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

$$ax + by = c$$

ma rozwiązanie $x, y \in \mathbb{Z}$

$$\Leftrightarrow$$

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

.

ELEMENTY ODWRACALNE PIERŚCIENIA. GRUPA $\mathbb{Z}_n^*$

Def Niech $(P, +, \cdot)$ pierścień z 1, elementem neutralnym mnożenia.
Element $a \in P$ nazywamy odwracalnym, gdy istnieje $b \in P$, że $a \cdot b = 1 = b \cdot a$

Np. Elementy odwracalne w $(\mathbb{Z}, +, \cdot)$ to 1 i (-1).

Ozn. Zbiór elementów odwracalnych $(P, +, \cdot)$ oznaczamy P^*.

$$P^* = \{a \in P : (\exists b \in P)\ a \cdot b = ba = 1\}$$

TW. Niech $(P, +, \cdot)$ pierścień z 1. Wtedy $(P^*, \cdot)$ jest grupą

D-d. (0): $\cdot$ jest działaniem na P^*:
$(\forall a, b \in P^*\quad a \cdot b \in P^*)$

Niech $a, b \in P^*$ tzn istnieją $a', b' \in P$

Tehe, że $a \cdot a' = b \cdot b' = 1$

Wiec $(a \cdot b) \cdot (b' a') \overset{\text{łączność}}{=} a \cdot (b b') a' = a \cdot 1 \cdot a' = a a' = 1$

Zatem $a \cdot b \in P^*$

(1) • jest łączne na P^* bo jest łączne na P.

(2) $1 \in P^*$ bo $1 \cdot 1 = 1$

(3) $\forall a \in P^* \quad a^{-1} \in P^*$:

Skoro $a \in P^*$ tzn $\exists b \quad a \cdot b = b a = 1$
tzn b jest elementem odwrotnym do a.
Skoro taki jest jedyny to $b = a^{-1}$.
Wtedy $a^{-1} \cdot a = 1 = a \cdot a^{-1}$ wiec $a^{-1} \in P^*$

0 + 1 + 2 + 3 : $(P^*, \cdot)$ jest grupa. □

Przykład: $(\mathbb{Z}, +, \cdot)$. Wtedy $\mathbb{Z}^* = \{a \in \mathbb{Z} : (\exists b \in \mathbb{Z}) ab = 1\}$
$= \{a \in \mathbb{Z} : \frac{1}{a} \in \mathbb{Z}\}$
Zatem: $(\{-1, 1\}, \cdot)$ jest grupą. $= \{1, -1\}$
$\cong C_2$

• Grupa $\mathbb{Z}_n^*$:

Przykład $n = 6$. $\mathbb{Z}_6 = (\{0, 1, 2, 3, 4, 5\}, \overset{+}{6}, \overset{\cdot}{6})$ ← jedynka

Elementy odwracalne: 0 NIE 3 NIE
• 1 TAK 4 NIE
2 NIE • 5 TAK $5 \cdot 5 = 1$

TW. Niech $n \in \mathbb{N}^+$. Element $a \in \{0,1,2,\dots,n-1\}$ elementem odwracalnym w pierścieniu $\mathbb{Z}_n \iff NWD(a,n)=1$.

Dowód $\rightarrow$: Niech a element odwracalny w $\mathbb{Z}_n$
tzn istnieje $x \in \mathbb{Z}_n$: $a \cdot_n x = 1$
$(\exists y \in \mathbb{Z})$ $a \cdot x = n \cdot y + 1$
$a \cdot x - n \cdot y = 1$
ozn $y' = -y$ $a \cdot x + n y' = 1$
Równ.: ma rozwiązanie $x, y' \in \mathbb{Z}$
Więc (TW): $NWD(a,n) \mid 1$
Więc $NWD(a,n) = 1$

$\leftarrow$: Niech $a \in \mathbb{Z}_n$ takie że $NWD(a,n) = 1$
Wtedy (TW) równanie $ax + ny = 1$ ma rozwiązanie.
$x, y \in \mathbb{Z}$.
Niech $b = x \pmod n$

Wtedy $a \cdot_n b = a \cdot_n x = a \cdot x \pmod n = ax + ny \pmod n$
$= 1 \pmod n = 1$. □

Przykład: 7^{-1} w $\mathbb{Z}_{12}$:

$7^{-1} = x$. tzn $7 \cdot_{12} x = 1$ tzn $(7 \cdot x) \bmod 12 = 1$

Więc $\exists y \in \mathbb{Z}$ $7x = 12y + 1$
$7x - 12y = 1$

AE: $(12,7) \rightarrow (7,5) \rightarrow (5,2) \rightarrow (2,1) \rightarrow (1,0)$ — NWD(12,7)

$1 = \underline{5} \cdot 1 - \underline{2} \cdot 2 = \underline{5} \cdot 1 - (7-5) \cdot 2 = \underline{7} \cdot (-2) + \underline{5} \cdot 3 =$
$7 \cdot (-2) + (12-7) \cdot 3 = 12 \cdot 3 + 7 \cdot (-5)$

$$\overset{x}{7}\cdot(-5)+12\cdot\overset{y}{3}=1$$

$x=(-5)$

$b=(-5) \bmod 12 = 7.$

Spr: $7 \cdot_{i_2} 7 = 49 \pmod{12} = 1$

Wniosek. $\mathbb{Z}_n^* = (\{k \in \{0,\dots n-1\} : NWD(n,k)=1\}, \cdot_n)$ jest grupą.

Przykłady:

$\mathbb{Z}_{12}^* = (\{1,2,3,4,5,6,7,8,9,10,11\}, \cdot_{12}) = (\{1,5,7,11\})$

Uwaga: $\mathbb{Z}_{12}^*$ jest grupą przemienną

$\begin{cases} \cdot \ Ord(5) = 2, \ Ord(7)=2, \ Ord(11)=2. \\ \cdot \ |\mathbb{Z}_n^*| = 4 \end{cases}$

$\mathbb{Z}_{12}^* \cong \mathbb{C}_2 \times \mathbb{C}_2.$

LICZBY PIERWSZE.

Def: Liczba $p \in \mathbb{N} \setminus \{0,1\}$ jest pierwsza, gdy $(\forall n \in \mathbb{N})\ n \mid p \to (n=1 \ \vee \ n=p)$.

2, 3, 5, 7, 11, 13, ...

Fakt. Dla każdej liczby naturalnej $n \geq 2$ istnieje liczba pierwsza p, taka, że $p \mid n$.

D-d: Załóżmy niewprost, że istnieje liczba naturalna $n \geq 2$ nie podzielna przez żadną liczbę pierwszą.

Zauważmy że n nie jest liczbą pierwszą

Więc $n = n_1 \cdot n_2$ gdzie $n_1, n_2 > 1$

Wtedy n_1 i n_2 nie są podzielne przez żadną liczbę pierwszą:
(bo gdyby np: $p \mid n_1$ (pierwsza) to $n_1 = p \cdot k$, wtedy $n = p \cdot k \cdot n_2$ tzn $p \mid n$).

... dalej: $n_2 = n_3 \cdot n_4$ n_3, n_4 nie podzielne przez żadną liczbę pierwszą.

$n = n_1 \cdot \bar{n}_2$
$n_1 \cdot n_3 \cdot \bar{n}_4$
$n_1 \cdot n_3 \cdot n_5 \cdot \bar{n}_6$

Wtedy ciąg $n_1, n_2, n_4, n_6, n_8, \ldots$ jest nieskończonym ciągiem malejącym.
Sprzeczność z zasadą dobrego porządku WO. □

TW Euklidesa
Istnieje nieskończenie wiele liczb pierwszych.

D-d Niewprost załóżmy, że jest tylko skończenie wiele liczb pierwszych.

Niech $\{p_1, p_2, \ldots, p_n\}$ zbiór wszystkich liczb pierwszych.

Niech $m = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$

Wtedy
$(\forall_{i=1\dots n})\ p_i \nmid m$ $\quad$ (bo: $m \pmod{p_i} = 1$)

Zatem m nie dzieli się przez żadną liczbę pierwszą. Sprzeczność $\square$

TW. Każda liczba naturalna $n \geq 2$ jest iloczynem liczb pierwszych.

D-d Należy pokazać, że $\forall n \geq 2\ \exists p_1, p_2 \dots, p_k$ pierwsze

$n = p_1 \cdot p_2 \cdots p_k$

Indukcja wzg n.
(*) Załóżmy że każda liczba naturalna $2 \leq m < n$ jest iloczynem liczb pierwszych

Rozważmy liczbę $n+1$:
I $n+1$ jest pierwsza. Wtedy ok.
II $n+1$ nie jest liczbą pierwszą.
Wtedy istnieją liczby naturalne $m_1, m_2 \geq 2$
że $m_1 \cdot m_2 = n+1$
Wtedy $m_1, m_2 \leq n$
Więc z założenia (*) istnieją liczby pierwsze $p_1, \dots, p_k$, $q_1, \dots, q_l$ takie że
$m_1 = p_1 \cdot p_2 \cdots p_k$ oraz $m_2 = q_1 \cdot q_2 \cdots q_l$

Wtedy $n+1 = m_1 \cdot m_2 = p_1 \cdot p_2 \cdots p_k \cdot q_1 \cdot \dots \cdot q_l$

jest rozkładem $n+1$ na iloczyn liczb pierwszych. $\square$