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 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots$ (zejména číslo 1 za prvočíslo ani za číslo složené nepovažujeme, je totiž invertibilní, neboli jednotkou okruhu celých čísel). Prvočísel je, jak brzy dokážeme, nekonečně mnoho, máme ovšem poměrně limitované výpočetní prostředky na zjištění, zda je dané číslo prvočíslem; číslo $2^{82\,589\,933} - 1$, které bylo v roce 2018 největším známým prvočíslem, má pouze 24 862 048 cifer a jeho dekadické vyjádření by se tak vešlo na kdejaký prehistorický datový nosič, při tisku knihy o 60 řádcích na stránku a 80 znacích na řádek by nicméně i tak zabralo 5 180 stran.

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

Věta 6 (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. „⇒“ 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.

„⇐“ 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. □

Příklad. Nalezněte všechna čísla $k \in \mathbb{N}_0$, pro která je mezi deseti po sobě jdoucími čísly $k + 1, k + 2, \ldots, k + 10$ 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 $k + 1$, $k + 2$, …, $k + 10$ aspoň šest složených, jsou tedy mezi nimi nejvýše čtyři prvočísla. Zadání proto vyhovuje jediné číslo $k = 1$. □

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

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

a tedy $k! \mid p \cdot a$, kde jsme označili $a = (p-1) \cdot \dots \cdot (p-k+1)$. 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. □

Věta 7. *Libovolné přirozené číslo n 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, $n = 1$ je součinem prázdné množiny[1] prvočísel)*

Poznámka. Dělitelnost je možné obdobným způsobem jako v 1.2 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 $p_1 \cdot p_2 \cdot \dots \cdot p_m = q_1 \cdot q_2 \cdot \dots \cdot q_s$, kde $p_1, \dots, p_m$, $q_1, \dots, q_s$ jsou prvočísla a navíc platí $p_1 \leq p_2 \leq \dots \leq p_m$, $q_1 \leq q_2 \leq \dots \leq q_s$ a $1 \leq m \leq s$. Indukcí vzhledem k m dokážeme, že $m = s$, $p_1 = q_1, \dots, p_m = q_m$.

Je-li $m = 1$, je $p_1 = q_1 \cdot \dots \cdot q_s$ 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 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

[1] V řeči teorie okruhů jde o jedničku okruhu celých čísel, která je dle obvyklé konvence součinem prázdné množiny prvků okruhu.

analogicky se dokáže, že $q_s = p_j$ pro vhodné $j \in \{1, 2, \ldots, m\}$. Odtud plyne

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

takže $p_m = q_s$. Vydělením dostaneme $p_1 \cdot p_2 \cdot \cdots \cdot p_{m-1} = q_1 \cdot q_2 \cdot \cdots \cdot q_{s-1}$, a tedy z indukčního předpokladu $m - 1 = s - 1$, $p_1 = q_1, \ldots, p_{m-1} = q_{m-1}$. Celkem tedy $m = s$ a $p_1 = q_1, \ldots, p_{m-1} = q_{m-1}$, $p_m = q_m$. Jednoznačnost, a proto i celá věta 7 je dokázána. □

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). Nejrychlejší obecně použitelný faktorizační algoritmus, tzv. *síto v číselném tělese*, je sub-exponenciální časové složitosti $O\left(\mathrm{e}^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$.

Peter Shor v roce 1994 vymyslel algoritmus, který číslo N faktorizuje v kubickém čase (tento algoritmus je tedy časové složitosti $O\left(\log^3 N\right)$) na kvantovém počítači. Je k tomu nicméně třeba sestrojit počítače s dostatečným počtem kvantových bitů (tzv. qubits) – jak je to obtížné, lze vysledovat z toho, ze v roce 2001 se IBM podařilo pomocí kvantového počítače rozložit číslo 15, v roce 2012 byl dosažen další faktorizační rekord rozkladem čísla 21, následovali čínští fyzikové (s využitím jistého triku jim stačil NMR kvantový počítač s pouhými čtyřmi qubity k rozkladu čísla 143) a v závěru roku 2014 bylo ukázáno, že tentýž počítač je schopný rozložit i číslo 56 153 (viz `https://en.wikipedia.org/wiki/Timeline_of_quantum_computing`).

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 další ale 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. *(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 $a = p_1^{n_1} \cdot \dots \cdot p_k^{n_k}$ tvaru $p_1^{m_1} \cdot \dots \cdot p_k^{m_k}$, kde $m_1, \dots, m_k \in \mathbb{N}_0$ a $m_1 \le n_1$, $m_2 \le n_2$, $\dots$, $m_k \le n_k$.*
Číslo a má tedy právě

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

kladných dělitelů, jejichž součet je

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

(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

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

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

2.1. Dokonalá čísla a jejich vztah k prvočíslům. Se součtem všech kladných dělitelů daného čísla souvisí pojem tzv. *dokonalého čísla*. Řekneme, že a je dokonalé, pokud splňuje podmínku $\sigma(a) = 2a$, resp. slovně, pokud *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 následující fakt.

Tvrzení 2.1. *Přirozené číslo a je sudé dokonalé číslo, právě když je tvaru $a = 2^{q-1}(2^q - 1)$, kde $2^q - 1$ je prvočíslo.*

Důkaz. Je-li $a = 2^{q-1}(2^q - 1)$, kde $p = 2^q - 1$ je prvočíslo, pak z předchozího tvrzení plyne

$$\sigma(a) = \frac{2^q - 1}{2 - 1} \cdot (p + 1) = (2^q - 1) \cdot 2^q = 2a.$$

Takové číslo a je tedy dokonalé.

Pro důkaz opačného směru uvažme libovolné sudé dokonalé číslo a a pišme

$$a = 2^k \cdot m, \text{ kde } m, k \in \mathbb{N} \text{ a } 2 \nmid m.$$

Protože je funkce σ multiplikativní (viz 3.2), je $\sigma(a) = \sigma(2^k) \cdot \sigma(m) = (2^{k+1} - 1) \cdot \sigma(m)$. Přitom ale z dokonalosti čísla a plyne $\sigma(a) = 2a = 2^{k+1} \cdot m$, odkud

$$2^{k+1} \cdot m = (2^{k+1} - 1) \cdot \sigma(m).$$

Protože je $2^{k+1} - 1$ liché, nutně $2^{k+1} - 1 \mid m$ a můžeme položit $m = (2^{k+1} - 1) \cdot n$ pro vhodné $n \in \mathbb{N}$. Úpravou dostáváme $2^{k+1} \cdot$

$n = \sigma(m)$. Mezi dělitele čísla m přitom patří čísla m i n (a protože $\frac{m}{n} = 2^{k+1} - 1 > 1$, jsou tato čísla nutně různá), proto

$$2^{k+1} \cdot n = \sigma(m) \geq m + n = 2^{k+1} \cdot n,$$

a tedy $\sigma(m) = m+n$. To znamená, že m je prvočíslo s jedinými děliteli m a $n = 1$, odkud $a = 2^k \cdot (2^{k+1} - 1)$, kde $2^{k+1} - 1 = m$ je prvočíslo. □

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

Mersenneho prvočísla jsou právě prvočísla tvaru $2^k - 1$. Není bez zajímavosti, 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 $2^k - 1$.

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), navíc 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 dolarů 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).

2.2. Rozložení prvočísel.

> *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

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. □

[2]Viz např. titulek iDnes z 6.února 2013: *Největší známé prvočíslo na světě má 17 milionů číslic a je k ničemu*