Matematyka dyskretna

Teoria podzielności liczb całkowitych
(NWD, algorytm Euklidesa, liczby pierwsze, kongruencje).

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

Przykład. $2 \mid 10 \quad (10 = 2 \cdot 5)$

NWD

NWD dla dwóch liczb całkowitych to największa liczba naturalna dzieląca każdą z nich.

Definicja formalna: największym wspólnym dzielnikiem liczb $a, b \in \mathbb{Z}$ nazywamy liczbę całkowitą d taką, że:

1. $d > 0$,
2. $d \mid a$ i $d \mid b$,
3. dla każdej liczby x, jeśli $x \mid a$ i $x \mid b$, to $x \mid d$.

Przykład. $nwd(625, 25) = 25$

Algorytm Euklidesa

Najprostsza wersja algorytmu:

1. Wybieramy dwie liczby naturalne, dla których chcemy wyznaczyć nwd.
2. Z liczb tworzymy parę: (mniejsza z liczb; różnica liczby większej i mniejszej).
3. Powtarzamy krok 2, aż obie liczby będą sobie równe – ich wartość to nwd.

Przykład. $nwd(75, 25) \rightsquigarrow nwd(25, 50) \rightsquigarrow nwd(25, 25)$

Druga wersja algorytmu:
W kroku 2. powyżej z liczb tworzymy parę: (mniejsza z liczb; reszta z dzielenia większej przez mniejszą) i powtarzamy, aż jedna z liczb będzie równa zero – druga wtedy jest nwd.

Przykład. $nwd(75, 25) = nwd(25, 75 \ mod \ 25) = nwd(25, 0)$

Liczby pierwsze

Liczbą pierwszą nazywamy liczbę naturalną, która ma dokładnie dwa dzielniki naturalne.

Przykład. $2, 3, 5, 7, 11, 13, 17, 19, 23, ...$
Istnieją wzory na obliczanie n-tej liczby pierwszej, jednak ich złożoność powoduje, że są całkowicie bezużyteczne.

Kongruencje

Zakładamy, że $m \in \mathbb{Z}_+$. Wówczas $a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b)$. *(Liczba a przystaje do liczby b modulo m).* Relację przystawania modulo m nazywa się kongruencją. Jest to relacja równoważności (zwrotność, symetryczność, przechodniość, *patrz: Relacje i funkcje*).

Przykłady.

a) $3 \equiv \ 24 \ (mod \ 7) \quad (7 \mid 24 - 3)$

b) $18 \equiv \ 0 \ (mod \ 9) \quad (9 \mid 18 - 0)$

c) $10 \equiv \ -1 \ (mod \ 11) \quad (11 \mid 10 - (-1))$

d) $a \equiv \ a \ (mod \ n)$

Zapis: $[x] = \{a \in \mathbb{Z} : m \mid (x - a)\}$ oznacza klasę abstrakcji (równoważności) elementu x względem relacji przystawania modulo m. Klasa abstrakcji elementu x jest wyznaczona przez resztę z dzielenia tego elementu przez m, a dwa elementy są w relacji wtedy, gdy dają taką samą resztę przy dzieleniu przez m.

Przykład. Dla $m = 5$ mamy:

$[0] = \{a \in \mathbb{Z} : 5 \mid a\} = m\mathbb{Z} = \{0, 5, 10, ...\}$,
$[1] = \{a \in \mathbb{Z} : 5 \mid (a - 1)\} = m\mathbb{Z} + 1 = \{1, 6, 11, ...\}$,
$[2] = \{a \in \mathbb{Z} : 5 \mid (a - 2)\} = m\mathbb{Z} + 2 = \{2, 7, 12, ...\}$,
$[3] = \{a \in \mathbb{Z} : 5 \mid (a - 3)\} = m\mathbb{Z} + 3 = \{3, 8, 13, ...\}$,
$[4] = \{a \in \mathbb{Z} : 5 \mid (a - 4)\} = m\mathbb{Z} + 4 = \{4, 9, 14, ...\}$,