

# Liczb pierwszych jest nieskończenie wiele

Karol GRYSZKA\*

\* Wydział Nauk Ścisłych i Przyrodniczych,  
Uniwersytet Pedagogiczny w Krakowie

Jest wiele dowodów na to, że zbiór liczb pierwszych jest nieskończony. Poniżej pragniemy przedstawić mało znany dowód, którego podstawą są działania na zbiorach. Jest to o tyle ciekawe, że fakt liczbowy dowodzimy przez operacje na zbiorach.

**Definicja.** Jeżeli  $m$  i  $r$  są liczbami całkowitymi oraz  $m \geq 1$ , to zbiór  $r + m\mathbb{Z}$  oznacza zbiór liczb całkowitych przystających do  $r$  modulo  $m$ , to jest

$$r + m\mathbb{Z} := \{r + mk : k \in \mathbb{Z}\}.$$

Każdy z takich zbiorów nazwiemy *zbiorem typu ciąg arytmetyczny*, w skrócie **CA**.

**Oznaczenie.** Zbiór

$$\mathbf{NW}(m) := (1 + m\mathbb{Z}) \cup (2 + m\mathbb{Z}) \cup ((m - 1) + m\mathbb{Z})$$

jest zbiorem wszystkich liczb niebędących wielokrotnościami liczby całkowitej  $m$ .

**Stwierdzenie 1.** Przecięcie skończenie wielu zbiorów **CA** jest albo zbiorem pustym albo zbiorem nieskończonym.

**Dowód.** Jeżeli  $x$  jest elementem każdego ze zbiorów  $r_i + m_i\mathbb{Z}$  dla  $i = 1, \dots, k$ , to  $x + ny$  również jest, gdzie  $y = \mathbf{NWW}(m_1, \dots, m_k)$  oraz  $n \in \mathbb{Z}$ .

**Stwierdzenie 2.** Jeżeli  $\mathcal{A}$  jest rodziną zbiorów, to każde skończone przecięcie skończonych sum zbiorów z  $\mathcal{A}$  jest skończoną sumą skończonych przecięć zbiorów z  $\mathcal{A}$ .

**Dowód.** Jest to konsekwencja równości

$$(A \cup B) \cap (C \cup D) = (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D),$$

która uogólnia się na więcej składników sum oraz więcej przecięć.

**Twierdzenie.** Liczb pierwszych jest nieskończenie wiele.

**Dowód za pomocą działań na zbiorach.** Gdyby  $p_1, \dots, p_k$  były pełną listą liczb pierwszych, to

$$\{-1, 1\} = \mathbf{NW}(p_1) \cap \mathbf{NW}(p_2) \cap \dots \cap \mathbf{NW}(p_k).$$

Po prawej stronie zapisane jest skończone przecięcie skończonych sum zbiorów typu **CA**, zatem na podstawie stwierdzenia 2 jest to również skończona suma skończonych przecięć zbiorów typu **CA**, czyli na podstawie stwierdzenia 1 zbiór  $\{-1, 1\}$  byłby sumą zbiorów albo pustych, albo nieskończonych, co jest oczywiście niemożliwe.

Przedstawimy jeszcze jeden dowód, który bazuje na tylko jednym, elementarnym fakcie.

**Fakt.** Dla dowolnego  $n > 1$  liczby  $n$  oraz  $n + 1$  są względnie pierwsze.

**Dowód.** Jeżeli Czytelnik nie jest przekonany, to algorytm Euklidesa go przekona.

Przejdźmy ponownie do dowodu naszego twierdzenia.

**Dowód (jeszcze raz).** Ustalmy  $n > 1$ . Liczby  $n$  oraz  $n + 1$  są względnie pierwsze, zatem liczba

$$N_2 = n(n + 1)$$

posiada co najmniej dwa różne dzielniki pierwsze. Liczby  $N_2$  oraz  $N_2 + 1$  są względnie pierwsze, zatem liczba

$$N_3 = N_2(N_2 + 1) = n(n + 1)[n(n + 1) + 1]$$

posiada co najmniej trzy różne dzielniki pierwsze. Liczby  $N_3$  oraz  $N_3 + 1$  są względnie pierwsze, zatem liczba

$$N_4 = N_3(N_3 + 1) = n(n + 1)[n(n + 1) + 1] \left\{ n(n + 1)[n(n + 1) + 1] + 1 \right\}$$

posiada co najmniej cztery różne dzielniki pierwsze. I tak dalej, w nieskończoność.

Jest to uproszczona wersja dowodu Hillela Furstenberga z 1955 roku (który otrzymał nagrodę Abela w roku 2020 – szczegóły w  $\Delta_{20}^{11}$ ), którą Idris D. Mercer przedstawił w 2009 roku na łamach czasopisma *The American Mathematical Monthly*.

Jest to fakt analogiczny do klasycznych działań: z prawa rozdzielności mnożenia względem dodawania możemy zapisać

$$(a + b)(c + d) = ac + ad + bc + bd.$$

Rolę mnożenia przejmuje część wspólna zbiorów, a rolę dodawania – suma zbiorów.

Autorem drugiego dowodu jest Filip Saidak, którego publikacja na ten temat ukazała się w 2006 roku również w *The American Mathematical Monthly*.