AE (Algorytm Euklidesa)

1. Dane są $a, b \in \mathbb{N}$; chcemy znaleźć NWD tych liczb (oznaczane jako $(a,b) := \mathrm{NWD}(a,b)$). Po grosie matematyki z podstawówki rozkładalibyśmy w tym celu a i b na czynniki pierwsze. Tymczasem już Euklides w „Elementach" (księga VII, stw. 2) podał lepszy przepis.

Załóżmy, że np. $b \le a$. Dzielimy a przez b z resztą r

$$a = qb + r, \quad 0 \le r < b.$$

Wobec $r = a - qb$ widać, że każdy wspólny dzielnik a i b jest też wspólnym dzielnikiem b, r; odwrotnie, każdy wspólny dzielnik b, r wobec $a = qb + r$ jest też wspólnym dzielnikiem a i b. Zatem

$$\{\text{dzielniki } a,b\} = \{\text{dzielniki } b,r\}$$

skąd

$$(a,b) = (b,r)$$

największa liczba z tego zbioru

największa liczba z tego zbioru

Schodzimy w dół odgrywając ten dowcip, tzn. dzielimy

$$b = q'r + r'$$

i mamy $(a,b) = (b,r) = (r,r') = \dots$. Ponieważ

$$b > r > r' > \dots \ge 0$$ (ściśle malejący ciąg liczb naturalnych)

musi być $r^{(n)} = 0$ w pewnym kroku, a więc

$$(a,b) = \dots = (r^{(n-1)}, r^{(n)}) = (r^{(n-1)}, 0) = r^{(n-1)}$$

ostatnia niezerowa reszta

Ogólniając notację $a = n_0$, $b = n_1$, $r = n_2$, $r' = n_3$, ... możemy to sobie zapisać w słupku

$$\begin{aligned}
n_0 &= q_1 n_1 + n_2 && , \ 0 \le n_2 < n_1 \\
n_1 &= q_2 n_2 + n_3 && , \ n_3 < n_2 \\
&\vdots && \vdots \\
n_{k-1} &= q_k n_k + n_{k+1} && , \ n_{k+1} < n_k \\
n_k &= q_{k+1} n_{k+1} + 0 = n_{k+2} && , \ 0 < n_{k+1}
\end{aligned}$$

$$(n_0, n_1) = (n_1, n_2) = \dots = (n_k, n_{k+1}) = (n_{k+1}, 0) = n_{k+1}$$

PRZYK. 1) $(45, 12) = 3$, bo

$45 = 3 \cdot 12 + 9$
$12 = 1 \cdot 9 + \underline{3}$ ← ost $\neq 0$ reszta
$9 = 3 \cdot 3$

2) $(34, 21) = 1$, bo

$34 = 1 \cdot 21 + 13$
$21 = 1 \cdot 13 + 8$
$13 = 1 \cdot 8 + 5$
$8 = 1 \cdot 5 + 3$
$5 = 1 \cdot 3 + 2$
$3 = 1 \cdot 2 + \underline{1}$
$2 = 2 \cdot 1$

3) $a = 25957 \; (= 257 \cdot 101)$
$b = 6667 \; (= 113 \cdot 59)$

2. Jak szybko działa AE? Tzn. ile trzeba wykonać dzieleń?

Jest jasne, że dzielić nie nam będzie najdłużej, gdy otrzymie $1 = q_{r_1} = q_{r_2} = \dots$ (jak w przyk. 2)), czyli najdłużej, gdy obliczamy NWD dwu kolejnych liczb Fibonacciego. Jednak i tak koszt działania algorytmu jest tylko logarytmiczny (liniowy względem rozmiaru danych).

TW. Do obliczenia NWD n_0 i n_1 $(n_0 \geq n_1)$ za pomocą AE potrzeba co najwyżej $5 \cdot$(liczba cyfr n_1) dzieleń.

D-D. Niech $(f_n)_{n=0,1,\dots}$ oznacza ciąg Fibonacciego ($f_0 = 0$, $f_1 = 1$, $f_n = f_{n-1} + f_{n-2}$, $n \geq 2$). Załóżmy, że wykonaliśmy $k+1$ dzieleń, tzn. AE przebiegał tak

$n_0 = q_1 n_1 + n_2$
$n_1 = q_2 n_2 + n_3$
$\vdots$
$n_{k-1} = q_k n_k + n_{k+1}$
$n_k = q_{k+1} n_{k+1}$ STOP.

Mamy stąd

$n_k \geq 2 \underbrace{n_{k+1}}_{\geq 1} \geq f_3$ ($q_{k+1} \geq 2$, bo $n_{k+1} < n_k$)
$n_{k-1} \geq n_k + n_{k+1} \geq f_3 + f_2 = f_4$
$n_{k-2} \geq n_{k-1} + n_k \geq f_4 + f_3 = f_5$
$\vdots$
$n_1 \geq f_{k+2}$.

Skorzystamy z następującej uwagi

0 1 1 2 3 5 8 13 21

⚠ $f_{n+5} > 10 f_n$, $n \geq 2$

D-D. Indukcja po n. OK dla $n=2,3$. Dalej

$$f_{n+1+5} = f_{n+5} + f_{n-1+5} > 10(f_n + f_{n-1}) = 10 f_{n+1}. \quad \square$$

Dzielimy $k+1$ z renta przez 5, tzn. $k+1 = 5l + r$, $0 \leq r < 5$. Mamy

$$n_1 \geq f_{k+2} = f_{5l+r+1} \overset{\text{tz}}{>} 10^l f_{r+1} \geq 10^l f_1 = 10^l$$

zatem n_1 ma co najmniej $l+1$ cyfr. Wobec tego

liczba dzieleń $= k+1 = 5l + r < 5(l+1) \leq 5 \cdot$ (liczba cyfr n_1). $\square$

3. AE ma ciekawe zastosowania.

1° Ułamki łańcuchowe.

PRZYK. 1) $\frac{8}{13} = \frac{1}{13/8} = \frac{1}{1 + \frac{5}{8}} = \frac{1}{1 + \frac{1}{8/5}} = \frac{1}{1 + \frac{1}{1 + \frac{1}{5/3}}}$

$$= \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}},$$

2) $3{,}1415 = \frac{31415}{10000} = 3 + \frac{1}{\frac{10000}{1415}} = \ldots = 3 + \frac{1}{7 + \frac{1}{14 + \frac{1}{1 + \frac{1}{8 + \frac{1}{2}}}}}$

Ogólnie

$$\begin{aligned} n_0 &= q_1 n_1 + n_2 \\ n_1 &= q_2 n_2 + n_3 \\ n_2 &= q_3 n_3 + n_4 \\ &\vdots \\ n_{k-1} &= q_k n_k + n_{k+1} \\ n_k &= q_{k+1} n_{k+1} \end{aligned}$$

$$\begin{aligned} \frac{n_0}{n_1} &= q_1 + \frac{n_2}{n_1} = q_1 + \frac{1}{n_1/n_2} \\ \frac{n_1}{n_2} &= q_2 + \frac{n_3}{n_2} \\ \frac{n_2}{n_3} &= q_3 + \frac{n_4}{n_3} \end{aligned}$$

$$= q_1 + \frac{1}{q_2 + \frac{1}{n_2/n_3}}$$

$$= q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{n_3/n_4}}}$$

$$\vdots$$

$$\frac{n_0}{n_1} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ldots + \frac{1}{q_k + \frac{1}{q_{k+1}}}}}.$$

2° Forma liniowa dla NWD

AE daje konstruktywny dowód następującego, b. ważnego

TW. $\exists x,y \in \mathbb{Z} \quad (a,b) = ax + by$.

D-D. Oznaczamy jak wyżej $a = n_0$, $b = n_1$ i $n_0 \geq n_1$ i jedziemy z AE

$$
\begin{aligned}
n_0 &= q_1 n_1 + n_2 && \rightsquigarrow && n_2 &= n_0 - q_1 n_1 \\
n_1 &= q_2 n_2 + n_3 && \rightsquigarrow && n_3 &= n_1 - q_2 n_2 \\
&\vdots && && &\vdots \\
n_{k-2} &= q_{k-1} n_{k-1} + n_k && \rightsquigarrow && n_k &= n_{k-2} - q_{k-1} n_{k-1} \\
n_{k-1} &= q_k n_k + n_{k+1} && \rightsquigarrow && n_{k+1} &= n_{k-1} - q_k n_k \\
n_k &= q_{k+1} n_{k+1} && && &
\end{aligned}
$$

i idziemy tym razem w górę

$$
\begin{aligned}
(a,b) = n_{k+1} &= n_{k-1} - q_k n_k = n_{k-1} - q_k (n_{k-2} - q_{k-1} n_{k-1}) \\
&= (1 + q_k q_{k-1}) n_{k-1} - q_k n_{k-2} \\
&= \ldots = x n_0 + y n_1 \quad , \quad x,y \in \mathbb{Z}
\end{aligned}
$$

wyrażają się jakoś parami przez $q_1, \ldots, q_k$. □

PRZYK. 1) $a = 93 \quad b = 57$

a	b	r	q	x	y
93	57	36	1	8	$-5 - 8 \cdot 1 = -13$
57	36	21	1	-5	$3 - (-5) \cdot 1 = 8$
36	21	15	1	3	$-2 - 3 \cdot 1 = -5$
21	15	6	1	-2	$1 - (-2) \cdot 1 = 3$
15	6	3	2	1	-2
6	3	0	2		

$\cdot(-1)$

← inicjalizacja

i rezultacie $3 = 93 \cdot 8 + 57 \cdot (-13)$.

2) Jako wniosek wyprowadzimy zasadnicze tw. arytmetyki

Jeśli $a \mid bc$, $a \perp b$ (względnie pierwsze) $\Rightarrow a \mid c$.

D-D. $1 = (a,b) = ax + by \quad /\cdot c \quad \Rightarrow \quad c = acx + \underbrace{bc}_{a \mid}y \quad \Rightarrow \quad a \mid c$. □

ZAD* Udowodnić, że $(f_n, f_m) = f_{(n,m)}$ ($(f_n)_{n=0,1,\ldots}$ oznacza ciąg Fibonacciego)