ALGEBRA

WYKŁAD 1

1. NWD, NWW i algorytm Euklidesa

Tw. 1 (o dzieleniu z resztą): Niech $a, b \in \mathbb{Z}$, $b \neq 0$. Wówczas istnieje dokładnie jedna para liczb całkowitych $q, r \in \mathbb{Z}$ taka, że:

$$a = qb + r \quad \text{oraz} \quad 0 \leq r < |b|.$$

Dowód: Istnienie: załóżmy, że $b > 0$ i zdefiniujmy

$$q := \left[\frac{a}{b}\right] \quad \text{oraz} \quad r := a - bq.$$

Wówczas $q \leq \frac{a}{b} < q + 1$, a zatem $bq \leq a < bq + b$, skąd $0 \leq r = a - bq < b = |b|$.

Załóżmy, że $b < 0$ i zdefiniujmy

$$q := -\left[\frac{a}{|b|}\right] \quad \text{oraz} \quad r = a - bq.$$

Dalej rozumujemy analogicznie [ćw.]

Jednoznaczność: załóżmy, że $a = bq_1 + r_1 = bq_2 + r_2$ gdzie $0 \leq r_1, r_2 < |b|$. Wówczas $r_2 - r_1 = b(q_1 - q_2)$. Jeśli $r_2 - r_1 \neq 0$, to $|b| \leq |r_2 - r_1| \leq \max\{r_1, r_2\} < |b|$ zatem $r_2 - r_1 = 0$ i w konsekwencji $q_1 - q_2 = 0$ □

Przykłady: (1) $a = 26$ $b = 11$ wtedy $q = 2$ $r = 4$

(2) $a = -26$ $b = 11$ wtedy $q = -3$ $r = 7$

Def. 1: Niech $a, b \in \mathbb{Z}$. Mówimy, że <u>a dzieli b</u> (lub że <u>b jest podzielne przez a</u>) jeśli dla pewnego $q \in \mathbb{Z}$ $aq = b$. Oznaczamy $a \mid b$.

Przykłady: $2 \mid 4$, $3 \mid 18$, $-8 \mid 16$, $15 \nmid 10$, $0 \nmid 77$

Tw. 2: Niech $a, b, c \in \mathbb{Z}$, $\neq 0$ o ile konieczne. Wówczas

(1) $a \mid a$ (2) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

(3) $a \mid b \wedge b \mid a \Rightarrow a = b \vee a = -b$ (4) $a \mid 0$

(5) $1 \mid a$ (6) $a \mid b \Rightarrow a \mid bc$

(7) $a \mid b \wedge a \mid c \Rightarrow a \mid b + c$

Dowód: Udowodnimy dla przykładu (3):

Niech $b = q_1 a$ i $a = q_2 b$ dla pewnych $q_1, q_2 \in \mathbb{Z}$. Wówczas $b = q_1 q_2 b$, a zatem $q_1 q_2 = 1$, skąd $q_1 = q_2 = 1$ lub $q_1 = q_2 = -1$ □

Def. 2: Niech $a_1, \dots, a_k \in \mathbb{Z}$, $k \geq 2$. Liczbę $d \in \mathbb{N}$ taką, że
(1) $d | a_1, \dots, d | a_k$
(2) $e | a_1, \dots, e | a_k \Rightarrow e | d$
nazywamy największym wspólnym dzielnikiem $a_1, \dots, a_k$
i oznaczamy $NWD(a_1, \dots, a_k)$. Liczbę $m \in \mathbb{N}$ taką, że
(1) $a_1 | m, \dots, a_k | m$
(2) $a_1 | n, \dots, a_k | n \Rightarrow m | n$
nazywamy najmniejszą wspólną wielokrotnością $a_1, \dots, a_k$
i oznaczamy $NWW(a_1, \dots, a_k)$.
Przykłady: $NWD(24,36) = 12$. Uwaga! $6 | 24$ i $6 | 36$, ale $6 \neq NWD(24,36)$.
$NWW(24,36) = 72$. Uwaga! $24 | 144$ i $36 | 144$, ale $144 \neq NWW(24,36)$.
Tw. 3: Niech $a, b \in \mathbb{N}$. Wówczas $NWD(a,b) \cdot NWW(a,b) = a \cdot b$
Dowód: Rozważmy $\frac{ab}{NWD(a,b)}$. Ponieważ $a, b, NWD(a,b) \in \mathbb{N}$,
widzimy że $\frac{ab}{NWD(a,b)} > 0$. Ponadto $\frac{ab}{NWD(a,b)} \in \mathbb{Z}$.
Niech $NWD(a,b) \cdot q_1 = a$. Wówczas $\frac{ab}{NWD(a,b)} = \frac{NWD(a,b) q_1 b}{NWD(a,b)} = q_1 b$
a więc $b \,|\, \frac{ab}{NWD(a,b)}$. Analogicznie $a \,|\, \frac{ab}{NWD(a,b)}$. Wobec tego
$NWW(a,b) \,|\, \frac{ab}{NWD(a,b)}$, czyli $NWW(a,b) \cdot NWD(a,b) \,|\, ab$.
Rozważmy $\frac{ab}{NWW(a,b)}$. Zauważmy, że $\frac{ab}{NWW(a,b)} \in \mathbb{N}$.
Niech $NWW(a,b) = s_1 a$. Wówczas $\frac{ab}{NWW(a,b)} = \cancel{\frac{ab}{NWW(a,b)}}\ \frac{ab}{s_1 a} = \frac{b}{s_1}$.
Wobec tego $\frac{ab}{NWW(a,b)} \,|\, b$. Analogicznie $\frac{ab}{NWW(a,b)} \,|\, a$.
Wobec tego $\frac{ab}{NWW(a,b)} \,|\, NWD(a,b)$, czyli $ab \,|\, NWD(a,b) \cdot NWW(a,b)$ □
Przykłady: $NWD(24,36) \cdot NWW(24,36) = 12 \cdot 72 = 864 = 24 \cdot 36$
Tw. 4 (algorytm Euklidesa): Niech $a, b \in \mathbb{Z}$ i niech:

$$\begin{aligned}
a &= q_1 b + r_1, & 0 < r_1 < |b| \\
b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

Wówczas $r_n = NWD(a,b)$
Dowód: Algorytm zawsze się zatrzymuje, bo jest skończenie
wiele liczb naturalnych w przedziale $[0, |b|]$.
Pokażemy, że $r_n = NWD(a,b) (= d)$.
$r_n | d$ bo $r_n | r_{n-1} | r_{n-2} | \dots | r_1 | b | a$.
$d | r_n$ bo $d | a, b, r_1, r_2, \dots, r_n$ □

Przykłady: (1) Obliczamy $NWD(66,48)$:

$$66 = 1\cdot 48 + 18$$
$$48 = 2\cdot 18 + 12$$
$$18 = 1\cdot 12 + 6$$
$$12 = 2\cdot 6 \qquad \text{a więc } NWD(66,48) = 6.$$

(2) Dane wygenerowane przez algorytm Euklidesa pozwalają wyznaczyć liczby x i y takie, że:

$$66x + 48y = NWD(66,48).$$

$$6 = 18 - 12 = 18 - (48 - 2\cdot 18) = 3\cdot 18 - 48 =$$
$$= 3(66-48) - 48 = 3\cdot 66 - 4\cdot 48$$

a więc $x = 3$ $y = -4$.

Uwaga: Algorytm Euklidesa dostarcza metody rozwiązywania równań

$$ax + by = c \quad , \ a,b,c \in \mathbb{Z}.$$

Tw. 5: Niech $a,b,c \in \mathbb{Z}$. Równanie

$$ax + by = c$$

ma rozwiązanie w liczbach całkowitych wtw. gdy $d = NWD(a,b) \mid c$

Dowód: ($\Rightarrow$) Załóżmy, że $ax_0 + by_0 = c$ dla $x_0, y_0 \in \mathbb{Z}$. Wówczas $d \mid a$ i $d \mid b$, więc $d \mid ax_0$ i $d \mid by_0$, więc $d \mid ax_0 + by_0 = c$

($\Leftarrow$) Załóżmy, że $d \mid c$, $dq = c$. Wobec algorytmu Euklidesa istnieją x_1, y_1 takie, że $ax_1 + by_1 = d$. Wówczas $aqx_1 + bqy_1 = c$ □

Przykład: Rozwiążemy równanie $66x + 48y = 18$.
Wiemy, że $66\cdot 3 + 48(-4) = 6$, a więc $66\cdot 9 + 48(-12) = 18$.

Tw. 6: Niech $a,b,c \in \mathbb{Z}$ i niech $d = NWD(a,b) \mid c$. Niech x_0, y_0 będą rozwiązaniem równania $ax + by = c$. Wówczas wszystkie całkowite rozwiązania dane są przez

$$x = x_0 + \frac{bt}{d} \qquad y = y_0 - \frac{bt}{d}$$

Dowód: Sprawdzamy, że:

$$a\left(x_0 + \frac{bt}{d}\right) + b\left(y_0 - \frac{bt}{d}\right) = ax_0 + by_0 = c.$$

Niech x, y będzie rozwiązaniem. Wtedy $ax + by = c = ax_0 + by_0$.
Stąd $a(x - x_0) = b(y_0 - y)$ i $a_1(x - x_0) = b_1(y_0 - y)$, gdzie $a = a_1 d$, $b = b_1 d$. Ponieważ $NWD(a_1, b_1) = 1$, więc $b_1 \mid x - x_0$. Niech $x - x_0 = b_1 t$. Stąd $x = x_0 + b_1 t = x_0 + \frac{bt}{d}$.
Ponadto $a_1 b_1 t = b_1(y_0 - y)$, stąd $y = y_0 - \frac{at}{d}$ □

Przykład: Wszystkie rozwiązania równania

$$66x + 48y = 18$$

wyrażą się wzorami

$$x = 9 + 8t, \quad y = -12 - 11t$$