Rzędy i Generatory

Artur Wojtuszkiewicz

Warsztaty Matematyczne 2022

1 Teoria

1.1 Rzędy

Def. 1 *Dla $a \perp m$, rząd a modulo m ($ord_m(a)$) to najmniejsza taka liczba całkowita dodatnia n, że $a^n \equiv 1 \mod m$.*

Twierdzenie 1 *$a^k \equiv 1 \mod m$ wtedy i tylko wtedy gdy $ord_m(a) \mid k$.*

Z tego twierdzenie wynikają następujące fakciki (najprzydatniejsze są fakciki 1, 2, 3):

1. $ord_m(a) \mid \varphi(m)$
2. $a^x \equiv a^y \mod m \iff x \equiv y \mod ord_m(a)$
3. $t \mid m \implies ord_t(a) \mid ord_m(a)$
4. $ord_m(a^k) = \frac{ord_m(a)}{NWD(k, ord_m(a))}$
5. $ord_m(a) \perp ord_m(b) \implies ord_m(ab) = ord_m(a) \cdot ord_m(b)$
6. $x \perp y \implies ord_{xy}(a) = NWW(ord_x(a), ord_y(a))$

Przykład 1 *Udowodnij że dla liczby pierwszej p, każdy dzielnik $2^p - 1$, inny od 1, jest większy od p.*

Rozwiązanie: Wystarczy udowodnić że każdy jej dzielnik pierwszy q jest większy niż p. $ord_{2^p-1}(2) = p$ oraz $ord_q(2) \mid ord_{2^p-1}(2)$. $ord_q(2) \neq 1$ ponieważ wtedy $2 \equiv 1 \mod q$. Pozostaje $ord_q(2) = p$, czyli $p = ord_q(2) \leq \varphi(q) < q$.

1.2 Generatory

Def. 2 *Generatorem (pierwiastkiem pierwotnym) modulo m nazywamy g takie, że $ord_m(g) = \varphi(m)$*

Nazwę "generator" wyjaśnia *fakcik 2*: biorąc potęgi generatora, od g^1 do $g^{\varphi(m)}$, modulo m, każdy $x \perp m$ zostaje "wygenerowany" dokładnie raz. W szczególności dla m pierwszego, są to wszystkie elementy oprócz 0.

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

Przykład 2 *Udowodnij że jeśli m jest potęgą nieparzystej liczby pierwszej p, to iloczyn liczb niepodzielnych przez p mniejszych od m, przystaje do -1 modulo m.*

Rozwiązanie: Elementy będące nawzajem swoimi odwrotnościami tworzą pary. Iloczyn elementów w każdej parze to 1, więc szukany iloczyn jest równy iloczynowi wszystkich elementów będących własną odwrotnością, czyli liczb spełniających $x^2 \equiv 1 \mod m$. m jest potęgą nieparzystej liczby pierwszej, więc istnieje generator g modulo m. Podstawiając $x = g^y$, otrzymujemy $g^{2y} \equiv 1 \mod m$, czyli $\varphi(m) \mid 2y$. Wynika z tego, że jedynymi takimi elementami są $g^0 \equiv 1 \mod m$ i $g^{\frac{\varphi(m)}{2}} \equiv -1 \mod m$.

2 Zadania

1. Wyznacz wszystkie liczby dodatnie n, takie że $n \mid 2^n - 1$.

2. Udowodnij, że dla liczby pierwszej p oraz k niepodzielnego przez $p-1$, zachodzi:
$$1^k + 2^k + \ldots + (p-1)^k \equiv 0 \mod p$$

3. Udowodnij, że każdy nieparzysty dzielnik pierwszy $a^{2^n} + 1$ jest postaci $k \cdot 2^{n+1} + 1$.

4. Udowodnij, że jeśli istnieje generator modulo m, to elementów rzędu x jest $\varphi(x)$.

5. (Kryterium Eulera) Udowodnij, że dla nieparzystej liczby pierwszej p oraz a niepodzielnego przez p, równanie $x^2 \equiv a \mod p$ ma rozwiązanie wtedy i tylko wtedy, gdy $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

6. Udowodnij, że dla liczby pierwszej p, $p^p - 1$ ma dzielnik pierwszy postaci $kp + 1$.

7. Udowodnij, że jeśli n jest całkowite większe od 1, oraz $n \mid 5^n + 6^n$, to $11 | n$.

8. (OM) Udowodnij, że jęśli k, n są liczbami całkowitymi większymi od 1, to nie istnieją takie liczby naturalne a, b, że zachodzi jednocześnie $k \mid 2^a - 1, 2^b + 1$ oraz $n \mid 2^b - 1, 2^a + 1$

9. Niech p będzie liczbą pierwszą. Udowodnij, że istnieje taka liczba pierwsza q, że dla każdej liczby całkowitej n, zachodzi $q \mid n^p - p$.

10. Wyznacz wszystkie pary liczb pierwszych p, q takie, że $pq \mid 2^p + 2^q$.