Powtórzenie przed II etapem - Teoria Liczb

Filip Manijak

12.01.2025

Lista tematów które będziemy przerabiać

- Wykładniki P-adyczne
- Modulo
- Chińskie Twierdzenie o Resztach
- Twierdzenia: Fermata, Eulera, Wilsona
- Rzędy
- Generatory

Wykładniki P-adyczne

Zauważmy, że każdą liczbę całkowitą dodatnią n możemy przedstawić jako:

$$n = {p_1}^{a_1} {p_2}^{a_2} \dots {p_k}^{a_k}$$

gdzie p_1, p_2, $\dots$ p_k są pierwsze, a a_1, a_2, $\dots$ a_k całkowite dodatnie.

Definicja 1 Wykładnik p-adyczny

Dla liczby pierwszej p wykładnikiem p-adycznym z liczby n nazywamy największą liczbę całkowitą i taką, że $p^i \mid n$ oraz $p^{i+1} \nmid n$. Zapisujemy $V_p(n) = i$.

Fakt 1 V_p

$$V_3(9) = 2, V_5(15) = 1, V_7(24) = 0, V_{p_1}(n) = a_1$$

Własności Vp

1. jeśli $V_p(a) \neq V_p(b)$, to $V_p(a+b) = MIN(V_p(a), V_p(b))$
2. jeśli wyraz minimalny ciągu $a_1 \ldots a_k$ nie potwarza się więcej niż raz, to $V_p(a_1 + \ldots + a_k) = MIN(V_p(a_1) \ldots V_p(a_k))$
3. jeśli $V_p(a) = V_p(b)$, to $V_p(a+b) \geqslant V_p(a)$
4. $V_p(ab) = V_p(a) + V_p(b)$
5. $V_p(\frac{a}{b}) = V_p(a) - V_p(b)$ dla $b \mid a$
6. $V_p(a^n) = nV_p(a)$
7. $a \mid b \iff \forall_p V_p(a) \leqslant V_p(b)$
8. $a \nmid b \iff \exists_p V_p(a) > V_p(b)$

Zadania Vp

Zadanie 1 Przykład Vp

Liczby $a, b \neq 0$ oraz $\frac{a^2}{b} + \frac{b^2}{a}$ są całkowite. Udowodnij, że $\frac{b^2}{a}$ jest liczbą całkowitą.

Zadanie 2 Przykład Vp

Liczby $a, b \neq 0$ są całkowite i spełniają $ab \mid a^2 + b^2 + a$. Udowodnij, że a jest kwadratem liczby całkowitej.

Wzór Legendre'a i LTE

Twierdzenie 1 Wzór Legendre'a

$$V_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \ldots + \lfloor \frac{n}{p^k} \rfloor$$

Twierdzenie 2 Lemat o zwiększaniu wykładnika p-adycznego

$V_p(x^n - y^n) = V_p(x - y) + V_p(n)$ Dla $p \neq 2$
$V_p(x^n - y^n) = V_p(x-y) + V_p(n) + V_p(x+y) - 1$ Dla $p = 2$

Zadanie 3 Zadanie z LTE

Niech n będzie bezkwadratową, nieparzystą liczbą naturalną. Udowodnij, że nie ma takich liczby $x \perp y$, które spełniają:

$$(x+y)^3 \mid x^n + y^n$$

MIKO

Modulo

Definicja 2 Modulo

$a \equiv b \bmod m \iff a$ daje tę samą resztę z dzielenia przez m co b (innymi słowy, $m \mid a - b$).

Fakt 2 Działania

$$a \equiv c \bmod m \land b \equiv d \bmod m \implies a + b \equiv c + d \bmod m$$
$$a \equiv c \bmod m \land b \equiv d \bmod m \implies a - b \equiv c - d \bmod m$$
$$a \equiv c \bmod m \land b \equiv d \bmod m \implies a \cdot b \equiv c \cdot d \bmod m$$

Fakt 3 Dzielenie działa tylko dla liczb pierwszych

$$ca \equiv cb \bmod p \implies a \equiv b \bmod p \lor c \equiv 0 \bmod p$$

Chińskie twierdzenie o resztach

Twierdzenie 3 CRT

Jeśli liczby $n_1, n_2, \ldots, n_k$ są względnie pierwsze, to z dokładnością do reszty z dzielenia przez $n_1 n_2, \ldots, n_k$ istnieje dokładnie jedno rozwiązanie układu kongruencji $(x < n_1 n_2 \ldots n_k)$:

$x \equiv r_1 \mod n_1$

$x \equiv r_2 \mod n_2$

...

$x \equiv r_k \mod n_k$

Zadanie 4 CRT

Czy dla każdej liczby n istnieje n kolejnych liczb naturalnych, z których żadna nie jest potęgą liczby pierwszej?

MTF i tw. Eulera

Twierdzenie 4 Małe Twierdzenie Fermata

$a^p \equiv a \mod p$; jeśli $p \nmid a$, to dodatkowo $a^{p-1} \equiv 1 \mod p$

Twierdzenie 5 Eulera

Jeśli $n \perp a$, to zachodzi $a^{\phi(n)} \equiv 1 \mod n$, gdzie $\phi(n)$ to liczba liczb względnie pierwszych z n mniejszych od n.

Fakt 4 własności funkcji Eulera

Jeśli $m \perp n$ to $\phi(mn) = \phi(m) * \phi(n)$
$\phi(p^k) = p^{k-1} \cdot (p-1)$

MIKO

Zadania - MTF

Zadanie 5 MTF

Znajdź wszystkie liczby k takie, że dla każdego n naturalnego $NWD(k, 2^n + 3^n + 6^n - 1) = 1$.

Zadanie 6 Euler

Znajdź resztę modulo 16 liczby $\underbrace{3^{3^{3^{\cdots}}}}_{\text{n razy}}$

Tw. Wilsona

Twierdzenie 6 Wilson

$p \mid (p-1)! + 1 \iff p$ jest liczbą pierwszą lub $p = 1$

Zadanie 7 Wilson

$p = 2q + 1$. Udowodnij, że $p \mid (q!)^2 + (-1)^q$.

Generatory

Definicja 3 Generator

Generatorem modulo n nazywamy taką liczbę g, że $g^k \equiv_n g^l \iff k \equiv_{\phi(n)} l$. Równoważnie: każda reszta z dzielenia modulo n względnie pierwsza z n jest postaci g^i dla pewnego i.

Fakt 5 Istnienie

Dla każdej liczby pierwszej istnieje generator (zazwyczaj więcej niż jeden!). Generator modulo n istnieje też dla:

$$n = 1, 2, 4, p^k, 2p^k$$

gdzie p jest liczbą pierwszą większą od 2.

Generatory - zadania

Zadanie 8 $4k + 1$

Udowodnij, że każdą liczbę pierwszą postaci $4k + 1$ da się zapisać jako sumę dwóch kwadratów liczb naturalnych.

Zadanie 9

Dana jest nieparzysta liczba pierwsza p oraz liczba całkowita k taka, że $p - 1 \perp k$. Wykazać

$$1^k + 2^k + \cdots + (p-1)^k \equiv_p 0$$

Bonus: Udowodnić dla $p - 1$ niedzielącego k.

Rzędy

Definicja 4 Rząd

Rzędem liczby całkowitej a modulo m (gdzie $a \perp m$) nazwiemy taką najmniejszą liczbę naturalną ($ord_m(a)$), że:

$$a^{ord_m(a)} \equiv_m 1$$

Fakt 6 Podzielności

1. $m \mid a^k - 1 \iff ord_m(a) \mid k$
2. $ord_m(a) \mid \phi(m)$
3. $m \mid n \implies ord_m(a) \mid ord_n(a)$

Rzędy cd.

Fakt 7 Więcej faktów

1. $a^x \equiv_m a^y \iff x \equiv_{ord_m(a)} y$
2. $ord_m(a^k) = \frac{ord_m(a)}{NWD(k, ord_m(a))}$
3. $ord_m(a) \perp ord_m(b) \implies ord_m(ab) = ord_m(a)ord_m(b)$

Rzędy - zadania

Zadanie 10

Znajdź wszystkie liczby naturalne n takie, że $n \mid 2^n - 1$.

Zadanie 11

Udowodnij, że jeśli $l \mid a^{2^n} + 1$ to $l = k2^{n+1} + 1$.