1. Arytmetyka modularna

Niech $n \in \mathbb{N}$. Liczba $a \in \mathbb{Z}$ *przystaje modulo* n do liczby $b \in \mathbb{Z}$ ($a \equiv_n b$) wtedy i tylko wtedy, gdy $n|(a-b)$.

Uwaga 1. *Niech $a, b, c, d \in \mathbb{Z}$. Wtedy*

- $a \equiv_n b \ \wedge \ c \equiv_n d \ \Rightarrow \ a \pm c \equiv_n b \pm d$
- $a \equiv_n b \ \wedge \ c \equiv_n d \ \Rightarrow \ a \cdot c \equiv_n b \cdot d$
- $a \equiv_n b \ \Rightarrow \ \forall k \in \mathbb{N} \quad a^k \equiv_n b^k$

Relację równoważności $\equiv_n \subseteq \mathbb{Z} \times \mathbb{Z}$ nazywamy *kongruencją*.

Twierdzenie 2 (Wilsona)**.** *Liczba naturalna $p > 1$ jest pierwsza wtedy i tylko wtedy, gdy*

$$(p-1)! + 1 \equiv_p 0.$$

Twierdzenie 3 (Twierdzenie Eulera)**.** *Niech $a, n \in \mathbb{N}$ oraz $NWD(a, n) = 1$. Wtedy*

$$a^{\varphi(n)} \equiv_n 1.$$

Wniosek 4 (Małe Twierdzenie Fermata)**.** *Jeżeli p jest liczbą pierwszą oraz $a \in \mathbb{Z}$ jest liczbą niepodzielną przez p, to*

$$a^{p-1} \equiv_p 1.$$

Twierdzenie 5. *Niech $n \in \mathbb{N}$ i $a, b \in \mathbb{Z}$. Równanie*

$$ax + ny = b \quad \Leftrightarrow \quad ax \equiv_n b \tag{1}$$

ma rozwiązanie $x, y \in \mathbb{Z}$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, n)|b$.

Jeśli istnieje rozwiązanie równania (1)*, to istnieje* $\mathrm{NWD}(a, n)$ *rozwiązań $x \in \{0, 1, \ldots, n-1\}$.*

Twierdzenie 6 (Chińskie Twierdzenie o resztach)**.** *Niech $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$, gdzie $NWD(m_i, m_j) = 1$, gdy $i \neq j$, $a_1, \ldots, a_r \in \mathbb{Z}$. Wtedy układ kongruencji*

$$\begin{aligned} x &\equiv_{m_1} a_1 \\ x &\equiv_{m_2} a_2 \\ &\vdots \\ x &\equiv_{m_r} a_r \end{aligned}$$

ma zawsze rozwiązanie całkowite.

Ponadto, jeśli b jest rozwiązaniem układu kongruencji, to każde inne rozwiązanie z spełnia warunek $z \equiv_m b$.

Algorytm szybkiego potęgowania modularnego.
Niech $m \in \mathbb{N}$. Dla obliczenia $r \equiv_n a^m$ przedstawiamy liczbę m w postaci dwójkowej:

$$m = \sum_{i=0}^{k} e_i 2^i, \quad \text{gdzie } e_i \in \{0, 1\}.$$

Wtedy

$$a^m = a^{\sum_{i=0}^{k} e_i 2^i} = \prod_{i=0}^{k} (a^{2^i})^{e_i} = \prod_{0 \leq i \leq k,\ e_i = 1} a^{2^i}.$$

Aby otrzymać $r \equiv_n a^m$:

- obliczamy kolejne kwadraty $r_i \equiv_n a^{2^i}$, dla $0 \leq i \leq k$;
- obliczamy $r \equiv_n a^m$, mnożąc r_i, dla których $e_i = 1$.

Zadania

1. Niech $a = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0$, gdzie $a_i \in \{0, \ldots, 9\}$, dla $i = 0, 1, \ldots, n$. Pokazać, że
   (a) $3|a$ wtedy i tylko wtedy, gdy $a_n + a_{n-1} + \ldots + a_1 + a_0 \equiv_3 0$,
   (b) $11|a$ wtedy i tylko wtedy, gdy $(a_1 + a_3 + \ldots) - (a_0 + a_2 + \ldots) \equiv_{11} 0$.
2. Korzystając z własności kongruencji, pokazać, że dla każdej liczby naturalnej n:
   (a) $31|2^{5n} - 1$,
   (b) $13|4^{2n+1} + 3^{n+2}$.

3. Obliczyć resztę z dzielenia:
   (a) liczby 59^{45} przez 13,
   (b) liczby 731^{512} przez 56.
4. Wykazać, że
   (a) $61! + 1 \equiv_{71} 0$,
   (b) $(36!)^2 \equiv_{73} -1$.
5. Niech $1 < m \in \mathbb{N}$, $a \in \mathbb{Z}$, $\mathrm{NWD}(a, m) = 1$ oraz $n \equiv_{\varphi(m)} k$. Pokazać, że
$$a^n \equiv_m a^k.$$
6. Obliczyć:
   (a) ostatnią cyfrę liczby $2^{1000000}$ w systemie o podstawie 7,
   (b) $2^{1000000}$ modulo 77.
7. Znaleźć rozwiązania równania:
   (a) $20x \equiv_{28} 16$,
   (b) $15x \equiv_{24} 9$.
8. Rozwiązać układ kongruencji:
$$x \equiv_{41} 36$$
$$x \equiv_{17} 5$$
9. Znaleźć najmniejszą liczbę całkowitą dodatnią, która daje resztę 4 przy dzieleniu przez 5, resztę 3 przy dzieleniu przez 7 i resztę 1 przy dzieleniu przez 9.
10. Korzystając z Chińskiego Twierdzenia o resztach obliczyć 2^{5423} modulo 5005.
11. Korzystając z algorytmu szybkiego potęgowania obliczyć:
   (a) 6^{73} modulo 100,
   (b) 3^{100} modulo 17.
12. Jak obliczyć a^{1000} za pomoca 14 mnożeń przy założeniu, że w pamięci mamy tylko a i ostatni wynik pośredni?
    Jak zmniejszyć liczbę tych mnożeń, gdy pamiętamy wszystkie wyniki pośrednie?