Velká prvočísla

Robert Káldy

Rozložení prvočísel na číselné ose

Definice. *Prvočíselná funkce $\pi(n)$ udává počet prvočísel menších než n.*

Je zřejmé, že prvočíselná funkce je neklesající a $\pi(n) < n$. Ze známého Euklidova důkazu nekonečného počtu prvočísel indukcí dostaneme $\pi(n) > \frac{\ln \ln n}{\ln 2}$. Tím dostáváme horní a dolní odhad prvočíselné funkce, ovšem zatím odhad velice hrubý. Na přednášce ukáži jemnější odhady zdola $\pi(n) > \ln n - 1$ a shora $\pi(n) < c \cdot \frac{n}{\ln \ln n}$, kde c je konstanta.

Přesnější omezení prvočíselné funkce učinil P. L. Čebyšev. Aproximoval ji funkcí $\frac{n}{\ln n}$. Ukázal, že existují konstanty $c_1 < 1 < c_2$, pro něž:

$$c_1 \cdot n/\ln n \leq \pi(n) \leq c_2 \cdot n/\ln n$$

Z tohoto výsledku například plyne, že ačkoliv jsou prvočísla rozložena mnohem řidčeji než přirozená čísla, řada jejich převrácených hodnot diverguje.

Konečný důkaz, že

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1$$

(tzv. *prvočíselnou větu*) dokázali v roce 1896 Hadamard a de la Vallée Poussin. Uvedu několik jejích zajímavých důsledků:

(1) Pro libovolná kladná reálná čísla $a < b$ existuje kladné reálné x_0 takové, že pro všechna $x > x_0$ existuje v intervalu (ax, bx) aspoň jedno prvočíslo.
(2) Pro libovolný sled číslic existuje prvočíslo, které tímto sledem začíná.
(3) Pro libovolné $x \in \mathbb{R}^+$ existuje posloupnost prvočísel $\{q_n\}$, pro níž $\lim_{n\to\infty} \frac{q_n}{n} = x$.

Prvočíselná dvojčata

Definice. *Prvočíselnými dvojčaty rozumíme dvojici prvočísel, jejichž rozdíl je* 2.

Kolem prvočíselných dvojčat zatím známe spíše hypotézy než dokázané věty. Například se pouze domníváme, že prvočíselných dvojčat je nekonečně mnoho. To je součástí mnohem obecnější Hypotézy H:

Hypotéza. (H) *Buďte $f_1(x)$, $f_2(x)$, ..., $f_k(x)$ ireducibilní polynomy s celočíselnými koeficienty, jejichž největší společný dělitel je 1. Pak existuje nekonečně mnoho*

přirozených čísel n, pro něž jsou všechna čísla $f_1(n),\ f_2(n),\ \ldots,\ f_k(n)$ prvočísla.

Největší známá prvočíselná dvojčata jsou čísla $570\,918\,348 \cdot 10^{5120} \pm 1$ objevená H. Dubnerem v roce 1994.

Mersennova čísla

Definice. *Mersennovo číslo je číslo tvaru $M_p = 2^p - 1$, kde p je prvočíslo.*

Proč se zajímáme zrovna o tato čísla? Protože pro čísla v takovémto tvaru lze najít relativně jednoduché podmínky, zda je prvočíslem či číslem složeným. Pokud je n složené číslo, lze jednoduše dokázat, že $2^n - 1$ je složené. Domníváme se, že Mersennových prvočísel je nekonečně mnoho, ale dokázáno to není. Nevíme ani, zda existuje nekonečně mnoho složených Mersennových čísel.

V následujícím odstavci nastíním jisté nutné podmínky pro Mersennova prvočísla a pro jejich dělitele.

Věta. (Malá Fermatova) *Je-li p prvočíslo, pak pro každé přirozené číslo a, které není dělitelné p je číslo $a^{p-1} - 1$ dělitelné p.*

Podobně jako velkou Fermatovu větu, vyslovil i tuto Fermat bez důkazu, ale později ji dokázal a zobecnil Euler.

Věta. (Eulerova) *Pro všechna vzájemně nesoudělná přirozená čísla a, n platí:*

$$n | a^{\varphi(n)} - 1,$$

kde $\varphi(n)$ je počet přirozených čísel menších než n nesoudělných s n.

Po dosazení $a = 2$ do malé Fermatovy věty dostaneme, že pokud q je prvočíselný dělitel M_p, pak je tvaru $q = 2kp + 1$, $k \in \mathbb{N}$.

Věta. (Gaussovo kritérium) *Budiž $q = 2Q + 1$ prvočíslo, a přirozené číslo, které není dělitelné q a $a_1,\ a_2,\ \ldots,\ a_Q$ všechna lichá přirozená čísla menší než q. Položme $r_i = aa_i \bmod q$, $i = 1,\ 2,\ \ldots,\ Q$ (tj. zbytky po dělení q) a nechť γ je počet sudých r_i. Pak*

$$q | a^Q - (-1)^\gamma.$$

Pro $a = 2$ lze ukázat, že všichni prvočíselní dělitelé Mersennových čísel jsou tvaru $8k \pm 1$, $k \in \mathbb{N}$.

Tato kritéria se používají při hledání prvočíselného rozkladu složených Mersennových čísel. Při zjišťování, zda je dané Mersennovo číslo prvočíslem, se užívá tzv. *Lucas-Lehmerův test*, který se opírá o následující větu:

Věta. *Budiž $\{s_i\}$ rekurentně definovaná posloupnost:*

$$s_1 = 4, \qquad s_{i+1} = s_i^2 - 2.$$

Mersennovo číslo M_p je prvočíslem právě tehdy, když M_p dělí s_{p-1}.

Protože pro velká p je člen s_{p-1} nepříjemně velké číslo i pro současné počítače, používáme místo $\{s_i\}$ upravenou posloupnost $\{r_i\}$ definovanou takto:

$$r_1 = 4, \qquad r_{i+1} = \left(r_i^2 - 2\right) \bmod M_p$$

Fermatova čísla

Definice. *Fermatovo číslo je číslo tvaru $F_n = 2^{2^n} + 1$ pro n přirozené.*

První čtyři Fermatova čísla jsou prvočísla. Pro $5 \leq n \leq 16$ je dokázáno, že F_n jsou složená, pro větší n to víme jen u některých. Nicméně zatím nebylo objeveno Fermatovo prvočíslo pro $n > 4$. Největší známé složené Fermatovo číslo je F_{1945}.

Vzhůru k nekonečnu

Tabulka vybraných objevů největších prvočísel:

Číslo	Rok objevu	Objevitel
M_{13}	1458	Regiomontanus
M_{19}	1588	Cataldi
M_{31}	1772	Euler
M_{127}	1876	Lucas
$(2^{148}+1)/17$	1951	Ferrier
$M_{2\,281}$	1952	Robinson (SWAC)
$M_{11\,213}$	1963	Gillies (Illiac 2)
$M_{44\,497}$	1979	Nelson, Slowinski (Cray 1)
$M_{216\,091}$	1985	Slowinski (Cray X-MP)
$M_{1\,257\,787}$	1996	Slowinski, Gage (Cray T94)
$M_{6\,972\,593}$	1999	Hajratwala, Woltman, Kurowski (GIMPS)