Tw. o dzieleniu z resztą

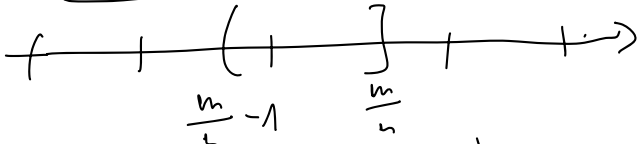
$\forall m \in \mathbb{Z}$ $\forall n \in \mathbb{N}$ $\exists! q, r \in \mathbb{Z}$

$m = qn + r$

$r \in \{0, 1, \dots, n-1\}$

1) Istnienie

$\left(\frac{m}{n} - 1, \frac{m}{n} \right]$



Istnieje dokładnie jedno $q \in \mathbb{Z}$, które należy do $\left(\frac{m}{n} - 1, \frac{m}{n} \right]$.

$r := m - qn$

$qn + r = qn + (m - qn) = m$

$\frac{m}{n} - 1 < q \leq \frac{m}{n} \quad | \cdot n$

$m - n < qn \leq m \quad | - m$

$-n < qn - m \leq 0 \quad | \cdot (-1)$

$0 \leq \underbrace{m - qn}_{r} < n$

2) „jedyność"

Załóżmy, że

$m = qn + r = q'n + r'$,

gdzie $q, q' \in \mathbb{Z}$, $r, r' \in \{0, 1, \dots, n-1\}$

$qn + r - (q'n + r') = 0$

$(q - q')n + (r - r') = 0$

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

$\Downarrow$

$n \mid r' - r$

$-n < -(n-1) \leq r' - r \leq n - 1 < n$

$\vee$

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

$(q - q')n = 0$

$q - q' = 0 \Rightarrow q' = q$

/ , %
//

IN: $m \geq 0$, $\boxed{n \geq 1}$

OUT: $q, r \in \mathbb{Z}$, $r \in \{0, 1, \dots, n-1\}$

$\boxed{m = qn + r \quad r \in \{0, 1, \dots, n-1\}}$

$q = 0$

$r = m$

while $\boxed{r \geq n}$ (Q)

$q \leftarrow q + 1$

$r \leftarrow r - n$ (S)

$\boxed{m = qn + r \wedge r \geq 0}$ —S→ $\boxed{m = qn + r \wedge r \geq 0}$

---

1) Dlaczego program się kończy?

$r \leftarrow r - n$

W każdym obrocie r zmniejsza się o ≥ 1, więc po pewnej liczbie kroków r będzie $< n$.

2) NIEZMIENNIK

$m = qn + r \wedge r \geq 0$ (*)

- przed wejściem w pętlę (*) zachodzi.
- jeśli (*) było prawdą przed wykonaniem S, to jest prawdą po wykonaniu S.

$m = qn + r \overset{(S)}{\Longrightarrow} m = (q+1)n + r - n$

3) Po zakończeniu mamy

$\underbrace{m = qn + r \wedge r \geq 0}_{(*)} \wedge \underbrace{\neg(r \geq n)}_{Q}$

$r < n$

Inne metody

1) Dzielenie pisemne

2) n^{-1}, Algorytm Newtona-Raphsona $f(x) = 0$.

/ %

Największy wspólny dzielnik

$m, n \in \mathbb{Z}$, $m \neq 0 \vee n \neq 0$

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

2) Przynajmniej jedna z liczb m lub n ma skończenie wiele dzielników.

3) Zbiór wspólnych dzielników m i n jest skończony.

4) NWD(m,n) ← największa liczba w zbiorze wspólnych dzielników

NWD(m,n) = gcd(m,n) = (m,n)

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

$660 = 2 \cdot 330 = 2 \cdot 2 \cdot 165 = 2 \cdot 2 \cdot 3 \cdot 55 = 2 \cdot 2 \cdot \boxed{3} \cdot \boxed{5} \cdot 11$

$525 = 3 \cdot 175 = 3 \cdot 5 \cdot 35 = \boxed{3} \cdot \boxed{5} \cdot 5 \cdot 7$

Algorytm Euklidesa

$NWD(m, n) \rightsquigarrow NWD(m', n')$

$m \geq n$

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

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

$k d'' - l \cdot d$

$d \mid m-n \wedge d \mid n \Rightarrow$ $m - n = kd \Rightarrow d \mid m \wedge d \mid n$

$m = k \cdot d + n$

$m = kd + ld = (k+l)d$

Tw. Euklidesa.

$m \geq 0, \; n \geq 1$

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

$NWD(m,n) = NWD(qn + r, n) = NWD((q-1)n + r, n) =$

$\ldots = NWD(1 \cdot n + r, n) = NWD(r, n) = NWD(m \bmod n, n)$

$NWD(660, 525) = NWD(525, 135) = NWD(135, 120) =$

$= NWD(120, 15) = NWD(15, 0)$

$\bigwedge_{m \in \mathbb{N}} NWD(m, 0) = m.$

660
525
135
120
15 ← NWD
0

NWD(17017, 6783) = 119

17017
6783
3451
3332
119 ← NWD
0

6783
2
13566
119
28
952
238
3332

/	%
1	0