Matematyka Dyskretna

Wykład III

Grzegorz Bobiński (UMK)

Definicja

Liczbę $p \in \mathbb{Z}$ nazywamy pierwszą, jeśli $p \geq 0$ i

$$\#\{a \in \mathbb{N} : a \mid p\} = 2.$$

Oznaczenie

$\mathbb{P} := \{p \in \mathbb{Z} : \text{liczba } p \text{ jest pierwsza}\}$.

Lemma 1.27

Niech $p \in \mathbb{P}$.

(1) Wtedy $p > 1$.

(2) Jeśli $a \in \mathbb{N}$ i $a \mid p$, to $a = 1$ lub $a = p$.

Przypomnienie

(1.4): $a \mid 1 \iff a = \pm 1$.
(1.5): $a \mid 0 \iff a \in \mathbb{Z}$.

Dowód

(1): Mamy $\#\{a \in \mathbb{N} : a \mid 0\} \overset{(1.5)}{=} \#\mathbb{N} = \infty \neq 2$ oraz $\#\{a \in \mathbb{N} : a \mid 1\} \overset{(1.4)}{=} \#\{1\} = 1 \neq 2$.
(2): Wiemy, że $\{1, p\} \subseteq \{a \in \mathbb{N} : a \mid p\}$.
Z definicji $\#\{a \in \mathbb{N} : a \mid p\} = 2$.
(1) $\implies$ $p \neq 1$ $\implies$ $\#\{1, p\} = 2$ $\implies$ $\{1, p\} = \{a \in \mathbb{N} : a \mid p\}$. $\square$

Lemat 1.28

Jeśli $a \in \mathbb{N}_+$, to istnieją $p_1, \ldots, p_n \in \mathbb{P}$, $n \in \mathbb{N}$, takie, że $a = p_1 \cdots p_n$.

Przypomnienie

(1.5): $0 \mid a \iff a = 0$.
(1.6): $a \mid b \neq 0 \implies |a| \leq |b|$.

Dowód

Indukcja na a.
I. $a = 1$:
Oczywiste ($n := 0$).
II. $a > 1$:
Załóżmy, że dla teza jest prawdziwa dla każdego $b \in [1, a-1]$.
1° $a \in \mathbb{P}$:
Oczywiste ($n := 1$ i $p_1 := a$).
2° $a \notin \mathbb{P}$:
Istnieje $b \in \mathbb{N} \setminus \{1, a\}$ takie, że $b \mid a$
(1.5) $\implies$ $b \neq 0$.
(1.6) $\implies$ $b \leq a$.
Ostatecznie, $1 < b < a$.
(ZI) $\implies$ istnieją $p_1, \ldots, p_{n_1} \in \mathbb{P}$ takie, że $b = p_1 \cdots p_{n_1}$.
Niech $c := \frac{a}{b}$.
$1 < b < a \implies 1 < c < a \overset{\text{(ZI)}}{\implies}$ istnieją $p_{n_1+1}, \ldots, p_{n_1+n_2} \in \mathbb{P}$ takie, że $c = p_{n_1+1} \cdots p_{n_1+p_{n_2}}$.
Wtedy $a = b \cdot c = p_1 \cdots p_{n_1} p_{n_1+1} \cdots p_{n_1+n_2}$. $\square$

Wniosek 1.29

Jeśli $a \in \mathbb{Z}$ i $a \neq \pm 1$, to istnieje $p \in \mathbb{P}$ takie, że $p \mid a$.

Dowód

1° $a = 0$:

Oczywiste.

2° $a \neq 0$:

(1.28) $\implies$ istnieją $p_1, \ldots, p_n \in \mathbb{P}$ takie, że $|a| = p_1 \cdot \ldots \cdot p_n$.

$|a| \neq 1 \implies n > 0 \implies p_1 \mid a$. $\square$

Twierdzenie 1.30

$|\mathbb{P}| = \infty$.

Przypomnienie

(1.7)+(1.8): $c \mid a, b \implies c \mid k \cdot a + l \cdot b$.

Dowód (Euklides)

Przypuśćmy, że $|\mathbb{P}| < \infty$.

Niech $a := \prod_{q \in \mathbb{P}} q + 1$.

$a > 1 \overset{(1.29)}{\implies}$ istnieje $p \in \mathbb{P}$ takie, że $p \mid a$.

Wtedy $p \mid p \cdot \prod_{q \in \mathbb{P} \setminus \{p\}} q = \prod_{q \in \mathbb{P}} q \overset{(1.7)+(1.8)}{\implies} p \mid a - \prod_{q \in P} q = 1 \overset{(1.4)}{\implies} p = 1$, sprzeczność z (1.27)(1). $\square$

Stwierdzenie 1.31

Niech $a_1, \ldots, a_n \in \mathbb{Z}$.
Jeśli $p \in \mathbb{P}$ i $p \mid a_1 \cdots a_n$, to istnieje $i \in [1, n]$ takie, że $p \mid a_i$.
W szczególności, $n > 0$.

Przypomnienie

(1.23): $\gcd(a, b) = 1$ i $a \mid b \cdot c \implies a \mid c$.

Dowód

Indukcja na n.

(1.27)(1) $\implies p > 1 \overset{(1.4)}{\implies} a_1 \cdots a_n \neq 1 \implies n > 0$.
I. $n = 1$:
Oczywiste.
II. $n > 1$:
1° $p \mid a_n$:
OK.
2° $p \nmid a_n$:

(1.27)(2) $\implies \gcd(p, a_n) = 1 \overset{(1.23)}{\implies} p \mid a_1 \cdots a_{n-1} \overset{(\mathrm{I})}{\implies}$ istnieje $i \in [1, n-1]$ takie, że $p \mid a_i$. □

Oznaczenia

Jeśli $F : \mathbb{P} \to \mathbb{N}$ i $|I_0| < \infty$, gdzie

$$I_0 := \{p \in \mathbb{P} : F(p) \neq 0\}$$

(mówimy, że F jest sumowalna), to definiujemy

$$\sum_{p \in \mathbb{P}} F(p) := \sum_{p \in I_0} F(p).$$

Analogicznie, jeśli $G : \mathbb{P} \to \mathbb{N}_+$ i $|I_1| < \infty$, gdzie

$$I_1 := \{p \in \mathbb{P} : F(p) \neq 1\},$$

(mówimy, że G jest wymnażalna), to definiujemy

$$\prod_{p \in \mathbb{P}} G(p) := \prod_{p \in I_1} G(p).$$

Niech $F : \mathbb{P} \to \mathbb{N}$. Jeśli $G : \mathbb{P} \to \mathbb{N}_+$ dana jest wzorem

$$G(p) := p^{F(p)} \qquad (p \in \mathbb{P}),$$

to F jest sumowalna wtedy i tylko wtedy, gdy G jest wymnażalna.

Twierdzenie 1.32 (Podstawowe Twierdzenie Arytmetyki)

Jeśli $a \in \mathbb{N}_+$, to istnieje jednoznacznie wyznaczona funkcja sumowalna $\alpha : \mathbb{P} \to \mathbb{N}$ taka, że $a = \prod_{p \in P} p^{\alpha(p)}$.

Dowód

1° Istnienie.

(1.28) $\implies$ istnieją $p_1, \ldots, p_n \in \mathbb{P}$ takie, że $a = p_1 \cdots p_n$.

Jeśli

$$\alpha(p) := \#\{i \in [1, n] : p_i = p\} \qquad (p \in \mathbb{P}),$$

to α jest sumowalna i $a = \prod_{p \in \mathbb{P}} p^{\alpha(p)}$.

2° Jednoznaczność.

Przypuśćmy, że $\alpha, \alpha' : \mathbb{P} \to \mathbb{N}_+$ są sumowalne i $\prod_{p\in\mathbb{P}} p^{\alpha(p)} = a = \prod_{p\in\mathbb{P}} p^{\alpha'(p)}$.

Udowodnimy, że $\alpha = \alpha'$, tzn. $\alpha(p) = \alpha'(p)$ dla każdego $p \in \mathbb{P}$.

Indukcja na a.

2.I. $a = 1$:

Wtedy $\alpha(p) = 0 = \alpha'(p)$ dla każdego $p \in \mathbb{P}$.

2.II. $a > 1$:

Istnieje $q \in \mathbb{P}$ takie, że $\alpha(q) > 0$.

Wtedy $q \mid \prod_{p\in\mathbb{P}} p^{\alpha(p)} = \prod_{p\in\mathbb{P}} p^{\alpha'(p)}$.

(1.31) $\implies$ istnieje $q' \in \mathbb{P}$ takie, że $\alpha'(q') > 0$ i $q \mid q'$.

(1.27) $\implies$ $q = q'$.

Definiujemy $\beta, \beta' : \mathbb{P} \to \mathbb{N}$ wzorami

$$\beta(p) := \begin{cases} \alpha(p) - 1 & p = q, \\ \alpha(p) & p \neq q, \end{cases} \quad (p \in \mathbb{P}) \quad \text{i} \quad \beta'(p) := \begin{cases} \alpha'(p) - 1 & p = q, \\ \alpha'(p) & p \neq q, \end{cases} \quad (p \in \mathbb{P}).$$

Wtedy

$$q \cdot \prod_{p\in\mathbb{P}} p^{\beta(p)} = \prod_{p\in\mathbb{P}} p^{\alpha(p)} = a = \prod_{p\in\mathbb{P}} p^{\alpha'(p)} = q \cdot \prod_{p\in\mathbb{P}} p^{\beta'(p)}.$$

Stąd $\prod_{p\in\mathbb{P}} p^{\beta(p)} = \frac{a}{q} = \prod_{p\in\mathbb{P}} p^{\beta'(p)}$.

(ZI) $\implies$ $\beta = \beta'$

W konsekwencji, $\alpha = \alpha'$. $\square$

Fakt 1.33

Niech $\alpha, \beta : \mathbb{P} \to \mathbb{N}$ będą funkcjami sumowalnymi.
Jeśli

$$a := \prod_{p \in \mathbb{P}} p^{\alpha(p)} \qquad \text{i} \qquad b := \prod_{p \in \mathbb{P}} p^{\beta(p)}$$

to $b \mid a$ wtedy i tylko wtedy, gdy $\beta(p) \leq \alpha(p)$ dla każdego $p \in \mathbb{P}$.

Dowód

$\Leftarrow$:

Załóżmy, że $\beta(p) \leq \alpha(p)$ dla każdego $p \in \mathbb{P}$.

Niech $c := \prod_{p \in \mathbb{P}} p^{\alpha(p)-\beta(p)}$.

Wtedy $c \in \mathbb{Z}$ i $a = b \cdot c$, więc $b \mid a$.

$\Rightarrow$:

Załóżmy, że $b \mid a$.

Ustalmy $c \in \mathbb{Z}$ takie, że $a = b \cdot c$.

Zauważmy, że $c > 0$ (gdyż $a, b > 0$).

(1.32) $\implies$ istnieje funkcja sumowalna $\gamma : \mathbb{P} \to \mathbb{N}$ taka, że $c = \prod_{p \in \mathbb{P}} p^{\gamma(p)}$.

Wtedy

$$\prod_{p \in \mathbb{P}} p^{\alpha(p)} = a = b \cdot c = \prod_{p \in \mathbb{P}} p^{\beta(p)} \cdot \prod_{p \in \mathbb{P}} p^{\gamma(p)} = \prod_{p \in \mathbb{P}} p^{\beta(p)+\gamma(p)}.$$

(1.32) $\implies$ $\alpha(p) = \beta(p) + \gamma(p)$ dla każdego $p \in \mathbb{P}$.

W szczególności, $\alpha(p) \geq \beta(p)$ dla każdego $p \in \mathbb{P}$. $\square$

Fakt 1.33

Niech $\alpha, \beta : \mathbb{P} \to \mathbb{N}$ będą funkcjami sumowalnymi.
Jeśli

$$a := \prod_{p \in \mathbb{P}} p^{\alpha(p)} \qquad \text{i} \qquad b := \prod_{p \in \mathbb{P}} p^{\beta(p)}$$

to $b \mid a$ wtedy i tylko wtedy, gdy $\beta(p) \leq \alpha(p)$ dla każdego $p \in \mathbb{P}$.

Fakt 1.34

Niech $\alpha, \beta : \mathbb{P} \to \mathbb{N}$ będą funkcjami sumowalnymi.
Jeśli

$$a := \prod_{p \in \mathbb{P}} p^{\alpha(p)} \qquad \text{i} \qquad b := \prod_{p \in \mathbb{P}} p^{\beta(p)},$$

to

$$\gcd(a, b) = d := \prod_{p \in \mathbb{P}} p^{\min\{\alpha(p), \beta(p)\}}.$$

Dowód

Oczywiście $d \geq 0$.

Ponieważ $\min\{\alpha(p), \beta(p)\} \leq \alpha(p), \beta(p)$, więc $d \mid a, b$ na mocy (1.33).

Ustalmy c takie, że $c \mid a$ i $c \mid b$.

Na mocy (1.32) istnieje funkcja sumowalna $\gamma \colon \mathbb{P} \to \mathbb{N}$ taka, że $|c| = \prod_{p \in \mathbb{P}} p^{\gamma(p)}$.

Wtedy $\gamma(p) \leq \alpha(p), \beta(p)$ dla każdego $p \in \mathbb{P}$ na mocy (1.33), więc $\gamma(p) \leq \min\{\alpha(p), \beta(p)\}$ dla każdego $p \in \mathbb{P}$.

Na mocy (1.33), $c \mid d$. □