2) Jedyność pary q, r

$$m = qn + r, \quad q, r \in \mathbb{Z}, \quad 0 \le r < n$$

Załóżmy, że (q, r), (q', r')

$$m = \underbrace{qn + r} = \underbrace{q'n + r'} \qquad 0 \le r, r' < n$$

$$qn - q'n = r' - r$$

$$n(q - q') = r' - r$$

I $q = q'$: $n \cdot 0 = r' - r$

$$0 = r' - r \Rightarrow r = r'$$

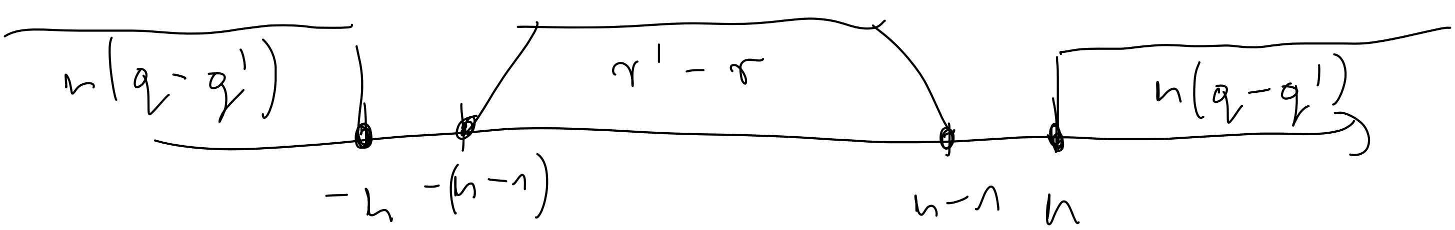
II $q \neq q' \Rightarrow q - q' \neq 0 \wedge q - q' \in \mathbb{Z}$

$$n \cdot \underbrace{|q - q'|}_{\ge 1} \ge n$$

$$0 \le r, r' \le n-1$$

$$\underline{-(n-1) \le r' - r \le n-1}$$

$$\underbrace{n(q - q')}_{|\cdot| \ge n} = \underbrace{r' - r}_{-(n-1) \le \cdot \le n-1}$$



sprzeczność.

$m = qn + r$

iloraz → q, reszta → r

$q \overset{ozn}{=} m \text{ div } n = m \,//\, n$

$r \overset{ozn}{=} m \bmod n = m \,\%\, n$

$-7 \% 4 = 1$

$-7 = (-2) \cdot 4 + 1$

$-7 \% 4 = -3$

$-7 = (-1) \cdot 4 - 3$

$17 \% 5$

12

7

2

IN: $m \in \mathbb{N}_0$, $n \in \mathbb{N}$

OUT: $q, r \in \mathbb{Z}$, $0 \le r < n$

$q \leftarrow 0$
$r \leftarrow m$
while $r \ge n$
S: $q \leftarrow q + 1$
$r \leftarrow r - n$
return q, r

NIEZMIENNIK

$m = qn + r \ \wedge \ r \ge 0$

1) Czy się zatrzymuje? TAK

$r_{nowe} = r - n < r$

$r < n$ po skończonej liczbie obrotów

2) P: $m = qn + r \wedge r \geq 0$

(2) $\boxed{m = qn + r \wedge r \geq 0} \wedge r \geq n$

(T) $m = q_{nowe} n + r_{nowe} \wedge \underset{\sim\sim\sim}{r_{nowe} \geq 0}$

$q_{nowe} = q + 1$

$r_{nowe} = r - n$

$q_{nowe} n + r_{nowe} = (q+1)n + r - n =$ (2)

$= qn + \cancel{n} + r - \cancel{n} = qn + r = m$

$r_{nowe} = r - n \geq 0.$

P jest niezmiennikiem pętli

3) $\boxed{m = qn + r \wedge r \geq 0}$ P jest prawdziwe przed wejściem w pętlę.

$q = 0$

$r = m$

$m = 0 \cdot n + m \wedge m \geq 0$

Tw. o niezmiennikach:

Po zakończeniu P jest prawdziwe oraz $\neg(r \geq n)$

$P \wedge \neg(r \geq n) \iff \underline{m = qn + r \wedge r \geq 0 \wedge r < n}.$

WOLNE, gdy n małe, a m duże.

$1893 \% 4$ //

Inne metody
1) „Dzielenie pisemne"
2) „Metoda Newtona-Raphsona ←

↳ n^{-1} ←

$NWD(m,n)$, $m,n \in \mathbb{Z}$, $m \neq 0 \lor n \neq 0$

$NWD(0,0)$ = nie istnieje

1) $\bigwedge_{m,n \in \mathbb{Z}} 1 | m \land 1 | n$

Liczby m i n mają przynajmniej jeden wspólny dzielnik.

2) Ponieważ $m \neq 0$ lub $n \neq 0$, to wspólnych dzielników jest skończenie wiele.

3) Istnieje zatem największy dzielnik m i n.

→ $NWD(m,n)$

$\gcd(m,n)$

(m,n)

$m = 660 \qquad n = 525$

$$\begin{array}{r|l} 660 & 2 \\ 330 & 2 \\ 165 & 3 \\ 55 & 5 \\ 11 & 11 \\ 1 & \end{array} \qquad \begin{array}{r|l} 525 & 3 \\ 175 & 5 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

$NWD(660, 525) = 3 \cdot 5 = 15$

$17017 \qquad 6783$

$$\boxed{NWD(m, n)} \overset{?}{=} NWD(m', n') = \ldots = NWD(d, 0) = d$$

$$NWD(m, 1) = 1$$

$$\boxed{NWD(m, 0) = m}, \qquad m \geq 1$$

$\%, \quad //$

$NWD(m, n) = NWD(m', n') \qquad m', n'$?

1) $d \mid m \wedge d \mid n$

$$m = qn + r = \underbrace{(m \operatorname{div} n)\, n + m \bmod n}$$

$$\underbrace{m \bmod n}_{r} = m - \underbrace{(m \operatorname{div} n)}_{q}\, n$$

$$d \mid m - (m \operatorname{div} n)\, n$$

$d \mid m \bmod n$

---

2) $d \mid n \wedge d \mid m \bmod n$

$m = qn + r = (m \operatorname{div} n) n + (m \bmod n)$

$\Rightarrow d \mid m$

Tw. Euklidesa . $m \in \mathbb{Z}, n \in \mathbb{N}$

$$\boxed{NWD(m, n) = NWD(n, m \bmod n)}$$

$NWD(m, n) = NWD(m-n, n)$

$d \mid m, n \Rightarrow d \mid m-n$

$m = (m-n)+n \Leftarrow d \mid m-n \wedge d \mid n$

$d \mid m$

$NWD(660, 525) = NWD(525, 660 \% 525) =$

$= NWD(525, 135) = NWD(135, 120) =$

$= NWD(120, 15) = NWD(15, 0) = \boxed{15}$

d

660
525
135
120
$\boxed{15}$ ← NWD
0

17017
6783
3451
3332
$\boxed{119}$ ← NWD
0

$$\begin{array}{r} 6783 \\ \times\ 2 \\ \hline 13566 \\ 17017 \\ \hline 3451 \end{array}$$

$$\begin{array}{r} 28 \\ 3332 : 119 \\ 2380 \\ \hline 952 \\ 952 \\ \hline 0 \end{array}$$

m, n

M bitów, N bitów

Liczba kroków w alg. Euklidesa

$\leq M + N + 1$ → 4001

$m \sim 2^{2000}$

$n \sim 2^{2000}$