Algorytm podnoszenia do potęgi modulo n.

Chcemy obliczyć $a^b \pmod n$.

1. Zapisujemy liczbę b w systemie przy podstawie 2. Niech $b = (b_k b_{k-1} \dots b_1 b_0)_2$.
2. Przyjmujemy $m = 1$. Wykonujemy następujące obliczenia:

$$t_0 = a, \quad m = \begin{cases} m \cdot t_0 \pmod n & \text{jeżeli } b_0 = 1 \\ m & \text{jeżeli } b_0 = 0 \end{cases}$$

$$t_1 = t_0^2 \pmod n, \quad m = \begin{cases} m \cdot t_1 \pmod n & \text{jeżeli } b_1 = 1 \\ m & \text{jeżeli } b_1 = 0 \end{cases}$$

$$\vdots$$

$$t_k = t_{k-1}^2 \pmod n, \quad m = \begin{cases} m \cdot t_k \pmod n & \text{jeżeli } b_k = 1 \\ m & \text{jeżeli } b_k = 0 \end{cases}$$

3. $a^b \pmod n = m$.

Przykład. Niech $a = 110$, $b = 101$, $n = 221$. Wtedy $b = (1100101)_2$, $m = 1$

$$\begin{aligned} t_0 &= 110, & m &= 1 \cdot 110 \equiv 110 \pmod{221} \\ t_1 &= 110^2 \equiv 166 \pmod{221}, & m &= 110 \\ t_2 &= 166^2 \equiv 152 \pmod{221}, & m &= 110 \cdot 152 \equiv 145 \pmod{221} \\ t_3 &= 152^2 \equiv 120 \pmod{221}, & m &= 145 \\ t_4 &= 120^2 \equiv 35 \pmod{221}, & m &= 145 \\ t_5 &= 35^2 \equiv 120 \pmod{221}, & m &= 145 \cdot 120 \equiv 162 \pmod{221} \\ t_6 &= 120^2 \equiv 35 \pmod{221}, & m &= 162 \cdot 35 \equiv 145 \pmod{221} \end{aligned}$$

stąd $a^b \equiv 145 \pmod{221}$.

Zadanie A Oblicz $2^{1000000} \pmod{238}$.