Funkcje arytmetyczne

wersja robocza

Jacek Cichoń
Politechnika Wrocławska
Wydział Podstawowych Problemów Techniki

Liczbami naturalnymi nazywany tutaj zbiór $\mathcal{N} = \{1, 2, 3 \ldots\}$. Zbiór liczb pierwszych oznaczamy przez $\mathcal{P}$. Dla $p \in \mathcal{P}$ określamy

$$\alpha_p(n) = \max\{k : p^k | n\} \ .$$

Zauważmy, że

$$n = \prod_{p|n} p^{\alpha_p(n)} = \prod_p p^{\alpha_p(n)}$$

Uwaga: stosujemy następującą konwencję: $\prod_p f(p) = \prod_{p \in \mathcal{P}} f(p)$ oraz $\sum_p f(p) = \sum_{p \in \mathcal{P}} f(p)$.

Następujące, łatwe do udowodnienia, wzory często się przydają w rozważaniach teoretycznych (w praktyce zaś mniej, bo wymagają znajomości rozkładu liczb na czynniki pierwsze):

$$\mathrm{nwd}(n, m) = \prod_p p^{\min\{\alpha_p(n), \alpha_p(m)\}}$$

oraz

$$\mathrm{nww}(n, m) = \prod_p p^{\max\{\alpha_p(n), \alpha_p(m)\}} \ .$$

Ze wzorów tych wynikają, na przykład, natychmiast następujące wzory:

$$\mathrm{nwd}(a, b, c) = \mathrm{nwd}(a, \mathrm{nwd}(b, c)) = \mathrm{nwd}(\mathrm{nwd}(a, b), c) \ .$$

1 Funkcje arytmetyczne

Funkcjami arytmetycznymi nazywamy funkcje o dziedzinie $\mathcal{N}$ o wartościach w zbiorze liczb zespolonych. Zbiór wszystkich funkcji arytmetycznych oznaczmy tutaj symbolem $\mathbb{AF}$. Na zbiorze tym rozważamy działanie $+$ określone wzorem $(f + g)((n) = f(n) + g(n)$. Struktura $(\mathbb{AF}, +)$ jest oczywiście grupą abelową z elementem neutralnym $\mathbf{0}$ (funkcją tożsamościowo równą zero).

Rozważać możemy operację mnożenia funkcji arytmetycznych określoną wzorem $(f \cdot g)((n) = f(n) \cdot g(n)$. Jednakże ta operacja nie ma ciekawych własności. Zamiast tego zajmować będziemy się splotem Dirichletta:

Definicja 1 (Splot Dirichletta)**.** *Niech $f, g \in \mathbb{AF}$. Splotem Dirichletta funkcji f i g nazywamy funkcję $f \star g \in \mathbb{AF}$ okresloną wzorem*

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

Zauważmy, że splot $f \star g$ możemy zapisać w równoważny sposób:

$$\sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d) = \sum_{d_1 d_2 = n} f(d_1) g(d_2) \ .$$

Z obserwacji tej wynika, że splot Dirichletta jest przemienny, czyli, że $f \star g = g \star f$. Bez trudu możemy pokazać, że $(f + g) \star h = (f \star h) + (g \star h)$.

Lemat 1. $(f \star g) \star h = f \star (g \star h)$

Dowód.

$$((f \star g) \star h)(n) = \sum_{d_2 d_3 = n} (f \star g)(d_2) h(d_3) = \sum_{d_2 d_3 = n} \sum_{k \cdot l = d_2} f(k) g(l) h(d_3) =$$
$$\sum_{k \cdot l = d_2} \sum_{d_2 d_3 = n} f(k) g(l) h(d_3) = \sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3) = (f \star (g \star h))(n) \ .$$

□

Niech

$$\delta(x) = \begin{cases} 1 & : x = 1 \\ 0 & : x > 0 \end{cases}$$

Dla dowolnej funkcji $f \in \mathbb{AF}$ mamy

$$(f \star \delta)(n) = \sum_{kl = n} f(k) \delta(l) = f(n),$$

więc δ jest neutralnym splotu Dirichletta.

Twierdzenie 1. *Struktura $(\mathbb{AF}, +, \star)$ jest pierścieniem przemiennym, z elementem neutralnym δ, bez dzielników zera. Funkcja $f \in \mathbb{AF}$ jest odwracalna wtedy i tylko wtedy, gdy $f(1) \neq 0$.*

Dowód. Pokażmy, że w strukturze $\mathbb{AF}$ nie ma dzielników zera. Niech bowiem $f, g \in \mathbb{AF} \setminus \{\mathbf{0}\}$. Niech $a = \min\{k \in \mathcal{N} : f(k) \neq 0\}$ oraz $f = \min\{k \in \mathcal{N} : g(k) \neq 0\}$. Wtedy

$$(f \star g)(ab) = \sum_{kl = ab} f(k) g(l) = \sum_{\substack{kl = ab \\ k \geqslant a, l \geqslant b}} f(k) g(l) = f(a) g(b) \neq 0 \ ,$$

więc $f \star g \neq \mathbf{0}$.

Zauważmy teraz, że jeśli $f(1) = 0$ to dla dowolnej funkcji $g \in \mathbb{AF}$ mamy $(f \star g)(1) = 0$, więc z pewnością $f \star g \neq \delta$, a więc f nie jest odwracalna. Załózmy więc, że $f(1) \neq 0$. Połóżmy $g(1) = f(1)^{-1}$ oraz indukcyjnie, dla $n > 1$

$$g(n) = -f(1)^{-1} \sum_{\substack{kl = n \\ l < n}} f(k) g(l) \ .$$

Wtedy $(f \star g)(1) = 1$ oraz dla $n > 1$ mamy

$$(f \star g)(n) = \sum_{kl=n} f(k)g(l) = \sum_{\substack{kl=n \\ l<n}} f(k)g(l) + f(1)g(n) = 0.$$

Zatem dla tak określonej funkcji g mamy $f \star g = \delta$. $\square$

2 Funkcje multiplikatywne

Definicja 2. *Funkcję $f : \mathcal{N} \to \mathbb{R}$ nazywamy multiplikatywną jeśli $f \neq \mathbf{0}$ oraz*

$$(\forall n, m \in \mathcal{N})(\mathrm{nwd}(n, m) = 1 \to f(nm) = f(n)f(m)) \ .$$

Zbiór funkcji multiplikatywnych ozanczać będziemy symbolem Mult.

Jeśli $f \in \mathrm{Mult}$ to $f(1) \neq 0$: rzeczywiście, gdyby $f(0) = 0$ to dla dowolnego n mielibyśmy $f(n) = f(1 \cdot n) = f(1)f(n) = 0$. Co więcej, jeśli $f \in \mathrm{Mult}$, to $f(1) = f(1 \cdot 1) = f(1)f(1)$, więc $f(1) = 1$.

Definicja 3. *Funkcję $f : \mathcal{N} \to \mathbb{R}$ nazywamy addytywna jeśli f nie jest równa funkcji zerowej oraz*

$$(\forall n, m \in \mathcal{N})(\mathrm{nwd}(n, m) = 1 \to f(nm) = f(n) + f(m))$$

Zauważmy, że

$$\prod_p p^{\alpha_p(n \cdot m)} = n \cdot m = \prod_p p^{\alpha_p(n)} \cdot \prod_p p^{\alpha_p(m)} =$$
$$\prod_p p^{\alpha_p(n)} p^{\alpha_p(m)} = \prod_p p^{\alpha_p(n)+\alpha_p(m)}$$

Zatem, dla dowolnego $p \in \mathcal{P}$, funkcja α_p jest addytywna.

Istnieje bliski związek między funkcjami multiplikatywnymi i addytywnymi. Mianowicie, jeśli f jest addytywna, to funkcja $g(x) = e^{g(x)}$ jest dodatnią funkcją multiplikatywną. Odwrotnie, jeśli g jest dodatnią funkcją multilikatywną, to funkcja $f(x) = \ln(g(x))$ jest funkcją addytywną.

Załóżmy, że f jest funkcją multiplikatywną oraz, że mamy wyznaczyć wartość funkcji $f(n)$. Do zadania tego może podejść w następujący sposób: poszukujemy najmniejszą liczbę naturalną $k \geqslant 2$ takiej, że $k|n$. Liczba ta musi być liczbą pierwszą. Znajdujemy następnie największa liczbę a taką, że $p^a|n$. Wtedy $\mathrm{nwd}(p^a, \frac{n}{p^a}) = 1$ więc $f(n) = f(p^a)f(\frac{n}{p^a})$.
Ta prosta uwaga przydaje się w wielu przypadkach do pisania efektywnego kodu procedur służąych do wyznaczania wartości fukcji multiplikatywneych.

Twierdzenie 2. *Jeśli f jest funkcją multiplikatywną zaś g jest funkcją addytywną, to*

$$f(n) = \prod_{p|n} f(p^{\alpha_p(n)}), \quad g(n) = \sum_p g(p^{\alpha_p(n)}) \ .$$

Dowód. Zauważmy, że $n = \prod_{p|n} p^{\alpha_p(n)}$. Zatem

$$f(n) = f\left(\prod_{p|n} p^{\alpha_p(n)}\right) = \prod_{p|n} f(p^{\alpha_p(n)}) \ .$$

□

Wniosek 1. *Złóżmy, że f o g są multiplikatywne. Jeśli $(\forall p \in \mathcal{P})(\forall k \in \mathcal{N})(f(p^k) = g(p^k)$ to $f = g$.*

2.1 Przykłady

- Funkcja **1** tożsamościowo równa 1 jest multiplikatywna
- Funkcja $\mathrm{Id}(n) = n$ jest multiplikatywna
- Funkcja $\mathrm{Id}^k(n) = n^k$ jest multiplikatywna
- Funkcja $\omega(n) = \sum_{p|n} 1$ (czyli liczba różnych dzielników pierwszych liczby n) jest addytywna
- Funkcja Ω określona wzorem $\Omega(\prod_{p|n} p^{\alpha_p(n)}) = \sum_{p|n} \alpha_p(n)$ jest addytywna

2.2 Funkcja Eulera

Definicja 4. $\phi(n) = |\{k \leqslant n : \mathrm{nwd}(k, n) = 1\}|$.

Twierdzenie 3. *Funkcja ϕ jest multiplikatywna.*

Dowód. Załóżmy, że $\mathrm{nwd}(a, b) = 1$. Niech $A = \{x \leqslant a : \mathrm{nwd}(x, a) = 1\}$, $B = \{y \leqslant b : \mathrm{nwd}(y, b) = 1\}$ oraz $C = \{z \leqslant ab : \mathrm{nwd}(z, ab) = 1\}$ Oczywiście $|A| = \phi(a)$, $|B| = \phi(b)$ oraz $|C| = \phi(ab)$. Niech

$$f(x, y) = (bx + ay) \mod ab \ .$$

Rozważmy zbiór

$$R = \{f(x, y) : x \in A \wedge y \in B\}$$

(1) Zaczniemy od pokazania, że $R \subseteq C$. Załóżmy, że $z \in R$. Wtedy $z = bx + ay + kab$ dla pewnej liczby k oraz pewnych x, y takich, że $\mathrm{nwd}(x, a) = 1$ oraz $\mathrm{nwd}(y, b) = 1$. Pokażemy, że $\mathrm{nwd}(z, ab) = 1$. Załóżmy, że $p \in \mathcal{P}$ oraz $p|ab$ i $p|z$. Możemy założyć, że $p|a$. Lecz $bx = z - (ay + ab)$ więc $p|bx$. Gdyby $p|b$, to $\mathrm{nwd}(a, b) > 1$. Zatem $p|x$. Lecz wtedy $\mathrm{nwd}(x, a) > 1$, co jest sprzeczne z tym, że $x \in A$.

(2) Pokażemy teraz, że $|R| = |A| \cdot |B|$. Załóżmy bowiem, że $(x_1, y_1) \in A \times B$ $(x_2, y_2) \in A \times B$ oraz $f(x_1, y_1) = f(x_2, y_2)$. Ustalmy liczby k_1 i k_2 takie, że $f(x_1, y_1) = bx_1 + ay_1 + k_1ab$ oraz $f(x_2, y_2) = bx_2 + ay_2 + k_2ab$. Wtedy

$$bx_1 + ay_1 + k_1ab = bx_2 + ay_2 + k_2ab \ ,$$

więc

$$b(x_1 - x_2) + a(y_1 - y_2) = (k_2 - k_1)ab \ .$$

Widzimy, że $a|b(x_1 - x_2)$. Lecz $\mathrm{nwd}(a, b) = 1$, więc $a|(x_1 - x_2)$, zatem $x_1 = x_2$ Podobnie pokazujemy, że $y_1 = y_2$. Zatem f jest funkcją różnowartościową.

(3) Pokażemy teraz, że $C \subseteq R$. Ustalmy takie liczby całkowite u i v, że $au + bv = 1$. Załóżmy, że $c \in C$. Wtedy $c = bX + aY$, gdzie $Y = cu$ i $X = cv$. Twierdzimy, że $\mathrm{nwd}(X, a) = 1$. Załóżmy, że $p \in \mathcal{P}$ oraz $p|X$ i $p|a$. Wtedy $p|c$. Więc $p|c$ i $p|ab$, więc $\mathrm{nwd}(c, ab) > 1$, co jest niemożliwe. Podobnie pokazujemy, że $\mathrm{nwd}(Y, b) = 1$. Niech $x = X \mod a$ oraz $y = Y \mod b$. Wtedy $x \in A$, $y \in B$ oraz $c = b(x+ka)+a(y+lb) = bx+ay+(k+l)ab$ dla pewnych liczb całkowitych k i l, więc $c = f(x, y)$.

Z (1) oraz (3) wynika, że $|C| = |R|$. Z (2) wynika, że $|R| = |A \times B|$. Zatem $\phi(ab) = |C| = |A| \cdot |B| = \phi(a)\phi(b)$. □

2.3 Splot Dirichleta funkcji multiplikatywnych

Twierdzenie 4. *Jeśli $f, g \in \mathbb{AF}$ są multiplikatywne, to $f \star g$ jest multiplikatywna.*

Dowód. Zauważmy najpierw, że jeśli $\mathrm{nwd}(m, n) = 1$ oraz $d|mn$, to istnieją takie liczby d_1, d_2, że $d_1|m$, $d_2|n$ oraz $d = d_1 d_2$.

Zauważmy teraz, że $\mathrm{nwd}(m, n) = 1$. Wtedy

$$(f \star g)(n) = \sum_{kl=mn} f(k)g(l) = \sum_{\substack{k_1|m, k_2|n \\ l_1|m, l_2|n \\ k_1 l_1 = m \\ k_2 l_2 = n}} f(k_1 l_1)g(k_2 l_2) =$$

$$\sum_{\substack{k_1|m, k_2|m \\ l_1|n, l_2|n \\ k_1 l_1 = m \\ k_2 l_2 = n}} f(k_1)f(l_1)g(k_2)g(l_2) = \sum_{k_1 l_1 = m} f(k_1)f(l_1) \cdot \sum_{k_2 l_2 = n} g(k_2)g(l_2) =$$

$$(f \star g)(m) \cdot (f \star g)(n).$$

□

Wniosek 2. *Funkcja $\mathbf{d}(n) = \sum_{d|n} 1$ jest multiplikatywna.*

Dowód. Mamy

$$(\mathbf{1} \star \mathbf{1})(n) = \sum_{d|n} (1)\mathbf{1}(\frac{n}{d}) = \sum_{d|n} 1 = \mathbf{d}(n) \ .$$

□

Wniosek 3. *Funkcja $\sigma(n) = \sum_{d|n} d$ jest multiplikatywna.*

Dowód. Mamy

$$(\mathrm{Id} \star \mathbf{1})(n) = \sum_{d|n} \mathrm{Id}(d)\mathbf{1}(\frac{n}{d}) = \sum_{d|n} d = \sigma(n) \ .$$

□

Wniosek 4. *Funkcja* $\sigma_k(n) = \sum_{d|n} d^k$ *jest multiplikatywna.*

Dowód wynika z oczywistej równości $\sigma_k = \mathrm{Id}^k \star \mathbf{1}$.

2.4 Funkcja Mobiusa

$$\mu(n) = \begin{cases} 1 & : n = 1 \\ 0 & : (\exists p \in \mathcal{P})(p^2|n) \\ (-1)^k & : n = p_1 \cdot p_2 \cdots p_k \end{cases}$$

A oto podstawowa własność funkcji Mobiusa:

Twierdzenie 5. $\mu \star \mathbf{1} = \delta$

Dowód. Obie strony są multiplikatywne. Wystarczy je sprawdzić dla liczb postaci p^k.

$$(\mu\star\mathbf{1})(p^k) = \sum_{d|p^k} \mu(d) = \mu(1)+\mu(p)+\mu(p^2)+\ldots\mu(p^k) = \mu(1)+\mu(p) = 1-1 = 0\ .$$

□

Twierdzenie 6. *Jeśli* f *jest multiplikatywna, to*

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|d}(1-f(p)), \quad \sum_{d|n} \mu(d)^2 f(d) = \prod_{p|d}(1+f(p))\ .$$

Dowód. Zauważmy, że funkcja $h(n) = \mu(n)f(n)$ jest multiplikatywna oraz, że $(h \star \mathbf{1})(n) = \sum_{d|n} \mu(d)f(d)$, więc lewa strona pierwszej równości jest multiplikatywna. Prawa jest również multiplikatywne (to wynika wprost z definicji). Równość wystarczy więc sprawdzić dla liczb postaci p^k (patrz Wniosek 1):

$$\sum_{d|p^k} \mu(d)f(d) = \mu(1)f(1) + \mu(p)f(p) = 1 - p\ .$$

Drugą równość dowodzi się podobnie. □

2.5 Jawny wzór na funkcję Eulera

Twierdzenie 7. $\phi(n) = n\prod_{p|n}(1-\frac{1}{p})$

Dowód. Obie strony są multiplikatywne. Sprawdzimy rowność dla liczb postaci p^k. Zauważmy, że

$$\{a \in \mathcal{N} : a \leqslant n : \mathrm{nwd}(a, p^k) > 1\} = \{p, 2\cdot p, 3\cdot p, \ldots, p^{k-1}\cdot p\}\ ,$$

więc

$$\phi(p^k) = p^k - p^{k-1} = p^k(1-\frac{1}{p})\ .$$

□

Wniosek 5. $\varphi = \mu \star \mathrm{Id}$

Dowód. Niech $f(n) = \frac{1}{n}$. To jest funkcja multiplikatywna. Z 6 mamy

$$(\mu \star \mathrm{Id})(n) = \sum_{d|n} \mu(d)\mathrm{Id}(\frac{n}{d}) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n} \mu(d)f(d) =$$
$$n\prod_{p|n}(1 - f(d)) = n\prod_{p|d}(1 - \frac{1}{p}) = \phi(n) \ .$$

□

Wniosek 6. $\varphi \star \mathbf{1} = \mathrm{Id}$

Dowód. Z równości $\varphi = \mu \star \mathrm{Id}$ otrzymujemy

$$\varphi \star \mathbf{1} = \mu \star \mathrm{Id} \star \mathbf{1} = (\mathbf{1}\mu\star)\mathrm{Id} = \delta \star \mathrm{Id} = \mathrm{Id} \ .$$

□

Ostatnią równość możemy zapisać w następujące postaci

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

A oto alternatywny, elementarny dowód tej równości:

$$n = |\{\frac{k}{n} : 1 \leqslant k \leqslant n\}| = |\bigcup_{d|n}\{k : \mathrm{nwd}(k,d) = 1\}| = \sum_{d|n} |\{k : \mathrm{nwd}(k,d) = 1\}| = \sum_{d|n} \phi(n) \ .$$