Podzielność

$a, b \in \mathbb{Z}$

$$a \mid b \iff \bigvee_{k \in \mathbb{Z}} b = k \cdot a$$

a dzieli b

a jest dzielnikiem b

b jest podzielne przez a

Własności relacji podzielności

$\bigwedge_{n \in \mathbb{Z}}$

1) $n \mid 0$ $0 \mid 0 \iff \bigvee_{k \in \mathbb{Z}} 0 = k \cdot 0$

2) $n \mid n$

3) $1 \mid n$, $-1 \mid n$

4) $0 \mid n \iff n = 0$

$\mid$ jest relacją w $\mathbb{Z}$ $(\mathbb{N}, \mid)$

$\mid$ jest przechodnia : $a \mid b \wedge b \mid c \Rightarrow a \mid c$

$\bigvee_{k} b = ka$ $c = m \cdot b \Rightarrow c = m \cdot b =$

$= m \cdot k \cdot a$

Twierdzenie o dzieleniu z resztą

Niech $m \in \mathbb{Z}$ oraz $n \in \mathbb{N}$. Istnieje dokładnie jedna para liczb całkowitych q i r, dla której

$$m = qn + r \qquad \text{oraz} \qquad 0 \leqslant r < n.$$

$17 : 5 \qquad 17 = \underset{q}{3} \cdot 5 + \underset{r}{2}$

Dowód.

q, r istnieją

Niech q będzie taką liczbą całkowitą, że $q \in \left(\frac{m}{n} - 1, \frac{m}{n}\right]$

$\boxed{\frac{m}{n} - 1} < q \leqslant \boxed{\frac{m}{n}} \quad | \cdot n$

$m - n < qn \leqslant m$

1) $m - qn \geqslant 0$

2) $m - qn < n$

$r := m - qn$

$0 \leqslant r < n$

$m = (m - qn) + qn = \boxed{qn + r}$

Jedyność q i r.

Załóżmy, że dla (q, r) i (q_1, r_1) zachodzi

$\longrightarrow m = qn + r = q_1 n + r_1$.

$$\underbrace{qn + r}_{m} - \underbrace{(q_1 n + r_1)}_{m} = 0 \qquad r = r_1$$

$$n(q - q_1) + r - r_1 = 0$$

$$n(q - q_1) = r_1 - r \Rightarrow \boxed{n \mid r - r_1} \Rightarrow \boxed{r - r_1 = 0}$$

$$0 \leqslant r \leqslant n-1 \qquad \boxed{-(n-1) \leqslant r - r_1 \leqslant n-1}$$

$$0 \leqslant r_1 \leqslant n-1$$

$$r = r_1 \Rightarrow n(q - q_1) = 0$$

$$q - q_1 = 0$$

$$q = q_1.$$

---

m, n

$$m = q \cdot n + r$$

ILORAZ RESZTA

$$\boxed{\begin{aligned} q &= m \operatorname{div} n \\ r &= m \operatorname{mod} n \end{aligned}} \quad \left\{ \begin{aligned} &m / n \\ &m \% n \end{aligned} \right.$$

$$m = (m \operatorname{div} n) \cdot n + m \operatorname{mod} n$$

Algorytm dzielenia

input: $m \geqslant 0,\ n > 0$
output: $q, r \in \mathbb{Z},\ m = qn + r,\ 0 \leqslant r < n$
$q \leftarrow 0$
$r \leftarrow m$
while $r \geqslant n$ **do**
  $q \leftarrow q + 1$
  $r \leftarrow r - n$
end while

$m \sim 2^{100}$

$n = 7$

$m = 17,\ n = 5$

q	r
0	17
1	12
2	7
$\boxed{3}$	$\boxed{2}$

$17 = 3 \cdot 5 + 2$

Dlaczego ten algorytm działa poprawnie?

Niezmienniki pętli

p – warunek

while q

S ;

end

Niezmienniki pętli

Zdanie p nazywamy **niezmiennikiem** pętli

while q **do**
    S
end while

jeżeli spełniony jest warunek:

p i q są prawdziwe zanim wykonamy S

$$\Downarrow$$

p jest prawdą po wykonaniu S

Twierdzenie o niezmiennikach

Załóżmy, że p jest niezmiennikiem pętli

$\rightarrow$

while q **do**
S
end while

$p(1)$ $\qquad$ $p(n) \Rightarrow p(n+1)$

Jeżeli p jest prawdą przed wejściem w pętlę, to p jest prawdą po każdej iteracji pętli. Jednocześnie jeśli pętla się kończy, to po jej zakończeniu zdanie p jest prawdziwe, a zdanie q fałszywe.

$\bigwedge_n p(n)$

Algorytm dzielenia

input: $m \geqslant 0,\ n > 0$

output: $q, r \in \mathbb{Z},\ m = qn + r,\ 0 \leqslant r < n$

$q \leftarrow 0$

$r \leftarrow m$

while $r \geqslant n$ **do**

$\quad q \leftarrow q + 1$

$\quad r \leftarrow r - n$

end while

S

$\Rightarrow m = qn + r = 0 \cdot n + m = m$ ✓

NIEZMIENNIK? $m = q \cdot n + r$ P

1) przed wejściem w pętlę P jest prawdą

1) + 2) + 3) + Tw. o NIEZM. $\Rightarrow$ po zakończeniu $m = q \cdot n + r \wedge r < n$

2) Czy P jest rzeczywiście niezmiennikiem?

Załóżmy, że $\boxed{m = qn + r}$ dla pewnych q i r.

Po wykonaniu S mamy

$q' = \text{nowe } q = q + 1$

$r' = \text{nowe } r = r - n$

$m \overset{?}{=} q' \cdot n + r' = (q+1) \cdot n + r - n = qn + r = m$

3) Czy pętla się kończy?

$r' = \text{nowe } r = r - n < r$ (ściśle maleje)

Największy wspólny dzielnik

$m, n \in \mathbb{Z}, \quad m \neq 0 \lor n \neq 0$

1) $1 | m$ i $1 | n$
2) Przynajmniej jedna z liczb m i n ma skończenie wiele dzielników.
3) Zbiór wspólnych dzielników m i n jest skończony.

$\Rightarrow$ Istnieje $\underbrace{\text{największy dzielnik } m \text{ i } n.}$

$$NWD(m,n) \qquad \underbrace{(m,n) = gcd(m,n)}$$

Przykład

NWD(135, 120)?

$135 = 3 \cdot 45 = 3 \cdot 3 \cdot 15 = 3 \cdot 3 \cdot 3 \cdot 5 = 3^3 \cdot 5$

$120 = 2 \cdot 60 = 2 \cdot 2 \cdot 30 = 2 \cdot 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 =$

$= 2^3 \cdot 3 \cdot 5$

$NWD(135, 120) = 15 = 3 \cdot 5$

Przykład

$$\text{NWD}(23598721938873, 5091259781239)?$$

Algorytm

input: $m, n \in \mathbb{N}$
output: $d = \mathrm{NWD}(m, n)$
$d \leftarrow 1$
$k \leftarrow 2$
while $k \leqslant m \wedge k \leqslant n$ **do**
  if $k|m \wedge k|n$ **then**
    $d \leftarrow d \cdot k$
    $m \leftarrow m/k$
    $n \leftarrow n/k$
  else
    $k \leftarrow k + 1$
  end if
end while

$m, n \sim 2^{100}$ $\sim 2^{100}$ obrotów

RSA $\sim 2^{4096}$