Matematyka Dyskretna

Wykład I

Grzegorz Bobiński (UMK)

Podstawowe oznaczenia

Oznaczenia

- $\mathbb{Z}$ – zbiór liczb całkowitych
- $\mathbb{N}$ – zbiór liczb całkowitych nieujemnych
- $\mathbb{N}_+$ – zbiór liczb całkowitych dodatnich
- $[i, j] := \{k \in \mathbb{Z} \mid i \leq k \leq j\}$.

1 Elementy teorii liczb

1.1 Twierdzenie o dzieleniu z resztą

Definicja

Niech $a, b \in \mathbb{Z}$.
Mówimy, że a dzieli b (i piszemy $a \mid b$), jeśli istnieje $c \in \mathbb{Z}$ takie, że $b = c \cdot a$.

Oznaczenie

Jeśli a nie dzieli b, to piszemy $a \nmid b$.

Przykłady

- $2 \mid 4$.
- $2 \nmid 5$.

Fakt 1.1

Jeśli $a \in \mathbb{Z}$, to $a \mid a$.

Dowód

Wynika z równości $a = 1 \cdot a$. $\square$

Fakt 1.2

Jeśli $a, b, c \in \mathbb{Z}$, $a \mid b$ i $b \mid c$, to $a \mid c$.

Dowód

Z definicji istnieją $k, l \in \mathbb{Z}$ takie, że $b = k \cdot a$ i $c = l \cdot b$.
Wtedy $c = (k \cdot l) \cdot a$. $\square$

Fakt 1.3

Jeśli $a, b \in \mathbb{Z}$, $a \mid b$ i $b \mid a$, to $b = \pm a$.

Dowód

Z definicji istnieją $k, l \in \mathbb{Z}$ takie, że $b = k \cdot a$ i $a = l \cdot b$.
1° $a = 0$.
Wtedy $b = k \cdot 0 = 0 = a$.
2° $a \neq 0$.
Wtedy $a = (l \cdot k) \cdot a$.
Stąd $l \cdot k = 1$.
W szczególności $k = \pm 1$.
Ostatecznie $b = k \cdot a = \pm a$. $\square$

Fakt 1.4

Niech $a \in \mathbb{Z}$.

(i) $1 \mid a$.

(ii) $a \mid 1 \iff a = \pm 1$.

Dowód

(i) Wynika z równości $a = a \cdot 1$.

(ii)

$\Rightarrow$: $a \mid 1 \overset{(i)+(1.3)}{\Longrightarrow} a = \pm 1$.

$\Leftarrow$: $a = \pm 1 \implies 1 = a \cdot a \implies a \mid 1$. $\square$

Fakt 1.5

Niech $a \in \mathbb{Z}$.

(i) $a \mid 0$.

(ii) $0 \mid a \iff a = 0$.

Dowód

(i) Wynika z równości $0 = 0 \cdot a$.

(ii)

$\Rightarrow$: $0 \mid a \overset{(i)+(1.3)}{\Longrightarrow} a = \pm 0 = 0$.

$\Leftarrow$: $a = 0 \overset{(1.1)}{\Longrightarrow} 0 \mid a$. $\square$

Fakt 1.6

Jeśli $a, b \in \mathbb{Z}$, $a \mid b$ i $b \neq 0$, to $|a| \leq |b|$.

Dowód

Z definicji istnieje $k \in \mathbb{Z}$ takie, że $b = k \cdot a$.
$b \neq 0 \implies k \neq 0 \implies |k| \geq 1$.
Stąd $|b| = |k| \cdot |a| \geq 1 \cdot |a| = |a|$. $\square$

Fakt 1.7

Jeśli $a, b, c \in \mathbb{Z}$, $a \mid b$ i $a \mid c$, to $a \mid b \pm c$.

Dowód

Z definicji istnieją $k, l \in \mathbb{Z}$ takie, że $b = k \cdot a$ i $c = l \cdot a$.
Wtedy $b \pm c = (k \pm l) \cdot a$. $\square$

Fakt 1.8

Jeśli $a, b, c \in \mathbb{Z}$ i $a \mid b$, to $a \mid b \cdot c$.

Dowód

Z definicji istnieje $k \in \mathbb{Z}$ takie, że $b = k \cdot a$.
Wtedy $b \cdot c = (k \cdot c) \cdot a$. $\square$

Fakt 1.9

Jeśli $a, b, c \in \mathbb{Z}$, $a \cdot c \mid b \cdot c$ i $c \neq 0$, to $a \mid b$.

Dowód

Z definicji istnieje $k \in \mathbb{Z}$ takie, że $b \cdot c = k \cdot a \cdot c$.

Ponieważ $c \neq 0$, więc $b = k \cdot a$. $\square$

Oznaczenie

Jeśli $a \in \mathbb{Z}$, to

$$\operatorname{sign} a := \begin{cases} -1 & a < 0, \\ 0 & a = 0, \\ 1 & a > 0. \end{cases}$$

Fakt 1.10

Jeśli $a \in \mathbb{Z}$, to

$$|a| = \operatorname{sign} a \cdot a \qquad \text{i} \qquad a = \operatorname{sign} a \cdot |a|.$$

Dowód

Ćwiczenie. $\square$

Definicja

Niech $a, b \in \mathbb{Z}$, $b \neq 0$.
Ilorazem (całkowitym) z dzielenia a przez b nazywamy każde $q \in \mathbb{Z}$ takie, że

$$q \cdot b = \max\{q' \cdot b \mid q' \in \mathbb{Z} \text{ i } q' \cdot b \leq a\}.$$

Fakt 1.11

Jeśli $a, b \in \mathbb{Z}$, $b \neq 0$, to istnieje iloraz z dzielenia a przez b.

Dowód

Niech $I := \{q' \in \mathbb{Z} : q' \cdot b \leq a\}$.
Wystarczy pokazać, że $I \neq \varnothing$.
$b \neq 0 \implies -\operatorname{sign} b \cdot b = -|b| \leq -1 \implies (-\operatorname{sign} b \cdot |a|) \cdot b \leq -|a| \cdot 1 = -|a| \leq a \implies$
$-\operatorname{sign} b \cdot |a| \in I$. □

Fakt 1.12

Niech $a, b \in \mathbb{Z}$, $b \neq 0$.
Jeśli q_1 i q_2 są ilorazami z dzielenia a przez b, to $q_1 = q_2$.

Dowód

Z definicji ilorazu wiemy, że

$$q_1 \cdot b = \max\{q' \cdot b \mid q' \in \mathbb{Z} \text{ i } q' \cdot b \leq a\} = q_2 \cdot b.$$

Stąd $q_1 \cdot b = q_2 \cdot b$.
Ponieważ $b \neq 0$, więc $q_1 = q_2$. □

Oznaczenie

Jeśli $a, b \in \mathbb{Z}$, $b \neq 0$, to przez $a \operatorname{div} b$ oznaczamy iloraz z dzielenia a przez b.

Definicja

Jeśli $a, b \in \mathbb{Z}$, $b \neq 0$, to resztą z dzielenia a przez b nazywamy $a \bmod b := a - (a \operatorname{div} b) \cdot b$.

Stwierdzenie 1.13

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

$$0 \leq a \bmod b < |b| \qquad \text{i} \qquad a = (a \operatorname{div} b) \cdot b + a \bmod b.$$

Dowód

Równość $a = (a \operatorname{div} b) \cdot b + a \bmod b$ wynika z definicji reszty.
Z definicji ilorazu całkowitego $(a \operatorname{div} b) \cdot b \leq a$, a więc $a \bmod b = a - (a \operatorname{div} b) \cdot b \geq 0$.
Musimy jeszcze udowodnić, że $a \bmod b < |b|$.
Przypuśćmy, że $a \bmod b \geq |b|$.
Wtedy $(a \operatorname{div} b) \cdot b = a - a \bmod b \leq a - |b|$.
Niech $q := a \operatorname{div} b + \operatorname{sign} b$.
Wtedy $q \cdot b = (a \operatorname{div} b) \cdot b + \operatorname{sign} b \cdot b = (a \operatorname{div} b) \cdot b + |b|$.
Zatem

$$(a \operatorname{div} b) \cdot b < q \cdot b \leq a - |b| + |b| = a,$$

co jest sprzeczne z definicją ilorazu. □

Stwierdzenie 1.13

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

$$0 \leq a \bmod b < |b| \qquad \text{i} \qquad a = (a \operatorname{div} b) \cdot b + a \bmod b.$$

Twierdzenie 1.14 (o dzieleniu z resztą)

Jeśli $a, b \in \mathbb{Z}$, $b \neq 0$, to istnieją jednoznacznie wyznaczone $q, r \in \mathbb{Z}$ takie, że

$$0 \leq r < |b| \qquad \text{i} \qquad a = q \cdot b + r.$$

Dowód

1° Istnienie.

Wynika z (1.13).

2° Jednoznaczność.

Przypuśćmy, że istnieją $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ takie, że

$$0 \leq r_1, r_2 < |b| \qquad \text{i} \qquad q_1 \cdot b + r_1 = a = q_2 \cdot b + r_2.$$

Wtedy $r_1 - r_2 = (q_2 - q_1) \cdot b$, więc $b \mid r_1 - r_2$.

Ponieważ

$$-|b| < -r_2 \leq r_1 - r_2 \leq r_1 < |b|,$$

więc $|r_1 - r_2| < |b|$.

$b \mid r_1 - r_2$ i $|r_1 - r_2| < |b| \overset{(1.6)}{\Longrightarrow} r_1 - r_2 = 0 \implies r_1 = r_2$.

Stąd $(q_2 - q_1) \cdot b = r_1 - r_2 = 0$.

Ponieważ $b \neq 0$, więc $q_2 - q_1 = 0$, tzn. $q_1 = q_2$. $\square$

Stwierdzenie 1.13

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

$$0 \leq a \bmod b < |b| \qquad \text{i} \qquad a = (a \operatorname{div} b) \cdot b + a \bmod b.$$

Twierdzenie 1.14 (o dzieleniu z resztą)

Jeśli $a, b \in \mathbb{Z}$, $b \neq 0$, to istnieją jednoznacznie wyznaczone $q, r \in \mathbb{Z}$ takie, że

$$0 \leq r < |b| \qquad \text{i} \qquad a = q \cdot b + r.$$

Wniosek 1.15

Niech $a, b \in \mathbb{Z}$, $b \neq 0$.

(i) Jeśli $q, r \in \mathbb{Z}$,

$$0 \leq r < |b| \qquad \text{i} \qquad a = q \cdot b + r,$$

to $q = a \operatorname{div} b$ i $r = a \bmod b$.

(ii) Jeśli $0 \leq a < |b|$, to $a \bmod b = a$ i $a \operatorname{div} b = 0$.

Dowód

(i): Natychmiast z (1.13) i (1.14).

(ii): $0 \leq a < |b|$ i $a = 0 \cdot b + a$, więc teza wynika z (i). □

Stwierdzenie 1.13

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

$$0 \leq a \bmod b < |b| \qquad \text{i} \qquad a = (a \operatorname{div} b) \cdot b + a \bmod b.$$

Wniosek 1.15(i)

Jeśli $q, r \in \mathbb{Z}$,

$$0 \leq r < |b| \qquad \text{i} \qquad a = q \cdot b + r,$$

to $q = a \operatorname{div} b$ i $r = a \bmod b$.

Wniosek 1.16

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

$$b \mid a \iff a \bmod b = 0.$$

Dowód

$\Rightarrow$:

$b \mid a \implies$ istnieje $q \in \mathbb{Z}$ takie, że $a = q \cdot b$.

Wtedy

$$0 \leq 0 < |b| \qquad \text{i} \qquad a = q \cdot b + 0.$$

$0 = a \bmod b$ na mocy (1.15)(i).

$\Leftarrow$:

$a \bmod b = 0 \overset{(1.13)}{\implies} a = (a \operatorname{div} b) \cdot b \implies b \mid a$. $\square$