7. Proč vůbec hledáme velká prvočísla

Víme, že prvočísel je sice nekonečně mnoho, jak jsme však již uvedli, nejen že neznáme žádnou formuli, která by nám postupně umožňovala počítat všechna prvočísla, ale nemáme k dispozici dokonce ani formuli f(n), která by v přirozených číslech nabývala postupně (navzájem různých) prvočíselných hodnot, byť ne nutně všech. (Problémy spojené s hledáním takové formule jsme viděli v odstavci o Fermatových prvočíslech.)

Je však zřejmé, že hledání stále větších a větších prvočísel bylo pro matematiky od dávnověku intelektuální výzvou. Nemá smyslu se ptát, „k čemu bylo toto hledání dobré“. K čemu je „dobré“ malování obrazů, hraní šachů či zdolávání velehor? Konáme mnoho činností jen proto, že jsme **lidé** obdařeni intelektem a emocemi, kteří cítí -- alespoň někteří z nás -- vnitřní potřebu poznávat nepoznané, zdolávat nezdolané a sdělovat jiným své vidění světa, své myšlenky a obohacovat se navzájem. Každý z nás, kdo svůj život více či méně spojil s matematikou, proto dobře rozumí i v této oblasti pohnutkám našich předchůdců.

A jak už nám historie mnohokrát ukázala, ideje a teorie, které se zpočátku zdály jen intelektuální hříčkou bez hlubšího významu a bez praktického využití, se dříve či později ukázaly přínosné a často nepostradatelné v oborech, o nichž v době jejich vzniku nebylo a nemohlo být ani potuchy. Tak našla teorie grup užití ve fyzice či krystalografii, teorie kvaternionů v kosmonautice a mohli bychom jmenovat mnoho dalších příkladů. Podobný osud čekal i na zdánlivě zcela neužitečné hledání velkých prvočísel, která dnes nacházejí zásadní využití například v testování hardwaru a softwaru či v intenzívně se rozvíjející kryptografii.

O některých postupech matematiků dřívějších období, kdy ještě nebyla k dispozici výpočetní technika, se můžeme jen dohadovat. Již mnohokrát jsme se zmínili o některých obdivuhodných výsledcích FERMATA a EULERA. Fermat vyslovil, většinou bez důkazů, řadu pozoruhodných hypotéz, které o století později Euler dokázal. Mezi takové příklady patří například hypotéza, že

každé prvočíslo tvaru 4n+1, lze jednoznačně vyjádřit jako součet čtverců dvou přirozených čísel.

Euler dokázal, že uvedená podmínka je dokonce nutná a postačující k tomu, aby číslo tvaru 4n + 1 bylo prvočíslem. Je velmi pravděpodobné, že právě na základě tohoto poznatku Euler odvodil, že 1 000 009 není prvočíslo. Snadno lze ověřit, že

$$1\,000\,009 = 1\,000^2 + 3^2 = 235^2 + 972^2.$$

Hledání velkých prvočísel však v dobách, kdy ještě nebyla k dispozici výpočetní technika, rozhodně nebylo snadnou záležitostí. Vzhledem k tomu, že pro výpočet prvočísel není známa žádná zákonitost, začala být v průběhu staletí studována prvočísla jistých tvarů ve víře, že mezi nimi budou adepti na nově objevená prvočísla.

Již jsme se zmínili o tzv. **Mersennových** a **Fermatových** prvočíslech. (Připomeňme, že Mersennova prvočísla jsou prvočísla tvaru $2^p - 1$, Fermatova prvočísla mají tvar $2^{2^m}+1$.) Kromě nich jsou studovány ještě například následující skupiny prvočísel:

- **faktoriálová prvočísla** tvaru $n! \pm 1$
- **eukleidovská prvočísla** tvaru $2 \times 3 \times 5 \times \ldots \times p + 1$
- **prvočísla SOPHIE GERMAIN**, což jsou taková lichá prvočísla p, že $2p+1$ je rovněž prvočíslo
- **CULLENOVA prvočísla** tvaru $n \times 2^n+1$
- **WOODALLOVA prvočísla** tvaru $n \times 2^n - 1$aj.

O žádné z uvedených skupin dodnes nevíme, kolik prvočísel obsahuje, zda je konečná nebo nekonečná. Nejméně nadějná se jeví Fermatova prvočísla, o nichž jsme hovořili podrobně v minulém odstavci a mezi nimiž nebylo od 17. století objeveno žádné další.

Ve všech uvedených skupinách jsou však pomocí počítačů objevována stále další prvočísla. Pro zajímavost uveďme stav platný v březnu 1999.

Všechna níže uvedená čísla byla objevena v roce 1998, pouze rekordman v kategorii eukleidovských prvočísel byl nalezen již v r. 1993:

- faktoriálové prvočíslo $6\,917!-1$, které má 23 560 cifer
- eukleidovské prvočíslo $2\times 3 \times 5 \times 24\,029+1$
- prvočíslo Sophie Germain $72\,021\times 2^{23\,630} - 1$, které má 7 119 cifer
- Cullenovo prvočíslo $481\,899\times 2^{481\,899} + 1$ o 145 072 cifrách
- Woodallovo prvočíslo $151\,023 \times 2^{151\,023} - 1$, které má 45 468 cifer.
-

Všechny tyto výsledky však samozřejmě bylo možno získat pouze za zcela zásadní pomoci výkonných počítačů. Vraťme se tedy ještě krátce do epochy, kdy počítače k dispozici ještě nebyly. V té době byl pokrok v této oblasti velmi obtížný a pomalý. Již v minulém pokračování jsme uvedli, že největší prvočíslo ve své době nalezl EULER, když v r. 1772 dokázal, že prvočíslem je číslo

$$2^{31} - 1 = 2\,147\,483\,647.$$

tj. 31. Mersennovo prvočíslo.

Další pokrok přišel až po téměř 100 letech, když v r. 1867 našel LANDRY prvočíslo 3 203 431 780 337.

V r. 1876 nalezl FRANCOIS EDOUARD ANATOLE LUCAS (1842 -- 1891) prvočíslo $2^{127} - 1$, které má dokonce 39 cifer. Poslední pokrok v „předpočítačovém“ věku byl učiněn v r. 1951, kdy FERRIER našel prvočíslo $(2^{148}+1)/17$, které má 44 cifer.

Již v témže roce však bylo nalezeno pomocí počítače další prvočíslo o 79 cifrách a definitivně tak skončila éra samostatných počtářů, kteří pracovali v nejlepším případě s mechanickým počitadlem. Současně bylo čím dál jasnější, že nejvhodnějšími kandidáty na hledání velkých prvočísel jsou tzv. *Mersennova prvočísla*, o nichž jsme se již několikrát zmínili. Tato čísla dnes hrají ve sledované problematice centrální roli; proto se o nich v další části zmíníme podrobněji.