Alg. Euklidesa $NHD(m,n)$

$m \geq n > 0$

while $n \neq 0$

$m, n = n, m \bmod n$

IN: m, n

OUT: $d = NHD(m,n)$

$d = m$

$d' = n$

while $d' \neq 0$

$d, d' = d', d \bmod d'$ ←

$m = 135, n = 40$

135
40
15
10
5 ← NHD
0

[while $d' \neq 0$ do { $d = d'$; $d' = d \bmod d'$ (S) }] $(d, d') \rightsquigarrow (k, k')$

$d' > 0$

$d' \in \{0, 1, \dots, d-1\}$

$(d, d') \rightsquigarrow (k, k')$

$k' = d \bmod d' < d'$

$d = q d' + k' \geq d' + k' > 2k'$ $\quad \{ \; d \geqslant d'$

$k' < \frac{d}{2}$

$k \cdot k' = d' \cdot k' < \frac{d \cdot d'}{2}$

$k \cdot k' < \frac{d \cdot d'}{2}$

$(m, n) \overset{S}{\rightsquigarrow} (\, , \,) \overset{S}{\rightsquigarrow} (\, , \,) \overset{S}{\rightsquigarrow} (\, , \,) \overset{S}{\rightsquigarrow} \dots \overset{S}{\rightsquigarrow} (\, , d) \overset{S}{\rightsquigarrow} (d, 0)$

$\bullet < \frac{mn}{2}$ $\quad \bullet < \frac{1}{2} \cdot \frac{mn}{2}$

i kroków ↖ liczba obrotów pętli

$\square \cdot d < \frac{mn}{2^{i-1}}$

$\square \neq 0$

$1 \leqslant d < \frac{mn}{2^{i-1}}$

$\frac{mn}{2^{i-1}} > 1$

$2^{i-1} < mn \quad | \log_2()$

$i - 1 < \log_2(mn)$

$i < \log_2 m + \log_2 n + 1.$

$m \sim 2^{1000}$ $n \sim 2^{1000}$

$\log_2 m + \log_2 n + 1 = 2001$

Th. Liczba obrotów w alg. Euklidesa nie przekracza $\log_2 m + \log_2 n + 1$. $\{m \geq n > 0\}$

---

d	q
135	
40	3
15	2
10	1
5	2
0	

$15 = 135 - 3 \cdot 40$

$10 = 40 - 2 \cdot 15$

$5 = 15 - 1 \cdot 10$ ←

NWD(135, 40) = $\boxed{5} = 15 - 1 \cdot 10 = 15 - 1 \cdot (40 - 2 \cdot 15) =$

$= -1 \cdot 40 + 3 \cdot 15 = -1 \cdot 40 + 3 \cdot (135 - 3 \cdot 40) =$

$= 3 \cdot \boxed{135} - 10 \cdot \boxed{40}$

Lemat Bezout'a. Dla dowolnych $m, n \in \mathbb{N}_0$, $m \neq 0$ lub $n \neq 0$, istnieją liczby całkowite s i t, dla których

$$NWD(m,n) = s \cdot m + t \cdot n.$$

---

while $d' \neq 0$
  $d = d'$
  $d' = d \bmod d'$

$$d = s \cdot m + t \cdot n$$

	d	q
$m = d_0$		
$n = d_1$		q_1
	d_2	q_2
	$\vdots$	$\vdots$
	d_N	q_N

$$d_i = s_i m + t_i n$$
$$d_{i+1} = s_{i+1} m + t_{i+1} n$$

$\Downarrow$

$$d_{i+2} = d_i \bmod d_{i+1} = d_i - q_{i+1} d_{i+1} =$$
$$= s_i m + t_i n - q_{i+1}(s_{i+1} m + t_{i+1} n)$$
$$= \underbrace{(s_i - q_{i+1} s_{i+1})}_{s_{i+2}} m + \underbrace{(t_i - q_{i+1} t_{i+1})}_{t_{i+2}} n$$

$$s_{i+2} = s_i - q_{i+1} s_{i+1}$$
$$t_{i+2} = t_i - q_{i+1} t_{i+1}$$

$\rightsquigarrow$

$$s = s'$$
$$s' = s - q s'$$
$$t = t'$$
$$t' = t - q \cdot t'$$

$d, d' = m, n$

$s = 1$ $\quad s' = 0$

$t = 0$ $\quad t' = 1$

$$\begin{cases} d = m = 1 \cdot m + 0 \cdot n \\ d' = n = 0 \cdot m + 1 \cdot n \end{cases}$$

NIEZMIENNIK

$d = sm + tn$

$d' = s'm + t'n$

while $d' \neq 0$

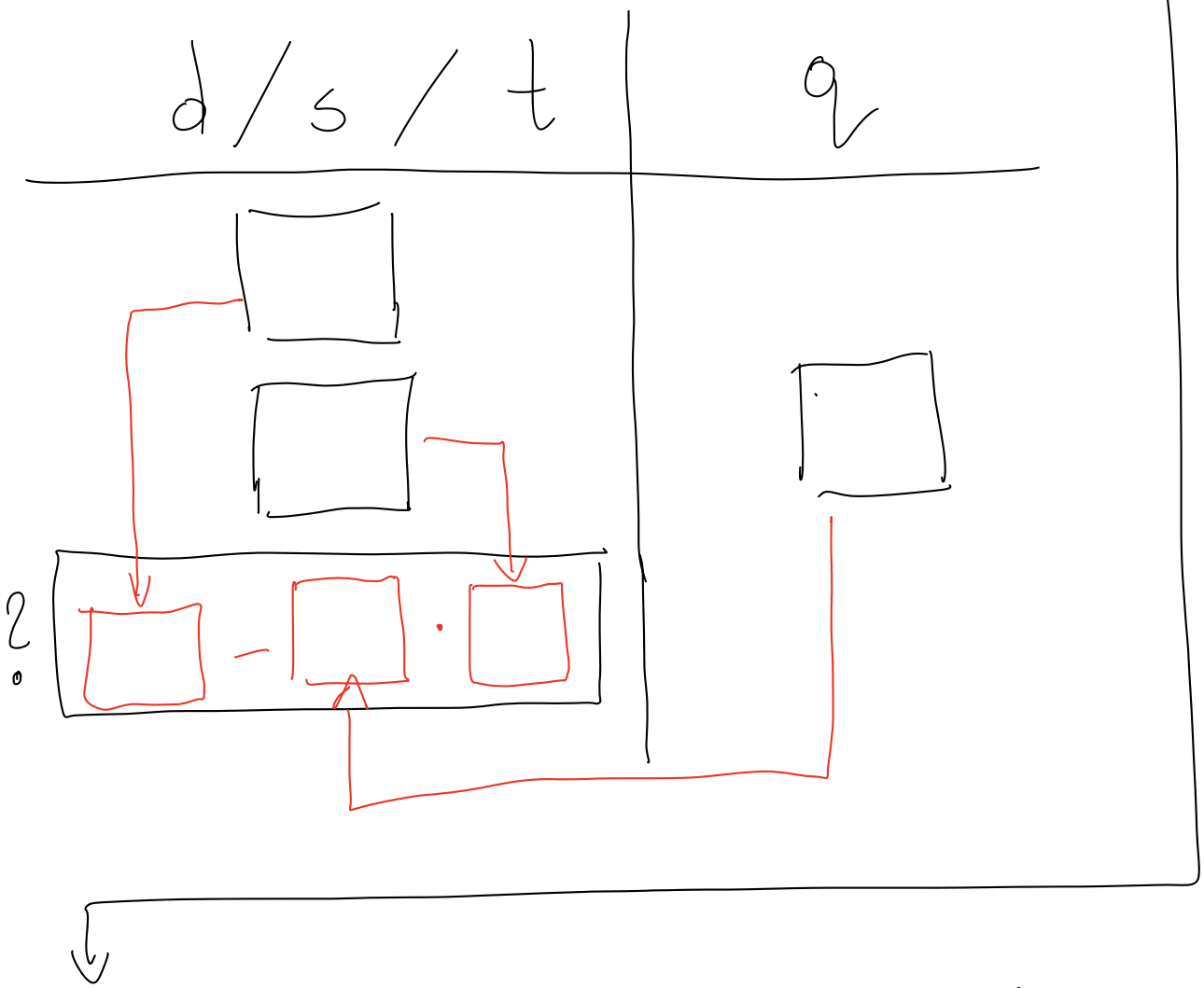
$q = d / d'$

$$\begin{cases} d = d' \\ d' = d - q \cdot d' \end{cases} \quad \{ = d \bmod d'$$

$$\begin{cases} s = s' \\ s' = s - q s' \end{cases}$$

$$\begin{cases} t = t' \\ t' = t - q t' \end{cases}$$

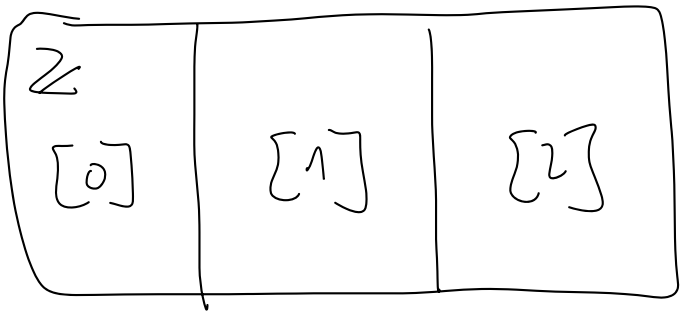
d	q	s	t
135		1	0
40	3	0	1
15	2	1	−3
10	1	−2	7
5	2	3	−10
0			



$$5 = 3 \cdot 135 + (-10) \cdot 40$$

$X = \mathbb{Z}$, $x R y \iff n \mid x - y$

$n = 3$



Klasy kongruencji

Relacja przystawania modulo n

$$x \equiv y \pmod{n} \iff n \mid x - y$$

$$13 \equiv 8 \pmod{5}$$
$$13 \equiv -2 \pmod{5}$$

Tw. Jeżeli $a, b, c, d \in \mathbb{Z}$ i $n \in \mathbb{N}$ oraz
$a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$,
to
$$a + c \equiv b + d \pmod{n},$$
$$a \cdot c \equiv b \cdot d \pmod{n}.$$

Dow. (ćw.)