KONGRUENCJE

Definicja. Niech $m \in \mathbb{Z}$ oraz $m > 0$. Wówczas liczba a **przystaje do** liczby b **modulo** m wtedy i tylko wtedy, gdy $m \mid a - b$.

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \mid a - b.$$

Inaczej: $a \equiv b \pmod{m}$ wtedy i tylko wtedy, gdy liczby a i b dają te same reszty przy dzieleniu przez m.

Przykłady.
(1) $22 \equiv 4 \pmod{9}$,
(2) $3 \equiv -6 \pmod{9}$,
(3) $13 \not\equiv 5 \pmod{9}$.

Twierdzenie 1. $a \equiv b \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z} \;\; a = b + km.$ ♠

Twierdzenie 2. Dla każdej liczby całkowitej dodatniej m relacja kongruencji

$$a \sim b \quad \Leftrightarrow \quad a \equiv b \pmod{m}$$

jest relacją równoważności w zbiorze $\mathbb{Z}$. ♠

Klasy abstrakcji relacji kongruencji nazywamy **klasami reszt** modulo m. **Zupełnym układem reszt** modulo m nazywamy zbiór m liczb całkowitych o tej własności, że każda liczba całkowita przystaje do dokładnie jednej z nich modulo m.

Twierdzenie 3. Załóżmy, że

$$a \equiv b \pmod{m} \;\text{ oraz }\; c \equiv d \pmod{m}.$$

Wtedy
(1) $a + c \equiv b + d \pmod{m}$,
(2) $ac \equiv bd \pmod{m}$.

Dowód. Wystarczy zauważyć, że
(1) $(a + c) - (b + d) = (a - b) + (c - d)$,
(2) $ac - bd = a(c - d) + d(a - b)$. ♠

Wniosek. Jeśli

$$a \equiv b \pmod{m} \;\text{ oraz }\; k \in \mathbb{N},$$

to

$$a^k \equiv b^k \pmod{m}. \quad ♠$$

Definicja. Niech P będzie dowolnym pierścieniem. Wtedy symbolem $P[X]$ oznaczamy pierścień wielomianów jednej zmiennej X.

Wniosek. Jeśli $f(X) \in \mathbb{Z}[X]$ oraz $a \equiv b \pmod{m}$, to

$$f(a) \equiv f(b) \pmod{m}. \quad \spadesuit$$

Wniosek. Jeśli $f(X) \in \mathbb{Z}[X]$ oraz $a, b \in \mathbb{Z}$, to

$$a - b \mid f(a) - f(b). \quad \spadesuit$$

Twierdzenie 4. Jeśli $ac \equiv bc \pmod{m}$ oraz $\mathrm{NWD}(m, c) = d$, to

$$a \equiv b \pmod{\frac{m}{d}}. \quad \spadesuit$$

Wniosek. Jeśli $ac \equiv bc \pmod{m}$ oraz $\mathrm{NWD}(m, c) = 1$, to

$$a \equiv b \pmod{m}. \quad \spadesuit$$

Twierdzenie 5. Jeśli

$$a \equiv b \pmod{m_i} \quad \text{dla} \quad i = 1, 2, \ldots, k,$$

to

$$a \equiv b \pmod{\mathrm{NWW}(m_1, m_2, \ldots, m_k)}. \quad \spadesuit$$

Twierdzenie 6. Jeśli liczby $r_1, r_2, \ldots, r_m$ tworzą zupełny układ reszt modulo m oraz $NWD(a, m) = 1$, to liczby

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

też tworzą zupełny układ reszt modulo m.

Dowód. Wystarczy pokazać, że jeśli

$$ar_i + b \equiv ar_j + b \pmod{m},$$

to $i = j$. Ale jeśli

$$ar_i + b \equiv ar_j + b \pmod{m},$$

to

$$ar_i \equiv ar_j \pmod{m}$$

i stąd $r_i \equiv r_j \pmod{m}$. Zatem $i = j$. $\spadesuit$

PIERŚCIEŃ $\mathbb{Z}_m$

Definicja. Symbolem $\mathbb{Z}_m$ oznaczamy zbiór klas reszt modulo m. W zbiorze $\mathbb{Z}_m$ wprowadzamy działania dodawania i mnożenia wzorami

$$[a] + [b] = [a + b] \ \text{ oraz } \ [a] \cdot [b] = [a \cdot b].$$

Te działania nazywamy działaniami modulo m.

Najczęściej jako reprezentantów klas reszt modulo m wybieramy liczby $0, 1, \ldots, m-1$. Możemy więc powiedzieć, że

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$$

z działaniami dodawania i mnożenia modulo m:

$$a +_m b = (a + b) \,\mathbf{mod}\, m, \quad a \cdot_m b = (ab) \,\mathbf{mod}\, m.$$

Twierdzenie 7. Działania w zbiorze $\mathbb{Z}_m$ są dobrze określone. ♠

Twierdzenie 8. Zbiór $\mathbb{Z}_m$ z działaniami dodawania i mnożenia modulo m jest pierścieniem. ♠

Uwaga dotycząca złożoności działań: działania dodawania i mnożenia modulo m można wykonać w czasie $O(\log^2 m)$. Pamiętajmy, że działania te wykonujemy na liczbach mniejszych od m, a zatem mających co najwyżej tyle cyfr co m.

POTĘGOWANIE MODULO m

Przykład. Obliczamy a^{1239}. Można to zrobić na dwa sposoby:

Sposób 1.

$p := 1;$
powtórz 1239 **razy:**
  $p := p \cdot a;$
podaj wynik p.

W ten sposób wykonamy 1239 mnożeń.

Sposób 2.

$$
\begin{array}{rcllll}
a^1 & = & a & p := a^1 & p = a^1 & 0 \text{ mnożeń} \\
a^2 & = & a^1 \cdot a^1 & p := p \cdot a^2 & p = a^3 & 2 \text{ mnożenia} \\
a^4 & = & a^2 \cdot a^2 & p := p \cdot a^4 & p = a^7 & 2 \text{ mnożenia} \\
a^8 & = & a^4 \cdot a^4 & & p = a^7 & 1 \text{ mnożenie} \\
a^{16} & = & a^8 \cdot a^8 & p := p \cdot a^{16} & p = a^{23} & 2 \text{ mnożenia} \\
a^{32} & = & a^{16} \cdot a^{16} & & p = a^{23} & 1 \text{ mnożenie} \\
a^{64} & = & a^{32} \cdot a^{32} & p := p \cdot a^{64} & p = a^{87} & 2 \text{ mnożenia} \\
a^{128} & = & a^{64} \cdot a^{64} & p := p \cdot a^{128} & p = a^{215} & 2 \text{ mnożenia} \\
a^{256} & = & a^{128} \cdot a^{128} & & p = a^{215} & 1 \text{ mnożenie} \\
a^{512} & = & a^{256} \cdot a^{256} & & p = a^{215} & 1 \text{ mnożenie} \\
a^{1024} & = & a^{512} \cdot a^{512} & p := p \cdot a^{1024} & p = a^{1239} & 2 \text{ mnożenia}
\end{array}
$$

W ten sposób wykonamy 16 mnożeń.

ALGORYTM

Wejście: $a \in \mathbb{Z}_m$, $n \in \mathbb{N}$.

Wyjście: $p = a^n \in \mathbb{Z}_m$.

$p := 1;\ \ b := a;$
while $n > 0$ **do begin**
  if $odd(n)$ **then** $p := bp \,\mathbf{mod}\, m;$
  $b := b^2 \,\mathbf{mod}\, m;$
  $n := n \,\mathbf{div}\, 2$
end

Złożoność tego algorytmu wynosi $O(\log^2 m \log n)$. Zauważmy bowiem, że jeśli wykładnik n ma k cyfr w rozwinięciu dwójkowym

$$n = c_{k-1} \cdot 2^{k-1} + c_{k-2} \cdot 2^{k-2} + \ldots + c_1 \cdot 2 + c_0,$$

to musimy obliczyć potęgi

$$a^2, a^4, a^8, \ldots, a^{2^{k-2}}, a^{2^{k-1}}.$$

Do tego potrzeba $k-1$ mnożeń (dokładniej: podnoszeń do kwadratu). Następnie potrzeba dodatkowego mnożenia zawsze wtedy, gdy $c_i = 1$. Zatem łączna liczba mnożeń jest równa

$$k - 1 + |\{i : \ c_i = 1\}|.$$

Ta liczba jest mniejsza od $2k$.

Uwagi:

(1) Przekonamy się wkrótce, że nie musimy obliczać potęg, których wykładnik jest większy od m. Złożoność tego algorytmu wyniesie zatem $O(\log^3 m)$.

(2) Ten algorytm potęgowania nie jest optymalny. Na przykład obliczenie a^{15} za pomocą tego algorytmu wymaga 6 mnożeń:

(a) $a^2 = a \cdot a$;
(b) $p := a \cdot a^2$; (teraz $p = a^3$)
(c) $a^4 = a^2 \cdot a^2$;
(d) $p := p \cdot a^4$; (teraz $p = a^7$)
(e) $a^8 := a^4 \cdot a^4$;
(f) $p := p \cdot a^8$; (teraz $p = a^{15}$).

Tę potęgę można obliczyć za pomocą 5 mnożeń:

(a) $a^2 = a \cdot a$;
(b) $a^4 = a^2 \cdot a^2$;
(c) $p := a \cdot a^4$; (teraz $p = a^5$)
(d) $p := p \cdot p$; (teraz $p = a^{10}$)
(e) $p := p \cdot a^5$; (teraz $p = a^{15}$).

Ten sposób obliczeń wymaga jednak zapamiętania czasami wielu wyników pośrednich. Problem wyznaczenia minimalnej liczby mnożeń potrzebnych do obliczenia potęgi a^n jest — o ile mi wiadomo — nadal otwarty.

Ten problem jest szeroko przedyskutowany w II tomie Knutha: rozdział 4.6.3

KONGRUENCJE LINIOWE

Twierdzenie 9. Kongruencja liniowa

$$ax \equiv c \pmod{m}$$

z niewiadomą x ma rozwiązanie wtedy i tylko wtedy, gdy

$$\mathrm{NWD}(a, m) \mid c.$$

Dowód. Kongruencja liniowa

$$ax \equiv c \pmod{m}$$

jest równoważna równaniu liniowemu

$$ax + my = c. \quad \spadesuit$$

Wniosek. Kongruencja liniowa

$$ax \equiv 1 \pmod{m}$$

ma rozwiązanie wtedy i tylko wtedy, gdy liczba a jest względnie pierwsza z m. ♠

Twierdzenie 10. Jeśli $\mathrm{NWD}(a, m) = d$ i $d \mid c$, to kongruencja liniowa

$$ax \equiv c \pmod{m}$$

ma dokładnie d rozwiązań nieprzystających do siebie modulo m.

Dowód. Wszystkimi rozwiązaniami tej kongruencji są liczby

$$x = x_0 + \frac{m}{d}n,$$

gdzie x_0 jest jakimkolwiek rozwiązaniem kongruencji i $n \in \mathbb{Z}$. Wystarczy zauważyć, że dla $n = 0, 1, \ldots, d-1$ otrzymane rozwiązania nie przystają do siebie modulo m. ♠

ELEMENTY ODWROTNE MODULO m

Definicja. Rozwiązanie kongruencji liniowej

$$ax \equiv 1 \pmod{m}$$

nazywamy **elementem odwrotnym** do a modulo m.

Twierdzenie 11. Liczba a ma element odwrotny modulo m wtedy i tylko wtedy, gdy jest względnie pierwsza z m. Jeśli element odwrotny istnieje, to jest wyznaczony jednoznacznie z dokładnością do przystawania modulo m. ♠

Twierdzenie 12. Jeśli liczba p jest pierwsza, to w pierścieniu $\mathbb{Z}_p$ każda licczba różna od zera ma element odwrotny. ♠

Wniosek. Pierścień $\mathbb{Z}_p$ jest ciałem. ♠

Twierdzenie 13. Niech p będzie liczbą pierwszą. Wówczas element a ciała $\mathbb{Z}_p$ jest odwrotny do siebie wtedy i tylko wtedy, gdy $a = 1$ lub $a = -1$.

Dowód. Implikacja „w lewo" jest oczywista.

Przypuśćmy, że element a jest odwrotny do siebie, tzn.

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

Wtedy

$$p \mid a^2 - 1,$$

czyli

$$p \mid (a-1)(a+1).$$

Zatem

$$a \equiv 1 \pmod{p} \text{ lub } a \equiv -1 \pmod{p}. \quad \spadesuit$$

TURNIEJE

Mamy n zawodników o numerach $1, 2, \ldots, n$. Zakładamy, że $2 \mid n$. Rozgrywają oni turniej systemem „każdy z każdym”. Wskażemy, kto z kim ma grać w kolejnych rundach.

Rundy numerujemy liczbami od 1 do $n-1$. Wtedy

(1) Niech $i \neq j$ oraz $i, j < n$. Jeśli

$$i + j \equiv k \pmod{n-1},$$

gdzie $1 \leq k \leq n-1$, to zawodnicy o numerach i oraz j grają ze sobą w rundzie k.

(2) Niech $i < n$. Jeśli

$$2i \equiv k \pmod{n-1},$$

gdzie $1 \leq k \leq n-1$, to zawodnicy o numerach i oraz n grają ze sobą w rundzie k.

Ćwiczenie. Każdy gra z każdym dokładnie jeden raz.

Przykład. Tabelka turnieju dla 6 zawodników:

	1	2	3	4	5	6
1	$\star$	3	4	5	1	2
2	3	$\star$	5	1	2	4
3	4	5	$\star$	2	3	1
4	5	1	2	$\star$	4	3
5	1	2	3	4	$\star$	5
6	2	4	1	3	5	$\star$

CHIŃSKIE TWIERDZENIE O RESZTACH

Twierdzenie 14. Dane są liczby $m_1, m_2, \ldots, m_r$ parami względnie pierwsze:

$$i \neq j \quad \Rightarrow \quad \mathrm{NWD}(m_i, m_j) = 1.$$

Niech $M = m_1 m_2 \cdot \ldots \cdot m_r$ oraz $a_1, a_2, \ldots, a_r \in \mathbb{Z}$. Wtedy układ kongruencji

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

ma rozwiązanie modulo M. Każde dwa rozwiązania przystają do siebie modulo M.

Dowód. Niech

$$M_i = m_1 \cdot \ldots \cdot m_{i-1} \cdot m_{i+1} \cdot \ldots \cdot m_r = M \,\mathbf{div}\, m_i.$$

Wtedy $\mathrm{NWD}(m_i, M_i) = 1$. Zatem istnieje y_i taki, że

$$M_i y_i \equiv 1 \pmod{m_i}.$$

Rozwiązanie układu dane jest wzorem

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r.$$

Jeśli x_1 i x_2 są rozwiązaniami, to $x_1 \equiv x_2 \pmod{m_i}$ dla każdego $i = 1, 2, \ldots, r$, skąd

$$x_1 \equiv x_2 \pmod{M}. \quad \spadesuit$$

ARYTMETYKA DUŻYCH LICZB

Wybieramy liczby $m_1, m_2, \ldots, m_r$ parami względnie pierwsze. Liczbę x reprezentujemy w postaci ciągu

$$(x \,\mathbf{mod}\, m_1, x \,\mathbf{mod}\, m_2, \ldots, x \,\mathbf{mod}\, m_r).$$

To przyporządkowanie zachowuje działania.

Przykład. Niech

$$m_1 = 95, \quad m_2 = 97, \quad m_3 = 98, \quad m_4 = 99.$$

Wtedy

$$M = 89403930.$$

Niech

$$x = 123684, \quad y = 413456.$$

Mamy zatem

$$x \rightarrow (89, 9, 8, 33)$$

oraz

$$y \rightarrow (16, 42, 92, 32).$$

Dodajemy „po współrzędnych”:

$$x + y \rightarrow (10, 51, 2, 65).$$

Z chińskiego twierdzenia o resztach wynika, że

$$x + y \equiv 537140 \pmod{89403930}.$$

Zatem

$$x + y = 537140.$$

DUŻE LICZBY PARAMI WZGLĘDNIE PIERWSZE

Twierdzenie 15. Jeśli $a \,\mathbf{mod}\, b = r$, to

$$(2^a - 1) \,\mathbf{mod}\, (2^b - 1) = 2^r - 1. \quad \spadesuit$$

Twierdzenie 16. Jeśli $\mathrm{NWD}(a, b) = d$, to

$$\mathrm{NWD}(2^a - 1, 2^b - 1) = 2^d - 1.$$

Twierdzenie 17.

$$\mathrm{NWD}(a, b) = 1 \quad \Leftrightarrow \quad \mathrm{NWD}(2^a - 1, 2^b - 1) = 1. \quad \spadesuit$$

Przykład. Liczby $31, 33, 34, 35$ są parami względnie pierwsze. Zatem liczby

$$2^{31} - 1, \quad 2^{33} - 1, \quad 2^{34} - 1, \quad 2^{35} - 1 \quad \spadesuit$$

też są parami względnie pierwsze.

SECRETS SHARING

Zadanie. Dany jest klucz K pozwalający odtworzyć hasło (do skarbca, systemu komputerowego, systemu kryptograficznego itp.). Mamy przydzielić r osobom częściowe informacje o kluczu K w taki sposób, by:

(1) każde s osób (gdzie $0 < s < r$) mogło zrekonstruować klucz K;

(2) żadna grupa licząca mniej niż s osób nie mogła zrekonstruować klucza K.

Taki system nazywamy (s, r)-**treshold scheme**.

Konstrukcja.

Wybieramy liczbę pierwszą $p > K$ oraz liczby

$$m_1, m_2, \ldots, m_r$$

takie, że:

(1) $i \neq j \quad \Rightarrow \quad \mathrm{NWD}(m_i, m_j) = 1$;

(2) $p \not| m_i$;

(3) $m_1 < m_2 < \ldots < m_r$;

(4) $m_1 m_2 \cdot \ldots \cdot m_s > p m_r m_{r-1} \cdot \ldots \cdot m_{r-s+2}$.

Warunek (4) mówi, że iloczyn s najmniejszych liczb m_i jest większy niż iloczyn p oraz $s-1$ największych liczb m_i.

Niech $M = m_1 m_2 \cdot \ldots \cdot m_s$. Wtedy liczba $\frac{M}{p}$ jest większa od iloczynu dowolnych $s-1$ liczb spośród $m_1, m_2, \ldots, m_r$.

Niech $0 \leq t < \lfloor \frac{M}{p} \rfloor$ – wybrana losowo. Kładziemy

$$K_0 = K + tp.$$

Wtedy

$$0 \leq K_0 = K + tp < p + tp = (t+1)p \leq \frac{M}{p} \cdot p = M.$$

Następnie definiujemy

$$k_i = K_0 \,\mathbf{mod}\, m_i$$

dla $i = 1, 2, \ldots, r$.

Wreszcie osoba o numerze i dostaje liczbę k_i.

Fakt 1. Każde s osób może zrekonstruować klucz K.

Przypuśćmy, że znamy $k_{i_1}, k_{i_2}, \ldots, k_{i_s}$. Niech

$$M_0 = m_{i_1} m_{i_2} \cdot \ldots \cdot m_{i_s}.$$

Korzystając z chińskiego twierdzenia o resztach obliczamy

$$K_0 \,\mathbf{mod}\, M_0.$$

Ale $0 \leq K_0 < M \leq M_0$, więc obliczyliśmy K_0. Stąd otrzymujemy

$$K = K_0 - tp.$$

Fakt 2. Mniej niż s osób nie może zrekonstruować klucza K.

Przypuśćmy, że znamy $k_{i_1}, k_{i_2}, \ldots, k_{i_{s-1}}$. Niech

$$M_1 = m_{i_1} m_{i_2} \cdot \ldots \cdot m_{i_{s-1}}.$$

Z chińskiego twierdzenia o resztach otrzymujemy

$$a = K_0 \,\mathbf{mod}\, M_1.$$

Zatem wiemy, że

$$K_0 = a + xM_1,$$

gdzie

$$0 \leq x < \frac{M}{M_1}.$$

Ale z warunku (4) wynika, że

$$\frac{M}{M_1} > p,$$

więc x przebiega wszystkie reszty modulo p. Ponieważ

$$\mathrm{NWD}(M_1, p) = 1,$$

więc $a + xM_1$ też przebiega wszystkie reszty modulo p.

Zatem K_0 może być w dowolnej klasie reszt modulo p. To znaczy, że mniej niż s liczb k_i nie wyznacza K_0, a więc i K.

RESZTY KWADRATOWE

Definicja. Niech
$$m \in \mathbb{Z} \quad \text{oraz} \quad m > 0.$$
Niech
$$a \in \mathbb{Z} \quad \text{oraz} \quad \mathrm{NWD}(a, m) = 1.$$
Liczbę a nazywamy **resztą kwadratową** modulo m jeśli istnieje liczba x taka, że
$$x^2 \equiv a \pmod{m}.$$
W przeciwnym przypadku liczbę a nazywamy **nieresztą kwadratową** modulo m.

Przykład. Wyznaczymy reszty kwadratowe modulo 11. Obliczamy
$$\begin{array}{rcrcl} 1^2 \,\mathbf{mod}\, 11 & = & 10^2 \,\mathbf{mod}\, 11 & = & 1, \\ 2^2 \,\mathbf{mod}\, 11 & = & 9^2 \,\mathbf{mod}\, 11 & = & 4, \\ 3^2 \,\mathbf{mod}\, 11 & = & 8^2 \,\mathbf{mod}\, 11 & = & 9, \\ 4^2 \,\mathbf{mod}\, 11 & = & 7^2 \,\mathbf{mod}\, 11 & = & 5, \\ 5^2 \,\mathbf{mod}\, 11 & = & 6^2 \,\mathbf{mod}\, 11 & = & 3. \end{array}$$
Zatem resztami kwadratowymi modulo 11 są liczby
$$1, \quad 3, \quad 4, \quad 5, \quad \text{oraz} \quad 9.$$
Nieresztami kwadratowymi modulo 11 są liczby
$$2, \quad 6, \quad 7, \quad 8, \quad \text{oraz} \quad 10.$$
Widzimy, że jest tyle samo reszt co niereszt. Okazuje się, że jest tak zawsze wtedy, gdy liczba m jest pierwsza.

Twierdzenie 18. Załóżmy, że p jest nieparzystą liczbą pierwszą oraz liczba a nie dzieli się przez p. Wtedy kongruencja
$$x^2 \equiv a \pmod{p}$$
albo ma dokładnie dwa rozwiązania modulo p, albo nie ma ani jednego rozwiązania modulo p.

Dowód. Przypuśćmy, że ta kongruencja ma co najmniej jedno rozwiązanie x_0:
$$x_0^2 \equiv a \pmod{p}.$$
Wtedy oczywiście $-x_0$ też jest rozwiązaniem tej kongruencji:
$$(-x_0)^2 = x_0^2 \equiv a \pmod{p}.$$

Ponadto

$$x_0 \not\equiv -x_0 \pmod{p}.$$

Gdyby bowiem

$$x_0 \equiv -x_0 \pmod{p},$$

to

$$p \mid 2x_0.$$

To jednak jest niemożliwe, gdyż liczba p jest nieparzysta oraz liczba x_0 nie dzieli się przez p.

Innych rozwiązań nie ma: przypuśćmy bowiem, że

$$x_1^2 \equiv a \pmod{p}.$$

Wtedy

$$x_1^2 \equiv x_0^2 \pmod{p}.$$

Zatem

$$p \mid x_1^2 - x_0^2,$$

czyli

$$p \mid (x_1 - x_0)(x_1 + x_0).$$

Zatem

$$p \mid x_1 - x_0 \ \text{ lub } \ p \mid x_1 + x_0.$$

Stąd wynika, że

$$x_1 \equiv x_0 \pmod{p} \ \text{ lub } \ x_1 \equiv -x_0 \pmod{p}.$$

Zatem istnieją dokładnie dwa rozwiązania modulo p; są nimi liczby x_0 i $-x_0$. ♠

Wniosek. Jeśli p jest nieparzystą liczbą pierwszą, to istnieje dokładnie $(p-1)$ **div** 2 reszt kwadratowych modulo p i tyle samo niereszt kwadratowych modulo p.

SYMBOL LEGENDRE'A

Definicja. Niech p będzie nieparzystą liczbą pierwszą i niech a będzie liczbą całkowitą niepodzielną przez p. Definiujemy **symbol Legendre'a** $\left(\frac{a}{p}\right)$ w następujący sposób.:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{jeśli } a \text{ jest resztą kwadratową modulo } p, \\ -1 & \text{jeśli } a \text{ jest nieresztą kwadratową modulo } p. \end{cases}$$

Przykład.

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$$

oraz

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1.$$

Twierdzenie 19. (Kryterium Eulera) Niech p będzie nieparzystą liczbą pierwszą i niech a będzie dodatnią liczbą całkowitą niepodzielną przez p. Wtedy

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

Przykład. Niech $p = 23$ oraz $a = 5$. Wtedy

$$5^{11} \equiv -1 \pmod{23},$$

więc

$$\left(\frac{5}{23}\right) = -1.$$

Zatem liczba 5 jest nieresztą kwadratową modulo 23.

Kryterium Eulera pozwala w pewnych przypadkach rozwiązać kongruencję

$$x^2 \equiv a \pmod p.$$

Przypuśćmy zatem, że

$$p \equiv 3 \pmod 4$$

oraz

$$\left(\frac{a}{p}\right) = 1.$$

Niech

$$x = a^{\frac{p+1}{4}} \,\mathbf{mod}\, p.$$

Pokażemy, że x jest rozwiązaniem naszej kongruencji. Mianowicie

$$x^2 \equiv a^{\frac{p+1}{2}} \pmod p.$$

Z kryterium Eulera wynika, że

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

Zatem

$$a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \equiv a \pmod p,$$

skąd wynika, że

$$x^2 \equiv a \pmod p.$$

Oczywiście drugim rozwiązaniem jest $-x$.

Niech

$$n = pq,$$

gdzie p i q są różnymi liczbami pierwszymi nieparzystymi. Załóżmy, że x_0 jest rozwiązaniem kongruencji

$$x^2 \equiv a \pmod{n}.$$

Wtedy ta kongruencja ma dokładnie cztery rozwiązania modulo n.

Niech

$$x_1 = x_0 \mathbin{\mathbf{mod}} p$$

oraz

$$x_2 = x_0 \mathbin{\mathbf{mod}} q.$$

Wtedy kongruencja

$$x^2 \equiv a \pmod{p}$$

ma dokładnie dwa rozwiązania

$$x = x_1 \quad \text{oraz} \quad x = -x_1.$$

Podobnie kongruencja

$$x^2 \equiv a \pmod{q}$$

ma dokładnie dwa rozwiązania

$$x = x_2 \quad \text{oraz} \quad x = -x_2.$$

Oczywiście x_0 jest rozwiązaniem układu kongruencji

$$\begin{cases} x \equiv x_1 \pmod{p} \\ x \equiv x_2 \pmod{q} \end{cases}$$

Niech y_0 będzie rozwiązaniem układu

$$\begin{cases} x \equiv -x_1 \pmod{p} \\ x \equiv x_2 \pmod{q} \end{cases}$$

Wtedy $-x_0$ jest rozwiązaniem układu

$$\begin{cases} x \equiv -x_1 \pmod{p} \\ x \equiv -x_2 \pmod{q} \end{cases}$$

oraz $-y_0$ jest rozwiązaniem układu

$$\begin{cases} x \equiv x_1 \pmod{p} \\ x \equiv -x_2 \pmod{q} \end{cases}$$

Liczby

$$x_0, \quad -x_0, \quad y_0 \text{ oraz } -y_0$$

są wszystkimi rozwiązaniami kongruencji

$$x^2 \equiv a \pmod{n}.$$

Przykład. Rozwiążmy kongruencję

$$x^2 \equiv 860 \pmod{11021}.$$

Zauważmy, że

$$11021 = 103 \cdot 107.$$

Następnie

$$860 \,\mathbf{mod}\, 103 = 36$$

oraz

$$860 \,\mathbf{mod}\, 107 = 4.$$

Rozwiązujemy kongruencję

$$x^2 \equiv 860 \equiv 36 \pmod{103}.$$

Otrzymujemy dwa rozwiązania:

$$x_1 = 6 \ \text{ oraz } \ -x_1 = -6.$$

Rozwiązujemy kongruencję

$$x^2 \equiv 860 \equiv 4 \pmod{107}.$$

Otrzymujemy rozwiązania

$$x_2 = 2 \ \text{ oraz } \ -x_2 = -2.$$

Teraz rozwiązujemy cztery układy kongruencji:

$$\begin{cases} x \equiv 6 \pmod{103} \\ x \equiv 2 \pmod{107}, \end{cases} \qquad \text{otrzymując } x_0 = 109; \tag{1}$$

$$\begin{cases} x \equiv -6 \pmod{103} \\ x \equiv 2 \pmod{107}, \end{cases} \qquad \text{otrzymując } y_0 = -212; \tag{2}$$

$$\begin{cases} x \equiv -6 \pmod{103} \\ x \equiv -2 \pmod{107} \end{cases} \qquad \text{otrzymując } -x_0 = -109; \tag{3}$$

$$\begin{cases} x \equiv 6 \pmod{103} \\ x \equiv -2 \pmod{107}, \end{cases} \qquad \text{otrzymując } -y_0 = 212. \tag{4}$$

Zatem rozwiązaniami kongruencji

$$x^2 \equiv 860 \pmod{11021}$$

są liczby

$$109, \quad -109, \quad 212 \ \text{ oraz } \ -212.$$

WŁASNOŚCI SYMBOLU LEGENDRE'A

Twierdzenie 20. Niech p będzie nieparzystą liczbą pierwszą. Niech a i b będą liczbami całkowitymi niepodzielnymi przez p. Wtedy

(1) jeśli $a \equiv b \pmod{p}$, to $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;

(3) $\left(\frac{a^2}{p}\right) = 1$. ♠

Twierdzenie 21. Niech p będzie nieparzystą liczbą pierwszą. Wtedy

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{jeśli } p \equiv 1 \pmod{4}, \\ -1 & \text{jeśli } p \equiv 3 \pmod{4}. \end{cases} \qquad \spadesuit$$

Twierdzenie 22. Niech p będzie nieparzystą liczbą pierwszą. Wtedy

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

Zatem, jeśli $p \equiv \pm 1 \pmod{8}$, to

$$\left(\frac{2}{p}\right) = 1$$

oraz jeśli $p \equiv \pm 3 \pmod{8}$, to

$$\left(\frac{2}{p}\right) = -1. \qquad \spadesuit$$

Przykłady.

(1) Ponieważ

$$317 \equiv 9 \pmod{11},$$

więc

$$\left(\frac{317}{11}\right) = \left(\frac{9}{11}\right) = \left(\frac{3^2}{11}\right) = 1.$$

(2) Ponieważ

$$89 \equiv -2 \pmod{13},$$

więc

$$\left(\frac{89}{13}\right) = \left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right) \cdot \left(\frac{2}{13}\right).$$

Następnie mamy $13 \equiv 1 \pmod{4}$ oraz $13 \equiv -3 \pmod{8}$. Zatem

$$\left(\frac{-1}{13}\right) = 1 \quad \text{oraz} \quad \left(\frac{2}{13}\right) = -1.$$

Stąd

$$\left(\frac{89}{13}\right) = 1 \cdot (-1) = -1.$$

PRAWO WZAJEMNOŚCI

Twierdzenie 23. (Prawo wzajemności dla reszt kwadratowych) Niech p i q będą nieparzystymi liczbami pierwszymi. Wtedy

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

Zatem, jeśli

$$p\equiv 1 \pmod 4 \ \text{ lub } \ q\equiv 1 \pmod 4,$$

to

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$$

oraz jeśli

$$p\equiv q\equiv 3 \pmod 4,$$

to

$$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right). \quad \spadesuit$$

Przykłady.

(1) Niech $p=13$ i $q=17$. Wtedy

$$p\equiv q\equiv 1 \pmod 4.$$

Zatem

$$\left(\frac{13}{17}\right)=\left(\frac{17}{13}\right)=\left(\frac{4}{13}\right)=\left(\frac{2^2}{13}\right)=1.$$

(2) Niech $p=7$ i $q=19$. Wtedy

$$p\equiv q\equiv 3 \pmod 4.$$

Zatem

$$\left(\frac{7}{19}\right)=-\left(\frac{19}{7}\right)=-\left(\frac{5}{7}\right).$$

Teraz

$$5\equiv 1 \pmod 4 \ \text{ oraz } \ 7\equiv 3 \pmod 4.$$

Zatem

$$\left(\frac{7}{19}\right)=-\left(\frac{5}{7}\right)=-\left(\frac{7}{5}\right)=-\left(\frac{2}{5}\right).$$

Ale

$$5\equiv -3 \pmod 8,$$

więc

$$\left(\frac{7}{19}\right)=-(-1)=1.$$

(3) Obliczymy $\left(\frac{713}{1009}\right)$. (Zauważmy, że liczba 1009 jest pierwsza). Mamy $713 = 23 \cdot 31$. Zatem

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right) \cdot \left(\frac{31}{1009}\right).$$

Teraz korzystamy z prawa wzajemności dla reszt kwadratowych. Ponieważ

$$1009 \equiv 1 \pmod 4,$$

więc

$$\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) \quad \text{oraz} \quad \left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right).$$

Teraz

$$\left(\frac{20}{23}\right) = \left(\frac{4 \cdot 5}{23}\right) = \left(\frac{5}{23}\right)$$

i jeszcze dwa razy korzystamy z prawa wzajemności dla reszt kwadratowych:

$$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Stąd

$$\left(\frac{23}{1009}\right) = -1.$$

Podobnie

$$\left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right) \cdot \left(\frac{7}{17}\right).$$

Teraz

$$\left(\frac{2}{17}\right) = 1$$

oraz

$$\left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Zatem

$$\left(\frac{31}{1009}\right) = -1.$$

Stąd ostatecznie dostajemy

$$\left(\frac{713}{1009}\right) = (-1) \cdot (-1) = 1.$$

SYMBOL JACOBIEGO

Definicja. Niech n będzie liczbą całkowitą nieparzystą oraz niech

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Niech a będzie liczbą całkowitą względnie pierwszą z n. Wtedy definiujemy **symbol Jacobiego** $\left(\frac{a}{n}\right)$ wzorem

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \left(\frac{a}{p_2}\right)^{\alpha_2} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{\alpha_k},$$

gdzie czynniki występujące po prawej stronie są symbolami Legendre'a.

Przykłady.

(1)

$$\left(\frac{2}{45}\right) = \left(\frac{2}{3^2 \cdot 5}\right) = \left(\frac{2}{3}\right)^2 \cdot \left(\frac{2}{5}\right) = (-1)^2 \cdot (-1) = -1.$$

(2)

$$\left(\frac{109}{385}\right) = \left(\frac{109}{5 \cdot 7 \cdot 11}\right) = \left(\frac{109}{5}\right) \cdot \left(\frac{109}{7}\right) \cdot \left(\frac{109}{11}\right).$$

Ponieważ

$$\left(\frac{109}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1, \qquad \left(\frac{109}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1$$

oraz

$$\left(\frac{109}{11}\right) = \left(\frac{10}{11}\right) = \left(\frac{-1}{11}\right) = -1,$$

więc

$$\left(\frac{109}{385}\right) = 1 \cdot 1 \cdot (-1) = -1.$$

Uwagi.

(1) Jeśli liczba n jest pierwsza, to symbol Jacobiego $\left(\frac{a}{n}\right)$ jest po prostu symbolem Legendre'a. W szczególności

$$\left(\frac{a}{n}\right) = 1$$

wtedy i tylko wtedy, gdy a jest resztą kwadratową modulo n.

(2) Jeśli liczba n jest złożona oraz kongruencja

$$x^2 \equiv a \pmod{n}$$

ma rozwiązanie, to

$$\left(\frac{a}{n}\right) = 1.$$

(3) Istnieje liczba złożona n taka, że kongruencja

$$x^2 \equiv a \pmod{n}$$

nie ma rozwiązania, ale

$$\left(\frac{a}{n}\right) = 1.$$

Na przykład, niech $n = 15$ oraz $a = 2$. Wtedy

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1,$$

ale kongruencja

$$x^2 \equiv 2 \pmod{15}$$

nie ma rozwiązania, bo liczba 2 jest nieresztą kwadratową modulo 3 i modulo 5.

WŁASNOŚCI SYMBOLU JACOBIEGO

Twierdzenie 24. Niech n będzie liczbą całkowitą nieparzystą. Niech $\mathrm{NWD}(a,n) = \mathrm{NWD}(b,n) = 1$. Wtedy

(1) jeśli $a \equiv b \pmod{n}$, to $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$;

(2) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$;

(3) $\left(\frac{a^2}{n}\right) = 1$;

(4) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$;

(5) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ ♠.

Twierdzenie 25. (Prawo wzajemności dla symbolu Jacobiego) Niech m i n będą liczbami całkowitymi nieparzystymi i niech $\mathrm{NWD}(m,n) = 1$. Wtedy

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}. \quad ♠$$

Przykład. Niech $a = 401$ i $b = 111$. Wtedy

$$\begin{aligned} 401 &= 111 \cdot 3 + 2^2 \cdot 17, \\ 111 &= 17 \cdot 6 + 2^0 \cdot 9, \\ 17 &= 9 \cdot 1 + 2^3 \cdot 1. \end{aligned}$$

Zatem (zauważmy, że 401 jest liczbą pierwszą):

$$\left(\frac{111}{401}\right) = \left(\frac{401}{111}\right) = \left(\frac{17}{111}\right) = \left(\frac{111}{17}\right) = \left(\frac{9}{17}\right) = \left(\frac{17}{9}\right) = \left(\frac{2}{9}\right) = 1.$$

Algorytm obliczania symbolu Jacobiego przypomina algorytm Euklidesa. Zauważmy, że symbole Legendre'a obliczamy traktując je jako symbole Jacobiego.

LICZBY PSEUDOPIERWSZE EULERA

Przypomnijmy: jeśli liczba n jest pierwsza oraz $\mathrm{NWD}(a, n) = 1$, to

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

Niech $n = 341$. Wtedy $n = 11 \cdot 31$. Niech $a = 2$. Wtedy

$$\left(\frac{2}{341}\right) = -1 \quad \text{oraz} \quad 2^{170} \equiv 1 \pmod{341}.$$

Zatem

$$\left(\frac{2}{341}\right) \not\equiv 2^{170} \pmod{341}.$$

Definicja. Liczbę nieparzystą n nazywamy **liczbą pseudopierwszą Eulera** przy podstawie a, jeśli jest liczbą złożoną oraz

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

Twierdzenie 26. Jeśli n jest liczbą złożoną nieparzystą, to istnieje co najmniej jedna liczba a taka, że $\mathrm{NWD}(a, n) = 1$ oraz

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod{n}. \quad \spadesuit$$

TEST SOLOVAYA - STRASSENA

Twierdzenie 27. Niech n będzie liczbą złożoną nieparzystą. Wtedy liczba takich a, że

(1) $1 \leq a < n$,
(2) $\mathrm{NWD}(a, n) = 1$,
(3) $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$

jest mniejsza od n **div** 2. $\spadesuit$

Test. Niech n będzie liczbą nieparzystą.

(1) Wybierzmy losowo k liczb $a_1, a_2, \ldots, a_k$ dodatnich mniejszych od n.
(2) Jeśli $\mathrm{NWD}(a_i, n) > 1$ dla co najmniej jednego i, to liczba n jest złożona.
(3) Jeśli $\mathrm{NWD}(a_i, n) = 1$ dla każdego i oraz
   (3.1) jeśli $\left(\frac{a_i}{n}\right) \not\equiv a_i^{\frac{n-1}{2}} \pmod{n}$ dla co najmniej jednego i, to liczba n jest złożona.
   (3.2) jeśli $\left(\frac{a_i}{n}\right) \equiv a_i^{\frac{n-1}{2}} \pmod{n}$ dla każdego i, to nie wiemy, czy liczba n jest złożona. Prawdopodobieństwo tego, że liczba n jest złożona, jest mniejsze od 2^{-k}.