Jędrzej Hodor
Piotr Micek

Zestaw 4
Semestr letni 2023/2024
Kraków, 27 marca 2024

THEORETICAL COMPUTER SCIENCE
Jagiellonian University

Teoria liczb

Niech $n, n' \in \mathbb{N}$ i $m \in \mathbb{N}_1$. Mówimy, że m *dzieli* n (co zapisujemy $m \mid n$) jeśli istnieje $d \in \mathbb{Z}$ taka, że $n = m \cdot d$. Jeśli m dzieli n to mówimy, że m *jest dzielnikiem* n. Jeśli $p \in \mathbb{N}_1$ ma dokładnie dwa dzielniki to mówimy, że p jest *liczbą pierwszą*. Piszemy, że $n \equiv n' \bmod m$ jeśli $m \mid n' - n$. Unikalną liczbę całkowitą r taką, że $0 \leqslant r < m$ i $n \equiv r \bmod m$ nazywamy resztą z dzielenia n przez m. *Rozkładem na czynniki pierwsze liczby* n nazywamy multizbiór liczb pierwszych takich, że ich iloczyn daje n. Rozkład na czynniki pierwsze jest unikalny.

Niech $n_1, \ldots, n_s$ będą niezerowymi liczbami całkowitymi. Wtedy *największy wspólny dzielnik* $n_1, \ldots, n_s$ (ang. greatest common divisor) definiujemy i oznaczamy następująco:

$$\gcd(n_1, \ldots, n_s) = \max\{d \in \mathbb{N}_1 : d \mid n_i \text{ dla każdego } i \in [s]\}.$$

Jeśli $\gcd(n_1, \ldots, n_s) = 1$ to mówimy, że liczby $n_1, \ldots, n_s$ są *względnie pierwsze*. *Największa wspólna wielokrotość* $n_1, \ldots, n_s$ (ang. least common multiplicity) definiujemy i oznaczamy następująco:

$$\operatorname{lcm}(n_1, \ldots, n_s) = \min\{d \in \mathbb{N}_1 : n_i \mid d \text{ dla każdego } i \in [s]\}.$$

Niech $\mathcal{A}$ będzie zbiorem wszystkich funkcji $\mathbb{N}_1 \to \mathbb{C}$. Zdefiniujemy kilka ciekawych elementów $\mathcal{A}$. Niech $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, gdzie dla każdego $i \in [k]$, p_i jest liczbą pierwszą i $\alpha_i \in \mathbb{N}_1$ (jeśli $n = 1$ to $k = 0$). Niech $\alpha \in \mathbb{C}$.

$$\begin{aligned} \varphi(n) &= |\{d \in [n] : \gcd(n, d) = 1\}|, & N_\alpha(n) &= n^\alpha, \\ \mu(n) &= (-1)^k \cdot [\alpha_1 = \cdots = \alpha_k = 1], & I(n) &= \left\lfloor \frac{1}{n} \right\rfloor, \\ \sigma_\alpha(n) &= \sum_{d \mid n} d^\alpha, & u(n) &= 1. \end{aligned}$$

Dla $f, g \in \mathcal{A}$, $f \cdot g$ to funkcja taka, że $f \cdot g(n) = f(n)g(n)$ dla każdego $n \in \mathbb{N}_1$.

Splot Dirichleta. Dla dwóch funkcji $f, g \in \mathcal{A}$ definiujemy splot Dirichleta $f * g$ w następujący sposób. Dla każdego $n \in \mathbb{N}_1$,

$$(f * g)(n) = \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right) = \sum_{ab = n} f(a)g(b).$$

Mówimy, że $f \in \mathcal{A}$ jest *multiplikatywna* jeśli $f(ab) = f(a)f(b)$ dla wszystkich $a, b \in \mathbb{N}_1$ takich, że $\gcd(a, b) = 1$. Mówimy, że $f \in \mathcal{A}$ jest *całkowicie multiplikatywna* jeśli $f(ab) = f(a)f(b)$ dla wszystkich $a, b \in \mathbb{N}_1$. Niech $\mathcal{M} \subseteq \mathcal{A}$ będzie zbiorem funkcji multiplikatywnych i niech $\mathcal{C} \subseteq \mathcal{M}$ będzie zbiorem funkcji całkowicie multiplikatywnych.

Zadania

Zadanie 1. Udowodnij korzystając z interpretacji kombinatorycznej, że dla każdego $n, k \in \mathbb{N}$ mamy

$$\binom{2n}{2k} \equiv \binom{n}{k} \mod 2.$$

Wskazówka: Rozważ binarne ciągi palindromiczne.

Zadanie 2. Niech S będzie skończonym zbiorem i niech $g : S \to S$. Załóżmy, że istnieje liczba pierwsza p taka, że dla każdego $x \in S$ mamy $g^p(x) = x$ (p-krotne złożenie). Niech $F = \{x \in S : g(x) = x\}$ będzie zbiorem punktów stałych względem g. Udowodnij, że

$$|S| \equiv |F| \mod p.$$

Zadanie 3. Niech p będzie liczbą pierwszą. Udowodnij korzystając z interpretacji kombinatorycznej, że dla każdego $n, k \in \mathbb{N}$ mamy

$$\binom{pn}{pk} \equiv \binom{n}{k} \mod p.$$

Zadanie 4. (Twierdzenie Wilsona) Udowodnij korzystając z interpretacji kombinatorycznej, że dla każdej liczby pierwszej p mamy

$$(p-1)! \equiv p-1 \mod p.$$

Wzkazówka: Lewa strona zlicza wszystkie permutacje $\{0, \ldots, p-1\}$ mające jeden cykl.

Zadanie 5. Niech dla każdego $n \in \mathbb{N}_1$, $\mathcal{P}_n$ oznacza zbiór liczb pierwszych p takich, że $p \leqslant n$. Udowodnij, że

$$\prod_{p \in \mathcal{P}_n} p < 4^n.$$

Zauważ, że z ostatniego zadania z pierwszego zestawu wynika następujący fakt. Jeśli p jest liczbą pierwszą, $\alpha \in \mathbb{N}_1$ i $x \in \mathbb{N}$ to

$$(1+x)^{p^\alpha} \equiv 1 + x^{p^\alpha} \mod p.$$

Zadanie 6. Korzystając z powyższego znajdź wszystkie $k \in \mathbb{N}$ takie, że liczba $\binom{82}{k}$ jest nieparzysta. A ile jest liczb $k \in \mathbb{N}$ takich, że liczba $\binom{1621}{k}$ jest nieparzysta? I ogólniej, dla danego $n \in \mathbb{N}$ ile jest liczb $k \in \mathbb{N}$, takich, że liczba $\binom{n}{k}$ jest nieparzysta?

Zadanie 7. Jeszcze ogólniej. Mając daną liczbę pierwszą p znajdź i udowodnij wzór na $\binom{n}{k} \mod p$ dla każdego $n, k \in \mathbb{N}$.

Zadanie 8. Przedstaw algorytm Euklidesa dla wielomianów i udowodnij tożsamość Bézouta dla wielomianów. Dokładniej, udowodnij, że jeśli $Q_1(x), Q_2(x) \in \mathbb{Z}[x]$ są względnie pierwszymi wielomianami (to znaczy mają rozłączne zbiory pierwiastków zespolonych) to istnieją wielomiany $R_1(x), R_2(x) \in \mathbb{Z}[x]$ takie, że

$$1 = R_1(x)Q_1(x) + R_2(x)Q_2(x).$$

Zadanie 9. Niech $Q_1(x), Q_2(x), P(x) \in \mathbb{Z}[x]$ i $Q(x) = Q_1(x)Q_2(x)$. Uwodonij, że jeśli $\deg(P) < \deg(Q)$ i $Q_1(x), Q_2(x)$ są względnie pierwsze to istnieją $P_1(x), P_2(x) \in \mathbb{Z}[x]$ takie, że $\deg(P_1) < \deg(Q_1)$ i $\deg(P_2) < \deg(Q_2)$ oraz

$$\frac{P(x)}{Q(x)} = \frac{P_1(x)}{Q_1(x)} + \frac{P_2(x)}{Q_2(x)}.$$

Zauważ, że powyższy fakt jest wystarczający w pominiętym przejściu dowodu twierdzenia o rekurencjach liniowych z wykładu.

Zadanie 10. Znajdź wszystkie rozwiązania w liczbach całkowitych następujących równań

(i) $-15x + 21y = 2$;
(ii) $870x - 640y = 30$;
(iii) $12x - 5y + 43z = -78$.

Zadanie 11. Znajdź wszystkie rozwiązania w liczbach całkowitych następujących układów równań

(i) $\begin{cases} x \equiv 1 \mod 6 \\ x \equiv 1 \mod 5 \\ x \equiv 1 \mod 7 \end{cases}$;

(ii) $\begin{cases} 5x \equiv 7 \mod 11 \\ 4x \equiv 3 \mod 9 \\ 2x \equiv 5 \mod 8 \end{cases}$;

(iii) $\begin{cases} x \equiv 5 \mod 6 \\ x \equiv 3 \mod 10 \end{cases}$.

Zadanie 12. Oblicz $1001^{8641} \bmod 10800$.

Zadanie 13. Udowodnij, że dla wszystkich $n \in \mathbb{N}_1$ mamy

$$\sum_{d|n} \varphi(d) = n.$$

Zadanie 14. Udowodnij, że splot Dirichleta jest łączny i przemienny w $\mathcal{A}$, a I jest jego elementem neutralnym.

Zadanie 15. Udowodnij, że jeśli dla $f \in \mathcal{A}$ mamy $f(1) \neq 0$ to istnieje element odwrotny względem splotu Dirichleta, to jest $f^{-1} \in \mathcal{A}$ takie, że $f * f^{-1} = I$.

Zadanie 16. Udowodnij, że dla każdego $n \in \mathbb{N}_1$ mamy

$$\sum_{d|n} \mu(d) = I(n).$$

Innymi słowy $\mu * u = I$. Wywnioskuj, formułę inwersyjną Möbiusa, to znaczy

$$f(n) = \sum_{d|n} g(d) \quad \text{wtedy i tylko wtedy, gdy} \quad g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right).$$

Zadanie 17. Udowodnij, że dla wszystkich $n \in \mathbb{N}_1$ mamy

$$n \sum_{d|n} \frac{\mu(d)}{d} = \varphi(n).$$

Zadanie 18. Niech $f, g \in \mathcal{A}$. Udowodnij, że

(i) jeśli $f, g \in \mathcal{M}$ to $f * g \in \mathcal{M}$;
(ii) jeśli $g, f * g \in \mathcal{M}$ i $g(1) \neq 0$ to $f \in \mathcal{M}$;
(iii) jeśli $f \in \mathcal{M}$ i $f(1) \neq 0$ to $f^{-1} \in \mathcal{M}$.

Zadanie 19. Niech $f \in \mathcal{M}$. Pokaż, że $f \in \mathcal{C}$ wtedy i tylko wtedy, gdy $f^{-1} = \mu \cdot f$. Wyznacz wzory na φ^{-1} i σ_α^{-1}.

Liczba pierwsza p jest *liczbą pierwszą Mersenne'a* jeśli można ją przedstawić jako $p = 2^n - 1$ dla pewnego $n \in \mathbb{N}$.

Zadanie 20. Znajdź warunek konieczny i wystarczający na to, że $\sigma_1(n)$ jest potęgą dwójki.

Symbol Legendre'a. Na koniec pochylimy się nad klasycznym zagadnieniem teori liczb. Będziemy rozwiązywać równania kwadratowe. Przedstawimy wypowiedzi kilku twierdzeń bez dowodów i spróbujemy je zastosować do naturanych problemów.

Niech $a \in \mathbb{Z}$ i p będzie nieparzystą liczbą pierwszą. Definiujemy

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{jeśli } p \mid a, \\ 1 & \text{jeśli istnieje } x \in \mathbb{Z} \text{ taki, że } x^2 \equiv a \mod p, \\ -1 & \text{wpp.} \end{cases}$$

Czyli na przykład $\left(\frac{10}{13}\right) = 1$ bo $7^2 \equiv 10 \mod 13$. Z drugiej strony $\left(\frac{2}{3}\right) = -1$ co jest znanym faktem często używanym w licealnych zadaniach. Liczby a takie, że $\left(\frac{a}{p}\right) = 1$ są zwykle nazywane *resztami kwadratowymi modulo p*, a te, gdzie $\left(\frac{a}{p}\right) = -1$ *nieresztami kwadratowymi modulo p*. Liczba reszt jest zawsze równa liczbie niereszt – czyli $\frac{p-1}{2}$ (brakuje nam pojęć, żeby udowodnić ten fakt). Okazuje się, że istnieje metoda obliczania wartości $\left(\frac{a}{p}\right)$ lepsza niż sprawdzanie wszystkich możliwości. W tym celu potrzebujemy trzech następujących klasycznych twierdzeń. Pierwsze z nich można elementarnie udowodnić, drugie można udowodnić elementarnie, ale nie prosto (dowód pominiemy), a trzecie według wikipedi można udowodnić na co najmniej 246 różnych sposobów, jednak tutaj dowód też pominiemy.

Kryterium Eulera. Jeśli $a \in \mathbb{Z}$ i p jest nieparzystą liczbą pierwszą to

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Lemat Gaussa. Jeśli $a \in \mathbb{Z}$ i p jest nieparzystą liczbą pierwszą, która nie dzieli a oraz

$$S = \left\{ ai \bmod p : i \in \left[\frac{p-1}{2} \right] \text{ oraz } ai \bmod p > \frac{p}{2} \right\}$$

to $\left(\frac{a}{p}\right) = (-1)^{|S|}$.

Prawo wzajemności reszt kwadratowych. Jeśli p, q są różnymi nieparzystmi liczbami pierwszymi to

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Zauważ, że kryterium Eulera implikuje multiplikatywność symbolu Legandre'a, to znaczy

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Zadanie 21. Udowodnij kryterium Eulera.

Zadanie 22. Korzystając z lematu Gaussa udowodnij, że $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Zadanie 23. Oblicz $\left(\frac{342}{113}\right)$.

Zadanie 24. Czy istnieje $x \in \mathbb{Z}$ taki, że $3x^2 + 7x + 10 \equiv 0 \bmod 37$? Zakładając, że umiemy liczyć symbol Legendre'a podaj ogólną metodę jak sprawdzić, czy równanie

$$Ax^2 + Bx + C \equiv 0 \mod p$$

ma rozwiązanie całkowite. Zakładamy, że $A, B, C \in \mathbb{Z}$ takie, że p nie dzieli A i p jest nieparzystą liczbą pierwszą.

Zadanie bonusowe do spisania

Problem 1. Udowodnij korzystając z interpretacji kombinatorycznej, że dla wszystkich $a, b \in \mathbb{Z}$ i dla każdej liczby pierwszej p mamy

$$\binom{pa}{pb} \equiv \binom{a}{b} \mod p^2.$$

Problem 2. Udowodnij korzystając z interpretacji kombinatorycznej, że dla wszystkich $a, b \in \mathbb{Z}$ i dla każdej liczby pierwszej $p \geqslant 5$ mamy

$$\binom{pa}{pb} \equiv \binom{a}{b} \mod p^3.$$

Uwaga: Dowód kombinatoryczny problemu 2, który znamy wymaga mimo wszystko kilku przeliczeń, ale główny pomysł jest kombinatoryczny.

Każdy problem jest wart 0,5 punkta. Przypominamy, że rozwiązania spisane **na komputerze** należy wysyłać na adres podany na stronie internetowej kursu. Termin: niedziela 31 marca 23:59.