Diskrétní matematika I

Zuzana Masáková

17. srpna 2015

Obsah

1 Dělitelnost a faktorizace v okruhu celých čísel $\mathbb{Z}$

Budeme se zabývat celými, speciálně přirozenými čísly. Pro $a, b \in \mathbb{N}$ značení $a|b$ znamená, že existuje takové $c \in \mathbb{N}$ tak, že $b = ac$. Čteme „Číslo a dělí číslo b.“ Pojem dělitelnosti lze zřejmě rozšířit na $a, b \in \mathbb{Z}$, nám ale povětšinou postačí držet úvahy v přirozených číslech. Tam platí $a|b \Rightarrow a \leq b$, potažmo $a|b$ a $b|a \Leftrightarrow a = b$. Za zjevné považujeme, že $a|b$ a $b|c$ implikuje $a|c$; $a|b$ a $a|c$ implikuje $a|(b \pm c)$; $a|b$ implikuje $a|bc$ pro každé $c \in \mathbb{N}$; $a|b$ a $c|d$ implikuje $ac|bd$.

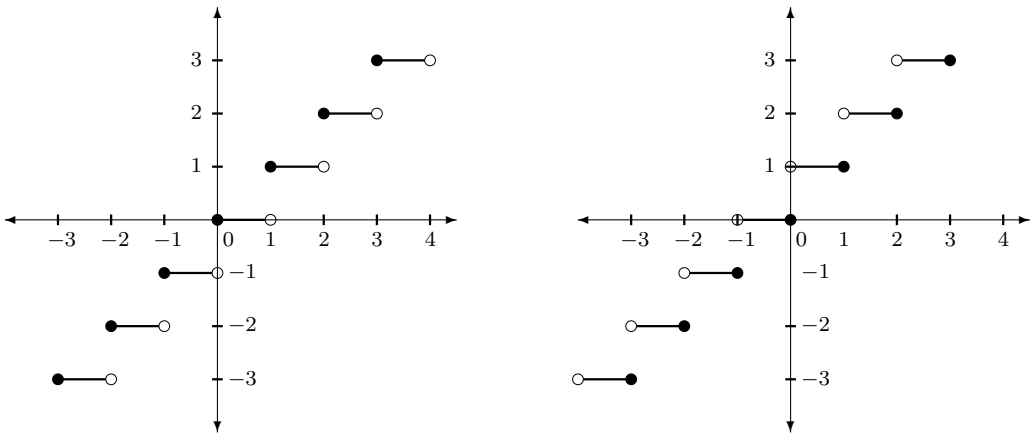
1.1 Eukleidův algoritmus

Věta 1.1 (Věta o zbytku)**.** *Pro všechna $m, n \in \mathbb{N}$ existuje právě jedno $k \in \mathbb{N}_0$ a právě jedno $r \in \mathbb{N}_0$, $0 \leq r < m$, takové, že $n = km + r$.*

Důkaz. Nejprve dokažme existenci čísel k a r. Za r vezměme nejmenší nezáporný prvek množiny $M := \{n - jm \mid j \in \mathbb{N}_0\}$. Číslo k pak označuje index j, pro který se tohoto minima nabývá, tedy $r := \min(M \cap \mathbb{N}_0) = n - km$. Zbývá ukázat, že k a r splňují požadované vlastnosti. Samozřejmě $k, r \in \mathbb{N}_0$. Navíc protože r je minimální nezáporný prvek z M, musí být $n - (k+1)m < 0$, odkud můžeme získat $r < m$.

Jednoznačnost čísel k, r ověříme sporem. Předpokládejme, že existují dva různé páry $(k_1, r_1) \neq (k_2, r_2)$ splňující $k_1, k_2 \in \mathbb{N}_0$, $r_1, r_2 \in \{0, 1, \ldots, m-1\}$ a $n = k_1 m + r_1 = k_2 m + r_2$. Buď platí $r_1 = r_2$, ale pak z rovnosti $k_1 m + r_1 = k_2 m + r_2$ plyne $k_1 = k_2$. Nebo je bez újmy na obecnosti $r_1 < r_2$. Pak ale $(k_1 - k_2)m = r_2 - r_1$. Na levé straně této rovnosti je číslo dělitelné m, na pravé straně číslo v množině $\{1, 2, \ldots, m-1\}$. To je ovšem spor. □

Čísla k a r z předchozí věty, tedy neúplný podíl a zbytek při dělení čísel n a m, se dají zapsat pomocí funkce $\lfloor x \rfloor$. Tento symbol pro reálné číslo x označuje tzv. (dolní) celou část čísla x, tedy největší celé číslo menší nebo rovno x. Je to tedy právě to jediné celé číslo, které splňuje $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ a ekvivalentně $x - 1 < \lfloor x \rfloor \leq x$. Pro neúplný podíl



Obrázek 1.1: Grafy funkcí $\lfloor x \rfloor$ a $\lceil x \rceil$.

a zbytek při dělení čísel n a m platí

$$k = \left\lfloor \frac{n}{m} \right\rfloor \quad \text{a} \quad r = n - m\left\lfloor \frac{n}{m} \right\rfloor .$$

Graf funkce $\lfloor x \rfloor$ je na obrázku 1.1. Všimněme si jejího chování na záporné poloose. Máme například $\lfloor -3, 4 \rfloor = -4$, tj. tato funkce se pro záporný argument chová jinak, než například zaokrouhovací funkce v počítači.

Poznamenejme, že celá část z x se někdy značí $[x]$. Značení $\lfloor x \rfloor$ je ale vhodnější vzhledem k tomu, že se pak tato funkce snadno odliší od horní celé části z x, označené symbolem $\lceil x \rceil$, která přiřazuje nejmenší celé číslo větší nebo rovno x, tj. splňující $\lceil x \rceil - 1 < x \leq \lceil x \rceil$. Horní a dolní celá část jsou samozřejmě úzce svázány,

$$\lceil x \rceil = \begin{cases} \lfloor x \rfloor + 1 & \text{pro } x \notin \mathbb{Z}, \\ \lfloor x \rfloor & \text{pro } x \in \mathbb{Z}. \end{cases}$$

Definice 1.2. Nechť $a, b \in \mathbb{N}_0$ nejsou obě nulová čísla. $\mathrm{nsd}(a, b)$ je takové $d \in \mathbb{N}$, že $d|a$ a $d|b$ a přitom pro každé $d' \in \mathbb{N}$, které taky splňuje $d'|a$ a $d'|b$ platí, že $d'|d$ (nebo $d' \leq d$). Když je $\mathrm{nsd}(a, b) = 1$, řekneme, že a a b jsou navzájem nesoudělná a značíme $a \perp b$.

Věta 1.3. *Pro každé $a, b \in \mathbb{N}$ existuje $x_0, y_0 \in \mathbb{Z}$ tak, že $ax_0 + by_0 = \mathrm{nsd}(a, b)$.*

Důkaz. Definujme množinu $M = \{ax + by \mid x, y \in \mathbb{Z}\}$. Snadno nahlédneme, že množina M má následující vlastnosti:

- M je uzavřená na sčítání, tj. $z, w \in M$ implikuje $z + w \in M$;
- M je uzavřená na násobení celým číslem, tj. $j \in \mathbb{Z}$, $z \in M$ implikuje $jz \in M$;

- M obsahuje prvky $a, b \in M$.

Dokážeme, že nejmenší kladný prvek z množiny M je roven $\mathrm{nsd}(a, b)$. Označme

$$n := \min\{z \in M \mid z > 0\}\,.$$

V prvé řadě $n = ax_0 + by_0$ pro nějaké $x_0, y_0 \in \mathbb{Z}$. Protože $\mathrm{nsd}(a, b)$ dělí čísla a, b, musí dělit i jejich kombinaci, jakou je číslo n. Proto $\mathrm{nsd}(a, b)|n$. Ukážeme, že to platí i naopak.

Dokážme, že n dělí a. Kdyby tomu tak nebylo, pak výsledkem dělení $a = kn + r$ podle věty 1.1 získáme nenulový zbytek $r \in \{1, 2, \ldots, n-1\}$. Z vlastností množiny M ale plyne, že $r = a - kn \in M$, což je spor s volbou n jako minimálního kladného prvku v M. Podobným způsobem ověříme, že n dělí i b, a tedy platí $n|\mathrm{nsd}(a, b)$. Odtud už plyne rovnost $n = ax_0 + by_0 = \mathrm{nsd}(a, b)$. □

Myšlenka důkazu věty nám umožní dokázat některé vlastnosti největšího společného dělitele. Označíme-li totiž $M_{a,b}$ množinu celočíselných kombinací čísel a a b, platí

$$\mathrm{nsd}(a, b) = \min\{z \in M_{a,b} \mid z > 0\}\,. \tag{1.1}$$

Protože ale platí

$$\begin{aligned} M_{a,b} = \{ax + by \mid x, y \in \mathbb{Z}\} &= \{(a-b)x + b(x+y) \mid x, y \in \mathbb{Z}\} \\ &= \{(a-b)x + by \mid x, y \in \mathbb{Z}\} = M_{a-b,b}\,, \end{aligned}$$

můžeme s pomocí (1.1) odvodit, že

$$\mathrm{nsd}(a, b) = \mathrm{nsd}(a - b, b)\,.$$

Toho využívá tzv. Eukleidův algoritmus pro hledání největšího společného dělitele. Ten převádí hledání $\mathrm{nsd}(a, b)$ na hledání nsd dvou menších čísel pomocí celočíselného dělení.

$$\begin{aligned} a &= k_1 b + r_1 & \mathrm{nsd}(a, b) &= \mathrm{nsd}(a - k_1 b, b) = \mathrm{nsd}(r_1, b) \\ b &= k_2 r_1 + r_2 & \mathrm{nsd}(b - k_2 r_1, r_1) &= \mathrm{nsd}(r_2, r_1) \\ r_1 &= k_3 r_2 + r_3 & &= \mathrm{nsd}(r_3, r_2) \\ &\vdots & &\vdots \\ r_{j-1} &= k_{j+1} r_j + r_{j+1} & &= \mathrm{nsd}(r_j, r_{j+1}) \end{aligned}$$

Protože v každém kroku je zbytek r_i nezáporný a přitom ostře menší než číslo r_{i-1}, kterým dělíme, tj. $b > r_1 > r_2 > \cdots \geq 0$, musí po konečném počtu kroků nastat rovnost $r_{j+1} = 0$. To ale znamená, že r_j dělí r_{j-1}, a proto $\mathrm{nsd}(r_j, r_{j-1}) = \mathrm{nsd}(a, b) = r_j$.

Příklad 1.4. Najděme $\mathrm{nsd}(432, 234)$. Bez újmy na obecnosti zvolíme $a = 432$ a $b = 234$, jinak by první krok Eukleidova algoritmu roli čísel pouze zaměnil. Máme

$$432 = 1 \cdot 234 + 198$$

$$234 = 1 \cdot 198 + 36$$

$$198 = 5 \cdot 36 + 18$$

$$36 = 2 \cdot 18 + 0$$

a proto $\mathrm{nsd}(432, 234) = 18$.

Eukleidův algoritmus zároveň umožňuje najít čísla x_0, y_0 z věty 1.3. Stačí postupovat od konce. Ukažme si postup na hodnotách z příkladu 1.4.

Příklad 1.5. Z předposlední z rovností můžeme číst, že

$$\mathrm{nsd}(432, 234) = 18 = 198 - 5 \cdot 36\,.$$

Ovšem číslo 36 lze z předcházející rovnice vyjádřit $36 = 234 - 1 \cdot 198$, tudíž

$$18 = 198 - 5 \cdot (234 - 198) = 6 \cdot 198 - 5 \cdot 234\,.$$

Nyní nahradíme $198 = 432 - 234$, abychom získali

$$18 = 6 \cdot (432 - 234) - 5 \cdot 234 = 6 \cdot 432 - 11 \cdot 234\,.$$

Pro hledanou kombinace $\mathrm{nsd}(432, 234) = x_0 \cdot 432 + y_0 \cdot 234$ je tedy $x_0 = 6$ a $y_0 = 11$.

Věta 1.6. *Nechť $a, b, c \in \mathbb{N}$. Rovnice $ax+by = c$ má řešení $x, y \in \mathbb{Z}$, právě když $\mathrm{nsd}(a, b)|c$.*

Důkaz. Nutnost podmínky $\mathrm{nsd}(a, b)|c$ je zřejmá. Číslo $\mathrm{nsd}(a, b)$ totiž dělí každou celočíselnou kombinaci $ax + by$. Abychom dokázali, že podmínka je i postačující, použijeme větu 1.3. Podmínka $\mathrm{nsd}(a, b)|c$ implikuje existenci čísla c' takového, že $c = c'\mathrm{nsd}(a, b)$. Z věty 1.3 najdeme $x_0, y_0 \in \mathbb{Z}$ tak, že $ax_0 + by_0 = \mathrm{nsd}(a, b)$. Po vynásobení celé rovnice číslem c' získáváme

$$a(x_0c') + b(x_0c') = c'\mathrm{nsd}(a, b) = c\,.$$

Hledané celočíselné řešení je tedy $x = x_0c'$ a $y = y_0c'$. □

Věta 1.6 vypovídá o řešitelnosti rovnice $ax + by = c$. Její důkaz spolu s Eukleidovým algoritmem pak ukazuje postup, jak nějaké řešení této rovnice najít. Dvojice $x, y \in \mathbb{Z}$ však k daným číslům $a, b, c \in \mathbb{N}$ není dána jednoznačně. Je-li totiž $ax + by = c$, pak také například $a(x + b) + b(y - a) = c$.

Věta 1.7. *Nechť $a, b, c \in \mathbb{N}$ splňují $\mathrm{nsd}(a,b)|c$. Je-li $x_0, y_0 \in \mathbb{Z}$ jedno řešení rovnice $ax + by = c$, pak všechna řešení $x, y \in \mathbb{Z}$ této rovnice jsou dána dvojicemi*

$$(x, y) = (x_0 + kb', y_0 - ka')\,, \qquad k \in \mathbb{Z}\,, \tag{1.2}$$

kde $a', b' \in \mathbb{N}$ jsou čísla taková, že

$$a = a'\mathrm{nsd}(a,b) \quad a \quad b = b'\mathrm{nsd}(a,b)\,.$$

Důkaz. Předpokládejme, že kromě $x_0, y_0 \in \mathbb{Z}$ splňujícího $ax_0 + by_0 = c$ máme ještě další pár $x, y \in \mathbb{Z}$ takový, že $ax + by = c$. Po odečtení dostaneme $a(x_0 - x) + b(y_0 - y) = 0$, a tedy

$$\frac{y_0 - y}{x - x_0} = \frac{a}{b} = \frac{a'\mathrm{nsd}(a,b)}{b'\mathrm{nsd}(a,b)} = \frac{a'}{b'}\,.$$

Poslední ze zlomků už je ve zkráceném tvaru, takže nutně musí platit

$$y_0 - y = ka' \quad \text{a} \quad x - x_0 = kb'\,.$$

Odtud už snadno plyne, že všechna řešení rovnice $ax + by = c$ jsou ve tvaru (1.2). K důkazu tvrzení věty stačí ověřit, že každá dvojice x, y daná předpisem (1.2) už rovnici $ax + by = c$ řeší. To je ale zřejmé z dosazení

$$\begin{aligned} a(x_0 + kb') + b(y_0 - ka') &= \underbrace{ax_0 + by_0}_{c} + akb' - bka' \\ &= c + \underbrace{ak\frac{b}{\mathrm{nsd}(a,b)} - bk\frac{a}{\mathrm{nsd}(a,b)}}_{0} = c\,. \end{aligned}$$

□

Příklad 1.8. Najděme všechna celočíselná řešení rovnice $24x + 105y = 33$. Nejprve ověřme podmínku řešitelnosti danou větou 1.6, tj. zda $\mathrm{nsd}(24, 105)|33$. Největší společný dělitel můžeme vypočítat například Eukleidovým algoritmem,

$$\begin{aligned} 105 &= 4 \cdot 24 + 9 \\ 24 &= 2 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

tj. $\mathrm{nsd}(24, 105) = 3$ a rovnice má zjevně řešení. Z Eukleidova algoritmu rovněž získáme

$$3 = 9 - 6 = 9 - (24 - 2 \cdot 9) = 3 \cdot 9 - 24 = 3 \cdot (105 - 4 \cdot 24) - 24 = -13 \cdot 24 + 3 \cdot 105\,.$$

Po vynásobení číslem $33/3 = 11$ získáme jedno řešení rovnice $24x + 105y = 33$, $x_0 = -13 \cdot 11 = -143$, $y_0 = 3 \cdot 11 = 33$. Každé jiné řešení x, y pak splňuje $24(x - x_0) + 105(y - y_0) = 0$, a tedy

$$\frac{y - y_0}{x_0 - x} = \frac{24}{105} = \frac{8}{35}\,.$$

1.2 Základní věta aritmetiky

Ukažme si ještě jinou aplikaci věty 1.3.

Lemma 1.9 (Eukleidovo)**.** *Nechť $a, b, c \in \mathbb{N}$. Jestliže $a \mid bc$ a platí $a \perp b$, pak $a|c$.*

Důkaz. Z předpokladu $a|bc$ plyne existence $d \in \mathbb{N}$ takového, že $bc = ad$. Protože a a b jsou navzájem nesoudělná, můžeme použít větu 1.3. Máme tedy $x, y \in \mathbb{Z}$ taková čísla, že $ax + by = 1$. Snadnou úpravou soustavy

$$ad - bc = 0$$

$$ax + by = 1$$

dostaneme $c = a(dy + cx)$, a tedy a dělí c. □

Jako jednoduchý důsledek Eukleidova lemmatu si uveďme následující.

Důsledek 1.10. *Nechť $k \in \mathbb{N}$. Pro po dvou nesoudělná čísla $m_1, \ldots, m_k \in \mathbb{N}$ a číslo $a \in \mathbb{N}$ platí*

$$m_1 \cdots m_k | a \quad \iff \quad m_i | a \text{ pro všechna } i \in \{1, 2, \ldots, k\}\,.$$

Důkaz. Tvrzení dokážeme nejprve pro $k = 2$. Z definice $m_1 m_2 | a$ znamená, že existuje $k \in \mathbb{N}$ takové, že $a = k m_1 m_2$. Odtud je jasně vidět, že $m_1 | a$ i $m_2 | a$. Naopak když $m_1 | a$ a $a = j m_2$, nutně $m_1 | j m_2$, ale z Eukleidova lemmatu a nesoudělnosti m_1, m_2 plyne $m_1 | j$, tudíž $j = l m_1$. Proto $a = j m_2 = l m_1 m_2$, a proto $m_1 m_2 | a$. Indukcí snadno přejdeme k obecnému $k \in \mathbb{N}$. □

Poznámka 1.11. Všimněme si, že tvrzení lemmatu 1.9 neplatí bez předpokladu $a \perp b$, protože např. $6 \mid 12 = 3 \cdot 4$, ale neplatí ani $6 \mid 3$ ani $6 \mid 4$.

Některá čísla a ovšem mají vlastnost, že kdykoliv dělí součin, dělí alespoň jednoho z činitelů, a to aniž bychom požadovali nesoudělnost s ostatními činiteli. Formálně $a \mid bc \Rightarrow a|b$ nebo $a|c$. Těmito čísly jsou prvočísla, tedy čísla, která mají právě dva dělitele, a to 1 a sebe sama. Číslo 1 se za prvočíslo nepovažuje. Ve skutečnosti výše zmíněná výjimečnost vzhledem k Eukleidově lemmatu prvočísla charakterizuje, jak dokazuje následující tvrzení.

Věta 1.12. *Nechť $p \in \mathbb{N}$, $p > 1$. Číslo p je prvočíslo, právě když platí*

$$p|bc \quad \Rightarrow \quad p|b \text{ nebo } p|c \qquad \text{pro každé } b, c \in \mathbb{N}. \tag{1.3}$$

Důkaz. Abychom dokázali, že prvočísla splňují (1.3), uvědomíme si, že jestliže prvočíslo p nedělí nějaké číslo b, pak je s ním nesoudělné, protože jediný společný dělitel p a b je 1. Nyní využijeme Eukleidova lemmatu 1.9. Kdyby totiž pro nějaké $b, c \in \mathbb{N}$ platilo $p|bc$, a navíc $p \not| b$, pak je $p \perp b$ a proto z Eukleidova lemmatu $p|c$.

Pro implikaci zprava doleva zkoumejme, jaké dělitele může mít číslo $p \in \mathbb{N}$ splňující (1.3). Kdyby $p = d_1 d_2$, pak p dělí součin $d_1 d_2$ a z předpokladu p dělí alespoň jeden z činitelů d_1, d_2, řekněme d_1. Toto číslo je ale nutně $\leq p$. Proto $d_1 = p$ a $d_2 = 1$. p je tedy prvočíslo. □

Z předchozívěty snadno odvodíme indukcí následující tvrzení.

Důsledek 1.13. *Nechť p je prvočíslo a $q_1, \ldots, q_s \in \mathbb{N}$. Jestliže $p|q_1 \cdots q_s$, pak existuje index $j \in \{1, \ldots, s\}$ takový, že $p|q_j$.*

Ještě mnohokrát uvidíme, jak významnou úlohu mezi celými čísly prvočísla hrají. Mezi nejvýznamější patří fakt, že všechna ostatní přirozená čísla $n > 1$ lze získat jejich součinem.

Věta 1.14 (Základní věta aritmetiky)**.** *Každé přirozené číslo $n > 1$ lze rozložit na součin prvočísel. Tento rozklad je určen jednoznačně až na pořadí činitelů.*

Důkaz. Dokažme nejdříve tvrzení o existenci rozkladu, a to indukcí na velikost n. Jestliže n je samo prvočíslo, pak je rozklad zřejmý. Nechť je to tedy číslo složené, tj. tvaru $n = n_1 n_2$, kde $n_1, n_2 \in \mathbb{N}$, $1 < n_1, n_2 < n$. Z indukčního předpokladu existují rozklady čísel n_1 a n_2, rozklad čísla n zřejmě dostaneme jako součin rozkladů čísel n_1 a n_2.

Nyní dokažme jednoznačnost rozkladu. Pokud n je prvočíslo, pak z definice prvočísla nelze n napsat jako součin jiných prvočísel. Jeho rozklad je tedy jednoznačný. Pro spor předpokládejme, že n je nejmenší přirozené číslo, pro které rozklad není jednoznačný. Je tedy nutně n složené. Nechť

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \,, \tag{1.4}$$

kde $p_1, \ldots, p_r, q_1, \ldots, q_s$ jsou – ne nutně různá – prvočísla. Protože n je složené, platí $r, s \geq 2$. Podle ekvivalentní vlastnosti prvočísel (věta 1.12) totiž p_1 nutně dělí alespoň

jedno q_i z prvočísel $q_1, \ldots, q_s$. Bez újmy na obecnosti $p_1 | q_1$, a proto $p_1 = q_1$. Lze tedy tímto číslem rovnost (1.4) vydělit. Přirozené číslo $n' = \frac{n}{p_1} = \frac{n}{q_1} > 1$ má tedy rovněž dva rozklady na prvočinitele, a to

$$n' = p_2 \cdots p_r = q_2 \cdots q_s \,.$$

Je ovšem $n' < n$, což je spor s volbou n jako nejmenšího s touto vlastností. □

Právě dokázaná základní věta aritmetiky vyjadřuje fakt, který každý čtenář jistě zná. Každé přirozené $n > 1$ lze napsat jako součin

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \,, \tag{1.5}$$

pro nějaká navzájem různá prvočísla $p_1, \ldots, p_r$, $r \in \mathbb{N}$, a exponenty $k_1, \ldots, k_r \in \mathbb{N}$. Každý dělitel takového čísla n je pak ve tvaru

$$d = p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r} \,, \tag{1.6}$$

kde celočíselné exponenty $j_1, \ldots, j_r$ teď splňují $0 \leq j_i \leq k_i$ pro každé $i \in \{1, 2, \ldots, r\}$. Všechny dělitele čísla n získáme z (1.6) uvažováním všech přípustných r-tic exponentů $j_1, \ldots, j_r$. Protože pro exponent j_i máme $k_i + 1$ možností $0, 1, \ldots, k_i$, je celkový počet dělitelů roven

$$\tau(n) := \tau(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = \prod_{i=1}^{r} (k_i + 1) \,. \tag{1.7}$$

Funkce $\tau : \mathbb{N} \mapsto \mathbb{N}$ přiřazující přirozenému číslu počet jeho dělitelů je jedna z tzv. aritmetických funkcí, o kterých bude řeč v kapitole 2.4.

Rozklad na prvočísla se zpravidla používá při středoškolské výuce k hledání největšího společného dělitele a nejmenšího společného násobku dvou přirozených čísel m, n. Máme-li formálně zapsat $\mathrm{nsd}(m, n)$ nebo $\mathrm{nsn}(m, n)$ pomocí jejich rozkladů na prvočísla, musíme v (1.5) uvažovat exponenty i nulové. Čtenář si správnost následujícího tvrzení rozmyslí jistě sám.

Věta 1.15. *Nechť $m, n \in \mathbb{N}$ a nechť $p_1, \ldots, p_r$ jsou prvočísla taková, že každé z nich dělí buď m nebo n. Pak lze psát*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \,, \qquad m = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r} \,,$$

kde nyní exponenty k_i, l_i patří do $\mathbb{N}_0$. Potom

$$\mathrm{nsd}(m, n) = \prod_{i=1}^{r} p_i^{\min\{k_i, l_i\}} \,, \qquad \mathrm{nsn}(m, n) = \prod_{i=1}^{r} p_i^{\max\{k_i, l_i\}} \,.$$

Jako důsledek pak odvodíme

Důsledek 1.16. *Nechť* $m, n \in \mathbb{N}$. *Potom platí* $\mathrm{nsd}(m,n)\mathrm{nsn}(m,n) = mn$.

Důkaz. Stačí si uvědomit, že $\min\{a,b\} + \max\{a,b\} = a + b$ pro všechna $a, b \in \mathbb{Z}$. □

1.3 Prvočísla

Než přejdeme k dalšímu výkladu, povězme si ještě něco o prvočíslech. Už Eukleidés ukázal, že prvočísel je nekonečně mnoho.

Věta 1.17. *Prvočísel je nekonečně mnoho.*

Důkaz. Předpokládejme, že prvočísel je konečný počet, řekněme k, tedy $p_1, p_2, \ldots, p_k$. Označme $n = p_1 p_2 \ldots p_k + 1$. Číslo n je zřejmě větší než p_i pro každé $i \in \{1, 2, \ldots, k\}$. Protože n není dělitelné žádným prvočíslem mezi $p_1, \ldots, p_k$, je n buď samo prvočíslo, nebo jeho rozklad obsahuje prvočíslo, které není mezi $p_1, p_2, \ldots, p_k$. V obou případech přicházíme ke sporu s tím, že seznam $p_1, \ldots, p_k$ vyčerpal všechna prvočísla. □

V pozdějších kapitolách uvidíme, že v různých aplikacích může být důležité umět rychle najít velké náhodné prvočíslo. Podstatou je mít test k rozhodnutí o prvočíselnosti, zajímá nás ovšem i to, s jakou pravděpodobností při náhodném výběru velkého čísla na prvočíslo narazíme. Není těžké ukázat, že mezi sousedními prvočísly může být libovolně velká mezera.

Věta 1.18. Pro každé $n \in \mathbb{N}$ lze nalézt posloupnost n po sobě jdoucích složených přirozených čísel.

Důkaz. Každé číslo tvaru $(n+1)!+j$, $j \in \{2, 3, \ldots, n+1\}$, je složené, protože má netriviální dělitel j. □

Sousední prvočísla tedy mohou být libovolně daleko od sebe. Naopak existují dvojice prvočísel, jejichž rozdíl je roven dvěma. Takovou dvojicí je například 11 a 13, 17 a 19, nebo 29 a 31.

Rozložení prvočísel však nejlépe vystihuje další aritmetická funkce $\pi : \mathbb{N} \mapsto \mathbb{N}$, která danému $n \in \mathbb{N}$ spočítá počet prvočísel menších nebo rovných n. Formálně

$$\pi(n) = \#\{p \leq n \mid p \text{ je prvočíslo}\}.$$

Asymptotické chování této aritmetické funkce popisuje netriviální Hadamardova – De la Vallée Poussinova věta, jejíž důkaz se čtenář může dozvědět v přednášce z teorie čísel.

Věta 1.19 (Hadamard, De La Vallée Poussin)**.**

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1\,.$$

Této větě se také někdy říká prvočíselná věta a dokázalo ji nezávisle hned několik matematiků. Věta velmi zhruba říká, že počet prvočísel menších nebo rovných n lze pro velké n odhadnout funkcí $\frac{n}{\ln n}$. Abychom měli představu, s jakou pravděpodobností při náhodném výběru získáme prvočíslo, odhadněme počet stomístných prvočísel. Ten je roven $\pi(10^{100}) - \pi(10^{99})$. S použitím věty odhadneme

$$\pi(10^{100}) - \pi(10^{99}) \sim \frac{10^{100}}{100\ln 10} - \frac{10^{99}}{99\ln 10} = \frac{99\cdot 10^{98} - 10\cdot 10^{98}}{99\ln 10} = \frac{89}{99\ln 10}10^{98} \sim 3,9\cdot 10^{97}$$

Poměříme-li tento výsledek s počtem $10^{100} - 10^{99}$ všech stomístných přirozených čísel, vyjde

$$\frac{9\cdot 10^{99}}{3,9\cdot 10^{97}} \sim 231\,,$$

tedy v průměru každé 231. stomístné číslo je prvočíslo.

2 Kongruence

2.1 Kongruence modulo m

Relace R na množině A je množina uspořádaných dvojic prvků z A. Mezi relace patří například každému známé pojmy jako rovnost, uspořádání, apod. označované symboly $=$, $<$, $\leq$, atd. Fakt, že dvojice prvků (a, b) je v relaci, se pak častěji značí $a\mathrm{R}b$ spíše než $(a, b) \in \mathrm{R}$, tedy $a = b$, $a < b$, $a \leq b$, apod.

Relace R na množině A se nazývá ekvivalence, pokud je

1. **reflexivní**, tj. $a\mathrm{R}a$ pro každé $a \in A$,
2. **symetrická**, tj. $a\mathrm{R}b$ právě když $b\mathrm{R}a$ a
3. **tranzitivní**, tj. $a\mathrm{R}b$ a $b\mathrm{R}c$ implikuje $a\mathrm{R}c$.

Relace ekvivalence zavedená na A rozdělí množinu A na disjunktní sjednocení podmnožin, v rámci kterých jsou si všechny prvky navzájem ekvivalentní. Těmto podmnožinám se říká třídy ekvivalence a jsou jednoznačně určeny libovolným svým prvkem.

Ekvivalencí je například obyčejné $=$ na množině celých čísel. V tomto případě jsou ale třídy ekvivalence právě všechny množiny $\{n\}$, kde $n \in \mathbb{Z}$. My zavedeme ekvivalenci, která rozdělí množinu $\mathbb{Z}$ do tříd méně triviálním způsobem.

Definice 2.1. Nechť $m \in \mathbb{N}$. Řekneme, že $a, b \in \mathbb{Z}$ jsou kongruentní modulo m, jestliže m dělí rozdíl $a - b$. Značíme $a \equiv b \bmod m$.

Je snadné ověřit, že uvedená relace na množině $\mathbb{Z}$ je reflexivní, symetrická i tranzitivní, tudíž je to relace ekvivalence. Značení $a \equiv b \bmod m$ je sice vžité, ale poněkud zavádějící, protože naznačuje neexistující nesymetrii. Z tohoto důvodu někteří autoři dávají přednost zápisu $a \equiv_m b$. S tímto značením ovšem neprorazili, a tak i my se nadále budeme držet zápisu klasického s vědomím, že poznámka „ mod m“ lze vynechat, pokud je z kontextu modulus jasný.

Čtenář si jistě uvědomil, že celá čísla jsou kongruentní modulo m, právě když mají stejný zbytek po dělení číslem m. Z toho je zřejmé, že třídy ekvivalence modulo m jsou množiny $[j] = \{km + j \mid k \in \mathbb{Z}\}$. Například pro $m = 3$ tedy máme celá čísla rozdělena do tří tříd podle toho, zda mají zbytek 0, 1, nebo 2 po dělení třemi, tj.

$$\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\} \cup \{\dots, -5, -2, 1, 4, 7, \dots\} \cup \{\dots, -4, -1, 2, 5, 8, \dots\}\,.$$

Kromě reflexivity, symetrie a tranzitivity má kongruence modulo m řadu dalších vlastností, které velmi snadno plynou z definice. Některé z nich vyslovíme:

V následujícím nechť $m \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$, případně $k \in \mathbb{N}$. Platí:

- K oběma stranám kongruence lze přičíst stejné číslo, tj.

$$a \equiv b \mod m \quad \Longrightarrow \quad a + c \equiv b + c \mod m\,. \tag{2.1}$$

- Obě strany kongruence lze vynásobit stejným číslem, tj.

$$a \equiv b \mod m \quad \Longrightarrow \quad ac \equiv bc \mod m\,. \tag{2.2}$$

- Kongruence lze sčítat,

$$\begin{aligned} a &\equiv b \mod m \\ c &\equiv d \mod m \end{aligned} \quad \Longrightarrow \quad a + c \equiv b + d \mod m\,, \tag{2.3}$$

- a násobit,

$$\begin{aligned} a &\equiv b \mod m \\ c &\equiv d \mod m \end{aligned} \quad \Longrightarrow \quad ac \equiv bd \mod m\,, \tag{2.4}$$

- tedy speciálně i mocnit

$$a \equiv b \mod m \quad \Longrightarrow \quad a^k \equiv b^k \mod m\,. \tag{2.5}$$

Všechny předchozí vlastnosti snadno plynou z definice. Odvození ilustrujme na „nejkomplikovanějším“ případě (2.4). Z předpokladu máme $m|(b - a)$ a $m|(d - c)$. Chceme dokázat, že $m|(bd - ac)$. Protože $bd - ac = bd - bc + bc - ac = b(d - c) + c(b - a)$, je výsledek zřejmý.

Abychom si ovšem osvojili pojem ekvivalence, je vhodné abychom výše uvedené vlastnosti odvodili i jiným způsobem. Z definice snadno dokážeme pouze vztah první, tj. (2.1), zbytek pak odvodíme pomocí tranzitivity relace $\equiv$.

Jestliže $a \equiv b \bmod m$ a platí (2.1), pak přičtením a k oběma stranám dostaneme $a + a \equiv b + a \bmod m$ a přičtením b dostaneme $a + b \equiv b + b \bmod m$. Z tranzivity pak $a + a \equiv b + b \bmod m$, tj. $2a \equiv 2b \bmod m$. Podobně přičtením $2a$ k oběma stranám $a \equiv b \bmod m$ získáme $a + 2a \equiv b + 2a$, přičtením b k již dokázanému $2a \equiv 2b \bmod m$ máme $2a + b = 2b + b \bmod m$. Z tranzitivity opět $3a \equiv 3b \bmod m$. Takto bychom odvodili (2.2) pro každé $c \in \mathbb{Z}$.

Pro důkaz (2.3) stačí přičíst c k oběma stranám $a \equiv b \bmod m$ a přičíst b k oběma stranám $c \equiv d \bmod m$. Tranzitivita opět implikuje výsledek. Vlastnost (2.4) pak obdržíme s použitím již odvozené (2.2), a to vynásobením obou stran kongruence $a \equiv b \bmod m$ číslem c a obou stran kongruence $c \equiv d \bmod m$ číslem b.

Z kongruencí (2.1)–(2.5), které jsme právě dokázali, lze snadno odvodit následující tvrzení.

Věta 2.2. *Nechť $f(x) = c_0 + c_1 x + \cdots + c_k x^k$ je polynom s celočíselnými koeficienty a nechť $m \in \mathbb{N}$. Jestliže a, b jsou celá čísla taková, že $a \equiv b \bmod m$, pak $f(a) \equiv f(b) \bmod m$.*

Použití této věty ilustrujme na příkladě.

Příklad 2.3. Je dán polynom $f(x) = 14x^5 - 25x^4 + 35x^3 + 15x^2 - 19x + 4$. Najděme zbytek r po dělení čísla $f(20)$ číslem 7. Nejprve k pravé straně zjevné kongruence $f(x) \equiv f(x) \bmod 7$ přičteme vhodný mnohočlen $\tilde{f}$ tak, aby se počítání co nejvíce zjednodušilo. Položme $\tilde{f}(x) = -14x^5 + 28x^4 - 35x^3 - 14x^2 + 21x$. Dostaneme $f(x) + \tilde{f}(x) = 3x^4 + x^2 + 2x + 4$. Dosáhli jsme redukce koeficientů u jednotlivých mocnin x. Přitom je zřejmé, že $\tilde{f}(a)$ je dělitelné sedmi pro každé celé číslo a. Přičtěme tedy kongruenci $0 \equiv \tilde{f}(20) \bmod 7$. Celkem

$$f(20) \equiv f(20) + \tilde{f}(20) = 3 \cdot 20^4 + 20^2 + 2 \cdot 20 + 4\,.$$

Stále se nám ovšem nechce do mocnění velkých čísel. Použijeme tedy větu (2.2). Protože $20 \equiv -1 \bmod 7$, platí

$$f(20) \equiv 3 \cdot (-1)^4 + (-1)^2 + 2 \cdot (-1) + 4 \mod 7\,,$$

což už je velmi jednoduchý výpočet. Máme tedy $f(20) \equiv 6 \bmod 7$.

Vraťme se nyní zpět k vlastnostem (2.1)–(2.5) kongruencí. Implikace v případě (2.1) lze samozřejmě obrátit. Můžeme ale obrátit implikaci i v případě (2.2)? Lze říci, že $m|(cb - ca)$ implikuje $m|(b - a)$? To jistě ne, jak jsme viděli na příkladě v poznámce 1.11. S použitím

Eukleidova lemmatu 1.9 však můžeme odvodit, že

$$\text{pro } c \perp m \text{ platí} \qquad a \equiv b \mod m \quad \Longleftrightarrow \quad ac \equiv bc \mod m\,. \tag{2.6}$$

Můžeme dokonce měnit i modulus v kongruenci. Snadno se totiž ověří, že

$$a \equiv b \mod m \quad \Longleftrightarrow \quad ac \equiv bc \mod cm\,. \tag{2.7}$$

Kongruence modulo $m_1, \ldots, m_k$ pro po dvou nesoudělná souvisí s kongruencí modulo jejich součin, jak lze snadno přímo z definice kongruence odvodit z důsledku 1.10.

Tvrzení 2.4. *Nechť $m_1, \ldots, m_k$ jsou po dvou nesoudělná přirozená čísla. Pak*

$$a \equiv b \mod m_1 \cdots m_k \quad \Longleftrightarrow \quad a \equiv b \mod m_i \text{ pro všechna } i \in \{1, 2, \ldots, k\}.$$

Ve skutečnosti můžeme podobné tvrzení zapsat i pro obecnou k-tici přirozených čísel.

Tvrzení 2.5. *Nechť $m_1, \ldots, m_k$ jsou přirozená čísla. Pak*

$$a \equiv b \mod m_i \text{ pro všechna } i \in \{1, 2, \ldots, k\} \quad \Longleftrightarrow \quad a \equiv b \mod \operatorname{nsn}(m_1, \ldots, m_k).$$

2.2 Poziční soustavy a kritéria dělitelnosti

Jako jednoduchou aplikaci práce s kongruencemi připomeňme známá i méně známá kritéria dělitelnosti přirozených čísel pomocí jejich ciferného součtu. Protože důležitou roli bude hrát zápis čísel v poziční soustavě s celočíselným základem, připomeňme, jak tyto zápisy vypadají.

Věta 2.6. *Nechť $q \in \mathbb{N}$, $q > 1$. Každé přirozené číslo n lze jednoznačně vyjádřit ve tvaru*

$$n = \sum_{i=0}^{k} a_i q^i, \qquad \text{kde } k \in \mathbb{N}_0,\ a_0, \ldots, a_k \in \{0, 1, \ldots, q-1\},\ a_k \neq 0. \tag{2.8}$$

Důkaz. Nejprve ukažme jednoznačnost. Nechť existuje přirozené číslo s dvěma vyjádřeními

$$n = \sum_{i=0}^{k} a_i q^i = \sum_{j=0}^{l} b_j q^j\,,$$

kde $k, l \in \mathbb{N}$, $a_0, \ldots, a_k, b_0, \ldots, b_l \in \{0, 1, \ldots, q-1\}$ pro $a_k, b_l \neq 0$. Nechť n je nejmenší s touto vlastností. Potom $k \neq l$. Jinak by totiž číslo $n - q^k$ mělo také dvojí zápis tvaru (2.8) a to by byl spor s minimalitou n.

Bez újmy na obecnosti tedy $k \geq l+1$. Pak platí

$$n = \sum_{i=0}^{k} a_i q^i \geq q^k\,, \quad \text{ale zároveň} \quad n = \sum_{j=0}^{l} b_j q^j \leq (q-1)\sum_{j=0}^{l} q^j = q^{l+1} - 1 \leq q^k - 1\,,$$

a to je spor.

Existenci vyjádření ve tvaru (2.8) dokážeme indukcí na n. Jestliže $n \in \{0, 1, \ldots, q-1\}$, pak $a_0 = n$ a jsme hotovi. Nechť $n \geq q$. Má-li být $n = \sum_{i=0}^{k} a_i q^i$, musí nutně a_0 být rovno zbytku po dělení čísla n číslem q, protože $n \equiv a_0 \bmod q$ a $a_0 \in \{0, 1, \ldots, q-1\}$. Položme tedy $n' = \frac{n-a_0}{q}$. To je přirozené číslo ostře menší než n. Z indukčního předpokladu existuje zápis čísla n' ve tvaru

$$n' = \sum_{j=0}^{l} a'_j q^j\,,$$

kde koeficienty $a'_j \in \{0, 1, \ldots, q-1\}$. Položme $k = l+1$ a $a_i = a'_{i-1}$ pro $i = 1, \ldots, k$. Protože $n = qn' + a_0$, dostali jsme vyjádření (2.8). □

Z důkazu předchozí věty lze vyčíst algoritmus hledání rozvoje čísla n v bázi q. Mohli bychom ho zapsat takto:

Vstup: n.

Polož $i = 0$. Dokud $n > 0$, prováděj: $a_i :=$ zbytek po dělení n mod q; $n := \frac{n-a_i}{q}$; $i := i+1$.

Výstup: $a_{i-1} \cdots a_1 a_0$.

Všimněme si, že tento algoritmus počítá cifry přirozeného čísla ‘odzadu’. Konstruovat rozvoje v bázi q lze ale i jiným způsobem, než byl popsán v důkazu předchozí věty. Tzv. hladový algoritmus určuje nenulové cifry postupně od první platné, a je užitečný především pokud kromě přirozených čísel začneme chtít rozvíjet libovolné kladné číslo.

Vstup: n.

Dokud $n > 0$, prováděj: najdi $k \in \mathbb{Z}$ tak, že $q^k \leq n < q^{k+1}$; $a_k := \lfloor \frac{n}{q^k} \rfloor$; $n := n - a_k q^k$.

Výstup: $a_{i-1} \cdots a_1 a_0$.

Příklad 2.7. Najděme rozvoj čísla 493 v soustavě se základem 7. Pro ilustraci použijeme oba předvedené postupy. Máme $493 \equiv 3 \bmod 7$, proto $a_0 = 3$. Dále platí $\frac{n-a_0}{7} = \frac{490}{7} = 70 \equiv 0 \bmod 7$, proto $a_1 = 0$. Podobně $\frac{70}{7} = 10 \equiv 3 \bmod 7$, proto $a_2 = 3$. Konečně $\frac{10-3}{7} = 1$, proto $a_3 = 1$. Celkem tedy $493 = (1303)_7$.

Hladovým algoritmem najděme nejvyšší mocninu 7 obsaženou v 493. Máme $7^3 = 343 \leq 493 < 7^4$. Navíc $\lfloor 493/343 \rfloor = 1$, a proto $a_3 = 1$. Postup opakujeme s číslem $n = 493 - 1 \cdot 7^3 = 150$. Nejvyšší mocnina sedmi, která se vejde do 150 je 7^2 a navíc

$\lfloor 150/49 \rfloor = 3$. Proto $a_2 = 3$. Pokračujeme s $n = 150 - 3 \cdot 49 = 3$. Zřejmě $3 = 3 \cdot 7^0$. Celkově tedy získáváme stejný výsledek $493 = (1303)_7$.

Tvrzení 2.8. *Přirozené číslo má stejný zbytek po dělení třemi jako jeho ciferný součet v desítkové soustavě.*

Důkaz. Ciferný zápis $a_k a_{k-1} \cdots a_1 a_0$ v desítkové soustavě vyjadřuje číslo $n = a_k \cdot 10^k + \cdots + a_1 \cdot 10 + a_0$. Označíme-li jako f polynom $f(x) = a_k \cdot x^k + \cdots + a_1 \cdot x + a_0$, v němž roli celočíselných koeficientů hrají právě cifry $a_k, \ldots, a_0$, máme zjevně $n = f(10)$. Protože $10 \equiv 1 \bmod 3$, můžeme z věty 2.2 odvodit, že $f(10) \equiv f(1) \bmod 3$. Ovšem $f(1)$ není nic jiného než součet cifer $f(1) = a_k + \cdots + a_1 + a_0$. □

Tvrzení 2.9. *Přirozené číslo má stejný zbytek po dělení jedenácti jako jeho ciferný součet v desítkové soustavě se střídavými znaménky.*

Důkaz. Vyjdeme z kongruence $10 \equiv -1 \bmod 11$. Opět použitím věty 2.2 a polynomu f z důkazu předchozího tvrzení máme $n = f(10) \equiv f(-1) \bmod 11$, přičemž $f(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$. □

Kdybychom obdobným způsobem odvozovali kritérium dělitelnosti sedmi v desítkové soustavě, dostali bychom kritérium $n = f(10) \equiv f(3) \bmod 7$, které není vůbec praktické, protože ověřování dělitelnosti čísla $f(3) = a_k 3^k + \cdots + a_1 3 + a_0$ sedmi není o nic jednodušší než původní úloha. Můžeme ale postupovat 'ručně'. I tak už by ale výsledek nebyl tak elegantní. Máme totiž

$$\begin{aligned} 10^1 &\equiv 3 \mod 7 \\ 10^2 &\equiv 2 \mod 7 \\ 10^3 &\equiv -1 \mod 7 \\ 10^4 &\equiv -3 \mod 7 \\ 10^5 &\equiv -2 \mod 7 \\ 10^6 &\equiv 1 \mod 7 \end{aligned} \tag{2.9}$$

Poslední kongruenci lze umocnit na $10^{6i} \equiv 1 \bmod 7$ pro každé i. Vynásobením této kongruence jednou z (2.9), lze odvodit poněkud ošklivé kritérium

$$\begin{aligned} n \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + \\ + a_6 + 3a_7 + 2a_8 - a_9 - 3a_{10} - 2a_{11} + \cdots \mod 7\,. \end{aligned} \tag{2.10}$$

Pro dělitelnost sedmi ovšem můžeme odvodit kritérium i jiného typu.

Tvrzení 2.10. *Číslo n se zápisem $a_k a_{k-1} \cdots a_1 a_0$ v desítkové soustavě je dělitelné sedmi, právě když je dělitelné sedmi číslo $m - 2a_0$, kde desítkový zápis čísla m je tvaru $m = a_k a_{k-1} \cdots a_1$.*

Důkaz. Nejprve si uvědomme, že čísla m, n se zápisem v desítkové soustavě ve tvaru $n = (a_k \cdots a_1 a_0)_{10}$ a $m = (a_k \cdots a_1)_{10}$ jsou ve vztahu $n = 10m + a_0$. Protože $2 \perp 7$, je kongruence $n = 10m + a_0 \equiv 0 \bmod 7$ ekvivalentní s $20m + 2a_0 \equiv 0 \bmod 7$. To je ekvivalentní kongruenci $-m + 2a_0 \equiv 0 \bmod 7$ vzniklé přičtením $-21m \equiv 0 \bmod 7$. Odtud už tvrzení věty snadno plyne. □

Příklad 2.11. Ilustrujme použití obou kritérií dělitelnosti sedmi na číslo 66951. Kritériem (2.10) zjistíme, že číslo 66951 má stejný zbytek po dělení sedmi jako

$$1 + 3 \cdot 5 + 2 \cdot 9 - 1 \cdot 6 - 3 \cdot 6 = 10 \equiv 3 \mod 7\,,$$

což odpovídá realitě, protože $66951 = 7 \cdot 9564 + 3$. Naopak kritérium dané tvrzením (2.10) nám pouze sdělí informaci, že 66951 není dělitelné sedmi, protože jinak by muselo být dělitelné sedmi číslo $6695 - 2 \cdot 1 = 6693$, potažmo číslo $669 - 2 \cdot 3 = 663$, a tedy i číslo $66 - 2 \cdot 3 = 60$, a to, jak víme, dělitelné sedmi není.

Kritéria dělitelnosti můžeme samozřejmě odvozovat i pro zápis čísel v soustavě s jinou bází. Podle věty (2.6) takový vždy existuje.

Příklad 2.12. Odvoďme kritérium dělitelnosti devíti v šestnáctkové soustavě. Připomeňme, že v této soustavě cifry nabývají hodnot $0, 1, 2 \ldots, 15$, přičemž cifry $0, 1, \ldots, 9$ zapisujeme běžným způsobem, pro cifry $10, 11, 12, 13, 14, 15$ používáme znaky po řadě A, B, C, D, E, F. Máme

$$16^1 \equiv -2 \mod 9$$

$$16^2 \equiv 4 \mod 9$$

$$16^3 \equiv 1 \mod 9$$

Proto platí

$$16^{3k} \equiv 1 \mod 9$$

$$16^{3k+1} \equiv -2 \mod 9$$

$$16^{3k+2} \equiv 4 \mod 9$$

pro každé $k \in \mathbb{N}_0$. Kritérium dělitelnosti pak lze formulovat následovně: Přirozené číslo $n = a_k 16^k + \cdots a_1 16 + a_0$, kde $a_i \in \{0, 1, \ldots, 15\}$, má stejný zbytek po dělení devíti jako číslo $a_0 - 2a_1 + 4a_2 + a_3 - 2a_4 + 4a_5 + a_6 - 2a_7 + 4a_8 + \cdots$.

Jako cvičení si čtenář může odvodit kritérium dělitelnosti devíti v desítkové, třemi v šestnáctkové, či sedmi v trojkové soustavě.

2.3 Malá Fermatova věta

Velmi užitečná je tzv. malá Fermatova věta. Uvidíme ji například v kapitole o testování prvočíselnosti, ale tím její význam zdaleka nekončí.

Věta 2.13 (Malá Fermatova)**.** *Nechť p je prvočíslo a nechť $a \in \mathbb{N}$, $a \perp p$. Potom platí* $a^{p-1} \equiv 1 \bmod p$.

Pro zajímavost uvedeme několik různých důkazů této věty. První z nich využívá vlastností systému tříd ekvivalence modulo p.

Důkaz. Uvažujme čísla $a, 2a, 3a, \ldots, (p-1)a$ a označme $r_1, r_2, r_3, \ldots, r_{p-1}$ jejich zbytky po dělení číslem p, tj.

$$ja \equiv r_j \mod p \quad \text{pro } j = 1, \ldots, p-1\,. \tag{2.11}$$

Ukážeme, že tato čísla r_j pokryjí právě všechny nenulové zbytky modulo p. Formálně

$$\{r_1, r_2, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}\,. \tag{2.12}$$

Aby tato rovnost byla zřejmá, musíme ověřit, že $r_i = r_j$ pouze pro $i = j$. Rovnost $r_i = r_j$ je ekvivalentní s $ia \equiv ja \bmod p$. Díky (2.6) to však znamená, že $i \equiv j \bmod p$, a protože uvažujeme $i, j \in \{1, 2, \ldots, p-1\}$, musí nutně $i = j$. Protože čísla $r_1, \ldots, r_{p-1} \in \{1, 2, \ldots, p-1\}$ jsou navzájem různá a je jich $p-1$, musí rovnost (2.12) platit.

Vynásobme mezi sebou všechny kongruence (2.11),

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv r_1 r_2 r_3 \cdots r_{p-1} = 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p\,,$$

tj. $a^{p-1}(p-1)! \equiv (p-1)! \bmod p$. Odtud už snadno plyne výsledek, pokud si uvědomíme, že čísla $2, 3, \ldots, (p-1)$ jsou nesoudělná s p, a je tedy možné jimi kongruenci zkrátit. □

Druhý důkaz využívá binomickou větu.

Důkaz. Nejprve dokážeme matematikcou indukcí na $n \in \mathbb{N}$, že pro všechna x_i platí

$$(x_1 + \cdots + x_n)^p \equiv x_1^p + \cdots + x_n^p \mod p\,. \tag{2.13}$$

Pro $n = 1$ tvrzení nic zajímavého neříká. Dokažme platnost vzorce (2.13) pro $n = 2$. Z binomické věty máme

$$(x_1 + x_2)^p = \sum_{j=0}^{p} \binom{p}{j} x_1^j x_2^{p-j} .$$

Protože p je prvočíslo, je pro $j = 1, \ldots, p-1$ kombinační číslo

$$\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{j!}$$

násobkem p. Proto platí

$$\sum_{j=0}^{p} \binom{p}{j} x_1^j x_2^{p-j} \equiv x_1^p + x_2^p \mod p . \tag{2.14}$$

Pro důkaz tvrzení (2.13) pro obecné $n > 2$ zapíšeme

$$(x_1 + \cdots + x_{n-1} + x_n)^p = \big((x_1 + \cdots + x_{n-1}) + x_n\big)^p \equiv (x_1 + \cdots + x_{n-1})^p + x_n^p \mod p ,$$

kde jsme využili faktu (2.14). Nyní už z indukčního předpokladu plyne platnost (2.13).

Abychom dokončili důkaz věty, v kongruenci (2.13) položme $n = a$ a $x_1 = \cdots = x_a = 1$. Dostaneme $a^p \equiv a \mod p$. Protože a je nesoudělné s p, můžeme podle (2.6) obě strany této kongruence vydělit číslem a, čímž dostaneme tvrzení věty. □

Konečně uveďme ještě jeden kombinatorický „počítací“ důkaz.

Důkaz. Položme si otázku: kolik nejednobarevných náhrdelníků z p korálků lze navléknout, máme-li k dispozici libovolné množství korálků a různých barev. Náhrdelníky počítáme, když jsou rozložené na stole, tj. za shodné považujeme jen takové náhrdelníky, které lze zaměnit jen šoupáním po stole, ale nezvedáme je.

Nejdříve navlékáme p korálků do řetízku. Protože v každém kroku máme volbu a barev, nespojených řetízků je a^p. Vyloučíme-li všechny jednobarevné, je jejich počet $a^p - a$.

Nyní je třeba si uvědomit, že z jednoho nejednobarevného náhrdelníku rozstřižením na různých místech vzniknou různé řetízky. Jinak by to totiž znamenalo, že řetízek lze rozdělit na několik stejných kousků. To ovšem nejde, protože by počet p korálků musel být celočíselným násobkem menšího počtu, ale p je prvočíslo.

Tudíž každý nejednobarevný náhrdelník odpovídá p různým řetízkům. Těch je celkem $a^p - a$, takže náhrdelníků je $\frac{1}{p}(a^p - a)$. Číslo $\frac{1}{p}(a^p - a)$ tedy vyjadřuje počet, a proto musí p dělit číslo $a^p - a$. To ale podle definice znamená $a^p \equiv a \mod p$. Protože pak máme předpoklad $p \perp a$, můžeme podělit obě strany kongruence a dostat tvrzení malé Fermatovy věty. □

2.4 Řešení kongruencí a čínské zbytky

Někdy je třeba najít všechna celá čísla, která splňují zadanou kongruenci. Podíváme se na případ lineárních kongruencí. Mějme zadaná čísla $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}$. Samozřejmě platí

$$ax + b \equiv cx + d \mod m \quad \iff \quad (a - c)x \equiv d - b \mod m\,,$$

takže bez újmy na obecnosti stačí uvažovat pouze lineární kongruence ve tvaru

$$ax \equiv b \mod m\,. \tag{2.15}$$

Taková kongruence nemá nutně řešení.

Příklad 2.14. Hledejme $x \in \mathbb{Z}$ splňující $21x \equiv 8 \bmod 39$. Ptáme se tedy po existenci $x, k \in \mathbb{Z}$ tak, aby $21x = 8+39k$. Protože ale $\mathrm{nsd}(21, 39) = 3$ a $3 \not| 8$, takové řešení neexistuje.

Na příkladě jsme viděli, že o existenci řešení rozhoduje vlastně věta 1.6. Podmínka řešitelnosti lze tedy přepsat následujícím tvrzením.

Tvrzení 2.15. *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Kongruence $ax \equiv b \bmod m$ má řešení $x \in \mathbb{Z}$, právě když $\mathrm{nsd}(a, m)|b$.*

Speciálním případem kongruence (2.15) je

$$ax \equiv 1 \mod m\,, \tag{2.16}$$

která je podle tvrzení 2.15 řešitelná, právě když $\mathrm{nsd}(a, m)|1$, a tedy a je nesoudělné s m. Přepíšeme-li kongruenci z definice, zjistíme, že řešení můžeme dostat zpětným chodem Eukleidova algrotimu, protože nám ve skutečnosti jde o nalezení řešení rovnice $ax - my = 1$, o které už byla řeč dříve. U konkrétních příkladů může být početně jednodušší použít jiný způsob.

Příklad 2.16. Vyřešme kongruenci

$$29x \equiv 1 \mod 17\,. \tag{2.17}$$

Oddečtením kongruence $17x \equiv 0 \bmod 17$ a přičtením $0 \equiv 17 \bmod 17$ získáme

$$12x \equiv 18 \mod 17\,.$$

Protože $6 \perp 17$, je tato kongruence ekvivalentní

$$2x \equiv 3 \mod 17\,,$$

přičtením $0 \equiv 17 \mod 17$ dostaneme

$$2x \equiv 20 \mod 17\,,$$

a dělením dvěma (opět $2 \perp 17$) vyjde

$$x \equiv 10 \mod 17\,.$$

Řešením (2.17) jsou tedy všechna x ve tvaru $x = 10 + 17k$, kde $k \in \mathbb{Z}$.

Podívejme se nyní na problém soustav kongruencí ve stejné proměnné. Podle tvrzení 2.15 můžeme o každé z nich rozhodnout, jestli je řešitelná. Pokud alespoň jedna z nich nesplňuje podmínku řešitelnosti, pak celý systém nemá řešení. Naopak pokud všechny jsou řešitelné, můžeme celý systém převést do tvaru

$$\begin{aligned} x &\equiv r_1 \mod m_1\,, \\ &\vdots \\ x &\equiv r_k \mod m_k\,. \end{aligned} \tag{2.18}$$

Nejjednodušší situace je, pokud věchna čísla $m_1, \ldots, m_k \in \mathbb{N}$ jsou po dvou nesoudělná. Následující věta, známá jako čínská věta o zbytcích, říká, že pak řešení soustavy existuje a navíc udává předpis, jak ho najít.

Věta 2.17 (Čínská věta o zbytcích)**.** *Nechť $m_1, \ldots, m_k$ jsou po dvou nesoudělná přirozená čísla. Nechť $r_1, \ldots, r_k$ jsou libovolná celá čísla. Pak $x \in \mathbb{Z}$ je řešením soustavy kongruencí* (2.18) *právě tehdy, když*

$$x \equiv c_1 \frac{m}{m_1} r_1 + c_2 \frac{m}{m_2} r_2 + \cdots + c_k \frac{m}{m_k} r_k \mod m, \tag{2.19}$$

kde $m = m_1 m_2 \cdots m_k$ a c_i splňují $c_i \frac{m}{m_i} \equiv 1 \mod m_i$.

Důkaz. Zvolme pevné $i \in \{1, \ldots, k\}$. Protože čísla $m_1, \ldots, m_k$ jsou po dvou nesoudělná, víme, že $m_i \perp m_1 \cdots m_{i-1} m_{i+1} \cdots m_k = \frac{m}{m_i}$. Podle tvrzení 2.15 existuje c_i takové, že $c_i \frac{m}{m_i} \equiv 1 \mod m_i$, a tudíž

$$c_i \frac{m}{m_i} r_i \equiv r_i \mod m_i\,. \tag{2.20}$$

Zároveň víme, že pro $j \neq i$ je $\frac{m}{m_j}$ dělitelné číslem m_i, takže

$$c_j \frac{m}{m_j} r_j \equiv 0 \mod m_i \tag{2.21}$$

Sečteme-li přes všechna j, dostaneme

$$c_1\frac{m}{m_1}r_1 + c_2\frac{m}{m_2}r_2 + \cdots + c_k\frac{m}{m_k}r_k \equiv r_i \mod m_i\,. \tag{2.22}$$

Tím jsme dokázali, že x podle (2.19) řeší soustavu (2.18). Ukažme, že žádné jiné řešení neexistuje.

Nechť x splňuje (2.19) a nechť $y \in \mathbb{Z}$ je nějaké řešení soustavy (2.18), tedy $y \equiv r_i \mod m_i$ pro všechna i. Protože podle (2.22) také platí $x \equiv r_i \mod m_i$, máme $y \equiv x \mod m_i$ pro všechna i. S použitím tvrzení 2.4 odvodíme, že $y \equiv x \mod m$, takže y rovněž splňuje (2.19). □

Příklad 2.18. Čínskou větu o zbytcích můžeme třeba použít k nenápadnému vylákání informace o věku osoby. Zeptáme se pouze na zbytky po dělení třemi, čtyřmi a pěti. Neznámý věk x pak zjistíme vyřešením soustavy kongruencí

$$x \equiv r_1 \mod 3\,,$$
$$x \equiv r_2 \mod 4\,,$$
$$x \equiv r_3 \mod 5\,.$$

Čísla $m_1 = 3, m_2 = 4, m_3 = 5$ jsou po dvou nesoudělná, takže můžeme použít větu 2.17. Máme $m = 3 \cdot 4 \cdot 5 = 60$. K nalezení čísel c_1, c_2, c_3 můžeme použít podobné triky, jako v příkladě 2.16.

$$c_1\frac{60}{3} \equiv 1 \mod 3 \iff 20c_1 \equiv -c_1 \equiv 1 \mod 3 \iff c_1 \equiv -1 \mod 3$$
$$c_2\frac{60}{4} \equiv 1 \mod 4 \iff 15c_2 \equiv -c_2 \equiv 1 \mod 4 \iff c_2 \equiv -1 \mod 4$$
$$c_3\frac{60}{5} \equiv 1 \mod 5 \iff 12c_3 \equiv 2c_3 \equiv 1 \equiv 6 \mod 5 \iff c_3 \equiv 3 \mod 5$$

Z věty 2.17 dostáváme, že

$$x \equiv -1 \cdot 20r_1 - 1 \cdot 15r_2 + 2 \cdot 12r_3 \equiv -20r_1 - 15r_2 + 36r_3 \mod 60\,.$$

Pokud nám tedy osoba například sdělí, že $r_1 = 1$, $r_2 = 3$ a $r_3 = 1$, pak

$$x \equiv -20 - 45 + 36 = -29 \equiv 31 \equiv 91 \mod 60\,.$$

Rozhodnout, zda dané osobě je 31 nebo 91 už budeme muset od oka.

Ve větě 2.17 je velmi důležitý předpoklad nesoudělnosti modulů $m_1, \ldots, m_k$, která zaručuje řešitelnost soustavy. Ukažme si, jak nakládat se soustavami, které tento předpoklad nesplňují. Pro jednoduchost položme $k = 2$.

Věta 2.19. *Nechť m_1, m_2 jsou přirozená čísla, a $r_1, r_2 \in \mathbb{Z}$. Pak soustava*

$$\begin{aligned} x &\equiv r_1 \mod m_1\,, \\ x &\equiv r_2 \mod m_2\,, \end{aligned} \tag{2.23}$$

má řešení $x \in \mathbb{Z}$, právě když $r_1 \equiv r_2 \bmod \mathrm{nsd}(m_1, m_2)$. Pokud je tato podmínka splněna a x splňuje (2.23)*, pak $y \in \mathbb{Z}$ je řešením* (2.23)*, právě když*

$$y \equiv x \mod \mathrm{nsn}(m_1, m_2)\,. \tag{2.24}$$

Důkaz. Nejprve si všimneme, že z (2.23) máme $x = r_1 + um_1 = r_2 + vm_2$ pro nějaká $u, v \in \mathbb{Z}$. Úpravou získáme $r_2 - r_1 = um_1 - vm_2$. Toto číslo je zjevně děiltelné $\mathrm{nsd}(m_1, m_2)$, což je ekvivalentní s

$$r_1 \equiv r_2 \mod \mathrm{nsd}(m_1, m_2)\,. \tag{2.25}$$

Naopak je-li tato podmínka splňena, pak existuje řešení $u, v \in \mathbb{Z}$ rovnice $um_1 - vm_2 = r_2 - r_1$, takže najdeme řešení soustavy (2.23) jako $x = r_1 + um_1 = r_2 + vm_2$.

Je-li x takové řešení, pak y je další řešení, právě když

$$x \equiv y \equiv r_1 \mod m_1 \quad \text{a} \quad x \equiv y \equiv r_2 \mod m_2\,,$$

což je podle tvrzení 2.5 ekvivalentní (2.24). □

Příklad 2.20. Soustava

$$\begin{aligned} x &\equiv 5 \mod 63\,, \\ x &\equiv 14 \mod 36\,, \end{aligned}$$

má řešení $x \in \mathbb{Z}$, protože $\mathrm{nsd}(63, 36) = 9$ a $5 \equiv 14 \bmod 9$. Z první kongruence máme $x = 5 + 63u$. Dosazením do druhé odvodíme

$$x = 5 + 63u \equiv 14 \mod 36\,,$$

tj.

$$63u \equiv 9 \mod 36\,.$$

Tato kongruence je podle (2.7) ekvivalentní s

$$7u \equiv 1 \mod 4\,.$$

Úpravou získáme $7u \equiv -u \equiv 1 \bmod 4$, tj. $u \equiv -1 \bmod 4$. Proto

$$x = 5 + 63u = 5 + 63(-1 + 4v) = 5 - 63 + 252v = -58 + 252v\,.$$

Takové x je řešením původní soustavy pro každé $v \in \mathbb{Z}$. Všimněme si, že $252 = 9 \cdot 7 \cdot 4 = \mathrm{nsn}(63, 36)$, takže řešení odpovídá větě 2.19.

MOZNA PRIDAT Thm 2.11 str. 64 + priklad z Nathansona.

3 Aritmetické funkce

V kapitolách 1.2 a 1.3 jsme narazili na dvě posloupnosti $\tau(n)$ a $\pi(n)$ popisující nějakým způsobem aritmetické vlastnosti přirozených čísel. Takové posloupnosti můžeme chápat jako fukce s definičním oborem $\mathbb{N}$ a zapisovat hodnotu n ne jako index, nýbrž jako argument. Takovým funkcím se někdy říká aritmetické funkce. Aritmetické funkce jsou často definovány tak, že určit hodnotu pro dané n přímo z definice nelze. Zajímá nás proto, zda je možné k dané funkci nalézt vzorec výpočtu hodnoty ze znalosti prvočíselného rozkladu. K tomu lze někdy využít vlastností jako je multiplikativita. Například u funkce počtu dělitelů τ víme, že pro $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ je hodnota

$$\tau(n) = \sum_{d\in\mathbb{N},\, d|n} 1 = \sum_{j_1=0}^{k_1} \cdots \sum_{j_r=0}^{k_r} 1 = \prod_{i=1}^{r} (k_i + 1)\,,$$

z čehož lze snadno odvodit, že

$$\tau(mn) = \tau(m)\tau(n) \quad \text{pro nesoudělná } \ m \text{ a } n \ .$$

Všimněme si ale, že obecně $\tau(mn) \neq \tau(m)\tau(n)$. Například máme $\tau(10) = 4$ a $\tau(15) = 4$, ale $\tau(150) = \tau(2 \cdot 3 \cdot 5^2) = 12 \neq 16 = \tau(10)\tau(15)$.

Definice 3.1. Aritmetickou funkci $f : \mathbb{N} \to \mathbb{Z}$ nazveme multiplikativní, pokud $f(mn) = f(m)f(n)$ pro každý pár navzájem nesoudělných čísel m, n. Řekneme, že f je úplně multiplikativní, jestliže $f(mn) = f(m)f(n)$ pro každé $m, n \in \mathbb{N}$.

Pojďme se tedy podívat na další příklady aritmetických funkcí, o kterých lze vypovědět něco zajímavého a které naopak něco zajímavého samy vypovídají.

3.1 Eulerova funkce

Eulerova funkce $\varphi : \mathbb{N} \to \mathbb{N}$ je velmi užitečným nástrojem, který se vyskytuje v různých matematických souvislostech. Hodnota $\varphi(n)$ je definována jako počet přirozených čísel nepřevyšujících n, která jsou s n nesoudělná, tedy formálně

$$\varphi(n) := \left|\{k \in \mathbb{N} \mid k \leq n, k \perp n\}\right|,$$

kde symbolem $|A|$ označujeme počet prvků množiny A.

Z definice snadno určíme $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, atd. Není těžké určit hodnoty Eulerovy funkce pro prvočíslo, mocninu prvočísla a součin dvou různých prvočísel.

Tvrzení 3.2. *Nechť p, q jsou různá prvočísla, $k \in \mathbb{N}$. Pak platí*

$$(i)\ \varphi(p) = p - 1\,, \qquad (ii)\ \varphi(p^k) = p^k - p^{k-1}\,, \qquad (iii)\ \varphi(pq) = (p-1)(q-1)\,.$$

Důkaz. Tvrzení (i) je zřejmé, protože všechna čísla menší než prvočíslo p jsou s ním nesoudělná. Pro důkaz (ii) si stačí uvědomit, že čísla soudělná s p^k jsou tvaru lp pro všechna $l \in \{1, 2, \ldots, p^{k-1}\}$. Pro (iii) musíme určit čísla soudělná s pq. To jsou právě čísla lp pro $l \in \{1, 2, \ldots, q\}$ a čísla jq pro $j \in \{1, 2, \ldots, p\}$. Jediné číslo, které je zároveň tvaru lp i jq je pq. Proto $\varphi(pq) = pq - q - p + 1 = q(p-1) - (p-1) = (p-1)(q-1)$. □

Není náhoda, že pro různá prvočísla p, q platí $\varphi(pq) = (p-1)(q-1) = \varphi(p)\varphi(q)$. Funkce φ je totiž multiplikativní, jak uvidíme později.

Věta 3.3. *Nechť $n \in \mathbb{N}$. Potom* $n = \sum_{d|n} \varphi(d)$.

Důkaz. Uvažujme n zlomků se jmenovatelem n v intervalu $(0, 1]$,

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}\,.$$

Po zkrácení má zlomek $\frac{j}{n}$ ve jmenovateli nutně d, kde d je dělitelem n. Naopak každý zkrácený zlomek se jmenovatelem d, které dělí n, lze rozšířit tak, aby měl jmenovatel n. Ovšem zlomků se jmenovatelem d ve zkráceném tvaru je v intervalu $(0, 1]$ právě $\varphi(d)$, jak plyne přímo z definice Eulerovy funkce. Tvrzení věty už dtud plyne. □

Poznámka 3.4. Věta 3.3 dává návod k rekurzivnímu počítání hodnot $\varphi(n)$. Platí totiž

$$\varphi(n) = n - \sum_{d|n, d\neq n} \varphi(d)\,. \tag{3.26}$$

Máme například

$$\varphi(12) = 12 - \varphi(6) - \varphi(4) - \varphi(3) - \varphi(2) - \varphi(1) = 12 - 2 - 2 - 2 - 1 - 1 = 4\,.$$

Ze vzorce (3.26) můžeme také zrekonstruovat výsledek Tvrzení 3.2. Je totiž

$$\begin{aligned} \varphi(p) &= p - \varphi(1) = p - 1\,, \\ \varphi(pq) &= pq - \varphi(p) - \varphi(q) - \varphi(1) = pq - (p-1) - (q-1) - 1 = (p-1)(q-1)\,. \end{aligned}$$

Existuje ale mnohem snazší způsob výpočtu hodnot Eulerovy funkce.

Věta 3.5. *Pro každé $n \in \mathbb{N}$ platí*

$$\varphi(n) = n \prod_{p|n} \left(1 - \tfrac{1}{p}\right),$$

kde index p v produktu probíhá přes všechny prvočíselné dělitele čísla n.

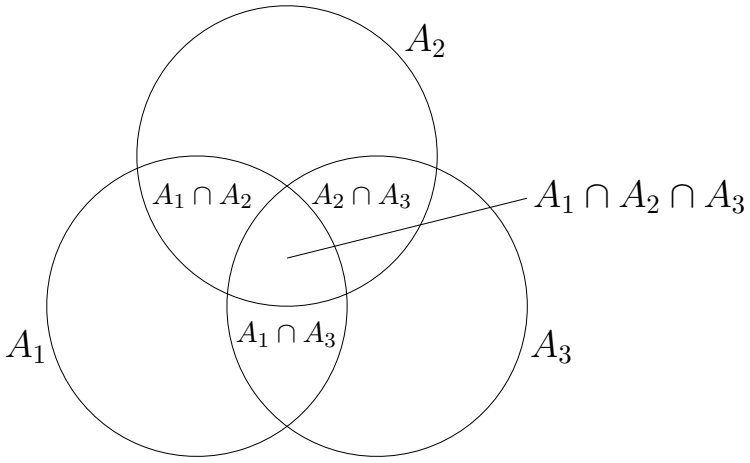
Důkaz využívá podobnou myšlenku jako u tvrzení 3.2. Čísla $k \leq n$ soudělná s n jsou právě všechny násobky prvočíselných dělitelů čísla n. Pro různé prvočíselné dělitele se ale množiny jejich násobků mohou překrývat. Abychom určili počet čísel soudělných s n, nesmíme žádné z nich počítat vícekrát. K tomu nám zásadně pomůže tzv. princip inkluze a exkluze, který určuje počet prvků ve sjednocení konečných množin, které mají neprázdné průniky. Máme-li mnpžiny A_1, A_2, pak zřejmě

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|\,.$$

Ještě pro sjednocení tří množin A_1, A_2, A_3 lze mohutnost sjednocení $A_1 \cup A_2 \cup A_3$ poměrně snadno zjistit

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_2| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|\,,$$

jak si čtenář může rozmyslet podle obrázku 3.2. Už pro čtyři množiny začínají být i diagramy dost nepřehledné. Přesto umíme mohutnost sjednocení konečného počtu množin spočítat.



Obrázek 3.2: Ilustrace principu inkluze a exkluze pro tři množiny.

Lemma 3.6 (Princip inkluze a exkluze)**.** *Nechť $A_1, \ldots, A_r$, $r \in \mathbb{N}$, jsou konečné množiny, jejich mohutnost označme $|A_i|$, $i = 1, \ldots, r$. Pro počet prvků ve sjednocení $\bigcup_{i=1}^{r} A_i$ platí*

$$\Big|\bigcup_{i=1}^{r} A_i\Big| = \sum_{j=1}^{r} (-1)^{j+1} \sum_{\{i_1,\ldots,i_j\} \subset \hat{r}} \big|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}\big|\,.$$

Důkaz. Tvrzení lemmatu dokážeme indukcí na počet prvků ve sjednocení $\bigcup_{i=1}^{r} A_i$. Pokud $\left|\bigcup_{i=1}^{r} A_i\right| = 0$, jsou všechny množiny $A_1, A_2, \ldots, A_r$ prázdné. Proto i všechny průniky na pravé straně rovnosti v tvrzení věty jsou prázdné a tvrzení platí.

Předpokládejme nyní, že sjednocení $\bigcup_{i=1}^{r} A_i$ obsahuje alespoň jeden prvek x. Množiny $A_1, \ldots, A_r$ lze tedy rozdělit na ty, které x obsahují, řekněme $A_1, \ldots, A_l$, kde $l \geq 1$, a ty, které x neobsahují, $A_{l+1}, \ldots, A_r$. Definujme nový systém množin $B_1, \ldots, B_r$ následovně:

$$B_i = \begin{cases} A_i \setminus \{x\} & \text{pro } i = 1, \ldots, l, \\ A_i & \text{pro } i = l+1, \ldots, r. \end{cases}$$

Sjednocení $\bigcup_{i=1}^{r} B_i$ tedy obsahuje všechny prvky jako $\bigcup_{i=1}^{r} A_i$ kromě x. Proto můžeme s použitím indukčního předpokladu psát

$$\left|\bigcup_{i=1}^{r} A_i\right| = 1 + \left|\bigcup_{i=1}^{r} B_i\right| = 1 + \sum_{j=1}^{r} (-1)^{j+1} \sum_{\{i_1,\ldots,i_j\}\subset\hat{r}} \left|B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_j}\right|, \tag{3.27}$$

kde v sumě na pravé straně rovnosti (3.27) sčítáme přes všechny j-prvkové podmnožiny množiny $\hat{r} = \{1, 2, \ldots, r\}$. Tyto neuspořádané j-tice $\{i_1, \ldots, i_j\}$ můžeme rozdělit na ty, pro které jsou všechny indexy $\leq l$, a ty, ve kterých je alespoň jeden index $> l$. U j-tic prvního typu platí

$$B_{i_1} \cap \cdots \cap B_{i_j} = (A_{i_1} \cap \cdots \cap A_{i_j}) \setminus \{x\},$$

tj.

$$\left|B_{i_1} \cap \cdots \cap B_{i_j}\right| = \left|A_{i_1} \cap \cdots \cap A_{i_j}\right| - 1.$$

Pro j-tice druhého typu alespoň jedna z množin A_i neobsahuje prvek x, a proto platí

$$B_{i_1} \cap \cdots \cap B_{i_j} = A_{i_1} \cap \cdots \cap A_{i_j},$$

a tedy

$$\left|B_{i_1} \cap \cdots \cap B_{i_j}\right| = \left|A_{i_1} \cap \cdots \cap A_{i_j}\right|.$$

Z rovnosti (3.27) proto odvodíme

$$\left|\bigcup_{i=1}^{r} A_i\right| - 1 = \left|\bigcup_{i=1}^{r} B_i\right| = \sum_{j=1}^{r} (-1)^{j+1} \sum_{\{i_1,\ldots,i_j\}\subset\hat{r}} \left|B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_j}\right| =$$

$$= \sum_{j=1}^{r} (-1)^{j+1} \left(\sum_{\{i_1,\ldots,i_j\}\subset\hat{l}} \underbrace{\left|B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_j}\right|}_{|A_{i_1}\cap\cdots\cap A_{i_j}|-1} + \sum_{\{i_1,\ldots,i_j\}\not\subset\hat{l}} \underbrace{\left|B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_j}\right|}_{|A_{i_1}\cap\cdots\cap A_{i_j}|} \right) =$$

$$= \sum_{j=1}^{r} (-1)^{j+1} \sum_{\{i_1,\ldots,i_j\}\subset\hat{r}} \left|A_{i_1} \cap \cdots \cap A_{i_j}\right| \; - \; \sum_{j=1}^{r} (-1)^{j+1} \sum_{\{i_1,\ldots,i_j\}\subset\hat{l}} 1.$$

Nyní je třeba si uvědomit, že j-prvkové podmnožiny $\hat{l}$ existují pouze pokud $j \leq l$, a je jich právě $\binom{l}{j}$. Proto můžeme podle binomické věty upravit

$$\sum_{j=1}^{r}(-1)^{j+1}\sum_{\{i_1,\ldots,i_j\}\subset\hat{l}} 1 \;=\; \sum_{j=1}^{l}(-1)^{j+1}\binom{l}{j} = -\sum_{j=0}^{l}(-1)^{j}\binom{l}{j} + 1 = -(1-1)^l + 1 = 1\,.$$

Tím je důkaz hotov porovnáním výsledku s (3.27). □

Důkaz věty 3.5. Je-li p prvočíselný dělitel čísla n, pak číslo lp pro $l \in \{1, 2, \ldots, \frac{n}{p}\}$ je soudělné s n a platí $lp \leq n$. Všechna čísla $k \leq n$ soudělná s n získáme, uvažujeme-li všechny prvočíselné dělitele čísla n. Nechť $n = p_1^{k_1}\cdots p_r^{k_r}$, $k_i \geq 1$, je prvočíselný rozklad čísla n. Pro $i = 1, \ldots, r$ označme

$$A_i = \Big\{ lp_i \;\Big|\; 1 \leq l \leq \frac{n}{p_i} \Big\}\,.$$

Zřejmě

$$\varphi(n) = n - \Big|\bigcup_{i=1}^{r} A_i\Big|\,.$$

Mohutnost sjednocení $\bigcup_{i=1}^{r} A_i$ zjistíme podle principu inkluze a exkluze (lemma 3.6), známe-li mohutnost průniků $A_{i_1}\cap\cdots\cap A_{i_j}$, tj. počet čísel $\leq n$, která jsou zároveň násobky navzájem různých prvočísel $p_{i_1}, \ldots, p_{i_j}$. Platí

$$\big|A_{i_1}\cap\cdots\cap A_{i_j}\big| = \frac{n}{p_{i_1}\cdots p_{i_j}}\,,$$

a proto můžeme psát

$$\varphi(n) = n - \Big|\bigcup_{i=1}^{r} A_i\Big| = n - \sum_{j=1}^{r}(-1)^{j+1}\sum_{\{i_1,\ldots,i_j\}\subset\hat{r}}\frac{n}{p_{i_1}\cdots p_{i_j}} =$$

$$= n\Big(1 + \sum_{j=1}^{r}(-1)^{j}\sum_{\{i_1,\ldots,i_j\}\subset\hat{r}}\frac{1}{p_{i_1}\cdots p_{i_j}}\Big) =$$

$$= n\sum_{j=0}^{r}(-1)^{j}\sum_{\{i_1,\ldots,i_j\}\subset\hat{r}}\frac{1}{p_{i_1}\cdots p_{i_j}} = n\prod_{i=1}^{r}\big(1-\frac{1}{p_i}\big)\,.$$

□

Uvidíme později, že důkaz lze provést i jiným způsobem, a to pomocí tzv. Möbiovy funkce (viz kapitola 3.2).

Z věty 3.5 přímo plyne následující tvrzení.

Důsledek 3.7. Eulerova funkce je multiplikativní, tj. $\varphi(nm) = \varphi(n)\varphi(m)$ pro každý pár nesoudělných čísel m, n.

Nyní dokážeme velmi důležité tvrzení, které použijeme například u šifrovacího algoritmu RSA na konci skripta.

Věta 3.8 (Euler)**.** *Jsou-li a, n navzájem nesoudělná přirozená čísla, pak*

$$a^{\varphi(n)} = 1 \bmod n\,.$$

Důkaz. Označme $a_1 < \cdots < a_{\varphi(n)}$ přirozená čísla nepřevyšující n, která jsou nesoudělná s n. Dokážeme, že množina zbytků $r_1, \ldots, r_{\varphi(n)}$ po dělení čísel $aa_1, \ldots, aa_{\varphi(n)}$ číslem n je shodná s množinou $\{a_1, \ldots, a_{\varphi(n)}\}$. K tomu si stačí uvědomit, že aa_i a tedy i r_i je číslo nesoudělné s n, a dále ověřit, že $aa_i \equiv aa_j \bmod n$ pouze pro $i = j$. To ale platí, protože díky nesoudělnosti n a a můžeme tuto kongruenci krátit a získat $a_i \equiv a_j \bmod n$, a proto $a_i = a_j$, a tedy také $i = j$.

Každý zbytek r_i je tedy roven nějakému a_j, a všechna $a_1, \ldots, a_{\varphi(n)}$ jsou vyčerpána. Všechny tyto rovnosti můžeme vynásobit a dostaneme

$$a_1 \cdots a_{\varphi(n)} = r_1 r_2 \cdots r_{\varphi(n)} \equiv (aa_1) \cdot (aa_2) \cdots (aa_{\varphi(n)}) = a^{\varphi(n)} a_1 \cdots a_{\varphi(n)} \bmod n\,.$$

Tuto kongruenci ovšem můžeme všemi čísly $a_1, \ldots, a_{\varphi(n)}$ zkrátit, čímž obdržíme znění věty. □

Čtenář si jistě všiml, že Eulerova věta ve speciálním případě, kdy $n = p$ je prvočíslo, splývá s malou Fermatovou větou 2.13, protože $\varphi(p) = p - 1$. I důkaz Eulerovy věty je zobecněním prvního z důkazů malé Fermatovy věty uvedených v kapitole 2.3.

3.2 Möbiova funkce

Dalším zajímavým příkladem aritmetické funkce je funkce Möbiova. Je to funkce $\mu : \mathbb{N} \to \{-1, 0, 1\}$ definovaná následovně: $\mu(1) = 1$, a pro $n \in \mathbb{N}, n > 1$ s prvočíselným rozkladem tvaru $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ je

$$\mu(n) = \begin{cases} (-1)^r\,, & \text{když } \alpha_1 = \alpha_2 = \ldots = \alpha_r = 1, \\ 0 & \text{jinak.} \end{cases}$$

Přímo z definice je vidět, že $\mu(n) \neq 0$ právě v případě, kdy n není dělitelné druhou mocninou žádného prvočísla. Taková čísla nazýváme čtvercuprostá.

Lemma 3.9.

$$\sum_{d|n} \mu(d) = \begin{cases} 1\,, & \text{když } n = 1, \\ 0 & \text{jinak.} \end{cases}$$

Důkaz. Pro $n = 1$ je tvrzení zřejmé. Nechť $n > 1$ a $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ je rozklad n na prvočísla. Každý dělitel d čísla n má tvar $d = q_1^{\beta_1} q_2^{\beta_2} \cdots q_r^{\beta_r}$, kde $0 \le \beta_i \le \alpha_i$. Protože $\mu(d)$ je nenulové pouze na čtvercuprostých d, v sumě jsou významné pouze členy, ve kterých indexy β_i nabývají pouze hodnot 0 a 1, a tedy platí

$$\sum_{d|n} \mu(d) = \sum_{\{i_1,\dots,i_k\}\subset\hat{r}} \mu(q_{i_1} q_{i_2} \cdots q_{i_k}) = \sum_{\{i_1,\dots,i_k\}\subset\hat{r}} (-1)^k = \sum_{k=0}^{r} \binom{r}{k} (-1)^r = 0.$$

□

Lemma 3.10 (Möbiova invertovací formule)**.** Nechť $f, g : \mathbb{N} \to \mathbb{R}$ jsou takové posloupnosti, že pro každé $n \in \mathbb{N}$ platí

$$g(n) = \sum_{d|n} f(d)\,.$$

Pak pro každé $n \in \mathbb{N}$ platí

$$f(n) = \sum_{d|n} \mu\big(\tfrac{n}{d}\big) g(d)\,.$$

Důkaz. Upravujme pravou stranu (PS) rovnosti, kterou chceme dokázat.

$$PS = \sum_{d|n} \mu\big(\tfrac{n}{d}\big) g(d) = \sum_{d|n} \mu\big(\tfrac{n}{d}\big) \sum_{d'|d} f(d')\,.$$

Je-li d dělitelem n, je rovněž $\ell = \frac{n}{d}$ dělitelem n. Proto dále lze pravou stranu upravit

$$PS = \sum_{\ell|n} \mu(\ell) \sum_{d'|\frac{n}{\ell}} f(d') = \sum_{\ell d'|n} \mu(\ell) f(d') = \sum_{d'|n} f(d') \sum_{\ell|\frac{n}{d'}} \mu(\ell) = f(n)\,,$$

kde při poslední rovnosti jsme podle lemmatu 3.9 využili, že suma $\sum\limits_{\ell|\frac{n}{d'}} \mu(\ell)$ je nenulová pouze v případě, kdy $\frac{n}{d'} = 1$. □

Jako příklad použití Möbiovy invertovací formule uvedeme jiný důkaz věty 3.5 pro Eulerovu funkci $\varphi(n)$.

Důkaz věty 3.5. Aplikujme Möbiovu invertovací formuli na vztah $n = \sum_{d|n} \varphi(d)$ daný větou 3.3,

$$\varphi(n) = \sum_{d|n} \mu\big(\tfrac{n}{d}\big) d = \sum_{d'|n} \mu(d') \frac{n}{d'}\,, \tag{3.28}$$

kde jsme využili symetrii při označení dělitele $d' = \frac{n}{d}$. Nechť $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ je prvočíselný rozklad čísla n. V sumě (3.28) stačí uvažovat sčítance s nenulovým $\mu(d)$. Proto

$$\varphi(n) = n \sum_{d|n} \mu(d) \frac{1}{d} = n \sum_{\{i_1,\ldots,i_k\} \subset \hat{r}} (-1)^k \frac{1}{q_{i_1} \cdots q_{i_k}} = n \prod_{i=1}^{r} \Big(1 - \frac{1}{q_i}\Big) .$$

□

3.3 Dokonalá čísla a Mersennova prvočísla

Další aritmetickou charakteristikou přirozených čísel je součet dělitelů. Můžeme definovat aritmetickou funkci $\sigma(n) : \mathbb{N} \to \mathbb{N}$,

$$\sigma(n) = \sum_{d|n} d \, .$$

Pokud p je prvočíslo, máme samozřejmě $\sigma(p) = p+1$. Pro mocninu prvočísla p^k, $k \in \mathbb{N}$, jsou jediní dělitelé tvaru p^j, $j = 0, \ldots, k$, a tedy platí

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \sum_{j=0}^{k} p^j = \frac{p^{k+1} - 1}{p - 1} \, .$$

Věta 3.11. *Je-li prvočíselný rozklad čísla n roven $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$, pak*

$$\sigma(n) = \sigma(q_1^{\alpha_1}) \cdots \sigma(q_r^{\alpha_r})$$

Důkaz. Vzhledem k tomu, že z prvočíselného rozvoje n lze získat tvar obecného dělitele čísla n, odvozujeme

$$\sigma(n) = \sum_{j_1=0}^{\alpha_1} \sum_{j_2=0}^{\alpha_2} \cdots \sum_{j_r=0}^{\alpha_r} q_1^{j_1} q_2^{j_2} \cdots q_r^{j_r} = \Big(\sum_{j_1=0}^{\alpha_1} q_1^{j_1} \Big) \Big(\sum_{j_2=0}^{\alpha_2} q_2^{j_2} \Big) \cdots \Big(\sum_{j_r=0}^{\alpha_r} q_r^{j_r} \Big) .$$

□

Důsledek 3.12. *σ je multiplikativní, tj. platí $\sigma(mn) = \sigma(m)\sigma(n)$ pro $m, n \in \mathbb{N}$, $m \perp n$.*

Definice 3.13. Přirozené číslo n je dokonalé, pokud je rovno polovině součtu svých dělitelů, tj. $\sigma(n) = 2n$.

Příklad 3.14. Nejmenší dokonalé číslo je $6 = 1 + 2 + 3$, tedy $\sigma(6) = 1 + 2 + 3 + 6 = 12$. Dále máme $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28$. Následující dvě dokonalá čísla jsou už ale 496 a 8128.

Můžeme se ptát, zda nějaké prvočíslo může být dokonalé. Odpověď je jednoduchá. Pro $p \in \mathbb{P}$ je $\sigma(p) = p + 1 < 2p$. Podobně ani mocnina prvočísla nemůže být dokonalé číslo, protože

$$\sigma(p^k) = 1 + p + \cdots + p^{k-1} + p^k = p^k + \frac{p^k - 1}{p - 1} \leq p^k + p^k - 1 < 2p^k \,.$$

Čtyři dokonalá čísla uvedená v příkladu 3.14 znal už Eukleides. Dokonce si všiml, že všechna jsou speciálního tvaru a tak se podařilo odvodit následující tvrzení.

Věta 3.15 (Eukleides)**.** *Nechť $n \in \mathbb{N}$. Jestliže existuje $k \in \mathbb{N}$ takové, že $2^{k+1} - 1$ je prvočíslo, pak $n = 2^k(2^{k+1} - 1)$ je dokonalé číslo.*

Důkaz. Dosadíme do vzorce pro součet dělitelů tvar čísla n. Máme

$$\sigma(n) = \sigma\big(2^k(2^{k+1} - 1)\big) = \sigma(2^k)\sigma(2^{k+1} - 1)\,,$$

kde jsme využili multiplikativnost funkce σ. Protože $2^{k+1} - 1$ je z předpokladu prvočíslo, můžeme dále psát

$$\sigma(n) = \frac{2^{k+1} - 1}{2 - 1}\big(2^{k+1} - 1 + 1\big) = 2^{k+1}(2^{k+1} - 1) = 2n\,.$$

□

Příklad 3.16. Podle předchozí věty tedy můžeme snadno hledat další dokonalá čísla. Budeme vyznačovat, které z čísel $2^{k+1} - 1$ je prvočíslem, tj. patří do $\mathbb{P}$, jak se občas značí množina všech prvočísel.

$k = 1$:	$2^{k+1} - 1 = 3 \in \mathbb{P}$	$n = 2^k(2^{k+1} - 1) = 6$	je dokonalé,
$k = 2$:	$2^{k+1} - 1 = 7 \in \mathbb{P}$	$n = 2^k(2^{k+1} - 1) = 28$	je dokonalé,
$k = 3$:	$2^{k+1} - 1 = 15$	$n = 2^k(2^{k+1} - 1) = 120$	není dokonalé,
$k = 4$:	$2^{k+1} - 1 = 31 \in \mathbb{P}$	$n = 2^k(2^{k+1} - 1) = 496$	je dokonalé,
$k = 5$:	$2^{k+1} - 1 = 63$	$n = 2^k(2^{k+1} - 1) = 2016$	není dokonalé,
$k = 6$:	$2^{k+1} - 1 = 127 \in \mathbb{P}$	$n = 2^k(2^{k+1} - 1) = 8128$	je dokonalé,
$k = 7$:	$2^{k+1} - 1 = 255$	$n = 2^k(2^{k+1} - 1) = 32640$	není dokonalé.

Poznamenejme, že pro čísla 120, 2016, 32640 platí $\sigma(n) > 2n$, jak si čtenář může sám ověřit.

Věta 3.17 (Euler)**.** *Každé sudé dokonalé číslo n je tvaru $n = 2^k(2^{k+1} - 1)$ pro nějaké $k \in \mathbb{N}$, kde navíc $2^{k+1} - 1$ je prvočíslo.*

Důkaz. Protože n je sudé, je $n = 2^k m$ pro nějaké $k \in \mathbb{N}$ a m liché. Protože σ je multiplikativní, můžeme psát

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

Z předpokladu je n dokonalé číslo, takže

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

Odtud získáme

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

Protože zlomek na levé straně je ve zkráceném tvaru, existuje $r \in \mathbb{N}$ tak, že platí

$$m = r(2^{k+1} - 1)\,, \qquad \sigma(m) = r2^{k+1}\,.$$

Pak ale můžeme psát

$$\sigma(m) = \sigma\big(r(2^{k+1} - 1)\big) \geq r + r(2^{k+1} - 1) = r2^{k+1} = \sigma(m)\,.$$

Vidíme tedy, že v předchozím vztahu nemůže platit ostrá nerovnost, tj.

$$\sigma\big(r(2^{k+1} - 1)\big) = r + r(2^{k+1} - 1)\,.$$

Číslo $m = r(2^{k+1}-1)$ má tedy právě dva dělitele. To lze jedině tak, že $r = 1$ a $m = 2^{k+1}-1$ je prvočíslo, což jsme chtěli dokázat. □

Sudá dokonalá čísla jsou podle vět 3.15 a 3.17 ve vzájemně jednoznačném vztahu s prvočísly tvaru $2^n - 1$.

Definice 3.18. Číslo $M_n = 2^n - 1$ pro $n \in \mathbb{N}$ se nazývá n-té Mersennovo číslo. Je-li M_n prvočíslo, nazývá se Mersennovo prvočíslo.

Jak jsme si mohli všimnout v příkladu 3.16, $2^m - 1$ je rovno prvočíslu pro $m = 2, 3, 5, 7$ a složenému číslu pro $n = 4, 6, 8$. To není náhoda. Snadno totiž ověříme, že M_n má šanci být prvočíslem, pouze pokud n samo je prvočíslo. Je-li totiž n složené, tedy $n = ab$ pro $a, b > 1$, pak

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

Protože $a, b \geq 2$, je $2^a - 1 \geq 3$ a $1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a} \geq 5$, a číslo $2^n - 1$ je tedy rovněž složené.

Vzhledem k tomu, že pro první čtyři prvočísla $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, odpovídající Mersennova čísla jsou prvočísly, mohlo by se zdát, že M_p je prvočíslo pro každé $p \in \mathbb{P}$. To ale zdaleka není pravda a poznáme to už u prvočísla $p_5 = 11$. Máme

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89\,.$$

Dnes je známo na 48 prvočísel tvaru M_n. Prvních osm Mersennových čísel jsou

$$\begin{gathered} M_2 = 3, \quad M_3 = 7, \quad M_5 = 31, \quad M_7 = 127, \quad M_{13} = 8191, \\ M_{17} = 131071, \quad M_{19} = 524287, \quad M_{31} = 2147483647, \end{gathered} \tag{3.29}$$

jejichž prvočíselnost tipoval už francouzský matematik Marin Mersenne na začátku 17. století. Dnes (listopad 2014) je známo na 48 Mersennových prvočísel. Největší známé prvočíslo vůbec je dnes číslo M_p, kde $p = 57885161$. Toto prvočíslo má 17425170 cifer! V posledních letech bylo největší známé prvočíslo vždy Mersennovo číslo, pravděpodobně i proto, že k jejich hledání je určen výpočetní projekt GIMPS (Great Internet Mersenne Prime Search), do kterého se může se svým počítačem zapojit každý uživatel internetu.

Čtenář si jistě všiml, že dosud nebyla zmínka o lichých dokonalých číslech. To proto, že jejich existence není dodnes vyjasněná. Žádné liché dokonalé číslo zatím nikdo nenašel, ale všechny pokusy dokázat, že lichá dokonalá čísla neexistují, zatím selhaly. Nicméně bylo dosaženo jistých částečných výsledků. Je například známo, že je-li N liché dokonalé číslo, pak $N > 10^{300}$, v jeho rozkladu se nachází nejméně 9 různých prvočísel a to největší z nich je větší než 10^8.

Pro ilustraci dokažme, že liché číslo n, které má v rozkladu pouze dvě různá prvočísla, nemůže být dokonalé.

Věta 3.19. *Je-li $n = p_1^{k_1} p_2^{k_2}$, kde p_1, p_2 jsou různá lichá prvočísla a $k_1, k_2 \in \mathbb{N}$, pak $\sigma(n) < 2n$.*

Důkaz. Pro součet dělitelů čísla n platí

$$\sigma(p_1^{k_1} p_2^{k_2}) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} < \frac{p_1^{k_1+1}}{p_1 - 1} \frac{p_2^{k_2+1}}{p_2 - 1} = n \frac{p_1}{p_1 - 1} \frac{p_2}{p_2 - 1}\,.$$

Protože funkce $f(y) = \frac{y}{y-1}$ je klesající na $(1, +\infty)$, zlomky $\frac{p_i}{p_i - 1}$ lze odhadnout hodnotou $\frac{q}{q-1}$ pro co nejmenší liché prvočíslo q. Protože jsou ale p_1, p_2 různá prvočísla, např. $p_1 < p_2$, víme, že $p_1 \geq 3$ a $p_2 \geq 5$. Odtud máme

$$\sigma(n) < n \frac{p_1}{p_1 - 1} \frac{p_2}{p_2 - 1} \leq n \cdot \frac{3}{2} \cdot \frac{5}{4} = n \frac{15}{8} < 2n\,.$$

□

Pro dokonalé číslo n je podíl $\frac{\sigma(n)}{n}$ roven 2. Čtenář si sám může rozmyslet, jakých hodnot tento podíl může nabývat pro obecné přirozené číslo n.

3.4 Fermatova čísla

U Mersennových čísel M_n jsme studovali, kdy je číslo $2^n - 1$ prvočíslem. Zjistili jsme, že nutně n musí samo být prvočíslo. Pro zajímavost se nyní podívejme, kdy je číslo tvaru $2^n + 1$ prvočíslem.

Věta 3.20. *Je-li $n = ab$, kde $b > 1$ je liché a $a \geq 1$, pak $2^n + 1$ je složené číslo.*

Důkaz. Máme

$$(2^{ab} + 1) = (2^a)^b + 1 = (2^a + 1)(1 - 2^a + 2^{2a} - 2^{3a} + \cdots + 2^{(b-1)a}) .$$

Protože $a \geq 1$, je $2^a + 1 \geq 3$ a navíc $1 - 2^a + 2^{2a} - 2^{3a} + \cdots + 2^{(b-1)a} > 1$, a číslo $2^n + 1$ je tedy složené. □

Předcházející tvrzení můžeme přeformulovat takto: Pokud $2^n + 1$ je prvočíslo, pak nutně $n = 2^m$ pro nějaké $m \geq 0$. Uvažujeme tedy pouze čísla tvaru $f_m = 2^{2^m} + 1$.

Definice 3.21. Číslo $f_m = 2^{2^m} + 1$ pro $m \in \mathbb{N}_0$ se nazývá m-té Fermatovo číslo. Je-li f_m prvočíslo, nazývá se Fermatovo prvočíslo.

Příklad 3.22. Máme

$$f_0 = 2^{2^0} + 1 = 3 , \quad f_1 = 2^{2^1} + 1 = 5 , \quad f_2 = 2^{2^2} + 1 = 17 ,$$
$$f_3 = 2^{2^3} + 1 = 2^8 + 1 = 257 , \quad f_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537 .$$

Všechna Fermatova čísla z příkladu 3.22 jsou prvočísla. To by mohlo navodit dojem, že všechna Fermatova čísla jsou prvočísla. Ve skutečnosti jsou ale zmíněná f_m, $m = 0, 1, 2, 3, 4$, jediná známá Fermatova prvočísla.

Příklad 3.23. Dokážeme, že $f_5 = 2^{32} + 1$ není prvočíslo, a to tak, že ověříme jeho dělitelnost číslem 641. Využijeme toho, že $641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4$. Máme proto

$$2^4 \equiv -5^4 \bmod 641 ,$$

ale také

$$5 \cdot 2^7 \equiv -1 \bmod 641 , \qquad \text{a tedy} \qquad 5^4 \cdot 2^{28} \equiv 1 \bmod 641 .$$

Vynásobením obou výsledných kongruencí máme

$$5^4 \cdot 2^{32} \equiv -5^4 \bmod 641\,,$$

$$2^{32} \equiv -1 \bmod 641\,,$$

kde jsme využili, že 5^4 je nesoudělné s modulem 641, a tedy jím můžeme krátit.

Vzhledem k tomu, jak rychle f_m roste s indexem m, je ověřování prvočíselnosti přímo, rozkladem, nemožné. Platí ale následující věta, která hledání dělitelů Fermatových čísel výrazně ulehčuje.

Věta 3.24 (Lucas)**.** *Každý dělitel Fermatova čísla f_n, $n \geq 3$, je tvaru $k2^{n+2}+1$ pro nějaké $k \in \mathbb{N}$.*

(Euler ukazal $k2^{n+1}+1$, Edouard Lucas zesilil tvrzeni. Dukaz je na `http://en.wikipedia.org/wiki/Fermat_number`)

Příklad 3.25. Podle předchozí věty je každý dělitel Fermatova čísla f_5 tvaru $k \cdot 2^7 + 1$. Chceme-li tedy ověřovat prvočíselnost f_5, testujeme dělitelnost čísly $k \cdot 2^7 + 1$, navíc ale pouze pro ta $k \in \mathbb{N}$, kdy je $k \cdot 2^7 + 1$ prvočíslem. Je-li totiž f_5 dělitelné složeným číslem d, pak je dělitelné i nějakým číslem $d' < d$, a to musí být opět tvaru $k \cdot 2^7 + 1$. Protože pro $k = 1, 3, 4$ máme

$$1 \cdot 2^7 + 1 = 129, \quad 3 \cdot 2^7 + 1 = 385, \quad 4 \cdot 2^7 + 1 = 513 \notin \mathbb{P}\,,$$

jediný kandidát na prvočíselného dělitele čísla f_5 menší než $641 = 5 \cdot 2^7 + 1$ je $2 \cdot 2^7 + 1 = 2^8 + 1 = 257$. Ten ale vyloučíme snadno, protože

$$2^{32}+1 = 2^{32}-1+2 = (2^{16}-1)(2^{16}+1)+2 = (2^8-1)(2^8+1)(2^{16}+1)+2 \equiv 2 \bmod (2^8+1)\,.$$

Kdybychom neměli větu 3.24, museli bychom prověřovat dělitelnost f_5 všemi prvočísly $\leq \sqrt{f_5}$, kterých je 6542 !

Dodnes není známo, je-li Fermatových prvočísel nekonečně mnoho. Neví se ale dokonce ani to, zda je nekonečně mnoho Fermatových čísel, která jsou složená. Nejmenší index m takový, že o prvočíselnosti Fermatova čísla f_m nebylo rozhodnuto, je $m = 33$. Naopak největší m takové, že známe nějaký netriviální dělitel f_m, je $m = 3329780$ (ještě v listopadu 2014). Víme totiž, že

$$f_{3329780} = 2^{2^{3329780}} + 1 \qquad \text{je dělitelné číslem} \qquad 193 \cdot 2^{3329782} + 1\,.$$

Zajímavé je, že například o f_{20} se ví, že je složené, ale není znám žádný jeho dělitel.

Velikost čísla, jako je $f_{3329780}$, sahá mimo všechny lidské představy. Pro ilustraci uveďme, že už f_{33} má cca miliardu cifer, tj. pokud by 1 cifra zabrala 1mm, zápis f_{33} by se táhl vzdušnou čarou z Prahy do Paříže. Už ale takové f_{73} by 60 miliard krát obeplo zemský rovník.

Na závěr poznamenejme, že hledání dělitelů Fermatových čísel se věnuje internetový projekt „Fermat Search“, do kterého se také můžete zapojit.

Fermatova čísla jsou zajímavou hříčkou pro rekreační matematiku, ale stejně jako Mersennova čísla se objevují v různých oblastech matematiky a mají svůj odborný význam. Gauss například ukázal, že pravidelný n úhelník je konstruovatelný pomocí pravítka (bez měřítka) a kružítka, právě když n je součinem mocniny dvojky a navzájem různých Fermatových prvočísel. My si zde pro ilustraci jejich použití předvedeme zajímavý důkaz nekonečnosti množiny prvočísel.

Lemma 3.26. *Pro $n \geq 1$ platí*

$$\prod_{k=0}^{n-1} f_k = f_n - 2\,. \tag{3.30}$$

Důkaz. Pro $n = 1$ je tvrzení pravdivé, protože $f_0 = 3 = 5 - 2 = f_1 - 2$. Pro $n > 1$ využijeme indukční předpoklad a můžeme psát

$$\prod_{k=0}^{n} f_k = \Big(\prod_{k=0}^{n-1} f_k\Big) f_n = (f_n - 2) f_n = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = \left(2^{2^{n+1}} - 1\right) = f_{n+1} - 2\,.$$

□

Předchozí lemma implikuje zajímavý výsledek, totiž že každá dvě Fermatova čísla jsou navzájem nesoudělná.

Důsledek 3.27. *Nechť $k, n \in \mathbb{N}$, $k \neq n$. Potom* $\operatorname{nsd}(f_k, f_n) = 1$.

Důkaz. Je-li $k < n$, pak ze vztahu (3.30) můžeme odvodit, že f_k dělí $f_n - 2$. Každý společný dělitel f_n a f_k by musel dělit f_n a $f_n - 2$, a tudíž být dělitelem dvojky. Samo číslo 2 ale nemůže být tímto společným dělitelem, protože Fermatova čísla jsou všechna lichá. Proto $\operatorname{nsd}(f_k, f_n) = 1$. □

Z důsledku 3.27 lze odvodit jiný důkaz nekonečnosti množiny prvočísel, který je přičítán Christianu Golbachovi. Protože jsou Fermatova čísla nesoudělná, mají v rozkladu různá prvočísla. Protože Fermatových čísel je nekonečně, je nekonečně i prvočísel.

Množinu prvočísel lze uspořádat podle velikosti do ostře rostoucí posloupnosti $(p_n)_{n\in\mathbb{N}}$, tedy

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ \ldots$$

Z Goldbachova důkazu plyne, že n-té prvočíslo p_n je menší než f_{n-1}. Máme tedy první odhad na velikost prvočísla

$$p_n \ \leq\ 2^{2^{n-1}} + 1\,.$$

4 Aplikace elementární teorie čísel

Z doposud probrané látky by se mohlo zdát, že elementární teorie čísel je plná matematických hříček, které po staletí neslouží k ničemu jinému než zábavě. I když tento účel zdaleka nepovažujeme za zbytečný, pokusíme se přesvědčit čtenáře, že ve skutečnosti je na zmíněných principech postavena řada aplikací, které denně používá snad každý z nás. Elementární teorie čísel je totiž základním materiálem pro konstrukci šifrovacích systémů, které používáme v emailové komunikaci nebo třeba při ověřování hesla na platební kartě v bankomatu.

4.1 Testování prvočíselnosti

Je 123456 prvočíslo? Ne! Je sudé.

Je 1234567 prvočíslo? Ne. Ovšem nejmenší netriviální dělitel je až 127.

Je 1234577 prvočíslo? Tentokrát ano, ale abychom to ověřili, museli bychom např. zkoušet dělitelnost všemi prvočísly $\leq \lfloor\sqrt{1234567}\rfloor = 1111$. Těch je 186.

Je $n = 1\,111\,222\,233\,334\,444\,555\,566\,667\,777\,888\,899\,967$ prvočíslo? Tady bychom s běžným testováním neuspěli. Prvočísel $\leq \sqrt{n}$ je totiž více než $2,4 \cdot 10^{16}$. Kdyby nám každé dělení trvalo 1 milisekundu, pak by celé prověřování zabralo téměř půl milionu let. Výsledkem by bylo, že dané číslo opravdu je prvočíslem. Otázkou tedy je, jak rozhodování o prvočíselnosti daného n urychlit.

Nejjednodušší je tzv. Fermatův test, založený na malé Fermatově větě 2.13. Ta říká, že je-li n prvočíslo a a nesoudělné s n, pak $a^{n-1} \equiv 1 \bmod n$, jinými slovy $a^{n-1} - 1$ je dělitelné n. Přeformulujeme-li tvrzení pomocí obrácené implikace, vidíme, že najdeme-li $a \in \{1, 2, \ldots, n-1\}$ takové, že n nedělí $a^{n-1} - 1$, pak je nutně n složené. A opravdu: pro namátkou vybraná složená lichá čísla n stačí dokonce zvolit $a = 2$ a Fermatův test prokáže složenost n. Máme např.

$$n = 9 \text{ nedělí } 2^8 - 1 = 255 \quad \text{nebo} \quad n = 21 \text{ nedělí } 2^{20} - 1 = 1048575\,.$$

Ověřování ve skutečnosti využívá modulární aritmetiku: Pro $n = 77$ fakticky nepočítáme $2^{76} - 1 = 75557863725914323419135$ a nezkoušíme jeho dělitelnost 77, ale všimneme si, že

$$76 = 2 \cdot 38 = 2 \cdot 2 \cdot 19 = 2 \cdot 2 \cdot (1 + 2 \cdot 9) = 2 \cdot 2 \cdot (1 + 2 \cdot (1 + 2 \cdot 2 \cdot 2)) \tag{4.1}$$

takže $2^{76} \bmod 77$ získáme postupem

$$\begin{aligned} 2^8 &\equiv 256 \equiv 25 \bmod 77 \\ 2^9 &\equiv 2 \cdot 25 \equiv 50 \bmod 77 \\ 2^{18} &\equiv 50^2 \equiv 36 \bmod 77 \\ 2^{19} &\equiv 2 \cdot 36 \equiv 72 \bmod 77 \\ 2^{38} &\equiv 72^2 \equiv 25 \bmod 77 \\ 2^{76} &\equiv 25^2 \equiv 9 \bmod 77 \end{aligned}$$

kde následující řádek je vždy druhá mocnina nebo dvojnásobek předchozího v souladu s (4.1). V každém kroku rovnou provedeme zbytek po dělení 77, takže tímto postupem nemusíme nikdy pracovat s čísly většími než 76^2.

V uvedených příkladech Fermatův test vždy potvrdil složenost čísla n už pro $a = 2$. Co ale můžeme říct o n, pokud nastane $2^{n-1} \equiv 1 \bmod n$? Implikace v malé Fermatově větě nelze obrátit, takže takové n může být prvočíslo, ale také nemusí.

Příklad 4.1. Mějme $n = 341 = 11 \cdot 31$. Ověříme, že platí $341|2^{340} - 1$. K tomu stačí zjistit, že 11 i 31 dělí číslo $2^{340} - 1$. To ale platí protože

$$2^{340} - 1 = (2^5)^{68} - 1 = \underbrace{(2^5 - 1)}_{31} \sum_{j=0}^{67} 2^{5j} \,,$$

ale rovněž

$$2^{340} - 1 = (2^{10})^{34} - 1 = (2^{10} - 1) \sum_{j=0}^{33} 2^{10j} \,.$$

Přitom podle malé Fermatovy věty víme, že $11|2^{10} - 1$. Takže také $11|2^{340} - 1$ a dohromady $341 = 31 \cdot 11|2^{340} - 1$. Číslo $n = 341$ se tedy v rámci Fermatova testu vzhledem k $a = 2$ tváří jako prvočíslo.

Je-li n složené číslo a $a \in \mathbb{N}$, pak mohou nastat dvě situace:

- $a^{n-1} \not\equiv 1 \bmod n$ a číslo a se nazývá Fermatův svědek složenosti čísla n.
- $a^{n-1} \equiv 1 \bmod n$ a číslo n se nazývá pseudoprvočíslo vzhledem k bázi a.

Poznamenejme, že číslo $n = 341$ je nejmenší pseudoprvočíslo vzhledem k bázi 2. Už $a = 3$ je ale svědek složenosti čísla 341, protože $3^{340} \equiv 56 \bmod 341$.

Mezi $a \in \{1, 2, \ldots, n-1\}$ svědkem složenosti jistě nemůže být $a = 1$, ale ani $a = n-1$. Máme totiž

$$(n-1)^{n-1} = \sum_{j=0}^{n-1} (-1)^{n-1-j} n^j \equiv (-1)^{n-1} \bmod n\,,$$

takže platí $n|(n-1)^{n-1} - 1$. (Uvažujeme pouze liché n, protože pro sudá čísla test prvočíselnosti nemá smysl provádět.)

Fermatův test nám může možná rychle označit složené číslo za složené, existence pseudoprvočísel nicméně vypovídá o tom, že v opačném směru je to poněkud složitější. Abychom měli kritérium prvočíselnosti (tedy pravidlo „Pokud něco, pak n je prvočíslo a pokud ne, pak n je složené.“) musíme vzít v úvahu následující větu.

Věta 4.2. *Přirozené číslo n je prvočíslo, právě když $a^{n-1} \equiv 1 \bmod n$ pro každé $a \in \{1, 2, \ldots, n-1\}$.*

Důkaz. Pro implikaci zleva doprava stačí použít malou Fermatovu větu 2.13. Čísla $a \in \{1, 2, \ldots, n-1\}$ jsou totiž všechna nesoudělná s prvočíslem n.

Místo opačné implikace dokážeme její obměnu: Je-li n složené, pak existuje $a \in \{1, 2, \ldots, n-1\}$ takové, že $a^{n-1} \not\equiv 1 \bmod n$. Jestliže je totiž n složené, pak existuje $a \in \{2, \ldots, n-1\}$ soudělné s n, a tedy existuje společný dělitel $d \in \{2, 3, \ldots, n-1\}$ čísel n a a. Předpoklad $n|a^{n-1} - 1$ vede ke sporu, protože $d \not| a^{n-1} - 1$. □

Poznámka 4.3. Ve skutečnosti jsme dokázali silnější tvrzení: Pro každé $a \in \{2, \ldots, n-2\}$ soudělné s n platí $a^{n-1} \not\equiv 1 \bmod n$.

Fermatův test nám tedy označí složené číslo za složené, kdykoliv za a zvolíme číslo soudělné s n. Jaká je ale pravděpodobnost, že při náhodném výběru $a \in \{2, \ldots, n-2\}$ narazíme na číslo soudělné s n? To samozřejmě závisí na n. Protože ale charakter n dopředu neznáme, je nutno počítat s nejhorším případem.

Příklad 4.4. Je-li n součinem dvou velkých prvočísel, $n = pq$, pak počet čísel menších nebo rovných n soudělných s n je $n - \varphi(n) = p + q - 1$. Pravděpodobnost volby soudělného a je tedy

$$\frac{n - \varphi(n)}{n} = \frac{p + q - 1}{pq}\,.$$

Pokud p, q jsou například 100místná prvočísla, pak $p+q-1 < 2\cdot 10^{100}$ a přitom $pq > 10^{198}$, takže

$$\frac{p+q-1}{pq} < \frac{2}{10^{98}}\,.$$

Chtěli-li bychom tedy použít Fermatův test, musíme doufat, že pro složená čísla n narazíme na svědka složenosti častěji než jen při volbě a soudělného s n. Například pro $n = 77$ jsou svědky jeho složenosti všechna $a \in \{2, \ldots, 75\}$ kromě $a = 34$ a $a = 43$. Z možných 74 je tedy 72 svědků složenosti, přitom čísel soudělných s $n = 77$ je mezi nimi pouze 16. I tato vlastnost ale není obecná a naše doufání v použitelnost Fermatova testu je marné. Existují totiž tzv. Carmichaelova čísla.

Definice 4.5. Složené číslo $n \in \mathbb{N}$ se nazývá Carmichaelovo, pokud $a^{n-1} \equiv 1 \bmod n$ pro všechna a nesoudělná s n.

Carmichaelova čísla n jsou tedy pseudoprvočísla vzhledem ke všem bázím $a \perp n$ a Fermatův test u nich selhává.

Příklad 4.6. Nejmenším Carmichaelovým číslem je $n = 561 = 3 \cdot 11 \cdot 17$. Platí pro něj $561 | a^{560} - 1$ pro každé a, které není dělitelné 3, 11 ani 17.

Dá se ovšem ukázat, že v případě, kdy n je složené číslo a není Carmichaelovo, je Fermatových svědků jeho složenosti dostatek (alespoň polovina).

Věta 4.7. *Jestliže složené číslo $n \in \mathbb{N}$ není Carmichaelovo číslo, pak množina*

$$S := \{a \in \mathbb{N} \mid 1 \le a \le n-1,\ a^{n-1} \not\equiv 1 \bmod n\}$$

svědků složenosti čísla n má více než $\frac{n-1}{2}$ prvků.

Důkaz. Uvažujme množinu všech čísel nesoudělných s n menších nebo rovných n. Rozdělíme ji na Fermatovy svědky složenosti, a ty druhé, tj. na sjednocení $U \cup V$, kde

$$U = \{a \in \mathbb{N} : 1 \le a \le n-1,\ a \perp n,\ a^{n-1} \equiv 1 \bmod n\}\,,$$
$$V = \{a \in \mathbb{N} : 1 \le a \le n-1,\ a \perp n,\ a^{n-1} \not\equiv 1 \bmod n\}\,.$$

Dokažme, že množina V obsahuje alespoň tolik prvků jako množina U. Označme $U = \{a_1, \ldots, a_k\}$. Vybereme libovolný prvek $b \in V$ a pro $i \in \{1, \ldots, k\}$ spočítáme zbytek r_i po dělení součinu ba_i číslem n. Protože $b \perp n$, platí implikace $ba_i \equiv ba_j \mod n \ \Rightarrow\ a_i \equiv a_j \mod n$, a tedy zbytky $r_1, \ldots, r_k$ jsou po dvou různé. Proto $k = |U|$. Navíc platí

$$r_i^{n-1} \equiv b^{n-1} a_i^{n-1} \equiv b^{n-1} \not\equiv 1 \mod n\,,$$

takže $r_i \in V$ pro všechna i. Proto $|V| \geq k = |U|$. Přitom $\varphi(n) = |U| + |V|$, takže $|V| \geq \varphi(n)/2$. Protože podle poznámky 4.3 jsou v množině S kromě prvků z V i čísla soudělná s n, můžeme celkově psát

$$|S| = n-1-\varphi(n)+|V| \geq n-1-\varphi(n)+\frac{\varphi(n)}{2} = n-1-\frac{\varphi(n)}{2} \geq n-1-\frac{n-1}{2} = \frac{n-1}{2}\,,$$

kde jsme použili, že $\varphi(n) \leq n-1$. □

O Carmichaelových číslech je známo mnoho zajímavých věcí, například to, že nejsou dělitelná druhou mocninou žádného prvočísla, nebo to, že pokud prvočíslo p dělí Carmichaelovo číslo n, pak $p-1$ dělí $n-1$. Nicméně neexistuje žádný snadný (tj. rychlý) způsob, jak rozhodnout, zda dané číslo je nebo není Carmichaelovo, a to je hlavní překážka pro to, aby byl výše uvedený Fermatův test prvočíselnosti použitelný v praxi. I když šance, že náhodně vybrané přirozené číslo je zrovna Carmichaelovo, je malá, přesto není zanedbatelná pro účely tak důležité, jako je kryptografie.

Proto si zde uvedeme jiný test prvočíselnosti, který tuto slabinu Fermatova testu odstraňuje, a to tzv. Millerův-Rabinův test. Je to sice test pravděpodobnostní, což znamená, že prvočíselnost zvoleného p nikdy nevíme se 100% jistotou, ale protože pravděpodobnost mylného výsledku exponencielně klesá s počtem průchodů testu, můžeme se na jeho výsledek spolehnout více, než na nezávadnost hardwaru, který k testování používáme.

Myšlenka Millerova-Rabinova testu pouze rozvíjí test Fermatův; my ji nejprve ilustrujeme na příkladě:

Příklad 4.8. Vezměme $n = 561$. Ilustrujeme, jak Millerův-Rabinův test odhalí složenost tohoto Carmichaelova čísla.

Zvolíme náhodné $a < 561$. Kdybychom měli štěstí a zvolili číslo soudělné s 561, pak $561 \not| a^{560}-1$. Pokud tomu tak ale není, pak $561|a^{560}-1$. Číslo $a^{560}-1$ můžeme rozložit podle vzorečku $A^2-B^2 = (A+B)(A-B)$ na součin

$$\begin{aligned} a^{560}-1 &= (a^{280}+1)(a^{280}-1) = \\ &= (a^{280}+1)(a^{140}+1)(a^{140}-1) = \\ &= (a^{280}+1)(a^{140}+1)(a^{70}+1)(a^{70}-1) = \\ &= (a^{280}+1)(a^{140}+1)(a^{70}+1)(a^{35}+1)(a^{35}-1)\,. \end{aligned}$$

Bylo-li by číslo 561 prvočíslem, muselo by – podle věty 1.12 – dělit alespoň jednu ze závorek v součinu. Jakmile najdeme a, pro které 561 nedělí žádnou ze závorek, rozhodneme o tom, že číslo 561 musí být složené. To je pravda například už pro $a = 2$. Snadno totiž ověříme,

že čísla $2^{280}+1$, $2^{140}+1$, $2^{70}+1$, $2^{35}-1$ nejsou dělitelná 3, a číslo $2^{35}+1$ zase není dělitelné 17.

Algoritmus Millerova-Rabinova testu ilustrovaného na předchozím případě lze zapsat takto:

Vstup: liché přirozené číslo $n > 3$, parametr spolehlivosti testu k.

Postupným dělením čísla $n-1$ dvěma najdi $m \in \mathbb{N}$ liché a $t \in \mathbb{N}$ tak, že $n-1 = 2^t m$.

Opakuj k krát smyčku S:

Vyber náhodné $a \in \{2, 3, \ldots, n-2\}$; $x := a^m \bmod n$.

Když $x = 1$ nebo $x = n-1$, začni novou iteraci smyčky S,

jinak polož $i = 1$ a dokud $i < t$ prováděj

$x := x^2 \bmod n$; $i := i+1$;

když $x = 1$, vrať „n je složené“ a konec;

když $x = n-1$, začni novou iteraci smyčky S.

Vrať „n je složené“ a konec.

Vrať „n je pravděpodobně prvočíslo“.

Výstup: „n je složené“, je-li n složené, jinak „n je pravděpodobně prvočíslo“.

Všimněme si, že algoritmus je sestaven tak, aby byla minimalizovaná výpočetní náročnost. Proto se při ověřování dělitelnosti závorek v rozkladu

$$a^{n-1} - 1 = (a^{2^{t-1}m} + 1)(a^{2^{t-2}m} + 1) \cdots (a^m + 1)(a^m - 1)$$

postupuje od poslední závorky. Pokud $a^m \equiv 1 \bmod n$, znamená to, že $(a^m - 1)$ je dělitelné n. Pokud $a^m \equiv n-1 \bmod n$, je $(a^m + 1)$ dělitelné n. V obou případech začínáme novou smyčku s jinou volbou a, protože n se vzhledem k tomuto a tváří jako prvočíslo. Pokud zbytek $a^m \bmod n$ není ani 1 ani $n-1$, pokračujeme mocněním na druhou od a^m po $a^{2^t m}$ a zjišťujeme zbytek po dělení n. Jakmile narazíme na zbytek 1, nemá cenu v mocnění pokračovat, protože $a^{2^i m} \equiv 1 \bmod n$ implikuje $a^{2^j m} \equiv 1 \bmod n$ pro všechna $j \geq i$, a tudíž žádná ze závorek $(a^{2^j m} + 1)$ není dělitelná n. V tomto případě proto lze rozhodnout o složenosti n. Pokud narazíme na zbytek $n-1$, narazili jsme na závorku, která je dělitelná n, a proto se opět n vzhledem k tomuto a tváří jako prvočíslo. Konečně pokud zbytky všech čísel $a^m, \ldots, a^{2^t m}$ jsou různé od 1 i $n-1$, pak žádná ze závorek není dělitelná n a a svědčí pro složenost čísla n.

Lze ukázat, že pro každé složené číslo je při Millerově-Rabinově testu více než 3/4 svědků složenosti. Proto při jednom průchodu smyčkou je pravděpodobnost lživé odpovědi

„n je prvočíslo“ menší než $1/4$. Pokud se n tváří jako prvočíslo pro k různých náhodně zvolených čísel $a \in \{2, 3, \ldots, n-2\}$, pak je pravděpodobnost chybného označení n za prvočíslo menší než $1/4^k$.

4.2 Šifrování s veřejně přístupným klíčem

Snad od chvíle, kdy lidé zjistili, jak důležité je komunikovat s ostatními, si zároveň uvědomovali, že snad ještě důležitější může být informace před nepovolanýma ušima umět skrývat. Šifrovacích metod bylo v historii vymyšleno spoustu. Asi nejjednodušší je substituční kódování, při kterém se nahrazuje každé písmeno jiným, a klíčem je tabulka nahrazovacích pravidel. Už například při substituci

$$A \mapsto B,\ B \mapsto C,\ C \mapsto D,\ D \mapsto E,\ \text{atd.}$$

zašifrovaný text

NJMVKJ EJTLSFUOJ NBUFNBUJLV

vypadá na první pohled úplně nečitelně, ve skutečnosti je ale tento typ šifry i bez klíče velice snadno rozlomitelný, například s využitím znalosti frekvencí písmen a skupin písmen v přirozeném jazyce.

Mnohem bezpečnější je šifra pomocí tzv. jednorázové náhodné pásky. Ta má ovšem nevýhodu, že vyžaduje bezpečný způsob, jak předat druhé straně velmi dlouhý klíč, který nelze použít opakovaně.

My se ovšem zaměříme na šifrovací metody, které využívají vlastností přirozených čísel a prvočísel. Jako příklad použití uveďme následující situaci: Alena a Bohouš hrají po telefonu šachy. Večer by chtěli přerušit hru. Jak ale zařídit, aby jeden z nich neměl na rozmyšlení svého tahu celou noc? Na šachových turnajích se poslední tah zaznamená do obálky a uschová u rozhodčího. Alena s Bohoušem ale nemají nezávislou třetí osobu. Musí zajistit, aby Alena mohla svůj tah zapsat do zprávy, kterou Bohouš nebude moci sám bez nějakého ‚klíče’ rozluštit. Zároveň ale Alena nesmí mít možnost si svůj tah přerozmyslet.

Řešení jejich problému je takové: Alena s Bohoušem se dohodnou na nějakém způsobu, jak zakódovat šachový tah do čísel. Například chce-li Alena sdělit tah jezdce na c2, napíše 1032, protože „10“ znamená „J“ (desáté písmeno v anglické abecedě), „3“ znamená „c“ a „2“ znamená „2“. Takto zakódují každý tah do čtyřciferného čísla.

V dalším kroku Alena doplní čtyřčíslí 1032 na stomístné prvočíslo $p = 1032\cdots$. S pomocí počítače je to velmi snadné. Program Maple na osobním počítači našel nejmenší

takové prvočíslo okamžitě,

$$p = 10320000000000000000000000000000000000000000000000$$
$$0000000000000000000000000000000000000000000000157\,.$$

Samozřejmě je lepší aby mezi všemi stomístnými prvočísly vybrala nějaké náhodně. To lze provést tak, že Maple nechá testovat prvočíselnost n v náhodně zvoleném intervalu stomístných čísel s daným čtyřčíslím na začátku. Vyjde například

$$p = 10323957188605341931398164158001874844592242417 04$$
$$6542755205686938640830745069460718926577301298 4933\,.$$

Pak Alena obdobným způsobem najde ještě jedno stomístné prvočíslo q, řekněme větší než p. Tato dvě prvočísla mezi sebou vynásobí a Bohoušovi sdělí výsledek $n = pq$. Ráno Alena Bohoušovi prozradí q, ten snadno vydělí $p = n/q$ a přečte si z prvního čtyřčíslí Alenin zamýšlený tah.

Teď je jasné, že Alena si svůj tah do rána nemůže přerozmyslet. Kdyby chtěla zaměnit původní tah za jiný, musela by dodat jiné stomístné prvočíslo $\tilde{p}$. Bohouš by snadno ověřil, že ho chce Alena ošálit. Jednoduše by vyzkoušel, zda je n dělitelné $\tilde{p}$. To by mu na papíře nějakou dobu trvalo, ale Maple to zvládne ještě rychleji, než cobydup.

Kdyby ale chtěl podvádět Bohouš, musel by bez klíče q sám zjistit, jaký je rozklad čísla n na prvočinitele. A v tom je zakopaný pes: Ačkoliv samotné dělení je rychlé, i v nejrychlejším známém algoritmu pro hlednání rozkladu na prvočinitele je počet kroků exponenciálně závislý na počtu cifer rozkládaného čísla. Rozložit n na součin pq by tak Bohoušovi mohlo trvat i s použitím nejrychlejšího počítače několik miliard let.

Oba hráči tak mohou být ujištěni, že hra je spravedlivá.

4.3 RSA

Šifrovací algoritmus RSA dostal název podle tří matematiků, kteří ho v roce 1977 navrhli. Byli to Ronald Linn Rivest, Adi Shamir a Leonard Max Adleman. Zkratka RSA odpovídá počátečním písmenům jejich příjmení v pořadí, v jakém byli uvedeni na článku, který algoritmus popisoval. Nejprve vysvětlíme postup, poté ověříme, že pracuje tak, jak má.

Alena zvolí dvě velká prvočísla p, q. Jejich součinem získá $n = pq$. Pak zvolí náhodné i nesoudělné s $\varphi(n) = (p-1)(q-1)$, $1 < i < \varphi(n)$. Při zvolení náhodného čísla i z $\{2, 3, \ldots, \varphi(n)-1\}$ je třeba ověřit nesoudělnost i a $\varphi(n)$. To se provádí Eukleidovým algoritmem hledání $\mathrm{nsd}\big(i, \varphi(n)\big)$. Z něj zároveň vyjdou koeficienty j a k takové, že $ij - k\varphi(n) = \mathrm{nsd}\big(i, \varphi(n)\big) = 1$. Takové j lze navíc zvolit opět v $\{2, 3, \ldots, \varphi(n)-1\}$, viz věta 1.7.

Alena tedy nyní má $n = pq$ a $ij \equiv 1 \bmod \varphi(n)$. Čísla n, i tvoří veřejný klíč. Naopak čísla $p, q, \varphi(n), j$ si nechává pro sebe.

Bohouš nyní může s pomocí veřejného klíče posílat Aleně zašifrované zprávy tak, aby je nikdo, kromě Aleny, nemohl rozluštit. Nejprve převede svou zprávu na číslo v množině $\{1, \ldots, n-1\}$. To by šlo například tak, že text, digitalizovaný na posloupnost nul a jedniček, rozseká na bloky takové délky m, aby $2^m < n$. Každý z bloků pak odpovídá číslu $x < n$. Aby text vždy šel rozdělit na tyto bloky, je třeba ho doplnit na délku dělitelnou m například posloupností cifer $10\cdots0$, případně 1. Pokud text sám má délku dělitelnou m, přidá se jeden celý blok $10\cdots0$ tak, aby při dekódování nebyl deformován význam. Bude totiž jasné, že ze zaslané zprávy je nutné vždy odebrat poslední jednčku a všechny nuly za ní.

Zašifrování probíhá takto: Bohouš umocní zprávu x na exponent i z veřejného klíče a spočítá zbytek po dělení číslem n. Získané číslo $y \equiv x^i \bmod n$ pak pošle Aleně.

Alena přečte y a zprávu rozšifruje pomocí privátního klíče j, který si schovala. Provede $y^j \bmod n$. Výsledkem je původní zpráva, tedy číslo x.

Než dokážeme, že uvedený postup opravdu funguje, předveďme ho na příkladě.

Příklad 4.9. Zvolme 'velká' prvočísla $p = 47$, $q = 67$. Potom $n = 47 \cdot 67 = 3149$ a $\varphi(n) = 46 \cdot 66 = 3036$. Jako šifrovací exponent do veřejného klíče zvolme například $i = 13$. K ověření nesoudělnosti i s číslem $\varphi(n)$ použijeme Eukleidův algoritmus:

$$3036 = 233 \cdot 13 + 7$$
$$13 = 1 \cdot 7 + 6$$
$$7 = 1 \cdot 6 + 1\,.$$

Proto $\mathrm{nsd}(3036, 13) = 1$ a zároveň lze odvodit, že

$$1 = 7 - 6 = 7 - (13 - 7) = 2(3036 - 233 \cdot 13) - 13 = 2 \cdot 3036 - 467 \cdot 13\,.$$

Máme tedy řešení $j = -467$, $k = -2$ rovnice $13j - 3036k = 1$, jenže bychom rádi řešení jiné, takové, kde $j \in \mathbb{N}$, $j < 3036$. To najdeme snadno:

$$1 = (2 - 13) \cdot 3036 + (-467 + 3036) \cdot 13 = -11 \cdot 3036 + 2569 \cdot 13\,.$$

Zvolíme-li nyní $j = 2569$, dostaneme $ij = 13 \cdot 2569 = 33397 \equiv 1 \bmod 3036$.

Vřejným klíčem je tedy $n = 3149$, $i = 13$. Číslo $j = 2569$ si naopak Alena pečlivě ukryje.

Bohouš chce šifrovat dejme tomu zprávu zdigitalizovanou na

$$01000001010|01000010011|11010010101\,.$$

kde už jsme pro přehlednost vyznačili rozdělení na bloky tak, aby každý blok odpovídal binárnímu zápisu čísla menšího než $n = 3149$. Proto bereme bloky délky 11 (největší číslo s jedenácti binárními ciframi je totiž $2^{11} - 1 = 2047 < n$.) Bloky v Bohoušově zprávě tedy odpovídají číslům $x = 522$, $x = 531$ a $x = 1684$.

Zašifrujeme $y = x^j \bmod n$, tj. konkrétně

$$\begin{aligned} 522^{13} = 522 \cdot \left((522 \cdot 522^2)^2\right)^2 &\equiv 1077 \mod 3149\,, \\ 531^{13} &\equiv 1901 \mod 3149\,, \\ 1685^{13} &\equiv 1761 \mod 3149\,. \end{aligned}$$

Zašifrovanou zprávu tedy vyšleme ve tvaru

$$10000110101|11101101101|11011100001\,.$$

Alena zprávu přijme a rozšifruje $y^j \bmod n$, tj.

$$\begin{aligned} 1077^{2569} &\equiv 522 \mod 3149\,, \\ 1901^{2569} &\equiv 531 \mod 3149\,, \\ 1761^{2569} &\equiv 1685 \mod 3149\,. \end{aligned}$$

Poněkud se divíme, že Aleně s Bohoušem stálo za to vynaložit tolik úsilí, aby si zašifrovali zprávu „AHOJ“, která vznikne z této posloupnsti nul a jedniček v ASCII kódu (po odebrání poslední 1, která dorovnávala čtyři osmibitové bloky na délku dělitelnou 11). Binárně totiž máme

$$\begin{aligned} (01000001)_2 &= 65 = \mathrm{A}\,, \\ (01001000)_2 &= 72 = \mathrm{H}\,, \\ (01001111)_2 &= 79 = \mathrm{O}\,, \\ (01001010)_2 &= 74 = \mathrm{J}\,. \end{aligned}$$

Poznamenejme, že ve skutečnosti je samožřejmě nutné zvolit mnohem větší prvočísla, než jsme předvedli v předchozím příkladě. Zde by totiž získání utajeného dešifrovacího klíče nebylo vůbec těžké. Stačilo by faktorizovat n na prvočinitele $n = pq$, odtud zjistit $\varphi(n) = (p-1)(q-1)$ a pak najít j podobně, jako jsme to udělali v příkladu my.

Pojďme nyní dokázat platnost šifrovacího algoritmu, totiž fakt, že zašifrované $y \equiv x^i \mod n$ lze rozluštit jako $x \equiv y^j \mod n$. Fakticky nám tedy jde o ověření kongruence $x^{ij} \equiv x \mod n$.

Věta 4.10. *Nechť p, q jsou prvočísla, $n = pq$, a nechť $i, j \in \mathbb{N}$ splňují $ij \equiv 1 \mod \varphi(n)$. Potom pro každé $x \in \mathbb{N}$, $x < n$, platí $x^{ij} \equiv x \mod n$.*

Důkaz. Uvažujme nejprve x nesoudělné s n. Z Eulerovy věty 3.3 pak plyne $x^{\varphi(n)} \equiv 1 \mod n$. Z předpokladu lze odvodit, že $ij = k\varphi(n) + 1$ pro nějaké $k \in \mathbb{N}$. Umocníme-li předchozí kongruenci na k, dostaneme $x^{\varphi(n)k} \equiv 1 \mod n$ a po vynásobení obou stran číslem x máme

$$x^{\varphi(n)k+1} = x^{ij} \equiv x \mod n\,,$$

což jsme měli dokázat.

V případě x soudělného s n nelze použít Eulerovu větu přímo. Takové x ovšem musí být tvaru $x = ap$ nebo $x = aq$ pro nějaké přirozené a. Uvažujme proto bez újmy na obecnosti, že $x = ap$. Protože $x < n$, je $a < q$, a tedy a je nesoudělné s q. Odtud je ovšem celé $x = ap$ nesoudělné s q. Použijeme Eulerovu větu pro čísla x a q, $x^{\varphi(q)} \equiv 1 \mod q$. Po umocnění máme $x^{k\varphi(p)\varphi(q)} \equiv 1 \mod q$. Tato kongruence je ekvivalentní existenci takového b, že $x^{k\varphi(pq)} = bq + 1$. Vynásobením obou stran této rovnosti číslem x dostaneme

$$x^{ij} = x^{k\varphi(pq)+1} = bqx + x\,.$$

Po dosazení $x = ap$ za první x na pravé straně odvozujeme, že $x^{ij} = ban + x \equiv x \mod n$. □

Literatura

[1] J. Herman, R. Kučera, J. Šimša, *Equations and Inequalities: Elementary Problems and Theorems in Algebra and Number Theory.* 1. vyd. New York : Springer-Verlag, 2000. 355 s. Canadian Mathematical Society Books in Math.

[2] P. Erdös, J. Surányi, *Topics in the Theory of Numbers*, Springer-Verlag, 2001.

[3] M. Klazar, *Kaleidoskop teorie čísel*, KAM-DIMATIA Series, UK, 2000.

[4] V. Kořínek, *Základy algebry*, NČSAV, Praha, 1956.

[5] M. Křížek, F. Luca, L. Somer, *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, CMS Books in Mathematics, vol. 9, Springer-Verlag, New York, 2001.

[6] L. Lovász, J. Pelikán, K. Vesztergombi, *Discrete mathematics: Elementary and Beyond*, *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.

[7] M. B. Nathanson, *Elementary methods in number theory*, volume 195 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[8] G. Tenenbaum, M. Mendès France, *The prime numbers and their distribution*, AMS Student Mathematical Library Series, Providence, RI, 2000.