Hledání rekordně velkých prvočísel

Martina Bekrová, Gymnázium Trutnov
(to.zapomenu@gmail.com)
Ondřej Bouchala, Gymnázium Komenského, Havířov
(ondrej.bouchala@gmail.com)
David Krška, Gymnázium J. V. Jirsíka, České Budějovice
(david_krska@volny.cz)
Lukáš Vacek, Gymnázium Teplice
(luk6@atlas.cz)

Abstrakt:
Hledání velkých prvočísel je velkou výzvou dneška. Šifrovací systémy jsou založené na operacích s velkými prvočísly. Hodí se tedy umět generovat obrovská prvočísla, abychom zajistili bezpečnost bankovních transakcí, soukromí elektronické komunikace,... Cílem našeho projektu byly programy testující prvočíselnost. Zabývali jsme se jak přesnými testy, tak i tzv. pseudotesty a pravděpodobnostními testy.

1 Prvočíslo

Prvočíslo je takové přirozené číslo p, které má pouze dva dělitele: 1 a p. Jsou základními stavebními prvky všech čísel. V současné době se využívají především v kryptografii. Prvočísla, která byla dříve považována za hrátku číselných teoretiků, se tak v současnosti stala matematickým objektem s nejširším uplatněním.

Nekonečně mnoho prvočísel?

Prvočísel je nekonečně mnoho a existuje mnoho způsobů, jak toto tvrzení dokázat. Uvedeme si zde nejelegantnější důkaz: Eukleidův důkaz sporem pomocí kongruence.

Předpokládejme, že by existovalo největší prvočíslo p_n. Pokud však vezmeme všechna prvočísla $p_1, p_2, \dots, p_n$, vytvoříme jejich součin a přičteme k němu jedničku, dostaneme další prvočíslo (není dělitelné žádným z menších prvočísel):

$$p_1p_2\dots p_n + 1 \equiv 1 \pmod{p_1}$$
$$p_1p_2\dots p_n + 1 \equiv 1 \pmod{p_2}$$
$$\dots$$
$$p_1p_2\dots p_n + 1 \equiv 1 \pmod{p_n}$$

A přitom číslo $p_1p_2\dots p_n + 1$ je očividně větší než naše zvolené p_n. Máme tedy spor s volbou p_n. Neexistuje proto největší prvočíslo, takže je prvočísel nekonečně mnoho.

Tento důkaz byl prvním důkazem sporem v dějinách matematiky.

Eratosthenovo síto

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Nejznámějším algoritmem pro vyhledávání prvočísel je pravděpodobně Eratosthenovo síto. Je dílem Eratosthena z Kyrény, významného matematika, astronoma a geografa antického Řecka.

Prvočísla menší než např. 101 vyhledává tak, že postupně prochází přirozená čísla větší než 1 a menší než 101, a pokaždé když nějaké prvočíslo najde, vyškrtne všechny jeho násobky. Další číslo v pořadí bude tudíž také prvočíslem a znovu se tedy ze seznamu vyloučí jeho násobky. Opakováním tohoto postupu dostatečně dlouho získáme všechna prvočísla menší než 101.

Například v programovacím jazyce Haskell vypadá tento algoritmus takto:

```
sito (x:xs) = x:sito [a | a <- xs, a `mod` x /= 0]
prvocisla = sito [2..]
```

Funkce „sito“ vezme seznam přirozených čísel větších než 1 a vytvoří nový seznam tak, že odtrhne první prvek a rekurzivně se spustí na seznam a, který vznikl ze zbytku původního seznamu vybráním čísel, která nejsou dělitelná prvním prvkem.

Mersennova čísla

Marin Mersenne byl francouzský teolog, filozof, hudební teoretik
a duchovní otec Akademie věd.
Mersenovo číslo je takové číslo, pro které platí: $M_p = 2^p - 1$, kde p je prvočíslo. Číslu M_p, které je prvočíslo, se říká Mersennovo prvočíslo.
Je evidentní, že pokud M_p má být prvočíslem, pak i p musí být prvočíslem:

$2^{mn} - 1 = (2^m)^n - 1 = (2^m - 1)(1 + 2^m + 2^{2m} + \dots + 2^{(n-1)m})$.

Podle Mersenna je mezi čísly 2 a 257 jedenáct takových čísel, a to p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. Dnes již víme, že mu jich tam pár chybí a pár přebývá. Ve skutečnosti tento seznam vypadá takto: p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127. Dodnes je objeveno 47 Mersennových prvočísel, největší z nich, $2^{43112609} - 1$, má 12 978 189 cifer.

Posledních 13 bylo objeveno pomocí projektu GIMPS (http://www.mersenne.org/) - Great Internet Mersenne Prime Search. Na počítačích dobrovolníků běží program, který ověřuje, zda pro dané p je $2^p - 1$ prvočíslem. Electronic Frontier Foundation (EFF) vypsala velkou odměnu za nalezení obrovských dosud neznámých prvočísel.

Fermatova čísla

Fermatovo číslo je každé číslo ve tvaru $F_m = 2^{2^{\wedge}m} + 1$, kde m je přirozené číslo. V případě, že by bylo ve tvaru $2^{k2^{\wedge}m} + 1$, kde k je liché číslo, dalo by se rozepsat:

$2^{kl} + 1 = (2^l + 1)(2^{l(k-1)} - 2^{l(k-2)} + \ldots - 2^l + 1)$, kde $l = 2^m$, což je složené číslo.

Tato čísla byla objevena francouzským matematikem Pierrem de Fermatem. Fermat byl přesvědčen, že každé takové číslo je zároveň prvočíslo. Prvních pět Fermatových čísel: 3, 5, 17, 257, 65537 jsou skutečně prvočísla. Až později Leonhard Euler zjistil, že $F_5 = 4294967297 = 641 \cdot 6700417$ je číslo složené. Dnes je známo, že čísla F_5 až F_{32} jsou čísla složená. Další Fermatova čísla zatím nejsou otestována a dodnes není známo, zda je nekonečně mnoho Fermatových čísel.
Jedno z užití Fermatový čísel je určení, zda lze zkonstruovat pravidelný mnohoúhelník pouze pomocí pravítka a kružítka. Karl Fridrich Gauss zjistil, že pravidelný n-úhelník lze zkonstruovat tehdy a jen tehdy, když liché dělitele *n* jsou různá Fermatova čísla.

2 Metody testování prvočíselnosti

Pro určování prvočíselnosti daných čísel existuje mnoho způsobů. My jsme se zabývali přesnými testy, pseudotesty a pravděpodobnostními testy.

Přesné testy

Pod tímto označením se rozumí testy, které jsou schopny pro přirozená čísla rozhodnout s naprostou jistotou, zda je dané číslo prvočíslo či nikoliv. Bývají buď časově hodně náročné (Eratosthenovo síto) nebo fungují jen pro omezenou množinu čísel (Lucas-Lehmerův test pro Mersennova čísla a Pépinův test pro Fermatova čísla).

Lucas-Lehmerův test

Pro zjišťování, zda je Mersennovo číslo prvočíslem, se používá Lucas-Lehmerův test. Vytvoříme posloupnost začínající číslem 4, další členy určíme podle vzorce:

$y_{(k+1)} = y_k^2 - 2$.

Mersennovo číslo je prvočíslem právě tehdy, když je dělitelem čísla $y_{(p-1)}$.

Tento algoritmus má asymptotickou složitost $O(p^2 \log p \log\log p)$. Je tedy rychlejší než všechny ostatní testy, a to včetně pravděpodobnostních. Dá se ovšem použít jen na Mersennova prvočísla. Lucas objevil (tímto testem) největší prvočíslo M_{127} bez použití počítače a Lehmer jako první prováděl numerické výpočty.

Pépinův test

Pro testování Fermatových prvočísel se používá Pépinův test. Tento test objevil francouzský matematik Pépin v roce 1877. Pépin zjistil, že platí pro základ 5. Později si Lukas všiml, že platí i pro základ 3. Test vypadá následovně:

Fermatovo číslo je prvočíslem právě tehdy, když platí:

$3^{((Fm-1)/2)} \equiv -1 \pmod{F_m}$, kde m je přirozené číslo.

Wilsonův test

Wilsonův test je další z řady přesných testů, které mohou s jistotou říci, že je dané číslo prvočíslem. Je však nepraktický pro aplikaci na počítači, protože počítání faktoriálu je časově náročné. Využívá se hlavně v důkazech.

Pro každé přirozené číslo p platí:

$p \geq 2$ je prvočíslo právě tehdy, když $(p - 1)! \equiv -1 \pmod{p}$.

Lze ho zjednodušit, pokud můžeme dané číslo p rozložit: $p = 4k + 1$. Pro takové prvočíslo p platí, že $((p - 1)/2)!)2 \equiv -1$. Již ale nelze implikaci otočit, tj. pokud podmínka $((p - 1)/2)!)2 \equiv -1$ platí, nelze z toho usoudit, že p je prvočíslo. Víme jen, že pokud tato podmínka neplatí, určitě p prvočíslem není. Tímto se dostáváme k tzv. pseudotestům – testům, které nám s jistotou neřeknou, jestli je číslo prvočíslem, jen případně potvrdí, že je číslem složeným.

Pseudotesty

Pseudotesty jsou testy, které nám dokážou s jistotou říci, že dané číslo je složené, ale nepotvrdí nám, že je to prvočíslo.

Fermatův test

Pierre de Fermat byl francouzský právník a matematikou se zabýval pouze ve svém volném čase. I přes to však byl významným odborníkem v teorii čísel – vymyslel Velkou a Malou Fermatou větu, je považován za jednoho ze zakladatelů teorie pravděpodobnosti a předchůdce diferenciálního počtu.

Fermatův test prvočíselnosti vychází z Malé Fermatovy věty:

$a^{p-1} \equiv 1 \pmod{p}$ (kde p je prvočíslo a a je přirozené číslo nesoudělné s p).

Když chceme zjistit, jestli je p prvočíslo, bereme různá a a zkoušíme, zda pro ně platí Malá Fermatova věta. Opět nemůžeme s jistou potvrdit, že dané p je prvočíslo, ale když podmínka neplatí, víme, že p prvočíslo není. Existují totiž Carmichaelova čísla, pro která platí Malá Fermatova věta, ačkoli to nejsou prvočísla. Například když:

$q = 6m + 1$, $r = 12m + 1$, $s = 18m + 1$,

pak qrs je Carmichaelovo číslo.

Pravděpodobnostní testy

Tyto testy jsou méně časově náročné (polynomiální v čase), ale jejich výsledek opět není stoprocentní.

Miller-Rabinův test

Tento test vytvořila dvojice počítačových vědců Gary Lee Miller a Michael Oser Rabin. Gary Miller je profesorem na univerzitě v Pittsbourghu. V roce 2003 byl oceněn v Paříži cenou Paris Kanellakis Award za Miller-Rabinův test. Michael Rabin se narodil roku 1931 v Německu. Po druhé světové válce odešel do Polska, kde žije i v současnosti. Za svůj dlouhý život se účastnil velkého množství projektů a dostal spoustu ocenění. Mezi nejcennější patří Turing Award z roku 1976 za dokument "Finite Automata and Their Decision Problem."

Základem Miller-Rabinova testu je, že pokud zapíšeme $p - 1 = 2^s d$, kde p je prvočíslo a d liché číslo, pak pro každé přirozené číslo $a < p$ platí buď:

$a^d \equiv 1 \pmod{p}$,

nebo:

$a^{d2^{\wedge}r} \equiv -1 \pmod{p}$, kde $0 \leq r \leq s - 1$.

V algoritmu si nejdříve vybereme náhodné $a < p$ a otestujeme podmínky z věty. Pokud podmínky věty neplatí, pak je číslo p složené. Jestliže však podmínky věty platí, vyberu si další a.

Příklad: Budeme počítat s číslem $p = 49$

$p - 1 = 48 \rightarrow 48 = 2^4 \cdot 3 \rightarrow s = 4, d = 3$

Jako a si zvolíme číslo 3

$3^3 = 27 \rightarrow 27 \bmod 49 = 27 \rightarrow 27 \neq 1$ nebo $-1 \bmod 49$

$3^{2 \cdot 3} = 729 \rightarrow 729 \bmod 49 = 43 \rightarrow 43 \neq -1 \bmod 49$

$3^{4 \cdot 3} \bmod 49 = 36 \rightarrow 36 \neq -1 \bmod 49$

$3^{8 \cdot 3} \bmod 49 = 22 \rightarrow 22 \neq -1 \bmod 49$

Číslo 49 je číslo složené, a proto se nejedná o prvočíslo.

Pravděpodobnost, že pro p složené test n-krát neodhalí neprvočíselnost p, je $1/4^n$. Proto si při dostatečném počtu opakování testu můžeme být s libovolně velkou pravděpodobností jisti, že testované číslo p je prvočíslo.

3 Shrnutí

Seznámili jsme se s novými testy prvočíselnosti a projektem GIMPS, který umožňuje každému zapojit se do hledání rekordně velkých prvočísel. Podařilo se nám naprogramovat všechny zmiňované testy prvočíselnosti a programy otestovat na prvočíslech do 150 000. Můžete je najít na: tigr.fjfi.cvut.cz v sekci Pro střední školy.

4 Poděkování

Slečně Ing. Ľubomíře Balkové a panu Ing. Štěpánu Starostovi, kteří si s námi dali tu práci a seznámili nás s problematikou prvočísel, a samozřejmě také panu Ing. Vojtěchu Svobodovi, CSc. A celému organizačnímu týmu Týdne vědy. Děkujeme i vám čtenářům, že jste našemu článku věnovali svou pozornost.

Reference:

[1] Crandall, R. – Pomerance, C.: Prime Numbers, A Computational Perspective Springer, 2005

[2] KŘÍŽek, M. - Sommer, L. - ŠolcovÁ, A.: Kouzlo čísel Galileo, 2009