Bardo, październik 2019

IV UNIWERSYTECKI OBÓZ OLIMPIADY MATEMATYCZNEJ

Teoria Liczb - Twierdzenia i definicje

Definicja 3. funkcje liczbowe. Dla $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ definiujemy następujące funkcje:

$\tau(n) = (\alpha_1 - 1)(\alpha_2 - 1)...(\alpha_k - 1)$ liczba dzielników n

$\sigma(n) = \left(\frac{p_1^{\alpha_1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{\alpha_2} - 1}{p_2 - 1}\right)...\left(\frac{p_k^{\alpha_k} - 1}{p_k - 1}\right)$ suma dzielników n

$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)$ tocjent Eulera, liczba liczb względnie pierwszych z n mniejszych od n

Twierdzenie 4. (multiplikatywność). Dla $n \perp m$ zachodzi

$$\tau(n \cdot m) = \tau(n) \cdot \tau(m) \qquad \sigma(n \cdot m) = \sigma(n) \cdot \sigma(m) \qquad \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

Fakt 6. Dla liczby pierwszej p, $k \geqslant 0$ i $a \perp p$

$$a^{p^k(p-1)} \equiv 1 \ (mod\ p^{k+1})$$

Twierdzenie 5. (Tw. Eulera). Dla $a \perp n$ zachodzi

$$a^{\varphi(n)} \equiv 1 \ (mod\ n)$$

Twierdzenie 6. (Chińskie tw. o resztach). Niech liczby $n_1, n_2, ..., n_k$ będą niezerowymi, parami względnie pierwszymi liczbami całkowitymi, a liczby $a_1, a_2, ..., a_k$ będą dowolnymi liczbami całkowitymi. wtedy układ kongruencji

$$\begin{cases} x \equiv a_1 \ (mod\ m_1) \\ x \equiv a_2 \ (mod\ m_2) \\ \quad \vdots \\ x \equiv a_k \ (mod\ m_k) \end{cases}$$

ma dokładnie jedno rozwiązanie $1 \leqslant x \leqslant m_1 \cdot m_2 \cdot m_3 \cdot ...m_k$

Twierdzenie 7. Ciągu a_n reszt modulo c zadany zależnością rekurencyjną $a_{n+k} = f(a_n, a_{n+1}, a_{n+2}, ..., a_{n+k})$ jest cykliczny.

Na przykład ciąg reszt kolejnych potęg dwójki modulo 5 jest zadany zależnością $a_{n+1} = (2 \cdot a_n)\ mod\ 2$. kolejne wartości tego ciągu to $1, 2, 4, 3, 1, 2, 4, 3, 1, ...$

Definicja 4. reszty i nieresty. Resztami kwadratowymi modulo n nazywamy takie liczby $x \in \mathbb{Z}_n$, że istnieje $y \in \mathbb{Z}$, że

$$y^2 \equiv x \ (mod\ n)$$

Liczby ze zbioru $\mathbb{Z}_n$ nie będące resztami kwadratowymi nazywamy nieresztami kwadratowymi modulo n.

Analogicznie definiujemy reszty i nieresty sześcienne i stopnia k.

Materiały przygotował: Adam Morawski.