Hledání rekordně velkých prvočísel

L'ubomíra Dvořáková

lubomira.dvorakova@fjfi.cvut.cz

Abstrakt: Slyšeli jste už o Mersennových prvočíslech? Jsou to prvočísla tvaru $2p-1$, kde p samotné je také prvočíslo, a zajímal se o ně v 1. polovině 17. století francouzský mnich řádu minimů Marin Mersenne. Kromě svých vlastních výsledků v oblasti teorie čísel, v mechanice a optice má tento učenec ještě další obrovskou zásluhu. Zprostředkovával komunikaci významných evropských vědců: Reného Descartese, Pierra de Fermata, Christiana Huygense, Galilea Galileiho a dalších.

Mersenne se domníval, že $2p-1$ je prvočíslo pro $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$. Jelikož se jedná o rychle rostoucí čísla, nedivme se, že se v několika případech spletl a že mu naopak některá Mersennova prvočísla v seznamu chyběla.

Jistě víte, že hledání velkých prvočísel je obrovskou výzvou dneška, protože na násobení velkých prvočísel jsou založeny šifry chránící bezpečnost bankovních transakcí, soukromí naší elektronické komunikace či bezpečnost plateb přes internet.

Největší známá prvočísla jsou právě Mersennova. Je to z toho důvodu, že existuje Lucasův-Lehmerův test prvočíselnosti, který je velice rychlý. Obecně totiž platí, že úloha zjišťovat, zda dané číslo je prvočíslo, je časově velmi náročná. Pokud bychom nepoužili žádný rafinovaný algoritmus, pak je třeba vyzkoušet, zda je dané číslo n dělitelné všemi prvočísly menšími než $\sqrt{n}$.

Přednáška je určena zájemcům o teorii čísel a diskrétní matematiku. Jednoduše řečeno - těm, kteří se rádi dozvědí něco nového o vlastnostech prvočísel. Popíšeme si Mersennova prvočísla a Lucasův-Lehmerův test. Seznámíme se s internetovým projektem GIMPS - Great Internet Mersenne Prime Search, a kdo bude chtít, může se do projektu zapojit (a možná vyhrát odměny, které jsou na nalézání rekordně velkých prvočísel vypsány). V souvislosti s Mersennovými prvočísly si prozradíme něco o dokonalých číslech. Dále poznáme také Fermatova prvočísla. A neopomeneme ani Rabinův-Millerův test, který je zástupcem testů pravděpodobnostních a je hojně využívaný v praxi.