Autor: Daniela Spurtacz
Prowadzący: Daniela Spurtacz

Rzędy i generatory

Wstęp teoretyczny

Definicja 1 Dla $a \perp n$ rząd liczby a modulo n (oznaczany $ord_n(a)$) to najmniejsza taka liczba dodatnia, że $a^{ord_n(a)} \equiv 1 \mod n$.

Lemat 1 $a^k \equiv 1 \mod n \iff ord_n(a) \mid k$

Definicja 2 Generator (inaczej: pierwiastek pierwotny) modulo n to taka liczba g, że $ord_n(g) = \varphi(n)$.

Lemat 2 Jeśli g jest generatorem modulo n, to zbiór $\{g, g^2, g^3, \ldots, g^{\varphi(n)}\}$ jest permutacją zbioru liczb względnie pierwszych z n modulo n.

Twierdzenie 3 Generator modulo n istnieje wtedy i tylko wtedy, gdy $n = 1$, $n = 2$, $n = 4$, $n = p^k$ lub $n = 2p^k$ dla p nieparzystego, pierwszego.

Fakciki

1. $ord_n(a) \mid \varphi(n)$
2. $ord_n(a^k) = \frac{ord_n(a)}{NWD(k, ord_{n(a)})}$
3. $ord_n(a) \perp ord_n(b) \Rightarrow ord_n(ab) = ord_n(a) ord_n(b)$

Zadania

1. Wyznacz wszystkie liczby dodatnie n takie, że $n \mid 2^n - 1$.
2. *Udowodnij, że jeśli $g \in \mathbb{N}$ jest generatorem modulo $n \in \mathbb{N}$ oraz $2 \nmid gn$, to g jest generatorem modulo $2n$.
3. Udowodnij, że dla liczby pierwszej p oraz k niepodzielnego przez $p-1$ zachodzi:
$$1^k + 2^k + 3^k + \cdots + (p-1)^k \equiv 0 \mod p$$
4. Udowodnij, że jeśli $p \mid 2^{2^n} + 1$ dla p pierwszego i n naturalnego to $p \equiv 1 \mod 2^{n+1}$.
5. *Załóżmy, że modulo $n \in \mathbb{N}$ istnieje liczba rzędu d. Ile jest wtedy reszt rzędu d modulo n?
6. Udowodnij, że istnieje takie naturalne n, że $n^2 \equiv -1 \mod p$ wtedy i tylko wtedy gdy p daje resztę 1 modulo 4 lub gdy $p = 2$.
7. Udowodnij, że $n \mid \varphi(a^n - 1)$ dla $a \perp n$ gdzie $n < a$ są liczbami naturalnymi.
8. Dana jest liczba pierwsza p. Znajdź wszystkie funkcje $f : \mathbb{Z} \to \mathbb{Z}$ takie że dla każdej pary całkowitych m, n zachodzą:
   - $m \equiv n \mod p \Rightarrow f(m) = f(n)$
   - $f(mn) = f(m)f(n)$
9. Znajdź wszystkie pary (p, n) liczby pierwszej p i liczby naturalnej n, że
$$p^n + 1 \mid n^p + 1$$
10. Udowodnij, że jeśli $n \mid 5^n - 2^n$ dla n naturalnego, to $3 \mid n$.
11. Dana jest liczba całkowita $n > 2$. Udowodnij, że największy dzielnik pierwszy liczby $2^{2^n} + 1$ jest większy niż $2^{n+2}(n+1)$.

Autor: Daniela Spurtacz

Prowadzący: Daniela Spurtacz

Szkice rozwiązań

1. Weźmy min $p \mid n$. $2^n \equiv 1 \equiv 2^{p-1} \Rightarrow p \mid 2^{NWD(n,p-1)} - 1 = 2^1 - 1$ sprzeczność
2. $4\varphi(2n) = \varphi(n)$ bo można parować $n-2k-1 \perp n$ z $2n-2k-1 \perp 2n$. Potem $g^r \equiv_{2n} 1 \Rightarrow_n 1 \Rightarrow r \geq \varphi(n) = \varphi(2n)$
3. Istnieje generator g i
$$\sum_1^{p-1} i^k = \sum_0^{p-2} \left(g^k\right)^i = \frac{g^{k(p-1)}}{g^k - 1}$$
Góra przystaje do 0 z MTF a dół nie, bo $p-1 \nmid k$.
4. $ord_p(2) \mid 2^{n+1}$ ale nie dzieli 2^n, więc $2^{n-1} = ord_p(2) \mid p-1$
5. a, a_2, $\ldots$, a^d to wszystkie rozwiązania $X^d \equiv 1$, ale tylko $\varphi(n)$ z nich ma rząd d (patrz fakt 2)
6. Jeśli $4 \nmid p-1$ to gdyby $-1 \equiv n^2 \equiv g^{2k}$ to $p-1 \mid 4k \Rightarrow p-1 \mid 2k$, czyli $1 \equiv g^{2k}$ sprzeczność Jeśli $4 \mid p-1$ to $n = g^{\frac{p-1}{4}}$
7. $ord_{a^n-1}(a) = a$ bo mniejsze potęgi są za małe, więc podzielność zachodzi
8. $f(0) = f(0)^2$, teraz jeśli $f(0) = 1$ to $1 = f(0 \cdot n) = 1 \cdot f(n)$ dla każdego n. W drugim przypadku $f(0) = 0$. Wtedy niech g jest generatorem $f(g)$ jednoznacznie wyznacza całe f. $f(g) = f(g^p) = f(g)^p$, czyli $f = 0$ jest rozwiązaniem, oraz $f(a) = 1$ dla $p \nmid a$ też jest rozwiązaniem. Ostatnim rozwiązaniem jest $f(a) = 1$ dla reszt kwadratowych i $f(a) = -1$ dla niereszt kwadratowych.
9. Sprawdzić ręcznie $p = 2$. Dla $p > 2$, n jest nieparzyste, czyli $p+1 \mid p^n + 1 \mid n^p + 1$. $NWD(n, p+1) = 1$, więc weźmy $r = ord_{p+1}(n)$. $r \mid 2p$ ale $r \nmid p$, oraz $r \leq \varphi(p+1) \leq p$ więc $r = 2$. Zatem $p+1 \mid n+1$. $p = n$ działa, ale $n > p$ już nie, bo $p^n + 1$ będzie za duże.
10. Niech p to będzie najmniejszy dzielnik pierwszy n. Oczywiście p nie jest równe 2 ani 5, więc $ord_p(\frac{5}{2}) \mid p-1 \Rightarrow ord_p\left(\frac{5}{2}\right) < p$. W dodatku $p \mid 5^n - 2^n$ więc
$$\left(\frac{5}{2}\right)^n \equiv 1 \mod p$$
Czyli $ord_p\left(\frac{5}{2}\right) \mid n$, czyli n ma mniejszy dzielnik niż p, czyli musi on być równy 1, to znaczy $ord_p\left(\frac{5}{2}\right) = 1$, czyli $5 \equiv 2 \mod p$ czyli $p = 3$, więc rzeczywiście $3 \mid n$.
11. Dowolne $p \mid 2^{2^n} + 1$ ma $ord_p(2) \mid 2^{n+1}$ ale nie dzieli 2^n więc jest równe 2^{n+1} czyli $2^{n+1} \mid p-1$.
$$2^{2^n} + 1 = \prod_{i=1}^{m} (k_i 2^{n+1} + 1) > 2^{m(n+1)} + 1$$
Więc $2^n > m(n+1)$.
$$1 \equiv 2^{2^n} + 1 \equiv 2^{2n+2} \cdot \text{coś} + 2^{n+1} \sum_{i=1}^{m} k_i + 1 \equiv 2^{n+1} \sum_{i=1}^{m} k_i + 1 \mod 2^{2n+2}$$
$$2^{2n+2} \leq 2^{n+1} \sum_{i=1}^{m} k_i$$
Jeśli każde $k_i \leq 2(n+1)$
$$2^{n+1} \leq \sum_{i=1}^{m} k_i \leq m \cdot 2(n+1) = 2m(n+1) < 2 \cdot 2^n = 2^{n+1}$$
sprzeczność. Zatem pewne $k_i > 2(n+1)$ wtedy $p_i = k_i 2^{n+1} + > 2(n+1)2^{n+1} + 1$.