Potegowania modulo

Wprowadzenie do potegowania modulo

- Potegowanie modulo to operacja polegajaca na podnoszeniu liczby do określonej potegi, a nastepnie obliczaniu reszty z dzielenia wyniku przez określona liczbe.
- Wyrażenie: $A \mod m = a$ oznacza, że reszta z dzielenia A przez m wynosi a.

Notacja modulo

- $A \mod m = a$
- $B \mod m = b$
- $AB \mod m = ?$

Notacja modulo

- $A \mod m = a$
- $B \mod m = b$
- $AB \mod m = ?$

$$
\begin{aligned}
A &= A_1 \cdot m + a \\
B &= B_1 \cdot m + b \\
AB &= (A_1 \cdot m + a)(B_1 \cdot m + b) \\
AB &= m(mA_1B_1 + A_1b + B_1a) + ab \\
AB \mod m &= ab \mod m
\end{aligned}
$$

Metoda 1: Iteracyjne mnożenie i obliczanie modulo

$$(g^a \mod p) =?$$

$$(\mathrm{g} \cdot g \cdot g \ldots \cdot g) \mod p =$$
$$(\ldots((\mathrm{g} \mod p) \cdot g) \mod p) \cdot g) \ldots \cdot g) \mod p)$$

Metoda 2: Potegowanie szybkie za pomoca rozkładu dwójkowego

$$(g \cdot g \cdot g \ldots \cdot g) \mod p =$$

$$(g^{n_1} \mod p) \cdot (g^{n_2} \mod p) \cdot \ldots \cdot (g^{n_m} \mod p) \mod p)$$

Przykład: Obliczmy $4^5 \mod 10$

- Kroki:

$$4^5 = 4^1 \cdot 4^4$$

$$4^1 \mod 10 = 4$$

$$4^2 \mod 10 = (4 \cdot 4) \mod 10 = 6$$

$$4^4 \mod 10 = (6 \cdot 6) \mod 10 = 6$$

$$4^5 \mod 10 = (4^1 \cdot 4^4) \mod 10 = (4 \cdot 6) \mod 10 = 4$$

Zadanie 1

Napisz funkcje, która oblicza potegowanie modulo przez iteracyjne mnożenie i obliczanie modulo na każdym kroku.

Zadanie 2

Napisz funkcje, która oblicza potegowanie modulo z użyciem szybkiej metody potegowania (rozkładu dwójkowego).

Przykłady do przetestowania

- $123^{456} \mod 789 = 699$
- $19^{1} \mod 23 = 19$
- $256^{40} \mod 100 = 76$
- $4321^{5678} \mod 9876 = 8941$