Porazdelitev praštevil

Matevž Miščič

22. avgust 2023

1 Uvod

Praštevila so v matematiki pomembna, saj so gradniki vseh naravnih števil. Velja namreč, da lahko vsako naravno število, večje od 1, zapišemo kot produkt praštevil. Poleg matematike so praštevila pomembna tudi v računalništvu, še posebej v kriptografiji. V tej predstavitvi si bomo ogledali nekaj zanimivih rezultatov o porazdelitvi praštevil.

2 Praštevilo

Začnimo z definicijo.

Definicija 1. Praštevilo je naravno število, ki ima natanko 2 delitelja.

Prvih nekaj praštevil je $2, 3, 5, 7, 11, 13, \ldots$.
Naslednja lastnost praštevil je ključnega pomena.

Trditev 1. *Vsako naravno število, večje od* 1*, se da zapisati kot produkt števil.*

Dokaz. Trditev bomo pokazali z indukcijo. Naj bo n naravno število, ki je večje od 1. Če sta 1 in n edina delitelja števila n, je n praštevilo in ni kaj dokazati. Sice obstaja nek delitelj a števila n, da velja $1 < a < n$. Torej je $n = ab$ za nek $b \in \mathbb{N}$. Ker je $1 < a, b < n$ lahko po indukcijski predpostavki a in b zapišemo kot produkt praštevil, zato enako velja za njun produkt n. $\square$

Posledice te trditve je, da je praštevil neskončno mnogo. To je rezultat, ki ga je poznal že Evklid okoli leta 300 pred našim štetjem.

Posledica 1. *Praštevil je neskončno mnogo.*

Dokaz. Recimo, da jih je le končno mnogo. Naj bodo $p_1, p_2, \ldots, p_k$ vsa praštevila. Vzemimo $n = p_1 p_2 \cdots p_k + 1$. Po prejšnji trditvi vemo, da lahko n zapišemo kot produkt praštevil, ampak očitno nobeno od praštevil ne deli n, torej smo prišli v protislovje. $\square$

Literatura

[1] J. A. Hocutt in P. L. Robinson, *Everywhere Differentiable, Nowhere Continuous Functions*, Amer. Math. Monthly **125** (2018) 923–928.

[2] P. R. Halmos, *Problems for Mathematicians, Young and Old*, Dolciani Mathematical Expositions **12**, Mathematical Association of America, Washington, 1991.