PODSTAWOWE POJĘCIA ALGEBRAICZNE

Definicja. Grupa — trójka $(G, e, \circ)$ taka, że:
(1) $e \in G$,
(2) $a, b \in G \Rightarrow a \circ b \in G$,
(3) $a, b, c \in G \Rightarrow a \circ (b \circ c) = (a \circ b) \circ c$,
(4) $a \in G \Rightarrow a \circ e = e \circ a = a$,
(5) $a \in G \Rightarrow \exists a^{-1}\ a \circ a^{-1} = a^{-1} \circ a = e$.

Definicja. Grupa abelowa:
(6) $a, b \in G \Rightarrow a \circ b = b \circ a$.

Definicja. Rząd grupy: $|G|$.

Definicja. $a^n = \underbrace{a \circ a \circ \ldots \circ a}_{n}, \quad a^{-n} = \left(a^{-1}\right)^n, \quad a^0 = e.$

Definicja. Grupa cykliczna: istnieje $a \in G$ taki, że:
- $G = \{e, a^1, a^2, \ldots, a^{n-1}\}$, gdy G jest skończona;
- $G = \{\ldots, a^{-2}, a^{-1}, e, a^1, a^2, \ldots\}$, gdy G jest nieskończona.

Definicja. Podgrupa: zbiór $H \subseteq G$ taki, że $a, b \in H \Rightarrow ab^{-1} \in H$.

Twierdzenie 1. (Lagrange) Jeśli H jest podgrupą G, to $|H| \,\Big|\, |G|$.

Definicja. Pierścień — piątka $(R, 0, 1, +, \cdot)$ taka, że:
(1) $(R, 0, +)$ jest grupą abelową,
(2) $a, b \in R \Rightarrow a \cdot b \in R$,
(3) $a, b \in R \Rightarrow a \cdot b = b \cdot a$,
(4) $a, b, c \in R \Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
(5) $a \in R \Rightarrow a \cdot 1 = a$,
(6) $a, b, c \in R \Rightarrow a \cdot (b + c) = a \cdot b + a \cdot c$.

Definicja. Ciało — piątka $(K, 0, 1, +, \cdot)$ taka, że
(1) $(K, 0, 1, +, \cdot)$ jest pierścieniem,
(2) $a \in K$ i $a \neq 0 \Rightarrow \exists a^{-1}\ a \cdot a^{-1} = 1$.

Definicja. Charakterystyka ciała: najmniejsza liczba $p > 0$ taka, że

$$\underbrace{1 + 1 + \ldots + 1}_{p} = 0,$$

jeśli taka istnieje, 0 w przeciwnym przypadku.

Twierdzenie 2. Istnieje ciało mające q elementów wtedy i tylko wtedy, gdy $q = p^k$, gdzie p jest liczbą pierwszą. Liczba p jest wtedy charakterystyką tego ciała. Każde dwa ciała skończone mające tę samą liczbę elementów są izomorficzne.

Definicja. $GF(q)$ — ciało skończone mające q elementów.

Przykład: ciało $GF(5)$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

PODZIELNOŚĆ

Definicja. Niech $a, b \in \mathbb{Z}$. Wtedy $\quad a \mid b \Leftrightarrow \exists c \in \mathbb{Z} \quad ac = b$.

Przykłady: $4 \mid 100, \quad 100 \mid 100, \quad -5 \mid 100, \quad 30 \not| \, 100$.

Własności:

(1) $a \mid a$,
(2) $a \mid b$ i $b \mid a \Rightarrow a = b$ lub $a = -b$,
(3) $a \mid b$ i $b \mid c \Rightarrow a \mid c$,
(4) $a \mid b \Rightarrow a \mid bc$,
(5) $a \mid b$ i $c \neq 0 \Leftrightarrow ac \mid bc$,
(6) $a \mid b$ i $a \mid c \Rightarrow a \mid (b + c)$.

Twierdzenie 3. Jeśli $a, b \in \mathbb{Z}$ oraz $b > 0$, to istnieją q i r takie, że

$$a = bq + r \quad \text{oraz} \quad 0 \leq r < b.$$

Twierdzenie 4. Jeśli $b > 0$ oraz $0 \leq a < b^n$, to istnieją $c_{n-1}, c_{n-2}, \ldots, c_1, c_0$ takie, że

$$a = c_{n-1}b^{n-1} + c_{n-2}b^{n-2} + \ldots + c_1 b + c_0$$

oraz

$$0 \leq c_{n-1}, c_{n-2}, \ldots, c_1, c_0 < b.$$

Ciąg $(c_{n-2}, c_{n-1}, \ldots, c_1, c_0)$ jest wyznaczony jednoznacznie.

LICZBY PIERWSZE

Definicja. Liczba pierwsza — taka liczba $p > 1$, że:

$$d \mid p \ \text{ i } \ d > 0 \quad \Rightarrow \quad d = 1 \ \text{ lub } \ d = p.$$

Twierdzenie 5. Każda liczba naturalna ma dzielnik pierwszy.

Dowód. Niech $n \in \mathbb{N}$ i niech $p = \min\{d : \ d > 1 \ \text{ oraz } \ d \mid n\}$. Wtedy $p \mid n$ oraz p jest pierwsza. ♠

Twierdzenie 6. Każda liczba złożona n ma dzielnik pierwszy $p \leq \sqrt{n}$.

Dowód. Niech $n = p \cdot m$, gdzie p jest najmniejszym dzielnikiem pierwszym n. Wtedy $p \leq m$ i stąd

$$p^2 \leq p \cdot m = n, \quad ♠$$

Twierdzenie 7. Każda liczba naturalna jest iloczynem liczb pierwszych.

Dowód. Indukcja. Niech $p \mid n$. Wtedy z założenia indukcyjnego

$$n \,\mathbf{div}\, p = p_1 \cdot \ldots \cdot p_k$$

i stąd

$$n = p \cdot p_1 \cdot \ldots \cdot p_k. \quad ♠$$

Twierdzenie 8. Rozkład liczby naturalnej na czynniki pierwsze jest jednoznaczny z dokładnością do kolejności czynników.

Dowód. Indukcja. Niech n — najmniejsza liczba naturalna mająca dwa różne rozkłady:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s.$$

Oczywiście $r, s \geq 2$. Ponadto $\{p_1, \ldots, p_r\} \cap \{q_1, \ldots, q_s\} = \varnothing$. Gdyby bowiem np. $p_1 = q_1$, to

$$n \,\mathbf{div}\, p_1 = p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s,$$

co przeczyłoby minimalności n. Możemy założyć, że $p_1 < q_1$. Definiujemy

$$N := (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_s.$$

Wtedy

$$N = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_s = p_1 \cdot (p_2 \cdot \ldots \cdot p_r - q_2 \cdot \ldots \cdot q_s).$$

Liczba N ma jednoznaczny rozkład, ale p_1 występuje w jednym (prawym) rozkładzie i nie występuje w drugim (lewym); sprzeczność. ♠

Twierdzenie 9. (Euklides) Istnieje nieskończenie wiele liczb pierwszych.

Dowód. (Oryginalny) Niech $p_1, \ldots, p_k$ — wszystkie liczby pierwsze. Kładziemy

$$n := p_1 \cdot \ldots \cdot p_k + 1.$$

Wtedy $\exists i\ p_i \mid n$, skąd wynika, że $p_i \mid n - p_1 \cdot \ldots \cdot p_k$, czyli $p \mid 1$; sprzeczność. ♠

Twierdzenie 10. Szereg $\sum\limits_p \frac{1}{p}$, gdzie p przebiega liczby pierwsze, jest rozbieżny.

Dowód. $p_1, p_2, \ldots, p_n, \ldots$ — liczby pierwsze w kolejności rosnącej. Przypuśćmy, że szereg $\sum\limits_i \frac{1}{p_i}$ jest zbieżny. Wtedy

$$\exists k \quad \sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}.$$

Niech $N = 2^{2k+2}$. Wtedy

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Oznaczmy:
(1) $N_b = \{n \leq N :\ \exists i > k\ p_i \mid n\}$,
(2) $N_s = \{n \leq N :\ \forall i > k\ p_i \not| \, n\}$.

Wtedy

$$|N_b| \leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}.$$

Niech teraz $n \in N_s$. Wtedy $n = a_n \cdot b_n^2$, gdzie a_n jest iloczynem różnych liczb pierwszych spośród $p_1, \ldots, p_k$. Istnieje 2^k takich liczb a_n. Ponadto $b_n \leq \sqrt{N} = 2^{k+1}$, więc istnieje 2^{k+1} takich liczb b_n. Zatem

$$|N_s| = 2^k \cdot 2^{k+1} = 2^{2k+1} = \frac{N}{2}.$$

Stąd

$$N = |N_b| + |N_s| < \frac{N}{2} + \frac{N}{2} = N, \quad \text{sprzeczność.}$$ ♠

TWIERDZENIE CZEBYSZEWA

Twierdzenie 11. Dla każdej liczby n istnieje liczba pierwsza p taka, że $n < p \leq n! + 1$.

Dowód. Niech $N = n! + 1$. Niech $p \mid N$ i p pierwsza. Wtedy $p \leq n! + 1$. Gdyby $p \leq n$, to $p \mid N$ oraz $p \mid n!$, skąd $p \mid 1$; sprzeczność. ♠

Twierdzenie 12. (Czebyszew) Dla każdej liczby n istnieje liczba pierwsza p taka, że $n < p \leq 2n$.

Dowód. Odkładamy na później

Twierdzenie 13. Dla każdej liczby n istnieje n kolejnych liczb złożonych.

Dowód. Liczby

$$(n+1)!+2, \quad (n+1)!+3, \quad (n+1)!+4, \quad \ldots, \quad (n+1)!+(n+1)$$

są złożone. ♠

Uwaga. Najniżej występująca luka długości 100:

$$396733 \quad - \quad 396833.$$

TWIERDZENIE O LICZBACH PIERWSZYCH

Definicja. $\pi(x) = |\{p: \ p \leq x \ \text{ i } \ p \ \text{ pierwsza } \}|$.

Przykłady: $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$.

Twierdzenie 14.

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Twierdzenie 15.

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1,$$

gdzie

$$\mathrm{Li}(x) = \int_0^x \frac{dt}{\ln t}.$$

Hipotezy dotyczące liczb pierwszych.

(1) Hipoteza Goldbacha: każda liczba parzysta jest sumą dwóch liczb pierwszych.

(2) Hipoteza liczb bliźniaczych: istnieje nieskończenie wiele par liczb pierwszych postaci p i $p+2$.

(3) Istnieją dowolnie długie ciągi arytmetyczne złożone z liczb pierwszych.

$n = 5$: $\quad 5, 11, 17, 23, 29$;
$n = 22$: $\quad p = 11410337850553$, $r = 4609098694200$.

SITO ERATOSTENESA

```
var
  A : array [2..n] of Boolean;
  p, j, k : integer;
begin
for p := 2 to n do
  A[p] := TRUE;
p := 2;
j := p * p;
while j ≤ n do begin
  k := j;
  while k ≤ n do begin
    A[k] := FALSE;
    k := k + p
  end;
  p := p + 1;
  while not A[p] do
    p := p + 1;
  j := p * p
end
{Liczba p ≤ n jest pierwsza wtedy i tylko wtedy, gdy A[p]}
end
```

ZŁOŻONOŚĆ DZIAŁAŃ ARYTMETYCZNYCH

Oznaczenie. Jeśli $x = c_{n-1}b^{n-1} + c_{n-2}b^{n-2} + \ldots + c_1 b + c_0$, gdzie $0 < c_{n-1} < b$ oraz $0 \le c_{n-2}, \ldots, c_1, c_0 < b$, to $lh_b(x) = n$. Jeśli $b = 2$, to piszemy po prostu $lh(x)$.

Twierdzenie 16. $lh_b(x) = 1 + \lfloor \log_b x \rfloor$ dla $x \neq 0$.

Twierdzenie 17. Niech $lh(x) = lh(y) = n$. Oznaczmy przez $T(x \circ y)$ czas potrzebny na wykonanie działania $x \circ y$. Wtedy dla algorytmów „szkolnych” mamy:

(1) $T(x + y) = O(n)$,
(2) $T(x - y) = O(n)$,
(3) $T(x \cdot y) = O(n^2)$;
(4) $T(x \,\mathbf{div}\, y) = O(n^2)$;
(5) $T(x \,\mathbf{mod}\, y) = O(n^2)$.

Istnieją algorytmy wykonujące mnożenie i dzielenie szybciej niż algorytmy „szkolne”.

Przykład. Niech $lh(a) = lh(b) = 2n$. Przedstawmy liczby a i b w postaci

$$a = 2^n A_1 + A_2, \quad b = 2^n B_1 + B_2,$$

gdzie

$$lh(A_1) = lh(A_2) = lh(B_1) = lh(B_2) = n.$$

Wtedy

$$ab = (2^{2n} + 2^n)A_1B_1 + 2^n(A_1 - A_0)(B_0 - B_1) + (2^n + 1)A_0B_0.$$

Oznaczmy przez $t(n)$ czas potrzebny do pomnożenia w ten sposób dwóch liczb długości n. Wtedy

$$t(2n) \leq 3t(n) + Cn.$$

Stąd przez łatwą indukcję dostajemy:

$$t(2^k) \leq c(3^k - 2^k).$$

Stąd zaś:

$$\begin{aligned} t(n) &= t(2^{lh(n)}) \leq c(3^{lh(n)} - 2^{lh(n)}) \leq \\ &\leq c \cdot 3^{1+\log_2 n} = 3c \cdot 3^{\log_2 n} = \\ &= 3c \cdot n^{\log_2 3}. \end{aligned}$$

Zatem $t(n) = O(n^{\log_2 3})$. Warto wiedzieć, że

$$\log_2 3 \approx 1,585.$$

Twierdzenie 18. Istnieje algorytm mnożenia działający w czasie

$$T(x \cdot y) = O(n \log_2 n \log_2 \log_2 n),$$

gdzie

$$n = lh(x) = lh(y).$$

Twierdzenie 19. Istnieje algorytm dzielenia działający w czasie

$$T(x \,\mathbf{div}\, y) = T(x \,\mathbf{mod}\, y) = O(M(n)),$$

gdzie

$$n = lh(x) = lh(y)$$

oraz $M(n)$ jest czasem potrzebnym do pomnożenia dwóch liczb długości n.

NWD I NWW

Definicja.

$$\begin{aligned}\mathrm{NWD}(a,b) &= \max\{d:\ d\mid a \ \text{ i } \ d\mid b\},\\ \mathrm{NWW}(a,b) &= \min\{m>0:\ a\mid m \ \text{ i } \ b\mid m\}.\end{aligned}$$

Twierdzenie 20. Jeśli

$$\begin{aligned}a &= p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n},\\ b &= p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_n^{\beta_n},\end{aligned}$$

to

$$\begin{aligned}\mathrm{NWD}(a,b) &= p_1^{\min(\alpha_1,\beta_1)}\cdot p_2^{\min(\alpha_2,\beta_2)}\cdot\ldots\cdot p_n^{\min(\alpha_n,\beta_n)},\\ \mathrm{NWW}(a,b) &= p_1^{\max(\alpha_1,\beta_1)}\cdot p_2^{\max(\alpha_2,\beta_2)}\cdot\ldots\cdot p_n^{\max(\alpha_n,\beta_n)}.\end{aligned}$$

Własności.

(1) $\mathrm{NWD}(a,b)=d\Rightarrow \mathrm{NWD}(a\,\mathbf{div}\,d, b\,\mathbf{div}\,d)=1$,
(2) $\mathrm{NWD}(a+cb,b)=\mathrm{NWD}(a,b)$,
(3) $a\mid b\Rightarrow \mathrm{NWD}(a,b)=a$,
(4) $\mathrm{NWD}(a,0)=a$,
(5) $\mathrm{NWD}(a,b)\cdot\mathrm{NWW}(a,b)=ab$,
(6) $a\mid bc$ i $\mathrm{NWD}(a,b)=1\Rightarrow a\mid c$,
(7) $a\mid c$ i $b\mid c$ i $\mathrm{NWD}(a,b)=1\Rightarrow ab\mid c$,
(8) $\mathrm{NWD}(a,b)=1$ i $c\mid ab\Rightarrow \exists d,e\ (d\mid a$ i $e\mid b$ i $c=de)$.

PODGRUPY $\mathbb{Z}$

Twierdzenie 21. Niech H będzie podgrupą $\mathbb{Z}$. Wtedy istnieje dokładnie jedna liczba $d\in\mathbb{Z}$ taka, że

$$H=\{0,\pm d,\pm 2d,\ldots\}=d\mathbb{Z}.$$

Dowód. Oczywiście $0\in H$. Jeśli $H=\{0\}$, to $d=0$.

Niech teraz $H\neq\{0\}$. Istnieje $a\in H$ taka, że $a\neq 0$. Wtedy również $-a\in H$. Zatem w H istnieje liczba dodatnia. Niech

$$d=\min\{a\in H:\ a>0\}.$$

Wtedy oczywiście $d\mathbb{Z}\subseteq H$. Niech $a\in H$. Istnieją q i r takie, że

$$a=dq+r \quad\text{oraz}\quad 0\le r<d.$$

Wtedy

$$r=a-dq\in H$$

i z minimalności d wynika, że $r = 0$. Zatem

$$a \in d\mathbb{Z}.$$

Gdyby były dwa takie generatory d i d', to

$$d = d't \quad \text{oraz} \quad d' = ds$$

dla pewnych t i s. Stąd $ts = 1$. Ale $d, d' > 0$, więc $t = s = 1$ i $d = d'$. ♠

Twierdzenie 22. Istnieją $x, y \in \mathbb{Z}$ takie, że

$$\mathrm{NWD}(a, b) = ax + by.$$

Dowód. Rozważamy podgrupę

$$H = \{ax + by : \ x, y \in \mathbb{Z}\} = a\mathbb{Z} + b\mathbb{Z}.$$

Istnieje wtedy $d \in \mathbb{Z}$ taki, że

$$H = d\mathbb{Z}.$$

Ponieważ $a, b \in H$, więc

$$d \mid a \quad \text{oraz} \quad d \mid b.$$

Jeśli zaś

$$d' \mid a \quad \text{oraz} \quad d' \mid b,$$

to oczywiście

$$d' \mid ax + by,$$

czyli $d' \mid d$. Zatem

$$d = \mathrm{NWD}(a, b). \quad ♠$$

Twierdzenie 23.

$$\mathrm{NWD}(a, b) = 1 \Leftrightarrow \exists s, t \ as + bt = 1.$$

Definicja. Liczby a i b są **względnie pierwsze** wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, b) = 1$. Piszemy wtedy $a \perp b$.

ALGORYTM EUKLIDESA

Niech $a \geq b > 0$. Oznaczmy

$$r_0 = a, \quad r_1 = b.$$

Wykonajmy dzielenia

$$\begin{array}{lll}
r_0 = r_1 q_1 + r_2, & & 0 \le r_2 < r_1, \\
r_1 = r_2 q_2 + r_3, & & 0 \le r_3 < r_2, \\
\ldots & \ldots & \ldots \\
r_{j-2} = r_{j-1} q_{j-1} + r_j, & & 0 \le r_j < r_{j-1}, \\
\ldots & \ldots & \ldots \\
r_{n-4} = r_{n-3} q_{n-3} + r_{n-2}, & & 0 \le r_{n-2} < r_{n-3}, \\
r_{n-3} = r_{n-2} q_{n-2} + r_{n-1}, & & 0 \le r_{n-1} < r_{n-2}, \\
r_{n-2} = r_{n-1} q_{n-1} + r_n, & & 0 \le r_n < r_{n-1}, \\
r_{n-1} = r_n q_n. & &
\end{array}$$

Ponieważ

$$r_0 \ge r_1 > r_2 > r_3 > \ldots > r_n \ge 0,$$

więc algorytm musi się zakończyć, tzn. ostatnie dzielenie musi dać resztę 0.

Zauważmy, że również

$$\begin{aligned}
\mathrm{NWD}(a,b) &= \mathrm{NWD}(r_0,r_1) = \mathrm{NWD}(r_1,r_2) = \mathrm{NWD}(r_2,r_3) = \\
&= \ldots = \\
&= \mathrm{NWD}(r_{n-3},r_{n-2}) = \mathrm{NWD}(r_{n-2},r_{n-1}) = \\
&= \mathrm{NWD}(r_{n-1},r_n) = r_n.
\end{aligned}$$

Zatem

$$\mathrm{NWD}(a,b) = r_n.$$

Przykład.

$$\begin{aligned}
574 &= 2 \cdot 252 + 70, \\
252 &= 3 \cdot 70 + 42, \\
70 &= 1 \cdot 42 + 28, \\
42 &= 1 \cdot 28 + 14, \\
28 &= 2 \cdot 14.
\end{aligned}$$

Zatem

$$\mathrm{NWD}(574, 252) = 14.$$

Ponadto za pomocą algorytmu Euklidesa możemy przedstawić $\mathrm{NWD}(a,b)$ w postaci kombinacji liniowej a i b:

$$\begin{aligned}
14 &= 42 - 1 \cdot 28 = \\
&= 42 - 1 \cdot (70 - 1 \cdot 42) = \\
&= 2 \cdot 42 - 1 \cdot 70 = \\
&= 2 \cdot (252 - 3 \cdot 70) - 1 \cdot 70 = \\
&= 2 \cdot 252 - 7 \cdot 70 = \\
&= 2 \cdot 252 - 7 \cdot (574 - 2 \cdot 252) = \\
&= 16 \cdot 252 - 7 \cdot 574 = \\
&= (-7) \cdot 574 + 16 \cdot 252.
\end{aligned}$$

Zatem
$$14 = \mathrm{NWD}(574, 252) = (-7) \cdot 574 + 16 \cdot 252.$$

Twierdzenie 24. Niech $a \geq b > 0$. Wtedy przy zachowaniu dotychczasowych oznaczeń mamy:
$$\mathrm{NWD}(a, b) = s_n a + t_n b,$$
gdzie
$$\begin{array}{ll} s_0 = 1, & t_0 = 0, \\ s_1 = 0, & t_1 = 1, \\ s_j = s_{j-2} - q_{j-1} s_{j-1}, & t_j = t_{j-2} - q_{j-1} t_{j-1}. \end{array}$$

LICZBY FIBONACCIEGO

Definicja.
$$f_1 = 1, \quad f_2 = 1, \quad f_{n+2} = f_{n+1} + f_n.$$

Definicja.
$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}.$$

Twierdzenie 25. (Wzór Bineta)
$$f_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

Twierdzenie 26. $f_n > \alpha^{n-2}$ dla $n \geq 3$.

Dowód. Indukcja. Zauważmy najpierw, że α jest pierwiastkiem równania kwadratowego
$$x^2 - x - 1 = 0,$$
a zatem
$$\alpha^2 = \alpha + 1.$$

Teraz:
(1) $n = 3$: $f_3 = 2 > \alpha$;
(2) $n = 4$: $f_4 = 3 > 1 + \alpha = \alpha^2$.
(3) Krok indukcyjny:
$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} > \alpha^{n-2} + \alpha^{n-3} = \\ &= \alpha^{n-2}(\alpha + 1) = \alpha^{n-3} \cdot \alpha^2 = \alpha^{n-1}. \quad \spadesuit \end{aligned}$$

Twierdzenie 27. $\mathrm{NWD}(f_{n+2}, f_{n+1}) = 1$ i algorytm Euklidesa wymaga dokładnie n dzieleń.

Twierdzenie 28. Jeśli $a > b$ i algorytm Euklidesa wymaga n dzieleń do obliczenia $\mathrm{NWD}(a, b)$, to $b \geq f_{n+1}$.

Dowód. Niech $a = r_0$ i $b = r_1$. Mamy wtedy

$$\begin{array}{lcll}
r_0 & = & r_1 q_1 + r_2, & 0 \leq r_2 < r_1, \\
r_1 & = & r_2 q_2 + r_3, & 0 \leq r_3 < r_2, \\
\ldots & & \ldots & \ldots \\
r_{j-2} & = & r_{j-1} q_{j-1} + r_j, & 0 \leq r_j < r_{j-1}, \\
\ldots & & \ldots & \ldots \\
r_{n-4} & = & r_{n-3} q_{n-3} + r_{n-2}, & 0 \leq r_{n-2} < r_{n-3}, \\
r_{n-3} & = & r_{n-2} q_{n-2} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2}, \\
r_{n-2} & = & r_{n-1} q_{n-1} + r_n, & 0 \leq r_n < r_{n-1}, \\
r_{n-1} & = & r_n q_n. &
\end{array}$$

Stąd

$$\begin{array}{lcl}
r_n & \geq & 1 = f_2, \\
r_{n-1} & \geq & 2f_2 = f_3, \\
r_{n-2} & \geq & r_{n-1} + r_n \geq f_3 + f_2 = f_4, \\
\ldots & & \ldots \\
r_1 & \geq & r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}, \quad \spadesuit
\end{array}$$

Twierdzenie 29. (Gabriel Lamé) Niech $a > b$. Wtedy liczba dzieleń w algorytmie Euklidesa nie przekracza $5 \cdot lh_{10}(b)$.

Dowód. Niech $lh_{10}(b) = k$ i załóżmy, że potrzeba n dzieleń. Wtedy

$$b \geq f_{n+1} > \alpha^{n-1}.$$

Stąd

$$\log_{10} b > (n-1) \log_{10} \alpha > \frac{n-1}{5}.$$

Zatem

$$n - 1 < 5 \cdot \log_{10} b < 5k,$$

czyli

$$n \leq 5k. \quad \spadesuit$$

Wniosek. Do obliczenia $\mathrm{NWD}(a, b)$, gdzie $a > b$ algorytm Euklidesa wymaga co najwyżej $O((\log a) \cdot (\log b)^2)$ działań.

Można przeprowadzić dokładniejszą analizę złożoności algorytmu Euklidesa.

Obserwacja: Do wykonania dzielenia z resztą

$$a = bq + r, \quad 0 \leq r < b$$

algorytm „szkolny" wymaga $O(lh(b) \cdot lh(q))$ działań.

Przypomnijmy algorytm Euklidesa:

$$
\begin{array}{lcll}
r_0 & = & r_1q_1 + r_2, & 0 \le r_2 < r_1, \\
r_1 & = & r_2q_2 + r_3, & 0 \le r_3 < r_2, \\
\ldots & & \ldots & \ldots \\
r_{j-2} & = & r_{j-1}q_{j-1} + r_j, & 0 \le r_j < r_{j-1}, \\
\ldots & & \ldots & \ldots \\
r_{n-4} & = & r_{n-3}q_{n-3} + r_{n-2}, & 0 \le r_{n-2} < r_{n-3}, \\
r_{n-3} & = & r_{n-2}q_{n-2} + r_{n-1}, & 0 \le r_{n-1} < r_{n-2}, \\
r_{n-2} & = & r_{n-1}q_{n-1} + r_n, & 0 \le r_n < r_{n-1}, \\
r_{n-1} & = & r_nq_n. &
\end{array}
$$

Dzielenie r_{i-1} przez r_i wymaga $O(lh(r_i) \cdot lh(q_i))$ działań. Zatem łączna liczba działań jest nie większa od (nie uwzględniając stałej):

$$\sum_{i=1}^{n}(lh(r_i) \cdot lh(q_i)).$$

Ale

$$lh(r_i) \le lh(b).$$

Zatem

$$\sum_{i=1}^{n}(lh(r_i) \cdot lh(q_i)) \le lh(b) \cdot \sum_{i=1}^{n} lh(q_i).$$

Następnie

$$lh(q_i) \le 1 + \log_2(q_i),$$

więc

$$\sum_{i=1}^{n} lh(q_i) \le n + \log_2\left(\prod_{i=1}^{n} q_i\right).$$

Łączna liczba działań jest zatem nie większa od

$$lh(b) \cdot \left(n + \log_2\left(\prod_{i=1}^{n} q_i\right)\right).$$

Wykażemy teraz, że

$$\prod_{i=1}^{n} q_i \le a.$$

Mianowicie:

$$
\begin{array}{lcl}
r_0 & \ge & r_1q_1, \\
r_1 & \ge & r_2q_2, \\
r_3 & \ge & r_3q_3, \\
\ldots & & \ldots \\
r_{n-2} & \ge & r_{n-1}q_{n-1}, \\
r_{n-1} & \ge & r_nq_n.
\end{array}
$$

Mnożąc te nierówności stronami otrzymujemy

$$r_0 r_1 r_2 \cdot \ldots \cdot r_{n-1} \geq (r_1 r_2 \cdot \ldots \cdot r_n) \cdot (q_1 q_2 \cdot \ldots \cdot q_n).$$

Po skróceniu otrzymamy

$$a = r_0 \geq r_n \cdot (q_1 q_2 \cdot \ldots \cdot q_n),$$

a więc rzeczywiście.

$$a \geq \prod_{i=1}^{n} q_i.$$

Stąd wynika, że

$$n + \log_2 \left(\prod_{i=1}^{n} q_i \right) = O(n + \log_2 a) = O(n + lh(a)).$$

Z twierdzenia Lamé wynika, że $n = O(lh(b))$. Zatem złożoność algorytmu Euklidesa nie przekracza

$$O(lh(b) \cdot (lh(b) + lh(a))),$$

czyli

$$O(lh(a) \cdot lh(b)).$$

BINARNY ALGORYTM EUKLIDESA

Zauważmy, że

(1) $2 \mid a \wedge 2 \mid b \;\Rightarrow\; \mathrm{NWD}(a,b) = 2 \cdot \mathrm{NWD}(a \,\mathbf{div}\, 2, b \,\mathbf{div}\, 2)$;
(2) $2 \mid a \wedge 2 \not| \, b \;\Rightarrow\; \mathrm{NWD}(a,b) = \mathrm{NWD}(a \,\mathbf{div}\, 2, b)$;
(3) $2 \not| \, a \wedge 2 \mid b \;\Rightarrow\; \mathrm{NWD}(a,b) = \mathrm{NWD}(a, b \,\mathbf{div}\, 2)$;
(4) $2 \not| \, a \wedge 2 \not| \, b \wedge a > b \;\Rightarrow\; \mathrm{NWD}(a,b) = \mathrm{NWD}(a-b, b)$.

To daje prosty algorytm:

Wejście: $a, b \in \mathbb{Z}$;

Wyjście: $d = \mathrm{NWD}(a,b)$;

$d := 1$;
while $even(a)$ **and** $even(b)$ **do begin**
  $a := a \,\mathbf{div}\, 2$;
  $b := b \,\mathbf{div}\, 2$;
  $d := 2d$
end;
while $even(a)$ **do** $a := a \,\mathbf{div}\, 2$;

while $even(b)$ **do** $b := b\,\textbf{div}\,2$;
if $a < b$ **then** $Zamien(a, b)$;
$a := a - b$;
while $a \neq 0$ **do begin**
  repeat $a := a\,\textbf{div}\,2$ **until** $odd(a)$;
  if $a < b$ **then** $Zamien(a, b)$;
  $a := a - b$
end;
return bd;

RÓWNANIA DIOFANTYCZNE

Rozważamy równania postaci
$$ax + by = c$$
z niewiadomymi x i y, gdzie a, b i c są liczbami całkowitymi. Szukamy rozwiązań w liczbach całkowitych.

Twierdzenie 30. Niech $a, b, c \in \mathbb{Z}$. Równanie
$$ax + by = c$$
ma rozwiązanie całkowite wtedy i tylko wtedy, gdy
$$\mathrm{NWD}(a, b) \mid c.$$

Dowód. Niech $d = \mathrm{NWD}(a, b)$. Jeśli równanie
$$ax + by = c$$
ma rozwiązanie, to
$$d \mid a \quad \text{i} \quad d \mid b,$$
skąd wynika, że $d \mid c$.

Na odwrót, jeśli $d \mid c$, to bierzemy liczbę k taką, że $c = dk$ oraz liczby p i q takie, że
$$d = ap + bq.$$
Teraz kładziemy
$$x = pk \quad \text{oraz} \quad y = qk$$
i zauważamy, że
$$ax + by = apk + bqk = dk = c. \quad \spadesuit$$

Twierdzenie 31. Załóżmy, że para liczb całkowitych (x_0, y_0) jest rozwiązaniem równania

$$ax + by = c.$$

Niech następnie $\mathrm{NWD}(a, b) = d$ oraz $a = a_1 d$ i $b = b_1 d$. Wtedy to równanie ma nieskończenie wiele rozwiązań danych wzorami

$$x = x_0 + b_1 n, \quad y = y_0 - a_1 n,$$

gdzie n jest dowolną liczbą całkowitą.

Dowód. Oczywiście

$$ab_1 = a_1 b_1 d = ba_1,$$

skąd otrzymujemy

$$ax + by = ax_0 + ab_1 n + by_0 - a_1 bn = ax_0 + by_0 = c.$$

Zatem para liczb (x, y) jest rozwiązaniem równania.
Na odwrót, przypuśćmy, że para liczb (x, y) jest rozwiązaniem równania:

$$ax + by = c.$$

Wiemy, że

$$ax_0 + by_0 = c.$$

Odejmijmy te równania stronami:

$$a(x - x_0) + b(y - y_0) = 0.$$

Po podzieleniu przez d otrzymujemy

$$a_1(x - x_0) = b_1(y_0 - y).$$

Ponieważ $b_1 \mid a_1(x - x_0)$ oraz $\mathrm{NWD}(a_1, b_1) = 1$, więc $b_1 \mid x - x_0$, skąd otrzymujemy

$$x = x_0 + b_1 n \ \text{ oraz } \ y = y_0 - a_1 n. \quad \spadesuit$$

PROBLEM FROBENIUSA

Twierdzenie 32. Dane są liczby całkowite dodatnie a i b. Zakładamy, że $\mathrm{NWD}(a, b) = 1$. Wtedy dla każdej liczby $c \geq (a - 1)(b - 1)$ istnieją liczby całkowite nieujemne x i y takie, że

$$ax + by = c.$$

Dowód. Indukcja względem c. Najpierw znajdujemy najmniejsze liczby całkowite nieujemne k i l takie, że

$$ak = bl + 1.$$

Można łatwo zauważyć, że wtedy

$$0 < k \leq b - 1 \quad \text{oraz} \quad 0 < l \leq a - 1.$$

Teraz:

$$a(k-1) + b(a-l-1) = \ldots = (a-1)(b-1).$$

Załóżmy następnie, że $c \geq (a-1)(b-1)$ oraz istnieją liczby nieujemne x i y takie, że

$$ax + by = c.$$

Możliwe są trzy przypadki.

(1) $y \geq l$. Wtedy

$$a(x+k) + b(y-l) = \ldots = c + 1.$$

(2) $x \geq b - k$. Wtedy

$$a(x-b+k) + b(y+a-l) = \ldots = c + 1.$$

(3) $y \leq l - 1$ oraz $x \leq b - k - 1$. Wtedy

$$c = ax + by \leq \ldots \leq ab - a - b - 1 < (a-1)(b-1),$$

sprzeczność. ♠