

## 2. Prvočísla

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,  $\dots$ . Prvočísel je, jak brzy dokážeme, nekonečně mnoho, máme ovšem poměrně limitované výpočetní prostředky na zjištění, zda je dané číslo prvočíslem (největší známé prvočíslo  $2^{30\,402\,457} - 1$  má pouze 9 152 052 cifer).

**VĚTA 6.** *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 věty 5.

„ $\Leftarrow$ “ 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  $b$ .  $\square$

**PŘÍKLAD.** Nalezněte všechna čísla  $k \in \mathbb{N}_0$ , pro která je mezi deseti po sobě jdoucími čísly  $k + 1, k + 2, \dots, k + 10$  nejvíce prvočísel.

**ŘEŠENÍ.** Pro  $k = 1$  je mezi našimi čísly pět prvočísel: 2, 3, 5, 7, 11. Pro  $k = 0$  a  $k = 2$  pouze čtyři prvočísla. Jestliže  $k \geq 3$ , není mezi zkoumanými čísly číslo 3. Mezi deseti po sobě jdoucími celými čísly pět sudých a pět lichých čísel, mezi kterými je zase aspoň jedno dělitelné třemi. Našli jsme tedy mezi čísly  $k + 1, k + 2, \dots, k + 10$  aspoň šest složených, jsou tedy mezi nimi nejvýše čtyři prvočísla. Zadání proto vyhovuje jedině číslu  $k = 1$ .  $\square$

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

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

**PŘÍKLAD.** Dokažte, že pro libovolné prvočíslo  $p$  a libovolné  $k \in \mathbb{N}$ ,  $k < p$ , je kombinační číslo  $\binom{p}{k}$  dělitelné  $p$ .

ŘEŠENÍ. Podle definice kombinačního čísla

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1) \cdots (p-k+1)}{1 \cdot 2 \cdots k} \in \mathbb{N},$$

a tedy  $k! \mid p \cdot a$ , kde jsme označili  $a = (p-1) \cdots (p-k+1)$ . Protože  $k < p$ , není žádné z čísel  $1, 2, \dots, k$  dělitelné prvočíslem  $p$ , a tedy podle věty 6 není ani  $k!$  dělitelné prvočíslem  $p$ , odkud  $(k!, p) = 1$ . Podle věty 5 platí  $k! \mid a$ , a tedy  $b = \frac{a}{k!}$  je celé číslo. Protože  $\binom{p}{k} = \frac{pa}{k!} = pb$ , je číslo  $\binom{p}{k}$  dělitelné číslem  $p$ .  $\square$

VĚTA 7. *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 jako v 1.1 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 činitelů 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  $p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_s$ , kde  $p_1, \dots, p_m, q_1, \dots, q_s$  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  $1 \leq m \leq s$ . Inducí vzhledem k  $m$  dokážeme, že  $m = s, p_1 = q_1, \dots, p_m = q_m$ .

Je-li  $m = 1$ , je  $p_1 = q_1 \cdots q_s$  prvočíslo. Kdyby  $s > 1$ , mělo by číslo  $p_1$  dělitele  $q_1$  takového, že  $1 < q_1 < p_1$  (neboť  $q_2 q_3 \cdots q_s > 1$ ), 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  $p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_s$ , dělí  $p_m$  součin  $q_1 \cdots q_s$ , což je podle věty 6 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  $p_1 \cdot p_2 \cdots p_{m-1} = q_1 \cdot q_2 \cdots q_{s-1}$ , 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 i celá věta 7 je dokázána.  $\square$

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/primality\\_v6.pdf](http://www.cse.iitk.ac.in/users/manindra/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).

Že je problém rozkladu přirozeného čísla na prvočísla výpočetně složitý, o tom svědčí i výzva učiněná firmou RSA Security (viz <http://www.rsasecurity.com/rsalabs/node.asp?id=2093>). Pokud se vám podaří rozložit čísla označená podle počtu cifer jako RSA-704, RSA-768, ..., RSA-2048, obdržíte 30 000, 50 000, ..., resp. 200 000 dolarů (čísla RSA-576 a RSA-640 již byla rozložena v roce 2003, resp. 2005; byla-li vyplacena slíbená odměna, mi není známo).

DŮSLEDEK. (1) Jsou-li  $p_1, \dots, p_k$  navzájem různá prvočísla a  $n_1, \dots, n_k \in \mathbb{N}_0$ , je každý kladný dělitel čísla  $a = p_1^{n_1} \cdots p_k^{n_k}$  tvaru  $p_1^{m_1} \cdots p_k^{m_k}$ , 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

$$\tau(a) = (n_1 + 1)(n_2 + 1) \cdots (n_k + 1)$$

kladných dělitelů, jejichž součet je

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

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

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

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

POZNÁMKA. 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.  $6 = 1 + 2 + 3$ ,  $28 = 1 + 2 + 4 + 7 + 14$ ,  $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$  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: *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“ – obecně je pro velká čísla, u kterých se nedaří nalézt netriviálního dělitele, obtížné prokázat, že jsou prvočísla. Pro Mersenneho prvočísla existuje poměrně jednoduchý a rychlý postup. Proto není náhodou, že největší známá prvočísla jsou obvykle tvaru  $2^k - 1$  (viz např. <http://www.utm.edu/research/primes/largest.html>).

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

**PŘÍKLAD.** Dokažte, že pro každé celé  $n > 2$  existuje mezi čísly  $n$  a  $n!$  alespoň jedno prvočíslo.

**ŘEŠENÍ.** Označme  $p$  libovolné prvočíslo dělící číslo  $n! - 1$  (takové existuje podle věty 7, 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.  $\square$

Nyní uvedeme několik důkazů toho, že existuje nekonečně mnoho prvočísel (i když tvrzení v podstatě vyplývá už z předchozího příkladu).

**VĚTA 8.** *Mezi přirozenými čísly existuje nekonečně mnoho prvočísel.*

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

(Kummer, 1878): Předpokládejme, že prvočísel je konečně mnoho a označme je  $p_1 < p_2 < \dots < p_n$ . Položme  $N = p_1 \cdot p_2 \cdot \dots \cdot p_n > 2$ . Číslo  $N - 1$  je podle věty 7 dělitelné některým prvočíslem  $p_i$ , které dělí zároveň číslo  $N$  a tedy i  $N - (N - 1) = 1$ . Spor.

(Fürstenberg, 1955):

*V této poznámce uvedeme elementární „topologický“ důkaz existence nekonečně mnoha prvočísel. Zavedeme topologii prostoru celých čísel pomocí báze tvořené aritmetickými posloupnostmi (od  $-\infty$  do  $+\infty$ ). Lze snadno ověřit, že jde skutečně o topologický prostor, navíc lze ukázat, že je normální a tedy metrizable. Každá aritmetická posloupnost je uzavřená i otevřená množina (její*

*komplement je sjednocení ostatních aritmetických posloupností se stejnou diferencí). Dostáváme, že sjednocení konečného počtu aritmetických posloupností je uzavřená množina. Uvažme množinu  $A = \cup A_p$ , kde  $A_p$  je tvořena všemi násobky  $p$  a  $p$  probíhá všechna prvočísla. Jediná celá čísla nepatřící do  $A$  jsou  $-1$  a  $1$  a protože množina  $\{-1, 1\}$  zřejmě není otevřená, množina  $A$  nemůže být uzavřená. A tedy není konečným sjednocením uzavřených množin, což znamená, že musí existovat nekonečně mnoho prvočísel.*

□

**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  $p_1 = 2, p_2 = 5, p_3 = 11, \dots, p_n$ . Položme  $N = 3p_2 \cdot p_3 \cdot \dots \cdot p_n + 2$ . Rozložíme-li  $N$  na součin prvočísel podle věty 7, musí v tomto rozkladu vystupovat aspoň jedno prvočíselo  $p$  tvaru  $3k + 2$ , neboť v opačném případě by bylo  $N$  součinem prvočísel tvaru  $3k + 1$  (uvažte, že  $N$  není dělitelné třemi), a tedy podle příkladu na str. 7 by bylo i  $N$  tvaru  $3k + 1$ , což neplatí. Prvočíselo  $p$  ovšem nemůže být žádné z prvočísel  $p_1, p_2, \dots, p_n$ , jak plyne z tvaru čísla  $N$ , a to je spor. □

Předchozí příklady je možné značně zobecnit. Platí totiž tvrzení, které bývá nazýváno Bertrandovým postulátem nebo Čebyševovou větou:

**VĚTA 9. (Čebyševova)**

- (1) *libovolné přirozené číslo  $n > 5$  existují mezi čísly  $n$  a  $2n$  alespoň dvě prvočísla.*
- (2) *Pro každé číslo  $n > 3$  existuje mezi čísly  $n$  a  $2n - 2$  alespoň jedno prvočíselo.*

**DŮKAZ.** Důkaz lze provést elementárními prostředky, je však poměrně dlouhý, proto zde není uveden. Viz např. <http://matholymp.com/TUTORIALS/Bertrand.pdf> □

Z tvrzení uvedených v této kapitole je možné si udělat hrubou představu o tom, jak „hustě“ se mezi přirozenými čísly prvočísla vyskytují. Přesněji (i když „pouze“ asymptoticky) to popisuje tzv. „prime number theorem“:

**VĚTA 10. (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  $x \rightarrow \infty$  limitně blíží k nule.

POZNÁMKA. To, jak jsou prvočísla hustě rozmístěna v množině přirozených čísel, rovněž udává Eulerův výsledek

$$\sum_{p \text{ prvočíslo}} \frac{1}{p} = \infty.$$

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 možnosti.

POUŽITÍ V PARI-GP. O tom, jak odpovídá asymptotický odhad  $\pi(x) \sim x/\ln(x)$ , v některých konkrétních příkladech vypovídá následující tabulka (získaná s využitím funkce `primepi(x)` v Pari-GP).

```
? v=[100,1000,10000,100000,500000];
? for(k=1,5,print(v[k], „&“, primepi(v[k]), „&“, \
v[k]/log(v[k]), „&“, \
(primepi(v[k])-v[k]/log(v[k]))/primepi(v[k])))
```

$x$	$\pi(x)$	$x/\ln(x)$	relativní chyba
100	25	21.71	0.13
1000	168	144.76	0.13
10000	1229	1085.73	0.11
100000	9592	8685.88	0.09
500000	41538	38102.89	0.08

Poslední příklad (o nekonečnosti počtu prvočísel tvaru  $3k + 2$ ) zobecňuje *Dirichletova věta o aritmetické posloupnosti*:

VĚTA 11. (*Dirichletova*) Jsou-li  $a, m$  nesoudělná přirozená čísla, existuje nekonečně mnoho přirozených čísel  $k$  tak, že  $mk + a$  je prvočíslo. Jinými slovy, mezi čísly  $1 \cdot m + a, 2 \cdot m + a, 3 \cdot m + a, \dots$  existuje nekonečně mnoho prvočísel.

DŮKAZ. Jde o hlubokou větu teorie čísel, k jejímuž důkazu je zapotřebí aparát značně přesahující její elementární část. Viz např. [2, kap. ???]  $\square$

OZNAČENÍ. Pro libovolné prvočíslo  $p$  a libovolné přirozené číslo  $n$  je podle věty 7 jednoznačně určen exponent, se kterým vystupuje  $p$  v rozkladu čísla  $n$  na prvočinitele (pokud  $p$  nedělí číslo  $n$ , považujeme tento exponent za nulový). Budeme jej označovat symbolem  $v_p(n)$ . Pro záporné celé číslo  $n$  klademe  $v_p(n) = v_p(-n)$ .

Podle důsledku 2 můžeme právě zavedené označení  $v_p(n)$  charakterizovat tím, že  $p^{v_p(n)}$  je nejvyšší mocninou prvočísla  $p$ , která dělí číslo  $n$ , nebo tím, že  $n = p^{v_p(n)} \cdot m$ , kde  $m$  je celé číslo, které není dělitelné číslem  $p$ . Odtud snadno plyne, že pro libovolná nenulová celá čísla  $a, b$  platí

$$v_p(ab) = v_p(a) + v_p(b) \quad (8)$$

$$v_p(a) \leq v_p(b) \wedge a + b \neq 0 \implies v_p(a + b) \geq v_p(a) \quad (9)$$

$$v_p(a) < v_p(b) \implies v_p(a + b) = v_p(a) \quad (10)$$

$$v_p(a) \leq v_p(b) \implies v_p((a, b)) = v_p(a) \wedge v_p([a, b]) = v_p(b) \quad (11)$$

Na následujícím příkladu demonstrováme užitečnost zavedeného označení.

**PŘÍKLAD.** Dokažte, že pro libovolná přirozená čísla  $a, b, c$  platí

$$([a, b], [a, c], [b, c]) = [(a, b), (a, c), (b, c)]$$

**ŘEŠENÍ.** Podle věty 7 budeme hotovi, ukážeme-li, že  $v_p(L) = v_p(P)$  pro libovolné prvočísla  $p$ , kde  $L$ , resp.  $P$  značí výraz na levé, resp. pravé straně. Nechť je tedy  $p$  libovolné prvočísla. Vzhledem k symetrii obou výrazů můžeme bez újmy na obecnosti předpokládat, že  $v_p(a) \leq v_p(b) \leq v_p(c)$ . Podle (11) platí  $v_p([a, b]) = v_p(b)$ ,  $v_p([a, c]) = v_p([b, c]) = v_p(c)$ ;  $v_p((a, b)) = v_p((a, c)) = v_p(a)$ ,  $v_p((b, c)) = v_p(b)$ , odkud  $v_p(L) = v_p(b) = v_p(P)$ , což jsme měli dokázat.  $\square$