Funkcje arytmetyczne

Antoni Łuczak

Teoria

Definicja 1

Funkcją arytmetyczną nazywamy dowolną funkcję $f : \mathbb{N} \longrightarrow \mathbb{C}$.

Definicja 2

Mówimy, że funkcja arytmetyczna f jest multiplikatywna, jeśli dla dowolnych względnie pierwszych liczb naturalnych a, b zachodzi $f(ab) = f(a)f(b)$.

Zdefiniujmy następujące funkcje:

- $id(x) = x$
- $\mathbf{1}(x) = 1$ dla każdego x.
- $\delta(x) = \begin{cases} 1 & x = 1 \\ 0 & \text{inaczej} \end{cases}$
- $\sigma_k(x) =$ suma k-tych potęg dzielników x.
- $\tau = \sigma_0$.
- $\Omega(x) =$ liczba dzielników pierwszych x z powtórzeniami.
- $\mu(x) = \begin{cases} 0 & \text{gdy } p^2 \mid x \\ (-1)^{\Omega(x)} & \text{inaczej} \end{cases}$
- $\lambda(x) = (-1)^{\Omega(x)}$
- $\varphi =$ funkcja Eulera

Ćwiczenie 1. Udowodnij, że powyższe funkcje (poza Ω) są multiplikatywne.

Definicja 3 Splot Dirichleta

Dla dwóch funkcji arytmetycznych f, g definiujemy Splot Dirichleta

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

Twierdzenie 1

Jeżeli funkcje f, g są multiplikatywne, to $f * g$ również jest multiplikatywna.

Dowód. Weźmy dowolne względnie pierwsze liczby a, b. Mamy

$$(f*g)(ab) = \sum_{d|ab} f(d)g\left(\frac{ab}{d}\right) = \sum_{d_1|a\ d_2|b} f(d_1d_2)g\left(\frac{ab}{d_1d_2}\right) =$$

$$= \sum_{d_1|a,\ d_2|b} f(d_1)f(d_2)g\left(\frac{a}{d_1}\right)g\left(\frac{b}{d_2}\right) = \left(\sum_{d_1|a} f(d_1)g\left(\frac{a}{d_1}\right)\right)\left(\sum_{d_1|a} f(d_2)g\left(\frac{b}{d_2}\right)\right) =$$

$$(f*g)(a)(f*g)(b)$$

□

Ćwiczenie 2. Pokaż, że zbiór wszystkich funkcji arytmetycznych wraz ze splotem tworzy monoid przemienny, którego identycznością jest δ.

Ćwiczenie 3. Pokaż, że $\mathbf{1} * \mu = \delta$.

Twierdzenie 2 (Inwersja Möbiusa)

Dane są funkcje arytmetyczne f, F spełniające

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

Wtedy

$$f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right)$$

Dowód. Chcemy pokazać, że jeśli $F = \mathbf{1} * f$, to $f = F * \mu$. Z poprzednich ćwiczeń mamy łączność splotu oraz równość $\mathbf{1} * \mu = \delta$. W takim razie

$$F = \mathbf{1} * f \implies \mu * F = \mu * \mathbf{1} * f = f.$$

□

Ćwiczenie 4. Udowodnij multiplikatywną wersję Inwersji Möbiusa: Jeżeli

$$F(n) = \prod_{d|n} f(d)$$

to

$$f(n) = \prod_{d|n} f(d)^{\mu(\frac{n}{d})}$$

Zadania

Zadanie 1. Udowodnij, że dla dowolnej liczby naturalnej n zachodzi

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

Zadanie 2. Udowodnij, że

$$\sum_{d|n} \tau(d)^3 = \left(\sum_{d|n} \tau(d)\right)^2$$

Zadanie 3. (IMO Shortlist 1989 11) Ciąg (a_n) spełnia zależność

$$\sum_{d|n} a_d = 2^n.$$

Pokaż, że $n \mid a_n$.

Zadanie 4. Dla $j \in \{1, 3\}$ definiujemy

$$f_j(n) = \sum_{d|n,\ d\equiv_4 j} d.$$

Udowodnij, że dla dowolnego naturalnego n, $f_1(n) \neq f_3(n)$.

Zadanie 5. Dana jest funkcja arytmetyczna f. Udowodnij, że

$$\sum_{k=1}^{n} f(NWD(k, n)) = (f * \varphi)(n).$$

Zadanie 6. Dane są funkcje arytmetyczne g, h. Niech $f = g * h$ oraz $G(n) = \sum_{k=1}^{n} g(k)$. Udowodnij, że

$$\sum_{k=1}^{n} f(k) = \sum_{k=1}^{n} h(k) G\left(\left\lfloor \frac{n}{k} \right\rfloor\right)$$

Zadanie 7. Udowodnij, że wartość oczekiwana sumy dzielników liczby $n \in \{1, \ldots, N\}$ jest mniejsza niż N.

Zadanie 8. (72 OM-III-1) Dana jest dodatnia liczba całkowita $k \geqslant 2$. Niech $p_1, p_2, \ldots, p_k$ będą k najmniejszymi liczbami pierwszymi i niech N będzie ich iloczynem. Wykazać, że w zbiorze $\{1, 2, \ldots, N\}$ dokładnie połowa elementów jest podzielna przez nieparzyście wiele spośród liczb $p_1, \ldots, p_k$.

Zadanie 9. Dana jest liczba naturalna N. Niech $f(N)$ oznacza liczbę par uporządkowanych liczb naturalnych (a, b) takich, że

$$\frac{ab}{a+b}$$

jest całkowite i jest dzielnikiem N. Udowodnij, że $f(N)$ jest kwadratem.

Zadanie 10. (Bułgaria 1989) Wyznacz

$$\sum_{n=1}^{1989} \lambda(n) \left\lfloor \frac{1989}{n} \right\rfloor$$

Zadanie 11. Udowodnij, że wielomiany cyklotomiczne mają współczynniki całkowite.

Rozwiązania ćwiczeń

Rozwiązanie 1. Multiplikatywność funkcji id, $\mathbf{1}$ jest oczywista. Multizbiór dzielników pierwszych liczby ab to suma multizbiorów dzielników pierwszych liczb a oraz b, zatem $\Omega(ab) = \Omega(a) + \Omega(b)$. Stąd dostajemy multiplikatywność funkcji μ, λ. Teraz sprawdźmy, że funkcja σ_k jest multiplikatywna dla dowolnego k. Niech a, b będą dowolnymi względnie pierwszymi liczbami naturalnymi. Mamy

$$\sigma_k(ab) = \sum_{d|ab} d^k = \sum_{d_1|a,\ d_2|b} (d_1 d_2)^k = \left(\sum_{d_1|a} d_1^k\right)\left(\sum_{d_2|b} d_2^k\right) = \sigma_k(a)\sigma_k(b).$$

Pozostaje sprawdzić multiplikatywność funkcji φ. Niech a, b będą względnie pierwszymi liczbami naturalnymi. Na mocy CRT dla dowolnych dwóch $x \in \mathbb{Z}/(a), y \in \mathbb{Z}/(b)$ istnieje dokładnie jedno takie $n \in \mathbb{Z}/(ab)$, że $n \equiv_a x$ oraz $n \equiv_b y$. Dodatkowo takie n jest względnie pierwsze z ab wtedy i tylko wtedy, gdy x jest względnie pierwszy z a oraz y z b. W takim razie mamy bijekcję między resztami względnie pierwszymi z ab, a parami reszt względnie pierwszych z a oraz b. W szczególności $\varphi(ab) = \varphi(a)\varphi(b)$.

Rozwiązanie 2. Oczywiście splot jest przemienny. Łatwo też zauważyć, że dla dowolnych funkcji arytmetycznych f, g, h mamy

$$(f * (g * h))(n) = \sum_{abc=n} f(a)g(b)h(c) = ((f * g) * h)(n),$$

zatem splot jest również łączny. Widać też, że splatanie z δ nie zmienia funkcji.

Rozwiązanie 3. Skoro $\mathbf{1}$, μ i δ są multiplikatywne, to ich splot również jest. Wystarczy zatem pokazać, że zgadza się on z δ w potęgach liczb pierwszych. Chcemy zatem pokazać, że $(\mathbf{1} * \mu)(p^\alpha) = 0$ dla $\alpha > 1$ (to, że $(\mathbf{1} * \sigma)(1) = 1$ jest jasne). Mamy jednak

$$(\mathbf{1} * \mu)(p^\alpha) = \sum_{k=0}^{\alpha} \mu(p^k) = \mu(1) + \mu(p) = 1 - 1 = 0.$$

Rozwiązanie 4. Wystarczy zastosować standardową inwersję Möbiusa dla funkcji $\log f$, $\log F$.

Rozwiązania zadań

Rozwiązanie 1. Przepisując tezę w języku splotów, chcemy pokazać, że $\varphi * \mathbf{1} = id$. Skoro funkcje te są multiplikatywne, to wystarczy pokazać, że obie strony zgadzają się dla potęg liczb pierwszych. Mamy

$$(\varphi * \mathbf{1})(p^\alpha) = \sum_{k=0}^{\alpha} \varphi(p^k) = 1 + \sum_{k=1}^{\alpha} \left(p^k - p^{k-1}\right) = p^\alpha.$$

Rozwiązanie 2. Równość ta jest równoważna $(\mathbf{1} * \tau^3) = (\mathbf{1} * \tau)^2$, gdzie górne indeksy oznaczają potęgowanie. Oczywiście jeżeli pewna funkcja f jest multiplikatywna, to dowolna jej potęga również jest. W szczególności obie strony równania są multiplikatywne i wystarczy sprawdzić ich zgodność dla potęg liczb pierwszych:

$$(\mathbf{1} * \tau^3)(p^\alpha) = \sum_{k=0}^{\alpha} \tau(k)^3 = \sum_{k=0}^{\alpha} (k+1)^3 = \left(\sum_{k=0}^{\alpha} (k+1)\right)^2 = (\mathbf{1} * \tau)^2(p^\alpha).$$

Rozwiązanie 3. Korzystając z inwersji Möbiusa dostajemy

$$a_n = \sum_{d|n} 2^{\frac{n}{d}} \mu(d).$$

Niech p będzie nieparzystym dzielnikiem n z wykładnikiem $p-$adycznym α. Zauważmy, że jedyne niezerowe elementy w powyższej sumie odpowiadają tym d, których wszystkie dzielniki pierwsze występują w pierwszej potędze. Możemy zatem sparować każdy dzielnik d niepodzielny przez p z dzielnikiem dp. Wtedy

$$a_n = \sum_{p \text{ nie dzieli } d} \pm\left(2^{\frac{n}{d}} - 2^{\frac{n}{dp}}\right) = \sum_{p \text{ nie dzieli } d} \pm 2^{\frac{n}{dp}} \left(2^{\frac{n}{d} - \frac{n}{dp}} - 1\right).$$

Widać, że wykładniki w powyższej sumie są wielokrotnościami $p^\alpha - p^{\alpha-1} = \varphi(p^\alpha)$, zatem na mocy twierdzenia Eulera $p^\alpha \mid a_n$. Łatwo zauważyć, że $v_2(a_n) = \frac{n}{p_1 \cdots p_k}$, gdzie $p_1, \ldots, p_k$ to wszystkie dzielniki pierwsze n. W szczególności $2^{v_2(n)-1} \mid v_2(a_n) \implies v_2(a_n) \geqslant 2^{v_2(n)-1} \geqslant v_2(n)$.

Rozwiązanie 4. Zauważmy, że

$$(f_1 - f_3)(n) = n \sum_{d|n} \left(\frac{n}{d}\right)^{-1} \chi(d),$$

gdzie

$$\chi(x) = \begin{cases} 1 \text{ jeśli } x \equiv_4 1 \\ -1 \text{ jeśli } x \equiv_4 3 \\ 0 \text{ jeśli } 2 \mid x \end{cases}.$$

Wystarczy pokazać, że wyrażenie na prawo od n nigdy nie jest zerowe. Naturalnie χ oraz x^{-1} są multiplikatywne. W takim razie ich splot również jest multiplikatywny i wystarczy sprawdzić, że jest niezerowy na potęgach liczb pierwszych:

$$(\chi * x^{-1})(p^\alpha) = \sum_{k=0}^{\alpha} p^{k-\alpha}\chi(p)^k.$$

Jednak każdy wyraz tej sumy ma różny wykładnik $p-$adyczny, zatem nie możemy otrzymać zera.

Rozwiązanie 5. Mamy

$$\sum_{k=1}^{n} f(NWD(k,n)) = \sum_{k=1,\ d=NWD(k,n)}^{n} f(d) = \sum_{d|n} f(d)|\{k \leqslant n | NWD(k,n) = d\}| =$$

$$= \sum_{d|n} f(d)\varphi\left(\frac{n}{d}\right) = (f * \varphi)(n).$$

Rozwiązanie 6. Mamy

$$\sum_{k=1}^{n} f(k) = \sum_{k=1}^{n}\sum_{d|k} h(d)g\left(\frac{k}{d}\right) = \sum_{k=1}^{n} h(k) \sum_{d|k\leqslant n} g\left(\frac{k}{d}\right) = \sum_{k=1}^{n} h(k)G\left(\left\lfloor\frac{n}{k}\right\rfloor\right).$$

Rozwiązanie 7. Wartość oczekiwana sumy dzielników liczby $n \in \{1, \ldots, N\}$ jest równa

$$\frac{1}{N}\sum_{n=1}^{N}\sigma(n).$$

Mamy $\sigma = \mathbf{1} * id$ oraz $x = \sum_{k=1}^{x} \mathbf{1}(x)$ zatem na mocy poprzedniego zadania mamy

$$\frac{1}{N}\sum_{n=1}^{N}\sigma(n) = \frac{1}{N}\sum_{n=1}^{N} n\left\lfloor\frac{N}{n}\right\rfloor < N.$$

Rozwiązanie 8. Zauważmy, że teza jest równoważna z

$$\sum_{k=1}^{N}\mu(NWD(k,N)) = 0.$$

Na mocy zadania 5 powyższa suma jest równa $(\mu * \varphi)(N)$. Skoro jest to splot funkcji multiplikatywnych oraz N jest bezkwadratowe, to mamy

$$(\mu * \varphi)(N) = \prod_{p|n}(\mu * \varphi)(p).$$

W szczególności w powyższej sumie występuje

$$(\mu * \varphi)(2) = \mu(1)\varphi(2) + \mu(2)\varphi(1) = 1 - 1 = 0.$$

Rozwiązanie 9. Zapiszmy $a = dx$, $b = dy$, gdzie d to największy wspólny dzielnik a, b. Jeżeli liczby te spełniają warunek z zadania, to $x + y \mid dxy$ oraz $dxy \mid (x + y)N$. Skoro x oraz y są względnie pierwsze, to $x+y \mid d$. Zapiszmy $d = k(x+y)$. Wtedy $k(x+y)xy \mid (x+y)N \implies kxy \mid N$. Dodatkowo z każdej takiej trójki (k, x, y) jesteśmy w stanie odzyskać dobrą parę (a, b). Innymi słowy $f(N)$ to liczba przedstawień N jako iloczyn $klxy$, gdzie $x \perp y$. Aby zliczyć liczbę takich podziałów zacznijmy od wybrania $d = xy$. Liczba przedstawień d jako iloczyn liczb względnie pierwszych jest równy $2^{\omega(d)}$, gdzie $\omega(d)$ oznacza liczbę dzielników pierwszych d bez powtórzeń (na tyle sposobów wybieramy dzielniki x). Następnie k można wybrać na $\tau\left(\frac{N}{d}\right)$ sposobów. W takim razie

$$f(N) = \sum_{d|N} 2^{\omega(d)} \tau\left(\frac{n}{d}\right) = (2^{\omega} * \tau)(N).$$

W takim razie f jest multiplikatywna i wystarczy sprawdzić, że jest kwadratem dla wszystkich potęg liczb pierwszych:

$$(2^{\omega} * \tau)(p^{\alpha}) = \sum_{k=0}^{\alpha} 2^{\omega(p^k)} \tau(p^{\alpha-k}) = \alpha + 1 + 2\sum_{k=1}^{\alpha}(\alpha - k + 1) =$$

$$= \alpha + 1 + \alpha(\alpha + 1) = (\alpha + 1)^2.$$

Rozwiązanie 10. Korzystając z zadania 6 dla $h = \lambda$, $g = \mathbf{1}$ dostajemy

$$\sum_{n=1}^{1989} \lambda(n) \left\lfloor \frac{1989}{n} \right\rfloor = \sum_{n=1}^{1989} (\lambda * \mathbf{1})(n).$$

Zauważmy, że $\lambda * \mathbf{1}$ zwraca 1 jeżeli liczba jest kwadratem oraz 0 w przeciwnym wypadku. Istotnie, powyższy splot jest multiplikatywny, więc wystarczy sprawdzić naszą hipotezę dla potęg liczb pierwszych:

$$(\lambda * \mathbf{1})(p^{\alpha}) = \sum_{k=0}^{\alpha} (-1)^{\Omega(p^k)} = \sum_{k=0}^{\alpha} (-1)^k.$$

Widać, że powyższa suma jest równa 1 dla parzystych α oraz 0 dla nieparzystych. W takim razie suma z zadania zlicza liczbę kwadratów w zbiorze $\{1, \ldots, 1989\}$, czyli jest równa $\lfloor\sqrt{1989}\rfloor = 44$.

Rozwiązanie 11. Z definicji mamy

$$\Phi_n(X) = \prod_{k \perp n,\ k<n} (X - \zeta^k),$$

gdzie ζ oznacza pewien pierwotny pierwiastek z 1 stopnia n. Skoro ζ jest pierwotny, to dowolny pierwiastek z 1 stopnia n da się zapisać jako ζ^{dk}, gdzie $d \mid n$, $k \perp n$ oraz $k < \frac{n}{d}$. Taki zapis jest jednoznaczny oraz ζ^d jest $(\frac{n}{d})-$tym pierwotnym pierwiastkiem z 1. W takim razie

$$\prod_{d|n} \Phi_d(x) = x^n - 1.$$

Korzystając z multiplikatywnej inwersji Möbiusa jesteśmy w stanie wyliczyć $\Phi_n(x)$ z powyższego równania. Widać, że wykonywane operacje pozostawiają nas w ciele liczb wymiernych, zatem Φ_n ma współczynniki wymierne.