

Prvočísla

prof. RNDr. Miroslav Vlček, DrSc.

vlcek@fd.cvut.cz

25. října 2007

Prvočísla

1. Co jsou to prvočísla?
2. Kolik je prvočísel?
3. Proč prvočísla ?
4. Mersenneova čísla a prvočísla
5. Prvočísla a Fermatova čísla
6. Problém faktorizace Fermatových čísel

Co jsou to prvočísla?

- prvočísla - definice
- základní stavební kameny - atomy číselné řady
- prvočíselné rozklady

$$143 = 11 \times 13$$

$$897 = 3 \times 13 \times 23$$

⋮

- Eratosthenovo síto pro vyhledání prvočísel

1	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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Uměli byste pokračovat dál?...

Kolik je prvočísel?

- označme $\pi(N)$ počet prvočísel $\leq N$
- v desítce čísel je $\pi(10) = 5$ prvočísel, tedy
$$\varrho_N = \frac{\pi(N)}{N} = \frac{5}{10} = 0.5$$
- ve stovce čísel je $\pi(100) = 24$ prvočísel, tedy
$$\varrho_N = \frac{\pi(N)}{N} = \frac{24}{100} = 0.24$$
- v tisícovce čísel je $\pi(1000) = 168$ prvočísel, tedy
$$\varrho_N = \frac{\pi(N)}{N} = \frac{168}{1000} = 0.168$$

Tabulka hustotot prvočísel

N	10	10^2	10^3	10^4	10^5	10^6
ϱ_N	0.500	0.240	0.168	0.123	0.096	0.078

V roce 1792 si mladý K.F. Gauss (bylo mu 15 let) povšiml, že hustota prvočísel je přibližně rovna $\varrho_N \approx \frac{N}{\ln(N)}$.

Vyslovil domněnku, že se nejedná o náhodný jev a že při dostatečně velkém N je hustota $\varrho_N \cong \frac{N}{\ln(N)}$ s libovolnou přesností. Důkaz tohoto tvrzení přišel až o 100 let později.

Výsledek

$$\lim_{N \rightarrow \infty} \frac{\varrho_N}{\frac{N}{\ln(N)}} = 1$$

se nazývá **prvočíselná věta**.

Co ještě víme o prvočíslech ?

- prvočísel je nekonečně mnoho - Eukleidův důkaz
- Předpokládejme, že existuje největší prvočíslo a označme jej p_M
- Sestrojíme součin všech prvočísel až do p_M

$$N = 2 \times 3 \times 7 \times \cdots \times p_M = \prod_{i=1}^M p_i$$

- Číslo $N+1$ není dělitelné ani jedním z prvočísel p_i , která jsou děliteli čísla N , jinak také

$$N + 1 \equiv 1 \pmod{p_i}$$

- To znamená, že $N + 1$ je buď prvočíslo, nebo složené číslo, které ve svém rozkladu

má jiné prvočíslo $p_N > p_M$. Spolu s Eukleidem jsme dospěli ke sporu !

- prvočísel je nekonečně mnoho
- Klasický existenční důkaz
- Takový důkaz neřeší otázku jak nalézt všechna prvočísla
- Eukleidova čísla definovaná rekurencí

$$e_n = e_1 e_2 e_3 \dots e_{n-1} + 1$$

- První čtyři Eukleidova čísla

$$e_1 = 1 + 1 = 2$$

$$e_2 = 2 + 1 = 3$$

$$e_3 = 2 \times 3 + 1 = 7$$

$$e_4 = 2 \times 3 \times 7 + 1 = 43$$

(1)

jsou **prvočísla**. Další Eukleidova čísla až na **e_6**

$$e_5 = 2 \times 3 \times 7 \times 43 + 1 = 1807 = 13 \times 139$$

$$\mathbf{e_6} = 2 \times 3 \times 7 \times 43 \times 1807 + 1 = 3263443$$

$$e_7 = 547 \times 607 \times 1033 \times 31051$$

$$e_8 = 29881 \times 67003 \times 9119521 \times 6212157481$$

jsou **složená čísla**. Pro všechna další čísla $e_9 \dots e_{17}$ je dokázáno, že jsou složená čísla.

- Eukleidova čísla jsou **nesoudělná čísla** (relative prime) protože jejich největší společný dělitel je roven 1

$$\gcd(e_m, e_n) = 1$$

- Goldbachova hypotéza - každé sudé číslo větší než 2 lze vyjádřit jako součet dvou prvočísel, například

$$8 = 3 + 5$$

$$10 = 3 + 7$$

$$12 = 5 + 7$$

$$14 = 3 + 11$$

$$16 = 5 + 11$$

$$18 = 7 + 11$$

(2)

Experimentálně prověřeno do hodnot 2×10^{17}

Proč prvočísla ?

- Příběh párových prvočísel (např. 17 a 19,...), největší dosud známé prvočíselné páry jsou

$$16869987339975 \times 2^{171960} \pm 1$$

$$100314512544015 \times 2^{171960} \pm 1$$

- Příběh, ve kterém pošetilý matematik natchytl firmu INTEL při předstírání, že chyba Pentia neexistuje (1995)
- Thomas Nicely, Lynchburg College, Virginia

harmonická řada $\sum_{n=1}^{\infty} \frac{1}{n} \rightarrow \infty$

prvočíselná harmonická řada $\sum_{\forall p}^{\infty} \frac{1}{p} \rightarrow \infty$

divergují

- avšak harmonická řada s párovými prvočísly

$$\sum_{\forall p_2}^{\infty} \frac{1}{p_2} = \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots + \frac{1}{29} + \frac{1}{31} + \dots$$

konverguje $\rightarrow$ 1.902160583104

- Zde nastupuje experimentální matematika

- Thomas Nicely (1996) obdržel hodnotu

$\rightarrow$ 1.9021605778

a objevil chybu v CPU Pentia

- rozšířil svoje podezření pomocí internetu a odezva byla jednoznačná, aritmetická jednotka Pentia je chybné

- Tim Coe, Vitesse Semiconductor, Southern California

$$c = \frac{4195835}{3145727} = \frac{5 \times 7 \times (2^3 \times 3^4 \times 5 \times 37 + 1)}{3 \times 2^{20} - 1} = \\ = 1.33382044 \dots$$

- Pentium procesor však dával hodnotu

$$c = \frac{4195835}{3145727} = \frac{5 \times 7 \times 119881}{13 \times 241979} = 1.33373906 \dots$$

- chyba při reprezentaci čísel typu

$$M_n = 2^n - 1$$

tzv. Mersenneova čísla

- Marin Mersenne (1588-1648) uveřejnil ve své knize Cogitata Physica-Mathematica (1644), že čísla tvaru

$$2^n - 1$$

jsou prvočísky pro

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

a jsou čísla složená pro ostatní přirozená čísla $n \leq 257$.

- Definice: Jestliže $2^n - 1$ je prvočíslo, pak se nazývá Mersenneovo prvočíslo.
- Nebylo snadné dokázat prvočíselný charakter Mersennových čísel. V roce 1750 dokázal Euler, že $2^{31} - 1$, je prvočíslo.
- V roce 1876, Lucas ověřil, že $2^{127} - 1$ je prvočíslo.

- Sedm let později Pervouchine ukázal, že $2^{61} - 1$ je také prvočíslo, které Mersenne neuváděl.
- V počátku 20. století Powers ukázal, že existují další čísla, která Mersenne neuvedl jako prvočísla $2^{89} - 1$ a $2^{107} - 1$.
- Nakonec v roce 1947 Mersenneův interval, $n \leq 257$, byl úplně prozkoumán a bylo dokázáno, že správné tvrzení obsahuje 12 exponentů :

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127.$$

- V současné době je známo, že existuje dalších 32 Mersennových prvočísel s celočíselnými exponenty

$$n = 521, 607, 1279, 2203, 2281, \dots$$

Poslední 44. Mersenneovo číslo bylo nalezeno 4. září 2006 ve tvaru

$$2^{32582657} - 1$$

Prvočísla a Fermatova čísla

Pro nezáporné $n \geq 0$ nazýváme výraz

$$F_n = 2^{2^n} + 1$$

Fermatovým číslem.

Je známo, že F_n je **prvočíslem** pro

$$0 \leq n \leq 4$$

a **číslo složené** pro

$$5 \leq n \leq 23.$$

Fermat se původně domníval, že F_n jsou obecně prvočísla.

Faktorizace Fermatových čísel

- V roce 1732 Euler našel rozklad Fermatova čísla

$$F_5 = 641 \times 6700417 = 4294967297.$$

- Žádné další prvočíslo tvaru $F_n = 2^{2^n} + 1$ není pro $n \geq 24$ známo.
- Dějiny rozkladu Fermatových čísel se od doby Eulera staly velkou soutěží o vhodné algoritmy a μ -kosmos numerické matematiky.
- Protože F_n roste v počtu cifer závratně rychle, algoritmus, který lze uplatnit pro faktorizaci F_n nemusí platit pro F_{n+1} .

Faktorizace Fermatových čísel - F_6 a F_7

- V roce 1880 Landry zveřejnil součin

$$F_6 = 274177 \times p_{14}$$

Algoritmus, kterým Landry k tomuto výsledku dospěl, nebyl nikdy publikován.

- V roce 1970 Morrison a Brillhart našli pomocí metod řetězových zlomků součin

$$F_7 = 59649589127497217 \times p_{22}$$

- V letech 1877 - 1970 bylo objeveno několik nevelkých součinitelů Fermatových čísel ve tvaru $k \times 2^{n+2} + 1$ pro $n \geq 9$.

- Například již v roce 1903 Western našel pro

$$F_9 = 2424833 \times C_{148},$$

kde C_{148} je celé 148-ciferné číslo.

Faktorizace Fermatových čísel - F_8 a F_9

- V roce 1980 Brent a Pollard našli součin

$$F_8 = 1238926361552897 \times p_{62}$$

Pollardova ρ -metodou.

- V roce 1990 skupina matematiků a počítačových odborníků kolem Pollarda použila více než 700 pracovních stanic rozmístěných po celém světě a odvodili metodou, která nese jméno "special number field sieve" (SNFS) pro

$$F_9 = 2424833 \times p_{49} \times p_{99}.$$

Faktorizace Fermatových čísel - současnost

- V říjnu 2003 John Cosgrave se spolupracovníky na St. Patrick's College našli součinitele

$$3 \times 2^{2478785} + 1$$

Fermatovu číslu $F_{2478782}$.

- Ne všechna Fermatova čísla, o kterých víme, že jsou rozložitelná, mají kompletní faktorizaci. Již například pro F_{12} není znám součinitel C_{1187} o velikosti 1187 cifer.
- Podobně pro F_{13} , F_{15} , F_{16} , F_{17} , F_{18} , F_{19} , F_{21} a F_{23} chybí součinitele různých ciferných délek.

Faktorizace Fermatových čísel - přehled

n	$F_n = 2^{2^n} + 1$
0	3
1	5
2	7
3	257
4	65537
5	641×6700417
6	$274177 \times 67280421310721$
7	$59649589127497217 \times$ $\times 5704689200685129054721$
8	$1238927497217 \times p_{62}$
9	$2424833 \times p_{49} \times p_{99}$

V tabulce označuje p_k k-ciferné prvočíslo. Například

$$F_6 = 274177 \times 67280421310721 = 274177 \times p_{14}$$

Pro rozklad velkých čísel na prvočíselné součinitele se používají celočíselné vlastnosti eliptických křivek

$$y^2 = x^3 + ax + b$$

Na stránkách

<http://www.alpertron.com.ar/ECM.HTM>

můžete ověřit účinnost těchto matematických metod.

