Diskrétní matematika B – 1. týden
Elementární teorie čísel

Michal Bulant

Masarykova univerzita
Fakulta informatiky

jaro 2014

Obsah přednášky

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant, *Matematika drsně a svižně*, MU Brno, 2013, 774 s. (též jako e-text).
- *Předmětové záložky v IS MU*
- Michal Bulant, výukový text k přednášce **Elementární teorie čísel**, `http://is.muni.cz/el/1431/podzim2013/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`

Na této přednášce se budeme zabývat úlohami o celých číslech. Převážně v nich půjde o dělitelnost celých čísel, popřípadě o řešení rovnic v oboru celých nebo přirozených čísel. Ačkoli jsou přirozená a konec konců i celá čísla v jistém smyslu nejjednodušší matematickou strukturou, zkoumání jejich vlastností postavilo před generace matematiků celou řadu velice obtížných problémů. Často jsou to problémy, které je možno snadno formulovat, přesto však dodnes neznáme jejich řešení.

God made integers, all else is the work of man. (L. Kronecker)

Notorické problémy teorie čísel

Uveďme některé z nejznámějších:

- *problém prvočíselných dvojčat* – rozhodnout, zda existuje nekonečně mnoho prvočísel p takových, že i $p + 2$ je prvočíslo,
- *problém existence lichého dokonalého čísla* – tj. čísla jehož součet dělitelů je roven dvojnásobku tohoto čísla
- *Goldbachovu hypotézu* (rozhodnout, zda každé sudé číslo větší než 2 je možno psát jako součet dvou prvočísel),
- nebo klenot mezi problémy teorie čísel *velkou Fermatovu větu* (Fermat's Last Theorem) – rozhodnout, zda existují přirozená čísla n, x, y, z tak, že $n > 2$ a platí $x^n + y^n = z^n$; Pierre de Fermat jej formuloval cca 1637, vyřešil Andrew Wiles v roce 1995.

Definice

Řekneme, že celé číslo a *dělí* celé číslo b (neboli číslo b je *dělitelné* číslem a, též b je *násobek* a), právě když existuje celé číslo c tak, že platí $a \cdot c = b$. Píšeme pak $a \mid b$.

Přímo z definice plyne několik jednoduchých tvrzení : Číslo nula je dělitelné každým celým číslem; jediné celé číslo, které je dělitelné nulou, je nula; pro libovolné číslo a platí $a \mid a$; pro libovolná čísla a, b, c platí tyto čtyři implikace:

$$\begin{aligned} a \mid b \ \wedge \ b \mid c &\implies a \mid c \\ a \mid b \ \wedge \ a \mid c &\implies a \mid b + c \ \wedge \ a \mid b - c \\ c \neq 0 &\implies (a \mid b \iff ac \mid bc) \\ a \mid b \ \wedge \ b > 0 &\implies a \leq b \end{aligned}$$

Příklad

Zjistěte, pro která přirozená čísla n je číslo $n^2 + 1$ dělitelné číslem $n + 1$.

Řešení

Platí $n^2 - 1 = (n + 1)(n - 1)$, a tedy číslo $n + 1$ dělí číslo $n^2 - 1$. Předpokládejme, že $n + 1$ dělí i číslo $n^2 + 1$. Pak ovšem musí dělit i rozdíl $(n^2 + 1) - (n^2 - 1) = 2$. Protože $n \in \mathbb{N}$, platí $n + 1 \geq 2$, a tedy z $n + 1 \mid 2$ plyne $n + 1 = 2$, proto $n = 1$. Uvedenou vlastnost má tedy jediné přirozené číslo 1. □

Dělení se zbytkem

Věta (o dělení celých čísel se zbytkem)

Pro libovolně zvolená čísla $a \in \mathbb{Z}$, $m \in \mathbb{N}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, m-1\}$ tak, že $a = qm + r$.

Důkaz.

Dokažme nejprve existenci čísel q, r. Předpokládejme, že přirozené číslo m je dáno pevně a dokažme úlohu pro libovolné $a \in \mathbb{Z}$. Nejprve budeme předpokládat, že $a \in \mathbb{N}_0$ a existenci čísel q, r dokážeme indukcí: Je-li $0 \leq a < m$, stačí volit $q = 0$, $r = a$ a rovnost $a = qm + r$ platí. Předpokládejme nyní, že $a \geq m$ a že jsme existenci čísel q, r dokázali pro všechna $a' \in \{0, 1, 2, \ldots, a-1\}$. Speciálně pro $a' = a - m$ tedy existují q', r' tak, že $a' = q'm + r'$ a přitom $r' \in \{0, 1, \ldots, m-1\}$. Zvolíme-li $q = q' + 1$, $r = r'$, platí $a = a' + m = (q' + 1)m + r' = qm + r$, což jsme chtěli dokázat. □

Dokončení důkazu.

Existenci čísel q, r jsme tedy dokázali pro libovolné $a \geq 0$. Je-li naopak $a < 0$, pak ke kladnému číslu $-a$ podle výše dokázaného existují $q' \in \mathbb{Z}$, $r' \in \{0, 1, \ldots, m-1\}$ tak, že $-a = q'm + r'$, tedy $a = -q'm - r'$. Je-li $r' = 0$, položíme $r = 0$, $q = -q'$; je-li $r > 0$, položíme $r = m - r'$, $q = -q' - 1$. V obou případech $a = q \cdot m + r$, a tedy čísla q, r s požadovanými vlastnostmi existují pro každé $a \in \mathbb{Z}$, $m \in \mathbb{N}$.

Nyní dokážeme jednoznačnost. Předpokládejme, že pro některá čísla $q_1, q_2 \in \mathbb{Z}$; $r_1, r_2 \in \{0, 1, \ldots, m-1\}$ platí $a = q_1 m + r_1 = q_2 m + r_2$. Úpravou dostaneme $r_1 - r_2 = (q_2 - q_1)m$, a tedy $m \mid r_1 - r_2$. Ovšem z $0 \leq r_1 < m$, $0 \leq r_2 < m$ plyne $-m < r_1 - r_2 < m$, odkud dostáváme $r_1 - r_2 = 0$. Pak ale i $(q_2 - q_1)m = 0$, a proto $q_1 = q_2$, $r_1 = r_2$. Čísla q, r jsou tedy určena jednoznačně. □

Číslo q, resp. r z věty se nazývá *(neúplný) podíl*, resp. *zbytek* při dělení čísla a číslem m se zbytkem. Vhodnost obou názvů je zřejmá, přepíšeme-li rovnost $a = mq + r$ do tvaru

$$\frac{a}{m} = q + \frac{r}{m}, \quad \text{přitom} \quad 0 \leq \frac{r}{m} < 1.$$

Příklad

Dokažte, že jsou-li zbytky po dělení čísel $a, b \in \mathbb{Z}$ číslem $m \in \mathbb{N}$ jedna, je jedna i zbytek po dělení čísla ab číslem m.

Řešení

Podle Věty o dělení se zbytkem existují $s, t \in \mathbb{Z}$ tak, že $a = sm + 1$, $b = tm + 1$. Vynásobením dostaneme

$$ab = (sm + 1)(tm + 1) = (stm + s + t)m + 1 = qm + r,$$

kde $q = stm + s + t$, $r = 1$, které je podle téže věty jednoznačné, a tedy zbytek po dělení čísla ab číslem m je jedna. □

Největší společný dělitel (gcd)

Jedním z nejdůležitějších nástrojů výpočetní teorie čísel je výpočet největšího společného dělitele. Protože jde, jak si ukážeme, o relativně rychlou proceduru, je i v moderních algoritmech velmi často využívána.

Definice

Mějme celá čísla a_1, a_2. Libovolné celé číslo m takové, že $m \mid a_1$, $m \mid a_2$ (resp. $a_1 \mid m$, $a_2 \mid m$) se nazývá *společný dělitel* (resp. *společný násobek*) čísel a_1, a_2. Společný dělitel (resp. násobek) $m \geq 0$ čísel a_1, a_2, který je dělitelný libovolným společným dělitelem (resp. dělí libovolný společný násobek) čísel a_1, a_2, se nazývá *největší společný dělitel* (resp. *nejmenší společný násobek*) čísel a_1, a_2 a značí se (a_1, a_2) (resp. $[a_1, a_2]$).

Poznámka

Přímo z definice plyne, že pro libovolné $a, b \in \mathbb{Z}$ platí $(a, b) = (b, a)$, $[a, b] = [b, a]$, $(a, 1) = 1$, $[a, 1] = |a|$, $(a, 0) = |a|$, $[a, 0] = 0$.

Poznámka

Analogicky se definuje i největší společný dělitel a nejmenší společný násobek více než dvou celých čísel a snadno se následně dokáže, že platí

$$(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$$
$$[a_1, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n]$$

Euklidův algoritmus

Dosud jsme nijak nezdůvodnili, zda pro každou dvojici $a, b \in \mathbb{Z}$ čísla (a, b) a $[a, b]$ vůbec existují.
Pokud však existují, jsou určena jednoznačně: Pro každá dvě čísla $m_1, m_2 \in \mathbb{N}_0$ totiž podle definice platí, že pokud $m_1 \mid m_2$ a zároveň $m_2 \mid m_1$, je nutně $m_1 = m_2$. Důkaz existence čísla (a, b) podáme (spolu s algoritmem jeho nalezení) v následující větě, důkaz existence čísla $[a, b]$ pak dostaneme snadno ze vztahu mezi (a, b) a $[a, b]$.

Věta (Euklidův algoritmus)

Nechť a_1, a_2 jsou přirozená čísla. Pro každé $n \geq 3$, pro které $a_{n-1} \neq 0$, označme a_n zbytek po dělení čísla a_{n-2} číslem a_{n-1}. Pak po konečném počtu kroků dostaneme $a_k = 0$ a platí $a_{k-1} = (a_1, a_2)$.

Důkaz.

Podle Věty o dělení se zbytkem platí $a_2 > a_3 > a_4 > \dots$. Protože jde o nezáporná celá čísla, je každé následující alespoň o 1 menší než předchozí, a proto po určitém konečném počtu kroků dostáváme $a_k = 0$, přičemž $a_{k-1} \neq 0$. Z definice čísel a_n plyne, že existují celá čísla $q_1, q_2, \dots, q_{k-2}$ tak, že

$$\begin{aligned} a_1 &= q_1 \cdot a_2 + a_3, \\ &\vdots \\ a_{k-3} &= q_{k-3} \cdot a_{k-2} + a_{k-1} \\ a_{k-2} &= q_{k-2} \cdot a_{k-1}. \end{aligned}$$

Z poslední rovnosti plyne, že $a_{k-1} \mid a_{k-2}$, dále $a_{k-1} \mid a_{k-3}$, atd., je tedy a_{k-1} společný dělitel čísel a_1, a_2. Naopak jejich libovolný společný dělitel dělí i číslo $a_3 = a_1 - q_1 a_2$, proto i $a_4 = a_2 - q_2 a_3, \dots$, a proto i $a_{k-1} = a_{k-3} - q_{k-3} a_{k-2}$. Dokázali jsme, že a_{k-1} je největší společný dělitel čísel a_1, a_2. □

Vlastnosti gcd

Poznámka

Z definice, z předchozího tvrzení a z toho, že pro libovolná $a, b \in \mathbb{Z}$ platí $(a, b) = (a, -b) = (-a, b) = (-a, -b)$, plyne, že existuje největší společný dělitel libovolných dvou celých čísel.

Věta (Bezoutova)

Pro libovolná celá čísla a_1, a_2 existuje jejich největší společný dělitel (a_1, a_2), přitom existují celá čísla k_1, k_2 tak, že $(a_1, a_2) = k_1 a_1 + k_2 a_2$.

Důkaz.

Jistě stačí větu dokázat pro $a_1, a_2 \in \mathbb{N}$. Všimněme si, že jestliže je možné nějaká čísla $r, s \in \mathbb{Z}$ vyjádřit ve tvaru $r = r_1 a_1 + r_2 a_2$, $s = s_1 a_1 + s_2 a_2$, kde $r_1, r_2, s_1, s_2 \in \mathbb{Z}$, můžeme tak vyjádřit i

$$r + s = (r_1 + s_1)a_1 + (r_2 + s_2)a_2$$

a také

$$c \cdot r = (c \cdot r_1)a_1 + (c \cdot r_2)a_2$$

pro libovolné $c \in \mathbb{Z}$. Protože $a_1 = 1 \cdot a_1 + 0 \cdot a_2$, $a_2 = 0 \cdot a_1 + 1 \cdot a_2$, plyne z (5), že takto můžeme vyjádřit i $a_3 = a_1 - q_1 a_2$, $a_4 = a_2 - q_2 a_3$, $\ldots$, $a_{k-1} = a_{k-3} - q_{k-3} a_{k-2}$, což je ovšem (a_1, a_2). □

Příklad

Výpočet největšího společného dělitele pomocí Euklidova algoritmu je s využitím výpočetní techniky i pro relativně velká čísla poměrně rychlý. V našem příkladu to vyzkoušíme na 2 číslech A,B, z nichž každé je součinem dvou 101-ciferných prvočísel. Všimněme si, že výpočet největšího společného dělitele i takto velkých čísel trval zandbatelný čas.
Příklad v systému SAGE je dostupný na
`https://sage.math.muni.cz/home/pub/6/`.

Poznámka

Euklidův algoritmus a Bezoutova věta jsou základními výsledky elementární teorie čísel a tvoří jeden z pilířů algoritmů algebry a teorie čísel.

To, že znalost těchto základů je občas důležitá i v praktickém životě, dokazuje Bruce Willis a Samuel Jackson ve filmu Smrtonosná past 3, kde mají za úkol zlikvidovat bombu pomocí 4 galonů vody, přičemž k dispozici mají pouze nádoby na 3, resp. 5 galonů. Zde stačí s využitím Euklidova algoritmu najít celá čísla k, l tak, že bude platit $3k + 5l = 4$. Netroufám si tvrdit, že zmínění herci ovládají uvedené základy teorie čísel (tuto konkrétní úlohu jistě snadno vyřešíte experimentálně), nicméně předchozí věty dávají návod, jak vyřešit úlohu tohoto typu s libovolnými zadanými parametry.

Nejmenší společný násobek

Věta

Pro libovolná celá čísla a_1, a_2 existuje jejich nejmenší společný násobek $[a_1, a_2]$ a platí $(a_1, a_2) \cdot [a_1, a_2] = |a_1 \cdot a_2|$.

Důkaz.

Věta jistě platí, je-li některé z čísel a_1, a_2 rovno nule. Můžeme navíc předpokládat, že obě nenulová čísla a_1, a_2 jsou kladná, neboť jejich znaménka se v dokazovaném vzorci neprojeví. Budeme hotovi, ukážeme-li, že $q = a_1 \cdot a_2/(a_1, a_2)$ je nejmenší společný násobek čísel a_1, a_2. □

Dokončení.

Protože (a_1, a_2) je společný dělitel čísel a_1, a_2, jsou $a_1/(a_1, a_2)$ i $a_2/(a_1, a_2)$ celá čísla, a proto

$$q = \frac{a_1 a_2}{(a_1, a_2)} = \frac{a_1}{(a_1, a_2)} \cdot a_2 = \frac{a_2}{(a_1, a_2)} \cdot a_1$$

je společný násobek čísel a_1, a_2. Podle věty 3 existují $k_1, k_2 \in \mathbb{Z}$ tak, že $(a_1, a_2) = k_1 a_1 + k_2 a_2$. Předpokládejme, že $n \in \mathbb{Z}$ je libovolný společný násobek čísel a_1, a_2 a ukážeme, že je dělitelný číslem q. Je tedy $n/a_1, n/a_2 \in \mathbb{Z}$, a proto je i celé číslo

$$\frac{n}{a_2} \cdot k_1 + \frac{n}{a_1} \cdot k_2 = \frac{n(k_1 a_1 + k_2 a_2)}{a_1 a_2} = \frac{n(a_1, a_2)}{a_1 a_2} = \frac{n}{q}.$$

To ovšem znamená, že $q \mid n$, což jsme chtěli dokázat. □

Nesoudělnost

Definice

Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *nesoudělná*, jestliže platí $(a_1, a_2, \ldots, a_n) = 1$. Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *po dvou nesoudělná*, jestliže pro každé i, j takové, že $1 \leq i < j \leq n$, platí $(a_i, a_j) = 1$.

Poznámka

V případě $n = 2$ oba pojmy splývají, pro $n > 2$ plyne z nesoudělnosti po dvou nesoudělnost, ne však naopak: například čísla 6, 10, 15 jsou nesoudělná, ale nejsou nesoudělná po dvou, neboť dokonce žádná dvojice z nich vybraná nesoudělná není: $(6, 10) = 2$, $(6, 15) = 3$, $(10, 15) = 5$.

Věta

Pro libovolná přirozená čísla a, b, c *platí*

1. $(ac, bc) = (a, b) \cdot c$,
2. *jestliže* $a \mid bc$, $(a, b) = 1$, *pak* $a \mid c$,
3. $d = (a, b)$ *právě tehdy, když existují* $q_1, q_2 \in \mathbb{N}$ *tak, že* $a = dq_1$, $b = dq_2$ *a* $(q_1, q_2) = 1$.

Důkaz.

ad 1. Protože (a, b) je společný dělitel čísel a, b, je $(a, b) \cdot c$ společný dělitel čísel ac, bc, proto $(a, b) \cdot c \mid (ac, bc)$. Podle Bezoutovy věty existují $k, l \in \mathbb{Z}$ tak, že $(a, b) = ka + lb$. Protože (ac, bc) je společný dělitel čísel ac, bc, dělí i číslo $kac + lbc = (a, b) \cdot c$. Dokázali jsme, že $(a, b) \cdot c$ a (ac, bc) jsou dvě přirozená čísla, která dělí jedno druhé, proto se rovnají.

ad 2. Předpokládejme, že $(a, b) = 1$ a $a \mid bc$. Podle Bezoutovy věty existují $k, l \in \mathbb{Z}$ tak, že $ka + lb = 1$, odkud plyne, že $c = c(ka + lb) = kca + lbc$. Protože $a \mid bc$, plyne odsud, že i $a \mid c$.

ad 3. Nechť $d = (a, b)$, pak existují $q_1, q_2 \in \mathbb{N}$ tak, že $a = dq_1$, $b = dq_2$. Pak podle 1. části platí $d = (a, b) = (dq_1, dq_2) = d \cdot (q_1, q_2)$, a tedy $(q_1, q_2) = 1$. Naopak, je-li $a = dq_1$, $b = dq_2$ a $(q_1, q_2) = 1$, pak $(a, b) = (dq_1, dq_2) = d(q_1, q_2) = d \cdot 1 = d$ (opět užitím 1. části tohoto 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 $p \mid b$ podle části 2. předchozí věty.

"$\Leftarrow$" 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: $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$; zkuste si rozmyslet, že všichni uvedení činitelé jsou skutečně v $\mathbb{Z}(\sqrt{-5})$ ireducibilní).

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 proto je i celá věta 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).
Lze ukázat, že sudá dokonalá čísla jsou v úzkém vztahu s tzv. *Mersenneho prvočísly*. Platí totiž:

Věta

Číslo a je sudé dokonalé, právě když je tvaru $a = 2^{q-1} \cdot (2^q - 1)$, *kde* $2^q - 1$ *je prvočíslo.*

Na druhou stranu popsat lichá dokonalá čísla se dodnes nepodařilo, resp. **dodnes se neví, jestli vůbec nějaké liché dokonalé číslo existuje**.

Hledání velkých prvočísel

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. 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).

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}.

Rozložení prvočísel

Nyní se budeme snažit zodpovědět následující otázky:

1. Je prvočísel nekonečně mnoho?
2. Je prvočísel nekonečně mnoho v každé (nebo aspoň některé) aritmetické posloupnosti?
3. Jak jsou prvočísla rozložena mezi přirozenými čísly?

> *There are two facts about the distribution of prime numbers. The first is that, [they are] the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision.*
>
> *Don Zagier*

Prvočísel je nekonečně mnoho

Věta (Eukleidés)

Mezi přirozenými čísly existuje nekonečně mnoho prvočísel.

Důkaz.

Předpokládejme, že prvočísel je konečně mnoho a označme je $p_1, p_2, \ldots, p_n$. Položme $N = p_1 \cdot p_2 \ldots p_n + 1$. Toto číslo je buď samo prvočíslem nebo je dělitelné nějakým prvočíslem různým od $p_1, \ldots, p_n$ (čísla $p_1, \ldots, p_n$ totiž dělí číslo $N - 1$), což je spor. □

Poznámka

Existuje mnoho variant důkazů nekonečnosti prvočísel z různých oblastí matematiky, uveďme ještě alespoň některá tvrzení, z nichž zároveň získáme alespoň částečnou informaci o rozložení prvočísel mezi přirozenými čísly.

Prvočísel je vcelku hodně

Příklad

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

Řešení

Označme p libovolné prvočíslo dělící číslo $n! - 1$ (takové existuje podle Základní věty aritmetiky, protože $n! - 1 > 1$). 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 $p < n!$. Prvočíslo p splňuje podmínky úlohy. □

Z této věty rovněž vyplývá nekonečnost prvočísel, její tvrzení je ale velice slabé. Následující tvrzení, uvedené bez důkazu, je podstatně silnější.

Věta (Čebyševova, Bertrandův postulát)

Pro libovolné číslo $n > 1$ existuje alespoň jedno prvočíslo p splňující $n < p < 2n$.

Prvočísel je vcelku málo

Příklad

Dokažte, že pro libovolné přirozené číslo n existuje n po sobě jdoucích přirozených čísel, z nichž žádné není prvočíslo.

Řešení

Zkoumejme čísla $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$. Mezi těmito n po sobě jdoucími čísly není žádné prvočíslo, protože pro libovolné $k \in \{2, 3, \ldots, n+1\}$ platí $k \mid (n+1)!$, a tedy $k \mid (n+1)!+k$, a proto $(n+1)!+k$ nemůže být prvočíslo. □

Prvočísla jsou relativně rovnoměrně rozložena v tom, smyslu, že v libovolné „rozumné“ aritmetické posloupnosti je jich nekonečně mnoho. Například zbytek 1 po dělení čtyřmi, stejně jako zbytek 3 po dělení čtyřmi dá vždy nekonečně mnoho prvočísel (zbytek 0 nedá samozřejmě žádné a zbytek 2 pouze jediné). Obdobná situace je pak při uvažování zbytků po dělení libovolným jiným přirozeným číslem, jak uvádí následující věta, jejíž důkaz je ovšem velmi obtížný.

Věta (Dirichletova o prvočíslech v aritmetické posloupnosti)

Jsou-li a, m nesoudělná přirozená čísla, existuje nekonečně mnoho přirozených čísel k tak, že $mk + a$ je prvočíslo. Jinými slovy, mezi čísly $1 \cdot m + a, 2 \cdot m + a, 3 \cdot m + a, \ldots$ existuje nekonečně mnoho prvočísel.

Uveďme proto alespoň důkaz ve speciálním případě.

Prvočísel tvaru $3k + 2$ je nekonečně mnoho

Příklad

Dokažte, že existuje nekonečně mnoho prvočísel tvaru $3k + 2$, kde $k \in \mathbb{N}_0$.

Řešení

Předpokládejme naopak, že existuje pouze konečně mnoho prvočísel tohoto tvaru a označme je $p_1 = 2$, $p_2 = 5$, $p_3 = 11$, $\ldots$, p_n. Položme $N = 3p_2 \cdot p_3 \cdot \cdots \cdot p_n + 2$. Rozložíme-li N na součin prvočísel, musí v tomto rozkladu vystupovat aspoň jedno prvočíslo p tvaru $3k + 2$, neboť v opačném případě by bylo N součinem prvočísel tvaru $3k + 1$ (uvažte, že N není dělitelné třemi), a tedy podle dřívějšího příkladu by bylo i N tvaru $3k + 1$, což není pravda. Prvočíslo p ovšem nemůže být žádné z prvočísel $p_1, p_2, \ldots, p_n$, jak plyne z tvaru čísla N, a to je spor.

Asymptotické chování prvočísel

Z tvrzení uvedených v této kapitole je možné si udělat hrubou představu o tom, jak "hustě" se mezi přirozenými čísla prvočísla vyskytují. Přesněji (i když "pouze" asymptoticky) to popisuje velmi důležitá tzv. "Prime Number Theorem":

Věta (Prime Number Theorem, věta o hustotě prvočísel)

Nechť $\pi(x)$ udává počet prvočísel menších nebo rovných číslu $x \in \mathbb{R}$. Pak

$$\pi(x) \sim \frac{x}{\ln x},$$

tj. podíl funkcí $\pi(x)$ a $x/\ln x$ se pro $x \to \infty$ limitně blíží k 1.

Poznámka

To, jak jsou prvočísla hustě rozmístěna v množině přirozených čísel, rovněž udává Eulerův výsledek $\sum_{p \in P} \frac{1}{p} = \infty$. Přitom např. $\sum_{n \in \mathbb{N}} \frac{1}{n^2} = \frac{\pi^2}{6}$, což znamená, že prvočísla jsou v $\mathbb{N}$ rozmístěna „hustěji“ než druhé mocniny.

Věta

Je-li P množina všech prvočísel, pak $\sum_{p\in P}\frac{1}{p}=\infty$.

Důkaz.

Buď n libovolné přirozené číslo a $p_1,\ldots,p_{\pi(n)}$ všechna prvočísla nepřevyšující n. Položme

$$\lambda(n)=\prod_{i=1}^{\pi(n)}\left(1-\frac{1}{p_i}\right)^{-1}.$$

Jednotlivé činitele lze chápat jako součet geometrické řady, proto

$$\lambda(n)=\prod_{i=1}^{\pi(n)}\left(\sum_{\alpha_i=0}^{\infty}\frac{1}{p_i^{\alpha_i}}\right)=\sum\frac{1}{p_1^{\alpha_1}\cdots p_{\pi(n)}^{\alpha_{\pi(n)}}},$$

kde sčítáme přes všechny $\pi(n)$-tice nezáporných celých čísel $(\alpha_1,\ldots,\alpha_{\pi(n)})$.

Důkaz.

Protože každé číslo nepřevyšující n se rozkládá pouze na prvočísla z množiny $\{p_1, \ldots, p_{\pi(n)}\}$, je určitě každé takové číslo v tomto součtu zahrnuto. Tedy $\lambda(n) > 1 + \frac{1}{2} + \cdots + \frac{1}{n}$, a protože harmonická řada diverguje , je i $\lim_{n\to\infty} \lambda(n) = \infty$.
S využitím rozvoje funkce $\ln(1+x)$ do mocninné řady dále dostáváme

$$\ln \lambda(n) = -\sum_{i=1}^{\pi(n)} \ln\left(1 - \frac{1}{p_i}\right) = \sum_{i=1}^{\pi(n)} \sum_{m=1}^{\infty} (m p_i^m)^{-1} =$$

$$= p_1^{-1} + \cdots + p_{\pi(n)}^{-1} + \sum_{i=1}^{\pi(n)} \sum_{m=2}^{\infty} (m p_i^m)^{-1}.$$

Důkaz.

$$\ln \lambda(n) = p_1^{-1} + \cdots + p_{\pi(n)}^{-1} + \sum_{i=1}^{\pi(n)} \sum_{m=2}^{\infty} (m p_i^m)^{-1}.$$

Protože vnitřní součet lze shora odhadnout jako

$$\sum_{m=2}^{\infty} (m p_i^m)^{-1} < \sum_{m=2}^{\infty} p_i^{-m} = \\ = p_i^{-2} \left(1 - p_i^{-1}\right)^{-1} \leq 2 p_i^{-2},$$

umíme shora odhadnout i divergující posloupnost $\ln \lambda(n) < \sum_{i=1}^{\pi(n)} p_i^{-1} + 2 \sum_{i=1}^{\pi(n)} p_i^{-2}$. Druhý součet přitom zřejmě konverguje (viz konvergence řady $\sum_{n=1}^{\infty} n^{-2}$), proto musí nutně divergovat první součet $\sum_{i=1}^{\pi(n)} p_i^{-1}$, což jsme chtěli dokázat. □

Příklad

O tom, jak odpovídá asymptotický odhad $\pi(x) \sim x/\ln(x)$,
v některých konkrétních příkladech vypovídá následující tabulka:

x	$\pi(x)$	$x/\ln(x)$	rel. chyba	Li(x)	rel. chyba
100	25	21,7	0,13	29,1	0,04
1000	168	144,7	0,13	176,6	0,01
10000	1229	1085,7	0,11	1245,1	0,002
100000	9592	8685,9	0,09	9628,8	0,0004
500000	41538	38102,9	0,08	41605,2	0,0001

$Li(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$ značí tzv. logaritmický integrál.