Matematyka Dyskretna

Wykład II

Grzegorz Bobiński (UMK)

1.2 Największy wspólny dzielnik

Definicja

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

Największym wspólnym dzielnikiem liczb a i b nazywamy każde $d \in \mathbb{Z}$ takie, że

(1) $d \geq 0$,

(2) $d \mid a$ i $d \mid b$,

(3) jeśli $c \in \mathbb{Z}$, $c \mid a$ i $c \mid b$, to $c \mid d$.

Przykład

0 jest największym wspólnym dzielnikiem 0 i 0.

Fakt 1.18

Jeśli $a, b \in \mathbb{Z}$ są liczbami całkowitymi, to istnieją $k, l \in \mathbb{Z}$ takie, że $k \cdot a + l \cdot b$ jest największym wspólnym dzielnikiem liczb a i b.

W szczególności istnieje największy wspólny dzielnik liczb a i b.

Przypomnienie

(1.7)+(1.8): $c \mid a, b \implies c \mid k \cdot a + l \cdot b$.
(1.13) $0 \leq a \bmod d < |d|$.
(1.16) $d \mid a \iff a \bmod d = 0$.

Dowód

1°. $a = 0 = b$, to $0 = 0 \cdot a + 0 \cdot b$ jest największym wspólnym dzielnikiem liczb a i b.

2°. Załóżmy, że $a \neq 0$ lub $b \neq 0$.

Niech $I := \{k \cdot a + l \cdot b : k, l \in \mathbb{Z}\} \cap \mathbb{N}_+$.

Ponieważ $0 < |a| + |b| = \operatorname{sign} a \cdot a + \operatorname{sign} b \cdot b$, więc $I \neq \varnothing$.

Niech $d := \min I$.

Wybierzmy $k, l \in \mathbb{Z}$ takie, że $d = k \cdot a + l \cdot b$.

Pokażemy, że d jest największym wspólnym dzielnikiem liczb a i b.

(1) Oczywiście $d \geq 0$.

(3) Załóżmy, że $c \mid a$ i $c \mid b$.

(1.7)+(1.8) $\implies c \mid k \cdot a + l \cdot b = d$.

(2) Mamy

$$a \bmod d = a - (a \operatorname{div} d) \cdot d = a - (a \operatorname{div} d) \cdot (k \cdot a + l \cdot b) = (1 - (a \operatorname{div} d) \cdot k) \cdot a - ((a \operatorname{div} d) \cdot l) \cdot b.$$

(1.13) $\implies a \bmod d < d \overset{d=\min I}{\implies} a \bmod d \notin I \implies a \bmod d \leq 0 \overset{(1.13)}{\implies} a \bmod d = 0 \overset{(1.16)}{\implies} d \mid a$.

Analogicznie, $d \mid b$. $\square$

Fakt 1.19

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

Jeśli d_1 i d_2 są największymi wspólnymi dzielnikami liczb a i b, to $d_1 = d_2$.

Przypomnienie

(1.3): $a \mid b$ i $b \mid a \implies b = \pm a$

Dowód

Warunek (2) definicji (dla $d = d_1$) $\implies d_1 \mid a$ i $d_1 \mid b$.

Warunek (3) definicji (dla $c = d_1$ i $d = d_2$) $\implies d_1 \mid d_2$.

Analogicznie $d_2 \mid d_1$. (1.3) $\implies d_1 = \pm d_2 \overset{d_1, d_2 \geq 0}{\implies} d_1 = d_2$. $\square$

Oznaczenie

Jeśli $a, b \in \mathbb{Z}$, to

$$\gcd(a, b) := \text{największy wspólny dzielnik liczb } a \text{ i } b.$$

Wniosek 1.20

Jeśli $a, b \in \mathbb{Z}$, to istnieją $k, l \in \mathbb{Z}$ takie, że

$$\gcd(a, b) = k \cdot a + l \cdot b.$$

Dowód

(1.18) $\implies$ istnieją $k, l \in \mathbb{Z}$ takie, że $d := k \cdot a + l \cdot b$ jest największym wspólnym dzielnikiem liczb a i b.

Wtedy $\gcd(a, b) \overset{(1.19)}{=} d = k \cdot a + l \cdot b$. $\square$

Lemat 1.21

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

(1) $\gcd(a, b) = \gcd(b, a \bmod b)$.

(2) Jeśli $k, l \in \mathbb{Z}$ i $\gcd(b, a \bmod b) = k \cdot b + l \cdot (a \bmod b)$, to

$$\gcd(a, b) = l \cdot a + (k - l \cdot (a \operatorname{div} b)) \cdot b.$$

Dowód

(1): Niech

$$I_1 := \{c \in \mathbb{Z} : c \mid a \text{ i } c \mid b\} \qquad \text{i} \qquad I_2 := \{c \in \mathbb{Z} : c \mid b \text{ i } c \mid a \bmod b\}.$$

Wystarczy pokazać, że $I_1 = I_2$.

$I_1 \subseteq I_2$:

Niech $c \in I_1$.

(1.7)+(1.8) $\implies$ $c \mid 1 \cdot a + [-(a \operatorname{div} b)] \cdot b = a \bmod b \implies c \in I_2$.

$I_2 \subseteq I_1$:

Niech $c \in I_2$.

(1.7)+(1.8) $\implies$ $c \mid (a \operatorname{div} b) \cdot b + 1 \cdot (a \bmod b) = a \implies c \in I_1$.

(2):

$$\gcd(a, b) \overset{(1)}{=} \gcd(b, a \bmod b) \overset{\text{zał}}{=} k \cdot b + l \cdot (a \bmod b)$$
$$= k \cdot b + l \cdot (a - (a \operatorname{div} b) \cdot b) = l \cdot a + (k - l \cdot (a \operatorname{div} b)) \cdot b. \quad \square$$

Uwaga

Powyższy lemat wraz z równościami $\gcd(a, 0) = |a| = \operatorname{sign}(a) \cdot a + 0 \cdot 0$ jest podstawą rozszerzonego algorytmu Euklidesa.

Lemat 1.22

(1) Jeśli $a, b \in \mathbb{Z}$, to $\gcd(a, b) \mid k \cdot a + l \cdot b$ dla dowolnych $k, l \in \mathbb{Z}$.

(2) Jeśli $a, b, k, l \in \mathbb{Z}$ i $1 = k \cdot a + l \cdot b$, to $\gcd(a, b) = 1$.

Przypomnienie

(1.4): $a \mid 1 \implies a = \pm 1$.

Dowód

(1): $\gcd(a, b) \mid a, b \overset{(1.7)+(1.8)}{\implies} \gcd(a, b) \mid k \cdot a + l \cdot b$.

(2): (1) $\implies \gcd(a, b) \mid 1 \overset{(1.4)}{\implies} \gcd(a, b) = \pm 1 \overset{\gcd(a,b) \geq 0}{\implies} \gcd(a, b) = 1$. □

Wniosek 1.23

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

Dowód

(1.20) $\implies$ istnieją $k, l \in \mathbb{Z}$ takie, że $1 = k \cdot a + l \cdot b$.

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

Wtedy

$$c = c \cdot 1 = c \cdot (k \cdot a + l \cdot b) = c \cdot k \cdot a + l \cdot b \cdot c = c \cdot k \cdot a + l \cdot q \cdot a = (c \cdot k + l \cdot q) \cdot a.$$ □

Wniosek 1.24

Jeśli $a, b_1, \ldots, b_n \in \mathbb{Z}$, $n \in \mathbb{N}_+$, oraz $\gcd(a, b_i) = 1$ dla każdego $i \in [1, n]$, to

$$\gcd(a, b_1 \cdots b_n) = 1.$$

Dowód

Indukcja na n.

$n = 1$:

Oczywiste.

$n > 1$:

Z założenia indukcyjnego $\gcd(a, b_1 \cdots b_{n-1}) = 1$.

(1.20) $\implies$ istnieją $x, y, k, l \in \mathbb{Z}$ takie, że

$$x \cdot a + y \cdot (b_1 \cdots b_{n-1}) = 1 = k \cdot a + l \cdot b_n.$$

Wtedy

$$1 = 1 \cdot 1 = (x \cdot a + y \cdot (b_1 \cdots b_{n-1})) \cdot (k \cdot a + l \cdot b_n)$$

$$= (x \cdot k \cdot a + y \cdot (b_1 \cdots b_{n-1}) \cdot k + x \cdot l \cdot b_n) \cdot a + (l \cdot y) \cdot (b_1 \cdots b_n).$$

(1.22) $\implies$ $\gcd(a, b_1 \cdots b_n) = 1$. □

Uwaga

Jeśli $a, b_1, \ldots, b_n \in \mathbb{Z}$, $n \in \mathbb{N}$, oraz $\gcd(a, b_1 \cdots b_n) = 1$, to $\gcd(a, b_i) = 1$ dla każdego $i \in [1, n]$.

Wniosek 1.25

Jeśli $a_1, \ldots, a_n, b \in \mathbb{Z}$, $n \in \mathbb{N}_+$, $\gcd(a_i, a_j) = 1$ dla wszystkich $i \neq j$, oraz $a_i \mid b$ dla wszystkich $i \in [1, n]$, to

$$a_1 \cdots a_n \mid b.$$

Dowód

Indukcja na n.

$n = 1$:

Oczywiste.

$n > 1$:

Z założenia indukcyjnego $a_1 \cdots a_{n-1} \mid b$, zatem istnieje $q \in \mathbb{Z}$ takie, że $b = q \cdot (a_1 \cdots a_{n-1})$.

Podobnie, istnieje $q' \in \mathbb{Z}$ takie, że $b = q' \cdot a_n$, gdyż $a_n \mid b$.

(1.24) $\implies$ $\gcd(a_1 \cdots a_{n-1}, a_n) = 1 \overset{(1.20)}{\implies}$ istnieją $k, l \in \mathbb{Z}$ takie, że

$$1 = k \cdot (a_1 \cdots a_{n-1}) + l \cdot a_n.$$

Wtedy

$$b = b \cdot 1 = b \cdot (k \cdot (a_1 \cdots a_{n-1}) + l \cdot a_n) = b \cdot k \cdot (a_1 \cdots a_{n-1}) + b \cdot l \cdot a_n$$

$$= q' \cdot a_n \cdot k \cdot (a_1 \cdots a_{n-1}) + q \cdot (a_1 \cdots a_{n-1}) \cdot l \cdot a_n = (k \cdot q' + l \cdot q) \cdot (a_1 \cdots a_n). \quad \square$$

Stwierdzenie 1.26

Niech $a, b \in \mathbb{Z}$ i $d := \gcd(a, b)$.
Jeśli $d \neq 0$, to $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Dowód

(1.20) $\Longrightarrow$ istnieją $k, l \in \mathbb{Z}$ takie, że $d = k \cdot a + l \cdot b$.
Wtedy $1 = k \cdot \frac{a}{d} + l \cdot \frac{b}{d}$.
(1.22) $\Longrightarrow$ $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. $\square$