GENERATORJI PRAŠTEVIL

JANKO BRAČIČ

Naravoslovnotehniška fakulteta
Univerza v Ljubljani

Math. Subj. Class. (2010): 11A41

Generator praštevil je postopek, ki nam na vsakem koraku vrne praštevilo oziroma množico praštevil. V članku predstavimo nekaj znanih in manj znanih generatorjev praštevil.

PRIME NUMBER GENERATORS

A prime generator is an algorithm which on each step returns a prime number or a set of prime numbers. In this paper we present some known and less known prime generators.

Uvod

Množica naravnih števil $\mathbb{N}$ ima po eni strani preprosto strukturo, ki se nanaša na seštevanje. Do vsakega naravnega števila pridemo z enostavnim postopkom: začnemo s številom 1, prištejemo 1 in dobimo 2, spet prištejemo 1 in dobimo 3 itd. Rečemo lahko, da ima aditivna struktura v $\mathbb{N}$ en sam osnovni gradnik, število 1. Tesno povezana z aditivno strukturo v $\mathbb{N}$ je dobra urejenost te množice.

Po drugi strani je multiplikativna struktura množice $\mathbb{N}$ manj enostavna. Potrebujemo veliko osnovnih gradnikov – praštevil, da lahko vsako naravno število izrazimo kot njihov produkt. Že starogrški matematiki so vedeli, da za vsako naravno število $n \geq 2$ obstajajo takšna enolično določena praštevila $p_1 < \cdots < p_k$ in naravna števila $e_1, \ldots, e_k$, da je $n = p_1^{e_1} \cdots p_k^{e_k}$. Na tem *osnovnem izreku aritmetike* sloni Evklidov dokaz, da je praštevil neskončno mnogo. Idejo njegovega dokaza lahko uporabimo za konstrukcijo generatorja praštevil. Z generatorjem praštevil imamo v mislih postopek, ki nam ob ustreznih začetnih podatkih da eno ali več praštevil. Iz Evklidovega dokaza lahko izluščimo naslednji postopek za generiranje praštevil.