Rzędy i generatory

Teoria

Oznaczenia. $\mathbb{Z}_+$ oznacza zbiór liczb całkowitych dodatnich.

Definicja 1. Dane są dodatnie liczby całkowite a i $m \geqslant 2$ względnie pierwsze. Wówczas **rząd** a **modulo** m to najmniejsza taka dodatnia liczba całkowita n, że $a^n \equiv 1 \pmod{m}$, i oznaczamy ją $\mathrm{ord}_m(a)$.

Twierdzenie 1. *Dane są dodatnie liczby całkowite a, k oraz $m \geqslant 2$ takie, że $a^k \equiv 1 \pmod{m}$. Wówczas*

$$ord_m(a) \mid k.$$

Twierdzenie 2. *Z powyższego twierdzenia wynika kilka następujących własności:*

1. $ord_m(a) \mid \varphi(m)$,
2. $a^k \equiv a^l \pmod{m} \iff k \equiv l \pmod{ord_m(a)}$,
3. $ord_m(a^k) = ord_m(a) \ / \ NWD(k, ord_m(a))$,
4. $ord_m(a) \perp ord_m(b)$ *to* $ord_m(ab) = ord_m(a) \cdot ord_m(b)$.

Twierdzenie 3. *Dana jest liczba całkowita $m \geqslant 2$ oraz względnie pierwsza liczba z nim liczba a. Niech $s \geqslant 1$ będzie najmniejsza dodatnia liczba całkowita taka, że $a^s \equiv -1 \pmod{m}$. Wówczas*

$$ord_m(a) = 2s$$

oraz dla dowolnej liczby całkowitej t taka, że $a^t \equiv -1 \pmod{m} \iff t = (2k-1)s$. $k \in \mathbb{Z}_+$.

Definicja 2. Dane są dodatnie liczby całkowite a i $m \geqslant 2$ względnie pierwsze. Wówczas a jest **generatorem** modulo m, jeżeli $\mathrm{ord}_m(a) = \varphi(m)$. Dla $m = p$ - liczba pierwsza mamy $\mathrm{ord}_p(g) = p - 1$.

Twierdzenie 4. *Generator modulo m istnieje wtedy i tylko wtedy, gdy $m = 2, 4, p^k, 2p^k$ dla nieparzystej liczby pierwszej p oraz $k \in \mathbb{Z}_+$.*

Twierdzenie 5. *Dane są dodatnie liczby całkowite a i $m \geqslant 2$. Niech $r = ord_m(a)$ to liczby*

$$1, a, a^2, \ldots, a^{t-1}$$

są parami różne modulo p. W szczególności, gdy $a = g$ jest generatorem modulo m to zbiór liczb

$$g, g^2, \ldots, g^{\varphi(m)}$$

zawiera wszystkie reszty modulo m wzglednie pierwsze z m. Czyli gdy $m = p$ jest liczbą pierwszą to liczby

$$g, g^2, \ldots, g^{p-1}$$

tworzą permutację zbioru $\{1, 2, \ldots, p-1\}$.

Przykłady

1. Znajdź wszystkie liczby $n \in \mathbb{Z}_+$, dla których $n \mid 2^n - 1$.
2. Dowieść, że jeżeli $n > 1$ jest nieparzystą liczbą całkowitą, to $n \nmid 3^n - 1$.

Zadania

1. Wykazać, że jeżeli $n \geqslant 2$ jest liczbą całkowitą oraz $n \mid 11^n - 2^n$, to $3 \mid n$.
2. Dana jest liczba całkowita $n > 1$ taka, że $n \mid 2^n + 3^n$. Dowieść, że $5 \mid n$.
3. Udowodnij, że dla dodatnich liczb całkowitych $a, n \geqslant 2$ zachodzi $n \mid \varphi(a^n - 1)$.
4. Dana jest liczba pierwsza p. Dowieść, że $p \equiv 1 \pmod 4$ wtedy i tylko wtedy, gdy istnieje liczba całkowita n taka, że $p \mid n^2 + 1$.
5. Udowodnić, że jeśli p jest liczbą pierwszą, to $p^p - 1$ ma dzielnik pierwszy w postaci $pk + 1$.
6. Wyznacz wszystkie pary liczb pierwszych p i q, dla których $pq \mid 2^p + 2^q$.
7. Dana jest liczba pierwsza p oraz dodatnia liczba całkowita k taka, że $p - 1 \nmid k$. Wykaż, że
$$p \mid 1^k + 2^k + \ldots + (p-1)^k.$$
8. Udowodnij, że jeśli k i n są liczbami całkowitymi większymi od 1, to nie istnieją takie liczby dodatnie liczby całkowite a i b, że zachodzą jednocześnie podzielności
$$k \mid 2^a - 1,\ 2^b + 1, \quad \text{oraz} \quad n \mid 2^b - 1, 2^a + 1.$$