Podzielność liczb

Definicja

Niech a, $b \in \mathbb{Z}$. Mówimy, że liczba $a > 0$ *dzieli* liczbę b, albo $a|b$, jeżeli istnieje taka *całkowita* liczba c, że $b = ac$.

Definicja

$$a|b \quad \Longleftrightarrow \quad a > 0 \quad \text{i} \quad b = ac, \quad c \text{ całkowite.}$$

Kilka oczywistych prawd

1. $a|0, \quad 1|a, \quad a|a.$
2. $a|1$ wtedy i tylko wtedy gdy $a = \pm 1$.
3. Jeżeli $a|b$ i $c|d$ to $ac|bd$.
4. Jeżeli $a|b$ i $b|c$ to $a|c$.
5. $a|b$ i $b|a$ wtedy i tylko wtedy gdy $a = \pm b$.
6. Jeżeli $a|b$ oraz $a|c$ to $a|(bu + cv)$, gdzie u i v – dowolne liczby całkowite.

Największy wspólny dzielnik

Algorytm Euklidesa: $\mathrm{NWD}(a,b) = ?, \quad a > b$

$$
\begin{array}{lllll}
1) & a : b & a = & q_0 b + r_1, & 0 < r_1 < b, \\
2) & b : r_1 & b = & q_1 r_1 + r_2, & 0 < r_2 < r_1, \\
3) & r_1 : r_2 & r_1 = & q_2 r_2 + r_3, & 0 < r_3 < r_2, \\
\vdots & \vdots & & & \\
n-1) & r_{n-3} : r_{n-2} & r_{n-3} = & q_{n-2} r_{n-2} + r_{n-1}, & 0 < r_{n-1} < r_{n-2}, \\
n) & r_{n-2} : r_{n-1} & r_{n-2} = & q_{n-1} r_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\
n+1) & r_{n-1} : r_n & r_{n-1} = & q_n r_n + 0. & r_{n+1} = 0
\end{array}
$$

Wniosek: r_n – *najmniejsza niezerowa reszta* – jest największym wspólnym dzielnikiem (a, b). Bo:
1)dzieli r_{n-1} 2)dzieli r_{n-2} 3)dzieli r_{n-3} ... dzieli r_1, dzieli b i a.

$\mathrm{NWD}(12\ 378, 3\,054) = ?$

$12\,378 = 4 \cdot 3\,054 + 162 \quad 3\,054 = 18 \cdot 162 + 138 \quad 162 = 1 \cdot 138 + 24$
$138 = 5 \cdot 24 + 18 \quad 24 = 18 + 6 \quad 18 = 3 \cdot 6 + 0 \ \rightarrow 6 = \mathrm{NWD}$

Algorytm Euklidesa – c.d

Działanie dwuargumentowe „mod”

$$n = m\lfloor n/m \rfloor + n \mod m, \qquad \text{albo}$$

$$n \mod m = n - m\lfloor n/m \rfloor.$$

Dla x, y rzeczywistego podobnie:

$$x \mod y = x - y\lfloor x/y \rfloor. \qquad y \neq 0.$$

Interpretacja: Okrąg o obwodzie y, którego punktom przyporządkowano liczby rzeczywiste z przedziału $[0, y]$.
Droga wzdłuż okręgu o długości x – kończymy ją w punkcie $x \bmod y$, a liczbę 0 napotkamy $\lfloor x/y \rfloor$ razy.

$$x = \lfloor x \rfloor + x \mod 1.$$

Prawo rozdzielności:

$$c(x \mod y) = c\,(x - y\lfloor x/y \rfloor) = cx - cy\lfloor cx/cy \rfloor = cx \mod cy.$$

Algorytm Euklidesa – c.d

Algorytm Euklidesa jest oparty w zasadzie na:

twierdzeniu

Jeżeli a, b, q, $r \in \mathbb{Z}$ i zachodzi $a = bq + r \quad (b > 0,\ 0 \leqslant r < b)$.
to $\mathrm{NWD}(a, b) = \mathrm{NWD}(b, r)$.

To twierdzenie jest podstawą

algorytmu: dla $n > m$

1. $\mathrm{NWD}(0, n) = n$;
2. $\mathrm{NWD}(m, n) = \mathrm{NWD}\left[(n \bmod m), m\right], \qquad \text{dla} \quad m > 0.$
3. $\mathrm{NWD}(12{,}18) = \mathrm{NWD}(6{,}12) = \mathrm{NWD}(0{,}6) = 6.$

Liczby pierwsze –

definicja:

Każda liczba całkowita $p > 1$ jest *liczbą pierwszą* jeżeli jej jedynymi dzielnikami jest sama liczba p i liczba 1.

Sito Eratostenesa

Eratostenes (276–194, p.Chr.)
pochodził z Cyreny (Libia)
filozof, astronom, geograf,
kustosz biblioteki aleksandryjskiej
znany z pierwszego (?) pomiaru
promienia Ziemi.

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13

Twierdzenie:

Dla liczb a i b $(a, b \neq 0)$ zachodzi: $\mathrm{NWD}(a, b) = ax + by$, gdzie x, y – pewne liczby całkowite.

NWD(12 378, 3 054) = ?

$12\,378 = 4 \cdot 3\,054 + 162 \quad 3\,054 = 18 \cdot 162 + 138 \quad 162 = 138 + 24$
$138 = 5 \cdot 24 + 18 \quad 24 = 1 \cdot 18 + 6 \quad 18 = 3 \cdot 6 + 0$
$\rightarrow 6 = \mathrm{NWD}(12\,378, 3\,054)$

$6 = x \cdot 12\,378 + y \cdot 3\,054$

$6 = 24 - 18 = 24 - (138 - 5 \cdot 24) = 6 \cdot 24 - 138 = 6 \cdot (162 - 138) - 138 =$
$6 \cdot 162 - 7 \cdot 138 = 6 \cdot 162 - 7 \cdot (3\,054 - 18 \cdot 162) = 132 \cdot 162 - 7 \cdot 3\,054 =$
$132 \cdot (12\,378 - 4 \cdot 3\,054) - 7 \cdot 3\,054 = 132 \cdot 12\,378 - 535 \cdot 3\,054 = \ldots ?$

$6 = 132 \cdot 12\,378 - 535 \cdot 3\,054 =$
$132 \cdot 12\,378 - 535 \cdot 3\,054 + 3\,054 \cdot 12\,378 - 3\,054 \cdot 12\,378 = (132 + 3\,054) \cdot$
$12\,378 + (-535 - 12\,378) \cdot 3\,054 = 3186 \cdot 12\,378 + (-12913) \cdot 3\,054$
nieskończenie wiele sposobów !!!!

Twierdzenie:

Dla liczb a i b $(a, b \neq 0)$ zachodzi: $\mathrm{NWD}(a, b) = ax + by$, gdzie x, y – pewne liczby całkowite.

Dlaczego takie ładne?
Bo istnienie x i y dostarcza dowodu, że nasz algorytm szukania NWD jest *poprawny*. Jest *algorytmem samouzasadniającym się*. Zobaczmy:

Przypuśćmy, że znaleźliśmy $\mathrm{NWD}(m, n) = d$ i że $xm + yn = d$.
A czy jednak NIE może istnieć inny NWD? $d' > d$. Nie może. Bo

- Każdy „nowy dzielnik” d' dzielnik m i n musi dzielić liczbę (ich kombinacje liniową) $xm + yn = d$.
- Skoro tak to dzieli także $xm + yn = d$.
- A więc nie ma $d' > d$. $\square$.

Inne

Twierdzenie

$k|m \quad \text{i} \quad k|n \qquad \Longleftrightarrow \qquad k|\text{NWD}(m,n).$

Bo skoro $k|m \quad \text{i} \quad k|n$ to dzieli także ich kombinacje liniową $xm + yn$. Każdą! a więc i $x'm + y'n = d$.
Na odwrót: jeżeli $k|\text{NWD}(m,n)$ to dzieli któryś z dzielników n, a także dzieli któryś z dzielników m.
A jeśli tak to dzieli zarówno m jak i n. □

Oczywiste wnioski: każdy wspólny dzielnik n i m musi być $\leqslant \text{NWD}(m,n)$. Ale teraz dochodzi:

Twierdzenie:

każdy wspólny dzielnik n i m musi być dzielnikiem $\text{NWD}(m,n)$.

Liczby względnie pierwsze

Definicja

Dwie liczby a, b nazywamy *liczbami względnie pierwszymi* jeżeli $\mathrm{NWD}(a, b) = 1$. takie liczby nie muszą być liczbami pierwszymi.

wniosek (z poprzedniego twierdzenia):

jeżeli liczby a, b są *liczbami względnie pierwszymi* to $1 = xa + yb$ gdzie x, y – pewne liczby całkowite.

wniosek (z poprzedniego wniosku)

jeżeli $\mathrm{NWD}(a, b) = d$ to $\mathrm{NWD}(a/d, b/d) = 1$.

$d = \mathrm{NWD}(a, b) = ax + by \rightarrow 1 = \mathrm{NWD}(a/d, b/d)$

kolejny ważny! wniosek

jeżeli $a|c$ i $b|c$, a NWD $(a, b) = 1$ to $ab|c$.

$c = ar = bs, \qquad 1 = ax + by \rightarrow c \cdot 1 = cax + cby = (bs)ax + (ar)by = ab(sx + ry)$

Liczby względnie pierwsze, c.d

Lemat Euklidesa

jeżeli liczby a, b są *liczbami względnie pierwszymi* i $a|bc$ to $a|c$.

$1 = xa + yb \rightarrow c = cxa + ybc$ mamy (z zał.) $a|(cxa + ybc) \rightarrow a|c$
uwaga: koniecznie muszą to być liczby względnie pierwsze!!

wniosek z poprzedniego lematu

jeżeli p jest liczbą pierwszą i $p|ab$ to $p|a$ albo $p|b$.

$p \not| a$ $\text{NWD}(a, p) = 1$ lemat: $p|b$

uogólnienie poprzedniego wniosku:

jeżeli p jest liczbą pierwszą i $p|a_1 a_2 \ldots a_k$ to $p|a_k$ dla pewnego k.

Liczby względnie pierwsze, c.d

i jeszcze jeden wniosek

Każda liczba złożona jest podzielna przez pewną liczbę pierwszą p.

n liczba złożona $\rightarrow \exists d,\ 1 < d < n, \quad d|n.$ Najmniejszym takim dzielnikiem musi być liczba pierwsza p. $(r.a.a.)$

przy badaniu podzielności liczby złożonej

a wystarczy badać potencjalne dzielniki mniejsze od $\ldots \sqrt{a}$.

no jasne: $a = bc;\ b \leqslant c;\ 1 < b \rightarrow b^2 \leqslant bc = a \rightarrow b \leqslant \sqrt{a}$
a przecież $b > 1$ musi mieć dzielnik p

Liczby pierwsze

podstawowe twierdzenie teorii liczb

Każda liczba $n > 1$ **...** może być przedstawiona jako iloczyn liczb pierwszych;
taka reprezentacja jest jedna (jeżeli nie liczyć permutacji).
Jest to tzw. *rozkład kanoniczny liczby n.*

$$\boxed{n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}} \qquad 4725 = 3^3 \cdot 5^2 \cdot 7$$

$\boxed{\sqrt{2} \neq a/b}$ $\qquad r.a.a.$

$\sqrt{2} = a/b, \quad (a,b) = 1 \rightarrow a^2 = 2b^2, \rightarrow b|a^2 \quad \rightarrow \exists p\ p|b \rightarrow p|a^2 \rightarrow p|a$!!

kolejne podstawowe twierdzenie teorii liczb

Istnieje nieskończenie wiele liczb pierwszych (Euklides!).

dowód: p; $\qquad N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p) + 1 \stackrel{def}{=} e_p + 1.$
Zgodnie z 1. podstawowym twierdzeniem istnieje liczba pierwsza q;
$q \mid N$. Widać, że nie może to być żadna z liczb 2, 3, 5, 7, 11, ... p –
bo wtedy q dzieliłoby też *różnicę* $N - (N-1)$ czyli 1.

Rozkład kanoniczny – wnioski

Największy Wspólny Dzielnik *NWD*

Jeżeli dwie liczby m i n mają rozkłady kanoniczne
$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ i $n = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$
(N.B. r jest *takie samo* – pamiętaj, że pewne wykładniki α_i i/lub β_j, $i, j = 1, 2, \dots, r$ mogą być równe zeru!) to jest oczywiste, że

$$NWD(m,n) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r}, \quad \text{gdzie} \quad \gamma_i = \min(\alpha_i, \beta_i).$$

Najmniejsza Wspólna Wielokrotność *NWW*

Analogicznie, *Najmniejsza Wspólna Wielokrotność* liczb m i n –
$w = NWW(m,n) \quad \Rightarrow \quad m \mid w \quad \wedge \quad n \mid w$, to

$$NWW(m,n) = p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_r^{\epsilon_r}, \quad \text{gdzie} \quad \epsilon_i = \max(\alpha_i, \beta_i).$$

wniosek:

$$NWD \cdot NWW = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r} \cdot p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_r^{\epsilon_r} = m \cdot n.$$

Sito Eratostenesa, c.d

- 1659 – J.H. Rahn *Teusche Algebra* czynniki pierwsze liczb do 24 000 (nieparzyste, niepodzielne przez 5).
- 1668 – John Pell rozszerzenie tablic do 100 000.
- 1776 – Anton Felkel – do 408 000 ale ... wydruk skonfiskowano i z papieru sporządzono ... naboje (wojna z Turkami)
- J.P. Kulik (Praga) (1773–1863) – tablice rozkładu na czynniki pierwsze aż do 100 000 000 (rękopis złożony w bibliotece cesarskiej w Wiedniu)
- 1909 – Derrick Norman Lehmer
  Factor Table for the First Ten Million
  – tablice rozkładu na czynniki pierwsze.