Diskrétní matematika – 2. týden
Elementární teorie čísel – kongruence a prvočísla

Jan Slovák

Masarykova univerzita
Fakulta informatiky

jaro 2014

Obsah přednášky

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant **Matematika drsně a svižně**, *e*-text na `www.math.muni.cz/Matematika_drsne_svizne`.
- Michal Bulant, výukový text k přednášce **Elementární teorie čísel**, `http://is.muni.cz/el/1431/podzim2012/M6520/um/main-print.pdf`
- Jiří Herman, Radan Kučera, Jaromír Šimša, **Metody řešení matematických úloh**. MU Brno, 2001.
- William Stein, **Elementary Number Theory: Primes, Congruences, and Secrets**, Springer, 2008. Dostupné na `http://wstein.org/ent/ent.pdf`
- Radan Kučera, výukový text k přednášce **Algoritmy teorie čísel**, `http://www.math.muni.cz/~kucera/texty/ATC10.pdf`

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 (též *kongruentní podle modulu* m), což zapisujeme takto:

$$a \equiv b \pmod{m}.$$

V opačném případě řekneme, že a, b nejsou kongruentní modulo m, a píšeme

$$a \not\equiv b \pmod{m}.$$

Lemma

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

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

Důkaz.

"(1)⇒(3)" Jestliže $a = q_1 m + r$, $b = q_2 m + r$, pak $a - b = (q_1 - q_2)m$.
"(3)⇒(2)" Jestliže $m \mid a - b$, pak existuje $t \in \mathbb{Z}$ tak, že $m \cdot t = a - b$, tj. $a = b + mt$.
"(2)⇒(1)" Jestliže $a = b + mt$, pak z vyjádření $b = mq + r$ plyne $a = m(q + t) + r$, tedy a i b mají při dělení číslem m týž zbytek r, tj. $a \equiv b \pmod{m}$. □

Základní vlastnosti kongruencí

Přímo z definice plyne, že kongruence podle modulu m je reflexivní (tj. $a \equiv a \pmod{m}$ platí pro každé $a \in \mathbb{Z}$), symetrická (tj. pro každé $a, b \in \mathbb{Z}$ z $a \equiv b \pmod{m}$ plyne $b \equiv a \pmod{m}$) a tranzitivní (tj. pro každé $a, b, c \in \mathbb{Z}$ z $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$ plyne $a \equiv c \pmod{m}$) relace, jde tedy o *ekvivalenci*. Dokážeme nyní další vlastnosti:

- **Kongruence** podle téhož modulu **můžeme sčítat**. Libovolný sčítanec můžeme přenést s opačným znaménkem z jedné strany kongruence na druhou. **K libovolné straně** kongruence **můžeme přičíst** jakýkoliv **násobek modulu.**

- **Kongruence** podle téhož modulu **můžeme násobit**. Obě strany kongruence je možné **umocnit na totéž přirozené číslo**. Obě strany kongruence je možné **vynásobit stejným celým číslem**.
- **Obě strany** kongruence **můžeme vydělit jejich společným dělitelem**, jestliže je tento dělitel **nesoudělný s modulem.**
- Obě strany kongruence i její modul můžeme současně vynásobit tímtéž přirozeným číslem.
- Obě strany kongruence i její modul můžeme vydělit jejich společným kladným dělitelem.
- **Jestliže kongruence** $a \equiv b$ **platí podle modulů** $m_1, \ldots, m_k$, **platí i podle modulu, kterým je nejmenší společný násobek** $[\mathbf{m_1}, \ldots, \mathbf{m_k}]$ **těchto čísel.**
- Jestliže kongruence platí podle modulu m, platí podle libovolného modulu d, který je dělitelem čísla m.
- Jestliže je jedna strana kongruence a modul dělitelný nějakým celým číslem, musí být tímto číslem dělitelná i druhá strana.

Poznámka

Některé vlastnosti kongruencí jsme již používali, aniž bychom si toho povšimli – například příklad z minulého týdne lze přeformulovat do tvaru "jestliže $a \equiv 1 \pmod{m}$, $b \equiv 1 \pmod{m}$, pak také $ab \equiv 1 \pmod{m}$", což je speciální případ zpředhozího tvrzení.

Nejde o náhodu. Libovolné tvrzení používající kongruence můžeme snadno přepsat pomocí dělitelnosti. Užitečnost kongruencí tedy netkví v tom, že bychom pomocí nich mohli řešit úlohy, které bez nich řešit nejsme schopni, ale v tom, že jde o velmi vhodný způsob zápisu. Osvojíme-li si ho, výrazně tím zjednodušíme jak vyjadřování, tak i některé úvahy. Je to typický jev: v matematice hraje vhodná symbolika velmi závažnou úlohu.

Příklad

Nalezněte zbytek po dělení čísla 5^{20} číslem 26.

Řešení

Protože $5^2 = 25 \equiv -1 \pmod{26}$, platí
$5^{20} \equiv (-1)^{10} = 1 \pmod{26}$, a tedy zbytek po dělení čísla 5^{20} číslem 26 je jedna.

Příklad

Dokažte, že pro libovolné $n \in \mathbb{N}$ je $37^{n+2} + 16^{n+1} + 23^n$ dělitelné sedmi.

Řešení

Platí $37 \equiv 16 \equiv 23 \equiv 2 \pmod{7}$, a tedy podle základních vlastností platí

$$37^{n+2}+16^{n+1}+23^n \equiv 2^{n+2}+2^{n+1}+2^n = 2^n(4+2+1) \equiv 0 \pmod{7}.$$

Příklad

Dokažte, že číslo $n = (835^5 + 6)^{18} - 1$ je dělitelné číslem 112.

Řešení

Rozložíme $112 = 7 \cdot 16$. Protože $(7, 16) = 1$, stačí ukázat, že $7 \mid n$ a $16 \mid n$. Platí $835 \equiv 2 \pmod 7$, a tedy

$$n \equiv (2^5 + 6)^{18} - 1 = 38^{18} - 1 \equiv 3^{18} - 1 = \\ = 27^6 - 1 \equiv (-1)^6 - 1 = 0 \pmod 7,$$

proto $7 \mid n$. Podobně $835 \equiv 3 \pmod{16}$, a tedy

$$n \equiv (3^5 + 6)^{18} - 1 = (3 \cdot 81 + 6)^{18} - 1 \equiv (3 \cdot 1 + 6)^{18} - 1 = \\ = 9^{18} - 1 = 81^9 - 1 \equiv 1^9 - 1 = 0 \pmod{16},$$

proto $16 \mid n$. Celkem tedy $112 \mid n$, což jsme měli dokázat.

Příklad

Dokažte, že pro libovolné prvočíslo p a libovolná $a, b \in \mathbb{Z}$ platí

$$a^p + b^p \equiv (a+b)^p \pmod{p}.$$

Řešení

Podle binomické věty platí

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + \binom{p}{p-1} a b^{p-1} + b^p.$$

Dále, protože $p \mid \binom{p}{k}$ pro libovolné $k \in \{1, \ldots, p-1\}$ (*dokažte*!), platí $\binom{p}{k} \equiv 0 \pmod{p}$, odkud plyne tvrzení.

Prvočíslo je jeden z nejdůležitějších pojmů elementární teorie čísel. Jeho důležitost je dána především větou o jednoznačném rozkladu libovolného přirozeného čísla na součin prvočísel, která je silným a účinným nástrojem při řešení celé řady úloh z teorie čísel.

Definice

Každé přirozené číslo $n \geq 2$ má aspoň dva kladné dělitele: 1 a n. Pokud kromě těchto dvou jiné kladné dělitele nemá, nazývá se *prvočíslo*. V opačném případě hovoříme o *složeném čísle*.

V dalším textu budeme zpravidla prvočíslo značit písmenem p. Nejmenší prvočísla jsou 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... (zejména číslo 1 za prvočíslo ani za číslo složené nepovažujeme, je totiž invertibilní, neboli tzv. jednotkou okruhu celých čísel). Prvočísel je, jak brzy dokážeme, nekonečně mnoho, máme ovšem poměrně limitované výpočetní prostředky na zjištění, zda je dané číslo prvočíslem (největší známé prvočíslo $2^{57\,885\,161} - 1$ má pouze 17 425 170 cifer).

Uveďme nyní větu, která udává ekvivalentní podmínku prvočíselnosti a je základní ingrediencí při důkazu jednoznačnosti rozkladu na prvočísla.

Věta (Euklidova o prvočíslech)

Přirozené číslo $p \geq 2$ je prvočíslo, právě když platí: pro každá celá čísla a, b z $p \mid ab$ plyne $p \mid a$ nebo $p \mid b$.

Důkaz.

"$\Rightarrow$" Předpokládejme, že p je prvočíslo a $p \mid ab$, kde $a, b \in \mathbb{Z}$. Protože (p, a) je kladný dělitel p, platí $(p, a) = p$ nebo $(p, a) = 1$. V prvním případě $p \mid a$, ve druhém $p \mid b$, jak jsme dokázali minulý týden.

"$\Leftarrow$" Jestliže p není prvočíslo, musí existovat jeho kladný dělitel různý od 1 a p. Označíme jej a; pak ovšem $b = \frac{p}{a} \in \mathbb{N}$ a platí $p = ab$, odkud $1 < a < p$, $1 < b < p$. Našli jsme tedy celá čísla a, b tak, že $p \mid ab$ a přitom p nedělí ani a, ani b. □

Základní věta aritmetiky

Věta

Libovolné přirozené číslo $n \geq 2$ je možné vyjádřit jako součin prvočísel, přičemž je toto vyjádření jediné, nebereme-li v úvahu pořadí činitelů. (Je-li n prvočíslo, pak jde o „součin“ jednoho prvočísla.)

Poznámka

Dělitelnost je možné obdobným způsobem definovat v libovolném oboru integrity (zkuste si rozmyslet, proč se omezujeme na obory integrity). V některých oborech integrity přitom žádné prvky s vlastností prvočísla (říkáme jim *ireducibilní*) neexistují (např. $\mathbb{Q}$), v jiných sice ireducibilní prvky existují, ale zase tam neplatí věta o jednoznačném rozkladu (např. v $\mathbb{Z}(\sqrt{-5})$ máme následující rozklady: $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

Důkaz.

Nejprve dokážeme indukcí, že každé $n \geq 2$ je možné vyjádřit jako součin prvočísel.
Je-li $n = 2$, je n součin jediného prvočísla 2.
Předpokládejme nyní, že $n > 2$ a že jsme již dokázali, že libovolné n', $2 \leq n' < n$, je možné rozložit na součin prvočísel. Jestliže n je prvočíslo, je součinem jediného prvočísla. Jestliže n prvočíslo není, pak existuje jeho dělitel d, $1 < d < n$. Označíme-li $c = \frac{n}{d}$, platí také $1 < c < n$. Z indukčního předpokladu plyne, že c i d je možné vyjádřit jako součin prvočísel, a proto je takto možné vyjádřit i jejich součin $c \cdot d = n$.
Nyní dokážeme jednoznačnost. Předpokládejme, že platí rovnost součinů $p_1 \cdot p_2 \cdot \cdots \cdot p_m = q_1 \cdot q_2 \cdot \cdots \cdot q_s$, kde $p_1, \ldots, p_m$, $q_1, \ldots, q_s$ jsou prvočísla a navíc platí $p_1 \leq p_2 \leq \cdots \leq p_m$, $q_1 \leq q_2 \leq \cdots \leq q_s$ a $1 \leq m \leq s$. Indukcí vzhledem k m dokážeme, že $m = s$, $p_1 = q_1, \ldots, p_m = q_m$.

□

Dokončení.

Je-li $m = 1$, je $p_1 = q_1 \cdot \dots \cdot q_s$ prvočíslo. Kdyby $s > 1$, mělo by číslo p_1 dělitele q_1 takového, že $1 < q_1 < p_1$ (neboť $q_2 q_3 \dots q_s > 1$), což není možné. Je tedy $s = 1$ a platí $p_1 = q_1$. Předpokládejme, že $m \geq 2$ a že tvrzení platí pro $m - 1$. Protože $p_1 \cdot p_2 \cdot \dots \cdot p_m = q_1 \cdot q_2 \cdot \dots \cdot q_s$, dělí p_m součin $q_1 \cdot \dots \cdot q_s$, což je podle Euklidovy věty možné jen tehdy, jestliže p_m dělí nějaké q_i pro vhodné $i \in \{1, 2, \dots, s\}$. Protože q_i je prvočíslo, plyne odtud $p_m = q_i$ (neboť $p_m > 1$). Zcela analogicky se dokáže, že $q_s = p_j$ pro vhodné $j \in \{1, 2, \dots, m\}$. Odtud plyne

$$q_s = p_j \leq p_m = q_i \leq q_s,$$

takže $p_m = q_s$. Vydělením dostaneme $p_1 \cdot p_2 \cdot \dots \cdot p_{m-1} = q_1 \cdot q_2 \cdot \dots \cdot q_{s-1}$, a tedy z indukčního předpokladu $m - 1 = s - 1$, $p_1 = q_1, \dots, p_{m-1} = q_{m-1}$. Celkem tedy $m = s$ a $p_1 = q_1, \dots, p_{m-1} = q_{m-1}$, $p_m = q_m$. Jednoznačnost, a tedy i celá věta, je dokázána. □

PRIMES is in P

Poznámka

Již jsme se zmínili, že je složité o velkých číslech s jistotou rozhodnout, jde-li o prvočíslo (na druhou stranu je o naprosté většině složených čísel snadné prokázat, že jsou skutečně složená). Přesto se v roce 2002 podařilo indickým matematikům (Agrawal, Saxena, Kayal: `http://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf`) dokázat, že problém prvočíselnosti je možné rozhodnout algoritmem s časovou složitostí polynomiálně závislou na počtu cifer vstupního čísla. Nic podobného se zatím nepodařilo v otázce rozkladu čísla na prvočísla (třebaže se obecně nevěří, že je to možné, exaktní důkaz zatím nebyl podán).

Is FACTOR in P?

Nic podobného se zatím nepodařilo v otázce rozkladu čísla na prvočísla (třebaže se obecně nevěří, že je to možné, exaktní důkaz zatím nebyl podán). Nejrychlejší obecně použitelný faktorizační algoritmus, tzv. *síto v číselném tělese*[1], je sub-exponenciální časové složitosti $O(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}})$.

Poznámka

Peter Shor v roce 1994 vymyslel algoritmus, který faktorizuje v kubickém čase (tj. $O((\log N)^3)$) na kvantovém počítači. Je k tomu nicméně třeba sestrojit počítače s dostatečným počtem qubits – jak je to obtížné, lze vysledovat z toho, ze v roce 2001 se IBM podařilo pomocí kvantového počítače rozložit číslo 15 a v roce 2012 byl dosažen další faktorizační rekord rozkladem čísla 21.

[1] Pro podrobnosti navštivte M8190 Algoritmy teorie čísel

RSA Challenge

Poznámka

Že je problém rozkladu přirozeného čísla na prvočísla výpočetně složitý, o tom svědčí i (již neplatná) výzva učiněná v roce 1991 firmou RSA Security (viz `http://www.rsasecurity.com/rsalabs/node.asp?id=2093`). Pokud se komukoliv podařilo rozložit čísla označená podle počtu cifer jako RSA-100, . . . , RSA-704, RSA-768, . . . , RSA-2048, mohl obdržet 1 000,. . . , 30 000, 50 000, . . . , resp. 200 000 dolarů (číslo RSA-100 rozložil v témže roce Arjen Lenstra, číslo RSA-704 bylo rozloženo v roce 2012, některá dosud rozložena nebyla).

Díky jednoznačnosti rozkladu na prvočísla jsme schopni (se znalostí tohoto rozkladu) snadno odpovědět i na otázky ohledně počtu či součtu dělitelů konkrétního čísla. Stejně snadno dostaneme i (z dřívějška intuitivně známý) postup na výpočet největšího společného dělitele dvou čísel ze znalosti jejich rozkladu na prvočísla.

Důsledek

- *Každý kladný dělitel čísla* $a = p_1^{n_1} \cdot \dots \cdot p_k^{n_k}$ *je tvaru* $p_1^{m_1} \cdot \dots \cdot p_k^{m_k}$, *kde* $m_1, \dots, m_k \in \mathbb{N}_0$ *a* $m_1 \leq n_1$, $m_2 \leq n_2$, $\dots$, $m_k \leq n_k$.
- *Číslo* a *má tedy právě* $\tau(a) = (n_1 + 1)(n_2 + 1) \cdot \dots \cdot (n_k + 1)$ *kladných dělitelů, jejichž součet je*

$$\sigma(a) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \dots \frac{p_k^{n_k+1} - 1}{p_k - 1}.$$

Důsledek (Pokr.)

- *Jsou-li* $p_1, \ldots, p_k$ *navzájem různá prvočísla a* $n_1, \ldots, n_k, m_1, \ldots, m_k \in \mathbb{N}_0$ *a označíme-li* $r_i = \min\{n_i, m_i\}$, $t_i = \max\{n_i, m_i\}$ *pro každé* $i = 1, 2, \ldots, k$, *platí*

$$(p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}, p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}) = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k},$$

$$[p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}, p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}] = p_1^{t_1} \cdot \ldots \cdot p_k^{t_k}.$$

Mersenneho prvočísla a dokonalá čísla

S pojmem *součet všech kladných dělitelů čísla a* souvisí pojem tzv. *dokonalého čísla a*, které splňuje podmínku $\sigma(a) = 2a$, resp. slovně: *součet všech kladných dělitelů čísla a menších než a samotné je roven číslu a*.
Takovými čísly jsou např. $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$, 496 a 8128 (jde o všechna dokonalá čísla menší než 10 000).

Poznámka

Lze ukázat, že sudá dokonalá čísla jsou v úzkém vztahu s tzv. *Mersenneho prvočísly*. Platí totiž: *a je sudé dokonalé číslo, právě když je tvaru* $a = 2^{q-1} \cdot (2^q - 1)$, *kde* $2^q - 1$ *je prvočíslo.*

Mersenneho prvočísla jsou právě prvočísla tvaru $2^k - 1$. Bez zajímavosti není ani to, že právě Mersenneho prvočísla jsou mezi všemi prvočísly nejlépe „vidět“ – pro Mersenneho čísla existuje poměrně jednoduchý a rychlý postup, jak ověřit, že jde o prvočísla.

Hledání velkých prvočísel

Proto není náhodou, že největší známá prvočísla jsou obvykle tvaru $2^k - 1$ (viz např. `http://www.utm.edu/research/primes/largest.html`).
Jakkoliv může být hledání největšího známého prvočísla chápáno jako pochybná zábava bez valného praktického užitku[2], jednak posunuje hranice matematického poznání a zdokonaluje použité metody (a často i hardware), jednak může přinést benefit i samotným objevitelům (Electronic Frontier Foundation vypsala odměny EFF Cooperative Computing Awards za nalezení prvočísla majícího alespoň $10^6, 10^7, 10^8$ a 10^9 číslic – odměny 50, resp. 100 tisíc $ za první dvě kategorie byly vyplaceny v letech 2000, resp. 2009 – v obou případech projektu GIMPS – na další odměny si ještě zřejmě nějaký čas počkáme).
Na druhou stranu popsat lichá dokonalá čísla se dodnes nepodařilo, resp. **dodnes se neví, jestli vůbec nějaké liché dokonalé číslo existuje**.

[2] Viz např. titulek iDnes z 6.února 2013: *Největší známé prvočíslo na světě*

Jak testovat Mersenneho prvočísla?

Přestože zatím nemáme jasno v tom, jak efektivně implementovat použité operace, ani neumíme dokázat jeho správnost, uveďme si pro ilustraci test, kterým lze zjistit, je-li dané Mersenneho číslo prvočíslem.

Lucas-Lehmerův test

Definujme posloupnost $(s_n)_{n=0}^{\infty}$ rekurzívně předpisem
$s_0 = 4, s_{n+1} = s_n^2 - 2$.
Pak je číslo $M_p = 2^p - 1$ prvočíslo, právě tehdy, když M_p dělí s_{p-2}.