2^n p \equiv 1, 2 \pmod 3$, ale nie może być $2^n p \equiv 2 \pmod 3$, bo nie była by wtedy pierwsza, zatem $2^n p \equiv 1 \pmod 3$, czyli $2^n p + 1 \equiv -1 \pmod 3$. □

Zajmijmy się pierwiastkiami pierwotnymi modulo p^α.

Przykład 11.10. Znajdźmy pierwiastek pierwotny modulo 25. Niech tym szukanym pp. będzie g. Zauważmy, że g będzie także pp. modulo 5, gdyż w przeciwnym razie, jeśli g nie byłoby pp. modulo 5, to g nie jest wstanie wygenerować wszystkich wartości modulo 5, a zatem nie jest też w stanie wygenerować wszystkich wartości modulo 25. Wnioskujemy stąd, że $g = \pm 2 + 5t$ dla pewnego t, gdyż ± 2 są wszystkimi pp. modulo 5.

Poszukajmy g wśród liczb postaci $2 + 5t$. Aby g było pierwiastkiem pierwotnym, to wystarczy, aby zachodziło:

$$g^{20/2} \not\equiv 1 \pmod{25} \qquad\qquad g^{20/5} \not\equiv 1 \pmod{25}.$$

Pierwsza nierówność da się wywnioskować z tego, że g jest pp. modulo 5. Otóż, gdyby $g^{10} \equiv 1 \pmod{25}$, to $g^{10} \equiv 1 \pmod 5$, skąd $g^2 \equiv 1 \pmod 5$, a to jest niemożliwe, bo g jest pp. modulo 5. Drugą nierówność trzeba spełnić.

$$(2+5t)^4 \equiv 2^4 + 4 \cdot 2^3 \cdot 5t \equiv 16 + 10t \pmod{25},$$

więc, aby $g^4 \not\equiv 1 \pmod{25}$, wystarczy, że weźmiemy t takie, że $16 + 10t \not\equiv 1 \pmod{25}$, czyli np. $t = 0$. Zatem pp. modulo 25 jest 2.

Powstaje pytanie, czy zawsze wystarczy brać $t = 0$. Niestety nie. Nawet jeśli założym, że dla dla danego p znajdziemy najmniejszy możliwy generator g modulo p, to może się zdarzyć tak, że $g^{p-1} \equiv 1 \pmod{p^2}$. Najmniejszym takim p jest $p = 40487$. Wtedy najmniejszy generator, to $g = 5$ oraz mamy

$$(g + pt)^{p-1} \equiv 1 + 24292pt \pmod{p^2}.$$

Fakt 11.11. *Jeżeli g jest p.p. modulo $p > 2$, to istnieje t, że $h = g + tp$ jest p.p. modulo p^2. Ponadto to h jest także p.p. modulo p^α dla dowolnego $\alpha \geq 1$.*

Lemat 11.12. *Jeżeli $a \equiv b \pmod{p^{\alpha-1}}$, to $a^p \equiv b^p \pmod{p^\alpha}$, dla $\alpha \geq 2$.*

Dowód. Z założenia istnieje t, że $a = b + tp^{\alpha-1}$. Mamy

$$a^p = \left(b + tp^{\alpha-1}\right)^p = b^p + \sum_{i=1}^{p} \binom{p}{i} b^{p-i} t^i p^{i(\alpha-1)}.$$

Wystarczy pokazać, że

$$p^\alpha \mid \binom{p}{i} b^{p-i} t^i p^{i(\alpha-1)} \quad \text{dla } i = 1, \ldots, p.$$

Rozpatrzmy dwa przypadki.

1. $1 \leq i < p$. Wtedy $p \mid \binom{p}{i}$, zatem $p^{1+i(\alpha-1)} \mid \binom{p}{i} b^{p-i} t^i p^{i(\alpha-1)}$, ale $1 + i(\alpha - 1) \geq \alpha$.
2. $i = p$. Wtedy $i(\alpha - 1) \geq 2(\alpha - 1) \geq \alpha$.

□

Lemat 11.13.

$$(1 + tp)^{p^{\alpha-2}} \equiv 1 + tp^{\alpha-1} \pmod{p^\alpha} \quad \textit{dla } \alpha \geq 2, p > 2.$$

Dowód. Indukcja po α. Dla $\alpha = 2$ mamy oczywistą równość. Dla $\alpha = 3$ mamy

$$(1 + tp)^p \equiv 1 + ptp + p\frac{p-1}{2}t^2p^2 \equiv 1 + tp^2 \pmod{p^\alpha}.$$

Niech $\alpha \geq 4$. Z założenia indukcyjnego mamy

$$(1 + tp)^{p^{\alpha-3}} \equiv 1 + tp^{\alpha-2} \pmod{p^{\alpha-1}},$$

zatem z lematu 11.12 mamy

$$(1 + tp)^{p^{\alpha-2}} \equiv \left(1 + tp^{\alpha-2}\right)^p \pmod{p^\alpha}.$$

Teraz liczymy

$$\left(1 + tp^{\alpha-2}\right)^p \equiv 1 + ptp^{\alpha-2} + p^{2(\alpha-2)}C \pmod{p^\alpha}.$$

Wystarczy sprawdzić, że $2(\alpha - 2) \geq \alpha$ dla $\alpha \geq 4$, a otrzymamy żądaną równość.
□

Teraz możemy przejść do dowodu faktu 11.11.

Dowód faktu 11.11. Będziemy wyznaczać t. Zauważmy, że jeśli $h^n \equiv 1 \pmod{p^\alpha}$, to wtedy $h^n \equiv 1 \pmod{p}$, czyli $g^n \equiv 1 \pmod{p}$, a to oznacza, że $p-1 \mid n$. Wynika zatem, że $p-1 \mid \operatorname{ord}_{p^\alpha} h$, więc aby pokazać, że h jest p.p. modulo p^α wystarczy stwierdzić, że $p^{\alpha-1} \mid \operatorname{ord}_{p^\alpha} h$, czyli, że $p^{\alpha-2} \nmid \operatorname{ord}_{p^\alpha} h$, a co za tym idzie wystarczy stwierdzić, że

$$h^{(p-1)p^{\alpha-2}} \not\equiv 1 \pmod{p^\alpha}. \tag{11.4}$$

Znajdźmy wpierw takie t, że $h = g + tp$ będzie spełniało (11.4) dla $\alpha = 2$. Z tego, że $g^{p-1} \equiv 1 \pmod{p}$ wiemy, że istnieje s takie, że $g^{p-1} = 1 + sp$. Liczymy

$$\begin{aligned} h^{(p-1)p^{\alpha-2}} = (g+tp)^{(p-1)} \equiv g^{p-1} + (p-1)g^{p-2}tp \equiv 1 + sp + (p-1)g^{p-2}tp = \\ 1 + \big(s + (p-1)g^{p-2}t\big)\, p \pmod{p^2}. \end{aligned}$$

Zatem, aby zachodziło (11.4), musi być

$$s + (p-1)g^{p-2}t \not\equiv 0 \pmod{p}.$$

Przekształcamy

$$\begin{aligned} s - g^{p-2}t &\not\equiv 0 \pmod{p} \\ g^{p-2}t &\not\equiv s \pmod{p} \\ t &\not\equiv gs \pmod{p} \end{aligned} \tag{11.5}$$

Wystarczy teraz znaleźć takie t, aby było spełnione (11.5). Kongruencja (11.5) ma aż $p-1$ rozwiązań modulo p. Zatem pokazaliśmy, że istnieje takie t, że $h = 1 + tp$ jest p.p. modulo p^2. Mamy też takie $u \not\equiv 0 \pmod{p}$, że

$$h^{p-1} \equiv 1 + up \pmod{p^2}. \tag{11.6}$$

Z lematu 11.13 otrzymujemy

$$h^{(p-1)p^{\alpha-2}} \overset{(11.6)}{\equiv} (1+up)^{p^{\alpha-2}} \equiv 1 + up^{\alpha-1} \not\equiv 1 \pmod{p^\alpha},$$

co oznacza, że zachodzi (11.4), czyli, że h jest pierwiastkiem pierwotnym modulo p^α. □

Wniosek 11.14. *Jeżeli g jest p.p. modulo p^α, to nieparzysta z liczb $g, g + p^\alpha$ jest p.p. modulo $2p^\alpha$.*

Dowód. Zauważmy, że jeżeli $a^n \equiv 1 \pmod{2p^\alpha}$, to $a^n \equiv 1 \pmod{p^\alpha}$. Innymi słowy jeżeli $a^n \not\equiv 1 \pmod{p^\alpha}$, to $a^n \not\equiv 1 \pmod{2p^\alpha}$, a ponieważ $|\mathbb{Z}^*_{p^\alpha}| = |\mathbb{Z}^*_{2p^\alpha}|$, więc wystarczy znaleźć takie a, że $a \equiv g \pmod{p^\alpha}$ i $a \in \mathbb{Z}^*_{2p^\alpha}$. Takie a, to nieparzysta z liczb $g, g + p^\alpha$. □

12 Indeksy

Definicja 12.1. W grupie cyklicznej G przy zadanym generatorze g indeksem elementu $a \in G$ nazywamy taki wykładnik $e \in Z_{|G|}$, że $g^e = a$ i oznaczamy go przez $\operatorname{ind}_g a$ lub po prostu $\operatorname{ind} a$, gdy wiemy o jaki generator chodzi.

Fakt 12.2.

$$\operatorname{ind} ab = \operatorname{ind} a + \operatorname{ind} b$$

Fakt 12.3. *Niech G będzie grupą cykliczną o mocy n i niech $a \in G$. Zachodzi:*

$$\operatorname{ord} a = \frac{n}{\mathrm{NWD}(\operatorname{ind} a, n)}$$

Dowód. Niech g będzie generatorem G i niech $e = \operatorname{ind} a$, czyli $a = g^e$. Szukamy najmniejszego $m \geq 1$ takiego, że $a^{em} = 1$, czyli takiego, że $em \equiv 0 \pmod{n} \Leftrightarrow n \,|\, em$.

Niech $d = \mathrm{NWD}(e, n)$. Oznaczając $e = de'$ i $n = dn'$ otrzymujemy $n' \,|\, e'm$. Ponieważ $\mathrm{NWD}(e', n') = 1$, więc musi być $n' \,|\, m$. Najmniejsze takie m, że $n' \,|\, m$ to po prostu n'. Zatem:

$$\operatorname{ord} a = m = n' = \frac{n}{d} = \frac{n}{\mathrm{NWD}(e, n)}.$$

□

Fakt 12.4. *Rozpatrzmy następujące równanie w grupie cyklicznej G o mocy n:*

$$x^e = a, \tag{12.1}$$

gdzie $a \in G$. Oznaczmy $d = \mathrm{NWD}(e, n)$.

(i) (12.1) *ma rozwiązanie wtedy i tylko wtedy, gdy $d \,|\, \operatorname{ind} a$. Ponadto jeśli* (12.1) *ma rozwiązanie, to ma ich dokładnie d.*

(ii) Ilość reszt stopnia e w grupie G wynosi $\frac{n}{d}$.

Dowód. (i) Równanie (12.1) równoznaczne jest kongruencji:

$$e \operatorname{ind} x \equiv \operatorname{ind} a \pmod{n}.$$

Niewiadomą jest teraz $\operatorname{ind} x \in \mathbb{Z}_n$. Na podstawie ćwiczenia 7.5 wiemy, że ta kongruencja ma rozwiązanie wtedy i tylko wtedy, gdy $d = \mathrm{NWD}(e, n) \,|\, \operatorname{ind} a$. Ponadto jeśli rozwiązanie istnieje to jest ich d.

(ii) Widzimy, że a jest resztą stopnia e wtw., gdy $d \,|\, \operatorname{ind} a$. Zatem ilość reszt stopnia e jest równa ilości liczb z $\mathbb{Z}_n$ podzielnych przez d, a takich liczb jest $\frac{n}{d}$, gdyż $d \,|\, n$.

□

Wniosek 12.5. *Niech $a \in G$, G – grupa cykliczna, wtedy a jest resztą stopnia e wtedy i tylko wtedy, gdy*

$$a^{\frac{n}{d}} = 1,$$

gdzie $n = |G|$ i $d = \mathrm{NWD}(n, e)$.

Dowód. Z faktu 12.4 wynika, że a jest resztą stopnia $e \Leftrightarrow d \,|\, \operatorname{ind} a \Leftrightarrow n \,|\, \frac{n}{d} \operatorname{ind} a \Leftrightarrow \frac{n}{d} \operatorname{ind} a \equiv 0 \pmod{n}$, a to jest równoznaczne z tym, że

$$a^{\frac{n}{d}} = 1.$$

□

Wniosek 12.6 (Uogólnione kryterium Eulera)**.** *W grupie cyklicznej* $\mathbb{Z}_n^*$*,* $a \in \mathbb{Z}_n^*$ *jest resztą stopnia* e *wtedy i tylko wtedy, gdy*

$$a^{\frac{\varphi(n)}{\mathrm{NWD}(\varphi(n),e)}} \equiv 1 \pmod n$$

Przykład 12.7. Rozwiązujemy

$$x^8 \equiv 23 \pmod{41}.$$

Za generator modulo 41 bierzemy 6. $\mathrm{NWD}(8, 40) = 8$, $\mathrm{ind}_6 23 = 36$, $8 \not| 36$, zatem nie ma rozwiązań. Reszt rzędu 8 modulo 41 jest $\frac{40}{8} = 5$.

Rozwiązujemy teraz

$$x^{12} \equiv 37 \pmod{41}.$$

$\mathrm{NWD}(12, 40) = 4$, $\mathrm{ind}_6 37 = 32$, $4 \mid 32$, zatem są 4 rozwiązania. Należy rozwiązać kongruencję

$$12 \,\mathrm{ind}_6 x \equiv 32 \pmod{40}.$$

Sprowadzamy ją do $3 \,\mathrm{ind}\, x \equiv 8 \pmod{10}$, skąd $\mathrm{ind}\, x \equiv 6 \pmod{10}$, czyli $\mathrm{ind}\, x \equiv 6, 16, 26, 36 \pmod{40}$. Wyliczając odpowiednie potęgowania otrzymujemy rozwiązania $x \equiv 39, 12, 2, 23 \pmod{41}$. Reszt rzędu 12 modulo 41 jest $\frac{40}{4} = 10$.

13 Liczenie pierwiastków

W tej sekcji zajmiemy się rozwiązywaniem równania

$$x^e = a \tag{13.1}$$

w grupie cyklicznej G o mocy n. Oznaczmy $d = \mathrm{NWD}(e, n)$.

Z faktu 12.4 wiemy, że (13.1) ma rozwiązanie wtw., gdy $d \mid n$. Załóżmy więc, że $d \mid n$. Wtedy wiemy, ze (13.1) ma d rozwiązań.

13.1 Pierwiastki z jedności ($a = 1$)

W przypadku, gdy $x^e = 1$, to trzeba znaleźć wszystkie takie x, że $\mathrm{ord}\, x \mid e$. Tak naprawdę wystarczy znaleźć takie g, że $\mathrm{ord}\, g = e$, bo wtedy g^i są różnymi elementami dla $i = 0, \dots, e-1$ i $\mathrm{ord}\, g^i \mid e$. W ten sposób możemy znaleźć wszystkie pierwiastki z jedności.

13.2 Przypadek $d = 1$

W tym przypadku wiemy, że istnieje takie α, że $\alpha e \equiv 1 \pmod n$. Wtedy jedynym rozwiązaniem jest

$$x = a^\alpha,$$

gdyż

$$x^e = a^{\alpha e} = a^1 = a.$$

13.3 Przypadek $d = e = p$, gdzie p jest pierwsza

Niech $n = p^s t$, gdzie $\mathrm{NWD}(p, t) = 1$ i $s \geq 1$. Załóżmy, że równanie (13.1) ma rozwiązanie, więc z wniosku 12.5 wynika, że jest:

$$a^{p^{s-1}t} = 1. \tag{13.2}$$

Ponadto wiemy, że jest p rozwiązań. Wystarczy, ze znajdziemy jedno, gdyż pozostałe można otrzymać przez pomnożenie przez pierwiastki stopnia p z jedności.

Zobaczmy co by było, gdyby $a^t = 1$. Wtedy dla dowolnego α byłoby $a^{1+\alpha t} = a$. Zatem wystarczyło by dobrać tak α, aby $p \mid 1+\alpha t$. To jest oczywiście możliwe, gdyż $\mathrm{NWD}(p, t) = 1$. Dla α, β takich, że $\beta p = 1 + \alpha t$ rozwiązaniem jest a^β. Niestety nie musi zachodzić wcale $a^t = 1$. Zauważmy jednak, że równanie (13.1) możemy zaburzyć mnożąc obie strony przez b^p:

$$(xb)^p = ab^p,$$

więc wystarczyło by rozwiązać równanie $(x')^p = a'$, gdzie $a' = ab^p$ i następnie wziąć $x = x'b^{-1}$. Zatem należy tak dobrać b, aby $(a')^t = 1$.

Będziemy konstruować tak ciąg $a_1, \ldots, a_s$, że dla $i = 1, \ldots, s$ zachodzi:

$$a_i^{p^{s-i}t} = 1 \tag{13.3}$$

Z równania (13.2) widzimy, że $a_1 = a$. Ponadto chcemy, żeby a_i było postaci ab^p. Zatem chcemy skonstruować także ciąg $b_1, \ldots, b_s$ taki, że

$$a_i = ab_i^p. \tag{13.4}$$

Dla $i = 1$ możemy przyjąć $b_i = 1$. Teraz spróbujmy skonstruować b_i, a co za tym idzie a_i dla $i \geq 2$, przy założeniu, że mamy już a_{i-1} i b_{i-1} spełniające własności (13.3) i (13.4). Wiemy, że

$$(ab_{i-1}^p)^{p^{s-(i-1)}t} = 1,$$

skąd

$$\left((ab_{i-1}^p)^{p^{s-i}t}\right)^p = 1,$$

a zatem liczba

$$\varepsilon = (ab_{i-1}^p)^{p^{s-i}t}$$

jest pierwiastkiem z jedności stopnia p. Gdyby teraz udało nam się przedstawić ε w postaci:

$$\varepsilon = c^{p^{s-i+1}t},$$

to wystarczyło by przyjąć $b_i = b_{i-1}c^{-1}$, gdyż wtedy

$$(ab_i^p)^{p^{s-i}t} = (ab_{i-1}^p c^{-p})^{p^{s-i}t} = (ab_{i-1}^p)^{p^{s-i}t} c^{-p^{s-i+1}t} = (ab_{i-1}^p)^{p^{s-i}t} \varepsilon^{-1} = 1$$

Jak znaleźć takie c? Wystarczy znaleźć takie h, aby $p^s \mid \operatorname{ord} h$, bo wtedy

$$\operatorname{ord} h^{p^{s-1}t} = \frac{\operatorname{ord} h}{\mathrm{NWD}(p^{s-1}t, \operatorname{ord} h)} = p,$$

czyli $h^{jp^{s-1}t}$ dla $j = 0, \ldots, p-1$ są wszystkimi pierwiastkami z jedności. Zatem

$$\varepsilon = h^{jp^{s-1}t} \quad \text{dla pewnego } j = 0, \ldots, s-1.$$

Wystarczy znaleźć to j i możemy wtedy przyjąć

$$c = h^{jp^{i-2}}.$$

W celu znalezienia takiego h, aby $p^s \mid \operatorname{ord} h$, wystarczy wybrać je tak, aby

$$h^{p^{s-1}t} \neq 1.$$

Podsumowując powyższe rozumowanie otrzymujemy algorytm na szukanie pierwiastka stopnia p przedstawiony na rysunku 5.

znajdź h takie, że $h^{p^{s-1}t} \neq 1$
$\omega \leftarrow h^{p^{s-1}t}$
$b_1 \leftarrow 1$
dla $i = 2, \ldots, s$ **rób**
    $\varepsilon \leftarrow (ab_{i-1}{}^p)^{p^{s-i}t}$
    znajdź $j = 0, \ldots, p-1$ takie, że $\varepsilon = \omega^j$
    $b_i \leftarrow b_{i-1} h^{-jp^{i-2}}$
$a_s \leftarrow ab_s^p$
znajdź β takie, że $\beta p \equiv 1 \pmod t$
$x_0 \leftarrow a_s^\beta b_s^{-1}$
i–te rozwiązanie, dla $i = 0, \ldots, p-1$, to $x_0 \omega^i$

Rysunek 5: Algorytm Tonneliego na wyliczanie $\sqrt[p]{a}$

Przykład 13.1.

$$x^5 \equiv 207 \pmod{625 = 5^4}$$

mamy $a = 207$, $e = 5$, $\varphi(n) = 500 = 5^3 \cdot 4$, $s = 3$, $t = 4$
bierzemy $h = 2$, bo $2^{100} \equiv 376 \pmod{625}$
$\omega \leftarrow 376$
$b_1 \leftarrow 1$
$i = 2:$
    $\varepsilon \leftarrow (207 \cdot 1^5)^{20} \equiv 251$
    szukamy j takie, że $376^j \equiv 251$:
        $376^2 \equiv 126, 376^3 \equiv 501, 376^4 \equiv 251$, zatem $j = 4$
    $b_2 \leftarrow 1 \cdot 2^{-4} \equiv 586$
$i = 3:$
    $\varepsilon \leftarrow (207 \cdot 586^5)^4 \equiv 1$
    szukamy j takie, że $376^j \equiv 1$, czyli $j = 0$
    $b_3 \leftarrow 586 \cdot 2^{-0 \cdot 5} \equiv 586$
$a_5 \leftarrow 207 \cdot 586^5 \equiv 182$
rozwiązujemy $5\beta \equiv 1 \pmod 4$, czyli $\beta = 1$
$x_0 \leftarrow 182^1 \cdot 586^{-1} \equiv 412$
$x_1 = 412 \cdot 376 \equiv 537$, $x_2 = 537 \cdot 376 \equiv 37$, $x_3 = 37 \cdot 376 \equiv 162$, $x_4 = 162 \cdot 376 \equiv 287$

14 Funkcje multiplikatywne

Definicja 14.1. Funkcję f z liczb całkowitych dodatnich nazywamy *multiplikatywną*, jeśli dla $\mathrm{NWD}(m,n)=1$ zachodzi

$$f(mn) = f(m)f(n). \tag{14.1}$$

Parę prostych faktów.

Fakt 14.2. $f(1)=1$ *o ile istnieje* a *takie, że* $f(a)\neq 0$.

Dowód. Jeżeli $f(a)\neq 0$, to $f(a\cdot 1)=f(a)f(1)$, skąd $f(1)=1$. □

Fakt 14.3. *Iloczyn funkcji multiplikatywnych jest funkcją multiplikatywną.*

Bardziej skomplikowaną konstrukcja jest za pomocą sumy. Mamy następujące twierdzenie.

Twierdzenie 14.4. *Załóżmy, że zachodzi tożsamość dwóch funkcji* f *i* g*:*

$$g(n) = \sum_{d\,|\,n} f(d), \tag{14.2}$$

wtedy f *jest multiplikatywna wtedy i tylko wtedy, gdy* g *jest multiplikatywna.*

Dowód.

$\Rightarrow$. Zakładamy, że f jest multiplikatywna. Dla $\mathrm{NWD}(m,n)=1$ mamy:

$$\begin{aligned} g(mn) = {} & \sum_{d\,|\,mn} f(d) = \sum_{\substack{d_1\,|\,m\\ d_2\,|\,n}} f(d_1d_2) = \sum_{\substack{d_1\,|\,m\\ d_2\,|\,n}} f(d_1)f(d_2)\\ = {} & \sum_{d_1\,|\,m} f(d_1) \sum_{d_2\,|\,n} f(d_2) = g(m)g(n). \end{aligned}$$

$\Leftarrow$. Zakładamy, że g jest multiplikatywna. Pokażemy, że $f(mn)=f(m)f(n)$ dla $\mathrm{NWD}(m,n)=1$ indukcją po iloczynie mn.

1. $mn=1$, wtedy $m=n=1$ i $f(1\cdot 1)=f(1)*f(1)$, bo albo $f(1)=0$, albo $f(1)=1$.
2. $mn>1$. Zakładamy, że dla $d_1d_2<mn$ zachodzi $f(d_1d_2)=f(d_1)f(d_2)$. Z jednej strony mamy

$$g(mn) = \sum_{d\,|\,mn} f(d) = \sum_{\substack{d_1\,|\,m\\ d_2\,|\,n}} f(d_1d_2),$$

a z drugiej

$$g(m)g(n) = \sum_{d_1\,|\,m} f(d_1) \sum_{d_2\,|\,n} f(d_2) = \sum_{\substack{d_1\,|\,m\\ d_2\,|\,n}} f(d_1)f(d_2).$$

Ponieważ $g(mn) = g(m)g(n)$ mamy więc równość

$$\sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2). \tag{14.3}$$

Z założenia indukcyjnego wiemy, że $f(d_1 d_2) = f(d_1)f(d_2)$ dla $d_1 d_2 < mn$ zatem, aby równość (14.3) była spełniona musi być także $f(d_1 d_2) = f(d_1)f(d_2)$ dla $d_1 d_2 = mn$, czyli dla $d_1 = m$ i $d_2 = n$, co kończy dowód indukcyjny.

□

Wniosek 14.5. *Następujące funkcje są multiplikatywne:*

- *liczba dzielników n*
$$\tau(n) = \sum_{d \mid n} 1,$$
- *suma dzielników n*
$$\sigma(n) = \sum_{d \mid n} d.$$

14.1 Funkcja Möbiusa

Funkcję Möbiusa oznaczamy przez μ. Jest kilka równoważnych definicji.

Twierdzenie 14.6. *Następujące definicje są równoważne:*

(i) Wzór przy znanym rozkładzie.

$$\mu(n) = \begin{cases} 0 & \text{jeżeli } p^2 \mid n \\ (-1)^k & \text{jeżeli } n = p_1 \cdots p_k \end{cases} \tag{14.4}$$

(ii) Równanie rekurencyjne.

$$\sum_{d \mid n} \mu(d) = [n = 1] = \begin{cases} 0 & \text{dla } n > 1 \\ 1 & \text{dla } n = 1 \end{cases} \tag{14.5}$$

(iii) Definicja multiplikatywna.

$$\mu(p^\alpha) = \begin{cases} 1 & \text{dla } \alpha = 0 \\ -1 & \text{dla } \alpha = 1 \\ 0 & \text{dla } \alpha \geq 2 \end{cases} \tag{14.6}$$

$$\mu(mn) = \mu(m)\mu(n) \quad \text{dla } \mathrm{NWD}(m, n) = 1 \tag{14.7}$$

Dowód. W (iii) funkcja μ jest zdefiniowana jednoznacznie. Równość (14.7) oznacza, że funkcja μ jest multiplikatywna, w związku z tym, aby określić wartości funkcji dla dowolnej liczby naturalnej, wystarczy podać jej wartość dla p^α, gdzie p jest liczbą pierwszą. Równość (14.7) to określa.

Pokażemy, że każda z definicji (i) i (ii) spełniają własności definicji (iii), czyli są określone w ten sam sposób dla dowolnej liczby naturalnej.

- Załóżmy, że funkcja μ dana jest równością (i). Wtedy (14.6) jest w oczywisty sposób spełnione. Pozostaje pokazać multiplikatywność.

  Jeżeli $p^2 \mid m$ lub $p^2 \mid n$, to $p^2 \mid mn$. Zatem wtedy $\mu(mn) = \mu(m)\mu(n) = 0$.

  Załóżmy, że m i n są iloczynem różnych liczb pierwszych: $m = p_1 \cdot \ldots \cdot p_k$ i $n = q_1 \cdot \ldots \cdot q_l$. Wtedy $\mu(mn) = (-1)^{k+l}$, a $\mu(m) = (-1)^k$ i $\mu(n) = (-1)^l$, zatem $\mu(mn) = \mu(m)\mu(n)$.

- Załóżmy, że μ spełnia własność (ii). Wtedy multiplikatywność wynika z twierdzenia 14.4. Pozostaje pokazać równość (14.6).

  - $\alpha = 0$, wtedy $\mu(p^0) = 1$.
  - $\alpha = 1$, z $\mu(p^0) + \mu(p^1) = 0$ mamy $\mu(p^1) = -1$.
  - $\alpha \geq 2$, wtedy korzystamy z dwóch równości:

  $$\begin{aligned} 0 &= \mu(p^0) + \ldots + \mu(p^{\alpha-1}), \\ 0 &= \mu(p^0) + \ldots + \mu(p^{\alpha-1}) + \mu(p^\alpha), \end{aligned}$$

  skąd $\mu(p^\alpha) = 0$.

□

14.2 Wzór na odwracanie

Załóżmy, że

$$g(n) = \sum_{d \mid n} f(d), \tag{14.8}$$

gdzie f i g są dowolnymi funkcjami określonymi dla liczb naturalnych. Chcemy teraz przedstawić f za pomocą g, tzn. chcemy taką równość, że z jednej strony występuje $f(n)$, a z drugiej strony odwołujemy się tylko do $g(\cdot)$. Równość (14.8) możemy przepisać jako:

$$f(n) = g(n) - \sum_{\substack{d \mid n \\ d<n}} f(d)$$

Jest to rekurencja na $f(n)$ z odwołaniem do $g(\cdot)$ i $f(x)$ dla $x < n$. Rozwijając tą rekurencję jesteśmy w stanie zlikwidować wszystkie odwołania $f(\cdot)$. Zamiast tego pojawią się odwołania do $g(x)$, gdzie x będzie dzielnikiem n, skąd wnioskujemy, że formuła będzie miała postać:

$$f(n) = \sum_{d \mid n} c(d, n) g(d), \tag{14.9}$$

gdzie $c(d, n)$ jest pewną funkcją zależną od d i n oznaczającą krotność $g(d)$. Wstawiając tą równość do (14.8) otrzymamy:

$$g(n) = \sum_{d \mid n} \sum_{d' \mid d} c(d', d) g(d') = \sum_{\substack{d \mid n \\ d' \mid d}} c(d', d) g(d').$$

Sumujemy po dwóch zmiennych d i d' będącymi dzielnikami n, zatem będą one postaci $\frac{n}{e}$ i $\frac{n}{e'}$, gdzie e i e' są również dzielnikami n. Wtedy własność $d' \mid d$ przeniesie się jako $e \mid e'$:

$$g(n) = \sum_{\substack{e' \mid n \\ e \mid e'}} c\Big(\frac{n}{e'}, \frac{n}{e}\Big) g\Big(\frac{n}{e'}\Big) = \sum_{e' \mid n} \Bigg(\sum_{e \mid e'} c\Big(\frac{n}{e'}, \frac{n}{e}\Big)\Bigg) g\Big(\frac{n}{e'}\Big)$$

Przyrównując współczynniki przy $g(n/e')$ po obu stronach otrzymamy równość:

$$\sum_{e \mid e'} c\Big(\frac{n}{e'}, \frac{n}{e}\Big) = [e' = 1]. \tag{14.10}$$

Równość (14.10) przypomina własność (ii) funkcji Möbiusa. Istotnie, wystarczy przyjąć

$$c\Big(\frac{n}{e'}, \frac{n}{e}\Big) = \mu(e'). \tag{14.11}$$

Wstawiając to po przekształceniu do (14.9) otrzymamy

$$f(n) \overset{(14.9)}{=} \sum_{d \mid n} c(d, n) g(d) = \sum_{d \mid n} c\Big(\frac{n}{d}, n\Big) g\Big(\frac{n}{d}\Big) \overset{(14.11)}{=} \sum_{d \mid n} \mu(d) g\Big(\frac{n}{d}\Big),$$

zatem otrzymujemy równość

$$f(n) = \sum_{d \mid n} \mu(d) g\Big(\frac{n}{d}\Big). \tag{14.12}$$

Twierdzenie 14.7. *Równości* (14.8) *i* (14.12) *są równoważne.*

14.3 Funkcja φ

Aby zdefiniować funkcję dla liczb naturalnych, wystarczy pokazać, że jest ona multiplikatywna i podać jej wartości dla p^α. W ten sposób zdefiniowaliśmy funkcję Möbiusa μ w definicji (iii). Podobnie możemy postąpić z funkcją $\varphi(n)$ – liczbą liczb całkowitych dodatnich nie większych od n względnie pierwszych z n.

Niech m i n będą względnie pierwsze. Zastanówmy się kiedy $1 \le x \le mn$ jest względnie pierwsze z mn. Otóż $\mathrm{NWD}(x, mn) = 1 \Leftrightarrow \mathrm{NWD}(x, m) = 1$ i $\mathrm{NWD}(x, n) = 1$, czyli x musi spełniać układ kongruencji:

$$\begin{cases} x \equiv a \pmod{m}, \\ x \equiv b \pmod{n}, \end{cases} \tag{14.13}$$

gdzie a jest względnie pierwsze z m, a b jest względnie pierwsze z n. Różnych liczb a modulo m o tej własności jest $\varphi(m)$, a różnych liczb b module n jest $\varphi(n)$. Dla każdej pary liczb a i b z chińskiego twierdzenia o resztach wiemy, że istnieje dokładnie jedno x z dokładnością modulo mn spełniające (14.13), skąd wynika, że całkowita liczba szukanych wartości x wynosi $\varphi(m)\varphi(n)$. Zatem funkcja φ jest multiplikatywna.

Zatem wystarczy podać wartość $\varphi(p^\alpha)$, ale to wynosi dokładnie $p^\alpha - p^{\alpha-1}$. Niech $n = p^\alpha$. Spróbujmy wyrazić $\varphi(n)$ tak, aby zależało tylko od n, ale w ten sposób, żeby wzór reprezentował funkcję multiplikatywną. Mamy:

$$\varphi(n) = n\left(1 - \frac{1}{p}\right). \tag{14.14}$$

Wzór (14.14) zawiera jeszcze liczbę pierwszą p. Zauważmy, że 1, jak i p są dzielnikami n. Pozostałymi dzielnikami n są $p^2, \ldots, p^\alpha$, ale one nie występują we wzorze. Sugeruje to użycie definicji (iii) funkcji μ:

$$\varphi(n) = n\sum_{d\,|\,n} \frac{1}{d}\mu(d). \tag{14.15}$$

Multiplikatywność tego wzoru wynika z multiplikatywności funkcji μ i $d \mapsto \frac{1}{d}$ oraz z twierdzenia 14.4. Zatem (14.15) reprezentuje wzór na $\varphi(n)$, nie tylko dla $n = p^\alpha$, ale dla dowolnego naturalnego n. Przepiszmy go do postaci

$$\varphi(n) = \sum_{d\,|\,n} \mu(d)\frac{n}{d}.$$

Stosując wzór na odwracanie (twierdzenie 14.7), dla $f = \varphi$ oraz dla $g : n \mapsto n$ otrzymamy:

$$n = \sum_{d\,|\,n} \varphi(d).$$

15 Ciągi Farey'a

Jak szybko wypisać wszystkie ułamki z przedziału $[0, 1]$ o mianownikach co najwyżej 8 posortowane rosnąco? Następująca technika działa zaskakująco dobrze. Zaczynamy od listy składającej się z dwóch ułamków: $\frac{0}{1}, \frac{1}{1}$. Następnie, między każde kolejne dwa ułamki wstawiamy ułamek o liczniku będącym sumą liczników i mianowniku będącego sumą mianowników. Powtarzamy to tak długo aż nie będziemy mogli wstawić już żadnego ułamka o odpowiednio małym mianowniku. Między $\frac{0}{1}$ i $\frac{1}{1}$ wstawiamy $\frac{0+1}{1+1} = \frac{1}{2}$:

$$\frac{0}{1}, \frac{1}{2}, \frac{1}{1}.$$

Między $\frac{0}{1}$ i $\frac{1}{2}$ wstawiamy $\frac{0+1}{1+2} = \frac{1}{3}$, a między $\frac{1}{2}$ i $\frac{1}{3}$ wstawiamy $\frac{1+1}{1+2} = \frac{2}{3}$:

$$\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}.$$

Między $\frac{0}{1}$ i $\frac{1}{3}$ wstawiamy $\frac{0+1}{1+3} = \frac{1}{4}$, między $\frac{1}{3}$ i $\frac{1}{2}$ wstawiamy $\frac{1+1}{3+2} = \frac{2}{5}$, między $\frac{1}{2}$ i $\frac{2}{3}$ wstawiamy $\frac{1+2}{2+3} = \frac{3}{5}$ oraz między $\frac{2}{3}$ i $\frac{1}{1}$ wstawiamy $\frac{2+1}{3+1} = \frac{3}{4}$:

$$\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}.$$

Dalej między $\frac{0}{1}$ i $\frac{1}{4}$ wstawiamy $\frac{0+1}{1+4} = \frac{1}{5}$, między $\frac{1}{4}$ i $\frac{1}{3}$ wstawiamy $\frac{1+1}{4+3} = \frac{2}{7}$, między $\frac{1}{3}$ i $\frac{2}{5}$ wstawiamy $\frac{1+2}{3+5} = \frac{3}{8}$, między $\frac{2}{5}$ i $\frac{1}{2}$ wstawiamy $\frac{2+1}{5+2} = \frac{3}{7}$, między

$\frac{1}{2}$ i $\frac{3}{5}$ wstawiamy $\frac{1+3}{2+5} = \frac{4}{7}$, między $\frac{3}{5}$ i $\frac{2}{3}$ wstawiamy $\frac{3+2}{5+3} = \frac{5}{8}$, między $\frac{2}{3}$ i $\frac{3}{4}$ wstawiamy $\frac{2+3}{3+4} = \frac{5}{7}$ oraz między $\frac{3}{4}$ i $\frac{1}{1}$ wstawiamy $\frac{3+1}{4+1} = \frac{4}{5}$:

$$\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{3}{8}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{5}{8}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}.$$

Między $\frac{0}{1}$ i $\frac{1}{5}$ wstawimy jeszcze ułamki $\frac{1}{8}$, $\frac{1}{7}$, $\frac{1}{6}$ oraz pomiędzy $\frac{4}{5}$ i $\frac{1}{1}$ wstawimy jeszcze $\frac{5}{6}$, $\frac{6}{7}$, $\frac{7}{8}$. Pomiędzy pozostałe ułamki już nic nie wstawimy, bo suma mianowników jest większa od 8. Ostatecznie otrzymujemy listę:

$$\frac{0}{1}, \frac{1}{8}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{3}{8}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{5}{8}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{7}{8}, \frac{1}{1}.$$

Są to wszystkie szukane ułamki. Dlaczego to działa?

Lemat 15.1. *Dla każdych dwóch sąsiednich ułamków na liście $\frac{a}{m}$ i $\frac{b}{n}$ zachodzi*

$$bm - an = 1. \tag{15.1}$$

Dowód. Indukcja. Dla ułamków $\frac{0}{1}$ i $\frac{1}{1}$ mamy $1 \cdot 1 - 0 \cdot 1 = 1$. Załóżmy, że między ułamki $\frac{a}{m} < \frac{b}{n}$ takie, że $bm - an = 1$ wstawiamy ułamek $\frac{a+b}{m+n}$. Liczymy:

$$(a+b)m - a(m+n) = am + bm - am - an = bm - an = 1,$$
$$b(m+n) - (a+b)n = bm + bn - an - bn = bm - an = 1.$$

□

Wniosek 15.2. *Każdy ułamek na liście jest nieskracalny.*

Wniosek 15.3. *Dla dwóch kolejnych ułamków z listy $\frac{a}{m} < \frac{b}{n}$ zachodzi:*

$$\frac{b}{n} - \frac{a}{m} = \frac{1}{mn}. \tag{15.2}$$

Lemat 15.4. *Dla dwóch dowolnych ułamków $\frac{u}{x} < \frac{v}{y}$ zachodzi $vx - uy \geq 1$ i*

$$\frac{v}{y} - \frac{u}{x} \geq \frac{1}{xy}.$$

Dowód.

$$0 < \frac{v}{y} - \frac{u}{x} = \frac{vx - uy}{xy},$$

więc $vx - uy > 0$, czyli $vx - uy \geq 1$, co kończy dowód. □

Fakt 15.5. *Niech $\frac{a}{m} < \frac{b}{n}$ będą kolejnymi ułamkami z listy, wtedy jeśli $\frac{a}{m} < \frac{c}{k} < \frac{b}{n}$, to $k \geq m + n$ i ponadto jeśli $k = m + n$, to $c = a + b$.*

Dowód. Z lematu 15.4 mamy nierówności:

$$\frac{c}{k} - \frac{a}{m} \geq \frac{1}{km},$$
$$\frac{b}{n} - \frac{c}{k} \geq \frac{1}{kn}.$$

Sumując stronami otrzymujemy:

$$\frac{1}{mn} \overset{(15.2)}{=} \frac{b}{n} - \frac{a}{m} \geq \frac{1}{km} + \frac{1}{kn}.$$

Mnożąc obie strony przez kmn otrzymujemy $k \geq n + m$. Załóżmy teraz, że $k = m + n$. Z $\frac{a}{m} < \frac{c}{m+n}$ i z lematu 15.4 mamy

$$\begin{aligned} cm - a(m+n) &\geq 1, \\ cm &\geq am + 1 + an \overset{(15.1)}{=} am + bm, \\ c &\geq a + b. \end{aligned}$$

Z $\frac{c}{m+n} < \frac{b}{n}$ i z lematu 15.4 mamy

$$\begin{aligned} b(m+n) - cn &\geq 1, \\ cn &\leq -1 + bm + bn \overset{(15.1)}{=} an + bn, \\ c &\leq a + b. \end{aligned}$$

Ostatecznie otrzymujemy $c = a + b$. □

Wiemy już, że ułamki na liście są nieskracalne. Pozostaje pokazać, że każdy ułamek o mianowniku nie przekraczającym pewnego ustalonego N zostanie wygenerowany. Załóżmy, że nie, tzn. niech ułamek $0 < \frac{c}{k} < 1$ będzie takim ułamkiem, którego nie udało się wygenerować oraz niech $k \leq N$. Dla ostatecznej listy będą istniały dwa kolejne ułamki $\frac{a}{m} < \frac{b}{n}$ takie, że $m + n > N$, między które wpada ułamek $\frac{c}{k}$, wtedy z faktu 15.5 wynika, że $k \geq m + n > N$, a to jest sprzeczność.

16 Przybliżanie liczb rzeczywistych ułamkami o niskich mianownikach

Szukamy dobrego przybliżenia liczby rzeczywistej $x \geq 0$ za pomocą ułamka $\frac{a}{m}$ tak, aby $|x - \frac{a}{m}|$ było jak najmniejsze wśród wszystkich ułamków o mianowniku $m \leq N$ dla pewnego ustalonego N. Najprościej jest utworzyć ciąg Farey'a wszystkich ułamków z przedziału $[\lfloor x \rfloor, \lfloor x \rfloor + 1]$ i zobaczyć, którym ułamkiem jest x, bądź między które dwa ułamki wpada i wybrać bliższy z nich. Zamiast generować całą listę ułamków możemy znaleźć tylko te dwa, które otaczają x.

Trzymamy tylko dwa ułamki, które otaczają x: $\frac{a}{m} < x < \frac{b}{n}$. Startujemy od ułamków $\frac{\lfloor x \rfloor}{1}$ i $\frac{\lfloor x \rfloor + 1}{1}$. Następnie, dopóki x nie jest równy jednemu z ułamków $\frac{a}{m}$, $\frac{b}{n}$ tak długo jak $m + n \leq N$ bierzemy ułamek $\frac{a+b}{m+n}$ i sprawdzamy, czy jest mniejszy, czy też większy od x zastępując nim odpowiednio mniejszy lub większy z dwóch ułamków $\frac{a}{m}$ i $\frac{b}{n}$.

Przykład 16.1. Przybliżamy $\sqrt{2}$ ułamkiem o mianowniku co najwyżej 10. Mamy $\frac{1}{1} < \sqrt{2} < \frac{2}{1}$. Bierzemy $\frac{1+2}{1+1} = \frac{3}{2} > \sqrt{2}$, więc $\frac{1}{1} < \sqrt{2} < \frac{3}{2}$. Bierzemy $\frac{1+3}{1+2} = \frac{4}{3} < \sqrt{2}$, więc $\frac{4}{3} < \sqrt{2} < \frac{3}{2}$. Bierzemy $\frac{4+3}{3+2} = \frac{7}{5} < \sqrt{2}$, więc $\frac{7}{5} < \sqrt{2} < \frac{3}{2}$. Bierzemy $\frac{7+3}{5+2} = \frac{10}{7} > \sqrt{2}$, więc $\frac{7}{5} < \sqrt{2} < \frac{10}{7}$. Teraz $5 + 7 > 10$, więc szukany ułamek to

$\frac{7}{5}$ lub $\frac{10}{7}$. Mamy

$$\sqrt{2} - \frac{7}{5} \approx 0.01421,$$
$$\sqrt{2} - \frac{10}{7} \approx 0.01436,$$

zatem lepszy jest $\frac{7}{5}$.

Powyższy sposób możemy jeszcze przyspieszyć. Niech

$$\frac{a}{m} < x < \frac{b}{n}.$$

Załóżmy, że najbliższe nowe t ułamków będzie nie większe od x, a $t+1$ już większy od x. Wtedy sytuacja wygląda tak:

$$\frac{a}{m} < \frac{a+b}{m+n} < \frac{a+2b}{m+2n} < \ldots < \frac{a+tb}{m+tn} \leq x < \frac{a+(t+1)b}{m+(t+1)n} < \frac{b}{n}.$$

Zamiast monotonie do lewego ułamka dodawać ułamek $\frac{b}{n}$, najlepiej od razu by znaleźć t i przejść do pary $\frac{a+tb}{m+tn}$, $\frac{b}{n}$. Znajdźmy to t. t jest największa liczbą całkowitą taką, że zachodzi

$$\begin{aligned} \frac{a+tb}{m+tn} &\leq x, \qquad \text{przekształcamy} \\ a+tb &\leq mx+tnx, \\ (b-nx)t &\leq mx-a. \end{aligned}$$

Ponieważ $x < \frac{b}{n}$, więc $b - nx > 0$, czyli mamy

$$t \leq \frac{mx-a}{b-nx},$$

skąd wzór na t:

$$t = \left\lfloor \frac{mx-a}{b-nx} \right\rfloor. \tag{16.1}$$

Podobnie rozumujemy, gdy najbliższe t będzie nie mniejsze od x, a $t+1$ już większy od x w takiej sytuacji:

$$\frac{a}{m} < \frac{(t+1)a+b}{(t+1)m+n} < x \leq \frac{ta+b}{tm+n} < \ldots < \frac{2a+b}{2m+n} < \frac{a+b}{m+n} < \frac{b}{n}.$$

Zamiast monotonie do prawego ułamka dodawać ułamek $\frac{a}{m}$, przejdziemy od razu do pary $\frac{a}{m}$, $\frac{ta+b}{tm+n}$. Szukamy największego całkowitego t takiego, że

$$\begin{aligned} x &\leq \frac{ta+b}{tm+n}, \qquad \text{przekształcamy} \\ tmx+nx &\leq ta+b, \\ (mx-a)t &\leq b-nx. \end{aligned}$$

Ponieważ $\frac{a}{m} < x$, więc $mx - a > 0$, czyli mamy

$$t \leq \frac{b-nx}{mx-a},$$

skąd wzór na t:

$$t = \left\lfloor \frac{b - nx}{mx - a} \right\rfloor . \tag{16.2}$$

Usystematyzujmy teraz nasze szukanie ułamków. Zacznijmy szukać przybliżenia x od ułamków $\frac{0}{1}$ i $\frac{1}{0}$. $\frac{1}{0}$ symbolicznie oznacza nieskończoność. Możemy sobie pozwolić na zaczynanie budowania ułamków Farey'a od tych ułamków, bo spełniony jest dla nich lemat 15.1. Oznaczmy

$$\frac{P_{-1}}{Q_{-1}} = \frac{0}{1} \qquad\qquad \frac{P_0}{Q_0} = \frac{1}{0}.$$

Będziemy budować kolejne ułamki $\frac{P_k}{Q_k}$ w ten sposób, że:

$$\begin{aligned} \frac{P_{k-1}}{Q_{k-1}} \leq x \leq \frac{P_k}{Q_k} \quad & \text{dla } k \text{ parzystego,} \\ \frac{P_k}{Q_k} \leq x \leq \frac{P_{k-1}}{Q_{k-1}} \quad & \text{dla } k \text{ nieparzystego.} \end{aligned}$$

Wyznaczymy wzory na P_k i Q_k. Dla $k-1$ parzystego będziemy prawy ułamek $\frac{P_{k-1}}{Q_{k-1}}$ dodawać do lewego $\frac{P_{k-2}}{Q_{k-2}}$ ile się da i wynikowy ułamek oznaczymy sobie przez $\frac{P_k}{Q_k}$. Z równania (16.1) wynika, że jeśli weźmiemy

$$q_k = \left\lfloor \frac{Q_{k-2}x - P_{k-2}}{P_{k-1} - Q_{k-1}x} \right\rfloor ,$$

to będzie

$$\frac{P_k}{Q_k} = \frac{P_{k-2} + q_k P_{k-1}}{Q_{k-2} + q_k Q_{k-1}}.$$

Dla $k-1$ nieparzystego będziemy lewy ułamek $\frac{P_{k-1}}{Q_{k-1}}$ dodawać do prawego $\frac{P_{k-2}}{Q_{k-2}}$ ile się da i wynikowy ułamek oznaczymy przez $\frac{P_k}{Q_k}$. Z równania (16.2) wynika, że jeśli weźmiemy

$$q_k = \left\lfloor \frac{Q_{k-2}x - P_{k-2}}{P_{k-1} - Q_{k-1}x} \right\rfloor ,$$

to będzie

$$\frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}}.$$

W obu przypadkach otrzymaliśmy ten sam wzór. Ostatecznie mamy wzory:

$$\begin{aligned} P_{-1} &= 0 & Q_{-1} &= 1 \\ P_0 &= 1 & Q_1 &= 0 \\ P_k &= q_k P_{k-1} + P_{k-2} & Q_k &= q_k Q_{k-1} + Q_{k-2} \end{aligned}$$

gdzie $q_k = \lfloor x_k \rfloor$ dla $k \geq 1$ przy oznaczeniu

$$x_k = \frac{Q_{k-2}x - P_{k-2}}{P_{k-1} - Q_{k-1}x}. \tag{16.3}$$

Używając powyższych wzorów będziemy budować kolejne ułamki tak długo jak $Q_k \leq N$. Niech $k \geq 1$ będzie największe takie, że $Q_k \leq N$. Wtedy x znajduje się między ułamkami $\frac{P_{k-1}}{Q_{k-1}}$ i $\frac{P_k}{Q_k}$. Dodając q_{k+1} razy ułamek $\frac{P_k}{Q_k}$ do ułamka $\frac{P_{k-1}}{Q_{k-1}}$ otrzymamy mianownik większy od N. Należy zatem tych dodań wykonać mniej, powiedzmy t razy, przy czym t jest największą liczbą całkowitą, że $tQ_k+Q_{k-1} \leq N$, skąd $t \leq \frac{N-Q_{k-1}}{Q_k}$. Zatem tych dodawań możemy wykonać maksymalnie:

$$\left\lfloor \frac{N - Q_{k-1}}{Q_k} \right\rfloor.$$

Podsumowując otrzymujemy następujące twierdzenie.

Twierdzenie 16.2. *Najlepszym przybliżeniem w postaci ułamka $\frac{a}{m}$ liczby $x \geq 0$, w tym sensie, że $|x - \frac{a}{m}|$ jest możliwie najmniejsze, takim, że $m \leq N$ będzie jeden z ułamków:*

$$\frac{P_k}{Q_k} \qquad \frac{tP_k + P_{k-1}}{tQ_k + Q_{k-1}}$$

gdzie $k \geq 1$ jest największą taką liczbą, że $Q_k \leq N$ oraz

$$t = \left\lfloor \frac{N - Q_{k-1}}{Q_k} \right\rfloor.$$

Pozostaje nam uprościć jeszcze wzór (16.3) na x_k.

Fakt 16.3. *Zachodzi $x_1 = x$ i dla $k \geq 2$*

$$x_k = \frac{1}{x_{k-1} - q_{k-1}}$$

Dowód. Liczymy

$$x_1 = \frac{Q_{-1}x - P_{-1}}{P_0 - Q_0 x} = \frac{1 \cdot x - 0}{1 - 0 \cdot x} = x$$

oraz

$$\frac{1}{x_{k-1} - q_{k-1}} = \frac{1}{\frac{Q_{k-3}x - P_{k-3}}{P_{k-2} - Q_{k-2}x} - q_{k-1}} = \frac{1}{\frac{Q_{k-3}x - P_{k-3} - q_{k-1}P_{k-2} + q_{k-1}Q_{k-2}x}{P_{k-2} - Q_{k-2}x}} =$$

$$\frac{P_{k-2} - Q_{k-2}x}{(q_{k-1}Q_{k-2} + Q_{k-3})x - (q_{k-1}P_{k-2} + P_{k-3})} = \frac{P_{k-2} - Q_{k-2}x}{Q_{k-1}x - P_{k-1}} = x_k$$

□

Z tego faktu mamy następujące wnioski pokazujące, że w istocie rzeczy pracujemy na ułamkach łańcuchowych.

Wniosek 16.4. *Dla $k \geq 1$ zachodzą wzory*

$$x = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \, \cfrac{}{q_{k-1} + \cfrac{1}{x_k}}}} \tag{16.4}$$

$$\frac{P_k}{Q_k} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \, \cfrac{}{q_{k-1} + \cfrac{1}{q_k}}}} \tag{16.5}$$

Dowód. Równość (16.4) wynika z faktu 16.3. Dowodzimy ją indukcją po k.

1. Dla $k = 1$ mamy $x = x_1$.
2. Niech $k \geq 2$. Z założenia indukcyjnego mamy:

$$x = q_1 + \cfrac{1}{\cfrac{\vdots}{q_{k-2} + \cfrac{1}{x_{k-1}}}}, \tag{16.6}$$

   a z faktu 16.3 wiemy, że:

$$x_k = \frac{1}{x_{k-1} - q_{k-1}},$$

   skąd po przekształceniu mamy

$$x_{k-1} = q_{k-1} + \frac{1}{x_k},$$

   wstawiając to do (16.6) otrzymujemy tezę.

Dowód równości (16.5) jest nieco trudniejszy. Znowu użyjemy indukcji po k.

1. Dla $k = 1$ mamy

$$\frac{P_1}{Q_1} = \frac{q_1 P_0 + P_{-1}}{q_1 Q_0 + Q_{-1}} = \frac{q_1 \cdot 1 + 0}{q_1 \cdot 0 + 1} = \frac{q_1}{1} = q_1.$$

2. Załóżmy, że $k \geq 2$. Z założenia indukcyjnego mamy, że

$$\frac{P_{k-1}}{Q_{k-1}} = q_1 + \cfrac{1}{\cfrac{\vdots}{q_{k-2} + \cfrac{1}{q_{k-1}}}}. \tag{16.7}$$

   Z drugiej strony wiemy, że

$$\frac{P_{k-1}}{Q_{k-1}} = \frac{q_{k-1} P_{k-2} + P_{k-3}}{q_{k-1} Q_{k-2} + Q_{k-3}}. \tag{16.8}$$

   Zauważmy, że liczby P_{k-2} i Q_{k-2} dadzą się wyrazić jako funkcja wymierna od liczb $q_1, q_2, \ldots, q_{k-2}$. Wynika to z założenia indukcyjnego na przedstawienie $\frac{P_{k-2}}{Q_{k-2}}$ za pomocą ułamka łańcuchowego. Analogicznie liczby P_{k-3} i Q_{k-3} dadzą się wyrazić za pomocą liczb $q_1, \ldots, q_{k-2}$, a zatem po prawej stronie wyrażenia (16.8) jest funkcja wymierna od liczb $q_1, \ldots, q_{k-1}$, przy czym liczba q_{k-1} pojawia się tylko dwa razy, raz w liczniku i raz w mianowniku. W pozostałej części tj. w $P_{k-2}, P_{k-3}, Q_{k-2}, Q_{k-3}$ liczba q_{k-1} nie pojawia się. Teraz, ponieważ prawe strony równości (16.7) i (16.8) są sobie równe oraz są to funkcje od $q_1, \ldots, q_{k-1}$, więc jeśli w obu tych wyrażeniach podmienimy q_{k-1} na $q_{k-1} + \frac{1}{q_k}$, to równość zostanie zachowana:

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \cfrac{}{q_{k-1} + \cfrac{1}{q_k}}}} = \frac{\left(q_{k-1} + \frac{1}{q_k}\right)P_{k-2} + P_{k-3}}{\left(q_{k-1} + \frac{1}{q_k}\right)Q_{k-2} + Q_{k-3}}$$

$$= \frac{\frac{1}{q_k}P_{k-2} + q_{k-1}P_{k-2} + P_{k-3}}{\frac{1}{q_k}Q_{k-2} + q_{k-1}Q_{k-2} + Q_{k-3}}$$

$$= \frac{\frac{1}{q_k}P_{k-2} + P_{k-1}}{\frac{1}{q_k}Q_{k-2} + Q_{k-1}} = \frac{P_{k-2} + q_kP_{k-1}}{Q_{k-2} + q_kQ_{k-1}} = \frac{P_k}{Q_k},$$

a to jest teza.

□

Liczby $\frac{P_k}{Q_k}$ nazywa się reduktami ułamka łańcuchowego.

Przykład 16.5. Znajdziemy najlepsze przybliżenie $\sqrt{3}$ ułamkiem o mianowniku nieprzekraczającym 10. Mamy $x = x_1 = \sqrt{3}$, $q_1 = 1$, $P_1 = 1 \cdot P_0 + P_{-1} = 1 \cdot 1 + 0 = 1$, $Q_1 = 1 \cdot Q_0 + Q_{-1} = 1 \cdot 0 + 1 = 1$. Dalej

$$x_2 = \frac{1}{x_1 - q_1} = \frac{1}{\sqrt{3} - 1} = \frac{\sqrt{3} + 1}{2},$$

skąd $q_2 = \lfloor x_2 \rfloor = 1$, $P_2 = 1 \cdot P_1 + P_0 = 1 \cdot 1 + 1 = 2$, $Q_2 = 1 \cdot Q_1 + Q_0 = 1 \cdot 1 + 0 = 1$. Dalej

$$x_3 = \frac{1}{x_2 - q_2} = \frac{1}{\frac{\sqrt{3}+1}{2} - 1} = \frac{1}{\frac{\sqrt{3}-1}{2}} = \frac{2}{\sqrt{3} - 1} = \sqrt{3} + 1,$$

skąd $q_3 = 2$, $P_3 = 2 \cdot 2 + 1 = 5$, $Q_3 = 2 \cdot 1 + 1 = 3$. Dalej otrzymamy $x_4 = x_2$, zatem $q_4 = 1$, $P_4 = 1 \cdot 5 + 2 = 7$, $Q_4 = 1 \cdot 3 + 1 = 4$. Następnie $x_5 = x_3$ i $q_5 = 2$, ale wtedy $Q_5 = 2 \cdot 4 + 3 = 11 > 10$. Zatem $k = 4$ jest maksymalne takie, że $Q_k \leq 10$. Liczymy $t = \lfloor \frac{N - Q_{k-1}}{Q_k} \rfloor = \lfloor \frac{10-3}{4} \rfloor = \lfloor \frac{7}{4} \rfloor = 1$. Najlepsze przybliżenie $\sqrt{3}$ jest wśród ułamków $\frac{7}{4}$ i $\frac{1 \cdot 7 + 5}{1 \cdot 4 + 3} = \frac{12}{7}$. Sprawdzamy:

$$\frac{7}{4} - \sqrt{3} \approx 0.01795,$$
$$\sqrt{3} - \frac{12}{7} \approx 0.01777,$$

zatem szukanym ułamkiem jest $\frac{12}{7}$ i wcale nie jest to redukt ułamka łańcuchowego.