Matematyka dyskretna

Wykład 4: Podzielność liczb całkowitych

Gniewomir Sarbicki

Literatura

- Kenneth A. Ross, Charles R. B. Wright *Matematyka Dyskretna* PWN 2005
- J. Jaworski, Z. Palka, J. Szymański *Matematyka Dyskretna dla Informatyków*
- A. Szepietowski *Matematyka Dyskretna*
- S. G. Krantz *Discrete Mathematics Demystified*
- Kenneth A. Rosen *Handbook of discrete and combinatorial mathematics*

Dzielenie całkowitoliczbowe

Twierdzenie:

Dla każdej pary liczb całkowitych (a, b) istnieje dokładnie jedna para liczb całkowitych (q, r) spełniająca równanie

$$a = qb + r$$

przy warunku $r \in \{0, \ldots b - 1\}$. Liczby te oznaczamy następująco:

- $q = a \text{ div } b$ lub $a \div b$ iloraz całkowitoliczbowy liczb a i b
- $a \mod b$ reszta z dzielenia a przez b

Relacja podzielności

Definicja:

Mamy dane dwie liczby $a, b \in \mathbb{Z}$. Jeżeli:

$$\exists k \in \mathbb{Z}\ b = a \cdot k$$

to mówimy że *liczba* a *dzieli liczbę* b i ozaczamy ten fakt jako $a|b$.

Fakt:

Relacja podzielności $| \subset (\mathbb{Z})^2$ jest relacją częściowego porządku (zwrotna, słabo antysymetryczna, przechodnia).

Własności relacji podzielności:

- $a|b \implies \forall c \in \mathbb{Z} \quad a|(cb)$
- $a|b \wedge a|c \implies a|(b+c), \quad a|(b-c)$

Największy wspólny dzielnik

Definicja:

Największy wspólny dzielnik liczb a i b to największa liczba całkowita, która dzieli obie liczby. Oznaczamy go jako $NWD(a, b)$.

Lemat:

Jeżeli $0 < a \leqslant b$, to $NWD(a, b) = NWD(b \mod a, a)$

Dowód: Oznaczmy $d = NWD(a, b)$.

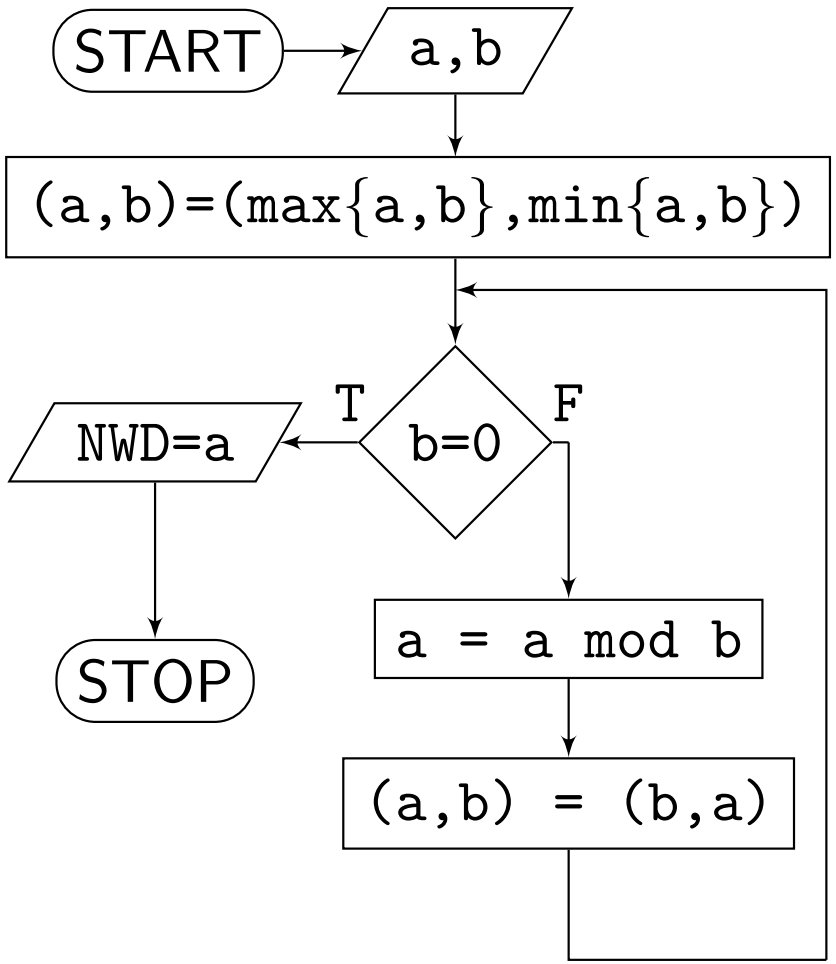
$$b \mod a = b - (b \div a) \cdot a$$

d dzieli oba składniki po prawej stronie równości, zatem dzieli lewą stronę ($d|b, a \implies d|a, b \mod a$). W drugą stronę:

$$b = b \mod a + (b \div a) \cdot a$$

d dzieli oba składniki po prawej stronie równości, zatem dzieli lewą stronę ($d|a, b \mod a \implies d|b, a$). Pary (b, a) i $(a, b \mod a)$ mają te same wspólne dzielniki, więc również NWD $\square$

Algorytm Euklidesa



Dowód poprawności algorytmu:

- Na podstawie lematu, NWD jest niezmiennikiem pętli.
- W każdym przebiegu pętli liczby a i b się zmniejszają i nie można dostać liczby mniejszej od 0, zatem pętla skończy swoje działanie.
- Gdy pętla skończy działanie, NWD będzie równy $NWD(a, 0) = a$.

Złożoność czasowa

Twierdzenie: Algorytm kończy się w mniej niż $2\log_2(a+b)$ krokach.

Dowód: Dla dowolnych dwóch liczb a, b:

$b + a \mod b < 2b < 2b(a \div b) \quad / + 2(a \mod b) + 2b$

$3(b + a \mod b) < 2(a + b)$

$b + a \mod b < \frac{2}{3}(a + b)$

W każdym przebiegu pętli, suma liczb a, b zmniejsza się przynajmniej o $\frac{2}{3}$.

$1 \leqslant \text{wynik} + 0 \leqslant \left(\frac{2}{3}\right)^k (a + b)$

$k \leqslant \log_{\frac{3}{2}}(a + b) = \frac{\log_2(a+b)}{\log_2(\frac{3}{2})} < 2\log_2(a + b)$ $\square$

Rozszerzony algorytm Euklidesa

Twierdzenie (Tożsamość Bézout):

Niech $a, b \in \mathbb{N}$ i $d = NWD(a, b)$:

1. Istnieją $x, y \in \mathbb{Z}$ takie, że $xa + yb = d$.
2. Dla każdych $x, y \in \mathbb{Z}$ wyrażenie $xa + yb$ jest wielokrotnością d.

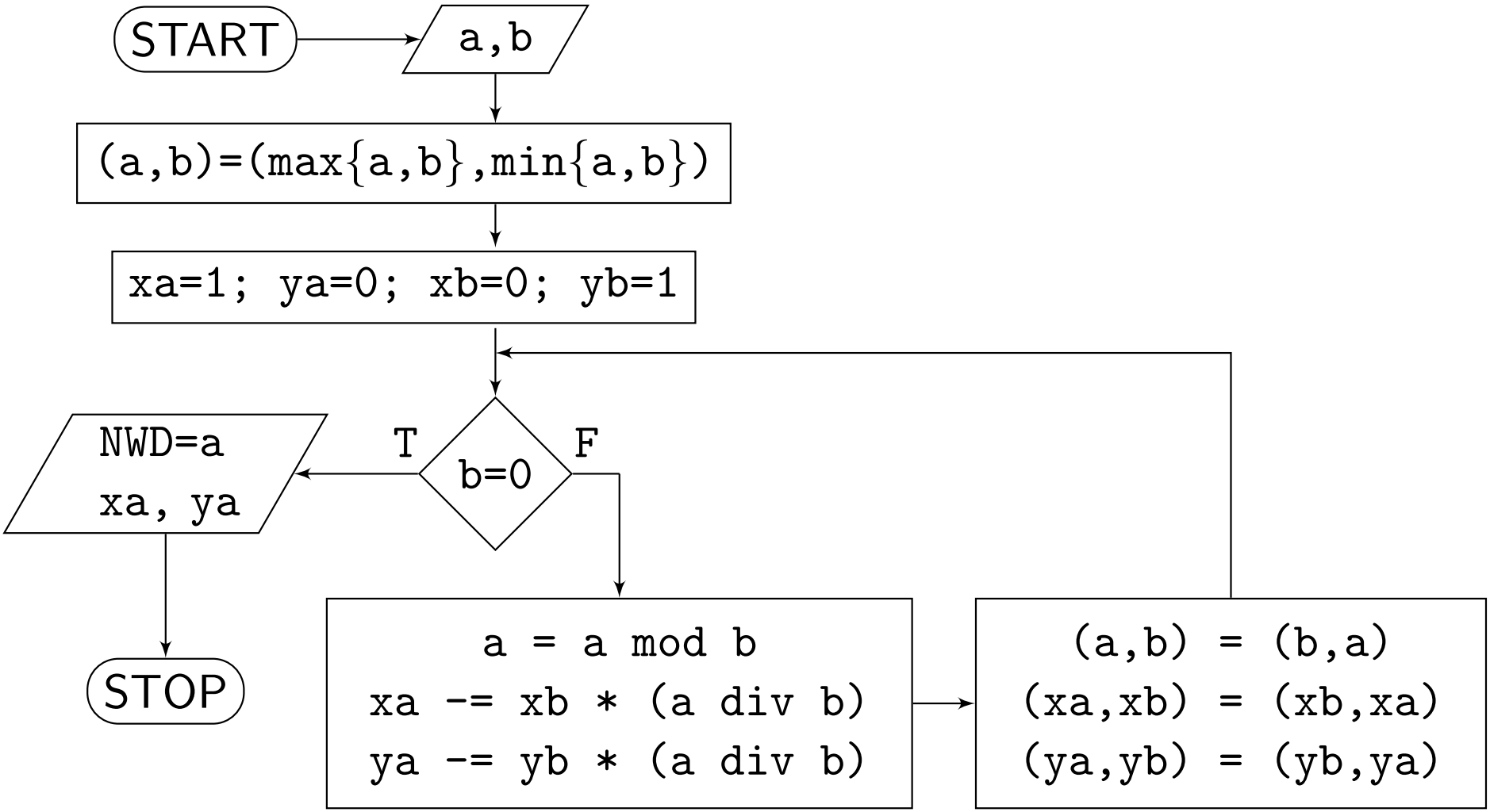
Dowód (1): Udowodnimy indukcyjnie, że w każdym przebiegu pętli algorytmu Eulidesa liczby a_n i b_n można przedstawić jako kombinację całkowitoliczbową liczb wejściowych a_0, b_0.

(P) Liczby a_0 i b_0 są swoimi kombinacjami w oczywisty sposób

(I) Niech $a_n = x_a a_0 + y_a b_0$ oraz $b_n = x_b a_0 + y_b b_0$. Wtedy $a_{n+1} = x_b a_0 + y_b b_0$, natomiast $b_{n+1} = a_n - (a_n \div b_n) b_n = (x_a - x_b \cdot (a_n \div b_n)) a_0 + (y_a - y_b \cdot (a_n \div b_n)) b_0$, zatem a_{n+1} i b_{n+1} znów są kombinacjami całkowitoliczbowymi liczb a_0 i b_0.

Zachodzi to również dla ostatniego przebiegu pętli, zatem własność tę posiada również $NWD(a_0, b_0)$ $\square$

Rozszerzony algorytm Euklidesa



Liczby pierwsze i względnie pierwsze

Definicja:

- Liczbę naturalną $p \geqslant 2$ nazywamy pierwszą, jeżeli jej jedynymi dzielnikami naturalnymi są 1 i samo p.
- Zbiór liczb pierwszych będziemy oznaczać jako $\mathcal{P}$

Liczby pierwsze mniejsze od 50:
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$

Definicja:

Liczby naturalne a i b nazywamy względnie pierwszymi, jeżeli $NWD(a, b) = 1$.

Przykład: Liczby 9 i 16 są względnie pierwsze

Rozkład na czynniki pierwsze

Definicja:

Liczbę naturalną, która nie jest liczbą pierwszą, nazywamy liczbą **złożoną**

Fakt:

Każdą liczbę złożoną da się przedstawić jako iloczyn liczb pierwszych.

Dowód: Indukcyjny: Każda liczba mniejsza niż n ma tę własność...

Jednoznaczność rozkładu

Lemat (L1)

Niech a, b względnie pierwsze. Wtedy $\forall c\ a|bc \implies a|c$

Dowód: $\exists x, y\ xa + yb = 1$. Zatem $xca + ycb = c$. Ponieważ a dzieli obie liczby po lewej stronie, dzieli też prawą stronę. $\square$

Lemat L2

Dla l. pierwszych $p, q_1, \ldots, q_n$ mamy $p|q_i \cdot \cdots \cdot q_n \implies \exists i\ p = q_i$

Dowód: (indukcyjny) Dla $n = 1$: $p|q_1$ (oczywiste)
‘ (I): $p|q_1 \cdot \cdots \cdot q_{n+1} \iff$

- $p|q_{n+1} \implies p = q_{n+1}$ - OK
- $NWD(p, q_{n+1}) = 1$ i jednocześnie $p|q_1 \cdot \cdots \cdot q_{n+1}$. Stąd (L1): $p|q_1 \cdot \cdots \cdot q_n \overset{z.ind.}{\implies} \exists i \leqslant n\ p|q_i$. $\square$

Jednoznaczność rozkładu

Zasadnicze twierdzenie arytmetyki:

Każdą liczbę naturalną można w sposób jednoznaczny przedstawić w postaci iloczynu:

$$n = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r},$$

dla l. pierwszych $p_1 < \dots < p_r$ oraz naturalnych wykładników α_i.

Dowód: Niech n będzie najmniejszą liczbą, dla której istnieją dwa różne rozkłady:

$$n = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r} = q_1^{\beta_1} \cdot \dots \cdot q_s^{\beta_s},$$

Żaden czynnik z lewej strony, powiedzmy p_1, nie może występować po prawej stronie (bo wtedy liczba $\frac{n}{p_1}$ byłaby mniejszą liczbą o niejednoznacznym rozkładzie). Z drugiej strony, liczba p dzieli prawą stronę, zatem na mocy (L2) występuje w tym iloczynie. $\square$

Lemat Euklidesa

Lemat: (Euklidesa)

Dla dowolnego zbioru liczb pierwszych $\{a_1, \ldots, a_n\}$ liczba $a_1 \cdot \ldots \cdot a_n + 1$ nie jest podzielna przez żadną z liczb z tego zbioru.

Wniosek: Ponieważ liczba $a_1 \cdot \ldots \cdot a_n + 1$ jest podzielna przez pewną liczbę pierwszą, zatem istnieje liczba pierwsza spoza tego zbioru $\implies$ Istnieje nieskończenie wiele liczb pierwszych.

Postulat Bertranda

$\forall n \geqslant 2 \; \exists p \in \mathcal{P} \; p \in [n, 2n)$

Udowodniony przez Czebyszewa.

Fakt:

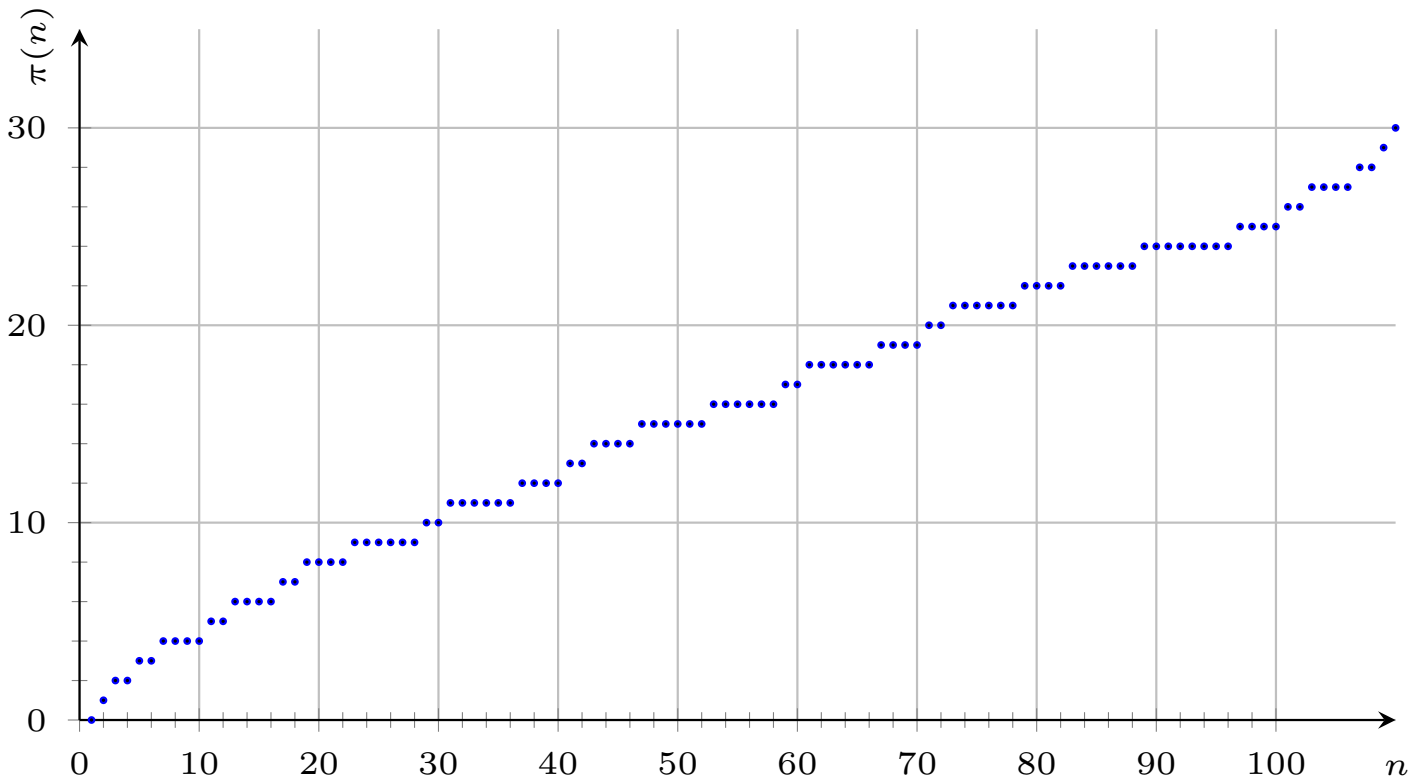
Istnieje dowolnej długości ciąg kolejnych liczb złożonych

Dowód: Rozważ ciąg $n! + 2, \ldots, n! + n$

Funkcja π

Definicja:

Wartością funkcji $\pi : \mathbb{N} \to \mathbb{N}$ jest ilość liczb naturalnych mniejszych bądź równych od jej argumentu.



Twierdzenie o liczbach pierwszych

Twierdzenie (o liczbach pierwszych)

Stosunek funkcji $\pi(x)$ i funkcji $\frac{x}{\ln x}$ zmierza do 1 dla $x \to \infty$.

Twierdzenie to zapostulował Gauss w 1792 roku. Zostało udowodnione przez Poussina i Hadamarda w 1896 roku we wzmocnionej wersji:

$$|\pi(x) - \mathrm{li}(x)| < c_1 x e^{-c_2\sqrt{\ln x}} \qquad \mathrm{li}(x) \stackrel{df}{=} \int_0^x \frac{dt}{\ln t} \stackrel{x\to\infty}{\longrightarrow} \frac{x}{\ln(x)}$$

W roku 1949 roku P.Erdős i A. Seberg podali dowód nie używający teorii funkcji zmiennej zespolonej.

Sito Eratostenesa

```
Wygeneruj tablicę liczb od 2 do N
i:=1
while i ⩽ sqrt(N):
  i:=i+1
  jeżeli i nie jest wykreślone, usuń z tablicy
  jego wielokrotności
Liczby które zostaną w tablicy są liczbami
pierwszymi
```

n-ta liczba pierwsza

Oznaczmy przez p_n n-tą liczbę pierwszą.

Nie istnieje praktyczny wzór pozwalający wyznaczyć p_n.

Istnieje wzór przybliżony:

$$p_n \approx n \ln n \quad (p_n > n \ln n)$$

$$\frac{p_n}{n \ln n} \to 1$$