Analiza - klasa 2a   Zestaw 8.   24.10.2024

Teoria liczb III – NWD i NWW

Największy wspólny dzielnik liczb $a_1, a_2, \dots, a_k \in \mathbb{Z} \setminus \{0\}$ jest to liczba

$$\mathrm{NWD}(a_1, a_2, \dots, a_k) = \max\{d \in \mathbb{N} : d \mid a_1, d \mid a_2, \dots, d \mid a_k\}.$$

Tw. 1. (Tożsamość Bezout'a) Dla dowolnych liczb naturalnych $a_1, a_2, \dots, a_k$ istnieją liczby całkowite $x_1, x_2, \dots, x_k$ takie, że

$$\mathrm{NWD}(a_1, a_2, \dots, a_k) = a_1x_1 + a_2x_2 + \ldots + a_kx_k.$$

Tw. 2. Jeżeli d jest wspólnym dzielnikiem liczb $a_1, a_2, \dots, a_k$, to

$$d \mid \mathrm{NWD}(a_1, a_2, \dots, a_k).$$

Definicja. Mówimy, że liczby $a, b \in \mathbb{Z}$ są względnie pierwsze, jeżeli $\mathrm{NWD}(a, b) = 1$.

Tw. 3. Liczby $a, b \in \mathbb{Z}$ są względnie pierwsze wtedy i tylko wtedy, gdy istnieją $x, y \in \mathbb{Z}$ takie, że $ax + by = 1$.

Tw. 4 (Zasadnicze twierdzenie arytmetyki) Niech $a, b, d \in \mathbb{N}$, $\mathrm{NWD}(a, d) = 1$ i $d \mid ab$. Wówczas $d \mid b$.

Algorytm Euklidesa. $\mathrm{NWD}(a, b)$, gdzie $a \geqslant b > 0$, można wyznaczyć za pomocą następującego algorytmu: Niech $x_1 = a$, $x_2 = b$. Wykonujemy kolejne dzielenia z resztą, aż do otrzymania zerowej reszty:

$$\begin{aligned}
x_1 &= q_1x_2 + x_3, && 0 < x_3 < x_2\\
x_2 &= q_2x_3 + x_4, && 0 < x_4 < x_3\\
&\dots\\
x_{k-1} &= q_{k-1}x_k + x_{k+1}, && 0 < x_{k+1} < x_k\\
x_k &= q_kx_{k+1}.
\end{aligned}$$

Wówczas $\mathrm{NWD}(a, b) = x_{k+1}$ (ostatnia niezerowa reszta).

Definicja. Niech $a_1, a_2, \dots, a_k \in \mathbb{Z}$. Każdą liczbę $m \in \mathbb{N}$ taką, że $a_1 \mid m$, $a_2 \mid m$, …, $a_k \mid m$ nazywamy *wspólną wielokrotnością* liczb $a_1, a_2, \dots, a_k$.

Najmniejsza wspólna wielokrotność liczb $a_1, a_2, \dots, a_k$ jest to liczba

$$\mathrm{NWW}(a_1, a_2, \dots, a_k) = \min\{m \in \mathbb{N} : a_1 \mid m, a_2 \mid m, \dots, a_k \mid m\}.$$

Tw. 5. Jeżeli $m \in \mathbb{N}$ jest wspólną wielokrotnością liczb $a_1, a_2, \dots, a_k$, to

$$\mathrm{NWW}(a_1, a_2, \dots, a_k) \mid m.$$

Tw. 6. Niech $a, b \in \mathbb{N}$. Wówczas

$$\mathrm{NWW}(a, b) \cdot \mathrm{NWD}(a, b) = ab.$$

---

1. Niech $n \in \mathbb{Z}$. Udowodnij, że (a) $\mathrm{NWD}(n, n+1) = 1$, (b) $\mathrm{NWD}(2n-1, 2n+1) = 1$

2. Załóżmy, że $a, b \in \mathbb{Z}$. Pokaż, że $\mathrm{NWD}(5a + 3b, 13a + 8b) = \mathrm{NWD}(a, b)$.

3. Niech $a, b \in \mathbb{Z}$ i $d = \mathrm{NWD}(a, b)$. Wykaż, że liczby $\frac{a}{d}$ i $\frac{b}{d}$ są względnie pierwsze.

4. Niech $a, b, c \in \mathbb{N}$, $\mathrm{NWD}(a, b) = 1$ i $c \mid a$. Wykaż, że $\mathrm{NWD}(b, c) = 1$.

5.

6. Liczby $a, b, n \in \mathbb{N}$ spełniają warunki $a \mid n$, $b \mid n$ i $\mathrm{NWD}(a, b) = 1$. Udowodnij, że $ab \mid n$

7. Niech $a, b, k \in \mathbb{N}$. Udowodnij, że

(a) jeżeli $k \in \mathbb{N}$, to $\mathrm{NWD}(ka, kb) = k \cdot \mathrm{NWD}(a, b)$;

(b) jeżeli $k \in \mathbb{N}$ i $\mathrm{NWD}(k, b) = 1$, to $\mathrm{NWD}(ka, b) = \mathrm{NWD}(a, b)$;

(c) $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - b, \min(a, b))$.

8. Udowodnij, że każda liczba naturalna $n > 6$ jest sumą dwóch liczb naturalnych większych od 1 i względnie pierwszych.

9. Niech $n \in \mathbb{N}$. Udowodnij, że $\mathrm{NWD}(n! + 1, (n + 1)! + 1) = 1$.

10. Niech $n \in \mathbb{N}$ i $\mathrm{NWD}(6, n) = 1$. Udowodnij, że $24 \mid n^2 - 1$

11. Stosując algorytm Euklidesa oblicz $\mathrm{NWD}(a, b)$ i znajdź $x, y \in \mathbb{Z}$ takie, że $\mathrm{NWD}(a, b) = ax + by$, dla

(a) $a = 329$, $b = 182$,

(b) $a = 1492$, $b = 1066$,

(c) $a = 1745$, $b = 1485$,

(d) $a = 13832$, $b = 7254$.

12. Niech $a, b, c \in \mathbb{N}$. Udowodnij, że $\mathrm{NWD}(a, b, c) = \mathrm{NWD}\big(\mathrm{NWD}(a, b), c\big)$.

13. Niech $m, n \in \mathbb{N}$ i m jest liczbą nieparzystą. Udowodnij, że liczby $2^m - 1$ i $2^n + 1$ są względnie pierwsze.

14. Niech $n \in \mathbb{N}$. Pokaż, że

$$\mathrm{NWW}(1, 2, 3, \dots, 2n) = \mathrm{NWW}(n + 1, n + 2, \dots, 2n).$$

15. Niech $a, b \in \mathbb{N}$. Udowodnij, że $\mathrm{NWD}(2^a - 1, 2^b - 1) = 2^{\mathrm{NWD}(a,b)} - 1$.

16. Liczby a, b, n są naturalne i $\mathrm{NWD}(a, b, n) = 1$. Udowodnij, że istnieją liczby naturalne x, y takie, że $\mathrm{NWD}(x, y) = 1$ oraz

$$a \equiv x \pmod{n} \qquad \text{i} \qquad b \equiv y \pmod{n}.$$