Matematyka Dyskretna

Wykład V

Grzegorz Bobiński (UMK)

1.5 Funkcja i twierdzenie Eulera

Definicja

Funkcją Eulera nazywamy funkcję $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ zdefiniowaną wzorem

$$\varphi(n) := \#U_n \qquad (n \in \mathbb{N}_+),$$

gdzie

$$U_n := \{a \in [0, n-1] : \gcd(a, n) = 1\} \qquad (n \in \mathbb{N}_+).$$

Przykłady

(1) $\varphi(1) = 1$.

(2) Jeśli $p \in \mathbb{P}$, to $\varphi(p) = p - 1$.

(3) $\varphi(12) = \#\{1, 5, 7, 11\} = 4$.

Lemat 1.42

Jeśli $p \in \mathbb{P}$ i $k \in \mathbb{N}_+$, to

$$\varphi(p^k) = p^k - p^{k-1} = (p-1) \cdot p^{k-1} = p^k \cdot \left(1 - \tfrac{1}{p}\right).$$

Przypomnienie

(1.34): $\gcd(\prod_{p\in\mathbb{P}} p^{\alpha(p)}, \prod_{p\in\mathbb{P}} p^{\beta(p)}) = \prod_{p\in\mathbb{P}} p^{\min\{\alpha(p),\beta(p)\}}$.

Dowód

(1.34) $\implies$ $[\gcd(a, p^k) \neq 1 \iff p \mid a]$.

Stąd

$$\varphi(p^k) = \#\{a \in [0, p^k - 1] : \gcd(a, p^k) = 1\}$$

$$= \#[0, p^k - 1] - \#\{a \in [0, p^k - 1] : p \mid a\} = p^k - p^{k-1}. \square$$

Lemat 1.43

Niech $n_1, \ldots, n_k \in \mathbb{N}_+$.
Jeśli $\gcd(n_i, n_j) = 1$ dla wszystkich $i \neq j$, to

$$\varphi(n_1 \cdots n_k) = \varphi(n_1) \cdots \varphi(n_k).$$

Przypomnienie

(1.21)(1): $a, b \in \mathbb{Z}$ i $b \neq 0 \implies \gcd(a, b) = \gcd(b, a \bmod b)$.
(1.24): $\gcd(a, b_i) = 1$ dla każdego $i \iff \gcd(a, b_1 \cdots b_k) = 1$.
(1.40): Chińskie twierdzenie o resztach.

Dowód

Niech $n := n_1 \cdots n_k$.
Definiujemy $\Phi : [0, n-1] \to [0, n_1 - 1] \times \cdots \times [0, n_k - 1]$ wzorem

$$\Phi(x) := (x \bmod n_1, \ldots, x \bmod n_k) \qquad (x \in [0, n-1]).$$

(1.40) $\implies$ Φ jest bijekcją.
Jeśli $x \in [0, n-1]$, to

$$x \in U_n \iff \gcd(x, n) = 1 \overset{(1.24)}{\iff} \gcd(x, n_i) = 1 \text{ dla każdego } i$$

$$\overset{(1.21)(1)}{\iff} \gcd(x \bmod n_i, n_i) = 1 \text{ dla każdego } i \iff \Phi(x) \in U_{n_1} \times \ldots \times U_{n_k}.$$

Zatem Φ indukuje bijekcję

$$U_n \to U_{n_1} \times \ldots \times U_{n_k}. \quad \square$$

Lemat 1.42

Jeśli $p \in \mathbb{P}$ i $k \in \mathbb{N}_+$, to

$$\varphi(p^k) = p^k - p^{k-1} = (p-1) \cdot p^{k-1} = p^k \cdot \left(1 - \tfrac{1}{p}\right).$$

Lemat 1.43

Niech $n_1, \ldots, n_k \in \mathbb{N}_+$.
Jeśli $\gcd(n_i, n_j) = 1$ dla wszystkich $i \neq j$, to $\varphi(n_1 \cdots n_k) = \varphi(n_1) \cdots \varphi(n_k)$.

Wniosek 1.44

Niech $P \subseteq \mathbb{P}$, $|P| < \infty$, $\alpha : P \to \mathbb{N}_+$ i $n := \prod_{p \in P} p^{\alpha(p)}$.
Wtedy

$$\varphi(n) = \prod_{p \in P} (p^{\alpha(p)} - p^{\alpha(p)-1}) = \prod_{p \in P} (p-1) \cdot p^{\alpha(p)-1} = n \cdot \prod_{p \in P} \left(1 - \tfrac{1}{p}\right).$$

Dowód

Dla $p \in P$ definiujemy $n_p \in \mathbb{N}_+$ wzorem $n_p := p^{\alpha(p)}$.
(1.34) $\implies$ $\gcd(n_p, n_q) = 1$ dla $p \neq q$.
Stąd

$$\varphi(n) = \varphi\Big(\prod_{p \in P} n_p\Big) \overset{(1.43)}{=} \prod_{p \in P} \varphi(n_p).$$

(1.42) $\implies$ teza. $\square$

Twierdzenie 1.46 (Euler)

Jeśli $a, n \in \mathbb{Z}$, $n > 0$ i $\gcd(a, n) = 1$, to

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Przypomnienie

(1.37)(1): $a \equiv_n b$ i $c \equiv_n d \implies a \cdot c \equiv_n b \cdot d$.

(1.37)(2): $a \cdot c \equiv_n b \cdot c \implies \gcd(c, n) = 1$, to $a \equiv_n b$.

(1.38)(2): $\gcd(a, n) \mid b \implies$ istnieje $x \in \mathbb{Z}$ takie, że $a \cdot x \equiv_n b$.

Dowód

Definiujemy $\Phi : U_n \to U_n$ wzorem

$$\Phi(b) := (a \cdot b) \bmod n \qquad (b \in U_n).$$

(1.24) + (1.21)(1) $\implies$ Φ jest dobrze określona.

(1.38)(2) $\implies$ Φ jest „na".

Ponieważ $|U_n| = |U_n| < \infty$, więc Φ jest bijekcją.

Stąd

$$\prod_{b \in U_n} b = \prod_{b \in U_n} \Phi(b) \overset{(1.37)(1)}{\equiv_n} \prod_{b \in U_n} (a \cdot b) = a^{\varphi(n)} \cdot \prod_{b \in U_n} b.$$

(1.24) $\implies$ $\gcd(\prod_{b \in U_n} b, n) = 1 \overset{(1.37)(2)}{\implies} 1 \equiv_n a^{\varphi(n)}$. □

Twierdzenie 1.46 (Euler)

Jeśli $a, n \in \mathbb{Z}$, $n > 0$ i $\gcd(a, n) = 1$, to

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Wniosek 1.47 (Małe Twierdzenie Fermata)

Jeśli $p \in \mathbb{P}$, $a \in \mathbb{Z}$ i $p \nmid a$, to $a^{p-1} \equiv 1 \pmod{p}$.

Dowód

Natychmiast z (1.46). □

Wniosek 1.48

Jeśli $p \in \mathbb{P}$ i $a \in \mathbb{Z}$, to $a^p \equiv a \pmod{p}$.

Dowód

1° $p \nmid a$:

$a^p = a \cdot a^{p-1} \overset{(1.47)}{\equiv_p} a \cdot 1 = a.$

2° $p \mid a$

$a^p \equiv_p 0 \equiv_p a.$ □