Oddział intensywnego myślenia

Kącik olimpijski nr 1 (7 marca 2026)

Grupy $\mathbb{Z}_n^\times$ i pierwiastki pierwotne modulo n

Niech $n \geqslant 2$ będzie liczbą całkowitą. Przez $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ oznaczamy zbiór reszt modulo n, $\mathbb{Z}_n^\times$ to zbiór reszt względnie pierwszych z n, a liczba elementów $\mathbb{Z}_n^\times$ to funkcja Eulera $\varphi(n)$. Dodawanie, odejmowanie, mnożenie i potęgowanie, a także równości w zbiorze $\mathbb{Z}_n$ rozumiemy modulo n. Reszta $b \in Z_n$ jest odwrotnością reszty $a \in \mathbb{Z}_n$ modulo n, jeśli $a \cdot b = 1$ w $\mathbb{Z}_n$, tj. $a \cdot b \equiv 1 \pmod{n}$.

Twierdzenie A. (a) Zbiór $\mathbb{Z}_n$ z działaniem + jest grupą przemienną.
(b) Zbiór $Z_n^\times$ z działaniem $\cdot$ również jest grupą przemienną.

Ćwiczenie 1. Udowodnij, że każda reszta $a \in \mathbb{Z}_n^\times$ ma odwrotność modulo n.
Wskazówka: *Reszty $k \cdot a$, gdzie $k \in \mathbb{Z}_n^\times$, są parami różne.*

Ćwiczenie 2. Udowodnij twierdzenie A.

Twierdzenie B. Jeśli G jest N-elementową grupą z działaniem $\cdot$, to $a^N = 1$ dla każdego $a \in G$.

Ćwiczenie 3. Udowodnij twierdzenie B.
Wskazówka: *Zbiory postaci $[b] = \{a^k \cdot b : k = 0, 1, \ldots\}$, gdzie $b \in G$, są równoliczne i parami rozłączne lub równe.*

Ćwiczenie 4. Wywnioskuj z twierdzenia B małe twierdzenie Fermata i twierdzenie Eulera.

Wielomianem stopnia k w $\mathbb{Z}_n$ nazywamy wyrażenie postaci

$$P(x) = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0,$$

gdzie $k \geqslant 0$, $a_0, a_1, \ldots, a_k \in \mathbb{Z}_n$ oraz $a_k \neq 0$, lub wielomian zerowy (stopnia $-\infty$). Działania na wielomianach w $\mathbb{Z}_n$ są określone w naturalny sposób (modulo n). Równość wielomianów zawsze oznacza równość odpowiednich współczynników. (W miejsce $\mathbb{Z}_n$ można podstawić dowolny *pierścień*.)

Twierdzenie C (twierdzenie Bézouta). Jeśli P jest wielomianem w $\mathbb{Z}_n$, $a \in \mathbb{Z}_n$ oraz $P(a) = 0$, to $P(x) = (x - a)Q(x)$ dla pewnego wielomianu Q w $\mathbb{Z}_n$.

Ćwiczenie 5. Udowodnij twierdzenie Bézouta.

Ćwiczenie 6. Udowodnij, że jeśli n jest liczbą pierwszą, to wielomian stopnia k w $\mathbb{Z}_n$ ma co najwyżej k pierwiastków w $\mathbb{Z}_n$.

Reszta $a \in \mathbb{Z}_n$ jest pierwiastkiem pierwotnym modulo n, jeśli każda reszta z $\mathbb{Z}_n^\times$ jest potęgą a.

Twierdzenie D (twierdzenie Gaussa). Pierwiastek pierwotny modulo n istnieje wtedy i tylko wtedy, gdy $n = 2$, $n = 4$, $n = p^k$ lub $n = 2p^k$, gdzie $p \geqslant 3$ jest pierwsza i $k = 1, 2, \ldots$

Ćwiczenie 7. Udowodnij twierdzenie Gaussa w przypadku, gdy n jest liczbą pierwszą.
Wskazówka: *Jeśli $d | n-1$, to reszty postaci $a^{(n-1)/d}$ spełniają równanie $x^d = 1$ w $\mathbb{Z}_n^\times$ i jest ich d.*

Ćwiczenie 8. Udowodnij twierdzenie Gaussa, gdy n jest kwadratem liczby pierwszej.
Wskazówka: *Jeśli a jest pierwiastkiem pierwotnym modulo p, to a lub $a + p$ jest pierwiastkiem pierwotnym modulo p^2.*

Ćwiczenie 9. Udowodnij twierdzenie Gaussa, gdy n jest potęgą nieparzystej liczby pierwszej.
Wskazówka: *Jeśli a jest pierwiastkiem pierwotnym modulo p^2, to jest też pierwiastkiem pierwotnym modulo p^k ($k \geqslant 3$).*

Ćwiczenie 10. Udowodnij twierdzenie Gaussa w pełnej ogólności.
Wskazówka: *Jeśli $\mathrm{NWD}(n, m) = 1$ oraz $a \in \mathbb{Z}_{n \cdot m}^\times$, to $a^{\mathrm{NWD}(\varphi(n), \varphi(m))} = 1$ w $\mathbb{Z}_{n \cdot m}$.*

Zadania

Zadanie 1. Dana jest liczba pierwsza $p > 2$. Liczbę całkowitą n nazwiemy *ładną*, jeśli suma reszt z dzielenia liczb $n, n^2, n^3, \ldots, n^{p-1}$ przez p jest równa $\frac{1}{2}p(p-1)$. Wykaż, że wśród liczb $1, 2, \ldots, p-1$ jest nieparzyście wiele liczb ładnych. [OM 2020]

Zadanie 2. Ile spośród liczb $1, 2, \ldots, p-1$ jest ładnych?

Zadanie 3. Wykaż, że dla $n = 1, 2, \ldots$ wszystkie dzielniki liczby $2^{2^n} + 1$ przystają do 1 modulo 2^{n+1}.

Zadanie 4. Wyznacz wszystkie liczby całkowite, które są względnie pierwsze z $2^n + 3^n + 6^n - 1$ dla wszystkich $n = 1, 2, \ldots$ [IMO 2005]

Zadanie 5. Dla danej liczby pierwszej p wyznacz resztę z dzielenia przez p iloczynu

$$(1^2 + 1) \cdot (2^2 + 1) \cdot (3^2 + 1) \cdot \ldots \cdot ((p-1)^2 + 1).$$

Zadanie 6. Udowodnij, że 2 jest pierwiastkiem pierwotnym modulo 3^k dla każdego $k = 1, 2, \ldots$

Zadanie 7 (twierdzenie Wilsona, twierdzenie Gaussa). Dla danej liczby całkowitej $n \geqslant 2$ wyznacz resztę z dzielenia przez n iloczynu wszystkich liczb $k \in \{1, 2, \ldots, n-1\}$ względnie pierwszych z n.

Zadanie 8. Dla danej liczby całkowitej $n > 1$ niech P_n oznacza iloczyn tych liczb $a \in \{1, 2, \ldots, n-1\}$, dla których $n | a^2 - 1$. Wyznacz (w zależności od n) resztę z dzielenia liczby P_n przez n. [IMO SL 2004]

Zadanie 9. Wyznacz wszystkie liczby całkowite $n \geqslant 2$ o następującej własności: dla wszystkich liczb całkowitych a i b względnie pierwszych z n warunki

$$a \equiv b \pmod{n} \qquad \text{oraz} \qquad ab \equiv 1 \pmod{n}$$

są równoważne. [IMO SL 2000]

Zadanie 10. Dana jest liczba całkowita $k \geqslant 2$. Udowodnij, że następujące warunki są równoważne:

(a) jeśli n jest liczbą całkowitą oraz k dzieli $n^n - 1$, to k dzieli $n - 1$;
(b) jeśli p, q są pierwsze, p dzieli k, zaś q dzieli $p - 1$, to q dzieli k. [OMO 2013]

Zadanie 11. Niech p będzie liczbą pierwszą, a P wielomianem o współczynnikach całkowitych stopnia co najwyżej $p - 2$. Przypuśćmy, że zbiór reszt z dzielenia $P(n)$ przez p dla całkowitych n liczy co najwyżej dwa elementy. Udowodnij, że zbiór ten jest wtedy jednoelementowy. [IMO SL 1997]

Zadanie 12. Ciąg (a_n) dany jest wzorami $a_0 = 2$ oraz $a_{n+1} = 2a_n^2 - 1$ dla $n = 0, 1, \ldots$ Udowodnij, że jeśli nieparzysta liczba pierwsza p dzieli a_n, to 2^{n+3} dzieli $p^2 - 1$. [IMO SL 2003]

Zadanie 13. Dana jest liczba pierwsza p. Udowodnij, że istnieje liczba pierwsza q o następującej własności: q nie dzieli $n^p - p$ dla żadnego całkowitego n. [IMO 2003]

Wskazówki do wybranych zadań

Zadanie 1. Dana jest liczba pierwsza $p > 2$. Liczbę całkowitą n nazwiemy *ładną*, jeśli suma reszt z dzielenia liczb $n, n^2, n^3, \ldots, n^{p-1}$ przez p jest równa $\frac{1}{2}p(p-1)$. Wykaż, że wśród liczb $1, 2, \ldots, p-1$ jest nieparzyście wiele liczb ładnych. [OM 2020]

Wskazówka: *Jeśli n jest ładna, to odwrotność n modulo p też jest ładna.*

Zadanie 2. Ile spośród liczb $1, 2, \ldots, p-1$ jest ładnych?

Wskazówka: *Jeśli a jest pierwiastkiem pierwotnym modulo p, to a^k jest ładna wtedy i tylko wtedy, gdy $v_2(k) < v_2(p-1)$, gdzie $v_2(n)$ oznacza liczbę dwójek w rozkładzie n na czynniki pierwsze.*

Zadanie 3. Wykaż, że dla $n = 1, 2, \ldots$ wszystkie dzielniki liczby $2^{2^n} + 1$ przystają do 1 modulo 2^{n+1}.

Wskazówka: *Jeśli liczba pierwsza p dzieli $2^{2^n} + 1$, to $2^k \equiv 1 \pmod{p}$ wtedy i tylko wtedy, gdy $2^{n+1} | k$.*

Zadanie 4. Wyznacz wszystkie liczby całkowite, które są względnie pierwsze z $2^n + 3^n + 6^n - 1$ dla wszystkich $n = 1, 2, \ldots$ [IMO 2005]

Wskazówka: *Skoro $2^{-1} + 3^{-1} + 6^{-1} - 1 = 0$, to również $2^{-1} + 3^{-1} + 6^{-1} - 1 \equiv 0 \pmod{p}$ gdy p jest liczbą pierwszą.*

Zadanie 5. Dla danej liczby pierwszej p wyznacz resztę z dzielenia przez p iloczynu

$$(1^2 + 1) \cdot (2^2 + 1) \cdot (3^2 + 1) \cdot \ldots \cdot ((p-1)^2 + 1).$$

Wskazówka: *Zachodzi $(x-1) \cdot (x-2) \cdot \ldots \cdot (x-(p-1)) = x^p - 1$ w $\mathbb{Z}_p$, także dla $x = \pm i$.*

Zadanie 6. Udowodnij, że 2 jest pierwiastkiem pierwotnym modulo 3^k dla każdego $k = 1, 2, \ldots$

Wskazówka: *Zachodzi $v_3(4^m - 1) = v_3(m) + 1$, gdzie $v_3(n)$ oznacza liczbę trójek w rozkładzie n na czynniki pierwsze.*

Zadanie 7 (twierdzenie Wilsona, twierdzenie Gaussa). Dla danej liczby całkowitej $n \geqslant 2$ wyznacz resztę z dzielenia przez n iloczynu wszystkich liczb $k \in \{1, 2, \ldots, n-1\}$ względnie pierwszych z n.

Wskazówka: *Jeśli $a^2 \equiv 1 \pmod{n}$, to $(n-a)^2 \equiv 1 \pmod{n}$, a jeśli $4|n$, to też $(a + \frac{n}{2})^2 \equiv 1 \pmod{n}$; ćwiczenie 10.*

Zadanie 8. Dla danej liczby całkowitej $n > 1$ niech P_n oznacza iloczyn tych liczb $a \in \{1, 2, \ldots, n-1\}$, dla których $n | a^2 - 1$. Wyznacz (w zależności od n) resztę z dzielenia liczby P_n przez n. [IMO SL 2004]

Wskazówka: *Zadanie 7.*

Zadanie 9. Wyznacz wszystkie liczby całkowite $n \geqslant 2$ o następującej własności: dla wszystkich liczb całkowitych a i b względnie pierwszych z n warunki

$$a \equiv b \pmod{n} \qquad \text{oraz} \qquad ab \equiv 1 \pmod{n}$$

są równoważne. [IMO SL 2000]

Wskazówka: *Gdy $n = 2^k m$ i m jest nieparzysta, to istnieje a spełniające $a \equiv 3 \pmod{2^k}$ oraz $a \equiv 2 \pmod{m}$.*

Zadanie 10. Dana jest liczba całkowita $k \geqslant 2$. Udowodnij, że następujące warunki są równoważne:

(a) jeśli n jest liczbą całkowitą oraz k dzieli $n^n - 1$, to k dzieli $n - 1$;

(b) jeśli p, q są pierwsze, p dzieli k, zaś q dzieli $p - 1$, to q dzieli k. [OMO 2013]

Wskazówka: ($\Rightarrow$) *Jeśli q dzieli $p-1$, ale nie k, to istnieje n podzielne przez q i spełniające warunek $n^q \equiv 1 \pmod{k}$.* ($\Leftarrow$) *Jeśli $n^n \equiv 1 \pmod{k}$, to $n^{\mathrm{NWD}(n,\varphi(k))} \equiv 1 \pmod{k}$.*

Zadanie 11. Niech p będzie liczbą pierwszą, a P wielomianem o współczynnikach całkowitych stopnia co najwyżej $p-2$. Przypuśćmy, że zbiór reszt z dzielenia $P(n)$ przez p dla całkowitych n liczy co najwyżej dwa elementy. Udowodnij, że zbiór ten jest wtedy jednoelementowy. [IMO SL 1997]

Wskazówka: *Jeśli a jest pierwiastkiem pierwotnym modulo p, to $1^k + 2^k + \ldots + (p-1)^k \equiv 1 + a^k + \ldots + a^{(p-2)k} \pmod{p}$.*

Mateusz Kwaśnicki