Największy wspólny dzielnik

Definicja

Największym wspólnym dzielnikiem liczb całkowitych a i b (NWD(a, b), gcd(a, b)) nazywamy liczbę całkowitą d taką, że:

0. $d \geq 0$;
1. $d \mid a$ i $d \mid b$ (tzn. $a = k \cdot d$ i $b = l \cdot d$ dla pewnych liczb całkowitych k i l);
2. jeśli $c \mid a$ i $c \mid b$ dla pewnej liczby całkowitej c, to $c \mid d$.

Przykłady

- NWD$(4, 9) = 1$.
- NWD$(100, 150) = 50$.

Tożsamość Bézout

Jeśli a i b są liczbami całkowitymi, to istnieją liczby całkowite k i l takie, że

$$\text{NWD}(a, b) = k \cdot a + l \cdot b.$$

Rozszerzony Algorytm Euklidesa I

Dane

Liczby całkowite a i b.

Wynik

Liczby całkowite d, k i l takie, że:

$$d = \mathrm{NWD}(a, b) \qquad \text{i} \qquad d = k \cdot a + l \cdot b.$$

Algorytm

Definiujemy liczby a_n, b_n, r_n, q_n, $n \geq 0$, oraz k_n i l_n, $n \geq -1$, w następujący sposób:

1. $k_{-1} := 1$, $l_{-1} := 0$, $a_0 := a$, $b_0 := b$, $k_0 := 0$, $l_0 := 1$.
2. Jeśli $n \geq 0$ i $b_n \neq 0$, to:
   $r_n := a_n \bmod b_n$, reszta z dzielenia a_n przez b_n,
   $q_n := a_n \operatorname{div} b_n$, iloraz (całkowity) z dzielenia a_n przez b_n,
   $a_{n+1} := b_n$, $b_{n+1} := r_n$,
   $k_{n+1} := k_{n-1} - q_n \cdot k_n$, $l_{n+1} := l_{n-1} - q_n \cdot l_n$.
3. Jeśli $n \geq 0$ i $b_n = 0$, to
   $$d := a_n, \qquad k := k_{n-1}, \qquad l := l_{n-1}.$$
4. Jeśli $d < 0$, to zmieniamy znak liczb d, k i l.

Przykład

Zastosujemy algorytm dla $a = 92$ i $b = 20$.

a	b	r	q	k	l
				1	0
92	20	12	4	0	1
20	12	8	1	1	-4
12	8	4	1	-1	5
8	4	0	2	2	-9
4	0				

Zatem

$$\mathrm{NWD}(92, 20) = 4 = 2 \cdot 92 + (-9) \cdot 20.$$

Uwaga

Dla każdego $n \geq 0$ mamy

$$k_{n-1} \cdot a + l_{n-1} \cdot b = a_n.$$