Matematyka Dyskretna

Wykład IV

Grzegorz Bobiński (UMK)

Definicja

Jeśli $a, b, n \in \mathbb{Z}$, $n \neq 0$, to mówimy, że a przystaje do b modulo n, i piszemy $a \equiv_n b$ (lub $a \equiv b \pmod{n}$), jeśli $n \mid a - b$.

Fakt 1.35

Jeśli $a, b, n \in \mathbb{Z}$ i $n \neq 0$, to

$$a \equiv_n b \iff a \bmod n = b \bmod n.$$

Przypomnienie

(1.13): $c, n \in \mathbb{Z}$, $n \neq 0 \implies 0 \leq c \bmod n < |n|$ i $c = (c \operatorname{div} n) \cdot n + c \bmod n$.

(1.15)(1): $a, n, q, r \in \mathbb{Z}$, $n \neq 0$, $0 \leq r < |n|$, $a = q \cdot n + r \implies r = a \bmod n$.

Dowód

$\Rightarrow$: Załóżmy, że $a \equiv_n b$.

Z definicji istnieje liczba całkowita q taka, że $a - b = q \cdot n$, a więc

$$a = b + q \cdot n \overset{(1.13)}{=} (b \operatorname{div} n + q) \cdot n + b \bmod n.$$

$$(1.13) \implies 0 \leq b \bmod n < |n| \overset{(1.15)(1)}{\implies} b \bmod n = a \bmod n.$$

$\Leftarrow$: Załóżmy, że $a \bmod n = b \bmod n$.

Wtedy

$$a - b \overset{(1.13)}{=} ((a \operatorname{div} n) \cdot n + (a \bmod n)) - ((b \operatorname{div} n) \cdot n + (b \bmod n)) = (a \operatorname{div} n - b \bmod n) \cdot n.$$

Stąd $n \mid a - b$, a więc $a \equiv_n b$. $\square$

Fakt 1.35

Jeśli $a, b, n \in \mathbb{Z}$ i $n \neq 0$, to

$$a \equiv_n b \iff a \bmod n = b \bmod n.$$

Wniosek 1.36

Niech $n \in \mathbb{Z}$ i $n \neq 0$.

(1) Jeśli $a \in \mathbb{Z}$, to $a \equiv_n a$.

(2) Jeśli $a, b \in \mathbb{Z}$ i $a \equiv_n b$, to $b \equiv_n a$.

(3) Jeśli $a, b, c \in \mathbb{Z}$, $a \equiv_n b$ i $b \equiv_n c$, to $a \equiv_n c$.

Innym słowy, relacja $\equiv_n$ jest relacją równoważności.

Dowód

Natychmiast z (1.35). □

Lemat 1.37

Niech $n \in \mathbb{Z}$ i $n \neq 0$.

(1) Jeśli $a, b, c, d \in \mathbb{Z}$, $a \equiv_n b$ i $c \equiv_n d$, to

$$a \pm c \equiv_n b \pm d \qquad \text{i} \qquad a \cdot c \equiv_n b \cdot d.$$

(2) Jeśli $a, b, c \in \mathbb{Z}$, $a \cdot c \equiv_n b \cdot c$ i $\gcd(c, n) = 1$, to $a \equiv_n b$.

(3) Jeśli $a, b, m \in \mathbb{Z}$ i $m \neq 0$, to

$$m \cdot a \equiv_{m \cdot n} m \cdot b \iff a \equiv_n b.$$

Przypomnienie

(1.7)+(1.8): $n \mid p, q \implies c \mid k \cdot p + l \cdot q$.
(1.9): $m \neq 0 \implies (n \cdot m \mid c \cdot m \iff n \mid c)$.
(1.23): $\gcd(n, c) = 1$ i $n \mid k \cdot c \implies n \mid k$.

Dowód

(1) Mamy

$$(a \pm c) - (b \pm d) = (a - b) \pm (c - d)$$

i

$$a \cdot c - b \cdot d = (a - b) \cdot c + (c - d) \cdot b.$$

Teza wynika z (1.7) i (1.8).

(2) Teza wynika z (1.23).

(3) Teza wynika z (1.9). □

Stwierdzenie 1.38

Niech $a, b, n \in \mathbb{Z}$, $a \neq 0 \neq n$ i $d := \gcd(a, n)$.

(1) Jeśli $d \nmid b$, to nie istnieje $x \in \mathbb{Z}$ takie, że $a \cdot x \equiv_n b$.

(2) Jeśli $d \mid b$, to istnieje $x \in \mathbb{Z}$ takie, że $a \cdot x \equiv_n b$.

Ponadto, jeśli $k \in \mathbb{Z}$ i $k \cdot a \equiv_n d$, to

$$\{x \in \mathbb{Z} : a \cdot x \equiv_n b\} = \{x \in \mathbb{Z} : x \equiv_{n/d} c\},$$

gdzie $c := (b/d) \cdot k$.

Przypomnienie

(1.2): $d \mid n$ i $n \mid l \implies d \mid l$.

Dowód

(1): Przypuśćmy, że istnieje $x \in \mathbb{Z}$ takie, że $a \cdot x \equiv_n b$.

(1.2) $\implies$ $a \cdot x \equiv_d b$.

$a \equiv_d 0 \overset{(1.37)(1)}{\implies} a \cdot x \equiv_d 0$.

Stąd $b \equiv_d a \cdot x \equiv_d 0$.

Stwierdzenie 1.38

Niech $a, b, n \in \mathbb{Z}$, $n \neq 0$ i $d := \gcd(a, n)$.

(1) Jeśli $d \nmid b$, to nie istnieje $x \in \mathbb{Z}$ takie, że $a \cdot x \equiv_n b$.

(2) Jeśli $d \mid b$, to istnieje $x \in \mathbb{Z}$ takie, że $a \cdot x \equiv_n b$.

Ponadto, jeśli $k \in \mathbb{Z}$ i $k \cdot a \equiv_n d$, to

$$\{x \in \mathbb{Z} : a \cdot x \equiv_n b\} = \{x \in \mathbb{Z} : x \equiv_{n/d} c\},$$

gdzie $c := (b/d) \cdot k$.

Przypomnienie

(1.20): Istnieją $k, l \in \mathbb{Z}$ takie, że $\gcd(a, n) = k \cdot a + l \cdot n$.

Dowód (c.d.)

(2): (1.20) $\implies$ istnieje $k \in \mathbb{Z}$ takie, że $k \cdot a \equiv_n d$.

1°: Jeśli $x \in \mathbb{Z}$ i $x \equiv_{n/d} c$, to $a \cdot x \equiv_n b$.

$x \equiv_{n/d} c \overset{(1.37)(3)}{\implies} d \cdot x \equiv_n d \cdot c = d \cdot (b/d) \cdot k = b \cdot k$.

Stąd

$$a \cdot x = (a/d) \cdot d \cdot x \overset{(1.37)(1)}{\equiv_n} (a/d) \cdot b \cdot k = a \cdot k \cdot (b/d) \overset{(1.37)(1)}{\equiv_n} d \cdot (b/d) = b.$$

2°: Jeśli $x \in \mathbb{Z}$ i $a \cdot x \equiv_n b$, to $x \equiv_{n/d} c$.

Mamy

$$d \cdot x \equiv_n k \cdot a \cdot x \equiv_n k \cdot b = d \cdot c.$$

(1.37)(3) $\implies$ $x \equiv_{n/d} c$. $\square$

Lemat 1.39

Niech $a, b \in \mathbb{Z}$, $n_1, \ldots, n_k \in \mathbb{Z} \setminus \{0\}$.
Jeśli

1. $\gcd(n_i, n_j) = 1$ dla $i \neq j$,
2. $a \equiv_{n_i} b$ dla każdego i,

to $a \equiv_n b$, gdzie $n := n_1 \cdot \ldots \cdot n_k$.

Przypomnienie

(1.25): $\gcd(n_i, n_j) = 1$ dla $i \neq j$ oraz $n_i \mid c$ dla każdego $i \implies n_1 \cdot \ldots \cdot n_k \mid c$.

Dowód

Wynika z (1.25). □

Lemat 1.39

Niech $a, b \in \mathbb{Z}$, $n_1, \ldots, n_k \in \mathbb{Z} \setminus \{0\}$.
Jeśli $\gcd(n_i, n_j) = 1$ dla $i \neq j$ i $a \equiv_{n_i} b$ dla każdego i, to $a \equiv_n b$, gdzie $n := n_1 \cdots n_k$.

Twierdzenie 1.40 (Chińskie twierdzenie o resztach)

Niech $n_1, \ldots, n_k \in \mathbb{N}_+$ oraz $\gcd(n_i, n_j) = 1$ dla $i \neq j$.
Jeśli $n := n_1 \cdots n_k$, to funkcja $\Phi : [0, n-1] \to [0, n_1 - 1] \times \cdots \times [0, n_k - 1]$ dana wzorem

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

jest bijekcją.

Przypomnienie

(1.15)(2): $0 \leq a < |b| \implies a \bmod b = a$.

Dowód

Wystarczy pokazać, że Φ jest różnowartościowa (gdyż dziedzina i przeciwdziedzina mają tyle samo elementów).

Ustalmy $x, y \in [0, n-1]$ i załóżmy, że $\Phi(x) = \Phi(y)$.

(1.35) $\implies$ $x \equiv_{n_i} y$ dla każdego i $\overset{(1.39)}{\implies}$ $x \equiv_n y$ $\overset{(1.35)}{\implies}$ $x \bmod n = y \bmod n$.

$0 \leq x, y < n \overset{(1.15)(2)}{\implies} x \bmod n = x$ i $y \bmod n = y$.

Ostatecznie

$$x = x \bmod n = y \bmod n = y. \quad \square$$