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 $n = 105$?

Rozwiązanie.

Obliczenia dla $n = 2, 3, 5, 7$ można przeprowadzić bezpośrednio, licząc wszystkie przypadki (i to jest bardzo dobry sposób). Można też zauważyć, że wielomian z zadania spełnia $(x - 1)(x^2 + x + 1) = x^3 - 1$. Wynika z niego, że dla każdego liczby pierwszej p i każdego $a \in \mathbb{Z}_p$, $a \neq 1 \mod p$, zachodzi równoważność

$$a^2 + a + 1 \equiv 0 \pmod{p} \text{ wtedy i tylko wtedy, gdy } a^3 \equiv 1 \pmod{p}.$$

Z zadania 3 z tej serii wiemy, że równanie $x^3 \equiv 1 \pmod{p}$ ma dokładnie $\mathrm{NWD}(p - 1, 3)$ rozwiązań w $\mathbb{Z}_p$. Jednym z tych rozwiązań jest $1 \mod p$. Zatem równanie $x^2 + x + 1 \equiv 1 \pmod{p}$ ma dokładnie $\mathrm{NWD}(p-1, 3)-1$ rozwiązań w $\mathbb{Z}_p \setminus \{1 \mod p\}$. Element $1 \mod p$ jest rozwiązaniem tylko dla $p = 3$, więc podsumowując, równanie $x^2 + x + 1 \equiv 0 \pmod{p}$ ma

$$\mathrm{NWD}(p - 1, 3) - 1 \text{ rozwiązań dla } p \neq 3 \text{ oraz jedno rozwiązanie dla } p = 3.$$

Z chińskiego twierdzenia o resztach wynika, że liczba rozwiązań dla $n = 21$ to dwa, zaś dla $n = 105$ to 0.

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.

Rozwiązanie.

Poniżej podajemy odpowiedzi, co do uzasadnienia, patrz następne zadania.
(a) Rozwiązania to $2^4 \mod 29, 2^8 \mod 29, 2^{12} \mod 29, \ldots, 2^{28} \mod 29$.
(b) Rozwiązania to $2^7 \mod 29$, $2^{14} \mod 29$, $2^{21} \mod 29$, $2^{28} \mod 29$.
(c) Zapiszmy $a \equiv 2^e \mod p$. Wtedy a jest generatorem wtedy i tylko wtedy, gdy e jest względnie pierwsze z 28. Takich liczb jest $\varphi(28) = (4-2)(7-1) = 12$.

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.*

Rozwiązanie.

Liczba $0 \mod p$ nie jest rozwiązaniem, więc możemy szukać rozwiązań w $\mathbb{Z}_p^*$. Niech g będzie generatorem grupy $\mathbb{Z}_p^*$. Wtedy każdy element $\mathbb{Z}_p^*$ zapisuje się jednoznacznie jako $g^e \mod p$, gdzie $e \in \{1, \ldots, p-1\}$. Element ten jest rozwiązaniem równania dokładnie gdy $g^{ke} \equiv 1 \pmod p$. Skoro g jest generatorem, to przystawanie powyżej zachodzi dokładnie, wtedy gdy $p-1$ dzieli ke.

Liczba $p-1$ dzieli ke wtedy i tylko wtedy, gdy $\frac{p-1}{\mathrm{NWD}(k,p-1)}$ dzieli iloczyn $\frac{k}{\mathrm{NWD}(k,p-1)} \cdot e$. Liczby $(p-1)/\mathrm{NWD}(k, p-1)$ oraz $k/\mathrm{NWD}(k, p-1)$ są względnie pierwsze, więc ostatnia podzielność zachodzi dokładnie, gdy $\frac{p-1}{\mathrm{NWD}(k,p-1)}$ dzieli e. Zatem zbiór rozwiązań to elementy

$$g^{\frac{p-1}{\mathrm{NWD}(k,p-1)}} \mod p, g^{2\frac{p-1}{\mathrm{NWD}(k,p-1)}} \mod p, \ldots, g^{p-1} \mod p.$$

Elementów tych jest $\mathrm{NWD}(k, p-1)$.

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.*

Rozwiązanie.

Załóżmy najpierw, że p jest nieparzysta. Z wykładu wiemy, że grupa $\mathbb{Z}^*_{p^e - p^{e-1}}$ jest cykliczna rzędu $p^e - p^{e-1}$, generowana przez pewien element $g \mod p^e$. Powtarzając rozumowanie z poprzedniego zadania, otrzymujemy liczbę rozwiązań $\mathrm{NWD}(k, p^e - p^{e-1})$.
Załóżmy teraz, że $p = 2$. W tym przypadku tylko szkicujemy dowód. Przypadki $e = 1, 2$ liczymy „na palcach". Załóżmy więc $e \geq 3$. Z zadania 6. poniżej wynika, że każdy x jest postaci $\pm 5^s$ dla $0 \leq s \leq 2^{e-2} - 1$. Jeśli k jest parzyste, to $(\pm 5^s)^k = 5^{sk}$, co daje resztę 1 dokładnie dla $2^{e-2} \mid sk$, zatem mamy $2\,\mathrm{NWD}(k, 2^{e-2})$ rozwiązań, gdzie czynnik dwa pochodzi stąd, że możemy wybrać znak $\pm$ dowolnie. Jeśli k jest nieparzyste, to otrzymujemy jedynie jedno rozwiązanie.

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

Rozwiązanie.

Zachodzi równość

$$5^{2^{n-2}} - 1 = (5^{2^{n-3}} + 1) \cdot (5^{2^{n-3}} - 1) = (5^{2^{n-3}} + 1) \cdot (5^{2^{n-4}} + 1) \cdot \ldots \cdot (5 + 1) \cdot (5 - 1).$$

Po prawej stronie mamy $n - 1$ nawiasów. Liczby w pierwszych $n - 2$ z nich przystają do $2 \mod 4$. Ostatnia liczba to 2^2. Zatem w rozkładzie $5^{2^{n-2}} - 1$ liczba 2 występuje z wykładnikiem $n - 2 + 2 = n$. To znaczy, że $5^{2^{n-2}} - 1 = 2^n \cdot (2k + 1)$ dla pewnego $k \in \mathbb{Z}$, czyli

$$5^{2^{n-2}} - 1 = 2^{n+1}k + 2^n \equiv 2^n \pmod{2^{n+1}}.$$

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 jeśli $n \geq 2$ to dla każdego elementu $g \in \mathbb{Z}^*_{2^{n+1}}$ zachodzi $g^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$.

Rozwiązanie.
(a) Grupa ta ma $\varphi(2^{n+1}) = 2^n$ elementów.
(b) Niech r będzie rzędem $5 \mod 2^{n+1}$. Wtedy r dzieli $|\mathbb{Z}^*_{2^{n+1}}| = 2^n$, zatem $r = 2^s$ dla pewnego $s \in \{0, 1, \ldots, n\}$. Z poprzedniego zadania wynika, że $5^{2^{n-2}} \equiv 1 + 2^n \mod 2^{n+1}$, zatem $5^{2^{n-2}} \not\equiv 1$, czyli r nie dzieli 2^{n-2}. Stąd wynika, że $r \geq 2^{n-1}$. Ponadto

$$5^{2^{n-1}} \equiv (1 + 2^n)^2 = 1 + 2^{n+1} + 2^{2n} \equiv 1 \pmod{2^{n+1}}, \tag{1.1}$$

więc rząd 5 to 2^{n-1}.
(c) Załóżmy, że $\pm 5^t \equiv \pm 5^s \pmod{2^{n+1}}$, gdzie $0 \leq s \leq t \leq 2^{n-1} - 1$. Podnosząc do kwadratu, otrzymujemy $5^{2t} \equiv 5^{2s} \pmod{2^{n+1}}$, stąd $5^{2(t-s)} \equiv 1 \pmod{2^{n+1}}$. Wynika stąd, że 2^{n-1} dzieli $2(t - s)$, więc 2^{n-2} dzieli $t - s$. Skoro $0 \leq t - s \leq 2^{n-1} - 1$, to wynika stąd, że $t = s + 2^{n-2}$ lub $t = s$. Przypadek $t = s$ prowadzi do $1 \equiv -1 \pmod{2^{n+1}}$, czyli sprzeczności. Przypadek $t = s$ daje

$$\pm 5^s \equiv \pm 5^s \cdot 5^{2^{n-2}} \equiv \pm 5^s \cdot (1 + 2^n) \pmod{2^{n+1}}.$$

Skracając przez 5^s, które jest względnie pierwsze z 2^{n+1}, otrzymujemy

$$\pm 1 \equiv \pm (1 + 2^n) \pmod{2^{n+1}},$$

czyli znowu sprzeczność.
(d) Skoro $n \geq 2$, to 2^{n-1} jest parzysta. Używamy kongruencji (1.1) by dostać

$$(\pm 5^s)^{2^{n-1}} = (-1)^{2^{n-1}} \cdot \left(5^{2^{n-1}}\right)^s \equiv 1 \cdot 1^s = 1 \pmod{2^{n+1}}.$$

Powyżej pokazaliśmy, że każdy element $g \in \mathbb{Z}^*_{2^{n+1}}$ jest postaci $\pm 5^s \mod 2^{n+1}$, więc powyższe obliczenie jest dowodem w tym podpunkcie.

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 $\mathbb{Z}^*_p$.*

Rozwiązanie.

Jeśli $p-1$ dzieli k, to $a^k \equiv 1 \pmod p$ dla każdego $1 \leq a \leq p-1$, zatem liczba przystaje do $p-1 \equiv -1 \pmod p$. Załóżmy, że $p-1$ nie dzieli k. Niech g będzie generatorem $\mathbb{Z}^*_p$. Mamy wtedy

$$1^k + 2^k + \ldots + (p-1)^k \equiv g^0 + g^k + g^{2k} + \ldots + g^{(p-2)k} \pmod p.$$

Skoro $p-1$ nie dzieli k, to $g^k - 1 \not\equiv 0 \pmod p$, więc możemy zapisać wzór na ciąg geometryczny

$$g^0+g^k+g^{2k}+\ldots+g^{(p-2)k} \equiv \frac{1}{1-g^k}\cdot(1-g^k)(g^0+g^k+g^{2k}+\ldots+g^{(p-2)k}) = \frac{1}{1-g^k}(1-g^{k(p-1)}) \pmod p.$$

Mamy $g^{k(p-1)} = (g^{p-1})^k \equiv 1^k \pmod p$, więc

$$\frac{1}{1-g^k}(1-g^{k(p-1)}) \equiv 0 \pmod p,$$

czyli suma przystaje do zera (gdy $p-1$ nie dzieli k).

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.

Rozwiązanie.

Niech r oznacza rząd liczby 3 w $\mathbb{Z}^*_q$. Z kongruencji $3^{\frac{q-1}{2}} \equiv -1 \pmod q$ wynika $3^{q-1} \equiv 1 \pmod q$, więc r dzieli $q-1$. Ale $q-1 = 2^m$, czyli r jest potęgą dwójki, powiedzmy $r = 2^l$, dla $l \leq m$. Ponadto $3^{\frac{q-1}{2}} = 3^{2^{m-1}} \equiv -1 \not\equiv 1 \pmod q$, więc r nie dzieli 2^{m-1}. To implikuje, że $r = 2^m = q-1$. To znaczy, że rząd 3 w $\mathbb{Z}^*_q$ to $q-1$, czyli $\mathbb{Z}^*_q$ ma $q-1$ elementów. To znaczy, że każda liczba ze zbioru $\{1, 2, \ldots, q-1\}$ jest względnie pierwsza z q, więc q jest pierwsza.

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.*

Rozwiązanie.

Niech r będzie rzędem $2 \mod p$. Z kongruencji $2^q \equiv 1 \pmod p$ wynika, że r dzieli q. Ale q jest pierwsza, więc albo $r = 1$ albo $r = q$. Przypadek $r = 1$ implikuje, że $2 \equiv 1 \pmod p$, sprzeczność. Zatem $r = q$. Z małego twierdzenia Fermata wynika, że $2^{p-1} \equiv 1 \pmod p$, a stąd r dzieli $p-1$. Zatem $p-1 \equiv 0 \pmod q$, czyli $p \equiv 1 \pmod q$.