$$NWD(m, n) = NWD(n, m \bmod n) \quad (*)$$

$m \bmod n \in 0, 1, \ldots, n-1$

IN: $m \in \mathbb{Z}$, $n \in \mathbb{N}$

OUT: $NWD(m, n)$

```
d <- m
d' <- n
while d' ≠ 0:
    d, d' <- d', d mod d'
return d
```

$d'_{nowe} \leq d' - 1$

NIEZMIENNIK

$NWD(m, n) = NWD(d, d')$

1) program się kończy, bo $\Rightarrow d'_{nowe} < d'$

2) $(*) \Rightarrow$ NIEZMIENNIK

3) $NWD(m, n) = NWD(d, d')$

$\Rightarrow NWD(m, n) = NWD(d, d') \wedge d' = 0$

$NWD(m, n) = NWD(d, 0) = d$

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

$NWD(m, n) \sim \sqrt{2^{1000}} \approx 2^{500}$

ILE JEST OBROTÓW PĘTLI

$$(d, d') \rightsquigarrow (d_{nowe}, d'_{nowe})$$

$$\begin{cases} d_{nowe} = d' \\ d'_{nowe} = d \bmod d' \end{cases}$$

$$d \geq d'$$

$$(m, n) = (d_0, d_0') \rightsquigarrow (d_1, d_1') \rightsquigarrow (d_2, d_2') \rightsquigarrow \ldots \rightsquigarrow (d_i, d_i') \rightsquigarrow (d_{i+1}, 0)$$

$\underline{d \geq d'} \Rightarrow q \geq 1$ $\qquad d \bmod d' = d'_{nowe}$

$$\underline{d = q d' + r} \geq d' + r \geq \qquad 0 \leq r \leq d' - 1$$

$$\geq d_{nowe} + d'_{nowe} \geq 2 d'_{nowe}$$

$$\boxed{d \cdot d'} \geq 2 d'_{nowe} d' = 2 \boxed{d'_{nowe} d_{nowe}}$$

$$(d_j, d_j') \rightsquigarrow (d_{j+1}, d'_{j+1})$$

$$d_j d_j' \geq 2 d_{j+1} d'_{j+1}$$

$$\boxed{(d_{i+1}, 0)}$$

$$(m,n) = (d_0, d_0') \rightsquigarrow (d_1, d_1') \rightsquigarrow (d_2, d_2') \rightsquigarrow \dots \rightsquigarrow \boxed{(d_i, d_i')}$$

$$mn = d_0 d_0' \geqslant 2 d_1 d_1' \geqslant 4 d_2 d_2' \geqslant 8 d_3 d_3' \geqslant \dots \geqslant$$

$$\geqslant 2^i \underbrace{d_i d_i'}_{>0} \geqslant 2^i$$

$$mn \geqslant 2^i \quad | \log_2()$$

$$\log_2(mn) \geqslant i$$

$$\boxed{i \leq \log_2 m + \log_2 n}$$

$m \in \mathbb{Z}, \ n \in \mathbb{N}$

LICCBA KROKδU $\leq \underline{\log_2 |m| + \log_2 n} + 2$

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

Liczba kroków $\leq 1000 + 1000 + 2 = 2002$

$$\begin{array}{r|l} 660 & \\ 525 & \\ 135 & \leftarrow 135 = 660 - 1\cdot 525 \\ 120 & \leftarrow 120 = 525 - 3\cdot 135 \\ \boxed{15} & \leftarrow 15 = 135 - 1\cdot 120 \\ 0 & \end{array}$$

$$\boxed{NWD(660,525)} = 15 = 135 - 1\cdot 120 = 135 - 1\cdot(525 - 3\cdot 135) =$$

$$= -1\cdot 525 + 4\cdot 135 = -1\cdot 525 + 4(660 - 1\cdot 525) =$$

$$= \boxed{4}\cdot 660 + \boxed{-5}\cdot 525$$

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

d_0
d_1
d_2
$\vdots$
d_i

Rozszerzony algorytm Euklidesa

$d, d' \leftarrow m, n$

while $d' \neq 0$
  $d, d' \leftarrow d', d \bmod d'$

$$NWD(m,n) = d_{i+1} = \underset{?}{s}\cdot m + \underset{?}{t}\cdot n$$

$$\left[\begin{array}{l} d_k = s_k m + t_k n \\ d_{k+1} = s_{k+1} m + t_{k+1} n \end{array}\right. \quad (2)$$

$$d_k = q_{k+1} d_{k+1} + \boxed{r_k}, \quad q_{k+1} = d_k \operatorname{div} d_{k+1}$$

$$d_{k+2} = \overline{d_k \bmod d_{k+1}} =$$

$$= d_k - \underbrace{(d_k \operatorname{div} d_{k+1})}_{q_{k+1}} \cdot d_{k+1} =$$

$$= d_k - q_{k+1} d_{k+1} =$$

$$= s_k m + t_k n - q_{k+1}(s_{k+1} m + t_{k+1} n)$$

$$= \underbrace{(s_k - q_{k+1} s_{k+1})}_{s_{k+2}} m + \underbrace{(t_k - q_{k+1} t_{k+1})}_{t_{k+2}} n$$

(2)

$$\begin{bmatrix} d_k = s_k m + t_k n \\ d_{k+1} = s_{k+1} m + t_{k+1} n \end{bmatrix}$$

$$d_k = q_{k+1} d_{k+1} + r_k$$

$$d_{k+2} = s_{k+2} m + t_{k+2} n$$

$$s_{k+2} = \underbrace{s_k - q_{k+1} s_{k+1}} \qquad \underbrace{t_k - q_{k+1} t_{k+1}} = t_{k+2}$$

$$\underbrace{d_{k+2} = d_k - q_{k+1} d_{k+1}}$$

$$\left\{ d = m = 1 \cdot m + 0 \cdot n \quad d' = n = 0 \cdot m + 1 \cdot n \right.$$

$d, d' \leftarrow m, n$

$s, s' \leftarrow 1, 0$

$t, t' \leftarrow 0, 1$

$d = sm + tn \qquad d' = s'm + t'n$

while $d' \neq 0$

~~$d, d' \leftarrow d', d \bmod d'$~~

$q \leftarrow d \text{ div } d'$

$d, d' \leftarrow d', \underline{d - q \cdot d'}$

$s, s' \leftarrow s', s - q \cdot s'$

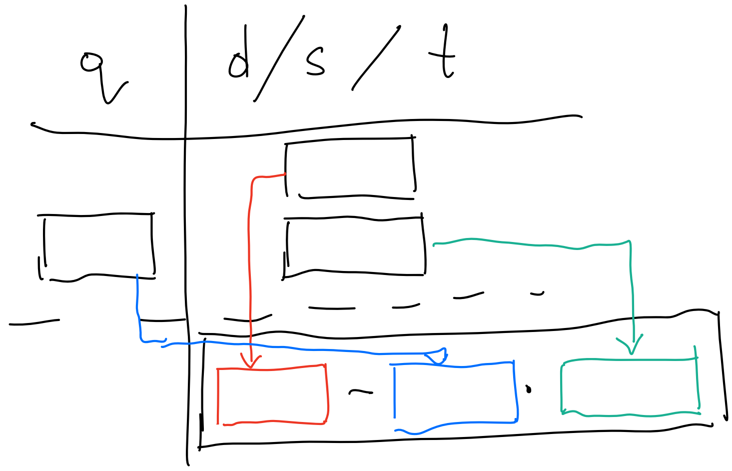
$t, t' \leftarrow t', t - q \cdot t'$

$\square, \square' \leftarrow \square', \square - q \cdot \square'$

$d, s, t \quad d', s', t' \quad d', s', t' \quad d, s, t \quad d', s', t'$

$d = sm + tn$

d	q	s	t
660		1	0
525	1	0	1
135	3	1	−1
120	1	−3	4
15	8	4	−5
0			



$$15 = 4 \cdot 660 - 5 \cdot 525$$

$$\boxed{\mathrm{NUD}(137, 92) = s \cdot 137 + t \cdot 92}$$

d	q	s	t
137		1	0
92	1	0	1
45	2	1	−1
2	22	−2	3
1	2	$\boxed{45}$	$\boxed{-67}$
0			

$$\mathrm{NUD}(137, 92) = 1 = \boxed{45 \cdot 137 - 67 \; 92}$$

Relacja przystawania (kongruencji)

$n \in \mathbb{N}$, $\quad X = \mathbb{Z}$

$a, b \in \mathbb{Z}$ $\quad a \sim b \iff n \mid a - b$

$\mathbb{Z}$

$[0]$	$[1]$	$[2]$	$[3]$

$a \sim b \rightsquigarrow \boxed{a \equiv b \pmod{n}}$ $\quad \boxed{a \equiv_n b}$

$10 \equiv 3 \pmod{7}$

$24 \equiv 3 \pmod{7}$

$-4 \equiv 10 \equiv 3 \pmod{7}$

$(a+b) \bmod n = \big((a \bmod n) + (b \bmod n)\big) \bmod n$

$(ab) \bmod n = \big((a \bmod n)(b \bmod n)\big) \bmod n$

Fakt.
$\begin{cases} a \equiv b \pmod{n}, \\ c \equiv d \pmod{n} \end{cases}$

$\boxed{a \equiv b \pmod{n}}$

$\Rightarrow \quad a + c \equiv b + d \pmod{n}$

$\Rightarrow \quad a \cdot c \equiv b \cdot d \pmod{n}$

$\Rightarrow \quad a^k \equiv b^k \pmod{n}$

Zad. Wyznacz resztę z dzielenia

$$7^{2025}$$

przez 15.

$7^1 \equiv 7 \pmod{15} \quad | \cdot 7$

$7^2 \equiv 49 \equiv 4 \pmod{15} \quad | \cdot 7$

$7^3 \equiv 4 \cdot 7 \equiv 28 \equiv 13 \pmod{15} \quad | \cdot 7$

$\underline{7^4} \equiv 13 \cdot 7 \equiv 91 \equiv \underline{1} \pmod{15} \quad | \, ()^k$

$$7^{4k} \equiv 1 \pmod{15}, \quad k \in \mathbb{N}$$

$$7^{2025} = 7^{2024+1} = 7^{2024} \cdot 7 = \underbrace{7^{4 \cdot \overset{506}{k}}}_{\equiv 1} \cdot 7 \equiv 1 \cdot 7 \equiv$$

$$\equiv 7 \pmod{15}$$