Powers and modulus

https://open.kattis.com/problems/powers

Soluzione

$$\sum_{i=1}^{a} i^b \mod a = \begin{cases} 0 & a \text{ dispari} \vee \\ & a \equiv_4 0 \wedge b \neq 1 \\ a/2 & \text{altrimenti} \end{cases}$$

Dimostrazione

$$\sum_{i=1}^{a} i^b = 1^b + 2^b + \ldots + m^b + \ldots + (a-2)^b + (a-1)^b + a^b$$

Si analizzino gli elementi che compongono la serie di potenze.

- L'elemento finale a^b non influenzerà il risultato della sommatoria $\pmod{a}$ in quanto multiplo di a.

$$a^b \equiv 0 \pmod{a}$$

- $\forall i \in [1, \lceil a/2 \rceil - 1],$ gli elementi i^b e $(a-i)^b$ si elidono a vicenda in modulo a.

$$\begin{aligned} & i^b + (a-i)^b \equiv_a \\ & \equiv_a i^b + (a-i) \cdot (a-i)^{b-1} \equiv_a \\ & \equiv_a i^b + a \cdot (a-i)^{b-1} - i \cdot (a-i)^{b-1} \equiv_a \\ & \equiv_a i^b - i \cdot (a-i)^{b-1} \equiv_a \\ & \equiv_a i^b - i \cdot (a-i) \cdot (a-i)^{b-2} \equiv_a \\ & \equiv_a i^b - i \cdot (a \cdot (a-i)^{b-2} - i \cdot (a-i)^{b-2}) \equiv_a \\ & \equiv_a i^b - i \cdot a \cdot (a-i)^{b-2} + i^2 \cdot (a-i)^{b-2} \equiv_a \\ & \equiv_a i^b + i^2 \cdot (a-i)^{b-2} \equiv_a \\ & \equiv_a \ \ldots \end{aligned}$$

Si notino tre espressioni particolari della serie di congruenze sopra:

$$i^b + (a-i)^b \equiv i^b - i \cdot (a-i)^{b-1} \equiv i^b + i^2 \cdot (a-i)^{b-2} \pmod{a}$$

Da esse si può dedurre che $\forall\, k \in [0, b]$, espressioni nella forma seguente sono congruenti a quella iniziale:

$$i^b + (a-i)^b \equiv_a \begin{cases} i^b + i^k \cdot (a-i)^{b-k} & k \text{ pari} \\ i^b - i^k \cdot (a-i)^{b-k} & k \text{ dispari} \end{cases}$$

$$k = b \text{ dispari} \Rightarrow i^b - i^b \cdot (a-i)^{b-b} \equiv 0 \pmod{a}$$

- Sia m il valore centrale della serie, a^b escluso:

$$m = \begin{cases} 0 & a \text{ dispari} \\ a/2 & a \text{ pari} \end{cases}$$

Si analizzi il valore di $m^b \mod a$ nel caso in cui a sia pari.

$$a \text{ pari} \;\Rightarrow\; \exists\, c \mid a = 2c$$

- $b = 1 \quad \Rightarrow \quad \left(\dfrac{a}{2}\right)^b = \dfrac{a}{2} = c \equiv_a c$
- $b \neq 1 \quad \Rightarrow \quad \left(\dfrac{a}{2}\right)^b = c^b = c \cdot c^{b-1}$

$$c \cdot k = \begin{cases} c \cdot 2h = a \cdot h \equiv_a 0 & k \text{ pari } \wedge\; k = 2h \\ c \cdot (k-1+1) = c \cdot (2h+1) = a \cdot h + c \equiv_a c & k \text{ dispari } \wedge\; (k-1) = 2h \end{cases}$$

  - c pari $\quad \Rightarrow \quad c^{b-1}$ pari $\wedge\; a \equiv_4 0 \quad \Rightarrow \quad c \cdot c^{b-1} \equiv_a 0$
  - c dispari $\quad \Rightarrow \quad c^{b-1}$ dispari $\quad \Rightarrow \quad c \cdot c^{b-1} \equiv_a c$

Ciò dimostra che $m^b \mod a$ può assumere due valori distinti, che dipendono da a e da b.

$$m^b \bmod a \;=\; \begin{cases} 0 & a \text{ dispari } \vee \\ & a \equiv_4 0 \;\wedge\; b \neq 1 \\ a/2 & \text{altrimenti} \end{cases}$$

In conclusione, la sommatoria delle potenze può essere riscritta come segue:

$$\sum_{i=1}^{a} i^b \;\equiv\; a^b + \sum_{i=1}^{\lceil a/2 \rceil - 1} \left(i^b + (a-i)^b\right) + m^b \;\equiv\; 0 + 0 + m^b \pmod a$$

$$\sum_{i=1}^{a} i^b \bmod a \;=\; m^b \bmod a \;=\; \begin{cases} 0 & a \text{ dispari } \vee \\ & a \equiv_4 0 \;\wedge\; b \neq 1 \\ a/2 & \text{altrimenti} \end{cases}$$