FUNKCJE MULTYPLIKATYWNE

Definicja. Funkcję $f : \mathbb{N} \to \mathbb{R}$ nazywamy **funkcją multyplikatywną**, jeśli dla dowolnych $m, n \in \mathbb{N}$

$$\mathrm{NWD}(m,n) = 1 \Rightarrow f(mn) = f(m) \cdot f(n).$$

Definicja. Funkcję $f : \mathbb{N} \to \mathbb{R}$ nazywamy **funkcją całkowicie multyplikatywną**, jeśli dla dowolnych $m, n \in \mathbb{N}$

$$f(mn) = f(m) \cdot f(n).$$

Oczywiście funkcja całkowicie multyplikatywna jest multyplikatywna.

Przykłady.

(1) Funkcja $f(n) = 1$ jest całkowicie multyplikatywna.
(2) Funkcja $f(n) = n$ jest całkowicie multyplikatywna.

Twierdzenie 1. Jeśli funkcja $f : \mathbb{N} \to \mathbb{R}$ jest multyplikatywna, to funkcja $g : \mathbb{N} \to \mathbb{R}$ określona wzorem

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

też jest multyplikatywna. ♠

Następne przykłady.

(3) Funkcja $\tau(n)$ określona wzorem $\tau(n) = \sum_{d|n} 1$ jest multyplikatywna. Zauważmy, że $\tau(n)$ jest liczbą dzielników dodatnich liczby n.

(4) Funkcja $\sigma(n)$ określona wzorem $\sigma(n) = \sum_{d|n} d$ jest multyplikatywna. Zauważmy, że $\sigma(n)$ jest sumą wszystkich dodatnich dzielników liczby n.

(5) Natomiast funkcja $s(n)$ określona wzorem $s(n) = \sigma(n) - n$ nie jest multyplikatywna. Zauważmy, że $s(n)$ jest sumą wszystkich właściwych (tzn. różnych od n) dzielników dodatnich liczby n.

Wartości tych trzech funkcji dla wybranych n są następujące:

n	1	2	3	4	5	6	7	8	9	10	28	100	101	220	284
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	6	9	2	12	6
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	56	217	102	504	504
$s(n)$	0	1	1	3	1	6	1	7	4	8	28	117	1	284	220

FUNKCJA τ

Twierdzenie 2. Jeśli liczba n jest pierwsza, to $\tau(n) = 2$.
Jeśli liczba n jest potęgą liczby pierwszej, np. $n = p^\alpha$, to $\tau(n) = \alpha + 1$.

Jeśli n jest liczbą złożoną oraz $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, to

$$\tau(n) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1). \quad \spadesuit$$

Przykład. Niech $n = 600 = 2^3 \cdot 3^1 \cdot 5^2$. Wtedy

$$\tau(600) = (3+1) \cdot (1+1) \cdot (2+1) = 24.$$

FUNKCJA σ

Twierdzenie 3. Jeśli liczba n jest pierwsza, to $\sigma(n) = p + 1$.
Jeśli liczba n jest potęgą liczby pierwszej, np. $n = p^\alpha$, to

$$\sigma(n) = 1 + p + p^2 + \ldots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

Jeśli n jest liczbą złożoną oraz $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, to

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \quad \spadesuit$$

Przykład. Niech $n = 600$. Wtedy

$$\sigma(600) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{5^3 - 1}{5 - 1} = 15 \cdot 4 \cdot 31 = 1860.$$

LICZBY DOSKONAŁE I ZAPRZYJAŹNIONE

Definicja. Liczbę n nazywamy **liczbą doskonałą**, jeśli $s(n) = n$ (lub równoważnie $\sigma(n) = 2n$).

Definicja. Liczby m i n nazywamy **liczbami zaprzyjaźnionymi**, jeśli $s(m) = n$ oraz $s(n) = m$.

Przykłady. Czterema najmniejszymi liczbami doskonałymi są:

$$6, \quad 28, \quad 496 \text{ i } 8128.$$

(1) Mianowicie: $6 = 2 \cdot 3$, skąd dostajemy

$$\sigma(6) = (1+2) \cdot (1+3) = 3 \cdot 4 = 12 = 2 \cdot 6.$$

(2) Podobnie $28 = 2^2 \cdot 7$, skąd dostajemy

$$\sigma(28) = (1 + 2 + 4) \cdot (7 + 1) = 7 \cdot 8 = 56 = 2 \cdot 28.$$

(3) Następnie $496 = 2^4 \cdot 31$, skąd dostajemy

$$\sigma(496) = (1 + 2 + 4 + 8 + 16) \cdot (31 + 1) = 31 \cdot 32 = 992 = 2 \cdot 496.$$

(4) Wreszcie $8128 = 2^6 \cdot 127$, skąd dostajemy

$$\sigma(496) = (1 + 2 + 4 + 8 + 16 + 32 + 64) \cdot (127 + 1) = 127 \cdot 128 = 16256 = 2 \cdot 128.$$

Twierdzenie 4. (Euklides, Euler) Liczba parzysta n jest doskonała wtedy i tylko wtedy, gdy

$$n = 2^{p-1} \cdot (2^p - 1),$$

gdzie liczba $2^p - 1$ jest liczbą pierwszą.

Dowód w jedną stronę. Niech

$$n = 2^{p-1} \cdot (2^p - 1)$$

i niech $2^p - 1$ będzie liczbą pierwszą. Wtedy

$$\begin{aligned} \sigma(n) &= (1 + 2 + 4 + \ldots + 2^{p-1}) \cdot (2^p - 1 + 1) = \\ &= (2^p - 1) \cdot 2^p = 2 \cdot n. \quad \spadesuit \end{aligned}$$

Uwaga. Nie wiemy, czy istnieją nieparzyste liczby doskonałe.

LICZBY MERSENNE'A

Twierdzenie 5. Jeśli liczba $2^n - 1$ jest pierwsza, to liczba n też jest pierwsza.

Dowód. Jeśli $k \mid n$, to $2^k - 1 \mid 2^n - 1$. $\spadesuit$

Definicja. Liczbę $M_n = 2^n - 1$ nazywamy **n-tą liczbą Mersenne'a**. Jeśli liczba M_n jest pierwsza, to nazywamy ją **liczbą pierwszą Mersenne'a**.

Marin Mersenne (1588 – 1648), mnich franciszkański żyjący w Paryżu, stwierdził bez dowodu, że liczby M_p dla

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

są pierwsze oraz że są to jedyne liczby pierwsze postaci M_p dla $p \leq 257$. W ciągu następnych 300 lat stwierdzono, że Mersenne popełnił 5 błędów: liczby M_{67} i M_{257} są złożone oraz liczby M_{61}, M_{89} i M_{107} są pierwsze.

Od lat poszukiwano coraz większych liczb pierwszych. Największe odkrywane liczby pierwsze to były z reguły liczby Mersenne'a. A oto tabela znanych liczb Mersenne'a:

ZNANE LICZBY MERSENNE'A

Nr	p	Liczba cyfr M_p	Rok odkrycia
1	2	1	starożytność
2	3	1	starożytność
3	5	2	starożytność
4	7	3	starożytność
5	13	4	1456
6	17	6	1588
7	19	6	1588
8	31	10	1772
9	61	19	1883
10	89	27	1911
11	107	33	1914
12	127	39	1876
13	521	157	1952
14	607	183	1952
15	1279	386	1952
16	2203	664	1952
17	2281	687	1952
18	3217	969	1957
19	4253	1281	1961
20	4423	1332	1961
21	9689	2917	1963
22	9941	2993	1963
23	11213	3376	1963
24	19937	6002	1971
25	21701	6533	1978
26	23209	6987	1979
27	44497	13395	1979
28	86243	25962	1982
29	110503	33265	1988
30	132049	39751	1983
31	216091	65050	1985
32	756839	227832	1992
33	859433	258716	1994
34	1257787	378632	1996
35	1398269	420921	1996
36	2976221	895932	1997
37	3021377	909526	1998
?	6972593	2098960	1999
?	13466917	4053946	2001

Liczby pierwsze Mersenne'a dla $p \leq 127$ zostały odkryte przed erą komputerów. Także złożoność liczby M_{257} została stwierdzona bez komputera: przez D. H. Lehmera w 1927 roku. Pierwsze próby wykorzystania komputera: Turing w 1951 roku, bez powodzenia. Pierwsza udana próba: R. M. Robinson w 1952 roku na komputerze SWAC w National Bureau of Standards w Los Angeles.

Na ogół liczby Mersenne'a były rekordzistkami, jedynym wyjątkiem była liczba

$$391581 \cdot 2^{216139} - 1,$$

która na pewien czas wyprzedziła liczbę M_{216091}.

Twierdzenie 6. Jeśli p jest liczbą pierwszą oraz $p \equiv 3 \pmod 4$, to liczba $2p+1$ jest dzielnikiem M_p wtedy i tylko wtedy, gdy $2p+1$ jest liczbą pierwszą. Zatem, jeśli $p > 3$ i liczba $2p+1$ jest pierwsza, to M_p jest liczbą złożoną. ♠

Z tego twierdzenia otrzymujemy więc:

$$23 \mid M_{11}, \quad 47 \mid M_{23}, \quad 167 \mid M_{83}, \quad 263 \mid M_{131},$$
$$359 \mid M_{179}, \quad 383 \mid M_{191}, \quad 479 \mid M_{239}, \quad 503 \mid M_{251}.$$

Twierdzenie 7. Jeśli $d \mid M_p$, to $d \equiv 1 \pmod{2p}$. ♠

Przykład. Niech $p = 23$. Wtedy $M_{23} = 8388607$. Najmniejszą liczbą postaci $46k+1$ jest 47. Łatwo sprawdzamy, że $47 \mid M_{23}$, a więc M_{23} jest liczbą złożoną.

Przykład. Niech $p = 13$. Wtedy $M_{13} = 8191$ oraz $\sqrt{M_{13}} = 90,504\ldots$. Jedynymi liczbami pierwszymi postaci $26k+1$ mniejszymi od 90 są 53 i 79. Ponieważ M_{13} nie dzieli się przez te liczby, więc jest pierwsza.

TEST LUCASA-LEHMERA

Twierdzenie 8. Niech p będzie liczbą pierwszą. Definiujemy następujący ciąg liczb:

$$r_1 = 4, \quad r_k = (r_{k-1}^2 - 2) \,\mathbf{mod}\, M_p \quad \text{dla } k \geq 2 \quad .$$

Wówczas liczba Mersenne'a M_p jest pierwsza wtedy i tylko wtedy, gdy

$$r_{p-1} = 0. \quad ♠$$

Wniosek. Do stwierdzenia, czy liczba M_p jest pierwsza, wystarczy $O(p^3)$ działań na bitach. ♠

Przykład. Niech $p = 5$. Wtedy $M_5 = 31$. Obliczamy kolejno:

$$\begin{aligned} r_1 &= 4, \\ r_2 &= (4^2 - 2)\,\mathbf{mod}\,31 = 14, \\ r_3 &= (14^2 - 2)\,\mathbf{mod}\,31 = 190\,\mathbf{mod}\,31 = 8, \\ r_4 &= (8^2 - 2)\,\mathbf{mod}\,31 = 62\,\mathbf{mod}\,31 = 0. \end{aligned}$$

Zatem liczba $M_5 = 31$ jest pierwsza.

Jeszcze jedno zastosowanie liczb Mersenne'a.

Twierdzenie 9. Istnieje nieskończenie wiele liczb pierwszych.

Dowód. Niech p będzie największą liczbą pierwszą. Niech q będzie dzielnikiem pierwszym liczby Mersenne'a $M_p = 2^p - 1$. Wtedy

$$2^p \equiv 1 \pmod{q},$$

a więc liczba 2 ma rząd p w grupie multyplikatywnej ciała $\mathbb{Z}_q$. Z twierdzenia Lagrange'a wynika, że $p \mid q - 1$, a więc $p < q$, sprzeczność. ♠

Nie znamy odpowiedzi na następujące pytania:
(1) Czy istnieje nieskończenie wiele liczb pierwszych Mersenne'a?
(2) Czy istnieje nieskończenie wiele liczb złożonych Mersenne'a?
(3) Czy każda liczba Mersenne'a jest bezkwadratowa?

Wiadomo, że jeśli M_p jest liczbą pierwszą Mersenne'a, to liczba M_{M_p} nie musi być liczbą pierwszą: liczba

$$M_{M_{13}} = 2^{8191} - 1$$

jest złożona. Ma ona ponad 2400 cyfr. Znamy nawet jej dzielnik pierwszy:

$$p = 2 \cdot 20644229 \cdot M_{13} + 1 = 338193759479.$$

FUNKCJA MÖBIUSA

Definicja. Funkcją Möbiusa $\mu(n)$ nazywamy funkcję określoną w następujący sposób:
- $\mu(1) = 1$;
- $\mu(n) = 0$, jeśli liczba n jest podzielna przez kwadrat liczby pierwszej (tzn. nie jest bezkwadratowa);
- $\mu(n) = (-1)^k$, jeśli liczba n jest bezkwadartowa i jest iloczynem k różnych liczb pierwszych.

Twierdzenie 10. Funkcja Möbiusa μ jest multyplikatywna. Ponadto, jeśli zdefiniujemy funkcję ν wzorem

$$\nu(n) = \sum_{d|n} \mu(d),$$

to

$$\nu(1) = 1 \quad \text{oraz} \quad \nu(n) = 0 \quad \text{dla } n > 1 \quad . \qquad \spadesuit$$

Wartości funkcji Möbiusa:

n	1	2	3	4	5	6	7	8	9	10	100	101	102
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	0	-1	-1

Twierdzenie 11. (Wzór inwersyjny Möbiusa) Jeśli $f : \mathbb{N} \to \mathbb{R}$ oraz

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

to

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot g(d) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right). \qquad \spadesuit$$

Twierdzenie 12. Jeśli

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot g(d),$$

to

$$g(n) = \sum_{d|n} f(d). \qquad \spadesuit$$

Wniosek. Załóżmy, że $f : \mathbb{N} \to \mathbb{R}$ oraz

$$g(n) = \sum_{d|n} f(d).$$

Wówczas, jeśli funkcja g jest multyplikatywna, to funkcja f też jest multyplikatywna.

FUNKCJA φ EULERA

Definicja. Niech n będzie liczbą całkowitą dodatnią. Wtedy definiujemy

$$\varphi(n) = |\{k : \ 1 \le k \le n \quad \text{oraz} \quad \mathrm{NWD}(k, n) = 1 \ \}|.$$

Funkcję φ nazywamy **funkcją Eulera**.

Wartości funkcji Eulera:

n	1	2	3	4	5	6	7	8	9	10	100	101	102	103
$\mu(n)$	1	1	2	2	4	2	6	4	6	4	40	100	32	102

Twierdzenie 13. Niech p będzie liczbą pierwszą. Wtedy

$$\varphi(p) = p - 1. \quad \spadesuit$$

Twierdzenie 14. Niech n będzie potęgą liczby pierwszej:

$$n = p^\alpha.$$

Wtedy

$$\varphi(n) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^\alpha \cdot \left(1 - \frac{1}{p}\right). \quad \spadesuit$$

Przykłady.

$$\begin{aligned} \varphi(2^{10}) &= 2^{10} - 2^9 = 512, \\ \varphi(11^2) &= 11^2 - 11 = 110. \end{aligned}$$

Twierdzenie 15. Funkcja φ jest multyplikatywna.

Dowód. Niech m i n będą liczbami względnie pierwszymi. Zapiszmy liczby od 1 do mn w tabeli:

$$\begin{array}{cccccc}
1 & m+1 & 2m+1 & \ldots & (n-2)m+1 & (n-1)m+1 \\
2 & m+2 & 2m+2 & \ldots & (n-2)m+2 & (n-1)m+2 \\
3 & m+3 & 2m+3 & \ldots & (n-2)m+3 & (n-1)m+3 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
r & m+r & 2m+r & \ldots & (n-2)m+r & (n-1)m+r \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
m & 2m & 3m & \ldots & (n-1)m & nm
\end{array}$$

Jeśli $\mathrm{NWD}(r, m) = d > 1$ to w r-tym wierszu wszystkie liczby mają wspólny dzielnik d z mn. Jeśli $\mathrm{NWD}(r, m) = 1$, to w r-tym wierszu mamy zupełny układ reszt modulo n, więc w tym wierszu jest $\varphi(n)$ liczb względnie pierwszych z n. Są one też względnie pierwsze z m, więc są względnie pierwsze z mn. Takich wierszy jest $\varphi(m)$, więc łącznie jest $\varphi(m) \cdot \varphi(n)$ liczb względnie pierwszych z mn. $\spadesuit$

Wniosek. Niech

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Wtedy

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right). \quad \spadesuit$$

Istnieje także prosty dowód kombinatoryczny korzystający z zasady włączeń i wyłączeń.

Twierdzenie 16. Niech n będzie liczbą całkowitą dodatnią. Wtedy

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

Dowód. Niech
$$\{1,2,\ldots,n\}=\bigcup_{d|n} C_d,$$
gdzie
$$C_d=\{m:\ 1\le m\le n \ \text{ oraz }\ \mathrm{NWD}(m,n)=d\ \}.$$
Wtedy
$$|C_d|=\varphi\left(\frac{n}{d}\right),$$
skąd łatwo wynika, że
$$n=\sum_{d|n}\varphi\left(\frac{n}{d}\right).$$
Ale jeśli d przebiega wszystkie dzielniki n, to $\frac{n}{d}$ też i stąd natychmiast wynika teza. ♠

Przykład. Niech $n=18$. Wtedy
$$\begin{array}{lcllcl}
C_1 &=& \{1,5,7,11,13,17\}, & |C_1| &=& \varphi(18)=6,\\
C_2 &=& \{2,4,8,10,14,16\}, & |C_2| &=& \varphi(9)=6,\\
C_3 &=& \{3,15\}, & |C_3| &=& \varphi(6)=2,\\
C_6 &=& \{6,12\}, & |C_6| &=& \varphi(3)=2,\\
C_9 &=& \{9\}, & |C_9| &=& \varphi(2)=1,\\
C_{18} &=& \{18\}, & |C_{18}| &=& \varphi(1)=1.
\end{array}$$

TWIERDZENIE EULERA

Twierdzenie 17. Niech n będzie dowolną liczbą całkowitą dodatnią i niech $\mathrm{NWD}(a,n)=1$. Wtedy
$$a^{\varphi(n)}\equiv 1 \pmod{n}.$$

Dowód. Niech
$$r_1,\quad r_2,\quad \ldots,\quad r_{\varphi(n)}$$
będą wszystkimi liczbami mniejszymi od n, względnie pierwszymi z n. Zauważmy, że liczba ar_i jest też względnie pierwsza z n. Zatem liczby
$$ar_1 \,\mathbf{mod}\, n,\quad ar_2 \,\mathbf{mod}\, n,\quad \ldots,\quad ar_{\varphi(n)} \,\mathbf{mod}\, n$$
są też względnie pierwsze z n. Zauważmy ponadto, że jeśli
$$r_i\ne r_j,$$
to
$$ar_i \,\mathbf{mod}\, n \ne ar_j \,\mathbf{mod}\, n.$$

Zatem

$$r_1 r_2 \cdot \ldots \cdot r_{\varphi(n)} \equiv a^{\varphi(n)} \cdot r_1 r_2 \cdot \ldots \cdot r_{\varphi(n)} \pmod{n}.$$

Stąd natychmiast wynika, że

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \quad \spadesuit$$

Możemy wykorzystać twierdzenie Eulera do rozwiązywania kongruencji liniowych. Jeśli chcemy znaleźć element odwrotny do a modulo n, to zauważamy, że

$$a \cdot a^{\varphi(n)-1} \equiv 1 \pmod{n},$$

a więc $a^{\varphi(n)-1}$ jest tym szukanym elementem odwrotnym.

Zatem rozwiązaniem kongruencji

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

jest

$$x = a^{\varphi(n)-1} \cdot b \,\mathbf{mod}\, n.$$

Rozwiązaniem kongruencji

$$3x \equiv 7 \pmod{10}$$

jest

$$x = 3^{\varphi(10)-1} \cdot 7 \,\mathbf{mod}\, 10 = 3^3 \cdot 7 \,\mathbf{mod}\, 10 = 9.$$

Na zakończenie podamy związek funkcji Eulera z funkcją Möbiusa:

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

RZĄD LICZBY

Wiemy, że jeśli n jest liczbą całkowitą dodatnią oraz $\mathrm{NWD}(a,n) = 1$, to istnieje liczba m taka, że

$$a^m \equiv 1 \pmod{n}.$$

Na przykład $m = \varphi(n)$.

Definicja. Rzędem liczby a modulo n nazywamy najmniejszą liczbę m taką, że

$$a^m \equiv 1 \pmod{n}.$$

Rząd liczby a modulo n oznaczamy symbolem $\mathrm{ord}_n a$.

Zauważmy, że rząd liczby a modulo n jest to dokładnie rząd elementu a w grupie multyplikatywnej $\mathbb{Z}_n^*$ elementów odwracalnych pierścienia $\mathbb{Z}_n$.

Rząd liczby a modulo n może być mniejszy od $\varphi(n)$. Na przykład

$$\varphi(7) = 6$$

oraz

$$2^3 = 8 \equiv 1 \pmod{7}.$$

Ponieważ

$$2^1 \not\equiv 1 \pmod{7}$$

oraz

$$2^2 \not\equiv 1 \pmod{7},$$

więc $\mathrm{ord}_7 2 = 3 < \varphi(7)$.

PIERWIASTKI PIERWOTNE

Z twierdzenia Lagrange'a wynika natychmiast następujące twierdzenie:

Twierdzenie 18. Jeśli n jest liczbą całkowitą dodatnią oraz $\mathrm{NWD}(a, n) = 1$, to

$$a^m \equiv 1 \pmod{n}$$

wtedy i tylko wtedy, gdy $\quad \mathrm{ord}_n a \mid m$. ♠

Wniosek. $\quad \mathrm{ord}_n a \mid \varphi(n)$. ♠

Wniosek. $\quad a^i \equiv a^j \pmod{n} \quad \Leftrightarrow \quad i \equiv j \pmod{\mathrm{ord}_n a}$. ♠

Definicja. Jeśli $\mathrm{NWD}(r, n) = 1$ oraz $\mathrm{ord}_n r = \varphi(n)$, to liczbę r nazywamy **pierwiastkiem pierwotnym** modulo n.

Przykład. Liczba 3 jest pierwiastkiem pierwotnym modulo 7. Liczba 2 jest pierwiastkiem pierwotnym modulo 9. Nie istnieje natomiast pierwiastek pierwotny modulo 8.

Twierdzenie 19. Jeśli $NWD(r, n) = 1$ oraz r jest pierwiastkiem pierwotnym modulo n, to liczby

$$r \,\mathbf{mod}\, n, \quad r^2 \,\mathbf{mod}\, n, \quad \ldots, \quad r^{\varphi(n)} \,\mathbf{mod}\, n$$

są wszystkimi liczbami względnie pierwszymi z n i mniejszymi od n. ♠

Twierdzenie 20. Jeśli $\mathrm{ord}_m a = t$ oraz $u > 0$, to

$$\mathrm{ord}_m(a^u) = \frac{t}{\mathrm{NWD}(t, u)}. \quad ♠$$

Twierdzenie 21. Jeśli r jest pierwiastkiem pierwotnym modulo m, to r^u jest pierwiastkiem pierwotnym modulo m wtedy i tylko wtedy, gdy

$$\mathrm{NWD}(u, \varphi(m)) = 1. \quad \spadesuit$$

Twierdzenie 22. Jeśli liczba m ma pierwiastek pierwotny, to ma $\varphi(\varphi(m))$ różnych pierwiastków pierwotnych (modulo m).

ISTNIENIE PIERWIASTKÓW PIERWOTNYCH

Najpierw przypomnienie:

Twierdzenie 23. (Lagrange'a) Wielomian stopnia n ma co najwyżej n pierwiastków w ciele $\mathbb{Z}_p$ (uwzględniając krotności pierwiastków).

Wniosek. W ciele $\mathbb{Z}_p$ każdy pierwiastek wielomianu $X^p - X$ jest pierwiastkiem jednokrotnym. $\spadesuit$

Wniosek. Niech $d \mid p-1$. Wtedy w ciele $\mathbb{Z}_p$ wielomian $X^d - 1$ ma dokładnie d pierwiastków. $\spadesuit$

Twierdzenie 24. Jeśli p jest liczbą pierwszą i $d \mid p-1$, to w ciele $\mathbb{Z}_p$ istnieje $\varphi(d)$ różnych elementów rzędu d.

Dowód. Oznaczmy:

$$F(d) = |\{a \in \mathbb{Z}_p : \ \mathrm{ord}_p a = d\}|.$$

Wtedy oczywiście

$$\sum_{d \mid p-1} F(d) = p - 1.$$

Ale także

$$\sum_{d \mid p-1} \varphi(d) = p - 1.$$

Wykażemy, że jeśli $d \mid p-1$, to

$$F(d) \leq \varphi(d).$$

Stąd oczywiście wyniknie, że jeśli $d \mid p-1$, to

$$F(d) = \varphi(d),$$

co zakończy dowód.

Jeśli $F(d) = 0$, to oczywiście $F(d) \leq \varphi(d)$.

jeśli $F(d) \neq 0$, to istnieje $a \in \mathbb{Z}_p$ rzędu d. Wtedy elementy

$$a, \quad a^2, \quad \ldots, \quad a^d$$

są różne i są to wszystkie pierwiastki wielomianu

$$X^d - 1.$$

Z poprzednich twierdzeń wynika, że rząd d mają te potęgi a^k, dla których $\mathrm{NWD}(k, d) = 1$. A takich jest $\varphi(d)$. Stąd $F(d) \leq \varphi(d)$. ♠

Wniosek. Każda liczba pierwsza ma pierwiastek pierwotny. ♠

Twierdzenie 25. Jeśli p jest liczbą pierwszą i r jest pierwiastkiem pierwotnym modulo p, to albo r albo $r + p$ jest pierwiastkiem pierwotnym modulo p^2. ♠

Twierdzenie 26. Jeśli p jest liczbą pierwszą nieparzystą i r jest pierwiastkiem pierwotnym modulo p^2, to r jest pierwiastkiem pierwotnym modulo p^k dla każdej liczby dodatniej k. ♠

Twierdzenie 27. Jeśli a jest liczbą nieparzystą oraz $k \geq 3$, to

$$a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}. \quad ♠$$

Wniosek. Jeśli $k \geq 3$, to nie istnieje pierwiastek pierwotny modulo 2^k. ♠

Twierdzenie 28. Jeśli $k \geq 3$, to

$$\mathrm{ord}_{2^k} 5 = \frac{\varphi(2^k)}{2} = 2^{k-2}. \quad ♠$$

Zatem 5 ma największy możliwy rząd.

Twierdzenie 29. Jedynymi liczbami mającymi pierwiastki pierwotne są liczby postaci:

$$2, \quad 4, \quad p^k, \quad 2p^k,$$

gdzie p jest liczbą pierwszą nieparzystą. ♠

CERTYFIKATY PIERWSZOŚCI

Twierdzenie 30. Niech n będzie liczbą całkowitą dodatnią. Jeśli istnieje liczba całkowita a taka, że

$$a^{n-1} \equiv 1 \pmod{n}$$

oraz

$$a^{(n-1)/d} \not\equiv 1 \pmod{n}$$

dla każdego dzielnika pierwszego d liczby $n-1$, to liczba n jest pierwsza.

Dowód. Ponieważ

$$a^{n-1} \equiv 1 \pmod{n},$$

więc

$$\mathrm{ord}_n a \mid (n-1).$$

Wykażemy, że

$$\mathrm{ord}_n a = n-1.$$

Oznaczmy

$$\mathrm{ord}_n a = m.$$

Niech

$$n-1 = k \cdot \mathrm{ord}_n a = km$$

i przypuśćmy, że $k > 1$.

Niech q będzie dzielnikiem pierwszym liczby k. Wtedy

$$a^{(n-1)/q} = a^{\frac{k}{q}\cdot m} = (a^m)^{\frac{k}{q}} \equiv 1 \pmod{n},$$

co jest sprzeczne z założeniami twierdzenia. Zatem

$$\mathrm{ord}_n a = n-1.$$

Ale wtedy

$$n-1 = \mathrm{ord}_n a \leq \varphi(n) \leq n-1,$$

skąd wynika, że

$$\varphi(n) = n-1,$$

czyli n jest liczbą pierwszą. ♠

Uwagi.

- Jeśli liczba n jest złożona, to do sprawdzenia tego wystarczy $O((\log_2 n)^2)$ działań na bitach.
- (Pratt) Jeśli liczba n jest pierwsza, to do sprawdzenia tego wystarczy $O((\log_2 n)^4)$ działań na bitach.

Nietrudny dowód indukcyjny drugiej uwagi (twierdzenia Pratta) pozostawimy jako ćwiczenie.

Do sporządzenia certyfikatu pierwszości dla liczby n potrzebne są:

(1) rozkład na czynniki liczby $n-1$:

$$n-1=p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k};$$

(2) pierwiastek pierwotny a modulo n (liczba a spełniająca założenia twierdzenia jest pierwiastkiem pierwotnym modulo n);

(3) certyfikaty pierwszości liczb $p_1,\ldots,p_k$.

Twierdzenie Pratta nie mówi nic o tym, w jaki sposób można uzyskać faktoryzację liczby $n-1$, pierwiastek pierwotny modulo n i certyfikaty pierwszości czynników pierwszych liczby $n-1$. Twierdzenie to mówi tylko, że sprawdzenie poprawności tak otrzymanego certyfikatu pierwszości liczby n może być wykonane w czasie wielomianowym (dokładniej $O(m^4)$, gdzie m jest liczbą cyfr liczby n).

Zatem problem weryfikacji pierwszości jest problemem klasy

$$NP\cap\text{co-}NP.$$

PRZYKŁAD CERTYFIKATU PIERWSZOŚCI

W 1867 roku F. Landry dowiódł, że liczba

$$1133836730401$$

jest pierwsza. Ta liczba jest jednym z dzielników liczby $2^{75}+1$:

$$2^{75}+1=3^2\cdot 11\cdot 251\cdot 331\cdot 4051\cdot 1133836730401.$$

Po wykazaniu, że ta liczba jest pierwsza, napisał on:

W tym momencie jesteśmy nieco zakłopotani. Rzeczywiście, jeśli komuś udało się rozłożyć liczbę na czynniki i podał on te czynniki, to każdy może to natychmiast sprawdzić. Inaczej rzecz się ma wtedy, gdy metody użyte do znalezienia dzielnika zawiodły i ta osoba twierdzi, że dana liczba jest **pierwsza**. *W jaki sposób może ona przekazać innym to swoje całkowicie osobiste przekonanie? Kto poczułby się przekonany nie powtarzając wszystkich obliczeń i nie rozumiejąc zasad, na których te obliczenia były oparte?*
Rozumiemy, że nasze stwierdzenie jest tylko hipotezą, prawdopodobną tak długo, aż ktoś nie udowodni twierdzenia przeciwnego lub aż nie ujawnimy naszych metod i w ten sposób nie umożliwimy innym zastosowania ich.

Pokażemy teraz certyfikat pierwszości dla liczby

$$p=1133836730401.$$

Po pierwsze zauważamy, że

$$p-1=1133836730400=2^5\cdot 3\cdot 5^2\cdot 11\cdot 31\cdot 41\cdot 33791.$$

Następnie

$$\begin{aligned}33790 &= 2\cdot 5\cdot 31\cdot 109,\\ 108 &= 2^2\cdot 3^3,\\ 40 &= 2^3\cdot 5,\\ 30 &= 2\cdot 3\cdot 5,\\ 10 &= 2\cdot 5,\\ 4 &= 2^2,\\ 2 &= 2^1.\end{aligned}$$

Wskażemy kolejno certyfikaty pierwszości dla liczb

$$3,5,11,31,41,109,33791,p,$$

wykorzystując do tego znalezione rozkłady na czynniki liczb o 1 mniejszych.

Certyfikat dla liczby 3:

$$\begin{aligned}3-1 &= 2,\\ 2^2 &\equiv 1 \pmod 3,\\ 2^1 &\equiv 2 \pmod 3.\end{aligned}$$

Certyfikat dla liczby 5:

$$\begin{aligned}5-1 &= =4=2^2,\\ 2^4 &\equiv 1 \pmod 5,\\ 2^2 &\equiv 4 \pmod 5.\end{aligned}$$

Certyfikat dla liczby 11:

$$\begin{aligned}11-1 &= 10=2\cdot 5,\\ 2^{10} &\equiv 1 \pmod{11},\\ 2^{10/2} &= 2^5\equiv 10 \pmod{11},\\ 2^{10/5} &= 2^2\equiv 4 \pmod{11}.\end{aligned}$$

Certyfikat dla liczby 31:

$$\begin{aligned}31-1 &= 30=2\cdot 3\cdot 5,\\ 3^{30} &\equiv 1 \pmod{31},\\ 3^{30/2} &= 3^{15}\equiv 30 \pmod{31},\\ 3^{30/3} &= 3^{10}\equiv 25 \pmod{31},\\ 3^{30/5} &= 3^6\equiv 16 \pmod{31}.\end{aligned}$$

Certyfikat dla liczby 41:

$$\begin{aligned}41-1 &= 40=2^3\cdot 5,\\ 6^{40} &\equiv 1 \pmod{41},\\ 6^{40/2} &= 6^{20}\equiv 40 \pmod{41},\\ 6^{40/5} &= 6^8\equiv 10 \pmod{41}.\end{aligned}$$

Certyfikat dla liczby 109:

$$\begin{aligned}
109-1 &= 108 = 2^2\cdot 3^3,\\
6^{108} &\equiv 1 \pmod{109},\\
6^{108/2} &= 6^{54}\equiv 108 \pmod{109},\\
6^{108/3} &= 6^{36}\equiv 63 \pmod{109}.
\end{aligned}$$

Certyfikat dla liczby 33791:

$$\begin{aligned}
33791-1 &= 33790 = 2\cdot 5\cdot 31\cdot 109,\\
7^{33790} &\equiv 1 \pmod{33791},\\
7^{33790/2} &= 7^{16895}\equiv 33790 \pmod{33791},\\
7^{33790/5} &= 7^{6758}\equiv 21152 \pmod{33791},\\
7^{33790/31} &= 7^{1090}\equiv 3746 \pmod{33791},\\
7^{33790/109} &= 7^{310}\equiv 31762 \pmod{33791}.
\end{aligned}$$

Certyfikat dla liczby $p = 1133836730401$:

$$\begin{aligned}
p-1 &= 1133836730400 = 2^3\cdot 3\cdot 5^2\cdot 11\cdot 31\cdot 41\cdot 33791,\\
13^{p-1} &\equiv 1 \pmod{1133836730401},\\
13^{(p-1)/2} &\equiv 1133836730400 \pmod{1133836730401},\\
13^{(p-1)/3} &\equiv 1133803175969 \pmod{1133836730401},\\
13^{(p-1)/5} &\equiv 1073741824 \pmod{1133836730401},\\
13^{(p-1)/11} &\equiv 533573983808 \pmod{1133836730401},\\
13^{(p-1)/31} &\equiv 403182718393 \pmod{1133836730401},\\
13^{(p-1)/41} &\equiv 474305688247 \pmod{1133836730401},\\
13^{(p-1)/33791} &\equiv 202504652001 \pmod{1133836730401}.
\end{aligned}$$

UŁAMKI DZIESIĘTNE

Każda liczba wymierna ma rozwinięcie dziesiętne skończone lub okresowe. Na przykład

$$\begin{aligned}
\tfrac{1}{8} &= 0,125\\
\tfrac{1}{3} &= 0,333333333333\ldots = 0,(3)\\
\tfrac{1}{7} &= 0,142857142857\ldots = 0,(142857)\\
\tfrac{1}{6} &= 0,166666666666\ldots = 0,1(6)
\end{aligned}$$

Proste ćwiczenie:

$$0,(c_1c_2\ldots c_k) = \frac{(c_1c_2\ldots c_k)_{10}}{10^k-1}.$$

Przypuśćmy, że dana jest liczba wymierna r zapisana w postaci ułamka nieskracalnego

$$r = \frac{a}{b},\quad \text{gdzie}\quad \mathrm{NWD}(a,b) = 1.$$

Powstają trzy naturalne pytania:

(1) Czy rozwinięcie dziesiętne jest skończone?

(2) Jeśli rozwinięcie dziesiętne jest nieskończone, to ile cyfr ma okres?

(3) Jeśli rozwinięcie dziesiętne jest nieskończone, to ile cyfr występuje między przecinkiem i pierwszą cyfrą okresu?

Twierdzenie 31. Niech a i b będą liczbami całkowitymi dodatnimi i niech

$$\mathrm{NWD}(a, b) = 1.$$

Wówczas rozwinięcie dziesiętne ułamka $\frac{a}{b}$ jest skończone wtedy i tylko wtedy, gdy rozkład liczby b na czynniki pierwsze ma postać

$$b = 2^k \cdot 5^l.$$

Liczba cyfr po przecinku jest wtedy równa

$$\max\{k, l\}.$$

Jeśli liczba b ma postać

$$b = 2^k \cdot 5^l \cdot m,$$

gdzie

$$\mathrm{NWD}(m, 10) = 1,$$

to ułamek $\frac{a}{b}$ ma rozwinięcie dziesiętne nieskończone takie, że:

(1) długość okresu wynosi $\mathrm{ord}_m 10$;

(2) liczba cyfr między przecinkiem i pierwszą cyfrą okresu jest równa

$$\max\{k, l\}. \quad \spadesuit$$

Nietrudny, ale żmudny dowód tego twierdzenia opuścimy.
Twierdzenie to ma naturalnę uogólnienie na systemy pozycyjne o innych podstawach. Sformułowanie i ewentualne udowodnienie tego uogólnienie pozostawimy jako ćwiczenie.

INDEKSY

Definicja. Załóżmy, że a jest generatorem grupy G rzędu m. Jeśli

$$a^x = b$$

w grupie G, gdzie $0 \leq x < m$, to liczbę x nazywamy **logarytmem dyskretnym** liczby b przy podstawie a w grupie G.

Jeśli grupa G jest grupą multyplikatywną pierścienia $\mathbb{Z}_m$, to logarytm dyskretny nazywamy także **indeksem** liczby b przy podstawie a modulo m.

Logarytm dyskretny będziemy oznaczać zwykłym symbolem logarytmu:

$$x = \log_a b,$$

nie zaznaczając, w jakiej grupie go rozważamy. Na ogół nie będzie to prowadziło do nieporozumień.

Najprostszy algorytm znajdowania logarytmu dyskretnego polega na przeszukiwaniu. Aby obliczyć

$$\log_2 15$$

w ciele $\mathbb{Z}_{19}$ obliczamy kolejno:

x	0	1	2	3	4	5	6	7	8	9	10	11
2^x	1	2	4	8	16	13	7	14	9	18	17	15

Zatem

$$\log_2 15 = 11.$$

ALGORYTM BABY-STEP GIANT-STEP

Jest to rodzaj „trade-off”: czas w zamian za pamięc. Niech m będzie rzędem elementu a w grupie G. Połóżmy $m = \lceil\sqrt{n}\rceil$. Jeśli

$$b = a^x,$$

to istnieją i oraz j takie, że

$$x = im + j \quad \text{oraz} \quad 0 \leq i, j < m.$$

Takie liczby i oraz j są wyznaczone jednoznacznie. Teraz mamy:

$$b = a^{im} \cdot a^j,$$

czyli

$$b \cdot (a^{-m})^i = a^j.$$

To sugeruje następujący algorytm:

Algorytm.

- **Dane:** generator a grupy G rzędu n i element b grupy G;
- **Wynik:** logarytm dyskretny $\log_a b$;

(1) Kładziemy $m = \lceil\sqrt{n}\rceil$;
(2) Tworzymy tablicę par (j, a^j) dla $0 \leq j < m$;
(3) Sortujemy utworzoną tablicę;
(4) Obliczamy a^{-m} i kładziemy $c = b$;
(5) Dla $i = 0, 1, \ldots, m-1$ wykonujemy:
  (5.1) Sprawdzamy, czy c jest następnikiem pary w tablicy;
  (5.2) Jeśli $c = a^j$, to kładziemy $x = im + j$ i kończymy;
  (5.3) Wpp kładziemy $c := c \cdot a^{-m}$.

PRZYKŁAD

Liczba $a = 3$ jest pierwiastkiem pierwotnym modulo $p = 113$. Obliczamy

$$\log_3 57$$

w ciele $\mathbb{Z}_{113}$.

(1) Obliczamy $m = \lceil\sqrt{112}\rceil = 11$.

(2) Tworzymy tablicę par $(j, 3^j \,\mathbf{mod}\, 113)$ dla $0 \leq j \leq 10$:

j	0	1	2	3	4	5	6	7	8	9	10
$3^j \,\mathbf{mod}\, 113$	1	3	9	27	81	17	51	40	7	21	63

(3) Sortujemy tablicę

j	0	1	8	2	5	9	3	7	6	10	4
$3^j \,\mathbf{mod}\, 113$	1	3	7	9	17	21	27	40	51	63	81

(4) Obliczamy $3^{-1} \,\mathbf{mod}\, 113 = 38$ i następnie $3^{-m} \,\mathbf{mod}\, 113 = 58$;

(5) Dla $i = 0, 1, \ldots, m-1$ obliczamy $c = b \cdot a^{-mi}$ i szukamy w tablicy; dla $i = 9$ otrzymamy $c = 3$. Zatem

$$b \cdot 3^{-9m} = 3 = a^1,$$

skąd dostajemy

$$b = a^{100}.$$

Zatem

$$\log_3 57 = 100$$

w ciele $\mathbb{Z}_{113}$.