WO Zasada dobrego uporządkowania.

$$\forall X \subseteq \mathbb{N} \quad (X \neq 0) \to (\exists a \in X \quad \forall b \in X \quad b \geq a)$$

TW. WO $\to$ IND.

TW. Nie istnieje nieskończony malejący ciąg liczb naturalnych, tzn taki ciąg $\{a_n\}_{n \in \mathbb{N}}$: $\forall n \; a_n \in \mathbb{N}$
$\forall n \; a_{n+1} < a_n$

Dowód (Wynika z zasady WO).

Załóżmy nie wprost, że istnieje ciąg

$\{a_n\}_{n \in \mathbb{N}}$ taki że $\forall n \; a_n \in \mathbb{N} \wedge a_{n+1} < a_n$

Rozważmy zbiór $X = \{a_0, a_1, a_2, \dots\}$

Wtedy (1). $X \subseteq \mathbb{N}$
(2). $X \neq 0$
(3). Zauważmy, że X nie ma elementu najmniejszego:

(gdyby pewne $a \in X$ był naj-mniejszy to $a = a_n$, dla pewnego n, ale $a_{n+1} < a_n = a$ zatem a nie mógłby być najmniejszy)

(1) $\wedge$ (2) $\wedge$ (3) przeczą zasadzie WO.

Sprzeczność $\square$

NAJWIĘKSZY WSPÓLNY DZIELNIK
ALGORYTM EUKLIDESA.

$k \neq 0 \vee l \neq 0$

Def Niech $k, l \in \mathbb{N}$. Największym wspólnym dzielnikiem k i l nazywamy liczbę naturalną

$$\max\{n \in \mathbb{N} : n|k \wedge n|l\} \overset{\text{ozn}}{=} NWD(k,l)$$

Przykład:

$NWD(12,15) = 3$, $NWD(21,10) = 1$

Algorytm Euklidesa:

- $(15,12) \to (12, 15 \pmod{12}) = (12,3) \to (3, 12 \pmod 3)$

$= (3,0)$ Koniec, $NWD(15,12) = 3$

- $a \geq b$ $(a,b) = (a_0, b_0) \to (b_0, a_0 \pmod{b_0}) = (a_1, b_1)$
... $(a_n, b_n) \to (b_n, a_n \pmod{b_n}) \to \dots \to (a_t, 0)$
Wtedy $NWD(a,b) = a_t$

- Dla $a \geq b$

```
NWD(a,b) {
while (b > 0)          a % b.
{ [a,b] → [b, a (mod b)] }
return a;
}
```

Fakt. Dla dowolnych liczb naturalnych $a > b$ algorytm Euklidesa startujący z pary (a,b) zatrzymuje się.

Dowód: Załóżmy nie wprost, że dla pewnej pary (a,b) alg. Rozważmy kolejne stany algorytmu nie zatrzymuje się
$(a,b) = (a_0,b_0) \to (a_1,b_1) \to \dots \to (a_n,b_n) \to \dots$

Definiujemy ciąg liczb naturalnych $\{c_i\}_{i \in \mathbb{N}}$

$c_i = a_i + b_i$

• Ciąg $\{c_i\}$ jest ciągiem malejącym:

$\forall i \quad c_{i+1} = a_{i+1} + b_{i+1} = b_i + a_i \pmod{b_i} < b_i + a_i = c_i$

$\forall i \quad c_{i+1} < c_i$.

Więc $\{c_i\}$ jest nieskończonym malejącym ciągiem liczb naturalnych.
Taki ciąg nie istnieje. Sprzeczność.

Więc AE zatrzymuje się na każdej parze (a,b). □

Uwaga $a,b,c,d \in \mathbb{N}^+$ takie, że

Jeśli $(\forall n \in \mathbb{N}) \; (n|a \wedge n|b) \overset{*}{\leftrightarrow} (n|c \wedge n|d)$
to $NWD(a,b) = NWD(c,d)$.

Dowód (szkic).

$NWD(a,b) \mid a \wedge NWD(a,b) \mid b \xrightarrow{*} NWD(a,b) \mid c \wedge NWD(c,b) \mid d.$

$\xrightarrow{!!} NWD(a,b) \mid NWD(c,d)$

analogicznie $NWD(c,d) \mid NWD(a,b)$

$\rightarrow NWD(a,b) = NWD(c,d).$

Fakt. Jeśli algorytm Euklidesa startujący z pary (a,b) zatrzymuje się na parze $(c,0)$ to $c = NWD(a,b)$.

D-d: Oznaczmy kolejne pary wyliczane przez AE:

$(a,b) = (a_0, b_0) \rightarrow (a_1, b_1) \rightarrow \dots \rightarrow (a_n, b_n) = (c, 0).$

Zauważmy że:

$(**)\ \forall i\ \forall n\ \left(n \mid a_i \wedge n \mid b_i\right) \leftrightarrow \left(n \mid a_{i+1} \wedge n \mid b_{i+1}\right)$

bo: Niech $n \mid a_i \wedge n \mid b_i$ wtedy

$(\rightarrow)$ $n \mid b_i$ tzn $n \mid a_{i+1}$

$n \mid a_i \pmod{b_i} = a_i - k b_i$ tzn $n \mid b_{i+1}$

więc $n \mid a_{i+1} \wedge n \mid b_{i+1}$.

$(\leftarrow)$ ćw.

Z $(**)$ wynika, że $\forall i\ NWD(a_i, b_i) = NWD(a_{i+1}, b_{i+1})$

Więc

$NWD(a,b) = NWD(a_0, b_0) = NWD(a_1, b_1) = \dots = NWD(a_n, b_n) =$

$NWD(c, 0) = c$ □

ALGORYTM EUKLIDESA I RÓWNANIA DIOFANTYCZNE.

• Niech $a, b \in \mathbb{Z}$.

• Szukamy rozwiązań $x, y \in \mathbb{Z}$ takich że

$$ax + by = NWD(a, b).$$

Przykład.

$$57x + 15y = NWD(57, 15) = 3.$$

AE:

$$(57, 15) \to (15, 57 \bmod 15) = (15, 12) \to (12, 3) \to (3, 0)$$

$$3 = 15 \cdot \boxed{1} + 12 \cdot \boxed{-1} = \underline{15} \cdot 1 + \underline{12} \cdot (-1)$$

$$12 = 57 \boxed{1} + 15 \boxed{-3} = \underline{57} \cdot 1 + \underline{15} \cdot (-3)$$

$$\cdot\ 3 = 15 \cdot 1 + \underline{12}(-1) = \underline{15} \cdot (1) + (\underline{57} \cdot 1 + \underline{15} \cdot (-3))(-1)$$

$$= 15 \cdot 1 + 57(-1) + 15 \cdot 3 = 57 \cdot (-1) + 15 \cdot 4$$

$$57 \cdot (-1) + 15 \cdot 4 = 3$$

TW. Niech $a, b, c \in \mathbb{Z}$. Równanie

$$ax + by = c$$

ma rozwiązanie $x, y \in \mathbb{Z}$ wtedy i tylko wtedy, gdy

$$NWD(a, b) \mid c$$

D-d $\to$ Niech $x, y \in \mathbb{Z}$ rozwiązania $NWD(a, b) \mid a$ i $NWD(a, b) \mid b \to NWD(a, b) \mid ax + by$ tzn $NWD(a, b) \mid c$

$\leftarrow$ Niech $NWD(a,b) \mid C$ tzn $C = k \cdot NWD(a,b)$.

!!! Wiemy że równanie

$ax' + by' = NWD(a,b)$ ma rozw $x', y' \in \mathbb{Z}$

Wtedy $x = k \cdot x'$, $y = k \cdot y'$ jest rozwiązaniem równania $ax + by = C$ $\square$