1.3 Podstawowe Twierdzenie Arytmetyki

Celem tego wykładu jest przedstawienie sformułowania i dowodu Podstawowego Twierdzenia Arytmetyki. Zaczniemy od przedstawienia pojęcia funkcji wymnażalnej.

Wiadomo, że przedstawienia liczb 12 i 50 w postaci iloczynów potęg liczb pierwszych mają postać

$$12 = 2^2 \cdot 3^1 \qquad \text{i} \qquad 20 = 2^1 \cdot 5^2.$$

Jeżeli chcielibyśmy ustalić „wspólny" zbiór liczby pierwszych do zapisu powyższych przedstawień (np. na potrzeby liczenia największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności), to możemy dopisać „brakujące" liczby pierwsze w potędze zerowej, a więc otrzymujemy zapisy

$$12 = 2^2 \cdot 3^1 \cdot 5^0 \qquad \text{i} \qquad 20 = 2^1 \cdot 3^0 \cdot 5^2.$$

Nie jest jednak możliwe znalezienie takiego wspólnego zbioru dla wszystkich liczb naturalnych. Nie mniej, możemy obejść ten problem, dopuszczając nieskończone „iloczyny", w których prawie wszystkie (a więc wszystkie poza skończoną ilością) czynniki są równe 1. Jest to uprawnione, gdyż 1 jest elementem neutralnym dla mnożenia, więc w praktyce taki nieskończony iloczyn sprowadza się do wymnożenia skończenie wielu czynników różnych od 1. To prowadzi do następującej definicji.

Definicja. Funkcję $\beta\colon \mathbb{P} \to \mathbb{N}_+$ nazywamy *wymnażalną*, jeśli $\beta(p) = 1$ dla prawie wszystkich $p \in \mathbb{P}$, tzn. zbiór

$$\{p \in \mathbb{P} : \beta(p) \neq 1\}$$

jest skończony.

Można oczywiście rozważać funkcję wymnażalne o innej dziedzinie i innym („większym") zbiorze wartości, ale powyższa definicja będzie wystarczająca dla naszych zastosowań.

Jeśli $\beta\colon \mathbb{P} \to \mathbb{N}_+$ jest funkcją wymnażalną, to możemy zdefiniować iloczyn $\prod_{p\in\mathbb{P}} \beta(p)$ jako (skończony) iloczyn różnych od 1 wartości funkcji β, tj.

$$\prod_{p\in\mathbb{P}} \beta(p) := \prod_{\substack{p\in\mathbb{P}\\ \beta(p)\neq 1}} \beta(p).$$

Na przykład, gdy

$$\beta(p) := \begin{cases} 2^2 & \text{gdy } p = 2, \\ 3^1 & \text{gdy } p = 3, \\ p^0 & \text{gdy } p \neq 2, 3, \end{cases}$$

to

$$\prod_{p\in\mathbb{P}} \beta(p) = 2^2 \cdot 3^1 = 12.$$

Będziemy rozważać funkcje wymnażalne β postaci $\beta(p) = p^{\alpha(p)}$, dla pewnej funkcji $\alpha\colon \mathbb{P} \to \mathbb{N}$. Zauważmy, że w takiej sytuacji $\beta(p) = 1$ wtedy i tylko wtedy, gdy $\alpha(p) = 0$. Ponieważ 0 jest elementem neutralnym dla dodawania, więc przez analogię możemy mówić o sumowaniu wartości takich funkcji i otrzymujemy następującą definicję.

Definicja. Funkcję $\alpha\colon \mathbb{P} \to \mathbb{N}_+$ nazywamy *sumowalną*, jeśli $\alpha(p) = 0$ dla prawie wszystkich $p \in \mathbb{P}$, tzn. zbiór

$$\{p \in \mathbb{P} : \alpha(p) \neq 0\}$$

jest skończony.

Używając powyższych pojęć, możemy powiedzieć, że jeśli $\alpha\colon \mathbb{P} \to \mathbb{N}$ jest funkcją oraz funkcja $\beta\colon \mathbb{P} \to \mathbb{N}_+$ dana jest wzorem $\beta(p) := p^{\alpha(p)}$, $p \in \mathbb{P}$, to funkcja β jest wymnażalna wtedy i tylko wtedy, gdy funkcja α jest sumowalna.

Wykorzystując powyższe pojęcia, Podstawowe Twierdzenie Arytmetyki można sformułować następująco.

Twierdzenie 1.32 (Podstawowe Twierdzenie Arytmetyki)**.** *Jeśli a jest dodatnią liczbą całkowitą, to istnieje jednoznacznie wyznaczona funkcja sumowalna $\alpha\colon \mathbb{P} \to \mathbb{N}$ taka, że*

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

Powyższe twierdzenie można inaczej sformułować następująco: dla każdej dodatniej liczby całkowitej a istnieje indeksowany liczbami pierwszymi ciąg $(\alpha(p))_{p\in\mathbb{P}}$ liczb naturalnych taki, że prawie wszystkie liczby $\alpha(p)$, $p \in \mathbb{P}$, są równe 0, oraz a jest iloczynem liczb postaci $p^{\alpha(p)}$, $p \in \mathbb{P}$ (dodatkowo można założyć, że bierzemy tylko te liczby pierwsze p, dla których $\alpha(p) \neq 0$).

Dowód powyższego twierdzenia składa się z dwóch części: najpierw udowodnimy istnienie stosownej funkcji α, potem jest jednoznaczność.

Dowód Twierdzenie 1.32, Część I: Istnienie. Dowód istnienia funkcji α jest indukcyjny ze względu na a.

Gdy $a = 1$, to teza jest oczywista, gdyż wystarczy wziąć funkcję $\alpha\colon \mathbb{P} \to \mathbb{N}$ tożsamościowo równą 0 (tj. $\alpha(p) = 0$ dla wszystkich $p \in \mathbb{P}$) i wtedy

$$\prod_{p\in\mathbb{P}} p^{\alpha(p)} = \prod_{p\in\mathbb{P}} p^0 = \prod_{p\in\mathbb{P}} 1 = 1 = a.$$

Gdy $a > 1$, to mamy dwie możliwości. Jeśli a jest liczbą pierwszą, to definiujemy funkcję $\alpha\colon \mathbb{P} \to \mathbb{N}$ wzorem

$$\alpha(p) := \begin{cases} 1 & \text{gdy } p = a, \\ 0 & \text{gdy } p \neq a, \end{cases}$$

i wtedy

$$\prod_{p\in\mathbb{P}} p^{\alpha(p)} = a^{\alpha(a)} \cdot \prod_{p\neq a} p^{\alpha(p)} = a^1 \cdot \prod_{p\neq a} p^0 = a \cdot \prod_{p\neq a} 1 = a.$$

Jeśli $a > 1$, ale a nie jest liczbą pierwszą, to a jest liczbą złożoną, a więc istnieją dodatnie liczby całkowite b i c takie, że $a = b \cdot c$ oraz $b, c < a$. Z założenia indukcyjnego istnieją funkcje sumowalne $\beta, \gamma\colon \mathbb{P} \to \mathbb{N}$ takie, że

$$b = \prod_{p\in\mathbb{P}} p^{\beta(p)} \qquad \text{i} \qquad c = \prod_{p\in\mathbb{P}} p^{\gamma(p)}.$$

Jeśli zdefiniujemy funkcję $\alpha\colon \mathbb{P} \to \mathbb{N}$ wzorem $\alpha := \beta + \gamma$, tzn.

$$\alpha(p) := \beta(p) + \gamma(p),$$

to funkcja α jest sumowalna oraz

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

co na mocy zasady indukcji matematycznej kończy dowód istnienia funkcji α o żądanej własności. □

W dowodzie jednoznaczności kluczową rolę odegra następujące stwierdzenie.

Stwierdzenie 1.31. *Niech $a_1, \ldots, a_n$, dla $n \in \mathbb{N}$, będą liczbami całkowitymi. Jeśli liczba pierwsza p dzieli iloczyn $a_1 \cdots a_n$, to istnieje indeks $i \in [1, n]$ taki, że p dzieli a_i. W szczególności, $n > 0$.*

W dowodzie powyższego stwierdzenia wykorzystamy następujący wniosek, który udowodnimy później. Przypomnijmy, że liczby całkowite m i n są względnie pierwsze, gdy $\gcd(m, n) = 1$.

Wniosek 1.23. *Jeśli a, b i c są liczbami całkowitymi takimi, że a dzieli $b \cdot c$ oraz a i b są względnie pierwsze, to a dzieli c.*

Dowód Stwierdzenia 1.31. Pokażemy najpierw, że $n > 0$. Istotnie, jeśli $n = 0$, to zgodnie z umową

$$a_1 \cdots a_n = 1.$$

Wtedy jednak $p \mid 1$, a więc $p = \pm 1$, sprzeczność, gdyż p jest liczbą pierwszą.

Udowodnimy teraz istnienie indeksu i przez indukcję ze względu na n. Gdy $n = 1$, to założenie mówi, że $p \mid a_1$, a więc teza jest oczywista (wystarczy wziąć $i = 1$).

Załóżmy zatem, że $n > 1$. Gdy $p \mid a_n$, to ponownie teza jest oczywista, gdyż zachodzi dla $i = n$. Możemy się zatem skoncentrować na przypadku, gdy p nie dzieli a_n. W tym przypadku, liczby p i a_n są względnie pierwsze, więc stosując Wniosek 1.23 dla $a = p$, $b = a_n$ i $c = a_1 \cdots a_{n-1}$, otrzymujemy, że p dzieli $a_1 \cdots a_{n-1}$. Z założenia indukcyjnego wiemy, iż istnieje $i \in [1, n-1]$ takie, że $p \mid a_i$, co kończy dowód. □

Dowód Wniosku 1.23. Ponieważ $\gcd(a, b) = 1$, więc z Wniosku 1.20 z wykładu wiemy, że istnieją liczby całkowite k i l takie, że

$$k \cdot a + l \cdot b = 1.$$

Mnożąc powyższą równość przez c, otrzymujemy

$$c = (k \cdot c) \cdot a + l \cdot (b \cdot c).$$

Oczywiście iloczyn $(k \cdot c) \cdot a$ jest podzielny przez a. Ponadto z założenia wiemy, że $b \cdot c$ jest podzielne przez a, więc również $l \cdot (b \cdot c)$ jest podzielne przez a. Zatem również c, jako suma $(k \cdot c) \cdot a$ i $l \cdot (b \cdot c)$, jest podzielne przez a. □

Dowód Twierdzenie 1.32, Część II: Jednoznaczność. Przypuśćmy, że mamy funkcje sumowalne $\alpha, \alpha' \colon \mathbb{P} \to \mathbb{N}$ takie, że

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

Przez indukcję ze względu na a pokażemy, że $\alpha = \alpha'$, tzn. $\alpha(p) = \alpha'(p)$ dla każdej liczby pierwszej p.

Jeśli $a = 1$, to mamy równość

$$\prod_{p \in \mathbb{P}} p^{\alpha(p)} = 1,$$

z której wynika, że $p^{\alpha(p)} = 1$, dla każdego $p \in \mathbb{P}$, a więc $\alpha(p) = 0$, dla każdego $p \in \mathbb{P}$. Analogicznie pokazujemy, że $\alpha'(p) = 0$, dla każdego $p \in \mathbb{P}$, co oczywiście implikuje, że $\alpha(p) = \alpha'(p)$ dla każdego $p \in \mathbb{P}$.

Załóżmy teraz, że $a > 1$. Wtedy

$$\prod_{p\in\mathbb{P}} p^{\alpha(p)} > 1,$$

więc istnieje liczba pierwsza q taka, że $q^{\alpha(q)} > 1$, a więc $\alpha(q) > 0$. Ponieważ

$$a = \prod_{p\in\mathbb{P}} p^{\alpha(p)} = q^{\alpha(q)} \cdot \prod_{p\neq q} p^{\alpha(p)} = q \cdot q^{\alpha(q)-1} \cdot \prod_{p\neq q} p^{\alpha(p)},$$

więc q dzieli liczbę a. Z drugiej strony, $a = \prod_{p\in\mathbb{P}} p^{\alpha'(p)}$, a więc q dzieli $\prod_{p\in\mathbb{P}} p^{\alpha'(p)}$. Korzystając ze Stwierdzenia 1.31 (dla $p = q$, n będącego liczbą liczb pierwszych p takich, że $\alpha'(p) > 0$, oraz

$$\{a_1, \ldots, a_n\} = \{p^{\alpha'(p)} : p \in \mathbb{P} \text{ i } \alpha'(p) > 0\})$$

otrzymujemy, że istnieje liczba pierwsza q' taka, że q dzieli $q'^{\alpha'(q')}$. Korzystając ponownie ze Stwierdzenia 1.31 (dla $p = q'$, $n = \alpha'(q')$ oraz $a_1 = \cdots = a_n = q'$), otrzymujemy, że q dzieli q' oraz $\alpha'(q') > 0$. Ponieważ q i q' są liczbami pierwszymi, więc warunek $q \mid q'$ oznacza, że $q = q'$, a więc $\alpha'(q) > 0$.

Niech $b = \frac{a}{q}$. Wtedy

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

gdzie

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

Z założenia indukcyjnego $\beta(p) = \beta'(p)$ dla każdej liczby pierwszej p. Wtedy

$$\alpha(q) = \beta(q) + 1 = \beta'(q) + 1 = \alpha'(q).$$

Podobnie, gdy $p \neq q$, to

$$\alpha(q) = \beta(q) = \beta'(q) = \alpha'(q),$$

co kończy dowód. □