Prvočísla

Michal Bulant

8. 10. 2011

Obsah přednášky

Prvočíslo

Definice

Přirozené číslo, které má právě 2 kladné dělitele, se nazývá **prvočíslo**.

Definice (alternativní)

Přirozené číslo n je prvočíslo, právě když pro libovolná $a, b \in \mathbb{Z}$ platí

$$p \mid ab \implies p \mid a \text{ nebo } p \mid b.$$

Je vidět, že obě definice popisují totéž?

Věta (Základní věta aritmetiky)

Každé přirozené číslo se dá jednoznačně (až na pořadí) zapsat jako součin prvočísel.

Prvočísel je ∞ – I. Eukleides apod.

Existuje spousta (ale jen konečně mnoho podstatně různých :) důkazů. Obvykle se postupuje sporem, kdy se všechna předpokládaná prvočísla označí jako $p_1 < p_2 < \ldots < p_k$:

Eukleides $p_1 p_2 \cdots p_k + 1$

Kummer $N = p_1 p_2 \cdots p_k$, pak $N - 1$ je násobkem prvočísla p_i, proto i $N - (N - 1) = 1$.

Stieltjes Rozložme $N = p_1 p_2 \cdots p_k$ na součin mn (jakkoliv). Každé prvočíslo dělí právě jedno z čísel m, n, proto $m + n$ není žádným z nich dělitelné (a to je samozřejmě spor).

Prvočísel je ∞ – II. posloupnosti

Je snadno vidět, že pokud se podaří sestavit **nekonečnou** posloupnost **po dvou nesoudělných** přirozených čísel (větších než 1), existuje nutně nekonečně mnoho prvočísel.

Věta (Goldbach, 1730)

Fermatova čísla[a] $F_n = 2^{2^n} + 1$ *jsou po dvou nesoudělná.*

[a] Viz Fermatova prvočísla, 641 | F_5 – Leonhard Euler

Důkaz.

Snadno se indukcí dokáže, že $F_0 F_1 \cdots F_m = F_{m+1} - 2$, odkud už snadno vyplyne, že F_n jsou po dvou nesoudělná. $\square$

S využitím vlastností největšího společného dělitele a toho, že je možné jej vypočítat pomocí tzv. Euklidova algoritmu, plyne následující:

Lemma

Pro $1 \leq i < j \leq n$ *platí* $(i \cdot (n!) + 1, j \cdot (n!) + 1) = 1$.

Kdyby existovalo pouze k prvočísel, tak z předchozího lemmatu s volbou $n = k + 1$ dostáváme posloupnost n po dvou nesoudělných čísel, což je opět spor.

Dokázat nekonečnost obdobným způsobem lze i pomocí jednoduchého, jinak velmi "plýtvavého" tvrzení:

Lemma

Pro každé celé $n > 2$ existuje mezi čísly n a $n!$ alespoň jedno prvočíslo.

Důkaz.

Označme p libovolné prvočíslo dělící číslo $n! - 1$ Kdyby $p \leq n$, muselo by p dělit číslo $n!$ a nedělilo by $n! - 1$. Je tedy $n < p$. Protože $p \mid (n! - 1)$, platí $p \leq n! - 1$, tedy $p < n!$. $\square$

Důsledek

V posloupnosti $a_1 = 3, a_{n+1} = a_n!$ máme vždy mezi dvěma po sobě jdoucími členy posloupnosti prvočíslo. Posloupnost je zřejmě rostoucí, máme tedy opět nekonečně mnoho prvočísel.

Prvočísel je ∞ – III. nekonečné řady (Euler)

Eulerův důkaz není úplně přímočarý, ale poskytuje silnější tvrzení než pouze nekonečnost počtu prvočísel.

Sestavíme pro každé prvočíslo p nekonečnou geometrickou řadu $\sum_{l=0}^{\infty} \frac{1}{p^l}$, jejíž součet je $\frac{1}{1-1/p}$. Jsou-li opět $p_1, \ldots, p_k$ všechna prvočísla, pak vynásobením příslušných k geometrických řad dostaneme

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{i=1}^{k} \frac{1}{1 - 1/p_i}.$$

Přitom se ale snadno dokáže, že řada $\sum_{n=1}^{\infty} \frac{1}{n}$ diverguje (tj. roste nade všechny meze), zatímco výraz na pravé straně je zřejmě konečný.

Poznámka

Obdobným způsobem se dá dokonce dokázat, že řada $\sum_{p \in P} \frac{1}{p}$ diverguje.

Kongruence

Pojem kongruence byl zaveden Gaussem. Ačkoliv je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel je nedocenitelná; projevuje se zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

Definice

Jestliže dvě celá čísla a, b mají při dělení přirozeným číslem m týž zbytek r, kde $0 \leq r < m$, nazývají se a, b *kongruentní modulo* m, tj. $a \equiv b \pmod{m}$.

Lemma

Pro libovolná $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ jsou následující podmínky ekvivalentní:

1. $a \equiv b \pmod{m}$,
2. $a = b + mt \quad$ *pro vhodné* $t \in \mathbb{Z}$,
3. $m \mid a - b$.

Vlastnosti kongruencí

Vlastnosti

1. Kongruence podle téhož modulu můžeme sčítat a násobit.
2. K libovolné straně kongruence můžeme přičíst jakýkoliv násobek modulu.
3. Obě strany kongruence je možné umocnit na totéž přirozené číslo. Obě strany kongruence je možné vynásobit stejným celým číslem.
4. Obě strany kongruence můžeme vydělit jejich společným dělitelem, jestliže je tento dělitel nesoudělný s modulem.
5. Jestliže kongruence $a \equiv b$ platí podle různých modulů $m_1, \dots, m_k$, platí i podle modulu, kterým je nejmenší společný násobek $[m_1, \dots, m_k]$ těchto čísel.

Eratosthenovo síto

Známá metoda, která poskytuje postup, jak nalézt dokonce všechna prvočísla až do jisté hranice.
Její jediný, zato však zásadní problém, je časová náročnost – pro zjištění prvočísel až do velikosti N potřebujeme znát prvočísla až do velikosti $\sqrt{N}$, což je obvykle příliš mnoho.

Některé důležité věty

Věta (Fermatova)

Je-li a nedělitelné prvočíslem p, pak $p \mid a^{p-1} - 1$, tj.

$$a^{p-1} \equiv 1 \pmod{p}.$$

Důkaz.

Lze dokázat poměrně snadno například matematickou indukcí (pro přirozená a, na celá se již rozšíří snadno) ekvivalentní tvrzení $p \mid a^p - a$.

Další možností je kombinatorický důkaz, kdy počet možných náhrdelníků o p špercích vybíraných z a druhů vyjde

$$\frac{a^p - a}{p} + a.$$

□

Eulerova funkce

Definice

Eulerova funkce $\varphi(m)$ označuje tzv. Eulerovu funkci, udávající počet přirozených čísel nepřevyšujících m, která jsou s m nesoudělná.

Základní vlastnosti:

- $\varphi(p) = p - 1$
- $\varphi(p^k) = (p - 1)p^{k-1}$
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ pro $(a, b) = 1$.

Některé důležité věty II.

Věta (Eulerova)

Je-li $a \in \mathbb{Z}, m \in \mathbb{N}$ a $(a, m) = 1$, pak

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Věta (Wilsonova)

Přirozené číslo n je prvočíslo, právě když

$$(n-1)! \equiv -1 \pmod{n}.$$

Řád čísla modulo, primitivní kořen

Definice

Řádem čísla a modulo m, kde $(a, m) = 1$, nazveme nejmenší přirozené číslo r takové, že $a^r \equiv 1 \pmod{m}$.

Fakt

- $r \mid \varphi(m)$;
- modulo prvočíslo p existuje právě $\varphi(p-1)$ čísel řádu $\varphi(p) = p - 1$ modulo p (menších než p), jde o takzvané primitivní kořeny.

Klasické testy s využitím kongruencí

Wilsonova věta dává sice nutnou i postačující podmínku prvočíselnosti, bohužel nikdo na světě dosud neumít *rychle* vypočítat faktoriál modulo velké číslo. Proto využijeme ostatní věty, které sice dávají pouze nutnou podmínku prvočíselnosti (*je-li p prvočíslo, pak ...*).
Takovým testem je např. klasický Fermatův test plynoucí ze stejnojmenné věty.

Fermatův test

Existuje-li pro dané N nějaké a takové, že $a^{N-1} \not\equiv 1 \pmod{N}$, pak N není prvočíslo.

Fermatův test není ideální

Bohužel nemusí být pro dané složené N snadné najít a takové, že Fermatův test odhalí složenost N, pro některá výjimečná N dokonce jediná taková a jsou soudělná s N, jejich nalezení je tedy ekvivalentní s rozkladem N na prvočísla.
Skutečně existují taková nehezká (nebo extrémně hezká?) složená čísla N, která splňují, že pro libovolné a nesoudělné s N platí $a^{N-1} \equiv 1 \pmod{N}$. Taková čísla se nazývají Carmichaelova, nejmenší z nich je $561 = 3 \cdot 11 \cdot 17$ a teprve v roce 1992 se podařilo dokázat, že jich je dokonce nekonečně mnoho.
Fermatův test lze zlepšit s využitím kvadratických zbytků na Eulerův test $a^{\frac{N-1}{2}} \equiv (a/N) \pmod{N}$, ale výše zmíněný problém se zcela neodstraní ani tímto vylepšením.
V praxi se často používají další vylepšení, zejména tzv. Rabin-Millerův test.

AKS – nedávná indická bomba

AKS

Veškeré předchozí testy (alespoň teoreticky) *strčili do kapsy* v roce 2002 indičtí matematici [a] Agrawal, Kayal a Saxena, kteří Fermatův test aplikovali v (jen o málo) složitější algebraické situaci a odvodili z něj test, který je polynomiální časové složitosti (do té doby se vůbec nevědělo, jakou složitost tohoto problému očekávat).

[a] nebo tedy spíše informatici

Fermatova prvočísla

Zmínili jsme se už o speciálních číslech tvaru $F_m = 2^{2^m} + 1$. Jinak geniální právník Pierre de Fermat vyslovil domněnku, že všechna tato čísla jsou prvočísly. Protože tato čísla enormně rychle rostou, o F_5 už to nebyl schopen ověřit tehdejšími prostředky (tj. “na prstech”). Ukážeme Eulerův geniální důkaz, že $641 \mid F_5$; do dnešních dnů nebylo nalezeno žádné další Fermatovo prvočíslo, navíc i jejich faktorizace nejde nijak závratným tempem – největší úplně rozložené Fermatovo číslo je F_{11}, největší Fermatovo číslo, o němž je známo, že je složené, je F_{23471} s dělitelem $5 \cdot 2^{23473} + 1$.

Poznámka

Do dnešních dnů se neví odpověď ani na jednu z následujících zásadních otázek:

- Existuje ∞ Fermatových prvočísel?
- Existuje ∞ Fermatových složených čísel?

F_5 je složené

Věta

Každý prvočíselný faktor $F_n (n \geq 2)$ je tvaru $k \times 2^{n+2} + 1$.

Důkaz.

Buď p prvočíselný faktor F_n. Řád 2 modulo p je tedy právě 2^{n+1}, odkud $2^{n+1} \mid p-1$, speciálně $8 \mid p-1$. Odtud $2^{\frac{p-1}{2}} \equiv (2/p) = 1 \pmod{p}$, a tedy $2^{n+1} \mid \frac{p-1}{2}$. □

$641 \mid F_5$

$$
\begin{aligned}
F_5 &= 33294320 \times (1 \cdot 2^7 + 1) + 17 \\
F_5 &= 16711935 \times (2 \cdot 2^7 + 1) + 2 \\
F_5 &= 11155759 \times (3 \cdot 2^7 + 1) + 82 \\
F_5 &= 8372255 \times (4 \cdot 2^7 + 1) + 482 \\
F_5 &= 6700417 \times (5 \cdot 2^7 + 1) + 0
\end{aligned}
$$

Konstrukce pravítkem a kružítkem

S Fermatovými čísly souvisí vynikající výsledek C.F.Gausse, který dokázal, že pravidelný n-úhelník je možné sestrojit pravítkem a kružítkem, právě když je $n = 2^k p_1 p_2 \cdots p_h$, kde p_i jsou po dvou různá Fermatova prvočísla. Viz např. `http://www.youtube.com/watch?v=_MJPg-pROrI` nebo sami snadno v Geogebře či Cabri.

Mersenneho prvočísla

Podíváme-li se do tabulek největších známých prvočísel, neujde naší pozornosti, že obvykle jsou všechna tvaru $2^m - 1$.
Má-li být číslo tvaru $2^m - 1$ prvočíslem, je snadným cvičením, že i m musí být prvočíslo. Čísla tvaru $M_q = 2^q - 1$, kde q je prvočíslo, se nazývají Mersenneho čísla[1].

Věta

Je-li q prvočíslo, $q \equiv 3 \pmod 4$, pak $2q + 1$ dělí M_q právě když $2q + 1$ je prvočíslo.

Příklad

Odtud např. $23 \mid M_{11}, 47 \mid M_{23}, 83 \mid M_{167}, atd.$

[1] Kněz Marin Mersenne byl Fermatovým současníkem a dopisoval si s ním.

Poznámka

Do dnešních dnů se neví odpověď ani na jednu z následujících zásadních otázek:

- Existuje ∞ Mersenneho prvočísel?
- Existuje ∞ Mersenneho složených čísel?

Dokonalá čísla

Dokonalá čísla jsou čísla se součtem všech dělitelů rovným svému dvojnásobku – např. 6, 28, 496, 8128. Dosud se neví, zda existuje nějaké liché dokonalé číslo, ví se ale, že *každé sudé dokonalé číslo je tvaru* $2^{q-1}(2^q - 1)$, *kde* q *i* $M_q = 2^q - 1$ *jsou prvočísla.* Samozřejmě se tedy ani neví, jestli existuje nekonečně mnoho (sudých) dokonalých čísel.

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^e \pmod{n}$
- dešifrování šifry C: $OT = D_d(C) \equiv C^d \pmod{n}$

Ukázka nachystána na `https://sage.math.muni.cz/home/pub/3/`.

Výměna klíčů

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)
Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýrů s kufříky, ...).

- Dohoda stran na **modulu** m a primitivním kořenu g (veřejné)
- Alice vybere náhodné a a pošle $g^a \pmod{m}$
- Bob vybere náhodné b a pošle $g^b \pmod{m}$
- Společným klíčem pro komunikaci je $g^{ab} \pmod{m}$.