Prvočísla, dělitelnost

Matematické algoritmy (K611MAG)

Jan Přikryl, Miroslav Vlček

2. přednáška 11MAG
úterý 2. října 2012

verze: 2012-10-10 15:47

1 Prvočísla

Známe dvě skupiny přirozených čísel $n \in \mathbb{N}$.

Prvočíslo

Prvočíslem nazýváme takové přirozené číslo $n \in \mathbb{N}$, které je *beze zbytku dělitelné právě dvěma různými přirozenými čísly* a to jedničkou a samo sebou.

Číslo 1 tedy není prvočíslo.

Číslo složené

Celé číslo různá od jedné, jež není prvočíslem, nazýváme **složené číslo**.

Vlastnosti prvočísel:

- Pro prvočíslo p platí $p \,|\, a \cdot b \;\Rightarrow\; (p \,|\, a) \vee (p \,|\, b)$.
- Každé složené číslo lze jednoznačně vyjádřit jako součin prvočísel.
  Příklad 1. ¡2-¿[Vzorový rozklad] Například $42 = 2 \cdot 21 = 2 \cdot 3 \cdot 7$.
- Pokud p je prvočíslo a $a \in \mathbb{Z} :\; 0 < a < p$, pak $p \,|\, (a^p - a)$.
- Ke všem celým kladným číslům $a \in \mathbb{Z} : a > 0$ lze nalézt prvočíslo $p : a < p \leq 2a$.
  Příklad 2. ¡4-¿ Nechť $a = 42$. Nerovnici $p : 42 < p \leq 84$ splňují prvočísla 43, 47, 53, 59, 61, 67, 71, 73, 79, a 83.

Uměli byste pokračovat dál?

Označme $\pi(N)$ počet prvočísel $\leq N$.

Počítejme zkusmo hustotu prvočísel ϱ_N v intervalu $\langle 1, N \rangle$:

- v desítce čísel je $\pi(10) = 4$ prvočísla, tedy

$$\varrho_{10} = \frac{\pi(10)}{10} = \frac{4}{10} = 0{,}4$$

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

Tabulka 1: Seznam prvočísel (vyznačena červeně) od 2 do 120.

- ve stovce čísel je $\pi(100) = 25$ prvočísel, tedy

$$\varrho_{100} = \frac{\pi(100)}{100} = \frac{25}{100} = 0{,}25$$

- v tisícovce čísel je $\pi(1000) = 168$ prvočísel, tedy

$$\varrho_{1000} = \frac{\pi(1000)}{1000} = \frac{168}{1000} = 0{,}168$$

V roce 1792 si mladý C. F. Gauss všiml, že $\pi(N)$ je přibližně rovna podílu $N/\ln N$.

N	10	10^2	10^3	10^4	10^5	10^6
ϱ_N	0,400	0,250	0,168	0,123	0,096	0,078
$1/\ln N$	0,434	0,217	0,145	0,108	0,086	0,072
$N/\ln N$	4,3429	21,715	144,76	1085,7	8685,9	72382
$\pi(N)$	4	25	168	1229	9592	78498

Matematici někdy píší, že

$$\pi(N) \sim \frac{N}{\ln N}$$

a říkají, že $\pi(N)$ se **asymptoticky blíží** k $N/\ln N$.

Proposition 3. *Nejedná se o náhodný jev, při dostatečně velkém N je hustota prvočísel v intervalu $\langle 1, N \rangle$ rovna*

$$\lim_{N\to\infty} \varrho_N = \frac{1}{\ln N}$$

Gaussovi bylo tehdy patnáct let. Důkaz tohoto tvrzení přišel až o 100 let později.

Definice 4 (Prvočíselná věta)**.**

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

1.1 Vlastnosti prvočísel

Prvočísel je nekonečně mnoho:

- Předpokládejme, že existuje největší prvočíslo a označme jej p_M

- Sestrojíme součin všech prvočísel až do p_M:

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

- Číslo $N+1$ nemůže být dělitelné ani jedním z prvočísel p_i, jež dělí N.
- To znamená, že $N+1$ je buď *prvočíslo*, nebo *číslo složené*, jež má ve svém rozkladu jiné prvočíslo $p_N > p_M$.
- Spolu s Eukleidem jsme dospěli ke sporu!
- Musí tedy platit, že *prvočísel je nekonečně mnoho.*

Eukleidův důkaz je klasický existenční důkaz: Řeší pouze otázku existence nekonečné množiny prvočísel, neřeší otázku jak nalézt všechna prvočísla.

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

$$\begin{aligned} 8 &= 3+5 \\ 10 &= 3+7 \\ 12 &= 5+7 \\ 14 &= 3+11 \\ 16 &= 5+11 \\ 18 &= 7+11 \end{aligned}$$

Experimentálně prověřeno do hodnot 2×10^{17}

1.2 Zajímavosti

Párová prvočísla: jejich rozdíl je 2 (například 17 a 19), největší dosud známé prvočíselné páry jsou

$$\begin{aligned} 16\,869\,987\,339\,975 &\cdot 2^{171960} \pm 1 \\ 100\,314\,512\,544\,015 &\cdot 2^{171960} \pm 1 \end{aligned}$$

Odhalení chyby matematického koprocesoru originálního Intel Pentium P5 (*The Intel FDIV Bug*).

Thomas Nicely, Lynchburg College, Virginia (1994): Numerický výpočet součtu *harmonické řady s párovými prvočísly.*

O jaké řady jde:

- harmonická řada

$$\sum_{n=1}^{\infty} \frac{1}{n} \to \infty$$

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

Obě tyto řady divergují.

Oproti tomu

$$\begin{aligned}\sum_{\forall p_2}^{\infty} \frac{1}{p_2} &= \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots + \frac{1}{29} + \frac{1}{31} + \ldots \\ &= 1{,}902160583104\end{aligned}$$

konverguje.

V červnu 1994 Thomas Nicely obdržel po povýšení starého počítače na P5 hodnotu

$$1{,}9021605778$$

lišící se od původních výpočtů na i486 – a v říjnu oznámil chybu v FPU Pentia.

Tim Coe, Vitesse Semiconductor, Southern California

$$\begin{aligned}c &= \frac{4195835}{3145727} = \frac{5 \cdot 7 \cdot (2^3 \cdot 3^4 \cdot 5 \cdot 37 + 1)}{3 \cdot 2^{20} - 1} = \\ &= 1{,}33382044\ldots\end{aligned}$$

FPU v Pentiu P5 však dávala hodnotu

$$c = \frac{4195835}{3145727} = \frac{5 \times 7 \times 119881}{13 \times 241979} = 1{,}33373906\ldots$$

Chyba nastává při reprezentaci čísel typu $M_n = 2^n - 1$, což jsou tak zvaná *Mersennova čísla*.

1.3 Mersennova čísla

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

$$2^n - 1$$

jsou prvočísly 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 5 (Mersennovo prvočíslo)**.** Jestliže $2^n - 1$ je prvočíslo, pak se nazývá **Mersennovo prvočíslo**.

Lze dokázat, že pokud je $2^n - 1$ prvočíslo, je i n prvočíslem.

Prvočíselný charakter Mersennových čísel nebylo snadné dokázat:

- Euler (1750): $2^{31} - 1$ je prvočíslo.
- Lucas (1876): $2^{127} - 1$ je prvočíslo.

- Pervouchine (1883): Mersenne zapomněl na $2^{61} - 1$.
- Powers (?) ukázal, že existují další čísla, která Mersenne neuvedl: $2^{89} - 1$ a $2^{107} - 1$.

Mersennův interval $n \leq 257$ byl úplně prozkoumán v roce 1947 a bylo dokázáno, že správné tvrzení obsahuje 12 exponentů:

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

K dnešnímu dni bylo nalezeno celkem 47 Mersennových prvočísel $M_{521}, M_{607}, M_{1\,279}, \ldots, M_{42\,643\,801}, M_{43\,112\,609}$. Čísla ovšem nejdou popořadě, k dnešnímu dni víme pouze, že známe prvních 41 Mersennových prvočísel.

Příklad 6 (**GIMPS** (The Great Internet Mersenne Prime Search)). Paralelizované hledání jehly v kupce sena:

- Distribuovaný výpočet ve volných cyklech procesoru
- Zatím poslední nalezené Mersennovo prvočíslo má 12837064 cifer a bylo nalezeno 12. dubna 2009 ve tvaru
$$2^{42\,643\,801} - 1.$$
- Zatím největší bylo nalezeno 23. srpna 2008 ve tvaru
$$2^{43\,112\,609} - 1.$$
- `http://www.mersenne.org/`

1.4 Fermatova čísla

Pro nezáporné $n \geq 0$ nazýváme n-tým **Fermatovým číslem** výraz

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

Je známo, že F_n je

- prvočíslem pro $0 \leq n \leq 4$ a
- číslem složeným pro $5 \leq n \leq 23$.

Fermat se původně domníval, že F_n jsou obecně prvočísla.

Jak vlastně rozhodneme, na jaké součinitele rozložit složené číslo N?

1.5 Faktorizace prvočísel

Definice 7 (Základní věta artimetiky)**.** Každé přirozené číslo větší než 1 lze jednoznačně rozložit na součin prvočísel.

Nalezení rozkladu malých čísel na prvočísla je relativně jednoduché:

Zkouška dělením

Pro výpočet prvočíselných součinitelů čísla N stačí otestovat všechna prvočísla $p_i < \sqrt{N}$. Prvočinitele získáme například použitím Eratosthenova síta.

Náročnost faktorizace *výrazně roste s délkou* prvočísla.

Praktické důsledky:

- (+) kryptografie (šifrování veřejným klíčem, RSA),

Metody prosévání:

- Eratosthenovo síto
- (Generické—Speciální) prosévání číselného pole
- Pollardova ρ-metoda
- Rozklad na řetězové zlomky

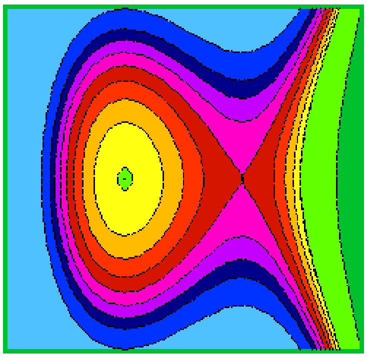
Pro rozklad velkých čísel na prvočíselné součinitele se používají celočíselné vlastnosti eliptických křivek

$$y^2 = x^3 + a\,x + b$$

Na stránkách

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

můžete ověřit účinnost těchto matematických metod.



- Euler (1732) nalezl rozklad

$$F_5 = 641 \cdot 6\,700\,417 = 4\,294\,967\,297.$$

- Žádné další prvočíslo tvaru $F_n = 2^{2^n} + 1$ není pro $n \geq 24$ známo.

Dějiny faktorizace

Rozklad Fermatových čísel se od doby Eulera stal velkou soutěží o vhodné algoritmy.

Samostatný mikrokosmos numerické matematiky: F_n roste v počtu cifer závratně rychle – algoritmus vhodný pro faktorizaci F_n nemusí být použitelný pro F_{n+1}.

V roce 1880 Landry zveřejnil součin

$$F_6 = 274\,177 \cdot p_{14}.$$

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

V roce 1970 Morrison a Brillhart nalezli pomocí metod řetězových zlomků součin

$$F_7 = 59\,649\,589\,127\,497\,217 \cdot p_{22}.$$

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

Western, 1903

Například již v roce 1903 Western nalezl

$$F_9 = 2\,424\,833 \times C_{148},$$

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

V roce 1980 Brent a Pollard nalezli součin

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

Pollardovou 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 SNFS (Special Number Field Sieve) pro

$$F_9 = 2\,424\,833 \times p_{49} \times p_{99}.$$

V říjnu 2003 John Cosgrave se spolupracovníky na St. Patrick's College nalezli součinitele Fermatova číslu

$$F_{2478782} = (3 \times 2^{2478785} + 1) \cdot k.$$

Faktorizace:

- není kompletní pro všechna Fermatova čísla, o kterých víme, že jsou rozložitelná (F_1 až F_{32}),
- například pro F_{12} není znám součinitel C_{1187} o velikosti 1187 cifer,
- podobně pro $F_{13}, F_{15}, \ldots, F_{19}, F_{25}, \ldots, F_{32}$ chybí součinitele různých ciferných délek,
- pro $F_{20}, \ldots, F_{24}$ součinitele neznáme vůbec.

n	$F_n = 2^{2^n} + 1$
0	3
1	5
2	7
3	257
4	65 537
5	$641 \cdot 6\,700\,417$
6	$274\,177 \cdot 67\,280\,421\,310\,721$
7	$59\,649\,589\,127\,497\,217 \cdot 5\,704\,689\,200\,685\,129\,054\,721$
8	$1\,238\,927\,497\,217 \cdot p_{62}$
9	$2\,424\,833 \cdot p_{49} \cdot p_{99}$

V tabulce označuje p_k k-ciferné prvočíslo. Například $F_6 = 274\,177 \cdot 67\,280\,421\,310\,721 = 274\,177 \cdot p_{14}$.

Euklidova čísla

Čísla definovaná rekurencí

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

nazýváme **Euklidova čísla**.

První čtyři Euklidova čísla

$$\begin{aligned} e_1 &= 1 + 1 = 2 \\ e_2 &= 2 + 1 = 3 \\ e_3 &= 2 \times 3 + 1 = 7 \\ e_4 &= 2 \times 3 \times 7 + 1 = 43 \end{aligned}$$

jsou *prvočísla.*

Další Euklidova čísla až na e_6

$$
\begin{aligned}
e_5 &= & 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1\,807 = 13 \cdot 139 \quad (1)\\
e_6 &= & 2 \cdot 3 \cdot 7 \cdot 43 \cdot 1\,807 + 1 = 3\,263\,443 \quad (2)\\
e_7 &= & 547 \cdot 607 \times 1\,033 \cdot 31\,051 \quad (3)\\
e_8 &= & 29\,881 \cdot 67\,003 \cdot 9\,119\,521 \cdot 6\,212\,157\,481 \quad (4)
\end{aligned}
$$

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

Fakt 8. *Euklidova čísla jsou **nesoudělná čísla**, protože jejich největší společný dělitel je roven 1:*

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

2 Nejvyšší společný dělitel

V celočíselné aritmetice dělíme se zbytkem: je

$$a = qb + r.$$

Pro dvojici celých čísel a a b má smysl hledat nejvyšší celé číslo d, které obě čísla dělí beze zbytku.

Nejvyšší společný dělitel

Nejvyšší společný dělitel dvou nenulových celých čísel $a \in \mathbb{Z}$ a $b \in \mathbb{Z}$ je největší nenulové přirozené číslo $d \in \mathbb{Z} - 0$ takové, že $d|a \wedge d|b$.

Zapisujeme $\gcd(a, b) = d$.

Nesoudělná čísla

Čísla $a \in \mathbb{Z}$ a $b \in \mathbb{Z}$ nazýváme **nesoudělná** *(relative primes)*, pokud $\gcd(a, b) = 1$.

2.1 Euklidův algoritmus

Původně formulován geometricky cca 300 př.n.l. Eukleidés hledal nejdelší úsečku, která by se beze zbytku vešla do dvou delších úseček.

Důkaz

1. Nechť a a b jsou nenulová celá čísla, jejichž gcd() počítáme.
2. Pokud $a > b$, platí $a = qb + r$.
3. Pokud existuje d takové, že $d|a$ a $d|b$, pak také $d|r$, protože pro $a = sd$ a $b = td$ bude $r = (s - qt)d$.
4. Je tedy $\gcd(a, b) = \gcd(b, r)$ a stačí tedy hledat $\gcd(b, r)$.
5. Protože $r < b$, výpočet v konečném počtu kroků skončí stavem $r = 0$.

3 Závěr

- Modulární aritmetika a zbytkové třídy
- Malá Fermatova věta
- Modulární inverze
- Čínská věta o zbytcích