O funkcjach arytmetycznych. Na podstawie: „Teoria Liczb”, BM – tom 50, Władysława Narkiewicza

Dominik Bojko
Department of Computer Science
Faculty of Fundamental Problems of Technology
Wrocław University of Science and Technology
Poland

3rd of March 2020

Władysław Narkiewicz

Urodzony w 1936 r., zajmował się teorią liczb, algebrą i historią matematyki, prof. zw. od 1976 r. Jego Alma Mater to UWr, gdzie był kierownikiem IM i dziekanem WMiF. Od 14 lat na emeryturze.

Funkcje arytmetyczne $\mathcal{A}$

Funkcja arytmetyczna to dowolna funkcja $f : \mathbb{N} \to \mathbb{C}$.
Najczęściej $f[\mathbb{N}] \subset \mathbb{Z}$. Czasem pozwala się, aby dziedzina była $\mathbb{N}_0$.

Funkcje arytmetyczne $\mathcal{A}$

Funkcja arytmetyczna to dowolna funkcja $f : \mathbb{N} \to \mathbb{C}$.
Najczęściej $f[\mathbb{N}] \subset \mathbb{Z}$. Czasem pozwala się, aby dziedzina była $\mathbb{N}_0$.

Przykłady:

1. $e(n) = 1_1(n) = \delta_{1,n}$,

Funkcje arytmetyczne $\mathcal{A}$

Funkcja arytmetyczna to dowolna funkcja $f : \mathbb{N} \to \mathbb{C}$.
Najczęściej $f[\mathbb{N}] \subset \mathbb{Z}$. Czasem pozwala się, aby dziedzina była $\mathbb{N}_0$.

Przykłady:

1. $e(n) = 1_1(n) = \delta_{1,n}$,
2. $I(n) \equiv 1$,

Funkcje arytmetyczne $\mathcal{A}$

Funkcja arytmetyczna to dowolna funkcja $f : \mathbb{N} \to \mathbb{C}$.

Najczęściej $f[\mathbb{N}] \subset \mathbb{Z}$. Czasem pozwala się, aby dziedzina była $\mathbb{N}_0$.

Przykłady:

1. $e(n) = 1_1(n) = \delta_{1,n}$,
2. $I(n) \equiv 1$,
3. $N(n) = n = id(n)$,

Funkcje arytmetyczne $\mathcal{A}$

Funkcja arytmetyczna to dowolna funkcja $f : \mathbb{N} \to \mathbb{C}$.
Najczęściej $f[\mathbb{N}] \subset \mathbb{Z}$. Czasem pozwala się, aby dziedzina była $\mathbb{N}_0$.

Przykłady:

1. $e(n) = 1_1(n) = \delta_{1,n}$,
2. $I(n) \equiv 1$,
3. $N(n) = n = id(n)$,
4. $d(n) = \# D_n = \sum_{d|n} 1, \qquad (D_n = \{d : 1 \leqslant d \leqslant n, d|n\})$,

Funkcje arytmetyczne $\mathcal{A}$

Funkcja arytmetyczna to dowolna funkcja $f : \mathbb{N} \to \mathbb{C}$.
Najczęściej $f[\mathbb{N}] \subset \mathbb{Z}$. Czasem pozwala się, aby dziedzina była $\mathbb{N}_0$.

Przykłady:

1. $e(n) = 1_1(n) = \delta_{1,n}$,
2. $I(n) \equiv 1$,
3. $N(n) = n = id(n)$,
4. $d(n) = \# D_n = \sum_{d|n} 1, \qquad (D_n = \{d : 1 \leqslant d \leqslant n, d|n\})$,
5. $\sigma(n) = \sum_{d \in D_n} d = \sum_{d|n} d$,

Funkcje arytmetyczne $\mathcal{A}$

Funkcja arytmetyczna to dowolna funkcja $f : \mathbb{N} \to \mathbb{C}$.
Najczęściej $f[\mathbb{N}] \subset \mathbb{Z}$. Czasem pozwala się, aby dziedzina była $\mathbb{N}_0$.

Przykłady:

1. $e(n) = 1_1(n) = \delta_{1,n}$,
2. $I(n) \equiv 1$,
3. $N(n) = n = id(n)$,
4. $d(n) = \#D_n = \sum_{d|n} 1, \qquad (D_n = \{d : 1 \leqslant d \leqslant n, d|n\})$,
5. $\sigma(n) = \sum_{d \in D_n} d = \sum_{d|n} d$,
6. Tocjent Eulera: $\varphi(n) = \#\{x \leqslant n : \mathrm{NWD}(x, n) = 1\}$.

Funkcje arytmetyczne $\mathcal{A}$

Funkcja arytmetyczna to dowolna funkcja $f : \mathbb{N} \to \mathbb{C}$.
Najczęściej $f[\mathbb{N}] \subset \mathbb{Z}$. Czasem pozwala się, aby dziedzina była $\mathbb{N}_0$.

Przykłady:

1. $e(n) = 1_1(n) = \delta_{1,n}$,
2. $I(n) \equiv 1$,
3. $N(n) = n = id(n)$,
4. $d(n) = \#D_n = \sum_{d|n} 1, \qquad (D_n = \{d : 1 \leqslant d \leqslant n, d|n\})$,
5. $\sigma(n) = \sum_{d \in D_n} d = \sum_{d|n} d$,
6. Tocjent Eulera: $\varphi(n) = \#\{x \leqslant n : \mathrm{NWD}(x, n) = 1\}$.
7. Funkcja Möbiusa:

$$\mu(n) = \begin{cases} 0 & \text{, gdy } (\exists p \in \mathcal{P}rime)\ p^2|n, \quad \text{n – kwadratowe} \\ 1 & \text{, gdy } n = 1, \\ (-1)^k & \text{, gdy } n = \prod_{i=1}^{k} p_i, \text{ gdzie } p_i \text{ – różne liczby pierwsze.} \end{cases}$$

Grupa

Grupa to struktura algebraiczna $(A, 0, +)$ typu $(0, 2)$, która spełnia własności:

1. Łączność $\quad x + (y + z) = (x + y) + z,$
2. Istnienie el. neutralnego $\quad 0 + x = x = x + 0,$
3. Dla każdego elementu x istnieje element odwrotny x^{-1} względem działania $+$. $\quad x + x^{-1} = 0 = x^{-1} + x.$

Jeśli w dodatku grupa jest przemienna, to $x + y = y + x$.

Grupa

Grupa to struktura algebraiczna $(A, 0, +)$ typu $(0, 2)$, która spełnia własności:

1. Łączność $\quad x + (y + z) = (x + y) + z,$
2. Istnienie el. neutralnego $\quad 0 + x = x = x + 0,$
3. Dla każdego elementu x istnieje element odwrotny x^{-1} względem działania $+$. $\quad x + x^{-1} = 0 = x^{-1} + x.$

Jeśli w dodatku grupa jest przemienna, to $x + y = y + x$.
Przykłady:

1. $(\mathbb{Z}, 0, +)$

Grupa

Grupa to struktura algebraiczna $(A, 0, +)$ typu $(0, 2)$, która spełnia własności:

1. Łączność $\quad x + (y + z) = (x + y) + z,$
2. Istnienie el. neutralnego $\quad 0 + x = x = x + 0,$
3. Dla każdego elementu x istnieje element odwrotny x^{-1} względem działania $+$. $\quad x + x^{-1} = 0 = x^{-1} + x.$

Jeśli w dodatku grupa jest przemienna, to $x + y = y + x$.

Przykłady:

1. $(\mathbb{Z}, 0, +)$
2. $(\mathbb{Z}_n, 0, +_n)$,

Grupa

Grupa to struktura algebraiczna $(A, 0, +)$ typu $(0, 2)$, która spełnia własności:

1. Łączność $\quad x + (y + z) = (x + y) + z,$
2. Istnienie el. neutralnego $\quad 0 + x = x = x + 0,$
3. Dla każdego elementu x istnieje element odwrotny x^{-1} względem działania $+$. $\quad x + x^{-1} = 0 = x^{-1} + x.$

Jeśli w dodatku grupa jest przemienna, to $x + y = y + x$.

Przykłady:

1. $(\mathbb{Z}, 0, +)$
2. $(\mathbb{Z}_n, 0, +_n),$
3. $(\mathbb{Z}_n^*, \cdot_n).$

Grupa

Grupa to struktura algebraiczna $(A, 0, +)$ typu $(0, 2)$, która spełnia własności:

1. Łączność $\quad x + (y + z) = (x + y) + z,$
2. Istnienie el. neutralnego $\quad 0 + x = x = x + 0,$
3. Dla każdego elementu x istnieje element odwrotny x^{-1} względem działania $+$. $\quad x + x^{-1} = 0 = x^{-1} + x.$

Jeśli w dodatku grupa jest przemienna, to $x + y = y + x$.

Przykłady:

1. $(\mathbb{Z}, 0, +)$
2. $(\mathbb{Z}_n, 0, +_n)$,
3. $(\mathbb{Z}_n^*, \cdot_n)$.
4. $\#\mathbb{Z}_n^* = \varphi(n)$.

Pierścień

Pierścień to struktura algebraiczna $(A, 0, 1, +, \cdot)$ typu $(0, 0, 2, 2)$, która spełnia własności:

1. $(A, 0, +)$ jest grupą przemienną.
2. $\cdot$ jest łączne $\quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. Elementem neutralnym $\cdot$ jest 1 $\quad x \cdot 1 = x = 1 \cdot x$.
4. Zachodzą rozdzielności $\cdot$ względem $+$ $\quad x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Pierścień

Pierścień to struktura algebraiczna $(A, 0, 1, +, \cdot)$ typu $(0, 0, 2, 2)$, która spełnia własności:

1. $(A, 0, +)$ jest grupą przemienną.
2. $\cdot$ jest łączne $\quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. Elementem neutralnym $\cdot$ jest 1 $\quad x \cdot 1 = x = 1 \cdot x$.
4. Zachodzą rozdzielności $\cdot$ względem $+$ $\quad x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Przykłady:

1. $(\mathbb{Z}, 0, 1, +, \cdot)$, nie istnieją z reguły elementy odwrotne względem $\cdot$,

Pierścień

Pierścień to struktura algebraiczna $(A, 0, 1, +, \cdot)$ typu $(0, 0, 2, 2)$, która spełnia własności:

1. $(A, 0, +)$ jest grupą przemienną.
2. $\cdot$ jest łączne $\quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. Elementem neutralnym $\cdot$ jest 1 $\quad x \cdot 1 = x = 1 \cdot x$.
4. Zachodzą rozdzielności $\cdot$ względem $+$ $\quad x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Przykłady:

1. $(\mathbb{Z}, 0, 1, +, \cdot)$, nie istnieją z reguły elementy odwrotne względem $\cdot$,
2. $(\mathbb{Z}_n, 0, 1, +_n, \cdot_n)$,

Pierścień

Pierścień to struktura algebraiczna $(A, 0, 1, +, \cdot)$ typu $(0, 0, 2, 2)$, która spełnia własności:

1. $(A, 0, +)$ jest grupą przemienną.
2. $\cdot$ jest łączne $\quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. Elementem neutralnym $\cdot$ jest 1 $\quad x \cdot 1 = x = 1 \cdot x$.
4. Zachodzą rozdzielności $\cdot$ względem $+$ $\quad x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Przykłady:

1. $(\mathbb{Z}, 0, 1, +, \cdot)$, nie istnieją z reguły elementy odwrotne względem $\cdot$,
2. $(\mathbb{Z}_n, 0, 1, +_n, \cdot_n)$,
3. $(\mathbb{C}, 0, 1, +, \cdot)$,

Pierścień

Pierścień to struktura algebraiczna $(A, 0, 1, +, \cdot)$ typu $(0, 0, 2, 2)$, która spełnia własności:

1. $(A, 0, +)$ jest grupą przemienną.
2. $\cdot$ jest łączne $\quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. Elementem neutralnym $\cdot$ jest 1 $\quad x \cdot 1 = x = 1 \cdot x$.
4. Zachodzą rozdzielności $\cdot$ względem $+$ $\quad x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Przykłady:

1. $(\mathbb{Z}, 0, 1, +, \cdot)$, nie istnieją z reguły elementy odwrotne względem $\cdot$,
2. $(\mathbb{Z}_n, 0, 1, +_n, \cdot_n)$,
3. $(\mathbb{C}, 0, 1, +, \cdot)$,
4. $(\mathbb{R}[x], 0, 1, +, \cdot)$, (tu też),

Pierścień

Pierścień to struktura algebraiczna $(A, 0, 1, +, \cdot)$ typu $(0, 0, 2, 2)$, która spełnia własności:

1. $(A, 0, +)$ jest grupą przemienną.
2. $\cdot$ jest łączne $\quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. Elementem neutralnym $\cdot$ jest 1 $\quad x \cdot 1 = x = 1 \cdot x$.
4. Zachodzą rozdzielności $\cdot$ względem $+$ $\quad x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Przykłady:

1. $(\mathbb{Z}, 0, 1, +, \cdot)$, nie istnieją z reguły elementy odwrotne względem $\cdot$,
2. $(\mathbb{Z}_n, 0, 1, +_n, \cdot_n)$,
3. $(\mathbb{C}, 0, 1, +, \cdot)$,
4. $(\mathbb{R}[x], 0, 1, +, \cdot)$, (tu też),
5. $(\mathcal{A}, 0, 1, +, \cdot)$.

Sploty

Klasyczny splot funkcji $f, g \in L^1(\mathbb{R})$ definiujemy jako

$$f * g(x) = \int_{\mathbb{R}} f(t)g(x-t)dt \ .$$

Użyteczny splot pierścienia w kategorii dystrybucji (przestrzeń Sobolewa).

Sploty

Klasyczny splot funkcji $f, g \in L^1(\mathbb{R})$ definiujemy jako

$$f * g(x) = \int\limits_{\mathbb{R}} f(t)g(x-t)dt \ .$$

Użyteczny splot pierścienia w kategorii dystrybucji (przestrzeń Sobolewa). Analogicznie można zdefiniować dyskretny splot funkcji $f, g : \mathbb{Z} \to \mathbb{C}$:

$$f * g(n) = \sum_{k=-\infty}^{\infty} f(k)g(n-k) \qquad [\Delta(k) \equiv 1]$$

Tutaj $(\mathbb{C}^{\mathbb{Z}}, \mathbf{0}, \delta_{0,n}, +, *)$ jest pierścieniem.

Sploty

Klasyczny splot funkcji $f, g \in L^1(\mathbb{R})$ definiujemy jako

$$f * g(x) = \int_{\mathbb{R}} f(t)g(x-t)dt \ .$$

Użyteczny splot pierścienia w kategorii dystrybucji (przestrzeń Sobolewa).
Analogicznie można zdefiniować dyskretny splot funkcji $f, g : \mathbb{Z} \to \mathbb{C}$:

$$f * g(n) = \sum_{k=-\infty}^{\infty} f(k)g(n-k) \qquad [\Delta(k) \equiv 1]$$

Tutaj $(\mathbb{C}^{\mathbb{Z}}, \mathbf{0}, \delta_{0,n}, +, *)$ jest pierścieniem.
Ograniczając zbiór $\mathbb{Z}$ do $\{0, 1, 2, \ldots, n\}$ dostajemy splot Abela $\times$.

Splot Dirichleta

Dla funkcji arytmetycznych, możemy zdefiniować splot Dirichleta:

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

Zatem $(\mathcal{A}, \mathbf{0}, e(n), +, *)$ jest również pierścieniem
(bez dzielników 0 i f^{-1} istnieje $\Leftrightarrow f(1) \neq 0$).

Splot Dirichleta

Dla funkcji arytmetycznych, możemy zdefiniować splot Dirichleta:

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

Zatem $(\mathcal{A}, 0, e(n), +, *)$ jest również pierścieniem
(bez dzielników 0 i f^{-1} istnieje $\Leftrightarrow f(1) \neq 0$).

1. $I * I(n) = \sum_{d|n} 1 \cdot 1 = d(n)$

Splot Dirichleta

Dla funkcji arytmetycznych, możemy zdefiniować splot Dirichleta:

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

Zatem $(\mathcal{A}, 0, e(n), +, *)$ jest również pierścieniem (bez dzielników 0 i f^{-1} istnieje $\Leftrightarrow f(1) \neq 0$).

1. $I * I(n) = \sum_{d|n} 1 \cdot 1 = d(n)$
2. $I * N(n) = \sum_{d|n} \frac{n}{d} = \sum_{d|n} d = \sigma(n)$

Funkcje addytywne i multiplikatywne

Jeśli dla każdej pary liczb względnie pierwszych n, m zachodzi

$$f(mn) = f(m) + f(n)$$

to taka funkcje nazywamy addytywną.

Funkcje addytywne i multiplikatywne

Jeśli dla każdej pary liczb względnie pierwszych n, m zachodzi

$$f(mn) = f(m) + f(n)$$

to taka funkcje nazywamy addytywną.
Podobnie jeśli dla takich par

$$f(mn) = f(m)f(n)$$

to taką funkcję nazywamy multiplikatywną. Zbiór funkcji multiplikatywnych będziemy oznaczać przez $\mathcal{M}$.

Funkcje addytywne i multiplikatywne

Jeśli dla każdej pary liczb względnie pierwszych n, m zachodzi

$$f(mn) = f(m) + f(n)$$

to taka funkcje nazywamy addytywną.
Podobnie jeśli dla takich par

$$f(mn) = f(m)f(n)$$

to taką funkcję nazywamy multiplikatywną. Zbiór funkcji multiplikatywnych będziemy oznaczać przez $\mathcal{M}$.
Jeśli natomiast te warunki nie zależą od względnej pierwszości, to dodajemy określenie „całkowicie". Przykładowo, $N(n) = n$ jest całkowicie multiplikatywna.

Funkcje addytywne i multiplikatywne

Jeśli dla każdej pary liczb względnie pierwszych n, m zachodzi

$$f(mn) = f(m) + f(n)$$

to taka funkcje nazywamy addytywną.
Podobnie jeśli dla takich par

$$f(mn) = f(m)f(n)$$

to taką funkcję nazywamy multiplikatywną. Zbiór funkcji multiplikatywnych będziemy oznaczać przez $\mathcal{M}$.
Jeśli natomiast te warunki nie zależą od względnej pierwszości, to dodajemy określenie „całkowicie". Przykładowo, $N(n) = n$ jest całkowicie multiplikatywna.

Fact

Jeśli f jest addytywna, to dla dowolnej stałej c, $g(n) = c^{f(n)}$ jest multyplikatywna.

Twierdzonko

Theorem

Jeśli f *jest addytywna, a* g *multiplikatywna oraz* $n = \prod p^{\alpha_p(n)}$ *jest kanonicznym rozkładem* n *na liczby pierwsze, to wtedy* $f(1) = 0$ *i* $g(1) = 1$ *oraz*

$$f(n) = \sum_p f\left(p^{\alpha_p(n)}\right)$$

i

$$g(n) = \prod_p g\left(p^{\alpha_p(n)}\right)$$

Twierdzonko

Theorem

Jeśli f jest addytywna, a g multiplikatywna oraz $n = \prod p^{\alpha_p(n)}$ jest kanonicznym rozkładem n na liczby pierwsze, to wtedy $f(1) = 0$ i $g(1) = 1$ oraz

$$f(n) = \sum_p f\left(p^{\alpha_p(n)}\right)$$

i

$$g(n) = \prod_p g\left(p^{\alpha_p(n)}\right)$$

Wniosek

Funkcje addytywne i muliplikatywne są wyznaczone przez wartości w punktach typu p^k, a całkowicie addytywne i multiplikatywne przez wartości w punktach typu p.

Przykłady funkcji addytywnych i multiplikatywnych

1. $\omega(n)$ — liczba różnych dzielników pierwszych liczby n.

Przykłady funkcji addytywnych i multiplikatywnych

1. $\omega(n)$ — liczba różnych dzielników pierwszych liczby n.
2. $\Omega(n)$ — liczba czynników w kanonicznym rozkładzie na liczby pierwsze liczby n.

Przykłady funkcji addytywnych i multiplikatywnych

1. $\omega(n)$ — liczba różnych dzielników pierwszych liczby n.
2. $\Omega(n)$ — liczba czynników w kanonicznym rozkładzie na liczby pierwsze liczby n.

Fact

Obie powyższe funkcje są addytywne.

Przykłady funkcji addytywnych i multiplikatywnych

1. $\omega(n)$ — liczba różnych dzielników pierwszych liczby n.
2. $\Omega(n)$ — liczba czynników w kanonicznym rozkładzie na liczby pierwsze liczby n.

Fact

Obie powyższe funkcje są addytywne.

Fact

$I(n), N(n), \mu(n), \varphi(n) \in \mathcal{M}$, *a w dodatku* I *i* N *są nawet całkowicie multiplikatywne.*

Tw o grupie

Lemma

Jeśli $NWD(n, m) = 1$*, to każdy dzielnik* d *liczby* nm *ma jednoznaczny rozkład* $d = d_1 d_2$*, gdzie* $d_1 | n$*, a* $d_2 | m$ *i* $NWD(d_1, d_2) = 1$*.*

Tw o grupie

Lemma

Jeśli $NWD(n, m) = 1$, *to każdy dzielnik* d *liczby* nm *ma jednoznaczny rozkład* $d = d_1 d_2$, *gdzie* $d_1 | n$, *a* $d_2 | m$ *i* $NWD(d_1, d_2) = 1$.

Theorem

Jeśli $f, g \in \mathcal{M}$, *to* $f * g \in \mathcal{M}$, *a nadto, jeśli* $f \in \mathcal{M}$, *to istnieje* $g \in \mathcal{M}$, *że* $f * g = e$. *Zatem* $(\mathcal{M}, e, *)$ *tworzy grupę.*

Tw o grupie

Lemma

Jeśli $NWD(n, m) = 1$, *to każdy dzielnik* d *liczby* nm *ma jednoznaczny rozkład* $d = d_1 d_2$, *gdzie* $d_1 | n$, *a* $d_2 | m$ *i* $NWD(d_1, d_2) = 1$.

Theorem

Jeśli $f, g \in \mathcal{M}$, *to* $f * g \in \mathcal{M}$, *a nadto, jeśli* $f \in \mathcal{M}$, *to istnieje* $g \in \mathcal{M}$, *że* $f * g = e$. *Zatem* $(\mathcal{M}, e, *)$ *tworzy grupę.*

Dowód.

Niech $d_1 | m, d_2 | n, d_1 d_2 = d, d_1' | m, d_2' | n$ i $d_1' d_2' = d'$

$$f * g(mn) = \sum_{dd' = mn} f(d)g(d') = \sum_{dd' = mn} f(d_1)g(d_1')f(d_2)g(d_2') = f * g(m) \cdot f * g(n)$$

Wiemy, że jeśli $f \in \mathcal{M}$, to istnieje $g \in \mathcal{A}$, że $f * g = e$. Pokażemy, że $g \in \mathcal{M}$. $\square$

C.d. dowodu

Dowód.

Dowód będzie indukcyjny, ze względu na mn. Z jednej strony:

$$0 = \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right) = \sum_{a|m} \sum_{b|n} f(a) f(b) g\left(\frac{mn}{ab}\right)$$

$$= \sum_{a|m} \sum_{b|n, ab \neq 1} \left\{ f(a) f(b) g\left(\frac{mn}{ab}\right) \right\} + g(mn)$$

Z drugiej strony:

$$0 = \sum_{a|m} f(a) g\left(\frac{m}{a}\right) \sum_{b|n} f(b) g\left(\frac{n}{b}\right)$$

$$= \sum_{a|m} \sum_{b|n, ab \neq 1} \left\{ f(a) f(b) g\left(\frac{mn}{ab}\right) \right\} + g(m) g(n) \, .$$

Wnioski z twierdzenia

1. Jeśli funkcja $f * g$ jest multiplikatywna, to albo $f, g \in \mathcal{M}$ albo $f, g \notin \mathcal{M}$.

Wnioski z twierdzenia

1. Jeśli funkcja $f * g$ jest multiplikatywna, to albo $f, g \in \mathcal{M}$ albo $f, g \notin \mathcal{M}$.
2. $d(n) = I * I(n)$ i $\sigma(n) = I * N(n)$ są multiplikatywne.

Wnioski z twierdzenia

1. Jeśli funkcja $f * g$ jest multiplikatywna, to albo $f, g \in \mathcal{M}$ albo $f, g \notin \mathcal{M}$.
2. $d(n) = I * I(n)$ i $\sigma(n) = I * N(n)$ są multiplikatywne.
3. $\mu(n)$ jest funkcją odwrotną do $I(n)$ $(\mu * I = e)$:

$$\sum_{d|n} \mu(d) = \delta_{1,n} \ .$$

Wnioski z twierdzenia

1. Jeśli funkcja $f * g$ jest multiplikatywna, to albo $f, g \in \mathcal{M}$ albo $f, g \notin \mathcal{M}$.
2. $d(n) = I * I(n)$ i $\sigma(n) = I * N(n)$ są multiplikatywne.
3. $\mu(n)$ jest funkcją odwrotną do $I(n)$ ($\mu * I = e$):

$$\sum_{d|n} \mu(d) = \delta_{1,n} \ .$$

Istotnie, dla $n = p^k$, gdzie $k > 0$, lewa strona daje $\sum_{i=0}^{k} \mu(p^i) = 1 - 1 + 0 = 0$.

Wnioski z twierdzenia

1. Jeśli funkcja $f * g$ jest multiplikatywna, to albo $f, g \in \mathcal{M}$ albo $f, g \notin \mathcal{M}$.
2. $d(n) = I * I(n)$ i $\sigma(n) = I * N(n)$ są multiplikatywne.
3. $\mu(n)$ jest funkcją odwrotną do $I(n)$ ($\mu * I = e$):

$$\sum_{d|n} \mu(d) = \delta_{1,n} \ .$$

   Istotnie, dla $n = p^k$, gdzie $k > 0$, lewa strona daje $\sum_{i=0}^{k} \mu(p^i) = 1 - 1 + 0 = 0$.
4. (Wzór Möbiusa na odwrócenie) Poniższe dwie formuły są równoważne dla dowolnych $f, g \in \mathcal{A}$:

$$(\forall n) g(n) = \sum_{d|n} f(d) \qquad g = I * f$$

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

Jeszcze trochę wniosków

Jeśli $f \in \mathcal{M}$, to

$$(\mu \cdot f) * I(n) = \prod_{p|n}(1 - f(p)) \qquad (\mu^2 \cdot f) * I(n) = \prod_{p|n}(1 + f(p))$$

Jeszcze trochę wniosków

Jeśli $f \in \mathcal{M}$, to

$$(\mu \cdot f) * I(n) = \prod_{p|n}(1 - f(p)) \qquad (\mu^2 \cdot f) * I(n) = \prod_{p|n}(1 + f(p))$$

Theorem

$$\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right) = \sum_{d|n}\mu(d)\frac{n}{d}\ ,$$

czyli $\varphi = \mu * N$. *Ponadto*

$$d(n) = \prod_{p \in \mathcal{P}\mathrm{rime}}(1 + \alpha_p(n))$$

Jeszcze trochę wniosków

Jeśli $f \in \mathcal{M}$, to

$$(\mu \cdot f) * I(n) = \prod_{p|n}(1 - f(p)) \qquad (\mu^2 \cdot f) * I(n) = \prod_{p|n}(1 + f(p))$$

Theorem

$$\varphi(n) = n \prod_{p|n}\left(1 - \frac{1}{p}\right) = \sum_{d|n} \mu(d)\frac{n}{d} ,$$

czyli $\varphi = \mu * N$. *Ponadto*

$$d(n) = \prod_{p \in \mathcal{P}\mathrm{rime}} (1 + \alpha_p(n))$$

Wniosek:

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

Zachowanie tocjentu Eulera

Theorem

$$\limsup_{n\to\infty} \frac{\varphi(n)}{n} = 1, \qquad \liminf_{n\to\infty} \frac{\varphi(n)}{n} = 0 \ .$$

Zachowanie tocjentu Eulera

Theorem

$$\limsup_{n\to\infty} \frac{\varphi(n)}{n} = 1, \qquad \liminf_{n\to\infty} \frac{\varphi(n)}{n} = 0\ .$$

Można pokazać nawet, że

$$\liminf_{n\to\infty} \frac{\varphi(n)\ln(\ln(n))}{n} = e^{-\gamma}\ ,$$

gdzie $\gamma = 0.577215\ldots$ to stała Eulera—Mascheroniego. (tzw. Problem dzielników)

Zachowanie tocjentu Eulera

Theorem

$$\limsup_{n\to\infty} \frac{\varphi(n)}{n} = 1, \qquad \liminf_{n\to\infty} \frac{\varphi(n)}{n} = 0 \ .$$

Dowód.

Niech (p_m) będzie rosnącym ciągiem wszystkich liczb pierwszych. $\varphi(p) = p - 1$, dla liczb pierwszych p, zatem $\frac{\varphi(p_m)}{p_m} \overset{m\to\infty}{\longrightarrow} 1$.

$\square$

Zachowanie tocjentu Eulera

Theorem

$$\limsup_{n\to\infty} \frac{\varphi(n)}{n} = 1, \qquad \liminf_{n\to\infty} \frac{\varphi(n)}{n} = 0 \ .$$

Dowód.

Niech (p_m) będzie rosnącym ciągiem wszystkich liczb pierwszych.
$\varphi(p) = p - 1$, dla liczb pierwszych p, zatem $\frac{\varphi(p_m)}{p_m} \overset{m\to\infty}{\longrightarrow} 1$.
Niech teraz $n_m = \prod_{i=1}^{m} p_i$. Wtedy

$$\frac{\varphi(n_m)}{n_m} = \prod_{p \leqslant p_m} \left(1 - \frac{1}{p}\right) = \prod_{p \leqslant p_m} \left(1 + p^{-1} + p^{-2} + \dots\right)^{-1} \overset{(Euler)}{\leqslant} \left(\sum_{x \leqslant p_m} \frac{1}{x}\right)^{-1} \to 0$$

$\square$

Gęstość naturalna

Jeśli $A \subset \mathbb{N}$, to przez $A(x)$ oznaczamy $|A \cap [1, x]|$.

Gęstość naturalna

Jeśli $A \subset \mathbb{N}$, to przez $A(x)$ oznaczamy $|A \cap [1, x]|$.
Gęstością górną nazywamy

$$d^*(A) = \limsup_{x \to \infty} \frac{A(x)}{x} \ ,$$

a dolną gętością:

$$d_*(A) = \liminf_{x \to \infty} \frac{A(x)}{x} \ .$$

Jeśli obie gęstości są równe, to mówimy wtedy o gęstości naturalnej zbioru A i oznaczamy przez $d(A)$.
Uwaga: Gęstość jest addytywna, ale nie jest przeliczalnie addytywna.

Gęstość naturalna

Jeśli $A \subset \mathbb{N}$, to przez $A(x)$ oznaczamy $|A \cap [1, x]|$.
Gęstością górną nazywamy

$$d^*(A) = \limsup_{x \to \infty} \frac{A(x)}{x} \ ,$$

a dolną gętością:

$$d_*(A) = \liminf_{x \to \infty} \frac{A(x)}{x} \ .$$

Jeśli obie gęstości są równe, to mówimy wtedy o gęstości naturalnej zbioru A i oznaczamy przez $d(A)$.
Uwaga: Gęstość jest addytywna, ale nie jest przeliczalnie addytywna.
Przykład: Postęp arytmetyczny $A_{a,r} = \{a + rn : n \in \mathbb{N}\}$. Wtedy $A_{a,r}(x) = \left\lfloor \frac{x-a}{r} \right\rfloor = \frac{x}{r} + O(1)$, czyli $d(A_{a,r}) = \frac{1}{r}$.

Ważne twierdzenie

Theorem

Niech (a_i) będzie nieskończonym ciągiem liczb parami względnie pierwszych. Niech A to zbiór liczb, które nie dzielą się przez żadną z liczb a_i. Wówczas A ma gęstość i wynosi ona

$$d(A) = \begin{cases} \prod_{i=1}^{\infty} \left(1 - \frac{1}{a_i}\right) & \text{gdy } \sum_{i=1}^{\infty} \frac{1}{a_i} \text{ — zbieżny,} \quad (1) \\ 0 & \text{gdy } \sum_{i=1}^{\infty} \frac{1}{a_i} \text{ — rozbieżny.} \quad (2) \end{cases}$$

Szkic dowodu

Definiujemy $A_i(x)$ jako zbiór liczb niedzielących się przez żadną z liczb $a_1, a_2, \ldots, a_i$. Wtedy $A_i(x)$ zbiega do $A(x)$ monotonicznie, z góry.
Ze wzoru na zbiór włączeń i wyłączeń można znaleźć dokładny wzór na $A_i(x)$, który daje

$$\lim_{n\to\infty} \frac{A_i(x)}{x} = \prod_{j=1}^{i} \left(1 - \frac{1}{a_j}\right) .$$

Jeśli szereg jest rozbieżny, to inf po i prawej strony wynosi 0.
W innym przypadku daję pewną liczbę g. Trzeba pokazać, że

$$A(x) \geqslant A_i(x) - \sum_{n\leqslant x,\, j>i,\, a_j|n} 1 ,$$

przez co dostaje się

$$\lim_{n\to\infty} \frac{A_i(x)}{x} - \sum_{j=i+1}^{\infty} \frac{1}{a_j} = \prod_{j=1}^{i} \left(1 - \frac{1}{a_j}\right) - \sum_{j=i+1}^{\infty} \frac{1}{a_j} .$$

Wnioski

Niech K będzie zbiorem liczb bezkwadratowych. Wtedy

$$d(K) = \left(\sum_{n=1}^{\infty} \frac{1}{n^2} \right)^{-1} = \frac{6}{\pi^2} \; .$$

Wnioski

Niech K będzie zbiorem liczb bezkwadratowych. Wtedy

$$d(K) = \left(\sum_{n=1}^{\infty} \frac{1}{n^2} \right)^{-1} = \frac{6}{\pi^2} \, .$$

Wystarczy wziąć $a_i = p_i^2$. Stąd

$$\frac{\pi^2}{6} = \sum_{n=1}^{\infty} \frac{1}{n^2} = \prod_{p \in \mathcal{P}\mathrm{rime}} \left(1 - \frac{1}{p^2} \right)^{-1} = \frac{1}{d(K)}$$

Wnioski

Niech K będzie zbiorem liczb bezkwadratowych. Wtedy

$$d(K) = \left(\sum_{n=1}^{\infty} \frac{1}{n^2} \right)^{-1} = \frac{6}{\pi^2} .$$

Wystarczy wziąć $a_i = p_i^2$. Stąd

$$\frac{\pi^2}{6} = \sum_{n=1}^{\infty} \frac{1}{n^2} = \prod_{p \in \mathcal{P}\mathrm{rime}} \left(1 - \frac{1}{p^2} \right)^{-1} = \frac{1}{d(K)}$$

Szeregi Dirichleta: $D(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, ją często szeregami eulerowskimi.

Niech $f \in \mathcal{A}$. Wtedy górną wartością średnią nazywamy

$$M^*(f) = \limsup_{x \to \infty} \frac{\sum_{n \leqslant x} f(n)}{x} \ ,$$

a dolną wartościa średnią:

$$M_*(f) = \liminf_{x \to \infty} \frac{\sum_{n \leqslant x} f(n)}{x} \ .$$

Znowu, jeśli oba kresy są równe, to mówimy o wartości średniej f i oznaczamy ją przez $M(f)$.

Niech $f \in \mathcal{A}$. Wtedy górną wartością średnią nazywamy

$$M^*(f) = \limsup_{x\to\infty} \frac{\sum_{n\leqslant x} f(n)}{x} \ ,$$

a dolną wartościa średnią:

$$M_*(f) = \liminf_{x\to\infty} \frac{\sum_{n\leqslant x} f(n)}{x} \ .$$

Znowu, jeśli oba kresy są równe, to mówimy o wartości średniej f i oznaczamy ją przez $M(f)$.
Warto zauważyć, że $d(A) = M(1(A))$. Co więcej, jeśli istnieje $\lim_{n\to\infty} f(n) = c$, to również $M(f) = c$.

Kluczowe twierdzenie

Lemma (tw. Lebesgue'a, o zbieżności zmajoryzowanej)

Niech $[a_{n,k}]$ *będzie nieskończoną macierzą. Jeśli* $(\exists C)\ |a_{n,k}| \leqslant C$ *oraz* $(\forall n)\ \lim_{n\to\infty} a_{n,k} = a_n$*, to dla każdego absolutnie zbieżnego szeregu* $\sum\limits_{n=1}^{\infty} x_n$ *mamy:*

$$\lim_{n\to\infty} \sum_{n=1}^{\infty} a_{n,k} x_n = \sum_{n=1}^{\infty} a_n x_n \ .$$

Theorem

Jeśli szereg $\sum\limits_{n=1}^{\infty} \frac{|g(n)|}{n}$ *jest zbieżny, a* $f = g * h$ *i istnieje* $M(h)$*, to istnieje wartość średnia* f*:*

$$M(f) = M(h) \sum_{n=1}^{\infty} \frac{g(n)}{n}$$

Dowód i ostatnie wnioski

Dowód.

$$\frac{1}{x}\sum_{n\leqslant x} f(n) = \frac{1}{x}\sum_{n\leqslant x}\sum_{k|n} g(k)h\left(\frac{n}{k}\right) = \frac{1}{x}\sum_{k\leqslant x} g(k)\sum_{m\leqslant \frac{x}{k}} h(m)$$

$$= \sum_{k\leqslant x}\frac{g(k)}{k}\frac{k}{x}\sum_{m\leqslant \frac{x}{k}} h(m) \overset{x\to\infty}{\to} M(h)\sum_{k=1}^{\infty}\frac{g(k)}{k}.$$

$\square$

Dowód i ostatnie wnioski

Wnioski:

Fact

$f(n) = \frac{\sigma(n)}{n}$ *ma wartość średnią* $\frac{\pi^2}{6}$.

Wystarczy wziąć $g(n) = \frac{1}{n}$ i zauważyć, że $g * I = f$.

Dowód i ostatnie wnioski

Wnioski:

Fact

$f(n) = \frac{\sigma(n)}{n}$ *ma wartość średnią* $\frac{\pi^2}{6}$.

Wystarczy wziąć $g(n) = \frac{1}{n}$ i zauważyć, że $g * I = f$.

Fact

$f(n) = \frac{\varphi(n)}{n}$ *ma wartość średnią* $\frac{6}{\pi^2}$.

Wystarczy przyjąć $g(n) = \frac{\mu(n)}{n}$, bo wtedy $g * I = f$, a następnie powtórzyć dowód dla gęstości liczb bezkwadratowych.

Dowód i ostatnie wnioski

Wnioski:

Fact

$f(n) = \frac{\sigma(n)}{n}$ *ma wartość średnią* $\frac{\pi^2}{6}$.

Wystarczy wziąć $g(n) = \frac{1}{n}$ i zauważyć, że $g * I = f$.

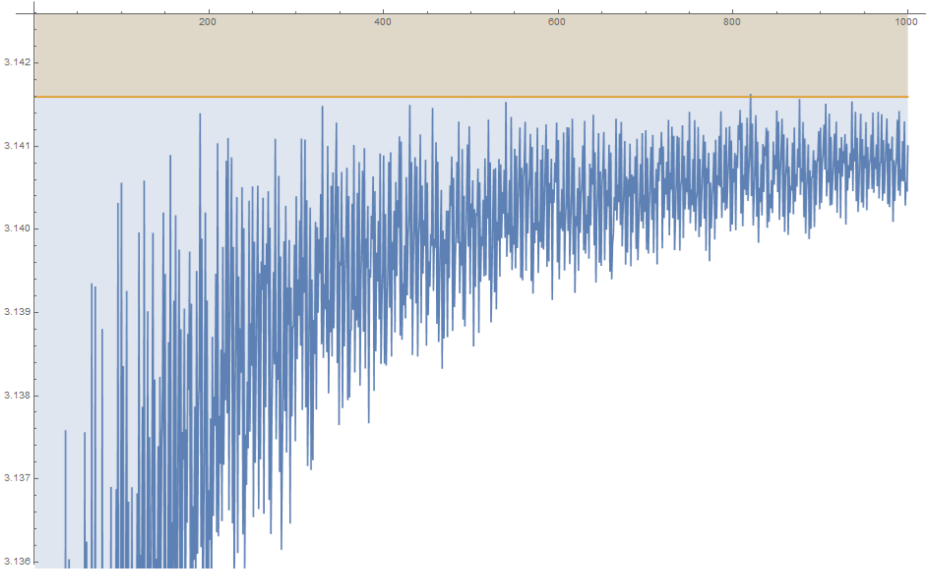
Fact

$f(n) = \frac{\varphi(n)}{n}$ *ma wartość średnią* $\frac{6}{\pi^2}$.

Wystarczy przyjąć $g(n) = \frac{\mu(n)}{n}$, bo wtedy $g * I = f$, a następnie powtórzyć dowód dla gęstości liczb bezkwadratowych.

Obliczanie liczby π.

W jednym z filmików Uwaga! Naukowy Bełkot przedstawiono przybliżenie liczby π przy pomocy poprzedniego faktu, na podstawie 883 komentarzy na Instagramie, gdzie fani wypisywali dwie liczby o co najwyżej 7 cyfrach. Na podstawie ich względnej pierwszości, przy użyciu metody Monte Carlo otrzymano przybliżenie $3,1551$.



Średnie wartości przybliżenia liczby π przy pomocy funkcji $\varphi(n)$ dla $n \leqslant 1000$.