Teoria liczb
kongruencje i rzędy, 6-9 marca

Zadanie 1. Rozważmy równanie $x^2 + x + 1 \equiv 0 \pmod{n}$.

(a) Ile rozwiązań ma to równanie w $\mathbb{Z}_n$ dla $n = 2$?

(b) Ile rozwiązań ma to równanie w $\mathbb{Z}_n$ dla $n = 3$?

(c) Ile rozwiązań ma to równanie w $\mathbb{Z}_n$ dla $n = 5$?

(d) Ile rozwiązań ma to równanie w $\mathbb{Z}_n$ dla $n = 7$?

(e) Ile rozwiązań ma to równanie w $\mathbb{Z}_n$ dla $n = 21$?

(f) Ile rozwiązań ma to równanie w $\mathbb{Z}_n$ dla $n = 105$?

Zadanie 2. Liczba 2 jest generatorem modulo 29.

(a) Podaj, bez przeliczania wszystkich przypadków, rozwiązania równania $x^7 \equiv 1 \pmod{29}$.

(b) Podaj tak samo rozwiązania równania $x^4 \equiv 1 \pmod{29}$ oraz rozwiązania równania $x^3 \equiv 1 \pmod{29}$.

(c) Ile jest elementów a takich, że $a \pmod{29}$ jest generatorem?

Wskazówka: zamień zadanie na potęgi generatora.

Zadanie 3. Daje są liczby całkowite dodatnie k i p, przy czym p jest pierwsza. Ile jest rozwiązań równania $x^k \equiv 1 \pmod{p}$ w zbiorze $\{0, 1, \ldots, p-1\}$? *Wskazówka: przepisz na potęgi generatora.*

Zadanie 4. Daje są liczby całkowite dodatnie k, e i p, przy czym p jest pierwsza. Ile jest rozwiązań równania $x^k \equiv 1 \pmod{p^e}$ w zbiorze $\{0, 1, \ldots, p^e - 1\}$? *Wskazówka: przepisz na potęgi generatora.*

Zadanie 5. Pokaż, że dla każdej liczby naturalnej $n \geq 2$ zachodzi $5^{2^{n-2}} \equiv 1 + 2^n \pmod{2^{n+1}}$.

Zadanie 6. Niech n będzie liczbą całkowitą dodatnią.

(a) Ile elementów ma $\mathbb{Z}^*_{2^{n+1}}$?

(b) Oblicz, że rząd 5 w $\mathbb{Z}^*_{2^{n+1}}$ to 2^{n-1}. *Wskazówka: rząd musi dzielić rząd grupy.*

(c) Pokaż, że każdy element grupy $\mathbb{Z}^*_{2^{n+1}}$ można zapisać jednoznacznie jako $\pm 5^s \mod 2^{n+1}$, gdzie $s \in \{0, 1, \ldots, 2^{n-1} - 1\}$. *Wskazówka: pokaż, że żadne dwa elementy $\pm 5^s$ nie są równe modulo 2^{n+1}.*

(d) Pokaż, że dla każdego elementu $g \in \mathbb{Z}^*_{2^{n+1}}$ zachodzi $g^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$.

Zadanie 7. Niech p będzie pierwsza, a k całkowita dodatnia. Jaka jest reszta z dzielenia przez p liczby $1^k + 2^k + \ldots + (p-1)^k$? *Wskazówka: zapisz podzielność za pomocą generatora grupy $\mathbb{Z}^*_p$.*

Zadanie 8 ($\star$). Niech m będzie liczbą całkowitą dodatnią. Niech $q = 2^m + 1$. Załóżmy, że $3^{\frac{q-1}{2}} \equiv -1 \pmod{q}$. Pokaż, że q jest liczbą pierwszą.

Zadanie 9 ($\star$, istnieją liczby pierwsze przystające do 1 modulo q.). Niech q będzie liczbą pierwszą. Pokaż, że każdy dzielnik pierwszy p liczby $2^q - 1$ spełnia $p \equiv 1 \pmod{q}$. *Wskazówka: rozważ rząd 2.*