Liczby pierwsze

Oznaczmy zbiór liczb pierwszych przez $\mathbb{P}$.

TW. Liczba $p \in \mathbb{N}$ jest liczbą pierwszą
$\Leftrightarrow$
$(\forall a,b \in \mathbb{N})\ p \mid a \cdot b \rightarrow (p \mid a \ \vee \ p \mid b)$

Przykład • $3 \mid 6 \cdot 4$ ale $3 \mid 6$

• $6 \mid 12 = 3 \cdot 4$ ale $6 \nmid 3$ i $6 \nmid 4$

$6 = 2 \cdot 3 \mid 3 \cdot 4$

TW Zasadnicze twierdzenie arytmetyki.
1. Każda liczba naturalna $n \geq 2$ rozkłada się na iloczyn liczb pierwszych.

2. Rozkład ten jest jednoznaczny.
tzn. dla dwóch liczb $n \geq 2$
jeśli ist. $p_1, p_2 \dots, p_k, q_1, \dots, q_l \in \mathbb{P}$ że, $n = \prod_{i=1}^{k} p_i = \prod_{i=1}^{l} q_i$

$p_1\ p_2$

$6 = 2 \cdot 3$

$6 = 3 \cdot 2$

$q_1\ q_2$

$\rightarrow$ 1. $k = l$

2. po pewnym przenumerowaniu $q_1 \dots q_l$ mamy $p_i = q_i$ dla $i = 1 \dots l = k$.

Dowód.
(1) Tw z poprzedniego wykładu.

(2) Załóżmy nie wprost, że istnieje liczba naturalna $n \geq 2$, oraz liczby pierwsze:

$p_1, p_2, \dots, p_k$

$q_1, q_2, \dots, q_l$

Istotnie różne, tzn dla dowolnego przenumerowania czegoś $q_1 \dots q_l$ jest i takie że $p_i \neq q_i$

Oraz $\prod_{i=1}^{k} p_i = n = \prod_{i=1}^{l} q_i$

Zauważmy, że jeśli istnieje $p \in P$ takie że $p = p_i = q_j$ dla pewnych i, j to możemy podzielić obie strony przez p i otrzymujemy RÓWNIEŻ dwie istotnie różne rozkłady liczby $\frac{n}{p}$.

- Możemy założyć że $\forall_{i,j} \; p_i \neq q_l$

$p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_l$

Zauważmy $p_1 \mid q_1 \cdot (q_2 \cdots q_l)$

Więc $p_1 \mid q_1 \vee p_1 \mid q_2 \cdot (q_3 \cdots q_l)$.

Więc $p_1 \mid q_1 \vee p_1 \mid q_2 \vee p_1 \mid q_3 q_n \cdots q_l$

$\vdots$

Więc $p_1 \mid q_1 \vee p_1 \mid q_2 \vee \dots \vee p_1 \mid q_l$

Więc dla pewnego $i \in \{1 \dots l\}$ $p_1 \mid q_i$

Skoro p_1, q_i są liczbami pierwszymi to $p_1 = q_i$

Sprzeczność z założeniem, że $\forall_{ij} \; p_i \neq q_j$ $\square$

Uwaga. $60 = 2\cdot 3\cdot 2\cdot 5 = 2^2\cdot 3^1\cdot 5^1 = 2^2\cdot 3^1\cdot 5^1\cdot 7^0\cdot 11^0\cdot 13^0 \dots$

• Każdą liczbę naturalną $n \geq 2$ możemy zapisać

$$n = \prod_{p_i \in \mathbb{P}} p_i^{\alpha_i} = \prod_{i=1}^{\infty} p_i^{\alpha_i}$$

$$\mathbb{P} = \{ \underset{2}{p_1^{11}}, \underset{3}{p_2^{11}}, \underset{5}{p_3^{11}}, \dots \}.$$

Fakt. Niech $n = \prod_{i=1}^{\infty} p_i^{\alpha_i}$, $m = \prod_{i=1}^{\infty} p_i^{\beta_i}$ $\alpha_i, \beta_i \in \mathbb{N}$

Wtedy $n \mid m \iff (\forall i)\ \alpha_i \leq \beta_i$

D-d. $\Leftarrow$:

Jeśli $\forall i\ \alpha_i \leq \beta_i$ to

$$m = \prod_{i=1}^{\infty} p_i^{\beta_i} = \prod_{i=1}^{\infty} p_i^{\alpha_i + (\beta_i - \alpha_i)} = \prod_{i=1}^{\infty} p_i^{\alpha_i} \cdot \prod_{i=1}^{\infty} p_i^{\beta_i - \alpha_i} =$$

$$= n \cdot \prod_{i=1}^{\infty} p_i^{\beta_i - \alpha_i} = n \cdot k$$

Zauważmy $\prod_{i=1}^{\infty} p_i^{\beta_i - \alpha_i}$ jest liczbą naturalną, oznaczmy.

Więc $n \mid m$ $\square$

$\longrightarrow$ Niewprost załóżmy, że $n \mid m$ oraz

$\exists i_0\ \alpha_{i_0} > \beta_{i_0}$ $\quad k = q_1 \cdots q_t$

$(\exists k)$ Wtedy $m = \prod_{i=1}^{\infty} p_i^{\beta_i} = n \cdot k = \prod_{i=1}^{\infty} p_i^{\alpha_i} \cdot k = \prod_{i=1}^{\infty} p_i^{\alpha_i} \cdot q_1 \cdots q_t$

Skoro $p_0^{\alpha_{i_0}}$ występuje w rozkładzie (prawej stronie), to ZTA musi wyst. w rozkł po lewej więc $\beta_{i_0} \geq \alpha_{i_0}$. $\square$

$20 \mid 60$ $\quad n = 20 = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdots$

$m = 60 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdots$

$n \mid m \iff \exists k \quad m = k \cdot n \quad , k =$

$\beta_1 \ \beta_2 \ \beta_3 \ \beta_4$

$2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdots = \left(2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdots\right) \cdot 3^1$

$\alpha_1 \ \alpha_2 \ \alpha_3 \ \alpha_4$

$i_0 = 2 \quad p_{i_0} = 3$

ZtA: $\alpha_i \leq \beta_i$

Wniosek. Niech $k = \prod_{i=1}^{\infty} p_i^{\alpha_i}$, $l = \prod_{i=1}^{\infty} p_i^{\beta_i}$, $\alpha_i, \beta_i \in \mathbb{N}$.

Wtedy $NWD(k,l) = \prod_{i=1}^{\infty} p_i^{\min\{\alpha_i, \beta_i\}}$.

D-d ćw

Def Najmniejszą wspólną wielokrotnością liczb $k, l \in \mathbb{N}$ nazywamy liczbę

$$NWW(k,l) = \min\{n : k \mid n \wedge l \mid n\}$$

Przykład $NWW(12,15) = 60$.

Wniosek 2. Jeśli $k = \prod_{i=1}^{\infty} p_i^{\alpha_i}$, $l = \prod_{i=1}^{\infty} p_i^{\beta_i}$.

Wtedy $NWW(k,l) = \prod_{i=1}^{\infty} p_i^{\max\{\alpha_i, \beta_i\}}$

D-d ćw.

Fakt: $(\forall k, l \in \mathbb{N}) \quad NWD(k,l) \cdot NWW(k,l) = k \cdot l$.

$$NWD(k,l) \cdot NWW(k,l) = \prod_{i=1}^{\infty} p_i^{\min\{\alpha_i,\beta_i\}} \cdot \prod_{i=1}^{\infty} p_i^{\max\{\alpha_i,\beta_i\}} =$$

$$= \prod_{i=1}^{\infty} p_i^{\min\{\alpha_i,\beta_i\}+\max\{\alpha_i,\beta_i\}} = \prod_{i=1}^{\infty} p_i^{\alpha_i+\beta_i} =$$

$$\prod_{i=1}^{\infty} p_i^{\alpha_i} \cdot \prod_{i=1}^{\infty} p_i^{\beta_i} = k \cdot l.$$