Wykład 1
Teoria podzielności w zbiorze liczb całkowitych

Andrzej Sładek
sladek@ux2.math.us.edu.pl

Instytut Matematyki, Uniwersytet Śląski w Katowicach

Wykład jest przewidziany na 4 godziny lekcyjne

Wykład jest przewidziany na 4 godziny lekcyjne

Tematy poruszane na wykładzie można znaleźć w:

Wykład jest przewidziany na 4 godziny lekcyjne

Tematy poruszane na wykładzie można znaleźć w:

- A.I. Kostrykin, *Wstęp do algebry, t. I,* PWN 2004, [rozdz. I, §7, §9]
- W. Marzantowicz, P. Zarzycki, *Elementarna teoria liczb,* PWN 2006, [wykłady 1,2,7]

Oznaczenia zbiorów liczbowych

$\mathbb{N}$ - zbiór liczb naturalnych

Oznaczenia zbiorów liczbowych

$\mathbb{N}$ - zbiór liczb naturalnych

$\mathbb{Z}$ - zbiór liczb całkowitych

Oznaczenia zbiorów liczbowych

$\mathbb{N}$ - zbiór liczb naturalnych

$\mathbb{Z}$ - zbiór liczb całkowitych

$\mathbb{Q}$ - zbiór liczb wymiernych

Oznaczenia zbiorów liczbowych

$\mathbb{N}$ - zbiór liczb naturalnych

$\mathbb{Z}$ - zbiór liczb całkowitych

$\mathbb{Q}$ - zbiór liczb wymiernych

$\mathbb{R}$ - zbiór liczb rzeczywistych

Zasada indukcji matematycznej

Zasada indukcji matematycznej

Niech $T(n)$ będzie zdaniem zależnym od liczby $n \in \mathbb{N}$.

Zasada indukcji matematycznej

Niech $T(n)$ będzie zdaniem zależnym od liczby $n \in \mathbb{N}$. Jeśli

- $T(1)$ jest zdaniem prawdziwym,

Zasada indukcji matematycznej

Niech $T(n)$ będzie zdaniem zależnym od liczby $n \in \mathbb{N}$. Jeśli

- $T(1)$ jest zdaniem prawdziwym,
- dla każdego $n \in \mathbb{N}$ z tego, że $T(n)$ jest zdaniem prawdziwym wynika, że $T(n+1)$ jest zdaniem prawdziwym,

Zasada indukcji matematycznej

Niech $T(n)$ będzie zdaniem zależnym od liczby $n \in \mathbb{N}$. Jeśli

- $T(1)$ jest zdaniem prawdziwym,
- dla każdego $n \in \mathbb{N}$ z tego, że $T(n)$ jest zdaniem prawdziwym wynika, że $T(n+1)$ jest zdaniem prawdziwym,

Zasada indukcji matematycznej

Niech $T(n)$ będzie zdaniem zależnym od liczby $n \in \mathbb{N}$. Jeśli

- $T(1)$ jest zdaniem prawdziwym,
- dla każdego $n \in \mathbb{N}$ z tego, że $T(n)$ jest zdaniem prawdziwym wynika, że $T(n+1)$ jest zdaniem prawdziwym,

to $T(n)$ jest zdaniem prawdziwym dla każdego $n \in \mathbb{N}$.

Zasada indukcji matematycznej

Niech $T(n)$ będzie zdaniem zależnym od liczby $n \in \mathbb{N}$. Jeśli

- $T(1)$ jest zdaniem prawdziwym,
- dla każdego $n \in \mathbb{N}$ z tego, że $T(n)$ jest zdaniem prawdziwym wynika, że $T(n+1)$ jest zdaniem prawdziwym,

to $T(n)$ jest zdaniem prawdziwym dla każdego $n \in \mathbb{N}$.

Zasada minimum

Dowolny niepusty podzbiór zbioru liczb naturalnych posiada element najmniejszy.

Zasada indukcji matematycznej

Niech $T(n)$ będzie zdaniem zależnym od liczby $n \in \mathbb{N}$. Jeśli

- $T(1)$ jest zdaniem prawdziwym,
- dla każdego $n \in \mathbb{N}$ z tego, że $T(n)$ jest zdaniem prawdziwym wynika, że $T(n+1)$ jest zdaniem prawdziwym,

to $T(n)$ jest zdaniem prawdziwym dla każdego $n \in \mathbb{N}$.

Zasada minimum

Dowolny niepusty podzbiór zbioru liczb naturalnych posiada element najmniejszy.

Zasada maksimum

Dowolny niepusty oraz ograniczony podzbiór zbioru liczb naturalnych posiada element największy.

Twierdzenie o dzieleniu z resztą

Dla dowolnych liczb $a, b \in \mathbb{Z}$, $b \neq 0$, istnieją jednoznacznie wyznaczone takie liczby $q \in \mathbb{Z}$ i $r \in \{0, 1, ..., |b| - 1\}$, że $a = bq + r$.

Twierdzenie o dzieleniu z resztą

Dla dowolnych liczb $a, b \in \mathbb{Z}$, $b \neq 0$, istnieją jednoznacznie wyznaczone takie liczby $q \in \mathbb{Z}$ i $r \in \{0, 1, ..., |b| - 1\}$, że $a = bq + r$.

Dowód. Zbiór

$$A = \{q \in \mathbb{Z} : |b|q \leqslant a\}$$

jest ograniczony z góry.

Twierdzenie o dzieleniu z resztą

Dla dowolnych liczb $a, b \in \mathbb{Z}$, $b \neq 0$, istnieją jednoznacznie wyznaczone takie liczby $q \in \mathbb{Z}$ i $r \in \{0, 1, ..., |b| - 1\}$, że $a = bq + r$.

Dowód. Zbiór

$$A = \{q \in \mathbb{Z} : |b|q \leqslant a\}$$

jest ograniczony z góry. Niech $q = \max(A)$.

Twierdzenie o dzieleniu z resztą

Dla dowolnych liczb $a, b \in \mathbb{Z}$, $b \neq 0$, istnieją jednoznacznie wyznaczone takie liczby $q \in \mathbb{Z}$ i $r \in \{0, 1, ..., |b| - 1\}$, że $a = bq + r$.

Dowód. Zbiór

$$A = \{q \in \mathbb{Z} : |b|q \leqslant a\}$$

jest ograniczony z góry. Niech $q = \max(A)$. Zatem

$$|b|q \leqslant a < |b|(q + 1).$$

Twierdzenie o dzieleniu z resztą

Dla dowolnych liczb $a, b \in \mathbb{Z}$, $b \neq 0$, istnieją jednoznacznie wyznaczone takie liczby $q \in \mathbb{Z}$ i $r \in \{0, 1, ..., |b| - 1\}$, że $a = bq + r$.

Dowód. Zbiór

$$A = \{q \in \mathbb{Z} : |b|q \leqslant a\}$$

jest ograniczony z góry. Niech $q = \max(A)$. Zatem

$$|b|q \leqslant a < |b|(q + 1).$$

Wtedy dla $r = a - |b|q$ mamy

$$0 \leqslant r \leqslant |b| - 1$$

Twierdzenie o dzieleniu z resztą

Dla dowolnych liczb $a, b \in \mathbb{Z}$, $b \neq 0$, istnieją jednoznacznie wyznaczone takie liczby $q \in \mathbb{Z}$ i $r \in \{0, 1, ..., |b| - 1\}$, że $a = bq + r$.

Dowód. Zbiór

$$A = \{q \in \mathbb{Z} : |b|q \leqslant a\}$$

jest ograniczony z góry. Niech $q = \max(A)$. Zatem

$$|b|q \leqslant a < |b|(q + 1).$$

Wtedy dla $r = a - |b|q$ mamy

$$0 \leqslant r \leqslant |b| - 1$$

Pozostaje udowodnić jednoznaczność pary q, r (*dowód na tablicy*). ¶

Twierdzenie o dzieleniu z resztą

Dla dowolnych liczb $a, b \in \mathbb{Z}$, $b \neq 0$, istnieją jednoznacznie wyznaczone takie liczby $q \in \mathbb{Z}$ i $r \in \{0, 1, ..., |b| - 1\}$, że $a = bq + r$.

Dowód. Zbiór

$$A = \{q \in \mathbb{Z} : |b|q \leqslant a\}$$

jest ograniczony z góry. Niech $q = \max(A)$. Zatem

$$|b|q \leqslant a < |b|(q + 1).$$

Wtedy dla $r = a - |b|q$ mamy

$$0 \leqslant r \leqslant |b| - 1$$

Pozostaje udowodnić jednoznaczność pary q, r (*dowód na tablicy*). ¶

Liczbę r z poprzedniego twierdzenia nazywamy ***resztą***, i oznaczamy ją $(a)_b$, natomiast liczbę q nazywamy ***ilorazem*** z dzielenia liczby a przez b.

Wniosek

Jeżeli X jest niepustym podzbiorem zbioru $\mathbb{Z}$ zamkniętym ze względu na odejmowanie, tzn.

$$x, y \in X \implies x - y \in X,$$

to istnieje liczba naturalna d taka, że $X = \{xd : x \in \mathbb{Z}\}$.

Wniosek

Jeżeli X jest niepustym podzbiorem zbioru $\mathbb{Z}$ zamkniętym ze względu na odejmowanie, tzn.

$$x, y \in X \implies x - y \in X,$$

to istnieje liczba naturalna d taka, że $X = \{xd : x \in \mathbb{Z}\}$.

Dowód na tablicy.

Definicja

Mówimy, że liczba całkowita b dzieli liczbę całkowitą a (ozn. $b \mid a$), jeśli istnieje liczba całkowita c, że $a = b \cdot c$.

Definicja

Mówimy, że liczba całkowita b dzieli liczbę całkowitą a (ozn. $b \mid a$), jeśli istnieje liczba całkowita c, że $a = b \cdot c$.

W przypadku $b \neq 0$ mamy

$$b \mid a \iff (a)_b = 0$$

Definicja

Mówimy, że liczba całkowita b dzieli liczbę całkowitą a (ozn. $b \mid a$), jeśli istnieje liczba całkowita c, że $a = b \cdot c$.

W przypadku $b \neq 0$ mamy

$$b \mid a \iff (a)_b = 0$$

Własności relacji podzielności:

Definicja

Mówimy, że liczba całkowita b dzieli liczbę całkowitą a (ozn. $b \mid a$), jeśli istnieje liczba całkowita c, że $a = b \cdot c$.

W przypadku $b \neq 0$ mamy

$$b \mid a \iff (a)_b = 0$$

Własności relacji podzielności:

- $a \mid 0$

Definicja

Mówimy, że liczba całkowita b dzieli liczbę całkowitą a (ozn. $b \mid a$), jeśli istnieje liczba całkowita c, że $a = b \cdot c$.

W przypadku $b \neq 0$ mamy

$$b \mid a \iff (a)_b = 0$$

Własności relacji podzielności:

- $a \mid 0$
- $0 \mid a \iff a = 0$

Definicja

Mówimy, że liczba całkowita b dzieli liczbę całkowitą a (ozn. $b \mid a$), jeśli istnieje liczba całkowita c, że $a = b \cdot c$.

W przypadku $b \neq 0$ mamy

$$b \mid a \iff (a)_b = 0$$

Własności relacji podzielności:

- $a \mid 0$
- $0 \mid a \iff a = 0$
- $a \mid a$

Definicja

Mówimy, że liczba całkowita b dzieli liczbę całkowitą a (ozn. $b \mid a$), jeśli istnieje liczba całkowita c, że $a = b \cdot c$.

W przypadku $b \neq 0$ mamy

$$b \mid a \iff (a)_b = 0$$

Własności relacji podzielności:

- $a \mid 0$
- $0 \mid a \iff a = 0$
- $a \mid a$
- $a \mid b \,,\ b \mid a \implies a = \pm b$

Definicja

Mówimy, że liczba całkowita b dzieli liczbę całkowitą a (ozn. $b \mid a$), jeśli istnieje liczba całkowita c, że $a = b \cdot c$.

W przypadku $b \neq 0$ mamy

$$b \mid a \iff (a)_b = 0$$

Własności relacji podzielności:

- $a \mid 0$
- $0 \mid a \iff a = 0$
- $a \mid a$
- $a \mid b\,,\ b \mid a \implies a = \pm b$
- $a \mid b\,,\ b \mid c \implies a \mid c$; w szczególności $a \mid b \implies a \mid kb$

Definicja

Mówimy, że liczba całkowita b dzieli liczbę całkowitą a (ozn. $b \mid a$), jeśli istnieje liczba całkowita c, że $a = b \cdot c$.

W przypadku $b \neq 0$ mamy

$$b \mid a \iff (a)_b = 0$$

Własności relacji podzielności:

- $a \mid 0$
- $0 \mid a \iff a = 0$
- $a \mid a$
- $a \mid b\,,\ b \mid a \implies a = \pm b$
- $a \mid b\,,\ b \mid c \implies a \mid c$; w szczególności $a \mid b \implies a \mid kb$
- $a \mid b\,,\ c \mid d \implies ac \mid bd$; w szczególności $a \mid b \implies ac \mid bc$

Definicja

Mówimy, że liczba całkowita b dzieli liczbę całkowitą a (ozn. $b \mid a$), jeśli istnieje liczba całkowita c, że $a = b \cdot c$.

W przypadku $b \neq 0$ mamy

$$b \mid a \iff (a)_b = 0$$

Własności relacji podzielności:

- $a \mid 0$
- $0 \mid a \iff a = 0$
- $a \mid a$
- $a \mid b\,,\ b \mid a \implies a = \pm b$
- $a \mid b\,,\ b \mid c \implies a \mid c$; w szczególności $a \mid b \implies a \mid kb$
- $a \mid b\,,\ c \mid d \implies ac \mid bd$; w szczególności $a \mid b \implies ac \mid bc$
- $d \mid a\,,\ d \mid b \implies d \mid xa + yb$.

Definicja

Liczbę całkowitą d nazywamy ***największym wspólnym dzielnikiem*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

Definicja

Liczbę całkowitą d nazywamy ***największym wspólnym dzielnikiem*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

- $d \mid a_1, \ldots, d \mid a_n$,

Definicja

Liczbę całkowitą d nazywamy ***największym wspólnym dzielnikiem*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

- $d \mid a_1, \ldots, d \mid a_n$,
- $c \mid a_1, \ldots, c \mid a_n \implies c \mid d$.

Definicja

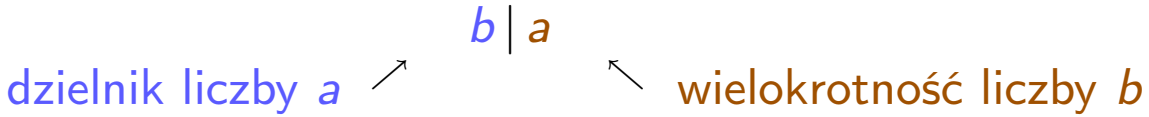
Liczbę całkowitą d nazywamy ***największym wspólnym dzielnikiem*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

- $d \mid a_1, \ldots, d \mid a_n$,
- $c \mid a_1, \ldots, c \mid a_n \implies c \mid d$.

Definicja

Liczbę całkowitą d nazywamy ***największym wspólnym dzielnikiem*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

- $d \mid a_1, \ldots, d \mid a_n$,
- $c \mid a_1, \ldots, c \mid a_n \implies c \mid d$.



Definicja

Liczbę całkowitą d nazywamy ***największym wspólnym dzielnikiem*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

- $d \mid a_1, \ldots, d \mid a_n$,
- $c \mid a_1, \ldots, c \mid a_n \implies c \mid d$.

$$b \mid a$$

dzielnik liczby a ↗ ↖ wielokrotność liczby b

Definicja

Liczbę całkowitą e nazywamy ***najmniejszą wspólną wielokrotnością*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

Definicja

Liczbę całkowitą d nazywamy ***największym wspólnym dzielnikiem*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

- $d \mid a_1, \ldots, d \mid a_n$,
- $c \mid a_1, \ldots, c \mid a_n \implies c \mid d$.

$b \mid a$

dzielnik liczby a ↗ ↖ wielokrotność liczby b

Definicja

Liczbę całkowitą e nazywamy ***najmniejszą wspólną wielokrotnością*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

- $a_1 \mid e, \ldots, a_n \mid e$,

Definicja

Liczbę całkowitą d nazywamy ***największym wspólnym dzielnikiem*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

- $d \mid a_1, \ldots, d \mid a_n$,
- $c \mid a_1, \ldots, c \mid a_n \implies c \mid d$.

$b \mid a$

dzielnik liczby a ↗ ↖ wielokrotność liczby b

Definicja

Liczbę całkowitą e nazywamy ***najmniejszą wspólną wielokrotnością*** liczb całkowitych $a_1, \ldots, a_n$, jeśli

- $a_1 \mid e, \ldots, a_n \mid e$,
- $a_1 \mid c, \ldots, a_n \mid c \implies e \mid c$.

Uwaga

Jeśli nie wszystkie $a_1, ..., a_n$ są równe zero, to

Uwaga

Jeśli nie wszystkie $a_1, ..., a_n$ są równe zero, to

- Największy wspólny dzielnik liczb $a_1, ..., a_n$ istnieje i jest wyznaczony jednoznacznie z dokładnością do znaku.
  Ozn. NWD$(a_1, ..., a_n)$.

Uwaga

Jeśli nie wszystkie $a_1, ..., a_n$ są równe zero, to

- Największy wspólny dzielnik liczb $a_1, ..., a_n$ istnieje i jest wyznaczony jednoznacznie z dokładnością do znaku.
  Ozn. $\mathrm{NWD}(a_1, ..., a_n)$.
- Najmniejsza wspólna wielokrotność liczb $a_1, ..., a_n$ istnieje i jest wyznaczona jednoznacznie z dokładnością do znaku.
  Ozn. $\mathrm{NWW}(a_1, ..., a_n)$.

Uwaga

Jeśli nie wszystkie $a_1, ..., a_n$ są równe zero, to

- Największy wspólny dzielnik liczb $a_1, ..., a_n$ istnieje i jest wyznaczony jednoznacznie z dokładnością do znaku.
  Ozn. $\mathrm{NWD}(a_1, ..., a_n)$.
- Najmniejsza wspólna wielokrotność liczb $a_1, ..., a_n$ istnieje i jest wyznaczona jednoznacznie z dokładnością do znaku.
  Ozn. $\mathrm{NWW}(a_1, ..., a_n)$.

Uwaga

Jeśli nie wszystkie $a_1, ..., a_n$ są równe zero, to

- Największy wspólny dzielnik liczb $a_1, ..., a_n$ istnieje i jest wyznaczony jednoznacznie z dokładnością do znaku.
  Ozn. $\mathrm{NWD}(a_1, ..., a_n)$.
- Najmniejsza wspólna wielokrotność liczb $a_1, ..., a_n$ istnieje i jest wyznaczona jednoznacznie z dokładnością do znaku.
  Ozn. $\mathrm{NWW}(a_1, ..., a_n)$.

Wyjaśnienie na tablicy.

Uwaga

Jeśli nie wszystkie $a_1, ..., a_n$ są równe zero, to

- Największy wspólny dzielnik liczb $a_1, ..., a_n$ istnieje i jest wyznaczony jednoznacznie z dokładnością do znaku.
  Ozn. $\mathrm{NWD}(a_1, ..., a_n)$.
- Najmniejsza wspólna wielokrotność liczb $a_1, ..., a_n$ istnieje i jest wyznaczona jednoznacznie z dokładnością do znaku.
  Ozn. $\mathrm{NWW}(a_1, ..., a_n)$.

Wyjaśnienie na tablicy.

Definicja

Liczby $a_1, ..., a_n$ nazywamy ***względnie pierwszymi***, jeśli $\mathrm{NWD}(a_1, ..., a_n) = 1$.

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\text{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\text{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\text{NWD}(a_1, ..., a_n) = \text{NWD}(\text{NWD}(a_1, ..., a_{n-1}), a_n)$

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\text{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\text{NWD}(a_1, ..., a_n) = \text{NWD}(\text{NWD}(a_1, ..., a_{n-1}), a_n)$
- $\text{NWD}(a, 0) = a$

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\text{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\text{NWD}(a_1, ..., a_n) = \text{NWD}(\text{NWD}(a_1, ..., a_{n-1}), a_n)$
- $\text{NWD}(a, 0) = a$
- $\text{NWD}(a, b) = \text{NWD}(a - kb, b)$ dla dowolnego $k \in \mathbb{Z}$;

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\text{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\text{NWD}(a_1, ..., a_n) = \text{NWD}(\text{NWD}(a_1, ..., a_{n-1}), a_n)$
- $\text{NWD}(a, 0) = a$
- $\text{NWD}(a, b) = \text{NWD}(a - kb, b)$ dla dowolnego $k \in \mathbb{Z}$;

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\text{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\text{NWD}(a_1, ..., a_n) = \text{NWD}(\text{NWD}(a_1, ..., a_{n-1}), a_n)$
- $\text{NWD}(a, 0) = a$
- $\text{NWD}(a, b) = \text{NWD}(a - kb, b)$ dla dowolnego $k \in \mathbb{Z}$;

  w szczególności $\text{NWD}(a, b) = \text{NWD}(b, (a)_b)$ o ile $b \neq 0$

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\mathrm{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\mathrm{NWD}(a_1, ..., a_n) = \mathrm{NWD}(\mathrm{NWD}(a_1, ..., a_{n-1}), a_n)$
- $\mathrm{NWD}(a, 0) = a$
- $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - kb, b)$ dla dowolnego $k \in \mathbb{Z}$;

  w szczególności $\mathrm{NWD}(a, b) = \mathrm{NWD}(b, (a)_b)$ o ile $b \neq 0$
- $\mathrm{NWD}(ac, bc) = c\,\mathrm{NWD}(a, b)$

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\mathrm{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\mathrm{NWD}(a_1, ..., a_n) = \mathrm{NWD}(\mathrm{NWD}(a_1, ..., a_{n-1}), a_n)$
- $\mathrm{NWD}(a, 0) = a$
- $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - kb, b)$ dla dowolnego $k \in \mathbb{Z}$;

  w szczególności $\mathrm{NWD}(a, b) = \mathrm{NWD}(b, (a)_b)$ o ile $b \neq 0$
- $\mathrm{NWD}(ac, bc) = c\,\mathrm{NWD}(a, b)$
- $d = \mathrm{NWD}(a, b) \implies \mathrm{NWD}(\frac{a}{d}, \frac{b}{d}) = 1$

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\mathrm{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\mathrm{NWD}(a_1, ..., a_n) = \mathrm{NWD}(\mathrm{NWD}(a_1, ..., a_{n-1}), a_n)$
- $\mathrm{NWD}(a, 0) = a$
- $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - kb, b)$ dla dowolnego $k \in \mathbb{Z}$;

  w szczególności $\mathrm{NWD}(a, b) = \mathrm{NWD}(b, (a)_b)$ o ile $b \neq 0$
- $\mathrm{NWD}(ac, bc) = c\,\mathrm{NWD}(a, b)$
- $d = \mathrm{NWD}(a, b) \implies \mathrm{NWD}(\frac{a}{d}, \frac{b}{d}) = 1$
- $c \mid ab,\ \mathrm{NWD}(c, a) = 1 \implies c \mid b$

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\mathrm{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\mathrm{NWD}(a_1, ..., a_n) = \mathrm{NWD}(\mathrm{NWD}(a_1, ..., a_{n-1}), a_n)$
- $\mathrm{NWD}(a, 0) = a$
- $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - kb, b)$ dla dowolnego $k \in \mathbb{Z}$;

  w szczególności $\mathrm{NWD}(a, b) = \mathrm{NWD}(b, (a)_b)$ o ile $b \neq 0$
- $\mathrm{NWD}(ac, bc) = c\,\mathrm{NWD}(a, b)$
- $d = \mathrm{NWD}(a, b) \implies \mathrm{NWD}(\frac{a}{d}, \frac{b}{d}) = 1$
- $c \mid ab,\ \mathrm{NWD}(c, a) = 1 \implies c \mid b$
- $a \mid c\ ,\ b \mid c,\ \mathrm{NWD}(a, b) = 1 \implies ab \mid c$

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\mathrm{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\mathrm{NWD}(a_1, ..., a_n) = \mathrm{NWD}(\mathrm{NWD}(a_1, ..., a_{n-1}), a_n)$
- $\mathrm{NWD}(a, 0) = a$
- $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - kb, b)$ dla dowolnego $k \in \mathbb{Z}$;

  w szczególności $\mathrm{NWD}(a, b) = \mathrm{NWD}(b, (a)_b)$ o ile $b \neq 0$
- $\mathrm{NWD}(ac, bc) = c\,\mathrm{NWD}(a, b)$
- $d = \mathrm{NWD}(a, b) \implies \mathrm{NWD}(\frac{a}{d}, \frac{b}{d}) = 1$
- $c \mid ab,\ \mathrm{NWD}(c, a) = 1 \implies c \mid b$
- $a \mid c\ ,\ b \mid c,\ \mathrm{NWD}(a, b) = 1 \implies ab \mid c$

Własności NWD

- Istnieją $x_1, ..., x_n \in \mathbb{Z}$ takie, że $\mathrm{NWD}(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$
- $\mathrm{NWD}(a_1, ..., a_n) = \mathrm{NWD}(\mathrm{NWD}(a_1, ..., a_{n-1}), a_n)$
- $\mathrm{NWD}(a, 0) = a$
- $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - kb, b)$ dla dowolnego $k \in \mathbb{Z}$;

  w szczególności $\mathrm{NWD}(a, b) = \mathrm{NWD}(b, (a)_b)$ o ile $b \neq 0$
- $\mathrm{NWD}(ac, bc) = c\,\mathrm{NWD}(a, b)$
- $d = \mathrm{NWD}(a, b) \implies \mathrm{NWD}(\frac{a}{d}, \frac{b}{d}) = 1$
- $c \mid ab,\ \mathrm{NWD}(c, a) = 1 \implies c \mid b$
- $a \mid c\ ,\ b \mid c,\ \mathrm{NWD}(a, b) = 1 \implies ab \mid c$

Dowód pierwszej własności na tablicy, a pozostałych na ćwiczeniach (zestaw 1, zad.6)

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$309 \quad = \quad 1 \cdot 186 + 123$$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \end{aligned}$$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \end{aligned}$$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \\ 63 &= 1 \cdot 60 + 3 \end{aligned}$$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \\ 63 &= 1 \cdot 60 + 3 \\ 60 &= 20 \cdot 3 + 0 \end{aligned}$$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \\ 63 &= 1 \cdot 60 + 3 \\ 60 &= 20 \cdot 3 + 0 \end{aligned}$$

Wtedy mamy $\text{NWD}(309, 186) = 3$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \\ 63 &= 1 \cdot 60 + 3 \\ 60 &= 20 \cdot 3 + 0 \end{aligned}$$

Wtedy mamy $\text{NWD}(309, 186) = 3$

Zobaczmy teraz jak znaleźć takie $x, y \in \mathbb{Z}$, że $\mathbf{3 = 309x + 186y}$.

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \\ 63 &= 1 \cdot 60 + 3 \\ 60 &= 20 \cdot 3 + 0 \end{aligned}$$

Wtedy mamy $\text{NWD}(309, 186) = 3$

Zobaczmy teraz jak znaleźć takie $x, y \in \mathbb{Z}$, że $\mathbf{3 = 309x + 186y}$.

$$3 = 63 - 1 \cdot 60 =$$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \\ 63 &= 1 \cdot 60 + 3 \\ 60 &= 20 \cdot 3 + 0 \end{aligned}$$

Wtedy mamy $\text{NWD}(309, 186) = 3$

Zobaczmy teraz jak znaleźć takie $x, y \in \mathbb{Z}$, że $\mathbf{3 = 309x + 186y}$.

$$\begin{aligned} 3 &= 63 - 1 \cdot 60 = \\ &= 63 - 1 \cdot (123 - 1 \cdot 63) = 2 \cdot 63 - 1 \cdot 123 = \end{aligned}$$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \\ 63 &= 1 \cdot 60 + 3 \\ 60 &= 20 \cdot 3 + 0 \end{aligned}$$

Wtedy mamy $\mathrm{NWD}(309, 186) = 3$

Zobaczmy teraz jak znaleźć takie $x, y \in \mathbb{Z}$, że $\mathbf{3 = 309x + 186y}$.

$$\begin{aligned} 3 &= 63 - 1 \cdot 60 = \\ &= 63 - 1 \cdot (123 - 1 \cdot 63) = 2 \cdot 63 - 1 \cdot 123 = \\ &= 2 \cdot (186 - 1 \cdot 123) - 1 \cdot 123 = 2 \cdot 186 - 3 \cdot 123 = \end{aligned}$$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \\ 63 &= 1 \cdot 60 + 3 \\ 60 &= 20 \cdot 3 + 0 \end{aligned}$$

Wtedy mamy $\text{NWD}(309, 186) = 3$

Zobaczmy teraz jak znaleźć takie $x, y \in \mathbb{Z}$, że $\mathbf{3 = 309x + 186y}$.

$$\begin{aligned} 3 &= 63 - 1 \cdot 60 = \\ &= 63 - 1 \cdot (123 - 1 \cdot 63) = 2 \cdot 63 - 1 \cdot 123 = \\ &= 2 \cdot (186 - 1 \cdot 123) - 1 \cdot 123 = 2 \cdot 186 - 3 \cdot 123 = \\ &= 2 \cdot 186 - 3 \cdot (309 - 1 \cdot 186) = \end{aligned}$$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \\ 63 &= 1 \cdot 60 + 3 \\ 60 &= 20 \cdot 3 + 0 \end{aligned}$$

Wtedy mamy $\text{NWD}(309, 186) = 3$

Zobaczmy teraz jak znaleźć takie $x, y \in \mathbb{Z}$, że $\mathbf{3 = 309x + 186y}$.

$$\begin{aligned} 3 &= 63 - 1 \cdot 60 = \\ &= 63 - 1 \cdot (123 - 1 \cdot 63) = 2 \cdot 63 - 1 \cdot 123 = \\ &= 2 \cdot (186 - 1 \cdot 123) - 1 \cdot 123 = 2 \cdot 186 - 3 \cdot 123 = \\ &= 2 \cdot 186 - 3 \cdot (309 - 1 \cdot 186) = \\ &= -3 \cdot 309 + 5 \cdot 186 \end{aligned}$$

Do obliczenia NWD(a, b) można zastosować tzw. algorytm Euklidesa. Pokażemy to na przykładzie liczb $\mathbf{a = 309}$ oraz $\mathbf{b = 186}$.

$$\begin{aligned} 309 &= 1 \cdot 186 + 123 \\ 186 &= 1 \cdot 123 + 63 \\ 123 &= 1 \cdot 63 + 60 \\ 63 &= 1 \cdot 60 + 3 \\ 60 &= 20 \cdot 3 + 0 \end{aligned}$$

Wtedy mamy $\text{NWD}(309, 186) = 3$

Zobaczmy teraz jak znaleźć takie $x, y \in \mathbb{Z}$, że $\mathbf{3 = 309x + 186y}$.

$$\begin{aligned} 3 &= 63 - 1 \cdot 60 = \\ &= 63 - 1 \cdot (123 - 1 \cdot 63) = 2 \cdot 63 - 1 \cdot 123 = \\ &= 2 \cdot (186 - 1 \cdot 123) - 1 \cdot 123 = 2 \cdot 186 - 3 \cdot 123 = \\ &= 2 \cdot 186 - 3 \cdot (309 - 1 \cdot 186) = \\ &= -3 \cdot 309 + 5 \cdot 186 \end{aligned}$$

Zatem $\mathbf{3 = 309 \cdot (-3) + 186 \cdot 5}$, więc $\mathbf{x = -3}$, $\mathbf{y = 5}$.

Definicja

Liczbę naturalną p nazywamy ***liczbą pierwszą***, jeśli posiada dokładnie dwa różne dzielniki naturalne.

Definicja

Liczbę naturalną p nazywamy ***liczbą pierwszą***, jeśli posiada dokładnie dwa różne dzielniki naturalne. Zbiór liczb pierwszych oznaczać będziemy literą $\mathbb{P}$.

Definicja

Liczbę naturalną p nazywamy ***liczbą pierwszą***, jeśli posiada dokładnie dwa różne dzielniki naturalne. Zbiór liczb pierwszych oznaczać będziemy literą $\mathbb{P}$.

Twierdzenie

Niech p będzie liczba naturalną różną od 1. Wtedy $p \in \mathbb{P}$ wtedy i tylko wtedy, gdy dla każdych $a, b \in \mathbb{N}$ spełniony jest warunek

$$p \mid ab \implies p \mid a \text{ lub } p \mid b.$$

Definicja

Liczbę naturalną p nazywamy ***liczbą pierwszą***, jeśli posiada dokładnie dwa różne dzielniki naturalne. Zbiór liczb pierwszych oznaczać będziemy literą $\mathbb{P}$.

Twierdzenie

Niech p będzie liczba naturalną różną od 1. Wtedy $p \in \mathbb{P}$ wtedy i tylko wtedy, gdy dla każdych $a, b \in \mathbb{N}$ spełniony jest warunek

$$p \mid ab \implies p \mid a \text{ lub } p \mid b.$$

Zasadnicze twierdzenie arytmetyki

Dowolna liczba naturalna $n > 1$ ma jednoznacze przedstawienie w postaci

$$n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}, \text{ gdzie } p_1, \ldots, p_s \in \mathbb{P} \text{ są parami różne}, s, k_1, \ldots, k_s \in \mathbb{N}.$$

Definicja

Liczbę naturalną p nazywamy ***liczbą pierwszą***, jeśli posiada dokładnie dwa różne dzielniki naturalne. Zbiór liczb pierwszych oznaczać będziemy literą $\mathbb{P}$.

Twierdzenie

Niech p będzie liczba naturalną różną od 1. Wtedy $p \in \mathbb{P}$ wtedy i tylko wtedy, gdy dla każdych $a, b \in \mathbb{N}$ spełniony jest warunek

$$p \mid ab \implies p \mid a \text{ lub } p \mid b.$$

Zasadnicze twierdzenie arytmetyki

Dowolna liczba naturalna $n > 1$ ma jednoznacze przedstawienie w postaci

$$n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}, \text{ gdzie } p_1, \ldots, p_s \in \mathbb{P} \text{ są parami różne}, s, k_1, \ldots, k_s \in \mathbb{N}.$$

Przedstawienie liczby n w tym twierdzeniu nazywamy ***rozkładem kanonicznym***.

Definicja

Liczbę naturalną p nazywamy ***liczbą pierwszą***, jeśli posiada dokładnie dwa różne dzielniki naturalne. Zbiór liczb pierwszych oznaczać będziemy literą $\mathbb{P}$.

Twierdzenie

Niech p będzie liczba naturalną różną od 1. Wtedy $p \in \mathbb{P}$ wtedy i tylko wtedy, gdy dla każdych $a, b \in \mathbb{N}$ spełniony jest warunek

$$p \mid ab \implies p \mid a \text{ lub } p \mid b.$$

Zasadnicze twierdzenie arytmetyki

Dowolna liczba naturalna $n > 1$ ma jednoznacze przedstawienie w postaci

$$n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}, \text{ gdzie } p_1, \ldots, p_s \in \mathbb{P} \text{ są parami różne}, s, k_1, \ldots, k_s \in \mathbb{N}.$$

Przedstawienie liczby n w tym twierdzeniu nazywamy ***rozkładem kanonicznym***.
Przy jego pomocy można wyznaczać NWD oraz NWW układu liczb, np.
$11781 = 3^2 \cdot 7 \cdot 11 \cdot 17$, $325703 = 7^2 \cdot 17^2 \cdot 23$

Definicja

Liczbę naturalną p nazywamy ***liczbą pierwszą***, jeśli posiada dokładnie dwa różne dzielniki naturalne. Zbiór liczb pierwszych oznaczać będziemy literą $\mathbb{P}$.

Twierdzenie

Niech p będzie liczba naturalną różną od 1. Wtedy $p \in \mathbb{P}$ wtedy i tylko wtedy, gdy dla każdych $a, b \in \mathbb{N}$ spełniony jest warunek

$$p \mid ab \implies p \mid a \text{ lub } p \mid b.$$

Zasadnicze twierdzenie arytmetyki

Dowolna liczba naturalna $n > 1$ ma jednoznacze przedstawienie w postaci

$$n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}, \text{ gdzie } p_1, \ldots, p_s \in \mathbb{P} \text{ są parami różne}, s, k_1, \ldots, k_s \in \mathbb{N}.$$

Przedstawienie liczby n w tym twierdzeniu nazywamy ***rozkładem kanonicznym***.
Przy jego pomocy można wyznaczać NWD oraz NWW układu liczb, np.
$11781 = 3^2 \cdot 7 \cdot 11 \cdot 17$, $325703 = 7^2 \cdot 17^2 \cdot 23$ i wtedy

$$\text{NWD}(11781, 325703) = 7 \cdot 17 = 119,$$

$$\text{NWW}(11781, 325703) = 3^2 \cdot 7^2 \cdot 11 \cdot 17^2 \cdot 23 = 32244597.$$

Równaniem diofantycznym nazywamy równanie, na ogół o kilku niewiadomych, którego rozwiązań szukamy w liczbach całkowitych. Nazwa pochodzi od nazwiska Diofantosa.

Równaniem diofantycznym nazywamy równanie, na ogół o kilku niewiadomych, którego rozwiązań szukamy w liczbach całkowitych. Nazwa pochodzi od nazwiska Diofantosa.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V. C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS

Diofantos - matematyk grecki żyjący w III w. n.e.

⟵ obok okładka z wydania w roku 1621 jego "Arytmetyki"

Definicja

Równanie diofantyczne $a_1x_1 + ... + a_nx_n = c$ nazywamy liniowym równaniem diofantycznym.

Definicja

Równanie diofantyczne $a_1x_1 + ... + a_nx_n = c$ nazywamy liniowym równaniem diofantycznym.

Twierdzenie

1. Równanie diofantyczne $ax + by = c$ posiada rozwiązanie wtedy i tylko wtedy, gdy NWD(a, b) dzieli c.

Definicja

Równanie diofantyczne $a_1x_1 + ... + a_nx_n = c$ nazywamy liniowym równaniem diofantycznym.

Twierdzenie

1. Równanie diofantyczne $ax + by = c$ posiada rozwiązanie wtedy i tylko wtedy, gdy NWD(a, b) dzieli c.
2. Jeśli para liczb całkowitych x_0, y_0 jest rozwiązaniem równania $ax + by = c$, to wszystkie rozwiązania dane są wzorami:

$$x = x_0 + \frac{b}{\mathrm{NWD}(a,b)} \cdot t, \quad y = y_0 - \frac{a}{\mathrm{NWD}(a,b)} \cdot t,$$

gdzie t jest dowolną liczbą całkowitą.

Definicja

Równanie diofantyczne $a_1x_1 + ... + a_nx_n = c$ nazywamy liniowym równaniem diofantycznym.

Twierdzenie

1. Równanie diofantyczne $ax + by = c$ posiada rozwiązanie wtedy i tylko wtedy, gdy NWD(a, b) dzieli c.
2. Jeśli para liczb całkowitych x_0, y_0 jest rozwiązaniem równania $ax + by = c$, to wszystkie rozwiązania dane są wzorami:

$$x = x_0 + \frac{b}{\mathrm{NWD}(a,b)} \cdot t, \quad y = y_0 - \frac{a}{\mathrm{NWD}(a,b)} \cdot t,$$

gdzie t jest dowolną liczbą całkowitą.

Definicja

Równanie diofantyczne $a_1x_1 + ... + a_nx_n = c$ nazywamy liniowym równaniem diofantycznym.

Twierdzenie

1. Równanie diofantyczne $ax + by = c$ posiada rozwiązanie wtedy i tylko wtedy, gdy NWD(a, b) dzieli c.
2. Jeśli para liczb całkowitych x_0, y_0 jest rozwiązaniem równania $ax + by = c$, to wszystkie rozwiązania dane są wzorami:

$$x = x_0 + \frac{b}{\mathrm{NWD}(a,b)} \cdot t, \quad y = y_0 - \frac{a}{\mathrm{NWD}(a,b)} \cdot t,$$

gdzie t jest dowolną liczbą całkowitą.

Szkic dowodu na tablicy.

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$1001 = 28 \cdot 35 + 21$$

$$\downarrow$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\begin{aligned} 1001 &= 28 \cdot 35 + 21 \\ 35 &= 1 \cdot 21 + 14 \\ &\downarrow \end{aligned}$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\begin{aligned} 1001 &= 28 \cdot 35 + 21 \\ \downarrow \quad 35 &= 1 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \end{aligned}$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

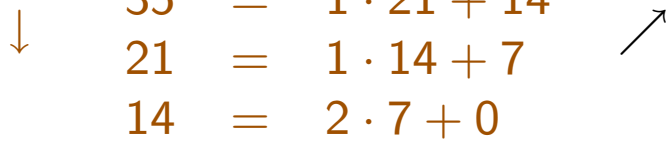
$$\begin{aligned} 1001 &= 28 \cdot 35 + 21 \\ \downarrow \quad 35 &= 1 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\begin{aligned} 1001 &= 28 \cdot 35 + 21 \\ 35 &= 1 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$



Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$
\begin{aligned}
1001 &= 28 \cdot 35 + 21 \\
35 &= 1 \cdot 21 + 14 \\
21 &= 1 \cdot 14 + 7 \\
14 &= 2 \cdot 7 + 0
\end{aligned}
$$

$\downarrow$ $\nearrow$

$$7 = 21 - 1 \cdot 14 =$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$
\begin{array}{rcl}
1001 & = & 28 \cdot 35 + 21 \\
35 & = & 1 \cdot 21 + 14 \\
21 & = & 1 \cdot 14 + 7 \\
14 & = & 2 \cdot 7 + 0
\end{array}
$$

$\downarrow$ $\nearrow$

$$
\begin{aligned}
7 &= 21 - 1 \cdot 14 = \\
&21 - 1 \cdot (35 - 1 \cdot 21) =
\end{aligned}
$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\begin{array}{rcl} 1001 & = & 28 \cdot 35 + 21 \\ \downarrow \quad 35 & = & 1 \cdot 21 + 14 \\ 21 & = & 1 \cdot 14 + 7 \\ 14 & = & 2 \cdot 7 + 0 \end{array} \qquad \nearrow \quad \begin{array}{l} 7 = 21 - 1 \cdot 14 = \\ 21 - 1 \cdot (35 - 1 \cdot 21) = \\ 2 \cdot 21 - 1 \cdot 35 = \end{array}$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\begin{array}{rcl} 1001 & = & 28 \cdot 35 + 21 \\ \downarrow \quad 35 & = & 1 \cdot 21 + 14 \\ 21 & = & 1 \cdot 14 + 7 \\ 14 & = & 2 \cdot 7 + 0 \end{array} \qquad \nearrow \qquad \begin{array}{l} 7 = 21 - 1 \cdot 14 = \\ 21 - 1 \cdot (35 - 1 \cdot 21) = \\ 2 \cdot 21 - 1 \cdot 35 = \\ 2 \cdot (1001 - 28 \cdot 35) - 1 \cdot 35 = \end{array}$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\begin{array}{rcl} 1001 & = & 28 \cdot 35 + 21 \\ \downarrow \quad 35 & = & 1 \cdot 21 + 14 \\ 21 & = & 1 \cdot 14 + 7 \\ 14 & = & 2 \cdot 7 + 0 \end{array} \qquad \nearrow \qquad \begin{array}{l} 7 = 21 - 1 \cdot 14 = \\ 21 - 1 \cdot (35 - 1 \cdot 21) = \\ 2 \cdot 21 - 1 \cdot 35 = \\ 2 \cdot (1001 - 28 \cdot 35) - 1 \cdot 35 = \end{array}$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\begin{array}{rcl} 1001 & = & 28 \cdot 35 + 21 \\ \downarrow \quad 35 & = & 1 \cdot 21 + 14 \\ 21 & = & 1 \cdot 14 + 7 \\ 14 & = & 2 \cdot 7 + 0 \end{array} \qquad \nearrow \qquad \begin{array}{l} 7 = 21 - 1 \cdot 14 = \\ 21 - 1 \cdot (35 - 1 \cdot 21) = \\ 2 \cdot 21 - 1 \cdot 35 = \\ 2 \cdot (1001 - 28 \cdot 35) - 1 \cdot 35 = \\ 2 \cdot 1001 - 57 \cdot 35 \end{array}$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\begin{array}{rcl} 1001 & = & 28 \cdot 35 + 21 \\ 35 & = & 1 \cdot 21 + 14 \\ 21 & = & 1 \cdot 14 + 7 \\ 14 & = & 2 \cdot 7 + 0 \end{array}$$

$$\begin{aligned} 7 &= 21 - 1 \cdot 14 = \\ &21 - 1 \cdot (35 - 1 \cdot 21) = \\ &2 \cdot 21 - 1 \cdot 35 = \\ &2 \cdot (1001 - 28 \cdot 35) - 1 \cdot 35 = \\ &2 \cdot 1001 - 57 \cdot 35 \end{aligned}$$

Stąd $1001 \cdot 2 + 35 \cdot (-57) = 7$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\begin{array}{rcl} 1001 & = & 28 \cdot 35 + 21 \\ 35 & = & 1 \cdot 21 + 14 \\ 21 & = & 1 \cdot 14 + 7 \\ 14 & = & 2 \cdot 7 + 0 \end{array} \qquad \begin{array}{l} 7 = 21 - 1 \cdot 14 = \\ 21 - 1 \cdot (35 - 1 \cdot 21) = \\ 2 \cdot 21 - 1 \cdot 35 = \\ 2 \cdot (1001 - 28 \cdot 35) - 1 \cdot 35 = \\ 2 \cdot 1001 - 57 \cdot 35 \end{array}$$

Stąd $1001 \cdot 2 + 35 \cdot (-57) = 7$ i mnożąc obie strony przez 7 mamy

$$1001 \cdot 14 + 35 \cdot (-399) = 49$$

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\begin{array}{rcl} 1001 & = & 28 \cdot 35 + 21 \\ 35 & = & 1 \cdot 21 + 14 \\ 21 & = & 1 \cdot 14 + 7 \\ 14 & = & 2 \cdot 7 + 0 \end{array} \qquad \begin{array}{l} 7 = 21 - 1 \cdot 14 = \\ 21 - 1 \cdot (35 - 1 \cdot 21) = \\ 2 \cdot 21 - 1 \cdot 35 = \\ 2 \cdot (1001 - 28 \cdot 35) - 1 \cdot 35 = \\ 2 \cdot 1001 - 57 \cdot 35 \end{array}$$

Stąd $1001 \cdot 2 + 35 \cdot (-57) = 7$ i mnożąc obie strony przez 7 mamy

$$1001 \cdot 14 + 35 \cdot (-399) = 49$$

Para $x_0 = 14,\ y_0 = -399$ jest rozwiązaniem.

Zadanie

Rozwiąż równanie diofantyczne $1001x + 35y = 49$.

Rozwiązanie. Obliczmy NWD$(1001, 35)$ stosując algorytm Euklidesa.

$$\downarrow \quad \begin{aligned} 1001 &= 28 \cdot 35 + 21 \\ 35 &= 1 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned} \qquad \nearrow \quad \begin{aligned} &7 = 21 - 1 \cdot 14 = \\ &21 - 1 \cdot (35 - 1 \cdot 21) = \\ &2 \cdot 21 - 1 \cdot 35 = \\ &2 \cdot (1001 - 28 \cdot 35) - 1 \cdot 35 = \\ &2 \cdot 1001 - 57 \cdot 35 \end{aligned}$$

Stąd $1001 \cdot 2 + 35 \cdot (-57) = 7$ i mnożąc obie strony przez 7 mamy

$$1001 \cdot 14 + 35 \cdot (-399) = 49$$

Para $x_0 = 14,\ y_0 = -399$ jest rozwiązaniem.
Zatem wszystkie rozwiązania naszego równania są postaci

$$\begin{aligned} x &= x_0 + \tfrac{35}{7} \cdot t = \quad 14 + 5 \cdot t \\ y &= y_0 - \tfrac{1001}{7} \cdot t = \quad -399 - 143 \cdot t, \quad t - \text{ liczba całkowita.} \end{aligned}$$

Twierdzenie

Równanie diofantyczne

$$a_1x_1 + ... + a_nx_n = b$$

posiada rozwiązanie wtedy i tylko wtedy, gdy

$$\mathrm{NWD}(a_1, ..., a_n)|b.$$

Twierdzenie

Równanie diofantyczne

$$a_1x_1 + ... + a_nx_n = b$$

posiada rozwiązanie wtedy i tylko wtedy, gdy

$$\mathrm{NWD}(a_1, ..., a_n)|b.$$

Pytanie

Jak rozwiązać równanie $a_1x_1 + ... + a_nx_n = b$, gdy $\mathrm{NWD}(a_1, ..., a_n)$ dzieli b?

Twierdzenie

Równanie diofantyczne

$$a_1x_1 + ... + a_nx_n = b$$

posiada rozwiązanie wtedy i tylko wtedy, gdy

$$\mathrm{NWD}(a_1, ..., a_n)|b.$$

Pytanie

Jak rozwiązać równanie $a_1x_1 + ... + a_nx_n = b$, gdy $\mathrm{NWD}(a_1, ..., a_n)$ dzieli b?

Podamy sposób na konkretnym przykładzie.

Zadanie

Rozwiąż równanie diofantyczne $3x + 5y + 2z = 149$.

Zadanie

Rozwiąż równanie diofantyczne $3x + 5y + 2z = 149$.

Rozwiązanie. Podstawmy $3x + 5y = w$.

Zadanie

Rozwiąż równanie diofantyczne $3x + 5y + 2z = 149$.

Rozwiązanie. Podstawmy $3x + 5y = w$. Zatem nasze równanie możemy zastąpić układem równań

$$\begin{cases} 3x + 5y &= w \\ w + 2z &= 149 \end{cases}.$$

Zadanie

Rozwiąż równanie diofantyczne $3x + 5y + 2z = 149$.

Rozwiązanie. Podstawmy $3x + 5y = w$. Zatem nasze równanie możemy zastąpić układem równań

$$\begin{cases} 3x + 5y &= w \\ w + 2z &= 149 \end{cases}.$$

Najpierw rozwiązujemy drugie równanie znanym nam sposobem otrzymując rozwiązanie

$$w = -149 + 2 \cdot u, \quad z = 149 - u.$$

Zadanie

Rozwiąż równanie diofantyczne $3x + 5y + 2z = 149$.

Rozwiązanie. Podstawmy $3x + 5y = w$. Zatem nasze równanie możemy zastąpić układem równań

$$\begin{cases} 3x + 5y &= w \\ w + 2z &= 149 \end{cases}.$$

Najpierw rozwiązujemy drugie równanie znanym nam sposobem otrzymując rozwiązanie

$$w = -149 + 2 \cdot u, \quad z = 149 - u.$$

Teraz zajmijmy się pierwszym równaniem

$$3x + 5y = w.$$

Zadanie

Rozwiąż równanie diofantyczne $3x + 5y + 2z = 149$.

Rozwiązanie. Podstawmy $3x + 5y = w$. Zatem nasze równanie możemy zastąpić układem równań

$$\begin{cases} 3x + 5y &= w \\ w + 2z &= 149 \end{cases}.$$

Najpierw rozwiązujemy drugie równanie znanym nam sposobem otrzymując rozwiązanie

$$w = -149 + 2 \cdot u, \quad z = 149 - u.$$

Teraz zajmijmy się pierwszym równaniem

$$3x + 5y = w.$$

Od razu można zauważyć, że $3 \cdot (2w) + 5 \cdot (-w) = w$,

Zadanie

Rozwiąż równanie diofantyczne $3x + 5y + 2z = 149$.

Rozwiązanie. Podstawmy $3x + 5y = w$. Zatem nasze równanie możemy zastąpić układem równań

$$\begin{cases} 3x + 5y &= w \\ w + 2z &= 149 \end{cases}.$$

Najpierw rozwiązujemy drugie równanie znanym nam sposobem otrzymując rozwiązanie

$$w = -149 + 2 \cdot u, \quad z = 149 - u.$$

Teraz zajmijmy się pierwszym równaniem

$$3x + 5y = w.$$

Od razu można zauważyć, że $3 \cdot (2w) + 5 \cdot (-w) = w$, a więc

$$\begin{aligned} x &= 2w + 5t \\ y &= -w - 3t \end{aligned}.$$

Zadanie

Rozwiąż równanie diofantyczne $3x + 5y + 2z = 149$.

Rozwiązanie. Podstawmy $3x + 5y = w$. Zatem nasze równanie możemy zastąpić układem równań

$$\begin{cases} 3x + 5y &= w \\ w + 2z &= 149 \end{cases}.$$

Najpierw rozwiązujemy drugie równanie znanym nam sposobem otrzymując rozwiązanie

$$w = -149 + 2 \cdot u, \quad z = 149 - u.$$

Teraz zajmijmy się pierwszym równaniem

$$3x + 5y = w.$$

Od razu można zauważyć, że $3 \cdot (2w) + 5 \cdot (-w) = w$, a więc

$$\begin{aligned} x &= 2w + 5t \\ y &= -w - 3t \end{aligned}.$$

Odp. Zatem rozwiązaniem naszego wyjściowego równania jest trójka

$$\begin{aligned} x &= 2w + 5t = 2(-149 + 2u) + 5t = -298 + 4u + 5t \\ y &= -w - 3t = 149 - 2u - 3t \\ z &= 149 - u \end{aligned},$$

gdzie t oraz u są dowolnymi liczbami całkowitymi.

Definicja

Niech n będzie liczbą naturalną oraz niech a oraz b będą liczbami całkowitymi. Mówimy, że a **przystaje do** b **modulo** n, jeśli n dzieli $a - b$.

$$a \equiv b \pmod{n} \iff a - b = t \cdot n \text{ dla pewnej liczby całk. } t$$

Definicja

Niech n będzie liczbą naturalną oraz niech a oraz b będą liczbami całkowitymi. Mówimy, że a **przystaje do** b **modulo** n, jeśli n dzieli $a - b$.

$$a \equiv b \pmod{n} \iff a - b = t \cdot n \text{ dla pewnej liczby całk. } t$$

Uwaga

$$a \equiv b \pmod{n} \iff (a)_n = (b)_n$$

Definicja

Niech n będzie liczbą naturalną oraz niech a oraz b będą liczbami całkowitymi. Mówimy, że a **przystaje do** b **modulo** n, jeśli n dzieli $a - b$.

$$a \equiv b \pmod{n} \iff a - b = t \cdot n \text{ dla pewnej liczby całk. } t$$

Uwaga

$$a \equiv b \pmod{n} \iff (a)_n = (b)_n$$

Które z poniższych kongruencji są prawdziwe?

$$10 \equiv 1 \pmod{9},$$

Definicja

Niech n będzie liczbą naturalną oraz niech a oraz b będą liczbami całkowitymi. Mówimy, że a **przystaje do** b **modulo** n, jeśli n dzieli $a - b$.

$$a \equiv b \pmod{n} \iff a - b = t \cdot n \text{ dla pewnej liczby całk. } t$$

Uwaga

$$a \equiv b \pmod{n} \iff (a)_n = (b)_n$$

Które z poniższych kongruencji są prawdziwe?

$$10 \equiv 1 \pmod{9}, \qquad -1 \equiv 113 \pmod{6},$$

Definicja

Niech n będzie liczbą naturalną oraz niech a oraz b będą liczbami całkowitymi. Mówimy, że a **przystaje do** b **modulo** n, jeśli n dzieli $a - b$.

$$a \equiv b \pmod{n} \iff a - b = t \cdot n \text{ dla pewnej liczby całk. } t$$

Uwaga

$$a \equiv b \pmod{n} \iff (a)_n = (b)_n$$

Które z poniższych kongruencji są prawdziwe?

$$10 \equiv 1 \pmod{9}, \qquad -1 \equiv 113 \pmod{6}, \qquad -12 \equiv 13 \pmod{5},$$

Definicja

Niech n będzie liczbą naturalną oraz niech a oraz b będą liczbami całkowitymi. Mówimy, że a **przystaje do** b **modulo** n, jeśli n dzieli $a - b$.

$$a \equiv b \pmod{n} \iff a - b = t \cdot n \text{ dla pewnej liczby całk. } t$$

Uwaga

$$a \equiv b \pmod{n} \iff (a)_n = (b)_n$$

Które z poniższych kongruencji są prawdziwe?

$$10 \equiv 1 \pmod{9}, \qquad -1 \equiv 113 \pmod{6}, \qquad -12 \equiv 13 \pmod{5},$$

$$-5 \equiv 31 \pmod{7},$$

Definicja

Niech n będzie liczbą naturalną oraz niech a oraz b będą liczbami całkowitymi. Mówimy, że a **przystaje do** b **modulo** n, jeśli n dzieli $a - b$.

$$a \equiv b \pmod{n} \iff a - b = t \cdot n \text{ dla pewnej liczby całk. } t$$

Uwaga

$$a \equiv b \pmod{n} \iff (a)_n = (b)_n$$

Które z poniższych kongruencji są prawdziwe?

$$10 \equiv 1 \pmod{9}, \qquad -1 \equiv 113 \pmod{6}, \qquad -12 \equiv 13 \pmod{5},$$

$$-5 \equiv 31 \pmod{7}, \qquad -26 \equiv 44 \pmod{10},$$

Definicja

Niech n będzie liczbą naturalną oraz niech a oraz b będą liczbami całkowitymi. Mówimy, że a **przystaje do** b **modulo** n, jeśli n dzieli $a - b$.

$$a \equiv b \pmod{n} \iff a - b = t \cdot n \text{ dla pewnej liczby całk. } t$$

Uwaga

$$a \equiv b \pmod{n} \iff (a)_n = (b)_n$$

Które z poniższych kongruencji są prawdziwe?

$$10 \equiv 1 \pmod{9}, \qquad -1 \equiv 113 \pmod{6}, \qquad -12 \equiv 13 \pmod{5},$$

$$-5 \equiv 31 \pmod{7}, \qquad -26 \equiv 44 \pmod{10}, \qquad 23 \equiv 71 \pmod{11}$$

Własności kongruencji

1. Kongruencja $\equiv \pmod{n}$ ma podobne własności jak zwykła równość $=$,

Własności kongruencji

1. Kongruencja $\equiv \pmod{n}$ ma podobne własności jak zwykła równość $=$, tzn.
   - $a \equiv a \pmod{n}$,

Własności kongruencji

1. Kongruencja $\equiv \pmod{n}$ ma podobne własności jak zwykła równość $=$, tzn.
   - $a \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$,

Własności kongruencji

1. Kongruencja $\equiv \pmod{n}$ ma podobne własności jak zwykła równość $=$, tzn.
   - $a \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n}, \; b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Własności kongruencji

1. Kongruencja $\equiv \pmod{n}$ ma podobne własności jak zwykła równość $=$, tzn.
   - $a \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n}$, $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.
2. Kongruencje można stronami dodawać, odejmować i mnożyć,

Własności kongruencji

1. Kongruencja $\equiv \pmod{n}$ ma podobne własności jak zwykła równość $=$, tzn.
   - $a \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n}, \; b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.
2. Kongruencje można stronami dodawać, odejmować i mnożyć,tzn.

$$a \equiv b \pmod{n}, \quad c \equiv d \pmod{n}$$

$$\Downarrow$$

$$a + c \equiv b + d \pmod{n}, \quad a - c \equiv b - d \pmod{n}, \quad ac \equiv bd \pmod{n}$$

Własności kongruencji

1. Kongruencja $\equiv \pmod{n}$ ma podobne własności jak zwykła równość $=$, tzn.
   - $a \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n},\ b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.
2. Kongruencje można stronami dodawać, odejmować i mnożyć,tzn.

$$a \equiv b \pmod{n},\quad c \equiv d \pmod{n}$$

$$\Downarrow$$

$$a + c \equiv b + d \pmod{n},\quad a - c \equiv b - d \pmod{n},\quad ac \equiv bd \pmod{n}$$

Oznacza to, że na kongruencjach można wykonywać podobne rachunki jak w przypadku równości. Zobaczmy to na przykładach.

Własności kongruencji

1. Kongruencja $\equiv \pmod{n}$ ma podobne własności jak zwykła równość $=$, tzn.
   - $a \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n}, \; b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.
2. Kongruencje można stronami dodawać, odejmować i mnożyć,tzn.

$$a \equiv b \pmod{n}, \quad c \equiv d \pmod{n}$$

$$\Downarrow$$

$$a + c \equiv b + d \pmod{n}, \quad a - c \equiv b - d \pmod{n}, \quad ac \equiv bd \pmod{n}$$

Oznacza to, że na kongruencjach można wykonywać podobne rachunki jak w przypadku równości. Zobaczmy to na przykładach.
Rozwiąż następujące kongruencje:

- $3X + 2 \equiv 5 \pmod{11}$,

Własności kongruencji

1. Kongruencja $\equiv \pmod{n}$ ma podobne własności jak zwykła równość $=$, tzn.
   - $a \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$,
   - $a \equiv b \pmod{n}, \; b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.
2. Kongruencje można stronami dodawać, odejmować i mnożyć,tzn.

$$a \equiv b \pmod{n}, \quad c \equiv d \pmod{n}$$

$$\Downarrow$$

$$a + c \equiv b + d \pmod{n}, \quad a - c \equiv b - d \pmod{n}, \quad ac \equiv bd \pmod{n}$$

Oznacza to, że na kongruencjach można wykonywać podobne rachunki jak w przypadku równości. Zobaczmy to na przykładach.
Rozwiąż następujące kongruencje:

- $3X + 2 \equiv 5 \pmod{11}$,
- $25X \equiv 12 \pmod{7}$.

Zauważmy, że jeśli $a \equiv b \pmod{n}$, to dla dowolnych liczb całkowitych $a_0, \ldots, a_m$ mamy

$$a_0 \equiv a_0 \pmod{n}$$

Zauważmy, że jeśli $a \equiv b \pmod{n}$, to dla dowolnych liczb całkowitych $a_0, \ldots, a_m$ mamy

$$\begin{aligned} a_0 &\equiv a_0 \pmod{n} \\ a_1 a &\equiv a_1 b \pmod{n} \end{aligned}$$

Zauważmy, że jeśli $a \equiv b \pmod{n}$, to dla dowolnych liczb całkowitych $a_0, \ldots, a_m$ mamy

$$\begin{aligned} a_0 &\equiv a_0 \pmod{n} \\ a_1 a &\equiv a_1 b \pmod{n} \\ a_2 a^2 &\equiv a_2 b^2 \pmod{n} \end{aligned}$$

Zauważmy, że jeśli $a \equiv b \pmod{n}$, to dla dowolnych liczb całkowitych $a_0, \ldots, a_m$ mamy

$$\begin{aligned} a_0 &\equiv a_0 \pmod{n} \\ a_1 a &\equiv a_1 b \pmod{n} \\ a_2 a^2 &\equiv a_2 b^2 \pmod{n} \\ &\vdots \\ a_m a^m &\equiv a_m b^m \pmod{n} \end{aligned}$$

Zauważmy, że jeśli $a \equiv b \pmod{n}$, to dla dowolnych liczb całkowitych $a_0, \ldots, a_m$ mamy

$$\begin{aligned} a_0 &\equiv a_0 \pmod{n} \\ a_1 a &\equiv a_1 b \pmod{n} \\ a_2 a^2 &\equiv a_2 b^2 \pmod{n} \\ &\vdots \\ a_m a^m &\equiv a_m b^m \pmod{n} \end{aligned}$$

$$a_m a^m + \ldots + a_1 a + a_0 \equiv a_m b^m + \ldots + a_1 b + a_0 \pmod{n},$$

Zauważmy, że jeśli $a \equiv b \pmod{n}$, to dla dowolnych liczb całkowitych $a_0, \ldots, a_m$ mamy

$$\begin{aligned} a_0 &\equiv a_0 \pmod{n} \\ a_1 a &\equiv a_1 b \pmod{n} \\ a_2 a^2 &\equiv a_2 b^2 \pmod{n} \\ &\vdots \\ a_m a^m &\equiv a_m b^m \pmod{n} \end{aligned}$$

$$a_m a^m + \ldots + a_1 a + a_0 \equiv a_m b^m + \ldots + a_1 b + a_0 \pmod{n},$$

tzn. $f(a) \equiv f(b) \pmod{n}$, gdzie $f(X) = a_m X^m + \ldots + a_1 X + a_0$

Zauważmy, że jeśli $a \equiv b \pmod{n}$, to dla dowolnych liczb całkowitych $a_0, \ldots, a_m$ mamy

$$\begin{aligned} a_0 &\equiv a_0 \pmod{n} \\ a_1 a &\equiv a_1 b \pmod{n} \\ a_2 a^2 &\equiv a_2 b^2 \pmod{n} \\ &\vdots \\ a_m a^m &\equiv a_m b^m \pmod{n} \end{aligned}$$

$$a_m a^m + \ldots + a_1 a + a_0 \equiv a_m b^m + \ldots + a_1 b + a_0 \pmod{n},$$

tzn. $f(a) \equiv f(b) \pmod{n}$, gdzie $f(X) = a_m X^m + \ldots + a_1 X + a_0$

Zatem

$$a \equiv b \pmod{n} \implies f(a) \equiv f(b) \pmod{n}$$

Jak skonstruowany jest system dziesiętny?

Jak skonstruowany jest system dziesiętny?

$$4326 = 4 \cdot 1000 + 3 \cdot 100 + 2 \cdot 10 + 6 \cdot 1$$

Jak skonstruowany jest system dziesiętny?

$$4326 = 4 \cdot 1000 + 3 \cdot 100 + 2 \cdot 10 + 6 \cdot 1 = 4 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10^1 + 6 \cdot 10^0$$

Jak skonstruowany jest system dziesiętny?

$$4326 = 4 \cdot 1000 + 3 \cdot 100 + 2 \cdot 10 + 6 \cdot 1 = 4 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10^1 + 6 \cdot 10^0$$

Ogólniej, liczbę naturalną N w systemie dziesiętnym można zapisać następująco:

$$N = (c_1 c_2 \ldots c_n)_{10} = c_1 10^{n-1} + c_2 10^{n-2} + \ldots + c_{n-1} 10^1 + c_n \cdot 10^0.$$

Jak skonstruowany jest system dziesiętny?

$$4326 = 4 \cdot 1000 + 3 \cdot 100 + 2 \cdot 10 + 6 \cdot 1 = 4 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10^1 + 6 \cdot 10^0$$

Ogólniej, liczbę naturalną N w systemie dziesiętnym można zapisać następująco:

$$N = (c_1 c_2 \ldots c_n)_{10} = c_1 10^{n-1} + c_2 10^{n-2} + \ldots + c_{n-1} 10^1 + c_n \cdot 10^0.$$

i wtedy

$$N = f(10), \text{ jeśli } f(X) = c_1 X^{n-1} + c_2 X^{n-2} + \ldots + c_{n-1} X^1 + c_n.$$

$$f(X) = c_1 X^{n-1} + c_2 X^{n-2} + \ldots + c_{n-1} X^1 + c_n$$

$$f(10) = (c_1 c_2 \ldots c_n)_{10}, \quad f(1) = c_1 + c_2 + \ldots + c_{n-1} + c_n$$

$$10 \equiv 1 \pmod{3}$$
$$\Downarrow$$
$$(c_1 c_2 \ldots c_n)_{10} = f(10) \equiv f(1) = c_1 + c_2 + \ldots + c_{n-1} + c_n \pmod{3}$$

$$f(X) = c_1 X^{n-1} + c_2 X^{n-2} + \ldots + c_{n-1} X^1 + c_n$$

$$f(10) = (c_1 c_2 \ldots c_n)_{10}, \quad f(1) = c_1 + c_2 + \ldots + c_{n-1} + c_n$$

$$10 \equiv 1 \pmod{3}$$
$$\Downarrow$$

$$(c_1 c_2 \ldots c_n)_{10} = f(10) \equiv f(1) = c_1 + c_2 + \ldots + c_{n-1} + c_n \pmod{3}$$

tzn. 3 dzieli $(c_1 c_2 \ldots c_n)_{10}$ wtedy i tylko wtedy, gdy dzieli sumę jej cyfr.

$$f(X) = c_1 X^{n-1} + c_2 X^{n-2} + \ldots + c_{n-1} X^1 + c_n$$

$$f(10) = (c_1 c_2 \ldots c_n)_{10}, \quad f(1) = c_1 + c_2 + \ldots + c_{n-1} + c_n$$

$$10 \equiv 1 \pmod{3}$$
$$\Downarrow$$
$$(c_1 c_2 \ldots c_n)_{10} = f(10) \equiv f(1) = c_1 + c_2 + \ldots + c_{n-1} + c_n \pmod{3}$$

tzn. 3 dzieli $(c_1 c_2 \ldots c_n)_{10}$ wtedy i tylko wtedy, gdy dzieli sumę jej cyfr.

Czy wiesz jak udowodnić cechę podzielności przez 9 oraz przez 11?

$$f(X) = c_1X^{n-1} + c_2X^{n-2} + \ldots + c_{n-1}X^1 + c_n$$

$$f(10) = (c_1c_2\ldots c_n)_{10}, \quad f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + \ldots - c_{n-1} + c_n$$

$$10 \equiv -1 \pmod{11}$$

$$\Downarrow$$

$$N = f(10) \equiv f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + \ldots - c_{n-1} + c_n \pmod{11}$$

$$f(X) = c_1X^{n-1} + c_2X^{n-2} + ... + c_{n-1}X^1 + c_n$$

$$f(10) = (c_1c_2...c_n)_{10}, \quad f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + ... - c_{n-1} + c_n$$

$$10 \equiv -1 \pmod{11}$$

$$\Downarrow$$

$$N = f(10) \equiv f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + ... - c_{n-1} + c_n \pmod{11}$$

tzn. 11 dzieli liczbę $N = (c_1c_2...c_n)_{10}$ wtedy i tylko wtedy, gdy dzieli naprzemienną sumę jej cyfr.

$$f(X) = c_1X^{n-1} + c_2X^{n-2} + ... + c_{n-1}X^1 + c_n$$

$$f(10) = (c_1c_2...c_n)_{10}, \quad f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + ... - c_{n-1} + c_n$$

$$10 \equiv -1 \pmod{11}$$
$$\Downarrow$$
$$N = f(10) \equiv f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + ... - c_{n-1} + c_n \pmod{11}$$

tzn. 11 dzieli liczbę $N = (c_1c_2...c_n)_{10}$ wtedy i tylko wtedy, gdy dzieli naprzemienną sumę jej cyfr.

Przykład

Aby sprawdzić podzielność liczby 123456789060704 przez 11 obliczamy sumę naprzemienną cyfr

$$f(X) = c_1X^{n-1} + c_2X^{n-2} + ... + c_{n-1}X^1 + c_n$$

$$f(10) = (c_1c_2...c_n)_{10}, \quad f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + ... - c_{n-1} + c_n$$

$$10 \equiv -1 \pmod{11}$$
$$\Downarrow$$
$$N = f(10) \equiv f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + ... - c_{n-1} + c_n \pmod{11}$$

tzn. 11 dzieli liczbę $N = (c_1c_2...c_n)_{10}$ wtedy i tylko wtedy, gdy dzieli naprzemienną sumę jej cyfr.

Przykład

Aby sprawdzić podzielność liczby 123456789060704 przez 11 obliczamy sumę naprzemienną cyfr

$$f(X) = c_1X^{n-1} + c_2X^{n-2} + \ldots + c_{n-1}X^1 + c_n$$

$$f(10) = (c_1c_2\ldots c_n)_{10}, \quad f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + \ldots - c_{n-1} + c_n$$

$$10 \equiv -1 \pmod{11}$$
$$\Downarrow$$
$$N = f(10) \equiv f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + \ldots - c_{n-1} + c_n \pmod{11}$$

tzn. 11 dzieli liczbę $N = (c_1c_2\ldots c_n)_{10}$ wtedy i tylko wtedy, gdy dzieli naprzemienną sumę jej cyfr.

Przykład

Aby sprawdzić podzielność liczby 123456789060704 przez 11 obliczamy sumę naprzemienną cyfr

$$4 - 0 + 7 - 0 + 6 - 0 + 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 22,$$

która jest podzielna przez 11.

$$f(X) = c_1X^{n-1} + c_2X^{n-2} + \ldots + c_{n-1}X^1 + c_n$$

$$f(10) = (c_1c_2\ldots c_n)_{10}, \quad f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + \ldots - c_{n-1} + c_n$$

$$10 \equiv -1 \pmod{11}$$
$$\Downarrow$$
$$N = f(10) \equiv f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + \ldots - c_{n-1} + c_n \pmod{11}$$

tzn. 11 dzieli liczbę $N = (c_1c_2\ldots c_n)_{10}$ wtedy i tylko wtedy, gdy dzieli naprzemienną sumę jej cyfr.

Przykład

Aby sprawdzić podzielność liczby 123456789060704 przez 11 obliczamy sumę naprzemienną cyfr

$$4 - 0 + 7 - 0 + 6 - 0 + 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 22,$$

która jest podzielna przez 11. Zatem 11 dzieli 123456789060704.

Cechy podzielności przez inne liczby są bardziej skomplikowane. Przyjrzyjmy się cesze podzielności przez 7 oraz przez 13.

Liczbę naturalną

$$N = (c_1 c_2 ... c_n)_{10} = c_1 10^{n-1} + c_2 10^{n-2} + ... + c_{n-1} 10^1 + c_n$$

możemy zapisać w postaci

$$N = ... + 1000^1 (c_{n-5} c_{n-4} c_{n-3})_{10} + (c_{n-2} c_{n-1} c_n)_{10}.$$

Cechy podzielności przez inne liczby są bardziej skomplikowane. Przyjrzyjmy się cesze podzielności przez 7 oraz przez 13.

Liczbę naturalną

$$N = (c_1 c_2 ... c_n)_{10} = c_1 10^{n-1} + c_2 10^{n-2} + ... + c_{n-1} 10^1 + c_n$$

możemy zapisać w postaci

$$N = ... + 1000^1 (c_{n-5} c_{n-4} c_{n-3})_{10} + (c_{n-2} c_{n-1} c_n)_{10}.$$

Zauważ, że jeśli

$$g(X) = ... + X(c_{n-5} c_{n-4} c_{n-3})_{10} + (c_{n-2} c_{n-1} c_n)_{10},$$

to

$$N = g(1000).$$

$$g(X) = \ldots + X(c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-2}c_{n-1}c_n)_{10},$$

$$1000 \equiv -1 \pmod{7, 13} \text{ (bo } 1001 = 7 \cdot 11 \cdot 13)$$

$$\Downarrow$$

$$N = g(1000) \equiv g(-1) \pmod{7, 13}$$

$$g(-1) = \ldots + (-1)^1(c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-2}c_{n-1}c_n)_{10}$$

$$g(X) = \ldots + X(c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-2}c_{n-1}c_n)_{10},$$

$$1000 \equiv -1 \pmod{7, 13} \text{ (bo } 1001 = 7 \cdot 11 \cdot 13)$$

$$\Downarrow$$

$$N = g(1000) \equiv g(-1) \pmod{7, 13}$$

$$g(-1) = \ldots + (-1)^1(c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-2}c_{n-1}c_n)_{10}$$

Stąd 7 (tak samo 13) dzieli liczbę N wtedy i tylko wtedy, gdy dzieli

"naprzemienną sumę" liczb powstałych z podziału liczby N na trójki.

$$g(X) = \ldots + X(c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-2}c_{n-1}c_n)_{10},$$

$$1000 \equiv -1 \pmod{7, 13} \text{ (bo } 1001 = 7 \cdot 11 \cdot 13)$$

$$\Downarrow$$

$$N = g(1000) \equiv g(-1) \pmod{7, 13}$$

$$g(-1) = \ldots + (-1)^1(c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-2}c_{n-1}c_n)_{10}$$

Stąd 7 (tak samo 13) dzieli liczbę N wtedy i tylko wtedy, gdy dzieli

"naprzemienną sumę" liczb powstałych z podziału liczby N na trójki.

Przykład

7 dzieli 23697678872, bo $872 - 678 + 697 - 23 = 868 = 7 \cdot 124$

I to już koniec!

♡♡♡

Dziękuję za uwagę