INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

A-Math-Net Síť pro transfer znalostí v aplikované matematice

CZ.1.07/2.4.00/17.0100

ÚVOD DO TEORIE ČÍSEL

Prof. Mgr. Radomír Halaš, Dr.

Oponenti:
RNDr. Jaroslav Švrček, CSc.
Mgr. Jozef Pócs, PhD.

2. upravené vydání

ISBN ????

Předmluva

Tato skripta jsou určena zejména studentům navazujícího studia matematických oborů na PřF UP v Olomouci. Jedná se o druhé přepracované vydání původního textu „Teorie čísel“ z roku 1997. Předpokládá se znalost algebry v rozsahu základního kurzu, přičemž některé kapitoly je možno studovat bez jakékoliv předchozí přípravy, a lze tedy předpokládat, že skripta najdou uplatnění i při výuce ve výběrových seminářích na středních školách či při přípravě na řešení některých úloh MO.

Jelikož problematika teorie čísel je velice obsáhlá, bylo do něj možno zařadit pouze některé vybrané partie.

Kapitola 1. je věnována zavedení základních pojmů a faktů z teorie dělitelnosti v oborech integrity, které jsou v některých směrech rozšířením znalostí ze základního kurzu.

Ve druhé kapitole jsou studována prvočísla zejména z hlediska jejich hustoty v množině $\mathbb{N}$ a prvočísla ve speciálních tvarech – Fermatova a Mersenneova.

Nejobsáhlejší 3. kapitola se zabývá řešením nejrůznějších typů kongruenčních rovnic a jejich soustav pomocí aparátu řetězových zlomků.

V kapitole 4. jsou zavedeny primitivní kořeny prvků a je ukázána jejich užitečnost zejména při řešení exponenciálních kongruenčních rovnic.

Další kapitola se zabývá možnostmi aproximace reálných čísel čísly racionálními užitím aparátu nekonečných řetězových zlomků. Teorie je aplikována při řešení Pellových rovnic.

Teorie iracionálních a transcendentních čísel patří k nejzajímavějším oblastem matematiky a zabývá se jí kapitola 6.

S některými významnými problémy aditivní teorie čísel je čtenář seznámen v následující kapitole a text je uzavřen problematikou některých vlastností tzv. kvadratických těles.

Skripta jsou doplněna kapitolou 9, v níž jsou prezentovány některé zajímavé (a přitom snadno formulovatelné) problémy teorie čísel a nastíněny další perspektivy vývoje.

Celý text je doprovázen řadou řešených i neřešených úloh, které by měly čtenáři usnadnit pochopení příslušné problematiky.

Únor 2014

autor

Obsah

Kapitola 1

Základní pojmy z teorie dělitelnosti v oborech integrity

Uveďme nejprve na úvod seznam základních pojmů a tvrzení, které lze nalézt v každém základním kurzu algebry.

- okruh:
  - je algebraická struktura $\mathcal{R} = (R, +, \cdot, 0)$ se dvěma binárními operacemi $+$ a $\cdot$, kde $(R, +, 0)$ je komutativní grupa, $(R, \cdot)$ je pologrupa a operace $\cdot$ je distributivní vzhledem k operaci $+$
  - okruh nazveme komutativní, je-li operace $\cdot$ komutativní
  - pokud má okruh neutrální prvek 1 vzhledem k operaci $\cdot$, budeme jej nazývat okruh s jedničkou (nebo také unitární)
  - prvek $a \neq 0$ okruhu $\mathcal{R}$ nazveme netriviální dělitel nuly, existuje-li v R prvek $b \neq 0$ takový, že $a \cdot b = 0$ nebo $b \cdot a = 0$
- obor integrity:
  - je každý alespoň dvouprvkový komutativní unitární okruh, v němž neexistují netriviální dělitelé nuly
- těleso:
  - je takový okruh $\mathcal{R} = (R, +, \cdot, 0, 1)$, kde $(R \setminus \{0\}, \cdot, 1)$ je grupa
- ideál v okruhu:
  - neprázdná podmnožina $I \subseteq R$ je ideál v okruhu $\mathcal{R}$, platí-li:
    1) $\forall a, b \in I : a - b \in I$
    2) $\forall a \in I,\ \forall b \in R : a \cdot b \in I,\ b \cdot a \in I$

- ideál $I \neq R$ nazveme maximální, platí-li pro každý ideál J okruhu $\mathcal{R}$ implikace $I \subseteq J \subseteq R \Rightarrow I = J$ nebo $J = R$
- ideál I okruhu $\mathcal{R}$ nazveme prvoideál, platí-li $\forall a, b \in R$:

$$a \cdot b \in I \Rightarrow a \in I \text{ nebo } b \in I$$

- kongruence na okruhu:
  - ekvivalence θ na nosiči R okruhu $\mathcal{R}$ se nazývá kongruence na $\mathcal{R}$, platí-li tzv. substituční podmínka:

$$\forall a, b, c, d \in R\colon ((a, b) \in \theta) \wedge ((c, d) \in \theta) \Rightarrow ((a+c, b+d) \in \theta,\ (a \cdot c, b \cdot d) \in \theta)$$

- faktorový okruh $\mathcal{R}/I$ okruhu $\mathcal{R}$ dle ideálu I:
  - je okruh na množině $R/I = \{r + I, r \in R\}$, kde pro prvek $r \in R$ je $r + I = \{r + i, i \in I\}$, s operacemi

$$(r + I) \oplus (s + I) = (r + s) + I,$$
$$(r + I) \odot (s + I) = (r \cdot s) + I.$$

1.1. V každém okruhu $\mathcal{R}$ platí:

- pro ideál I na $\mathcal{R}$ je relace $\theta_I = \{(x, y) \in R^2; x - y \in I\}$ kongruence na $\mathcal{R}$
- pro kongruenci θ na okruhu $\mathcal{R}$ je množina $I_\theta = \{x \in R; (x, 0) \in \theta\}$ ideál v $\mathcal{R}$
- pro každý ideál I a každou kongruenci θ na $\mathcal{R}$ platí $\theta_{I_\theta} = \theta$ a $I_{\theta_I} = I$, tj. existuje vzájemně jednoznačný vztah mezi kongruencemi a ideály.

1.2. Faktorový okruh $\mathcal{R}/I$ unitárního okruhu $\mathcal{R}$ dle ideálu I je

- těleso, právě když ideál I je maximální
- obor integrity, právě když ideál I je prvoideál.

1.3. Průnik libovolného systému ideálů okruhu $\mathcal{R}$ je opět ideál tohoto okruhu. Pro danou podmnožinu $M \subseteq R$ existuje nejmenší ideál $I(M)$ v $\mathcal{R}$ obsahující množinu M, přičemž

$$I(M) = \bigcap \{J; J \text{ je ideál v } \mathcal{R},\ M \subseteq J\}.$$

Nazýváme jej ideál generovaný množinou M. Ideály $I(\{m\}) = I(m)$ pro $m \in M$ nazýváme hlavní.

Buď $\mathcal{J} = (J, +, 0, \cdot, 1)$ obor integrity a $a, b, c \in J$:

- řekneme, že prvek a dělí prvek b (zapisujeme $a|b$), existuje-li prvek c tak, že $b = a \cdot c$
- prvek $j \in J$, pro který platí $j|1$, nazveme jednotka dělení v $\mathcal{J}$
- prvky a, b nazveme asociované, platí-li $(a|b) \wedge (b|a)$, píšeme $a \parallel b$
- prvek $d \in J$ nazveme společný dělitel (násobek) prvků a, b, je-li $(d|a) \wedge (d|b)$ $((a|d) \wedge (b|d))$
- prvek $d \in J$ nazveme největší společný dělitel prvků a, b, je-li d společný dělitel a pro každého dalšího společného dělitele d' prvků a, b platí $d'|d$; píšeme $d = (a, b)$
- prvek $n \in J$ nazveme nejmenší společný násobek prvků a, b, je-li n jejich společný násobek a pro každý společný násobek n' prvků a, b platí $n|n'$; píšeme $n = [a, b]$
- prvky $a \in J$, pro které platí $a \parallel 1$ nebo $a \parallel b$, se nazývají triviální dělitelé prvku b
- nenulový prvek, který není jednotka a má pouze triviální dělitele, nazýváme ireducibilní (nerozložitelný)
- nenulový prvek a, který není jednotka, a pro který platí implikace

$$a|(b \cdot c) \Rightarrow ((a|b) \vee (a|c)),$$

nazýváme prvočinitel.

1.4 Prvek $j \in J$ je jednotka dělení v $\mathcal{J}$, právě když je prvek j invertibilní v $\mathcal{J}$, tj. existuje prvek $j^{-1} \in J$. Množina $\mathfrak{J}(\mathcal{J})$ všech jednotek oboru integrity $\mathcal{J}$ tvoří vzhledem k operaci $\cdot$ grupu.

1.5 Největší společný dělitel (nejmenší společný násobek) je v oboru integrity $\mathcal{J}$ určen jednoznačně (pokud existuje) až na asociovanost, tj. jsou-li d, d' největší společní dělitelé (nejmenší společné násobky) prvků $a, b \in J$, pak $d \parallel d'$.

1.6 Každý prvočinitel oboru integrity $\mathcal{J}$ je ireducibilní prvek, opak však obecně neplatí.

Řekneme, že obor integrity $\mathcal{J}$ splňuje podmínku

- *existence ireducibilních rozkladů* (EIR), lze-li každý prvek $a \in \mathcal{J}$, $a \neq 0$, $a \nparallel 1$, rozložit na součin konečného počtu ireducibilních prvků.

- *jednoznačnosti ireducibilních rozkladů* (JIR), jsou-li každé dva rozklady daného prvku $a = p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$ v součin ireducibilních prvků asociovány, tj. platí $m = n$ a po vhodném uspořádání prvků v rozkladech platí $p_i \parallel q_i$ pro $i = 1, \ldots, n$
- *prvočinitelovou* (P), je-li každý ireducibilní prvek z $\mathcal{J}$ prvočinitel
- *existence největších společných dělitelů* (ENSD), má-li každá dvojice prvků z J největšího společného dělitele
- *existence nejmenších společných násobků* (ENSN), má-li každá dvojice prvků z J nejmenší společný násobek
- *konečnosti řetězců vlastních dělitelů* (KŘVD), je-li každá posloupnost prvků $a_1, \ldots, a_n, \ldots$ z J konečná, kde pro každé i je a_i je netriviální dělitel a_{i+1} pro každé i

Obor integrity $\mathcal{J}$ nazveme

- *Gaussův*, splňuje-li podmínky (EIR) a (JIR)
- *obor integrity hlavních ideálů* (OIHI), je-li každý ideál v $\mathcal{J}$ hlavní
- *eukleidovský obor integrity* (EOI), existuje-li taková funkce $\delta\colon J\setminus\{0\} \to \mathbb{N}_0$, že pro každé dva prvky $a, b \in J$, $b \neq 0$, existují prvky $q, r \in J$ tak, že $a = b \cdot q + r$, kde $r = 0$ nebo $\delta(r) < \delta(b)$ (taková funkce na J se nazývá eukleidovská)

1.7. V každém oboru integrity platí tyto vztahy:

- (KŘVD) $\Rightarrow$ (EIR)
- (P) $\Rightarrow$ (JIR)
- (ENSD) $\Leftrightarrow$ (ENSN)
- (ENSD) $\Rightarrow$ (P)
- (G) $\Rightarrow$ ((KŘVD) $\wedge$ (ENSD))
- (G) $\Leftrightarrow$((KŘVD) $\wedge$ (P))
- (OIHI) $\Rightarrow$ ((KŘVD) $\wedge$ (ENSD))
- (EOI) $\Rightarrow$ (OIHI) $\Rightarrow$ (G)

1.8. V každém oboru integrity hlavních ideálů $\mathcal{J}$ jsou ekvivalentní podmínky:

- prvek $p \in J$ je prvočinitel
- ideál $I(p)$ je maximální
- ideál $I(p)$ je prvoideál.

1.9. V každém eukleidovském oboru integrity $\mathcal{J}$ lze největšího společného dělitele (a, b) prvků $a, b \in J$, $b \neq 0$, najít pomocí tzv. Eukleidova algoritmu:

$$\begin{aligned}
a &= bq_0 + r_1, & \delta(r_1) &< \delta(b)\\
b &= r_1q_1 + r_2, & \delta(r_2) &< \delta(r_1)\\
&\vdots & &\\
r_{i-1} &= r_iq_i + r_{i+1}, & \delta(r_{i+1}) &< \delta(r_i)\\
&\vdots & &\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, & \delta(r_n) &< \delta(r_{n-1})\\
r_{n-1} &= r_nq_n,
\end{aligned}$$

přičemž $(a,b) = (r_1,b) = (r_1,r_2) = \ldots = (r_{n-2},r_{n-1}) = (r_{n-1},r_n) = r_n$.

Pro prvky $a, b \in J$ navíc existují prvky $x, y \in J$ tak, že platí

$$a \cdot x + b \cdot y = (a,b).$$

1.10. $\mathbb{Z}$ je eukleidovský obor integrity s eukleidovskou funkcí

$$\delta \colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}, \delta(z) = |z|.$$

Celá část reálného čísla

Mějme dána čísla $a, b \in \mathbb{Z}$, $b \in \mathbb{N}$. Jelikož obor integrity $\mathbb{Z}$ je dle 1.10. eukleidovský, existují čísla $q, r \in \mathbb{Z}$ tak, že platí

$$a = b \cdot q + r, \quad 0 \leq r < b,$$

tj.

$$\frac{a}{b} = q + \frac{r}{b},$$

kde $0 \leq \frac{r}{b} < 1$ a $q \leq \frac{a}{b} < q+1$. Číslo q je možné interpretovat jako největší celé číslo nepřevyšující zlomek $\frac{a}{b}$. Nazýváme jej *celá část racionálního čísla* $\frac{a}{b}$ a značíme $q = [\frac{a}{b}]$.

Pro reálné číslo α podobně definujeme jeho celou část $[\alpha]$ jako nejmenší celé číslo nepřevyšující α, tj.

$$[\alpha] \leq \alpha < [\alpha] + 1.$$

Hledejme nyní mocninu prvočísla p, v níž vystupuje v kanonickém rozkladu čísla $n!$. Všech čísel menších než n dělitelných číslem p v právě k-té mocnině je právě $\left[\frac{n}{p^k}\right]$, tedy exponent prvočísla p v rozkladu čísla $n!$ je právě

$$\operatorname{ord}_p n! = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^k}\right],$$

kde k je největší přirozené číslo vlastnosti $p^k \leq n$.

Cvičení

1. Najděte mocninu daného prvočísla v rozkladu daného čísla:
   a) 7 v 89! b) 5 v 313! c) 11 v 887! d) 3 v 569!
2. Určete, kolika nulami končí čísla 295! a 299!.
3. Najděte kanonické rozklady čísel 10! a 20!.
4. Najděte největší přírozené číslo x splňující vlastnost $13^x | 201 \cdot 202 \cdot \ldots \cdot 700$.
5. Dokažte, že $[x+y] \geq [x] + [y]$ a obecně $[x+y+\ldots+z] \geq [x] + [y] + \ldots + [z]$.
6. Dokažte, že pro reálná čísla α, β platí $[2\alpha] + [2\beta] \geq [\alpha] + [\beta] + [\alpha+\beta]$.
7. Dokažte, že pro přirozená čísla m, n je číslo $\frac{(2m)!\,(2n)!}{m!n!(m+m)!}$ celé.
8. Dokažte, že pro libovolné reálné číslo x a přirozené číslo n platí

$$[x] + \left[x + \frac{1}{n}\right] + \ldots + \left[x + \frac{n-1}{n}\right] = [nx].$$

Okruhy zbytkových tříd a kongruence v $\mathbb{Z}$

Z 1.10 a 1.7 vyplývá, že $\mathbb{Z}$ je oborem integrity hlavních ideálů a každý ideál v $\mathbb{Z}$ je tvaru $I(n) = \{k \cdot n; k \in \mathbb{Z}\}$ pro $n \in \mathbb{N}$. Každá kongruence na $\mathbb{Z}$ je dle 1.1 tedy ve tvaru

$$\theta_{I(n)} = \{(x, y) \in \mathbb{Z}^2 \colon x - y \in I(n)\} = \{(x, y) \in \mathbb{Z}^2 \colon n | x - y\}.$$

Kongruenci $\theta_{I(n)}$ bývá zvykem značit symbolem $\equiv_n$ a vlastnost $(x, y) \in \equiv_n$ budeme zapisovat

$$x \equiv y \pmod{n}$$

(čteme x je kongruentní s y modulo n). Faktorové okruhy $\mathbb{Z}/\equiv_n$ značíme $\mathbb{Z}_n$ a nazýváme *okruhy zbytkových tříd modulo n*. Prvky okruhů $\mathbb{Z}_n$ budeme značit symboly $\overline{a}$ pro $a \in \mathbb{Z}$, přitom $\mathbb{Z}_n$ má právě n prvků. Operace v $\mathbb{Z}_n$ jsou definovány formulemi

$$\overline{a} + \overline{b} = \overline{a + b}, \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

V okruhu $\mathbb{Z}$ vzhledem k vlastnosti (EOI) splývají prvočinitelé a ireducibilní prvky a nazývají se *prvočísla*. Rozložitelné prvky v $\mathbb{Z}$ pak nazýváme *čísla složená*.

Z 1.8 dále vyplývá, že okruh $\mathbb{Z}_n$ je tělesem, právě když n je prvočíslo, přičemž pro složené n není $\mathbb{Z}_n$ ani obor integrity. (Proč?)

1.11 Základní vlastnosti kongruencí:

1) platí-li $a \equiv a' \pmod{m}$, $b \equiv b' \pmod{m}$, pak také

$$a + b \equiv a' + b' \pmod{m}, \qquad a \cdot b \equiv a' \cdot b' \pmod{m}.$$

Důkaz: Tato vlastnost je substituční podmínka relace $\equiv_m$.

2) platí-li $a \equiv b \pmod{m}$, $d|a$, $d|b$, $(d, m) = 1$, pak

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

Důkaz: Platí $m|(a - b) = d \cdot (a_1 - b_1)$, kde $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Vzhledem k podmínce $(m, d) = 1$ platí nutně $m|(a_1 - b_1) = \frac{a}{d} - \frac{b}{d}$.

3) platí-li $a \equiv b \pmod{m}$, pak $a \cdot c \equiv b \cdot c \pmod{m \cdot c}$.

Důkaz: Je-li $m|(a - b)$, pak $m \cdot c|(a - b) \cdot c = a \cdot c - b \cdot c$.

4) platí-li $a \equiv b \pmod{m}$, $d|a$, $d|b$, $d|m$, pak

$$\frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right).$$

Důkaz: Jestliže položíme $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$, $m_1 = \frac{m}{d}$, pak z $m|(a - b)$ plyne $m_1 \cdot d|d \cdot (a_1 - b_1)$, odkud $m_1|(a_1 - b_1)$.

5) platí-li $a \equiv b \pmod{m_i}$, kde $\{m_i\}$ je konečná množina prvků z $\mathbb{N}$, pak

$$a \equiv b \pmod{[\{m_i\}]}.$$

Důkaz: Z podmínek $m_i|(a-b)$ plyne $[\{m_i\}]|(a-b)$.

6) platí-li $a \equiv b \pmod{m},\ d|m$, pak $a \equiv b \pmod{d}$.

Důkaz: Z vlastností $d|m,\ m|(a-b)$ plyne $d|(a-b)$.

7) platí-li $a \equiv b \pmod{m}$, $d|a$, $d|m$, pak $d|b$.

Důkaz: Položíme-li $a_1 = \frac{a}{d}$, $m_1 = \frac{m}{d}$, pak z podmínky $m_1 \cdot d|(a_1 \cdot d - b)$ plyne $a_1 \cdot d - b = m_1 \cdot d \cdot t$ pro nějaké $t \in \mathbb{Z}$, odkud $b = a_1 \cdot d - m_1 \cdot d \cdot t$, tj. $d|b$.

8) platí-li $a \equiv b \pmod{m}$, pak $(a, m) = (b, m)$.

Důkaz: Důsledek vlastnosti 7.

9) platí-li $a \cdot d \equiv b \cdot d \pmod{m}$, pak $a \equiv b \pmod{\frac{m}{(m,d)}}$.

Důkaz: Nechť $k = (m, d), m_1 = \frac{m}{k}, d_1 = \frac{d}{k}$. Pak platí $a \cdot d_1 \cdot k \equiv b \cdot d_1 \cdot k \pmod{m_1 \cdot k}$, odkud dle 4) dostaneme $a \cdot d_1 \equiv b \cdot d_1 \pmod{m_1}$. Ovšem $(m_1, d_1) = 1$, tedy dle 2) je $a \equiv b \pmod{m_1}$.

Následující tvrzení popisuje nedělitele nuly, resp. všechny invertibilní prvky v okruzích $\mathbb{Z}_n$:

Věta 1.12. *Nechť $n \in \mathbb{N} \setminus \{1\}$, $a \in \mathbb{Z}$. Následující podmínky jsou ekvivalentní:*

(i) $\overline{a}$ *je nedělitel nuly v* $\mathbb{Z}_n$

(ii) $(a, n) = 1$

(iii) $\overline{a}$ *je invertibilní prvek v* $\mathbb{Z}_n$

(iv) $\overline{a}$ *je generátor grupy* $(\mathbb{Z}_n, +, \overline{0})$.

Důkaz: (i) $\Rightarrow$ (ii) Nechť $\overline{a}$ je nedělitel nuly v $\mathbb{Z}_n$ a nechť $(a, n) = d \neq 1$. Pak existují prvky $u, v \in \mathbb{Z}$, $u \neq n$, tak, že $d \cdot u = n$, $a = d \cdot v$. Pak

$$\overline{a} \cdot \overline{u} = \overline{v} \cdot \overline{d} \cdot \overline{u} = \overline{v} \cdot \overline{n} = \overline{v} \cdot \overline{0} = \overline{0}.$$

Jelikož $\overline{a}$ je nedělitel nuly, nutně $\overline{u} = \overline{0}$, spor.

(ii) $\Rightarrow$ (iii) Platí-li $(a, n) = 1$, existují dle 1.9 prvky $x, y \in \mathbb{Z}$ takové, že $a \cdot x + n \cdot y = 1$. Pak ovšem $\overline{a} \cdot \overline{x} + \overline{n} \cdot \overline{y} = \overline{a} \cdot \overline{x} = \overline{1}$, tedy $\overline{x} = \overline{a}^{-1}$.

(iii) $\Rightarrow$ (i) Nechť $\overline{a}$ je invertibilní prvek v $\mathbb{Z}_n$ a pro $\overline{b} \in \mathbb{Z}_n$ platí $\overline{a} \cdot \overline{b} = \overline{0}$. Vynásobením poslední rovnosti prvkem $\overline{a}^{-1}$ dostaneme $\overline{b} = \overline{0}$, tedy $\overline{a}$ je nedělitel nuly.

(iv) $\Rightarrow$ (i) Je-li $\overline{a}$ generátor uvedené grupy, pak řád prvku $\overline{a}$ je roven n (tj. je roven řádu grupy). Nejmenší přirozené číslo k vlastnosti $k \times \overline{a} = \overline{0}$ je tedy $k = n$. Pro $0 \leq b \leq n-1$ tudíž $\overline{b} \cdot \overline{a} \neq \overline{0}$, odkud $\overline{a}$ je nedělitel nuly.

(i) $\Rightarrow$ (iv) Je-li $\overline{a}$ nedělitel nuly, pak pro $0 < b \leq n-1$ je $\overline{b} \cdot \overline{a} \neq \overline{0}$, tedy nejmenší přirozené číslo k, pro něž je $k \times \overline{a} = \overline{0}$, je $k = n$. □

Eulerova funkce

Dokázali jsme, že počet invertibilních prvků, resp. nedělitelů nuly, resp. různých generátorů grupy $(\mathbb{Z}_n, +)$ je roven počtu přirozených čísel menších než n nesoudělných s n. Funkci $\phi\colon \mathbb{N} \to \mathbb{N}$, která každému přirozenému číslu $n \in \mathbb{N}$ přiřadí počet přirozených čísel menších než n a nesoudělných s n, nazýváme *Eulerova funkce*. Ukažme některé základní vlastnosti funkce ϕ, vedoucí k jejímu vyčíslení z kanonického rozkladu čísla n.

Věta 1.13. *Je-li $\mathcal{C}$ cyklická grupa řádu a, $\mathcal{H}$ cyklická grupa řádu b a $(a, b) = 1$, pak direktní součin $\mathcal{C} \times \mathcal{H}$ je cyklická grupa řádu $a \cdot b$.*

Důkaz: Buďte g, resp. h, generátory grupy $\mathcal{C}$, resp. $\mathcal{H}$. Jelikož je $(a, b) = 1$, platí $[a \cdot b] = a \cdot b$. Ukážeme, že $a \cdot b$ je řád prvku (g, h) v grupě $\mathcal{C} \times \mathcal{H}$. Evidentně platí

$$(g, h)^{ab} = (g^{ab}, h^{ab}) = (1_G, 1_H).$$

Je-li c nyní takové přirozené číslo, že platí $(g, h)^c = (1_G, 1_H)$, pak $g^c = 1_G$, $h^c = 1_H$. Jelikož a, resp. b, je řád prvku g, resp. h, je nutně $a|c$, $b|c$, odtud $[a, b] = a \cdot b|c$. Všechny generátory grupy $\mathcal{C} \times \mathcal{H}$ jsou přitom ve tvaru (g, h), kde g, resp. h, je generátor grupy $\mathcal{C}$, resp. $\mathcal{H}$. □

Důsledkem je následující věta.

Věta 1.14. *Funkce ϕ je multiplikativní, tj. pro $a, b \in \mathbb{N}$, $(a, b) = 1$, je*

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b).$$

Důkaz: Pole důkazu předchozí věty 1.14 má cyklická grupa řádu $a \cdot b$ právě $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ navzájem různých generátorů. □

Dalším důsledkem je pak věta:

Věta 1.15. *Je-li $n = p_1^{\alpha_1} \cdot \ldots p_k^{\alpha_k}$ kanonický rozklad čísla n, pak platí*

$$\phi(p_1^{\alpha_1} \cdot \ldots p_k^{\alpha_k}) = \phi(p_1^{\alpha_1}) \cdot \ldots \cdot \phi(p_k^{\alpha_k}),$$

přičemž

$$\phi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}.$$

Důkaz: Přirozená čísla menší než $p_i^{\alpha_i}$, která jsou s n soudělná, jsou právě $1 \cdot p_i$, $2 \cdot p_i$, …, $p_i^{\alpha_i - 1} \cdot p_i$, a je jich tedy právě $p_i^{\alpha_i - 1}$. □

Úplný a redukovaný systém zbytků

Množinu celých čísel $\{a_1, \ldots, a_n\}$ nazveme *úplný systém zbytků modulo* n, platí-li $\overline{a}_i \neq \overline{a}_j$ pro $i \neq j$.

Příklad. Zřejmě množina $\{0, 1, \ldots, n-1\}$ je úplný systém zbytků modulo n. Pro sudé n je také $\{0, \pm 1, \ldots, \pm(\frac{1}{2}n - 1), \frac{1}{2}n\}$ úplný systém zbytků, přičemž se jedná o úplný systém s nejmenšími absolutními hodnotami. Podobně pro n liché je $\{0, \pm 1, \ldots, \pm\frac{1}{2}(n-1)\}$ úplný systém zbytků s nejmenšími absolutními hodnotami.

Věta 1.16. (První věta o zbytcích lineární formy) *Probíhá-li x úplný systém zbytků modulo n, pak pro $a, b \in \mathbb{Z}$, $(a, n) = 1$, probíhá množina $a \cdot x + b$ také úplný systém zbytků modulo n.*

Důkaz: Nechť pro prvky x, x' platí $a \cdot x + b \equiv a \cdot x' + b \pmod{n}$. Pak je $a(x - x') \equiv 0 \pmod{n}$. Jelikož $(a, n) = 1$, je $\overline{a}$ nedělitel nuly v $\mathbb{Z}_n$, tedy platí $x \equiv x' \pmod{n}$. □

Množina prvků $\{a_1, \ldots, a_{\phi(n)}\}$ se nazývá *redukovaný systém zbytků modulo* n, je-li množina $\{\overline{a}, \ldots, \overline{a}_{\phi(n)}\}$ množinou právě všech nedělitelů nuly v $\mathbb{Z}_n$.

Příklad. Jak jsme odvodili, je počet prvků každého redukovaného systému zbytků modulo n roven $\phi(n)$; v $\mathbb{Z}_{10}$ je množina $\{1, 3, 7, 9\}$ redukovaný systém zbytků, přitom množina $\{1, 3, -3, -1\}$ je redukovaným systémem s nejmenšími absolutními hodnotami.

Věta 1.17. (Druhá věta o zbytcích lineární formy) *Probíhá-li x redukovaný systém zbytků modulo n, pak pro $a \in \mathbb{Z}$, $(a, n) = 1$, probíhá množina $a \cdot x$ také redukovaný systém zbytků modulo n.*

Důkaz: Jelikož $(a, n) = 1$, je prvek $\overline{a}$ invertibilní v $\mathbb{Z}_n$. Každý z prvků $\overline{x}$ je také invertibilní, tedy i prvky $\overline{a} \cdot \overline{x}$ jsou invertibilní. Kdyby platilo $\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{x}_1$, pak by $\overline{a} \cdot (\overline{x} - \overline{x}_1) = \overline{0}$, což vzhledem k invertibilitě prvku $\overline{a}$ znamená $\overline{x} = \overline{x}_1$. □

Kapitola 2

Vlastnosti prvočísel

2.1 Obecné vlastnosti prvočísel

Některé vlastnosti prvočísel byly známy už ve starověkém Řecku. Eratosthenes např. vypracoval velice jednoduchou metodu, zvanou *Eratosthenovo síto*, pro hledání prvočísel v řadě všech přirozených čísel. Bral postupně všechna čísla a z posloupnosti všech přirozených čísel vyškrtával všechny jejich násobky. Čísla, která mu zůstávala, byla právě prvočísla. Hledání prvočísel umožní následující věta.

Věta 2.1. *Číslo n je složené, právě když je dělitelné některým prvočíslem $p \leq \sqrt{n}$.*

Důkaz: Je-li n složené, pak má alespoň dva netriviální dělitele u, v, tj. $n = uv$. Je-li např. $u \leq v$, pak $n = uv \geq u^2$, tedy $u \leq \sqrt{n}$. □

Při rozhodování, zda je dané číslo n prvočíslem tedy stačí vyšetřit dělitelnost pouze všemi prvočísly, která jsou menší nebo rovna $\sqrt{n}$.

Otázka o konečnosti či nekonečnosti počtu prvočísel byla vyřešena také už ve starověku, a to Eukleidem:

Věta 2.2. *Prvočísel je nekonečně mnoho.*

Důkaz: Předpokládejme sporem, že $p_1, \ldots, p_m$ jsou všechna prvočísla. Kdyby číslo $p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1$ bylo prvočíslem, pak by se muselo rovnat některému z prvočísel p_i. Ovšem číslo $p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1$ dává po vydělení číslem p_i zbytek 1, což je spor. Kdyby uvedené číslo bylo složené, pak je dělitelné některým z prvočísel p_i a dostaneme opět spor. □

Další zajímavou otázkou týkající se prvočísel je problém, zda pro posloupnost přirozených čísel existuje nějaká konstanta k taková, že každá po sobě následující prvočísla od sebe nejsou dále než k. Jak snadno zjistíme, žádná taková konstanta neexistuje. Uvažujeme-li totiž čísla

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (k+1),$$

dostaneme pro $k > n$ posloupnost k po sobě následujících přirozených čísel, která jsou všechna složená. Platí tedy:

Věta 2.3. *Pro každé $k \in \mathbb{N}$ existuje v posloupnosti přirozených čísel k členů této posloupnosti jdoucích za sebou, jež jsou všechna složená.*

Tato věta vypovídá o nepravidelnosti uspořádání prvočísel v posloupnosti přirozených čísel. Přirozeně také matematikové hledali formuli, pomocí níž by bylo možno generovat prvočísla, zvláště pak se hledaly polynomy s celočíselnými koeficienty, nabývající pouze prvočíselných hodnot. *L. Euler* (1707-1783) si např. povšiml, že polynom $f(x) = x^2 + x + 41$ nabývá prvočíselných hodnot pro $x = 0, \ldots, 39$. Snadno se dá ověřit, že $41|f(40)$. Podobně polynom $g(y) = y^2 - 79y + 1601$ nabývá prvočíselných hodnot dokonce pro $y = 0, \ldots, 79$ a polynom $h(x) = 4x^2 + 2x + 41$ pro $x = 0, \ldots, 19$. Ukažme, že najít takový polynom, aby pro skoro všechny hodnoty x nabýval prvočíselných hodnot, není principiálně možné.

Věta 2.4. *Neexistuje polynom s celočíselnými koeficienty různý od konstanty tak, aby nabýval prvočíselných hodnot pro skoro všechna $n \in \mathbb{N}$.*

Důkaz: Nechť $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ a nechť $a_n > 0$, tj. $f(n) \to \infty$ pro $n \to \infty$. Je tedy $f(n) > 1$ pro všechna $n > N$ pro některé $N \in \mathbb{N}$. Nechť $x > N$ a položme $y = f(x) = a_n x^n + \cdots + a_1 x + a_0 > 1$. Uvažujme hodnoty

$$f(ry + x) = a_n(ry + x)^n + \cdots + a_1(ry + x) + a_0$$

pro $r \in \mathbb{N}$. V okruhu $\mathbb{Z}_y$ pak platí $\overline{y} = \overline{0}$, odkud

$$\overline{f(ry + x)} = \overline{a_n}(\overline{ry} + \overline{x})^n + \cdots + \overline{a_1}(\overline{ry} + \overline{x}) + \overline{a_0} = \overline{a_n}\overline{x}^n + \cdots + \overline{a_1 x} + \overline{a_0} = \overline{y} = \overline{0},$$

tedy $y|f(ry+x)$ pro každé r. Jelikož $f(ry+x) \to \infty$ pro $r \to \infty$, nabývá polynom $f(x)$ nekonečně mnoha složených hodnot pro libovolně velká x. □

Za zmínku stojí, že v r. 1976 byl nalezen polynom 25. stupně o 26 proměnných, jehož všechny kladné hodnoty v celočíselných nezáporných bodech jsou prvočísly [6].

Označme nyní pro $n \in \mathbb{N}$ symbolem p_n n-té prvočíslo, tedy $p_1 = 2$, $p_2 = 3$, atd. Zabývejme se dále otázkou odhadu n-tého prvočísla pomocí prvočísel předcházejících.

Věta 2.5. *Je-li p_n n-té prvočíslo, pak $p_{n+1} \leq p_1 \cdot \ldots \cdot p_n + 1$.*

Důkaz: Označme $p = p_1 \cdot \cdots \cdot p_n + 1$. Je-li p prvočíslo, pak vzhledem k tomu, že $p > p_j$ pro $j = 1, \ldots, n$, je $p_{n+1} \leq p$. Je-li p složené, pak je dělitelné některým prvočíslem větším než p_n (prvočísly $p_1, \ldots, p_n$ totiž číslo p dělitelné není). To ale opět znamená, že $p_{n+1} \leq p$. □

Věta 2.6. *Pro každé $n \in \mathbb{N}$ platí $p_n < 2^{2^n}$.*

Důkaz: Tvrzení dokážeme indukcí. Zřejmě $p_1 < 4$. Předpokládejme, že $p_k < 2^{2^k}$ pro každé $k \leq n$. Dle předchozího tvrzení pak dostaneme

$$p_{n+1} \leq p_1 \cdot \ldots \cdot p_n + 1 < 2^{2^1} \cdot \ldots \cdot 2^{2^n} + 1 = 2^{2^1 + \cdots + 2^n} + 1 = 2^{2^{n+1}-2} + 1 = \\ = \frac{1}{4} \cdot 2^{2^{n+1}} + 1 < 2^{2^{n+1}}.$$

□

Označme nyní pro každé $x \in \mathbb{R}$, $x \geq 2$, symbolem $\pi(x)$ funkci udávající počet prvočísel menších nebo rovných než x (je tedy $\pi(3) = 2$, $\pi(4) = 2$, $\pi(5) = 3$ atd.). Tato funkce hraje v teorii čísel důležitou roli. Podíl $\frac{\pi(x)}{x}$ udává *hustotu prvočísel* v množině všech přirozených čísel menších než x a hodnota

$$\lim_{x \to \infty} \frac{\pi(x)}{x}$$

udává *hustotu prvočísel v množině všech přirozených čísel.*

Věta 2.7. *Pro každé $x \geq 2$ platí $\pi(x) \geq \ln \ln x$.*

Důkaz: Zřejmě pro $2 \leq x \leq \mathrm{e}$ je $\pi(x) = \pi(2) = 1 \geq \ln \ln x$. Ke každému $x \in \mathbb{N}$, $x > \mathrm{e}$, existuje $n \in \mathbb{N}$ tak, že $\mathrm{e}^{\mathrm{e}^{n-1}} < x \leq \mathrm{e}^{\mathrm{e}^n}$. Přitom pro $n \geq 4$ platí $\mathrm{e}^{n-1} > 2^n$, tedy $\mathrm{e}^{\mathrm{e}^{n-1}} > 2^{2^n}$. Pak

$$\pi(x) \geq \pi\left(\mathrm{e}^{\mathrm{e}^{n-1}}\right) \geq \pi\left(2^{2^n}\right) \geq \pi(p_n) = n.$$

Ovšem $x \leq \mathrm{e}^{\mathrm{e}^n}$, tedy $\ln \ln x \leq n$ a celkem $\pi(x) \geq \ln \ln x$. □

Věta 2.8. *Pro každé $x \geq 2$ platí $\pi(x) \geq \dfrac{\ln x}{2 \ln 2}$.*

Důkaz: Pro $n \in \mathbb{N}$ nechť $\gamma(n)$ je množina všech prvočíselných dělitelů čísla n a nechť $\mathbb{P}$ je množina všech prvočísel. Označme pro $S \subseteq \mathbb{P}$ symbolem $f_S(x)$ počet čísel n menších nebo rovných x takových, že $\gamma(n) \subseteq S$. Nechť dále množina S má právě t prvků a nechť $n = m^2 s$, kde s už neobsahuje v rozkladu kvadráty. Pak $m \leq \sqrt{n} \leq \sqrt{x}$. Z podmínky $\gamma(n) \subseteq S$ plyne, že v rozkladu čísla s se mohou vyskytovat pouze prvočísla z S a to nejvýše v první mocnině. Jelikož S má právě t prvků, lze prvek s vybrat nejvýše 2^t způsoby. Protože $m \leq \sqrt{x}$, lze prvek m vybrat nejvýše $\sqrt{x}$ způsoby, a tedy n nejvýše $f_S(x) \leq 2^t \sqrt{x}$ způsoby. Je-li nyní $\pi(x) = m$, tj. $p_{m+1} > x$, pak pro $S = \{p_1, \ldots, p_m\}$ je $f_S(x) = x$, tedy

$$x \leq 2^m \sqrt{x} = 2^{\pi(x)} \sqrt{x},$$

odkud logaritmováním dostaneme dokazovanou nerovnost. □

S funkcí $\pi(x)$ těsně souvisí funkce

$$\theta(x) = \sum_{p \le x} \ln p,$$

kde v sumě sčítáme přes všechna prvočísla $p \le x$ (předpokládáme $x \ge 1$ a definitoricky klademe $\theta(1) = 0$). Zabývejme se dále jejím horním odhadem:

Věta 2.9. *Pro každé $x > 1$ platí $\theta(x) < (4 \ln 2)x$.*

Důkaz: Uvažujme kombinační čísla $\binom{2n}{n} = \frac{(n+1)\cdot\ldots\cdot(2n)}{n!}$. Zřejmě pro každé prvočíslo p, $n < p < 2n$, platí $p \mid \binom{2n}{n}$. Dále

$$2^{2n} = (1+1)^{2n} = \sum_{j=0}^{2n} \binom{2n}{j} > \binom{2n}{n},$$

odkud

$$2^{2n} > \binom{2n}{n} > \prod_{p>n}^{p<2n} p,$$

tj.

$$2n \ln 2 > \sum_{p>n}^{p<2n} \ln p = \theta(2n) - \theta(n).$$

Sečtením posledních nerovností pro $n = 1, \ldots, 2^{m-1}$ dostaneme

$$\theta(2^m) = \theta(2^m) - \theta(1) < 2 \ln 2 \cdot (1 + \ldots + 2^{m-1}) = 2 \ln 2 \frac{2^m - 1}{2 - 1} =$$
$$= \ln 2 \cdot (2^{m+1} - 2) < \ln 2 \cdot 2^{m+1}.$$

Je-li $2^{m-1} < x \le 2^m$, pak

$$\theta(x) \le \theta(2^m) < \ln 2 \cdot 2^{m+1} = 4 \ln 2 \cdot 2^{m-1} < (4 \ln 2)x. \qquad \square$$

Předchozí odhad funkce θ má velký význam pro popis funkce $\pi(x)$:

Věta 2.10. *Existuje konstanta $c > 0$ taková, že pro $x \ge 2$ platí*

$$\pi(x) < \frac{cx}{\ln x}.$$

Důkaz: Nejprve si uvědomme, že pro funkci π platí nerovnosti $\pi(\sqrt{x}) \le \sqrt{x}$, a tedy $-\pi(\sqrt{x}) \ge -\sqrt{x}$, a že rozdíl $\pi(x) - \pi(\sqrt{x})$ udává počet prvočísel mezi čísly $\sqrt{x}$ a x. Odtud odvodíme nerovnost

$$\theta(x) \ge \sum_{p>\sqrt{x}}^{p \le x} \ln p \ge \ln \sqrt{x}\,(\pi(x) - \pi(\sqrt{x})) \ge \ln \sqrt{x}\,\pi(x) - \sqrt{x} \ln \sqrt{x}.$$

Pak ale vydělením předchozí nerovnosti hodnotou $\ln\sqrt{x}$ a užitím věty 2.8 dostaneme

$$\pi(x) \leq \frac{\theta(x)}{\ln\sqrt{x}} + \sqrt{x} = \frac{2\theta(x)}{\ln x} + \sqrt{x} \leq \frac{(8\ln 2)x}{\ln x} + \sqrt{x}.$$

Pro $x \geq 2$ ale platí $\sqrt{x} < \frac{2x}{\ln x}$ (je totiž $\ln x < 2\sqrt{x}$), odkud

$$\pi(x) < \frac{(8\ln 2)x}{\ln x} + \frac{2x}{\ln x} = (8\ln 2 + 2)\frac{x}{\ln x} = c\,\frac{x}{\ln x}.$$

□

Jakožto bezprostřední důsledek předchozí věty dostáváme následující tvrzení:

Věta 2.11. *Platí* $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{x} = 0.$

Definice. Je-li A nějaká podmnožina množiny všech přirozených čísel a pro každé $n \in \mathbb{N}$ je $A(n)$ počet těch čísel z A, která jsou menší nebo rovna n, pak se limita

$$h(A) = \lim_{n\to\infty} \frac{A(n)}{n}$$

(existuje-li) nazývá *hustota množiny* A v množině $\mathbb{N}$. Je-li přitom tato limita rovna 0, nazýváme množinu A *řídkou* v $\mathbb{N}$.

Označíme-li $\mathbb{P}$ množinu všech prvočísel, lze Tvrzení 2.11 přeformulovat takto:

Věta 2.12. *Množina* $\mathbb{P}$ *je řídká v* $\mathbb{N}$.

Čebyšev dokázal v roce 1852 následující větu:

Věta 2.13. *Existuje konstanta* $c^* > 0$ *taková, že*

$$\pi(x) > c^*\frac{x}{\ln x}.$$

I když nebudeme uvádět důkaz, zmiňme alespoň, že existence konstant c z věty 2.10 a c^* z 2.13 sehrála důležitou roli při důkazu *zákona asymptotického rozdělení prvočísel.* Řekneme, že funkce $f(x)$ a $g(x)$ (definované na nějakém intervalu (a, ∞)) jsou *asymptoticky ekvivalentní,* platí-li

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

a zapisujeme $f(x) \sim g(x)$. Na základě hypotézy zformulované Gaussem (bylo mu tehdy 15 let) dokázal v r. 1896 Hamard následující větu:

Věta 2.14. (Zákon asymptotického rozdělení prvočísel) *Funkce* $\pi(x)$ *a* $\frac{x}{\ln x}$ *jsou asymptoticky ekvivalentní.*

Uveďme pro zajímavost rozdíly ve funkčních hodnotách funkcí $\pi(x)$ a $\frac{x}{\ln x}$ pro některé hodnoty čísel x:

x	10^3	10^6	10^9
$\pi(x)$	168	78 498	50 847 478
$\frac{x}{\ln x}$	145	72 382	48 254 942

Ze zákona asymptotického rozdělení prvočísel lze odvodit asymptotický odhad n-tého prvočísla p_n.

Věta 2.15. *Platí* $p_n \sim n(\ln n)$.

Důkaz: Označme $y = \frac{x}{\ln x}$. Pak $\ln y = \ln x - \ln\ln x$. Odtud plyne

$$\lim_{x\to\infty} \frac{\ln y}{\ln x} = \lim_{x\to\infty} \left(1 - \frac{\ln\ln x}{\ln x}\right) = 1 - \lim_{x\to\infty} \frac{\ln x}{x} = 1,$$

tedy $\ln y \sim \ln x$. Dále pak $x = y \ln x \sim y \ln y$ a dle věty 2.14 je $y \sim \pi(x)$, tj. $x \sim \pi(x) \ln \pi(x)$ a konečně

$$p_n \sim \pi(p_n) \ln \pi(p_n) = n \ln n.$$

□

Poznámka. Snadno se dá ukázat, že funkce $\frac{x}{\ln x}$ je asymptoticky ekvivalentní funkci

$$\mathrm{li}(x) = \int_1^x \frac{1}{\ln t}\, dt.$$

Uvedená funkce se nazývá *logaritmusintegrál*. Dle tvrzení 2.13 tedy platí, že funkce $\pi(x)$ a $\mathrm{li}(x)$ jsou také asymptoticky ekvivalentní. Poprvé si této skutečnosti všiml Gauss při zkoumání tabulky prvočísel.

Velice důležitou úlohu v teorii čísel hrají následující tři tvrzení.

Věta 2.16. (Eulerova) *Jsou-li* $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $(a, n) = 1$, *pak*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Důkaz: Dle 1.12 víme, že podmínka $(a, n) = 1$ znamená, že prvek $\overline{a}$ je nedělitel nuly v $\mathbb{Z}_n$. Nechť $\overline{a_1}, \ldots, \overline{a}_{\phi(n)}$ jsou všichni nedělitelé nuly v $\mathbb{Z}_n$. Zřejmě každý z prvků $\overline{a} \cdot \overline{a_i}$ je také nedělitel nuly. Kdyby platilo $\overline{a} \cdot \overline{a_i} = \overline{a} \cdot \overline{a_j}$ pro některé indexy i, j, bylo by také $\overline{a_i} = \overline{a_j}$. Jsou tedy také prvky $\overline{a} \cdot \overline{a_i}$ všichni nedělitelé nuly v $\mathbb{Z}_n$. Pak ale platí

$$\overline{a} \cdot \overline{a_1} \cdot \ldots \cdot \overline{a} \cdot \overline{a}_{\phi(n)} = \overline{a} \cdot \ldots \cdot \overline{a}_{\phi(n)},$$

tj. $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Důsledkem je pak následující věta.

Věta 2.17. (malá Fermatova věta) *Pro prvočíslo p a číslo $a \in \mathbb{Z}$, $(a,p)=1$, platí*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Důkaz: Je-li p prvočíslo, pak $\phi(p) = p-1$. □

Věta 2.18. (Wilsonova věta) *Pro prvočíslo p platí* $(p-1)! \equiv -1 \pmod{p}$.

Důkaz: Dokažme nejprve, že $\overline{a}^2 = \overline{1}$ v $\mathbb{Z}_p$ právě když $\overline{a} = \overline{1}$ nebo $\overline{a} = \overline{p-1}$. Je-li $\overline{a}^2 = \overline{1}$, pak $(\overline{a}-\overline{1})\cdot(\overline{a}+\overline{1}) = \overline{0}$. Protože $\mathbb{Z}_p$ je těleso, je buď $\overline{a} = \overline{1}$ nebo $\overline{a} = -\overline{1} = \overline{p-1}$. To znamená, že pro $p > 2$ je každý z prvků $\overline{a} \in \mathbb{Z}_p, 2 \le a \le p-2$ různý od prvku k němu inverzního, tedy

$$\overline{2}\cdot\overline{3}\cdot\ldots\cdot\overline{p-2} = \overline{1},$$

odkud

$$\overline{1}\cdot\overline{2}\cdot\overline{3}\cdot\ldots\cdot\overline{p-2}\cdot\overline{p-1} = \overline{p-1} = -\overline{1},$$

neboli $(p-1)! \equiv -1 \pmod{p}$. □

Okruhy $\mathbb{Z}(\mathrm{i})$ a $\mathbb{Z}(\omega)$

Některé důležité vlastnosti prvočísel lze odvodit při studiu dělitelnosti ve speciálních oborech integrity. Takovými jsou obory integrity $\mathbb{Z}(\mathrm{i})$ a $\mathbb{Z}(\omega)$ celých algebraických čísel v tělesech $\mathbb{Q}(\mathrm{i})$ a $\mathbb{Q}(\omega)$, kde $\mathrm{i} = \sqrt{-1}$ a $\omega = -\frac{1}{2} + \frac{1}{2}\mathrm{i}\sqrt{3}$ (jedná se o speciální kvadratická tělesa, o nichž pojednává kapitola 8). Obor integrity $\mathbb{Z}(\mathrm{i}) = \{a + b\mathrm{i}; a, b \in \mathbb{Z}\}$ se nazývá *obor integrity Gaussových celých čísel*. V kapitole 8 je dokázáno, že $\mathbb{Z}(\mathrm{i})$ je EOI s eukleidovskou funkcí $n : \mathbb{Z}(\mathrm{i}) \setminus \{0\} \to \mathbb{N}$, kde pro $\alpha = a + b\mathrm{i}$ je

$$n(\alpha) = a^2 + b^2 = \alpha \cdot \overline{\alpha},$$

přičemž $\overline{\alpha} = a - b\mathrm{i}$ je komplexně sdružené číslo k α. Jednotky dělení v $\mathbb{Z}(\mathrm{i})$ jsou právě ty prvky α, pro něž je $n(\alpha) = 1$, tj. jsou to prvky $\pm 1, \pm\mathrm{i}$. Hledejme nyní všechny prvočinitele (tj. dle 1.8 také všechny ireducibilní prvky) v $\mathbb{Z}(\mathrm{i})$. Je-li α takový prvek, pak z vlastnosti $n(\alpha) = \alpha \cdot \overline{\alpha}$ bezprostředně plyne $\alpha | n(\alpha)$. Přitom $n(\alpha)$ je přirozené číslo. Provedeme-li kanonický rozklad čísla $n(\alpha)$ v $\mathbb{N}$ na součin mocnin prvočísel, pak vzhledem k ireducibilitě prvku α dělí nutně α některé z nich. Ukažme, že α nemůže dělit dvě různá prvočísla p_1, p_2. Kdyby tomu tak bylo, pak vzhledem k $(p_1, p_2) = 1$ by z 1.9 a 1.10 plynula existence celých čísel u, v tak, že $p_1 u + p_2 v = 1$. Platilo by tedy také $\alpha | (p_1 u + p_2 v = 1)$, tj. α by byla jednotka, což je spor s ireducibilitou α. Dokázali jsme tak následující větu:

Věta 2.19. *Pro ireducibilní prvek $\alpha \in \mathbb{Z}(\mathrm{i})$ existuje jediné prvočíslo p tak, že $\alpha | p$.*

Věta 2.20. *Buď p prvočíslo. Pak buď p je prvočinitel v $\mathbb{Z}(\mathrm{i})$ nebo $p = a^2 + b^2$, kde $a + b\mathrm{i}$, $a - b\mathrm{i}$ jsou prvočinitelé v $\mathbb{Z}(\mathrm{i})$.*

Důkaz: Víme, že $\mathbb{Z}(\mathrm{i})$ je EOI s eukleidovskou funkcí $n(a+b\mathrm{i}) = a^2+b^2$. Buď $p = q_1 \cdot \ldots \cdot q_k$ rozklad p na součin ireducibilních prvků $q_1, \ldots, q_k$. Pak platí $n(p) = p^2 = n(q_1) \cdot \ldots \cdot n(q_k)$. Jelikož $n(q_i)$ jsou přirozená čísla, je nutně $k \leq 2$. Pro $k = 1$ je $p = q_1$, a tedy p je ireducibilní prvek v $\mathbb{Z}(\mathrm{i})$. Pro $k = 2$ je $n(q_1) = n(q_2) = p$. Je-li $q_1 = a + b\mathrm{i}$, pak

$$p = n(q_1) = a^2 + b^2 = (a+b\mathrm{i}) \cdot (a-b\mathrm{i}) = q_1 \cdot q_2.$$

Vzhledem k jednoznačnosti rozkladů v $\mathbb{Z}(\mathrm{i})$ je $q_2 = a - b\mathrm{i}$. □

Ireducibilní prvky v $\mathbb{Z}(\mathrm{i})$ jsou tedy dělitelé prvočísel. Stačí tudíž prozkoumat, která z prvočísel jsou ireducibilní v $\mathbb{Z}(\mathrm{i})$. Uvažujeme-li prvočíslo $p = 2$, pak $2 = (1+\mathrm{i})(1-\mathrm{i})$, kde $(1-\mathrm{i})$, resp. $(1+\mathrm{i})$ jsou ireducibilní prvky. Pro lichá prvočísla lze dokázat následující větu.

Věta 2.21. *Buď p liché prvočíslo. Pak p je ireducibilní prvek v $\mathbb{Z}(\mathrm{i})$ právě když $p \equiv 3 \pmod 4$.*

Důkaz: Nechť $p \equiv 3 \pmod 4$. Není-li p ireducibilní, pak dle předchozí věty existují $a, b \in \mathbb{Z}$ tak, že $p = a^2+b^2$. Kvadráty celých čísel přitom mohou dát pouze zbytky 0 nebo 1 po dělení 4 (ověřte!), tedy $a^2+b^2 \equiv 0, 1, 2 \pmod 4$, spor. Je tedy prvek p ireducibilní.

Nechť nyní $p \equiv 1 \pmod 4$. Pak platí

$$\frac{1}{2}(p+1) \cdot \left(\frac{1}{2}(p+1)+1\right) \cdot \ldots \cdot (p-1) = \prod_{i=\frac{1}{2}(p+1)}^{p-1} i = \prod_{i=1}^{\frac{1}{2}(p-1)} (p-i).$$

Položme $x = \left(\frac{1}{2}(p-1)\right)!$. Protože $p \equiv 1 \pmod 4$, je číslo $\frac{1}{2}(p-1)$ sudé, tedy $x = \prod_{i=1}^{\frac{1}{2}(p-1)}(-i)$. Dále

$$x = \prod_{i=1}^{\frac{1}{2}(p-1)} (-i) \equiv \prod_{i=1}^{\frac{1}{2}(p-1)} (p-i) = \prod_{i=\frac{1}{2}(p+1)}^{p-1} i,$$

neboť $p - i \equiv -i \pmod p$. Celkem $x^2 \equiv (p-1)! \equiv -1 \pmod p$ (dle Wilsonovy věty), a tedy je $x^2 + 1 \equiv 0 \pmod p$. To ale znamená, že $p|(x-\mathrm{i}) \cdot (x+\mathrm{i})$. Kdyby byl prvek p ireducibilní v $\mathbb{Z}(\mathrm{i})$, pak by $p|(x-\mathrm{i})$ nebo $p|(x+\mathrm{i})$, což není možné (ověřte!). Tedy prvek p není ireducibilní. □

Jakožto důsledek předchozích dvou tvrzení dostaneme následující větu:

Věta 2.22. (Fermatova) *Je-li p prvočíslo, $p \equiv 1 \pmod 4$, pak existují celá čísla a, b tak, že $p = a^2 + b^2$.*

Věta 2.23. *Ireducibilní prvky v* $\mathbb{Z}(\mathrm{i})$ *jsou až na asociovanost právě*

(i) $1+\mathrm{i}$, $1-\mathrm{i}$,

(ii) *všechna prvočísla* $p \equiv 3 \pmod 4$,

(iii) *netriviální dělitelé prvočísel* $p \equiv 1 \pmod 4$.

Již víme, že prvočísel je nekonečně mnoho. Víme také, že pro každé liché prvočíslo p je buď $p \equiv 1 \pmod 4$ nebo $p \equiv 3 \pmod 4$. Ukažme nyní, že v obou třídách je prvočísel nekonečně mnoho.

Věta 2.24. *Existuje nekonečně mnoho prvočísel* $p \equiv 3 \pmod 4$.

Důkaz: Předpokládejme sporem, že $p_1, \ldots, p_k$ jsou právě všechna prvočísla $\equiv 3 \pmod 4$. Uvažujme číslo $n = 4 \cdot p_1 \cdot \ldots \cdot p_k - 1$. Zřejmě je $n \equiv 3 \pmod 4$. Nechť dále je $n = q_1 \cdot \ldots \cdot q_m$ rozklad čísla n v součin prvočísel. Kdyby $q_i \equiv 1 \pmod 4$ pro každé $i = 1, \ldots, m$, pak by také $n \equiv 1 \pmod 4$. Existuje tedy prvočíslo $p|n$, $p \equiv 3 \pmod 4$. Dle předpokladu $p = p_i$ pro některé $i = 1, \ldots, k$, tedy platilo by $n = 4px - 1 \equiv -1 \pmod p$, což je spor s $p|n$. □

Věta 2.25. *Nechť* $a, b \in \mathbb{Z}$, $(a, b) = 1$, *a buď* p *liché prvočíslo. Platí-li* $p|(a^2+b^2)$, *pak* $p \equiv 1 \pmod 4$.

Důkaz: Ukažme nejprve, že $(a, p) = 1$. Kdyby platilo $p|a$, pak vzhledem k předpokladu $p|(a^2+b^2)$ by platilo také $p|b$, což by byl spor s $(a, b) = 1$. Dle Fermatovy věty tedy platí $a^{p-1} \equiv 1 \pmod p$. Dále, $b^2 \equiv -a^2 \pmod p$, odkud plyne

$$(a^{p-2}b)^2 \equiv (a^{p-2})^2 b^2 \equiv (a^{p-2})^2(-a^2) \equiv -(a^{p-1})^2 \equiv -1 \pmod p.$$

To ale znamená, že prvek $\overline{a^{p-2}b}$ je řádu 4 v multiplikativní grupě tělesa $\mathbb{Z}_p$ řádu $p-1$. Platí tedy $4|(p-1)$, neboli $p \equiv 1 \pmod 4$. □

Důsledkem je pak následující tvrzení:

Věta 2.26. *Existuje nekonečně mnoho prvočísel* $p \equiv 1 \pmod 4$.

Důkaz: Předpokládejme sporem, že $p_1, \ldots, p_k$ jsou právě všechna prvočísla $\equiv 1 \pmod 4$. Uvažujme číslo $u = p_1^2 \cdot \ldots \cdot p_k^2 + 4$. Je-li $p|u$ pro prvočíslo p, pak $p|(p_1 \cdot \ldots \cdot p_k)^2 + 2^2$. Dále platí $(p_1 \cdot \ldots \cdot p_k, 2) = 1$, tedy dle věty 2.25 dostaneme $p \equiv 1 \pmod 4$. Kdyby nyní platilo $p = p_i$ pro některé i, pak bychom z $p|u$ dostali $p|4$, což je spor s tím, že p je liché. Existuje tedy prvočíslo $p \equiv 1 \pmod 4$, $p \neq p_i$, spor. □

Podobnými úvahami lze dokázat, že existuje také nekonečně mnoho prvočísel ve tvaru $6k+1$, $8k+5$, $10k+7$ atd. Obecně lze dokázat následující větu.

Věta 2.27. (Dirichletova věta) *Jsou-li* $a, b \in \mathbb{Z}$, $a > 0$, $(a, b) = 1$, *pak existuje nekonečně mnoho prvočísel ve tvaru* $an + b$.

Mnohem překvapivější je následující tvrzení z r. 2008:

Věta 2.28. (Green–Taova věta) *Pro každé přirozené k obsahuje množina prvočísel aritmetickou posloupnost délky k.*

Sílu Green–Taovy věty lze nahlédnout již hledáním posloupností malých délek. Snadno jistě najdeme aritmetickou posloupnost prvočísel délky 5:

$$5, 11, 17, 23, 29.$$

Najít posloupnost délky 10 už je mnohem obtížnější:

$$199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089.$$

Nalézt posloupnost např. délky 100 už je zajisté velká výzva.

Podobně lze dokázat, že obor integrity $\mathbb{Z}(\omega) = \{a + b\omega; a, b \in \mathbb{Z}\}$ je EOI s eukleidovskou funkcí $\delta : \mathbb{Z}(\omega) \setminus \{0\} \to \mathbb{N}$, kde pro $\alpha = a + b\omega = (a - \frac{1}{2}b) + \frac{1}{2}b\mathrm{i}\sqrt{3}$ položíme

$$\delta(\alpha) = \alpha \cdot \overline{\alpha} = a^2 - ab + b^2,$$

přičemž $\overline{\alpha} = (a - \frac{1}{2}b) - \frac{1}{2}b\mathrm{i}\sqrt{3}$ je číslo komplexně sdružené k číslu α. Prvky $\mathbb{Z}(\omega)$ nazýváme *Eisensteinova celá čísla*. Elementárními úvahami lze odvodit, že množina jednotek v $\mathbb{Z}(\omega)$ obsahuje právě prvky $\{\pm 1, \pm\omega, \pm(1 + \omega)\}$.

Hledáme-li ireducibilní prvky v $\mathbb{Z}(\omega)$, dají se z vlastnosti $\alpha | \delta(\alpha)$ podobně jako v $\mathbb{Z}(\mathrm{i})$ dokázat následující věty:

Věta 2.29. *Je-li α ireducibilní prvek v $\mathbb{Z}(\omega)$, pak existuje jediné prvočíslo p tak, že $\alpha | p$.*

Věta 2.30. *Prvočíslo p je buď v $\mathbb{Z}(\omega)$ ireducibilní nebo existují čísla $a, b \in \mathbb{N}$ tak, že $p = a^2 - ab + b^2 = \alpha \cdot \overline{\alpha}$, kde α, $\overline{\alpha}$ jsou ireducibilní prvky v $\mathbb{Z}(\omega)$.*

Stačí se tedy opět zabývat pouze otázkou, která z prvočísel ze $\mathbb{Z}$ jsou prvočísly v $\mathbb{Z}(\omega)$. Odpověď na tuto otázku dává věta:

Věta 2.31. *Prvočíslo p je ireducibilní prvek v $\mathbb{Z}(\omega)$ právě když $p \equiv 2 \pmod 3$. Každé z prvočísel $p \equiv 1 \pmod 3$ lze vyjádřit ve tvaru $p = a^2 - ab + b^2$.*

Důkaz: Provedeme jen nástin důkazu, protože se dělá podobně jako pro okruh $\mathbb{Z}(i)$. Prvočíslo 3 je možno v $\mathbb{Z}(\omega)$ rozložit v součin $3 = -\omega^2(1 - \omega)^2$, kde $1 - \omega$ je ireducibilní prvek v $\mathbb{Z}(\omega)$. Výraz $a^2 - ab + b^2$ dává v modulu 3 pouze zbytky 0, 1 (ověřte!), tedy prvočísla $p \equiv 2 \pmod 3$ jsou nutně ireducibilní v $\mathbb{Z}(\omega)$. Podobnými úvahami se dokáže, že prvočísla $p \equiv 1 \pmod 3$ nejsou ireducibilní. □

Celkem tedy můžeme na základě shora uvedených tvrzení charakterizovat ireducibilní prvky v $\mathbb{Z}(\omega)$:

Věta 2.32. *Ireducibilní prvky v $\mathbb{Z}(\omega)$ jsou až na asociovanost právě*

(i) $1 - \omega$,

(ii) *prvočísla $p \equiv 2 \pmod 3$*,

(iii) *netriviální dělitelé prvočísel $p \equiv 1 \pmod 3$*.

Cvičení

9. Užitím přibližného vzorce $\pi(x) \approx \frac{x}{\ln x}$ určete:
   a) $\pi(10^7)$
   b) $\pi(10^8)$
10. Dokažte, že existuje nekonečně mnoho prvočísel typu $4n + 3$.
11. Dokažte, že existuje nekonečně mnoho prvočísel typu $6n + 5$.
12. Dokažte, že existuje nekonečně mnoho prvočísel typu $6n + 1$.

2.2 Fermatova a Mersenneova prvočísla

Při zkoumání vlastností prvočísel se matematikové zabývali také otázkou, kdy budou prvočísla v předepsaném tvaru nabývat prvočíselných hodnot. Mezi prvními byla studována čísla ve tvarech $a^n \pm 1$ pro $a \in \mathbb{N}$, $a \geq 2$.

Věta 2.33. *Je-li číslo ve tvaru $a^n + 1$ prvočíslem, pak a je sudé a $n = 2^m$ pro $m \in \mathbb{N}$.*

Důkaz: Kdyby a bylo liché, bylo by $a^n + 1$ sudé, a tedy by nebylo prvočíslem. Není-li n mocninou 2, pak zřejmě existuje liché číslo $k \neq 1$ tak, že $k|n$, tj. $n = kl$ pro některá $k, l \in \mathbb{Z}$. Pak ale platí $a^n + 1 = a^{kl} + 1 = (a^l)^k + 1$. Obecně pro liché číslo k platí $a + 1|(a^k + 1)$, tedy také $a^l + 1|(a^n + 1)$ a číslo $a^l + 1$ je netriviálním dělitelem čísla $a^n + 1$. □

Uvažujme tedy na základě předchozí věty čísla ve tvaru $F_n = 2^{2^n} + 1$ a nazývejme je *Fermatova*. Prvočísla ve tvaru F_n budeme nazývat *Fermatova prvočísla*. Fermat vyslovil (nepravdivou) domněnku, že všechna prvočísla ve tvaru F_n jsou prvočísla: L. Euler již v roce 1732 ukázal, že platí $641|F_5 = (2^{2^5} + 1)$. Navíc odvodil, že každý faktor čísla F_n musí být ve tvaru $k \cdot 2^{n+1} + 1$ (později upřesněno Lucasem na tvar $k \cdot 2^{n+2} + 1$).

Prvočíselnost Fermatových čísel se zdá být spíše vyjímečnou vlastností, neboť $F_4 = 65\,537$ je dosud největší známé Fermatovo prvočíslo.

Číslo F_{11} je dosud největší Fermatovo číslo se známým prvočíselným rozkladem (Brent, Morain, 1988).

$F_{2\,747\,497}$ je dosud největší známé složené Fermatovo číslo, jeho prvočíselným faktorem je číslo $57 \cdot 2^{\,747\,499} + 1$ (Bishop, 2013).

Fermatova čísla F_n pro $n \in \{5, \ldots, 32\}$ jsou všechna složená. Přitom pro číslo F_{24}, mající přes 5 milionů cifer, není dosud znám žádný prvočíselný faktor. Uveďme pro zajímavost, že výpočet si vyžádal provedení asi 10^{17} aritmetických operací, a byl to asi jeden z nejrozsáhlejších výpočtů, jehož výsledkem byla jednobitová odpověď ANO-NE.

Dodnes není známo, za Fermatových prvočísel je konečně či nekonečně mnoho.

Fermatova prvočísla byla do až do 1796 brána spíše jako matematická kuriozita. Nabyla na významu zejména v souvislosti s problémem konstruovatelnosti pravidelných n-úhelníků pouze pomocí pravítka a kružítka: Gauss ve svých 17 letech nalezl konstrukci pravidelného 17úhelníka. Na počest tohoto objevu je na podstavci Gaussovy sochy v rodném Braunschweigu zobrazena pravidelná 17cípá hvězda. Ta byla zvolena proto, že pravidelný 17úhelník se podobá již téměř kružnici. Obecně byla otázka konstruovatelnosti řešena až s rozvojem *Galoisovy teorie*:

Věta 2.34. *Pravidelný n-úhelník lze sestrojit pouze pomocí pravítka a kružítka právě když $n \geq 3$ pro $n = 2^m \cdot p_1 \cdot \ldots \cdot p_j$, kde $m \in \mathbb{N}_0$ a pro každé $i = 0, \ldots, j$ jsou čísla $p_1, \ldots, p_j$ Fermatova prvočísla.*

Věta 2.35. *Je-li číslo ve tvaru $a^n - 1$ prvočíslem, pak nutně $a = 2$ a n je prvočíslo.*

Důkaz: Zřejmě $a - 1 | a^n - 1$, tedy nutně $a = 2$. Kdyby $n = kl$ bylo složené, pak $2^n - 1 = (2^k)^l - 1$ je dělitelné číslem $2^k - 1$, což vzhledem ke $k \neq 1$ by znamenalo, že číslo $2^k - 1$ je netriviálním dělitelem. □

Podobně jako v předchozím případě budeme uvažovat čísla ve tvaru $M_n = 2^n - 1$ a nazývat je *Mersenneova čísla*. Prvočísla v tomto tvaru pak budeme nazývat *Mersenneova prvočísla*. Jak snadno nahlédneme, ne všechna Mersenneova čísla M_p pro $p \in \mathbb{P}$ jsou prvočísla: např. číslo $2^{11} - 1$ je dělitelné 23. Věta 2.34 tedy udává pouze nutnou a nikoliv postačující podmínku pro to, aby Mersenneovo číslo bylo prvočíslem. Není opět známo, zda Mersenneových prvočísel je konečně nebo nekonečně mnoho. Více se lze o Mersenneových prvočíslech dočíst v kapitole 9.

Funkce σ a τ

Pro $n \in \mathbb{N}$ označme $\sigma(n)$ součet dělitelů čísla n, a $\tau(n)$ počet dělitelů čísla n.

Věta 2.36. *Je-li $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ kanonický rozklad čísla n, pak*

$$\sigma(n) = \frac{(p_1^{\alpha_1+1} - 1) \cdot \ldots \cdot (p_k^{\alpha_k+1} - 1)}{(p_1 - 1) \cdot \ldots \cdot (p_k - 1)}, \qquad \tau(n) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1).$$

Důkaz: Každý dělitel d čísla n je ve tvaru $d = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$, kde $0 \leq \beta_i \leq \alpha_i$. Pak ovšem

$$\sigma(n) = \sum_{\beta_1, \ldots, \beta_k} p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k} = (1 + p_1 + \ldots + p_1^{\alpha_1}) \cdot \ldots \cdot (1 + p_k + \ldots + p_k^{\alpha_k}) =$$
$$= \frac{(p_1^{\alpha_1+1} - 1) \cdot \ldots \cdot (p_k^{\alpha_k+1} - 1)}{(p_1 - 1) \cdot \ldots \cdot (p_k - 1)}.$$

Číslo β_i lze vybrat právě $\alpha_i + 1$ způsoby, tedy počet dělitelů čísla n je

$$(\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1).$$

□

Cvičení

13. Určete počet dělitelů čísla n:

    a) 378, b) 2 205, c) 5 775, c) 36 000, d) 31 652.

14. Určete počet řešení kongruenčních rovnic:

    a) $59 \equiv 23 \pmod{x}$,

    b) $173 \equiv 47 \pmod{x}$,

    c) $159 \equiv 75 \pmod{2x}$,

    d) $319 \equiv 39 \pmod{3x}$.

15. Určete počet řešení kongruenčních rovnic:

    a) $127 \equiv 87 \pmod{x}$,

    b) $127 \equiv 87 \pmod{2x}$,

    c) $167 \equiv 68 \pmod{5x}$,

16. Dokažte, že $\tau(n)$ je rovno počtu celočíselných bodů hyperboly $xy = n$ v prvním kvadrantu.

17. Najděte nejmenší přirozené číslo s právě 10 děliteli.

Každé číslo $n \in \mathbb{N}$ má alespoň dva různé triviální dělitele, 1 a n, a tedy vždy platí $\sigma(n) \geq n + 1$. Z hlediska hodnot $\sigma(n)$ lze přirozená čísla rozdělit do následujících skupin:

1) *deficitní čísla* – pro ně je $\sigma(n) < 2n$. Takovými jsou např. všechna prvočísla nebo čísla ve tvaru 2^k pro $k \in \mathbb{N}$.

2) *abundantní čísla* (nadbytečná čísla) – pro ně je $\sigma(n) > 2n$. Ukažme, že čísla ve tvaru $n = 2^k \cdot 3$ pro $k > 1$ jsou nadbytečná: dle tvrzení 2.35 dostaneme

$$\sigma(n) = \frac{2^{k+1} - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} = 4(2^{k+1} - 1) = 3 \cdot 2^{k+1} + 2^{k+1} - 4 > 3 \cdot 2^{k+1} = 2n.$$

   Nejmenší liché abundantní číslo je 945, obecněji každé číslo ve tvaru $945k$ pro k nedělitelné $3, 5, 7$ je liché abundantní (dokažte!).

3) *čísla dokonalá* (čísla perfektní) – pro ně je $\sigma(n) = 2n$, tj. n je rovno součtu všech dělitelů čísla n různých od n.

Z předchozích úvah plyne, že existuje nekonečně mnoho sudých i lichých abundantních i deficitních čísel. Označíme-li $h(A)$ hustotu abundantních čísel, v roce 1998 byl odvozen vztah (M. Deléglise)

$$0,2474 < h(A) < 0,2480,$$

tedy většina přirozených čísel je deficitních. Uveďme ještě pro zajímvost, že každý vlastní násobek dokonalého čísla a každý násobek abundantního čísla je číslo opět abundantní, každé číslo větší než 20 161 je součtem dvou abundantních čísel.

Dokonalá čísla byla zkoumána už Pythagorejci, dnes je známo 48 dokonalých čísel (leden 2013), z nichž všechna jsou sudá. Není dosud známo ani jedno liché dokonalé číslo. Dosud největším známým dokonalým číslem je $2^{57\,885\,161}(2^{57\,885\,161}-1)$ (leden 2013). Při hledání všech sudých dokonalých čísel se ukázala jejich souvislost s Mersenneovými prvočísly:

Věta 2.37. (Eulerova) *Sudé číslo n je dokonalé, právě když je ve tvaru*

$$n = D_s = 2^{s-1}(2^s - 1),$$

kde $M_s = 2^s - 1$ je Mersenneovo prvočíslo.

Důkaz: Je-li M_s prvočíslo, pak $2^{s-1}(2^s - 1)$ je prvočíselný rozklad čísla n. Pak podle věty 2.35 dostaneme

$$\sigma(n) = \frac{2^s - 1}{2 - 1} \cdot \frac{M_s^2 - 1}{M_s - 1} = (2^s - 1)(M_s + 1) = 2^s(2^s - 1) = 2n,$$

tedy číslo n je dokonalé. Obráceně, nechť n je dokonalé číslo. Uvědomme si nejprve, že číslo ve tvaru $n = 2^\alpha$ nemůže být dokonalé pro žádné $\alpha \in \mathbb{N}$, platí totiž:

$$\sigma(n) = \frac{2^{\alpha+1} - 1}{2 - 1} = 2^{\alpha+1} - 1 \neq 2^{\alpha+1} = 2n.$$

V prvočíselném rozkladu čísla n musí nutně tedy být alespoň jedno liché prvočíslo. Pak $n = 2^\alpha \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, kde $p_1, \ldots, p_k$ jsou různá lichá prvočísla. Položme $l = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ (zřejmě $l > 1$ a l je liché) a $s = \alpha + 1$. Dle 2.35 je

$$\sigma(n) = \frac{2^{\alpha+1} - 1}{2 - 1} \cdot \underbrace{\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}}_{\sigma(l)} = (2^s - 1)\sigma(l) = 2^s l. \qquad (1)$$

Z poslední rovnosti plyne, že $2^s | (2^s - 1)\sigma(l)$, ovšem $(2^s, 2^s - 1) = 1$, tedy $2^s | \sigma(l)$, tj. $\sigma(l) = 2^s q$ pro nějaké $q \in \mathbb{N}$. Dosazením této rovnosti do (1) dostaneme $(2^s - 1) \cdot q = l$, neboli $2^s \cdot q = l + q$. Kdyby $l = q$, pak by platilo $2^s \cdot q = 2l$. Ale l je liché a $s \geq 2$, což není možné. Je tedy $l \neq q$. Ze vztahu $\sigma(l) = 2^s q = l + q$ plyne, že jedinými děliteli čísla l jsou čísla l a q. Tedy l má právě dva různé dělitele, tudíž l je prvočíslo a $q = 1$. Konečně máme $l = 2^s - 1$, $n = 2^{s-1}(2^s - 1)$, kde l je Mersenneovo prvočíslo. □

Pro lichá dokonalá čísla je známa pouze následující nutná podmínka:

Věta 2.38. *Je-li n liché dokonalé číslo, pak*

$$n = p^{4k+1} \cdot N^2,$$

kde $k \geq 0$, p je prvočíslo ve tvaru $4s + 1$ a $(N, p) = 1$.

Bylo také dokázáno, že pokud existuje nějaké liché dokonalé číslo, musí být nutně větší než 10^{300} (v současné době se výzkum zabývá důkazem pro hodnotu 10^{500}). Navíc by takové číslo muselo mít nejméně 75 dělitelů, alespoň 9 různých prvočíselných dělitelů a největší prvočíselný dělitel by musel být větší než 10^8 (2006).

S dokonalými čísly úzce souvisí dvojice tzv. *spřátelených čísel*. Dvojici čísel $a, b \in \mathbb{N}$ nazveme *spřátelená*, je-li součet pravých dělitelů čísla a roven b a naopak, tj. platí

$$\sigma(a) - a = b, \qquad \sigma(b) - b = a,$$

neboli

$$\sigma(a) = \sigma(b) = a + b.$$

První spřátelená čísla byla nalezena už Pythagorem – dvojice 220 a 284, dnes jich známe více než 12 000 000. Přitom není známa ani jedna dvojice nesoudělných spřátelených čísel. Bylo dokázáno, taková dvojice by musela mít součin větší než 10^{67}.

První obecný vzorec pro generování spřátelených čísel byl vytvořen r. 830 arabským astronomem a matematikem Thabitem:

Věta 2.39. (Thabitův vzorec) *Jsou-li* $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$, $r = 9 \cdot 2^{2n-1} - 1$ *pro* $n > 1$ *prvočísla, pak čísla* $2^n pq$ *a* $2^n r$ *jsou spřátelená.*

Důkaz: Proveďte sami pomocí tvrzení 2.4. □

Pro $n = 2$ dostaneme z předešlé věty právě dvojici spřátelených čísel 220, 284, obdrženou Pythagorem.

Zabývejme se nyní stejně jako u prvočísel otázkou hustoty dokonalých a spřátelených čísel v množině $\mathbb{N}$ (viz. def. na str. 21). Uveďme nejprve některé základní vlastnosti hustoty:

Věta 2.40.

(i) *Každá konečná podmnožina v* $\mathbb{N}$ *je řídká,*

(ii) $h(L) = h(S) = \frac{1}{2}$, *kde L, resp. S jsou lichá, resp. sudá čísla,*

(iii) *Množina* $Q_k = \{n^k; n \in \mathbb{N}\}$ *všech k-tých mocnin prvků z* $\mathbb{N}$ *je pro* $k > 1$ *řídká,*

(iv) *Jsou-li* $A, B \subseteq \mathbb{N}$, $A \subseteq B$, *a existují-li hustoty* $h(A), h(B)$, *pak* $h(A) \leq h(B)$; *speciálně, podmnožina řídké množiny je opět řídká,*

(v) *Je-li* $h(A) = h(B) = 0$ *pro* $A, B \subseteq \mathbb{N}$, *pak* $h(A \cup B) = 0$,

(vi) *Je-li* $a \geq 0$, $d > 0$ *a* $A = \{a + kd; k \in \mathbb{N}\}$, *pak* $h(A) = \frac{1}{d}$.

Důkaz: (i) Je-li $|A| = k \in \mathbb{N}$, pak $A(n) \leq k$ pro každé $n \in \mathbb{N}$. Odtud dostaneme $0 \leq \frac{A(n)}{n} \leq \frac{k}{n}$, což vzhledem k $\lim_{n\to\infty} \frac{k}{n} = 0$ dává $h(A) = \lim_{n\to\infty} \frac{A(n)}{n} = 0$.

(ii) Zřejmě $S(2n) = n - 1$ a $S(2n + 1) = n$.

Pro limity platí $\lim_{n\to\infty} \frac{S(2n)}{2n} = \lim_{n\to\infty} \frac{S(2n+1)}{2n+1} = \frac{1}{2}$, existuje tedy

$$h(S) = \lim_{n\to\infty} \frac{S(n)}{n} = \frac{1}{2}.$$

Podobně se důkaz provede pro lichá čísla.

(iii) Nechť s je největší přirozené číslo s vlastností $s^k \leq n$, tj. $s \leq \sqrt[k]{n}$. Zřejmě $s = Q_k(n)$, a tedy $0 \leq \frac{Q_k(n)}{n} \leq \frac{\sqrt[k]{n}}{n}$. Přitom

$$\lim_{n\to\infty} \frac{Q_k(n)}{n} \leq \lim_{n\to\infty} \frac{\sqrt[k]{n}}{n} \leq \lim_{n\to\infty} \frac{\sqrt{n}}{n} = 0,$$

odkud $h(Q_k) = 0$.

(iv) Je-li $A \subseteq B$, pak $A(n) \leq B(n)$, a tedy

$$h(A) = \lim_{n\to\infty} \frac{A(n)}{n} \leq \lim_{n\to\infty} \frac{B(n)}{n} = h(B).$$

(v) Platí $(A \cup B)(n) \leq A(n) + B(n)$, odkud

$$h(A \cup B) = \lim_{n\to\infty} \frac{(A \cup B)(n)}{n} \leq \lim_{n\to\infty} \frac{A(n)}{n} + \lim_{n\to\infty} \frac{B(n)}{n} = 0 + 0 = 0.$$

(vi) Buď s největší přirozené číslo vlastnosti $a + sd \leq n$. Pak $n < a + (s+1)d$ a $A(n) = s$. Odtud dostaneme

$$A(n) = s \leq \frac{n-a}{d}, \frac{A(n)}{n} \leq \frac{n-a}{nd},$$

podobně $\frac{n-a}{d} - 1 < s = A(n)$, tj. $\frac{A(n)}{n} > \frac{n-a}{nd} - \frac{1}{n}$. Konečně tedy

$$\frac{1}{d} = \lim_{n\to\infty} \left(\frac{n-a}{nd} - \frac{1}{n} \right) \leq \lim_{n\to\infty} \frac{A(n)}{n} = h(A) \leq \lim_{n\to\infty} \frac{n-a}{nd} = \frac{1}{d},$$

odkud $h(A) = \frac{1}{d}$. □

Věta 2.41. *Množina všech dokonalých čísel je řídká.*

Důkaz: Označme D množinu všech dokonalých čísel, D_s, resp. D_l, nechť je množina všech sudých, resp. lichých dokonalých čísel. Zřejmě platí $D = D_s \cup D_l$.

1) Dokažme, že D_l je řídká množina. Dle věty 2.37 platí

$$D_l \subseteq \{p^{4k+1}N^2; p \text{ je prvočíslo}, (p, N) = 1, p \equiv 1 \pmod 4\}.$$

Uvažujme libovolné $N \in \mathbb{N}$ a ukažme, že k němu existuje nejvýše jedno prvočíslo p a nejvýše jeden exponent $\alpha \in \mathbb{N}$ tak, že $(p, N) = 1$ a $p^\alpha N^2$ je dokonalé.

Předpokládejme, že existují dvě prvočísla $p, q, (p, N) = 1 = (q, N)$, a exponenty $\alpha, \beta \in \mathbb{N}$, pro něž jsou $p^\alpha N^2$ a $q^\beta N^2$ dokonalá. Pak platí

$$\sigma(p^\alpha N^2) = \frac{p^{\alpha+1}-1}{p-1}\sigma(N^2) = 2p^\alpha N^2,$$
$$\sigma(q^\beta N^2) = \frac{q^{\beta+1}-1}{q-1}\sigma(N^2) = 2q^\beta N^2.$$

Vydělením levých a pravých stran předchozích rovností a užitím vztahu $\frac{p^{\alpha+1}-1}{p-1} = = p^\alpha + p^{\alpha-1} + \ldots + 1$ dále dostaneme

$$\frac{p^\alpha + p^{\alpha-1} + \ldots + 1}{q^\beta + q^{\beta-1} + \ldots + 1} = \frac{p^\alpha}{q^\beta}.$$

Z poslední rovnosti odstraněním zlomku snadno vidíme, že $p|q^\beta(p^\alpha+p^{\alpha-1}+\ldots+1)$, což vzhledem k nesoudělnosti p a $p^\alpha + p^{\alpha-1} + \ldots + 1$ dává $p|q$. To ale znamená, že $p = q$. Pak ale platí $p^\alpha + p^{\alpha-1} + \ldots + 1 = p^\beta + p^{\beta-1} + \ldots + 1$, a tedy $\alpha = \beta$.

Celkem jsme dokázali, že lichých dokonalých čísel není více než kvadrátů přirozených čísel. Vzhledem k tomu, že kvadráty tvoří dle Věty 2.39(iii) řídkou množinu v $\mathbb{N}$, je nutně dle 2.39(iv) D_l jakožto její podmnožina také řídká.

2) Ukažme, že D_s je řídká množina. Dle tvrzení 2.36 platí

$$D_s \subseteq \{2^{s-1}(2^s - 1); s \in \mathbb{N}\}.$$

Buď t největší přirozené číslo takové, že $2^{t-1}(2^t - 1) \leq n$, tj. pak $D_s(n) \leq t$. Vyřešením této nerovnosti (užijte substituce $y = 2^{t-1}$) dostaneme

$$t \leq 1 + \frac{\ln\left(\frac{1}{4}(1 + \sqrt{1+8n})\right)}{\ln 2}.$$

To ovšem znamená, že

$$\frac{D_s(n)}{n} \leq \frac{t}{n} \leq \frac{\ln\left(\frac{1}{4}(1 + \sqrt{1+8n})\right)}{n \ln 2} + \frac{1}{n} \to 0$$

pro $n \to \infty$, tedy D_s je řídká množina. □

Bez důkazu alespoň uveďme, že množina všech spřátelených čísel je také řídká. O obtížnosti důkazu svědčí fakt, že uvedené tvrzení bylo dokázáno až v r. 1955 maďarským matematikem Paulem Erdösem.

V analytické teorii čísel byl zkoumán následující problém: je dobře známo, že řada $\sum_{n=1}^{\infty} \frac{1}{n}$ diverguje (jde o tzv. harmonickou řadu). Je tedy přirozené ptát se, zda řada $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverguje či konverguje.

Věta 2.42. *Řada $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverguje.*

Důkaz: Označme pro $x \in \mathbb{N}$ symbolem $N_j(x)$ počet přirozených čísel menších nebo rovných x, která nejsou dělitelná žádným z prvočísel počínaje p_{j+1}, tj. dělitelnými pouze některými z prvočísel $p_1, \ldots, p_j$. V důkazu věty 2.8 bylo ukázáno, že platí $N_j(x) \leq 2^j\sqrt{x}$. Předpokládejme nyní, že uvažovaná řada konverguje. Pak k číslu $\frac{1}{2}$ existuje index j tak, že

$$\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \ldots < \frac{1}{2}.$$

Počet čísel menších nebo rovných x dělitelných prvočíslem p je nejvýše roven $\frac{x}{p}$, tedy počet čísel $\leq x$ dělitelných některým z prvočísel $p_{j+1}, \ldots$, je nejvýše

$$\frac{x}{p_{j+1}} + \frac{x}{p_{j+2}} + \ldots < \frac{1}{2}x.$$

Odtud ale plyne, že počet čísel $\leq x$ nedělitelných žádným z prvočísel $p_{j+1}, \ldots$, je alespoň $x - \frac{1}{2}x = \frac{1}{2}x$, tedy

$$\frac{1}{2}x < N_j(x) \leq 2^j\sqrt{x},$$

odkud $x < 2^{2j+2}$. Zvolíme-li tedy dostatečně velké x, dostaneme spor. □

Podobný analytický problém lze zkoumat pro tzv. prvočíselná dvojčata. To jsou takové dvojice prvočísel, lišící se o hodnotu 2. Takovými jsou např. dvojice $(2,3)$, $(3,5)$, $(5,7)$, $(17,19)$ atd. Z předešlé věty víme, že součet převrácených hodnot všech prvočísel roste nade všechny meze. Evidentně ne ke každému prvočíslu existuje prvočíselné dvojče, má tedy smysl otázka, jak to bude se součtem převrácených hodnot všech prvočíselných dvojčat. V roce 1919 bylo dokázáno následující tvrzení:

Věta 2.43. (Brunova věta) *Řada*

$$\sum_q \frac{1}{q} = \left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \ldots,$$

kde sčítáme přes všechny dvojice prvočíselných dvojčat vyjma první $(2,3)$*, konverguje k hodnotě* B*, nazývané Brunova konstanta.*

Přibližná hodnota Brunovy konstanty B=1,90216054... byla vyčíslena v roce 1976 R. Brentem. Předchozí výsledek znamená, že prvočíselná dvojčata se v posloupnosti prvočísel vyskytují velmi řídce, nicméně dlouho otevřeným problémem je otázka, zda je jich konečně nebo nekonečně mnoho.

Cvičení

18. Dokažte, že pro prvočíslo p z podmínek $p|(a+b)$ a $p|ab$ vyplývá, že $p|a$ a $p|b$.
19. Dokažte, že pro prvočíslo p z podmínek $p|a$ a $p|(a^2+b^2)$ vyplývá, že $p|b$.
20. Dokažte, že pro prvočíslo p z podmínek $(a, bp) = d$ a $(a, b) = 1$ vyplývá, že $d = 1$ nebo $d = p$.
21. Dokažte, že jestliže $(a, b) = 1$, pak $(a + b, ab) = 1$ a $(a - b, ab) = 1$.
22. Dokažte, že $(a + b, abp)$ je rovno 1 nebo p, platí-li, že $(a, b) = 1$ a p je prvočíslo.
23. Dokažte, že jestliže $(a, b) = 1$, pak $(a + b, a^2 - ab + b^2) = 1$.
24. Dokažte, že $(a, b) = (a + b, [a, b])$.
25. Dokažte, že druhou mocninu libovolného prvočísla většího než 3 lze vyjádřit jako $12k+1$.
26. Najděte všechna prvočísla p taková, aby čísla $p + 10$ a $p + 20$ byla také prvočísla.
27. Dokažte, že pro $n > 2$ nemohou být čísla $2^n - 1$ a $2^n + 1$ zároveň prvočísla.
28. Čísla p a $8p^2 + 1$ jsou prvočísla. Dokažte, že $8p^2 + 2p + 1$ je také prvočíslo.
29. Dokažte, že kladné celé číslo a, které lze vyjádřit jako $3k + 2$, má prvočíselného dělitele, který lze vyjádřit stejným výrazem.

Kapitola 3

Kongruenční rovnice

3.1 Základní pojmy

Každou rovnici ve tvaru

$$f(x) \equiv 0 \pmod{m} \tag{1}$$

s neznámou $x \in \mathbb{Z}$, kde $m \in \mathbb{N}$, $m > 1$, $f(x) = a_n x^n + \ldots + a_1 x + a_0$ je polynom ze $\mathbb{Z}[x]$ a $a_n \not\equiv 0 \pmod{m}$, nazýváme *kongruenční rovnice stupně n s neznámou x.*

Poznámka. Je-li $x \in \mathbb{Z}$ řešením rovnice $f(x) \equiv 0 \pmod{m}$ a $x \equiv y \pmod{m}$, pak vzhledem k vlastnostem kongruencí je y také řešením této rovnice. Proto *řešením* uvažované rovnice rozumíme celou třídu $\overline{x} \in \mathbb{Z}_m$. Rovnici (1) je tedy možno chápat jakožto algebraickou rovnici nad $\mathbb{Z}_m$ ve tvaru

$$f(\overline{x}) = \overline{a}_n \overline{x}^n + \ldots + \overline{a}_1 \overline{x} + \overline{a}_0 = \overline{0} \tag{2}$$

pro $\overline{a}_n \neq \overline{0}$. Nebudeme tedy rozlišovat mezi tvary rovnice (1) a (2) a budeme používat vždy ten tvar, který se nám v dané situaci bude lépe hodit.

Odtud také okamžitě plyne, že rovnice (1) *nemůže* mít více než m řešení (počet prvků $\mathbb{Z}_m$ je totiž právě m).

Příklad. Řešte kongruenční rovnice
a) $2x^3 + 3x - 5 \equiv 0 \pmod{7}$,
b) $x^2 + x - 2 \equiv 0 \pmod{5}$.

Řešení:

a) Hledáme všechny třídy ze $\mathbb{Z}_7$ vyhovující této rovnici. Pro zjednodušení budeme uvažovat úplný systém zbytků $\mathbb{Z}_7$ majících nejmenší absolutní hodnotu, tj. $\mathbb{Z}_7 = \{\overline{0}, \pm\overline{1}, \pm\overline{2}, \pm\overline{3}\}$. Snadno se ověří, že vyhovuje pouze $x = \overline{1}$, tj. rovnice má jediné řešení.

b) Podobně uvažujeme úplný systém zbytků $\mathbb{Z}_5 = \{\overline{0}, \pm\overline{1}, \pm\overline{2}\}$. Rovnici vyhovují prvky $x = \overline{1}, x = -\overline{2}$. Platí tedy $x^2 + x - \overline{2} = (x - \overline{1}) \cdot (x + \overline{2})$.

Může se stát, že kongruenční rovnici (1) vyhovují všechny zbytkové třídy ze $\mathbb{Z}_m$. Takové rovnice nazýváme *identické*. Příkladem takových rovnic jsou např. rovnice

$$x^p - x \equiv 0 \pmod{p}$$

(v důsledku malé Fermatovy věty) nebo rovnice (1), v níž jsou všechny koeficienty a_i násobky čísla m.

Poznámka. Při úpravách kongruenčních rovnic je třeba dát pozor na skutečnost, že při násobení obou stran rovnice číslem soudělným s modulem m nemusíme dostat ekvivalentní rovnice, např. $x^3 - x + 1 \equiv 0 \pmod 3$ a $3x^3 - 3x + 3 \equiv 0 \pmod 3$ nejsou ekvivalentní, neboť první nemá žádné řešení a druhá je identická.

3.2 Kongruenční rovnice 1. stupně, řetězové zlomky

Obecný tvar kongruenčních rovnic 1. stupně je

$$ax \equiv b \pmod{m},$$

kde $a \not\equiv 0 \pmod m$. Ve tvaru (2) má lineární rovnice tvar

$$\overline{a} \cdot \overline{x} = \overline{b} \tag{3}$$

v $\mathbb{Z}_m$ pro $\overline{a} \neq \overline{0}$.

1. Předpokládejme nejprve, že $(a, m) = 1$.

V tom případě víme, že prvek $\overline{a}$ je invertibilní v $\mathbb{Z}_m$. Vynásobíme-li obě strany rovnice prvkem $\overline{a}^{-1}$, dostaneme $\overline{x} = \overline{b}\overline{a}^{-1}$, tedy rovnice (3) má *jediné řešení.*

Příklad. Řešme rovnici $5x \equiv 7 \pmod 8$.
Řešení: Vidíme, že $(5, 8) = 1$. Z tabulky pro násobení v $\mathbb{Z}_m$ zjistíme, že $\overline{5}^{-1} = \overline{5}$, odkud $\overline{x} = \overline{57} = \overline{3}$, neboli $x \equiv 3 \pmod 8$.

2. Nechť nyní $(a, m) = d > 1$. Mohou nastat dvě možnosti:

a) $d \nmid b$ – v tomto případě rovnice *nemá* řešení, neboť obě strany rovnice musí mít s modulem stejné společné dělitele.

Příklad. Rovnice $6x \equiv 7 \pmod{15}$ není řešitelná, neboť $3 = (6, 15) \nmid 7$.

b) $d|b$ – v tomto případě $d|ax$, $d|b$, $d|m$, platí tedy

$$\frac{a}{d}\, x \equiv \frac{b}{d} \pmod{\frac{m}{d}}, \quad \text{kde } \left(\frac{a}{d}, \frac{m}{d}\right) = 1. \tag{4}$$

Jak vidíme, vydělením obou stran rovnice a modulu číslem d převede případ b) na případ a), ovšem už v modulu $\frac{m}{d}$. Rovnice (4) má tedy v $\mathbb{Z}_{\frac{m}{d}}$ jediné řešení $x \equiv x_1 \pmod{\frac{m}{d}}$, tedy $x = x_1 + \frac{m}{d}t$, $t \in \mathbb{Z}$. Probíhá-li t úplný systém zbytků modulu d, tj. $t \in \{0, \dots, d-1\}$, dostaneme právě všechna navzájem různá řešení rovnice (1) v $\mathbb{Z}_m$, tj. rovnice (1) má *právě d řešení*, a to

$$\overline{x}_t \in \left\{ \overline{x}_1 + \overline{\left(\frac{m}{d}\right)}\overline{t};\ t \in \{0, \dots, d-1\} \right\}.$$

Příklad. Řešme rovnici $15x \equiv 35 \pmod{55}$.
Řešení: Platí $d = (15, 55) = 5|35$. Rovnici převedeme na tvar (4)

$$3x \equiv 7 \pmod{11}.$$

V $\mathbb{Z}_{11}$ je $\overline{3}^{-1} = \overline{4}$, tedy $x \equiv 4 \cdot 7 \equiv 6 \pmod{11}$.

Čísla t volíme z množiny $\{0, 1, 2, 3, 4\}$, odkud

$$\overline{x} \in \left\{ \overline{6} + \overline{11} \cdot \overline{t};\ t \in \{0, 1, 2, 3, 4\} \right\} = \left\{ \overline{6}, \overline{17}, \overline{28}, \overline{39}, \overline{50} \right\} \text{ v } \mathbb{Z}_{55}.$$

Shrneme-li shora uvedené případy, platí:

1) je-li $(a, m) = 1$, pak má rovnice (3) jediné řešení,

2) je-li $(a, m) = d > 1$, pak
   a) pro $d \nmid b$ rovnice (3) není řešitelná,
   b) pro $d|b$ má rovnice (3) právě d řešení.

Řešení kongruenčních rovnic 1. stupně metodou úpravy koeficientů

Někdy bývá výhodné rovnice ve tvaru (3) upravit tak, abychom na pravé straně rovnice dostali násobek čísla a. V tom případě je možno buď celou kongruenční rovnici (i s modulem) nebo pouze obě strany kongruence krátit číslem a. Musíme ovšem dávat pozor na to, zda dostáváme rovnici ekvivalentní s původní či ne.

Příklad. Řešme kongruenční rovnici $5x \equiv 7 \pmod{8}$.
Řešení: Tato rovnice je ekvivalentní rovnici $5x \equiv 7 + 8 \equiv 15 \pmod{8}$, $(5, 8) = 1$, tedy $x \equiv 3 \pmod{8}$.

Příklad. Řešme kongruenční rovnici $7x \equiv 6 \pmod{15}$.
Řešení: V rovnici je $(6, 15) = 3$, tedy nutně $3|7x$. To ale vzhledem k $(3, 7) = 1$ znamená, že $3|x$. Zvolíme tedy substituci $x = 3y$ a dosaďme do původní rovnice: $7 \cdot 3y \equiv 6 \pmod{15}$, tedy $7y \equiv 2 \pmod{5}$, $2y \equiv 2 \pmod{5}$, $(2, 5) = 1$, tedy $y \equiv 1 \pmod{5}$, $x = 3y \equiv 3 \pmod{15}$ (uvedené úpravy jsou ekvivalentní, neboť $(3, 5) = (2, 5) = 1$).

Řešení kongruenčních rovnic 1. stupně pomocí Eulerovy věty

Užitečnou, i když ne vždy efektivní metodou řešení kongruenčních rovnic prvního stupně je metoda užití Eulerovy věty. Ta nám říká, že pro $(a, m) = 1$ platí $a^{\phi(m)} \equiv 1 \pmod{m}$, kde ϕ je Eulerova funkce. V řeči zbytkových tříd lze Eulerovu větu přepsat do tvaru $\overline{a^{\phi(m)}} = \overline{1}$ v $\mathbb{Z}_m$. Lze ji také interpretovat tak, že k prvku $\overline{a}$ existuje v okruhu $\mathbb{Z}_m$ prvek inverzní, přičemž

$$\overline{a}^{-1} = \overline{a^{\phi(m)-1}}.$$

Vynásobíme-li obě strany kongruence prvkem b, dostaneme

$$a^{\phi(m)}b \equiv b \pmod{m},$$

odkud srovnáním s rovnicí (3) máme

$$x \equiv a^{\phi(m)-1}b \pmod{m}.$$

Příklad. Řešme rovnici $3x \equiv 7 \pmod{11}$.
Řešení: Pro danou rovnici postupně dostáváme

$$x \equiv 3^{\phi(11)-1} \cdot 7 = 3^9 \cdot 7,$$

$$x \equiv 3^9 \cdot 7 \equiv (3^2)^4 \cdot 3 \cdot 7 \equiv 16 \cdot 3 \cdot 7 \equiv 6 \pmod{11}.$$

Příklad. Řešme rovnici $17x \equiv 25 \pmod{28}$.
Řešení: Pro danou rovnici máme

$$x \equiv 17^{\phi(28)-1} \cdot 25 \pmod{28},$$

kde $\phi(28) = \phi(4) \cdot \phi(7) = 2 \cdot 6 = 12$, tedy $x \equiv 17^{11} \cdot 25 \pmod{28}$. Dále, $17 \equiv -11$, $17^2 \equiv 121 \equiv 9$, $17^4 \equiv 9^2 = 81 \equiv -3$, $17^8 \equiv 9$, $17^{10} \equiv 9 \cdot 9 \equiv -3$, $17^{11} \equiv \equiv (-11)(-3) \equiv 5$. Celkem tedy $x \equiv 5 \cdot 25 \equiv 13 \pmod{28}$.

Poznámka. Uvedené příklady ukazují, že pro velké moduly funkce ϕ nabývá velkých hodnot a bývá často obtížné určit, do které zbytkové třídy v tomto modulu padne číslo $a^{\phi(m)-1}b$. Ani jedna ze shora uvedených metod tedy není pro velké moduly efektivní. V tomto případě je výhodné užít např. metody řetězových zlomků.

Cvičení

30. Řešte metodou dosazovací kongruenční rovnice:

a) $3x \equiv 1 \pmod{7}$,
b) $5x \equiv -2 \pmod{11}$,
c) $4x \equiv 7 \pmod{17}$,
d) $7x \equiv 5 \pmod{8}$,
e) $15x \equiv 25 \pmod{35}$,
f) $15x \equiv 11 \pmod{36}$,
g) $11x \equiv 15 \pmod{36}$,
h) $13x \equiv 1 \pmod{15}$,
i) $21x \equiv 4 \pmod{35}$,
j) $4x \equiv 21 \pmod{35}$.

31. Řešte metodou úpravy koeficientů kongruence:

a) $27x \equiv 14 \pmod{25}$,
b) $13x \equiv 10 \pmod{11}$,
c) $5x \equiv 3 \pmod{11}$,
d) $7x \equiv 5 \pmod{24}$,
e) $16x \equiv 19 \pmod{31}$,
f) $19x \equiv 12 \pmod{35}$.

32. Řešte kongruence užitím Eulerovy věty:
a) $7x \equiv 5 \pmod{17}$, b) $13x \equiv 3 \pmod{19}$, c) $27x \equiv 7 \pmod{58}$.

Řetězové zlomky

1. Celá a zbytková část racionálního čísla

Jelikož $\mathbb{Z}$ je eukleidovský obor integrity s eukleidovskou funkcí rovnou absolutní hodnotě, existují pro každé $a \in \mathbb{Z}$, $m \in \mathbb{N}$ jednoznačně určené prvky $q, r \in \mathbb{Z}$ tak, že platí $a = mq + r$, $0 \leq r < m$. Tuto rovnost lze přepsat ve tvaru

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

Příklad. $\frac{147}{17} = 8 + \frac{11}{17}$, $-\frac{79}{17} = -5 + \frac{6}{17}$

Zřejmě $q \leq \frac{a}{m} < q+1$, je tedy q *největší* celé číslo, které není větší než $\frac{a}{m}$. Číslo q nazýváme *celá část čísla* $\frac{a}{m}$ a značí se $q = \left[\frac{a}{m}\right]$. Rozdíl $\frac{r}{m} = \frac{a}{m} - q$ nazýváme *zbytková část čísla* $\frac{a}{m}$ a značíme $\frac{r}{m} = \left\{\frac{a}{m}\right\}$. Platí tedy

$$\frac{a}{m} = \left[\frac{a}{m}\right] + \left\{\frac{a}{m}\right\}.$$

2. Rozklad racionálního čísla do řetězového zlomku

Uvažujme libovolné racionální číslo $\frac{a}{b}$, $b > 0$. Aplikací Eukleidova algoritmu pro prvky a, b dostaneme

$$\begin{array}{rcll} a &=& bq_1 + r_2, & 0 < r_2 < b \\ b &=& r_2q_2 + r_3, & 0 < r_3 < r_2 \\ \vdots & & \vdots & \vdots \\ r_{n-2} &=& r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &=& r_nq_n. & \end{array}$$

Přepisem těchto rovností dostaneme

$$\begin{array}{lll} \frac{a}{b} &= q_1 + \frac{r_2}{b} &= q_1 + \frac{1}{\frac{b}{r_2}}, \\ \frac{b}{r_2} &= q_2 + \frac{r_3}{r_2} &= q_2 + \frac{1}{\frac{r_2}{r_3}}, \\ \vdots & \vdots & \vdots \\ \frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{r_n}{r_{n-1}} &= q_n + \frac{1}{\frac{r_{n-1}}{r_n}}, \\ \frac{r_{n-1}}{r_n} &= q_n. & \end{array}$$

Postupným dosazováním levých stran rovnic do rovnic předcházejících dostaneme

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}. \tag{1}$$

Takové vyjádření čísla $\frac{a}{b}$ se nazývá *řetězový zlomek* příslušný číslu $\frac{a}{b}$. Vidíme, že v řetězovém zlomku se vyskytují pouze celé části čísel $q_1, \ldots, q_n$ Eukleidova algoritmu pro zlomek $\frac{a}{b}$, přičemž $q_1 \in \mathbb{Z}$, $q_2, \ldots, q_n \in \mathbb{N}$. Konečnost množiny čísel $q_1, \ldots, q_n$ je zaručena konečností algoritmu postupného dělení. Je tedy vhodnější řetězový zlomek (1) přepsat do přehlednějšího tvaru

$$\frac{a}{b} = (q_1, \ldots, q_n).$$

Zřejmě platí

$$(q_1, \ldots, q_n) = q_1 + \frac{1}{(q_2, \ldots, q_n)}.$$

Čísla $q_1, \ldots, q_n$ nazýváme *prvky řetězového zlomku* $(q_1, \ldots, q_n)$.

Příklad.

$$\frac{95}{42} = 2 + \frac{11}{42} = 2 + \frac{1}{\frac{42}{11}} \qquad \frac{42}{11} = 3 + \frac{9}{11} = 3 + \frac{1}{\frac{11}{9}}$$

$$\frac{11}{9} = 1 + \frac{2}{9} = 1 + \frac{1}{\frac{9}{2}} \qquad \frac{9}{2} = 4 + \frac{1}{2} = 4 + \frac{1}{\frac{2}{1}}$$

Tedy

$$\frac{95}{42} = 2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{2}}}} = (2, 3, 1, 4, 2).$$

Zabývejme se nyní otázkou jednoznačnosti řetězového zlomku pro dané racionální číslo. Povšimneme si nejprve, že je-li $q_n > 1$ v řetězovém zlomku $(q_1, \ldots, q_n)$, pak vzhledem k rovnosti

$$q_n = q_n - 1 + \frac{1}{1}$$

platí $(q_1, \ldots, q_n) = (q_1, \ldots, q_n - 1, 1)$, a tedy připustíme-li na posledním místě řetězového zlomku číslo 1, vyjádření nebude jednoznačné.

Ukážeme, že za podmínky $q_n > 1$ existuje *jediný* řetězový zlomek $(q_1, \ldots, q_n)$ reprezentující číslo $\frac{a}{b}$:

1) je-li $n = 1$, pak $[(q_1)] = [q_1] = q_1$;

2) je-li $n = 2$, pak $(q_1, q_2) = q_1 + \frac{1}{q_2}$, $q_2 > 1$, a tedy $[(q_1, q_2)] = q_1$;

3) je-li $n > 2$, pak

$$(q_1, \ldots, q_n) = q_1 + \frac{1}{(q_2, \ldots, q_n)};$$

v posloupnosti $(q_2, \ldots, q_n)$ jsou alespoň dva prvky, což vzhledem k $q_2 \in \mathbb{N}$ znamená, že $(q_2, \ldots, q_n) > 1$, a tedy $[(q_1, \ldots, q_n)] = q_1$.

Nechť nyní $(q_1, \ldots, q_n)$ a $(p_1, \ldots, p_m)$; $q_n, p_m > 1$, jsou dva řetězové zlomky reprezentující totéž číslo $\frac{a}{b}$. Dokázali jsme, že $[\frac{a}{b}] = q_1 = p_1$. Platí tedy nutně $(q_2, \ldots, q_n) = (p_2, \ldots, p_m)$. Celé části těchto čísel jsou opět stejné, tj. $q_2 = p_2$. Tak postupujeme dále a kdyby $m \neq n$, např. $m > n$ pak by bylo $(p_{n+1}, \ldots, p_m) = 0$, což není možné.

Poznámka. Při rozkladu záporného zlomku je vždy $q_1 < 0$, $q_2, \ldots, q_n \in \mathbb{N}$, pro $m \in \mathbb{Z}$ je $m = (m)$ a zlomek $\frac{1}{m} = (0, m)$ pro $m > 0$.

3. Parciální zlomky řetězového zlomku

Opačnou úlohou k úloze vyjádřit číslo $\frac{a}{b}$ řetězovým zlomkem je pro dané hodnoty čísel $q_1 \in \mathbb{Z}$, $q_2, \ldots q_n \in \mathbb{N}$ nalezení hodnoty řetězového zlomku $(q_1, \ldots, q_n)$. Tu lze pochopitelně určit z formule (1), ovšem při větším počtu prvků řetězového zlomku není výpočet efektivní. Pro řešení této úlohy hrají důležitou roli zlomky

$$\delta_1 = q_1,\ \delta_2 = q_1 + \frac{1}{q_2},\ \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}},\ \ldots,$$

neboli

$$\delta_1 = (q_1),\ \delta_2 = (q_1, q_2),\ \delta_3 = (q_1, q_2, q_3),\ \ldots,\ \delta_n = (q_1, \ldots, q_n). \tag{2}$$

Zlomky (2) nazýváme *parciální zlomky* řetězového zlomku $(q_1, \ldots, q_n)$, přičemž δ_k nazýváme *parciální zlomek řádu k*. Dokažme nyní rekurentní formule pro výpočet parciálních zlomků:

$$\begin{aligned} \delta_k &= \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}}, \\ P_k &= q_k P_{k-1} + P_{k-2},\ P_0 = 1,\ P_1 = q_1, \\ Q_k &= q_k Q_{k-1} + Q_{k-2},\ Q_0 = 0,\ Q_1 = 1. \end{aligned} \tag{3}$$

Důkaz provedeme matematickou indukcí.

Pro $k = 1$ je $\delta_1 = \frac{P_1}{q_1} = q_1$, pro $k = 2$ je $P_2 = q_2 P_1 + P_0 = q_2 q_1 + 1$, $Q_2 = q_2 Q_1 + Q_0 = q_2$, tedy $\delta_2 = \frac{P_2}{q_2}$.

Předpokládejme nyní platnost vzorce (3) pro některé k. Pak zlomek δ_{k+1} dostaneme ze zlomku δ_k záměnou $q_k + \frac{1}{q_{k+1}}$ za q_k, tedy

$$\delta_{k+1} = \frac{P_{k+1}}{Q_{k+1}} = \frac{\left(q_k + \frac{1}{q_{k+1}}\right)P_{k-1} + P_{k-2}}{\left(q_k + \frac{1}{q_{k+1}}\right)Q_{k-1} + Q_{k-2}} = \frac{q_{k+1}(q_k P_{k-1} + P_{k-2}) + P_{k-1}}{q_{k+1}(q_k Q_{k-1} + Q_{k-2}) + Q_{k-1}} =$$

$$= \frac{q_{k+1}P_k + P_{k-1}}{q_{k+1}Q_k + Q_{k-1}}.$$

Prakticky se výpočet zlomků δ_k provádí pomocí následující tabulky:

		q_1	q_2		q_{k-2}	q_{k-1}	q_k		q_n
P_k	$P_0 = 1$	$P_1 = q_1$	P_2	$\dots$	P_{k-2}	P_{k-1}	P_k	$\dots$	P_n
Q_k	$Q_0 = 0$	$Q_1 = 1$	Q_2	$\dots$	Q_{k-2}	Q_{k-1}	Q_k	$\dots$	Q_n

Příklad. $\frac{95}{42} = (2, 3, 1, 4, 2)$

		2	3	1	4	2
P_k	$P_0 = 1$	2	$3 \cdot 2 + 1 = 7$	$1 \cdot 7 + 2 = 9$	$4 \cdot 9 + 7 = 43$	$2 \cdot 43 + 9 = 95$
Q_k	$Q_0 = 0$	1	$3 \cdot 1 + 0 = 3$	$1 \cdot 3 + 1 = 4$	$4 \cdot 4 + 3 = 19$	$2 \cdot 19 + 4 = 42$

Uveďme některé důležité vlastnosti parciálních zlomků, kterých budeme užívat v dalším textu.

α) Označme $P_kQ_{k-1} - P_{k-1}Q_k = \triangle_k$. Dosazením za P_k a Q_k z formulí (3) dostaneme

$$\triangle_k = (q_kP_{k-1}+P_{k-2})Q_{k-1} - P_{k-1}(q_kQ_{k-1}+Q_{k-2}) = -(P_{k-1}Q_{k-2} - P_{k-2}Q_{k-1}),$$

tedy $\triangle_k = -\triangle_{k-1}$.

Platí ovšem $\triangle_1 = P_1Q_0 - Q_1P_0 = -1$, celkem tedy $\triangle_k = (-1)^k$.

β) Z poslední rovnosti

$$\triangle_k = (-1)^k = P_kQ_{k-1} - P_{k-1}Q_k$$

plyne, že $(P_k, Q_k)|(-1)^k$, tedy $(P_k, Q_k) = 1$. *Každý parciální zlomek je tedy v základním tvaru.* Dále odtud plyne, že je-li zlomek $\frac{a}{b}$ v základním tvaru, platí $a = P_n$, $b = Q_n$.

γ) Počítejme rozdíl sousedních parciálních zlomků:

$$\delta_k - \delta_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{\triangle_k}{Q_kQ_{k-1}} = \frac{(-1)^k}{Q_kQ_{k-1}},$$

tedy

$$|\delta_k - \delta_{k-1}| = \frac{1}{Q_kQ_{k-1}}.$$

Řešení kongruenčních rovnic 1. stupně pomocí řetězových zlomků

Jak již bylo zmíněno v předcházejícím textu, dosud uvedené metody řešení kongruenčních rovnic 1. stupně

$$ax \equiv b \pmod{m}, \quad (a, m) = 1 \tag{1}$$

nejsou v případě velkých modulů m efektivní. Ukažme, jak je možno v tomto případě při řešení rovnic (1) užít řetězových zlomků.

Především lze předpokládat, že navíc v rovnici (1) je $a > 0$. V opačném případě je totiž vždy možno najít číslo $a^* \in \mathbb{N}$ tak, že $a \equiv a^* \pmod{m}$, a tedy prvek a lze nahradit prvkem a^*.

Nejprve rozložíme číslo $\frac{m}{a}$ v řetězový zlomek $(q_1, \ldots, q_n)$ a nechť $\delta_k = \frac{P_k}{Q_k}$ jsou jeho parciální zlomky. Jelikož $(m, a) = 1$, platí vzhledem k vlastnosti β) řetězových zlomků $P_n = m$, $Q_n = a$. Protože

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n,$$

je $mQ_{n-1} - P_{n-1}a = (-1)^n$, odkud

$$aP_{n-1} = (-1)^{n-1} + mQ_{n-1} \equiv (-1)^{n-1} \pmod{m}.$$

Vynásobením poslední rovnosti číslem $(-1)^{n-1}b$ konečně dostaneme

$$a\left((-1)^{n-1} b P_{n-1}\right) \equiv b \pmod{m},$$

což porovnáním s rovnicí (1) znamená, že

$$x \equiv (-1)^{n-1} P_{n-1} b \pmod{m}. \tag{2}$$

Příklad. Řešme rovnici $285x \equiv 177 \pmod{924}$.
Řešení: Platí $(285, 924) = 3$, $177 = 59 \cdot 3$, dostaneme tedy ekvivalentní rovnici

$$95x \equiv 59 \pmod{308}.$$

Dále

$$\frac{m}{a} = \frac{308}{95},$$

tedy

$$\begin{array}{ccccccccccc} 308 & : & 95 & : & 23 & : & 3 & : & 2 & : & 1 \\ & & 3 & & 4 & & 7 & & 1 & & 2 \end{array},$$

odkud

$$\frac{m}{a} = (3, 4, 7, 1, 2)$$

(do horního řádku jsou zapisovány zbytky po naznačených děleních, do dolního pak neúplné podíly). Sestavíme tabulku pro výpočet parciálních zlomků, přičemž nás vzhledem ke vztahu (2) zajímá pouze člen P_{n-1} (v našem případě je $n = 5$, jde tedy o člen P_4):

		3	4	7	1	2
P_k	1	3	13	94	$\underline{107}$	308

Dosazením $P_4 = 107$ do vzorce (2) dostáváme

$$x \equiv (-1)^4 \cdot 107 \cdot 59 \pmod{308},$$
$$x \equiv 153 \pmod{308}.$$

Původní rovnice má pak řešení $x \equiv 153,\ 153 + 308,\ 153 + 2 \cdot 308 \pmod{924}$, neboli

$$x \equiv 153,\ 461,\ 769 \pmod{924}.$$

Cvičení

33. Najděte celou a zlomkovou část čísel:
    a) $\frac{317}{45}$, b) $-47,3$, c) $0,73$, d) $-\frac{15}{23}$.
34. Najděte počet bodů s celočíselnými souřadnicemi, které jsou umístěny mezi osou x a přímkou
    $$3x + 5y - 4 = 0,$$
    jestliže mají x-ovou souřadnici: (a) 17, (b) -33. Nakreslete graf.
35. Najděte počet bodů s celočíselnými souřadnicemi, které jsou umístěny mezi osou y a přímkou
    $$5x + 3y - 8 = 0,$$
    jestliže mají y-ovou souřadnici: (a) 23, (b) -28. Nakreslete graf.
36. Rozložte zlomek $\frac{a}{b}$ v periodický řetězový zlomek a najděte jeho parciální zlomky, je-li $\frac{a}{b}$ rovno:
    a) $\frac{317}{31}$, b) $\frac{521}{143}$, c) $\frac{247}{74}$, d) $-\frac{313}{57}$, e) $\frac{77}{187}$, f) $-\frac{53}{217}$.
37. Řešte kongruence:
    a) $67x \equiv 64 \pmod{183}$,
    b) $89x \equiv 86 \pmod{241}$,
    c) $213x \equiv 137 \pmod{516}$.
38. Řešte kongruence:
    a) $111x \equiv 81 \pmod{447}$,
    b) $186x \equiv 374 \pmod{422}$,
    c) $129x \equiv 321 \pmod{471}$.
39. Řešte kongruence:
    a) $-50x \equiv 67 \pmod{177}$,
    b) $-73x \equiv 60 \pmod{311}$,
    c) $-53x \equiv 84 \pmod{219}$.

Užití kongruenčních rovnic 1. stupně při řešení neurčitých rovnic 1. stupně se 2 neznámými

Uvažujme nejprve následující jednoduchou úlohu z praxe. Máme dvě nádoby o objemech 5 l a 7 l a třetí nádobu dostatečně velkého objemu. Ptáme se, zda je možno pouze pomocí prvních dvou nádob do třetí nádoby nalít 8 l vody. Jedno z možných řešení může vypadat tak, že nejprve nalejeme do třetí nádoby 4 nádoby o objemu 7 l a pak odebereme ze třetí nádoby 4 nádoby 5 litrové. Kdybychom měli ale první dvě nádoby o objemech 12 l a 20 l a chtěli do třetí nádoby pomocí nich dostat 38 l vody, nikdy se nám to nepovede (čtenář nechť to raději nezkouší a přečte si další text).

Úlohy uvedeného typu vedou k řešení rovnic ve tvaru

$$ax + by = c, \tag{1}$$

přičemž $a, b, c \in \mathbb{Z}$ jsou daná čísla a hledáme všechny uspořádané dvojice $(x, y) \in \in \mathbb{Z}^2$ vyhovující rovnosti (1). Rovnice (1) nazýváme *neurčité rovnice 1. stupně o dvou neznámých* nebo také *lineární diofantické rovnice o dvou neznámých.*

Z rovnice (1) okamžitě dostaneme kongruenční rovnici 1. stupně

$$ax \equiv c \pmod{b}. \tag{2}$$

Využijeme nyní toho, co už víme o řešení rovnic (2). Jestliže $d = (a, b) \nmid c$, pak rovnice (2) (a tedy ani rovnice (1)) není řešitelná. V opačném případě lze celou rovnici (1) vydělit číslem b a zabývat se pouze případem, kdy $(a, b) = 1$.

Jak už víme, rovnice (2) má v tom případě jediné řešení

$$x \equiv x_1 \pmod{b}, \quad \text{tj. } x = x_1 + bt,\ t \in \mathbb{Z}.$$

Dosadíme-li nyní za x do rovnice (1), dostaneme pro y vyjádření

$$y = \frac{c - ax_1}{b} - at = y_1 - at, \quad t \in \mathbb{Z}.$$

Zřejmě $y_1 = \frac{c-ax_1}{b} \in \mathbb{Z}$, neboť $b|c - ax_1$ (x_1 je totiž řešením rovnice (2)), a tedy obecné řešení rovnice (1) je ve tvaru

$$\begin{aligned} x &= x_1 + bt \\ y &= y_1 - at,\ t \in \mathbb{Z}. \end{aligned}$$

Příklad. Řešme rovnici $53x + 17y = 25$.
Řešení: Platí

$$53x \equiv 25 \pmod{17},$$

neboli

$$x \equiv 4 \pmod{17}, \quad x = 4 + 17t,\ t \in \mathbb{Z},\ x_1 = 4.$$

Proto

$$53x_1 + 17y_1 = 25,$$

odkud $y_1 = -11$. Obecné řešení rovnice je ve tvaru

$$\begin{aligned} x &= 4 + 17t \\ y &= -11 - 53t,\ t \in \mathbb{Z}. \end{aligned}$$

Obecně lze uvažovat rovnice typu

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \tag{3}$$

kde $a_1, \ldots, a_n, b$ jsou daná celá čísla, řešením jsou všechny n-tice $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ vyhovující vztahu (3). Rovnice (3) nazýváme *neurčité rovnice 1. stupně s n neznámými* nebo *lineární diofantické rovnice o n neznámých*. Pro řešitelnost rovnic (3) lze dokázat následující větu.

Věta 3.1. *Rovnice* (3) *je řešitelná právě když* $d = (a_1, \ldots, a_n)|b$, *přičemž řešení závisí na* $n - 1$ *nezávislých celočíselných parametrech.*

Důkaz: Platnost implikace ($\Rightarrow$) je zřejmá. Obrácenou implikaci dokážeme indukcí dle n.

Případ $n = 2$ byl řešen v předcházejícím textu a řešení rovnice závisí na $2 - 1 = 1$ parametru. Předpokládejme platnost tvrzení pro n a dokažme platnost pro $n + 1$. Uvažujme rovnici

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n + a_{n+1}x_{n+1} = b \tag{4}$$

a nechť $d = (a_1, \ldots, a_n, a_{n+1})|b$. Označme dále $d_1 = (a_1, \ldots, a_n)|b$.

Evidentně $d|d_1$ a $d_1|(a_1x_1 + \ldots + a_nx_n)$, a tedy

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n \equiv 0 \pmod{d_1},$$

odkud

$$a_{n+1}x_{n+1} \equiv b \pmod{d_1}. \tag{5}$$

Zřejmě $(a_{n+1}, d_1) = d|b$, tedy rovnice (5) je řešitelná a existuje její jediné řešení v modulu $\frac{d_1}{d}$. Je tedy

$$a_{n+1}x_{n+1} = b + d_1t_1, \quad t_1 \in \mathbb{Z}. \tag{6}$$

Dosazením vztahu (6) do rovnice (4) dostaneme

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b - b - d_1t_1 = -d_1t_1.$$

Vzhledem k tomu, že $d_1 = (a_1, \ldots, a_n)|d_1t_1$, je poslední rovnice dle indukčního předpokladu řešitelná a její řešení závisí na $n-1$ parametrech. Přidáme-li k těmto parametrům parametr t_1, dostaneme, že rovnice (4) je řešitelná a její řešení závisí na n parametrech. □

Poznámka. Rovnice (3) je pro $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$ rovnicí nadroviny v eukleidovském prostoru $\mathcal{E}_n$. Řešit rovnici (3) tedy znamená najít všechny body této nadroviny s celočíselnými souřadnicemi. Takovým bodům říkáme *mřížové body* nadroviny.

Příklad. Najděte všechny mřížové body nadroviny $9x - 15y + 4z = 6$ v $\mathcal{E}_3$.
Řešení: Platí $(9, -15, 4) = 1$, tedy rovnice je řešitelná. Dále $d_1 = (9, -15) = 3$, odkud $4z \equiv 6 \pmod 3$, neboli $z \equiv 0 \pmod 3$ a $z = 3t_1$, $t_1 \in \mathbb{Z}$. Dosadíme z do původní rovnice: $9x - 15y = 6 - 12t_1$, neboli

$$3x - 5y = 2 - 4t_1. \tag{7}$$

Odtud

$$3x \equiv 2 - 4t_1 \pmod 5,$$

tedy

$$\begin{aligned} 3x &\equiv -3 - 9t_1 \pmod 5, \\ x &\equiv -1 - 3t_1 \pmod 5, \end{aligned}$$

tj.

$$x = -1 - 3t_1 + 5t_2, \quad t_2 \in \mathbb{Z}.$$

Konečně dosazením za x do (7) dostaneme

$$y = -1 - t_1 + t_2.$$

Cvičení

40. Řešte diofantické rovnice:

    a) $17x - 16y = 31$,
    b) $23x + 15y = 19$,
    c) $12x - 37y = -3$,
    d) $18x - 33y = 26$,
    e) $11x + 16y = 156$.

41. Určete den narození, znáte-li součet S čísla měsíce násobeného číslem 31 a dne měsíce násobeného 12, např. pro $S = 436$.
42. Pro která nejmenší celá kladná čísla a, b má neurčitá rovnice $ax + by = 31$ řešení $(5, 9)$?
43. Na přímce $ax + by = c$ najděte množinu celočíselných bodů ležících mezi body (a_1, y) a (a_2, y):

    a) $8x - 13y + 6 = 0$, $a_1 = -100$, $a_2 = 150$,
    b) $7x - 29y = 584$, $a_1 = -20$, $a_2 = 160$,
    c) $90x - 74y = 50$, $a_1 = -100$, $a_2 = 200$.

44. Dokažte, že počet celočíselných bodů ležících na úsečce s koncovými body $A = (x_1, y_1), B = (x_2, y_2)$ je roven $d - 1$, kde $d = (y_1 - y_2, x_1 - x_2)$.
45. Kolika celočíselnými body prochází trojúhelník, jehož vrcholy jsou v bodech $A = (2, 1)$, $B = (20, 7)$ a $C = (8, 15)$?
46. Najděte vzdálenost r mezi sousedními celočíselnými body ležícími na přímce $ax + by = c$, kde $(a, b) = 1$.

Soustavy kongruenčních rovnic 1. stupně

Při řešení praktických úloh se setkáváme nejen s kongruenčními rovnicemi, ale také s jejich soustavami. Uveďme alespoň jednu motivační úlohu.

Einsteinova úloha: *Uvažujeme schodiště mající následující vlastnosti: budeme-li přecházet po dvou schodech najednou, zůstane nám na konci jeden schod, půjdeme-li po třech schodech, zůstanou nám nakonec dva schody, půjdeme-li po čtyřech, zůstanou tři schody, po pěti zůstanou čtyři schody, po šesti pět schodů a teprve překročili bychom-li najednou sedm schodů, došli bychom na konec schodiště. Kolik schodů má schodiště?*

Snadno je vidět, že Einsteinova úloha je ekvivalentní nalezení všech přirozených čísel vyhovujících následující soustavě kongruenčních rovnic 1. stupně:

$$\begin{aligned} &x \equiv 1 \pmod 2, \qquad x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 4, \\ &x \equiv 4 \pmod 5, \qquad x \equiv 5 \pmod 6, \qquad x \equiv 0 \pmod 7. \end{aligned}$$

Uvažujme systém kongruenčních rovnic 1. stupně s neznámou $x \in \mathbb{Z}$

$$A_1 x \equiv B_1 \pmod{m_1}, \ \ldots, \ A_k x \equiv B_k \pmod{m_k}. \tag{1}$$

Z předešlých úvah je zřejmé, že pokud je soustava (1) řešitelná, je řešitelná každá z rovnic soustavy, a má tedy smysl zabývat se pouze soustavami ve tvaru

$$x \equiv b_1 \pmod{m_1}, \ \ldots, \ x \equiv b_k \pmod{m_k}. \tag{2}$$

Soustavu (1) nazýváme *soustava lineárních kongruenčních rovnic 1. stupně.*

Ukažme, že v případě řešitelnosti soustavy (2) lze řešení vždy hledat ve tvaru

$$x \equiv x_1 \pmod{[m_1, \ldots, m_k]}.$$

Rozeberme nejprve případ dvou rovnic. Z první rovnice plyne, že $x = b_1 + m_1 t$ pro některá $t \in \mathbb{Z}$. Dosazením do druhé rovnice dostaneme

$$b_1 + m_1 t \equiv b_2 \pmod{m_2},$$

tedy

$$m_1 t \equiv b_2 - b_1 \pmod{m_2}.$$

Poslední rovnice je řešitelná právě když $d = (m_1, m_2) | (b_2 - b_1)$. V tom případě je

$$\frac{m_1}{d} t \equiv \frac{b_2 - b_1}{d} \pmod{\frac{m_2}{d}}, \quad \text{kde } \left(\frac{m_1}{d}, \frac{m_2}{d}\right) = 1.$$

Pak

$$t \equiv t_1 \pmod{\frac{m_2}{d}}$$

pro nějaké $t_1 \in \mathbb{Z}$, tj. $t = t_1 + \frac{m_2}{d}r$, kde $r \in \mathbb{Z}$. Po dosazení t do vztahu pro x dostaneme

$$x = b_1 + m_1 t = b_1 + m_1 t_1 + \frac{m_1 m_2}{d} r = b_1 + m_1 t_1 + [m_1, m_2]r,$$

tj. $x \equiv x_1 \pmod{[m_1, m_2]}$ pro $x_1 = b_1 + m_1 t$.

Tvrzení pro obecný počet rovnic se analogicky dokáže matematickou indukcí s využitím případu pro dvě rovnice.

Příklad. Řešme soustavu

$$\begin{aligned} x &\equiv 5 \pmod{18} \\ x &\equiv 8 \pmod{21}. \end{aligned}$$

Řešení: Z první rovnice máme $x = 5 + 18t$ pro nějaké $t \in \mathbb{Z}$, odkud dosazením do druhé rovnice máme

$$5 + 18t \equiv 8 \pmod{21},$$

neboli

$$t \equiv -1 \pmod{7}, \quad t = -1 + 7r,\ r \in \mathbb{Z},$$

Dosazením t do x konečně máme $x = -13 + 126r$, tj.

$$x \equiv -13 \pmod{126}.$$

Příklad. Řešme Einsteinovu úlohu.
Řešení: Z první rovnice plyne $x = 2k+1$, $k \in \mathbb{Z}$. Dosadíme-li x do druhé rovnice, pak $2k + 1 \equiv 2 \pmod 3$, odkud $2k \equiv 1 \equiv 4 \pmod 3$, což vzhledem k $(2, 3) = 1$ dává $k \equiv 2 \pmod 3$, tj. $k = 3l + 2$, $l \in \mathbb{Z}$. Dosadíme za k do vztahu pro x a dostaneme $x = 6l + 5$. Opět x dosadíme do třetí rovnice:

$$6l + 5 \equiv 3 \pmod 4, \qquad 3l \equiv -1 \equiv 3 \pmod 2,$$

tj. vzhledem k $(3, 2) = 1$ je $l \equiv 1 \pmod 2$, neboli $l = 2m + 1$, $m \in \mathbb{Z}$. Dosazením za l do vztahu pro x pak $x = 12m + 11$. Z následující rovnice plyne

$$12m + 11 \equiv 4 \pmod 5, \qquad m \equiv 4 \pmod 5,$$

tedy $m = 5r+4$, $r \in \mathbb{Z}$ a $x = 60r+59$. Další rovnice dává kongruenci $60r+59 \equiv 5 \pmod 6$, která je splněna pro každé $r \in \mathbb{Z}$. Odtud konečně dosazením do poslední rovnice je

$$60r + 59 \equiv 0 \pmod 7, \qquad r \equiv 1 \pmod 7, \quad r = 7s + 1$$

a tedy

$$x = 420s + 119, \quad s \in \mathbb{Z},$$

Nejmenší možný počet schodů schodiště je tedy 119 a všechna přirozená x v uvedeném tvaru vyhovují naší úloze.

Případ vzájemně nesoudělných modulů

Zabývejme se nyní soustavami (2), v nichž jsou moduly po dvou nesoudělné, tj. platí $(m_i, m_j) = 1$ pro $i \neq j$.V tomto případě zřejmě platí

$$[m_1, \ldots, m_k] = m_1 \cdot \ldots \cdot m_k = M$$

a z předchozích úvah vyplývá, že řešení soustavy (2) lze hledat ve tvaru

$$x \equiv x_0 \pmod{M}.$$

Položme $M_i = \frac{M}{m_i}$ pro $i = 1, \ldots, k$. Vzhledem ke vzájemné nesoudělnosti modulů platí $(m_i, M_i) = 1$ (ověřte!). To ovšem znamená, že existují prvky M_i^* tak, že

$$M_i \cdot M_i^* = 1 \pmod{m_i}$$

(prvky M_i jsou totiž invertibilní v $\mathbb{Z}_m$). Položme

$$x_0 = M_1 M_1^* b_1 + \ldots + M_k M_k^* b_k.$$

Pak $x_0 \equiv M_1 M_1^* b_1 \equiv b_1 \pmod{m_1}$, neboť $M_k \equiv 0 \pmod{m_j}$ pro $j \neq k$. Podobně $x_0 \equiv b_j \pmod{m_j}$ pro každé $j = 1, \ldots, k$, tedy

$$x \equiv x_0 \pmod{M}.$$

Povšimněme si přitom, že čísla M_i, M_i^* vůbec nezávisejí na číslech b_i.

Příklad. Řešme soustavu

$$\begin{aligned} x &\equiv 20 \pmod{21} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 5 \pmod{8}. \end{aligned}$$

Řešení: Platí $M = 21 \cdot 5 \cdot 8 = 840$, $M_1 = \frac{M}{21} = 40$, $M_2 = \frac{M}{5} = 168$, $M_3 = \frac{M}{8} = 105$. Postupně tak dostáváme:

$$\begin{aligned} 40M_1^* &\equiv 1 \pmod{21} \\ -2M_1^* &\equiv -20 \pmod{21} \\ M_1^* &\equiv 10 \pmod{21} \end{aligned}$$

$$\begin{aligned} 168M_2^* &\equiv 1 \pmod{5} \\ 3M_2^* &\equiv 6 \pmod{5} \\ M_2^* &\equiv 2 \pmod{5} \end{aligned}$$

$$\begin{aligned} 105M_3^* &\equiv 1 \pmod{8} \\ M_3^* &\equiv 1 \pmod{8} \end{aligned}$$

Odtud

$$x_0 = 40 \cdot 10 \cdot 20 + 168 \cdot 2 \cdot 3 + 105 \cdot 1 \cdot 5 \equiv 293 \pmod{840},$$

$$x \equiv 293 \pmod{840}.$$

Na závěr ještě uveďme, že soustavy typu (2) vyjadřují zadání staré čínské úlohy: *najít číslo, které po vydělení číslem m_1 dává zbytek b_1, atd., až po vydělení číslem m_k dá zbytek b_k.* Řešitelnost soustavy (2) lze shrnout do následující věty:

Věta 3.2. (čínská věta o zbytcích)
Buďte $m_1, \ldots, m_k$ po dvou nesoudělná přirozená čísla a $b_1, \ldots, b_k$ libovolná k-tice celých čísel. Pak je soustava lineárních kongruenčních rovnic (2) řešitelná a její řešení lze najít v modulu $m = m_1 \cdot \ldots \cdot m_k$.

Cvičení

47. Řešte soustavu kongruenčních rovnic:

    a) $x \equiv 6 \pmod{15}$, $x \equiv 18 \pmod{21}$, $x \equiv 3 \pmod{12}$;

    b) $x \equiv 13 \pmod{14}$, $x \equiv 6 \pmod{35}$, $x \equiv 26 \pmod{45}$;

    c) $x \equiv 19 \pmod{56}$, $x \equiv 3 \pmod{24}$, $x \equiv 7 \pmod{20}$;

    d) $x \equiv 19 \pmod{22}$, $x \equiv 8 \pmod{33}$, $x \equiv 14 \pmod{21}$.

48. Najděte přirozená čísla ≤ 1000, která při dělení danými čísly dají uvedená zbytky:

    a) čísla: 3, 5, 8; zbytky: 2, 4, 1;

    b) čísla: 5, 7, 9; zbytky: 4, 6, 1;

    c) čísla: 15, 14, 11; zbytky: 11, 3, 5;

    d) čísla: 13, 21, 23; zbytky: 9, 1, 13.

49. Mezi čísly 200 a 500 najděte všechna, která při dělení čísly 4, 5, 7 dají odpovídající zbytky 3, 4, 5.

3.3 Kongruenční rovnice 2. stupně obecného typu

Zabývejme se nyní řešením kongruenčních rovnic 2. stupně. Jejich obecný tvar je

$$Ax^2 + Bx + C \equiv 0 \pmod{M}, \tag{1}$$

kde $A, B, C \in \mathbb{Z}$ jsou daná čísla, $A \not\equiv 0 \pmod{M}$ a neznámá $x \in \mathbb{Z}$.

Ukažme, že každou rovnici tvaru (1) je možno převést na tvar

$$x^2 \equiv a \pmod{m} \tag{2}$$

pro nějaké $a \in \mathbb{Z}$. Rovnici (1) nejprve vynásobíme číslem $4A$:

$$4A^2x^2 + 4ABx + 4AC \equiv 0 \pmod{4AM}, \tag{3}$$

která je ekvivalentní s rovnicí (1) (proč?). Z rovnice (3) plyne

$$(2Ax + B)^2 \equiv B^2 - 4AC \pmod{4AM}.$$

Substitucemi $y = 2Ax + B, D = B^2 - 4AC$ dostaneme

$$y^2 \equiv D \pmod{4AM}, \tag{4}$$

která je už rovnicí tvaru (2). Je třeba si uvědomit, že řešitelnost rovnice (4) ještě neznamená řešitelnost původní rovnice (1). Je-li totiž y_1 řešením rovnice (4), $y \equiv y_1 \pmod{4AM}$, pak po dosazení za y dostaneme rovnici $2Ax \equiv y_1 - B \pmod{4AM}$, která v případě $2A \nmid (y_1 - B)$, není řešitelná. Dále je třeba mít na paměti fakt, že řešení rovnice (4) jsou v modulu $2M$, kdežto řešení rovnice (1) hledáme v modulu M. Počet řešení rovnice (4) se tedy přechodem k původnímu modulu může zmenšit.

Příklad. Řešme rovnice:

a) $4x^2 - 11x - 3 \equiv 0 \pmod{13}$, b) $x^2 - 5x + 6 \equiv 0 \pmod{24}$.

Řešení:

a)

$$4x^2 - 24x - 16 \equiv 0 \pmod{13},$$
$$x^2 - 6x - 4 = (x-3)^2 - 13 \equiv 0 \pmod{13},$$
$$(x-3)^2 \equiv 0 \pmod{13}.$$

Vzhledem k tomu, že 13 je prvočíslo, je $x - 3 \equiv 0 \pmod{13}$, tj.

$$x \equiv 3 \pmod{13}.$$

b) Vynásobením rovnice číslem 4 dostaneme

$$4x^2 - 20x + 64 \equiv 0 \pmod{96},$$
$$(2x-5)^2 \equiv -39 \pmod{96},$$
$$y^2 \equiv -39 \pmod{96}$$

pro $y = 2x - 5$. Aniž se budeme zabývat řešením poslední rovnice, uveďme, že jejími řešeními jsou $y = \pm 21, \pm 27 \pmod{96}$. Odtud snadno dostaneme, že $x \equiv 13, -8, 16, -11 \pmod{48}$, což v původním modulu 24 dává řešení

$$x \equiv 13, 16 \pmod{24}.$$

Je-li rovnice (2) řešitelná pro $a \not\equiv 0 \pmod{m}$, nazýváme číslo a *kvadratický zbytek* modulo m; v opačném případě se nazývá *kvadratický nezbytek* modulo m. Řešení rovnic (2) vede při složeném modulu m k řešení následujících rovnic:

(i) $x^2 \equiv a \pmod{p}$, kde p je liché prvočíslo,
(ii) $x^2 \equiv a \pmod{p^\alpha}$, $\alpha > 1$, p je liché prvočíslo,
(iii) $x^2 \equiv a \pmod{2^\alpha}$, $\alpha \geq 1$.

Nejprve se podívejme na případ (i).

Kongruenční rovnice 2. stupně v lichém prvočíselném modulu p

Uvažujme tedy rovnice

$$x^2 \equiv a \pmod{p}, \quad (2,p) = 1, \quad (a,p) = 1. \tag{1}$$

Snadno se vidí, že je-li $\overline{x}_1$ řešením rovnice (1), pak také třída $-\overline{x}_1$ je jejím řešením a platí $\overline{x}_1 \neq -\overline{x}_1$. Kdyby totiž platilo $\overline{x}_1 = -\overline{x}_1$, pak by $2\overline{x}_1 = \overline{0}$ v $\mathbb{Z}_p$, tj. $p|2x_1$, což vzhledem k tomu, že p je prvočíslo a $(2,p) = 1$ znamená, že $p|x_1$. Pak ale $\overline{x}_1 = \overline{0}$ a $\overline{a} = \overline{0}$, což je spor s $(a,p) = 1$.

Ukázali jsme tedy, že má-li rovnice (1) řešení, pak má alespoň dvě řešení. Jelikož p je prvočíslo, je $\mathbb{Z}_p$ těleso. Algebraická rovnice 2. stupně nad tělesem ovšem nemůže mít více jak dva kořeny, proto má rovnice (1) v případě řešitelnosti právě dvě řešení.

Řešení rovnice (1) jsou prvky některého redukovaného systému zbytků modulo p. Uvažujme redukovaný systém s nejmenšími absolutními hodnotami, tj. jde o systém $\{\pm 1, \pm 2, \ldots, \pm\frac{1}{2}(p-1)\}$. Rovnice (1) ovšem nezávisí na znaménku čísla x, proto její řešení hledáme v množině $M = \{1, 2, \ldots, \frac{1}{2}(p-1)\}$. Dosazením každého z prvků z M do rovnice (1) dostaneme na levé straně čísla

$$1^2, 2^2, \ldots, \Big(\frac{1}{2}(p-1)\Big)^2. \tag{2}$$

Je zřejmé, že každé z čísel v posloupnosti (2) je kvadratickým zbytkem modulo p a že všechny kvadratické zbytky modulo p jsou prvky posloupnosti (2). Ukažme, že prvky posloupnosti (2) jsou právě všechny kvadratické zbytky modulo p, tj. že žádné dvě z čísel v (2) nejsou kongruentní modulo p. Předpokládejme opak, tj. že pro některá $1 \leq k < l \leq \frac{1}{2}(p-1)$ platí

$$k^2 \equiv l^2 \pmod{p}.$$

Pak by platilo $p|(k+l)\cdot(l-k)$, což vzhledem k $p \in \mathbb{P}$ dává

$$p|(k+l) \quad \text{nebo} \quad p|(l-k).$$

První případ není vzhledem k $1 \leq k+l \leq p-2$ možný, druhý není možný vzhledem k $1 \leq l-k \leq \frac{1}{2}(p-1)-1$. Dokázali jsme tedy, že

počet kvadratických zbytků modulo p je právě $\frac{1}{2}(p-1)$ a jsou to právě všechny prvky posloupnosti (2).

Podobně platí

počet kvadratických nezbytků modulo p je $\frac{1}{2}(p-1)$ a jsou to právě všechny prvky redukovaného systému zbytků nepatřící posloupnosti (2).

Příklad. Kvadratických zbytků (mod 17) je právě $\frac{1}{2}(17-1) = 8$ a jsou to čísla $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 25 \equiv 8$, $6^2 = 36 \equiv 2$, $7^2 = 49 \equiv 15$, $8^2 = 64 \equiv 13$. Kvadratické nezbytky jsou potom čísla 3, 5, 6, 7, 10, 11, 12, 14.

Eulerovo kritérium pro kvadratické zbytky

Je přirozené, že při řešení rovnic (1) se v prvé řadě zajímáme o to, kdy je rovnice řešitelná. Jak již bylo uvedeno, řešitelnost rovnic (1) je ekvivalentní hledání kvadratických zbytků modulo p. Následující věta je kritériem pro kvadratické zbytky:

Věta 3.3. (Eulerovo kritérium) *Buď $a \in \mathbb{Z}$, $(a,p)=1$. Pak*

i) a je kvadratický zbytek modulo p, právě když

$$a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p},$$

ii) a je kvadratický nezbytek modulo p, právě když

$$a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}.$$

Důkaz: Podle Fermatovy věty pro $a \in \mathbb{Z}$, $(a,p)=1$, platí $a^{p-1} \equiv 1 \pmod{p}$, tedy

$$(a^{\frac{1}{2}(p-1)} - 1) \cdot (a^{\frac{1}{2}(p-1)} + 1) \equiv 0 \pmod{p}.$$

Ovšem $\mathbb{Z}_p$ je těleso, tedy buď

$$a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p} \qquad \text{nebo} \qquad a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p} \qquad (3).$$

Zřejmě také

$$a^{\frac{1}{2}(p-1)} + 1 \not\equiv a^{\frac{1}{2}(p-1)} - 1 \pmod{p},$$

neboť $1 \not\equiv -1 \pmod{p}$ pro $p \neq 2$, a pro a tedy platí právě jedna z možností (3). Je-li a kvadratický zbytek, pak existuje $x \in \mathbb{Z}$, $(x,p)=1$, tak že $a \equiv x^2 \pmod{p}$, odkud

$$a^{\frac{1}{2}(p-1)} \equiv (x^2)^{\frac{1}{2}(p-1)} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Jelikož kvadratických zbytků je právě $\frac{1}{2}(p-1)$, má rovnice $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ (chápeme-li a jako neznámou) alespoň $\frac{1}{2}(p-1)$ řešení a jelikož je stupně $\frac{1}{2}(p-1)$, má jich právě $\frac{1}{2}(p-1)$. Žádný kvadratický nezbytek tedy této rovnici nevyhovuje a splňuje tedy rovnici $a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$. □

Příklad. Určete, zda je řešitelná rovnice $x^2 \equiv 7 \pmod{19}$.
Řešení: Zjistíme, zda 7 je kvadratický zbytek mod 19: $\frac{1}{2}(19-1) = 9$,

$$7^2 = 49 \equiv 11 \pmod{19}, \quad 7^3 \equiv 77 \equiv 1 \pmod{19}, \quad 7^9 \equiv (7^3)^3 \equiv 1 \pmod{19},$$

tedy dle Eulerova kritéria je rovnice řešitelná.

Legendrův symbol

Pro velké moduly p je Eulerovo kritérium velmi nepraktické. Efektivní způsob řešení umožňuje výpočet tzv. *Legendrova symbolu*. Ten je pro $a \in \mathbb{Z}$, $(a,p)=1$, definován takto:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{je-li } a \text{ kvadratický zbytek modulo } p \\ -1, & \text{je-li } a \text{ kvadratický nezbytek modulo } p, \end{cases}$$

a čteme jej „a nad p“.

Příklad. Sami ověřte, že $\left(\frac{7}{19}\right)=1$, $\left(\frac{5}{17}\right)=-1$.

Díky Eulerově kritériu dostaneme základní vlastnosti Legendrova symbolu.

1. Platí

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}. \tag{I}$$

2. Je-li $a \equiv b \pmod{p}$, pak

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right). \tag{II}$$

Tato vlastnost vyplývá z toho, že čísla z téže zbytkové třídy jsou zároveň kvadratickými zbytky či nezbytky. Lze ji také vyjádřit ve tvaru

$$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right), \quad k \in \mathbb{Z}.$$

3. Platí

$$\left(\frac{1}{p}\right) = 1. \tag{III}$$

Rovnice $x^2 \equiv 1 \pmod{p}$ je vždy řešitelná, jejím řešením jsou čísla $x \equiv \pm 1 \pmod{p}$. Je tedy 1 kvadratickým zbytkem.

4. Platí

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}. \tag{IV}$$

Dle vlastnosti (I) je

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{1}{2}(p-1)} \pmod{p}.$$

Výrazy na obou stranách kongruence nabývají hodnot ± 1, což vzhledem k tomu, že $1 \not\equiv -1 \pmod{p}$ znamená, že v kongruenci nastane rovnost.

Z této vlastnosti vyplývá, že pro prvočísla $p \equiv 1 \pmod{4}$ je $\frac{1}{2}(p-1)$ sudé, a tedy $\left(\frac{-1}{p}\right)=1$, pro prvočísla $p \equiv 3 \pmod{4}$ je $\frac{1}{2}(p-1)$ liché, a tedy $\left(\frac{-1}{p}\right)=-1$.

Příklad.

a) Rovnice $x^2 \equiv -1 \pmod{433}$ je řešitelná, neboť $433 \equiv 1 \pmod 4$.

b) Rovnice $x^2 \equiv -1 \pmod{587}$ není řešitelná, neboť $587 \equiv 3 \pmod 4$.

5. Platí

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right). \tag{V}$$

Díky vlastnosti (I) platí

$$\left(\frac{a \cdot b}{p}\right) \equiv (ab)^{\frac{1}{2}(p-1)} = a^{\frac{1}{2}(p-1)} \cdot b^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod p.$$

Obě strany nabývají hodnot ± 1, opět $1 \not\equiv -1 \pmod p$ a obě strany jsou si rovny. Jako důsledek pak platí

$$\left(\frac{a^2}{p}\right) = 1, \qquad \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

6. Platí

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}. \tag{VI}$$

Tuto vlastnost dokážeme později. Má tyto důsledky:

- je-li $p \equiv \pm 1 \pmod 8$, je $p = 8m \pm 1$, tedy

  $$\frac{p^2-1}{8} = \frac{(8m \pm 1)^2 - 1}{8} = \frac{64m^2 \pm 16m}{8} = 8m^2 \pm 2m \equiv 0 \pmod 2,$$

  tj. 2 je kvadratický zbytek mod p;

- je-li $p \equiv \pm 3 \pmod 8$, je $p = 8m \pm 3$, tedy

  $$\frac{p^2-1}{8} = \frac{(8m \pm 3)^2 - 1}{8} = \frac{64m^2 \pm 48m + 8}{8} = 8m^2 \pm 6m + 1 \equiv 1 \pmod 2,$$

  tj. 2 je kvadratický nezbytek mod p.

Příklad. Jelikož $1097 \equiv 1 \pmod 8$, je 2 kvadratický zbytek (mod 1097), protože $1709 \equiv 5 \pmod 8$, je 2 kvadratický nezbytek (mod 1 097).

7. *Zákon vzájemnosti pro různá lichá prvočísla p, q*:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}. \tag{VII}$$

Důkaz provedeme také později. Vynásobíme-li obě strany v (VII) číslem $\left(\frac{q}{p}\right)$, dostaneme

$$\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)} \cdot \left(\frac{q}{p}\right).$$

Odtud plyne, že je-li alespoň jedno z prvočísel $p, q \equiv 1 \pmod 4$, je exponent v (VII) sudý a platí

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right);$$

platí-li $p, q \equiv 3 \pmod 4$, pak je exponent v (VII) lichý a platí

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Poznamejme, že zákon vzájemnosti poprvé dokázal C. F. Gauss a nazval jej *Theorema aureum* (Zlatá věta). Jde totiž o velmi silný nástroj při výpočtu Legendrova symbolu. Vlastnosti (I)–(VII) jsou pro jeho výpočet plně dostačující.

Příklad. Rozhodněte o řešitelnosti rovnice $x^2 \equiv 426 \pmod{491}$.
Řešení: Číslo 491 je prvočíslo, budeme tedy počítat hodnotu Legendrova symbolu $\left(\frac{426}{491}\right)$. Předně $426 = 2 \cdot 3 \cdot 71$, tedy podle (V) je

$$\left(\frac{426}{491}\right) = \left(\frac{2}{491}\right) \cdot \left(\frac{3}{491}\right) \cdot \left(\frac{71}{491}\right).$$

1) $\left(\frac{2}{491}\right) = -1$, neboť je $491 \equiv 3 \pmod 8$,

2) $\left(\frac{3}{491}\right) = -\left(\frac{491}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$,
neboť $491 \equiv 3 \pmod 4$, $3 \equiv 3 \pmod 4$, $3 \equiv 3 \pmod 8$, $491 \equiv 2 \pmod 3$.

3) $\left(\frac{71}{491}\right) = -\left(\frac{491}{71}\right) = -\left(\frac{65}{71}\right) = -\left(\frac{5}{71}\right) \cdot \left(\frac{13}{71}\right) = -\left(\frac{71}{5}\right) \cdot \left(\frac{71}{13}\right) = -\left(\frac{1}{5}\right) \cdot \left(\frac{6}{13}\right) =$
$= -\left(\frac{2}{13}\right) \cdot \left(\frac{3}{13}\right) = -(-1) \cdot \left(\frac{13}{3}\right) = 1 \cdot \left(\frac{1}{3}\right) = 1$,
neboť $491, 71 \equiv 3 \pmod 4$; $491 \equiv 65 \pmod{71}$; $5, 13 \equiv 1 \pmod 4$;
$71 \equiv 1 \pmod 5$; $71 \equiv 6 \pmod{13}$; $13 \equiv 5 \pmod 8$; $13 \equiv 1 \pmod 4$;
$13 \equiv 1 \pmod 3$.

Celkem tedy

$$\left(\frac{426}{491}\right) = (-1) \cdot 1 \cdot 1 = -1$$

a rovnice není řešitelná.

Cvičení

50. Použitím Eulerova kritéria určete, zda jsou řešitelné následující kongruence:

a $x^2 \equiv 7 \pmod{23}$,
b) $x^2 \equiv 5 \pmod{31}$,
c) $x^2 \equiv 8 \pmod{37}$,
d) $x^2 \equiv 37 \pmod{43}$.

51. Dokažte, že kongruence $x^2 \equiv a \pmod{p^\alpha}$, $\alpha > 1$, $(a,p) = 1$, $(2,p) = 1$ je řešitelná a má v tom případě 2 řešení tehdy a jen tehdy, když je řešitelná odpovídající kongruence pro $\alpha = 1$.
52. Najděte nutnou podmínku pro řešení kongruence $x^2 \equiv a \pmod{2^\alpha}$, $\alpha > 0$, $(a,2) = 1$.
53. Najděte postačující podmínku pro řešení kongruence $x^2 \equiv a \pmod{2^\alpha}$, $\alpha > 0$, $(a,2) = 1$, $\alpha = 1, 2, 3$ a odpovídající řešení.
54. Určete hodnoty Legendrových symbolů:

    a) $\left(\frac{19}{67}\right)$, b) $\left(\frac{56}{73}\right)$, c) $\left(\frac{54}{83}\right)$, d) $\left(\frac{297}{337}\right)$, e) $\left(\frac{157}{401}\right)$,

    f) $\left(\frac{165}{373}\right)$, g) $\left(\frac{238}{593}\right)$, h) $\left(\frac{114}{277}\right)$, i) $\left(\frac{1015}{1621}\right)$, j) $\left(\frac{230}{457}\right)$.

55. Určete, prochází-li následující paraboly celočíselnými body:

    a) $73y = x^2 - 37$,
    b) $83y = x^2 - 34$,
    c) $443y = x^2 - 152$,
    d) $43y = x^2 - 42$.

56. Určete, jsou-li následující kongruence řešitelné:

    a) $x^2 \equiv 37 \pmod{93}$,
    b) $x^2 \equiv 29 \pmod{105}$,
    c) $x^2 \equiv 31 \pmod{77}$,
    d) $x^2 \equiv 51 \pmod{175}$,
    e) $x^2 \equiv 54 \pmod{143}$,
    f) $x^2 \equiv 20 \pmod{171}$,
    g) $x^2 \equiv 23 \pmod{1189}$.

57. Pro která čísla a platí:

    a) $3a^2 - 5$ je dělitelné 17,
    b) $7a^2 + 13$ je dělitelné 23,
    c) $13a^2 - 11$ je dělitelné 29.

58. Pro která lichá prvočísla p je číslo 3 kvadratický zbytek?
59. Pro která lichá prvočísla p je číslo -3 kvadratický zbytek?

Gaussovo lemma

K důkazu vlastnosti (VI) Legendrova symbolu nám poslouží následující lemma. Nechť p je prvočíslo, $(a,p) = 1$, $(2,p) = 1$. Jak již víme, množina

$$R = \{\pm 1, \ldots, \pm\frac{1}{2}(p-1)\}$$

tvoří redukovaný systém zbytků modulo p. Označme $M = \{1, \ldots, \frac{1}{2}(p-1)\}$. Z tvarů množin R a M bezprostředně plyne, že pro každé $x \in M$ existují čísla $\varepsilon_x = \pm 1$ a $r_x \in M$ tak, že

$$\overline{a} \cdot \overline{x} = \overline{\varepsilon}_x \cdot \overline{r}_x. \tag{1}$$

Ukažme, že probíhá-li x množinu M, pak r_x také probíhá množinu M. Jelikož $(a,p)=1$, je $\overline{a}\neq\overline{0}$ v $\mathbb{Z}_p$, a tedy pro $\overline{x}\neq\overline{x}_1$ je také $\overline{a}\cdot\overline{x}\neq\overline{a}\cdot\overline{x}_1$. Stačí dokázat, že pro každé $r_x\in M$ existují $\varepsilon_x=\pm1$ a $x\in M$ tak, že platí (1).

Pro $r_x\in M$ existuje prvek $\overline{y}$ tak, že $\overline{a}\cdot\overline{y}=\overline{r}_x$, totiž $\overline{y}=\overline{a}^{-1}\cdot\overline{r}_x$. Je-li nyní y kongruentní s některým prvkem z M, položíme $\varepsilon_x=1$ a $x=y$; v opačném případě položíme $\varepsilon_x=-1$ a $x=-y$.

Vynásobením všech rovnic (1), kde x probíhá množinu M, s přihlédnutím ke shora zmíněným skutečnostem dostaneme

$$\overline{a}^{\frac{1}{2}(p-1)}\cdot\overline{1}\cdot\ldots\cdot\overline{\frac{1}{2}(p-1)}=\overline{\varepsilon}_1\cdot\ldots\cdot\overline{\varepsilon}_{\frac{1}{2}(p-1)}\cdot\overline{1}\cdot\ldots\cdot\overline{\frac{1}{2}(p-1)},$$

tedy

$$\overline{a}^{\frac{1}{2}(p-1)}=\overline{\varepsilon}_1\cdot\ldots\cdot\overline{\varepsilon}_{\frac{1}{2}(p-1)}=\overline{\varepsilon_1\cdot\ldots\cdot\varepsilon_{\frac{1}{2}(p-1)}}.$$

Vzhledem ke vztahu

$$\left(\frac{a}{p}\right)\equiv a^{\frac{1}{2}(p-1)}\pmod p$$

dále dostaneme

$$\left(\frac{a}{p}\right)\equiv\varepsilon_1\cdot\ldots\cdot\varepsilon_{\frac{1}{2}(p-1)}\pmod p.$$

Protože obě strany poslední kongruence nabývají pouze hodnot ±1 a platí $1\not\equiv-1\pmod p$, platí v ní rovnost, tj.

$$\left(\frac{a}{p}\right)=\varepsilon_1\cdot\ldots\cdot\varepsilon_{\frac{1}{2}(p-1)}.$$

Poslední rovnost lze přepsat do tvaru

$$\left(\frac{a}{p}\right)=(-1)^{\mu},\tag{2}$$

kde μ je počet záporných hodnot mezi čísly $\varepsilon_1,\ldots,\varepsilon_{\frac{1}{2}(p-1)}$. Formule (2) se nazývá *Gaussovo lemma*.

Příklad. Vypočtěme pomocí formule (2) hodnotu $(\frac{5}{19})$.
Řešení: Platí $p=19$; $M=\{1,\ldots,9\}$; $5\cdot1\in M$, $5\cdot2\notin M$, $5\cdot3\notin M$, $5\cdot4\equiv1\in M$, $5\cdot5\equiv6\in M$, $5\cdot6\equiv11\notin M$, $5\cdot7\equiv16\notin M$, $5\cdot8\equiv2\in M$, $5\cdot9\equiv7\in M$. Celkem tedy $\mu=4$ a $\left(\frac{5}{19}\right)=(-1)^4=1$.

Je-li ve vztahu (1) $\varepsilon_x=1$, pak $\overline{a}\cdot\overline{x}=\overline{r}_x$, tedy $a\cdot x$ po vydělení číslem p dá zbytek r_x, kde $0<r_x\leq\frac{1}{2}(p-1)<\frac{1}{2}p$. Je tedy

$$\varepsilon_x=1\Leftrightarrow\left\{\frac{ax}{p}\right\}<\frac{1}{2}.$$

Z nerovnosti $0 < \{\frac{ax}{p}\} < \frac{1}{2}$ plyne $0 < 2\{\frac{ax}{p}\} < 1$, neboli

$$\varepsilon_x = 1 \Leftrightarrow \left[2\left\{\frac{ax}{p}\right\}\right] = 0. \tag{3}$$

Z rovnosti $\frac{ax}{p} = [\frac{ax}{p}] + \{\frac{ax}{p}\}$ dále dostaneme

$$2\frac{ax}{p} = 2\left[\frac{ax}{p}\right] + 2\left\{\frac{ax}{p}\right\} \quad \text{a} \quad \left[2\frac{ax}{p}\right] = 2\left[\frac{ax}{p}\right] + \left[2\left\{\frac{ax}{p}\right\}\right].$$

Z posledních rovností je zřejmé, že

$$\left[2\left\{\frac{ax}{p}\right\}\right] = 0 \Leftrightarrow \left[2\frac{ax}{p}\right] = 2\left[\frac{ax}{p}\right] \Leftrightarrow \left[2\frac{ax}{p}\right] \text{ je sudé číslo,}$$

$$\left[2\left\{\frac{ax}{p}\right\}\right] = 1 \Leftrightarrow \left[2\frac{ax}{p}\right] = 2\left[\frac{ax}{p}\right] + 1 \Leftrightarrow \left[2\frac{ax}{p}\right] \text{ je liché číslo.}$$

Dohromady tak z vlastnosti (3) platí

$$\varepsilon_x = 1 \Leftrightarrow \left[2\frac{ax}{p}\right] \text{ je sudé číslo,} \qquad \varepsilon_x = -1 \Leftrightarrow \left[2\frac{ax}{p}\right] \text{ je liché číslo,}$$

a můžeme tedy psát

$$\varepsilon_x = (-1)^{[2\frac{ax}{p}]}. \tag{4}$$

Z formulí (2) a (4) pak obdržíme

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{1}{2}(p-1)} = (-1)^{\sum[2\frac{ax}{p}]}, \tag{5}$$

kde v sumě sčítáme přes všechna $x \in M$.

Předpokládejme nyní, že a je liché číslo. Pak

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4}{p}\right)\cdot\left(\frac{\frac{1}{2}(a+p)}{p}\right) = \left(\frac{\frac{1}{2}(a+p)}{p}\right) =$$

$$= (-1)^{\sum[\frac{(a+p)x}{p}]} = (-1)^{\sum[\frac{ax}{p}]+\sum x}.$$

Přitom

$$\sum_{x\in M} x = 1 + \ldots + \frac{1}{2}(p-1) = \frac{1}{8}(p^2-1),$$

odkud dostaneme

$$\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\cdot\left(\frac{a}{p}\right) = (-1)^{\sum[\frac{ax}{p}]+\frac{1}{8}(p^2-1)}. \tag{6}$$

Položíme-li v (6) $a = 1$, pak

$$\sum_{x\in M}\left[\frac{ax}{p}\right] = \left[\frac{1}{p}\right] + \ldots + \left[\frac{\frac{1}{2}(p-1)}{p}\right] = 0 + \ldots + 0 = 0,$$

odkud již dostaneme vlastnost (VI)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$

Dokažme nyní zákon vzájemnosti pro lichá prvočísla (VII). Z formule (6) vyplývá, že pro liché a a $x \in M$ platí

$$\left(\frac{a}{p}\right) = (-1)^{\sum[\frac{ax}{p}]}.$$

Pro lichá čísla p, q tedy dostaneme

$$\left(\frac{q}{p}\right) = (-1)^{\alpha}, \quad \text{kde } \alpha = \sum_{x\in M}\left[\frac{qx}{p}\right],$$

$$\left(\frac{p}{q}\right) = (-1)^{\beta}, \quad \text{kde } \beta = \sum_{y\in M'}\left[\frac{py}{q}\right],$$

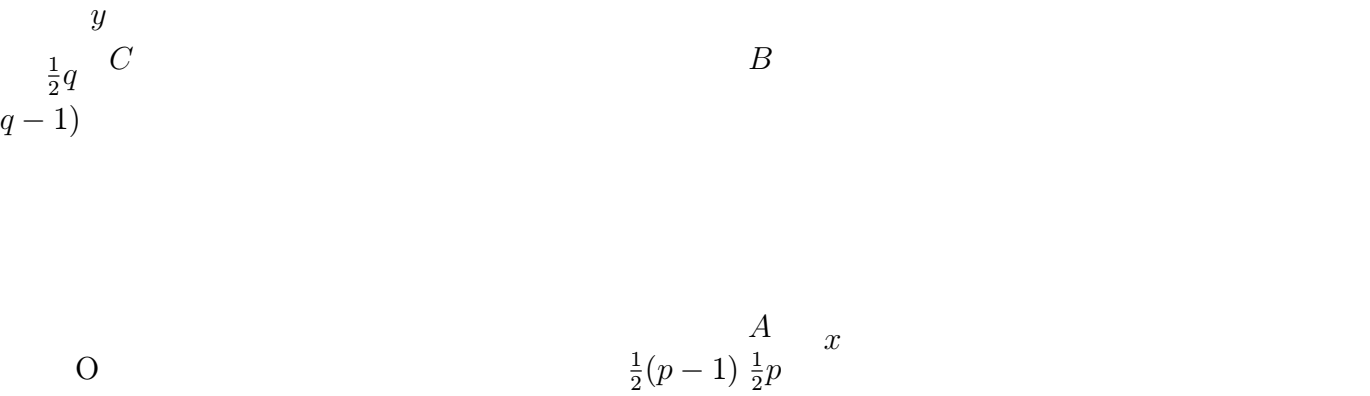
pro $M' = \{1, \ldots, \frac{1}{2}(q-1)\}$. Odtud

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\alpha+\beta}$$

a stačí dokázat, že

$$\alpha + \beta \equiv \frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1) \pmod 2.$$

Uvažujme v soustavě souřadnic body $O = (0,0)$, $A = (\frac{1}{2}p, 0)$, $B = (\frac{1}{2}p, \frac{1}{2}q)$, $C = (0, \frac{1}{2}q)$:



Je zřejmé, ž počet bodů s celočíselnými souřadnicemi uvnitř obdélníka $OACD$ je právě $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$. Ukažme, že uvnitř úsečky OB není žádný celočíselný bod. Rovnice přímky OB je $y = \frac{q}{p}x$ a pro $x \in M$ hodnota y nemůže být celé číslo. Určeme počty mřížových bodů uvnitř trojúhelníků OAB a OBC.

Mřížové body uvnitř trojúhelníka OAB leží na přímkách $x = k$ pro $x \in M$. Každá z nich protne OB v bodě $(k, \frac{qk}{p})$ a počet celočíselných bodů na takové úsečce je právě $\left[\frac{qk}{p}\right]$. Proto uvnitř trojúhelníka OAB je právě

$$\left[\frac{q \cdot 1}{p}\right] + \ldots + \left[\frac{q \cdot \frac{1}{2}(p-1)}{p}\right] = \sum_{x \in M} \left[\frac{q \cdot x}{p}\right] = \alpha$$

celočíselných bodů. Podobně uvnitř trojúhelníka OBC je

$$\left[\frac{p \cdot 1}{q}\right] + \ldots + \left[\frac{p \cdot \frac{1}{2}(q-1)}{q}\right] = \sum_{y \in M'} \left[\frac{p \cdot y}{q}\right] = \beta$$

celočíselných bodů. Je tedy

$$\alpha \cdot \beta = \frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1),$$

čímž je důkaz zákona vzájemnosti hotov.

3.4 Kongruenční rovnice n-tého stupně

Obecná kongruenční rovnice n-tého stupně je každá rovnice

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}, \tag{1}$$

kde $a_i \in \mathbb{Z}$, $m \in \mathbb{N}$, $m \nmid a_n$. Je-li $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, pak je rovnice (1) ekvivalentní soustavě

$$f(x) \equiv 0 \pmod{p_1^{\alpha_1}}, \ \ldots \ , f(x) \equiv 0 \pmod{p_k^{\alpha_k}}. \tag{2}$$

Fundamentální význam pro řešení obecných rovnic (1) budou tedy mít rovnice ve tvaru

$$f(x) \equiv 0 \pmod{p}, \tag{3}$$

kde p je prvočíslo. Zabývejme se tedy nejprve rovnicemi (3). Při jejich řešení je výhodné rovnici nejprve upravit pomocí následujících ekvivalentních úprav:

i) Kongruenční rovnice (3) je vždy ekvivalentní rovnici stupně nejvýše $p-1$. Důkaz vychází z důsledku malé Fermatovy věty: je-li p prvočíslo, pak platí $x^p \equiv x \pmod{p}$ pro každé $x \in \mathbb{Z}$.

Příklad. Rovnice $x^8 + 2x^7 + x^5 - x^4 - x + 3 \equiv 0 \pmod{5}$ je ekvivalentní rovnici $2x^3 + 3 \equiv 0 \pmod{5}$, neboť

$$x^5 \equiv x, \quad x^7 \equiv x^3, \quad x^8 \equiv x^4 \pmod{5}.$$

ii) Koeficienty $a_n, \ldots, a_0$ polynomu $f(x)$ lze nahradit prvky z příslušných tříd (mod p) s nejmenšími absolutními hodnotami. Rovnice tím nabude přehlednějšího tvaru.

Příklad. Rovnice

$$25x^3 + 17x^2 - 13 \equiv 0 \pmod{11}$$

je ekvivalentní rovnici

$$3x^3 - 5x^2 - 2 \equiv 0 \pmod{11},$$

neboť $25 \equiv 3$, $17 \equiv -5$, $-13 \equiv -2 \pmod{11}$.

iii) Je-li $(a_n, p) = 1$, pak k prvku $\overline{a}_n$ existuje v $\mathbb{Z}_p$ inverzní prvek $\overline{a}_n^{-1}$. Někdy je výhodné celou rovnici (3) vynásobit prvkem $\overline{a}_n^{-1}$, abychom dostali rovnici, v níž koeficient u nejvyšší mocniny x je roven 1.

Wilsonova věta

Ukažme, jak je možno elegantně dokázat Wilsonovu větu 2.18 pomocí řešení kongruenčních rovnic.

Dle Fermatovy věty pro $x \not\equiv 0 \pmod{p}$ platí $x^{p-1} \equiv 1 \pmod{p}$. Vynásobením prvkem x dostaneme $x^p \equiv x \pmod{p}$ pro *každé* $x \in \mathbb{Z}_p$, tj. tato kongruenční rovnice má v $\mathbb{Z}_p$ právě p řešení. Odtud

$$x^p - x = x \cdot (x - \overline{1}) \cdot \ldots \cdot (x - \overline{p-1}), \quad x^{p-1} - \overline{1} = (x - \overline{1}) \cdot \ldots \cdot (x - \overline{p-1}).$$

Dosazením $x = \overline{0}$ do poslední rovnosti obdržíme

$$-1 \equiv (-1)^{p-1} \cdot (p-1)! \pmod{p}.$$

Pro liché p je

$$-1 \equiv (p-1)! \pmod{p}, \tag{4}$$

pro $p = 2$ je $(p-1)! \equiv 1 \equiv -1 \pmod{p}$, celkem tedy formule (4) platí pro každé prvočíslo p. Kdyby číslo p bylo složené a d by byl vlastní dělitel čísla p, $0 < d < p$, platilo by $d|(p-1)!$, tedy $(p-1)! + 1 \equiv 1 \pmod{d}$, tj. $d \nmid (p-1)! + 1$ a $p \nmid (p-1)! + 1$. Pro složené číslo p tedy formule (4) neplatí. Celkem dostaneme

Věta 3.4. (Wilsonova) *Číslo $p > 1$ je prvočíslo, právě když* $-1 \equiv (p-1)! \pmod{p}$.

Cvičení

60. Zjednodušte následující kongruenční rovnice (snižte stupeň, zmenšete absolutní hodnoty koeficientů a koeficient u nejvyšší mocniny položte 1) a řešte metodou dosazovací:

    a) $28x^9 + 29x^8 - 26x^7 + 20x^4 - 17x + 23 \equiv 0 \pmod{3}$,

    b) $34x^{10} - 29x^7 + 43x^4 - 19x + 37 \equiv 0 \pmod{3}$,

    c) $75x^{13} - 62x^{12} - 53x^{11} - 24x^6 + 13x - 27 \equiv 0 \pmod{7}$.

61. Rozložte mnohočlen na součin činitelů v daném modulu:

    a) $x^3 + 3x^2 - 3$ v modulu 17,

    b) $x^3 + 11x^2 + 8x + 3$ v modulu 23,

    c) $x^3 - 13x^2 - 3x + 11$ v modulu 31.

62. Dokažte, že pro prvočísla $p = 4n + 1$ platí:

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \equiv 0 \pmod{p}$$

    a pro prvočísla $p = 4n + 3$ platí:

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 - 1 \equiv 0 \pmod{p}.$$

63. Dokažte, že pro prvočíslo p a libovolné celé číslo a platí $a^p + (p-1)!\, a \equiv 0 \pmod{p}$.

64. Dokažte Leibnizovo kritérium pro prvočísla: přirozené číslo $p > 2$ je prvočíslo, právě když platí $(p-2)! - 1 \equiv 0 \pmod{p}$.

Zabývejme se nyní otázkou počtu řešení rovnice (1), známe-li počty řešení rovnic v soustavě (2). Předpokládejme, že k-tá rovnice soustavy (2) má právě n_k řešení. Nechť $\overline{b}_i$ je libovolné řešení i-té rovnice. Pak soustava $x \equiv b_i \pmod{m_i}$, kde $m_i = p_i^{\alpha_i}$, má jediné řešení (viz čínská věta o zbytcích)

$$x \equiv x_0 = M_1 M_1^* b_1 + \ldots + M_k M_k^* b_k \pmod{m}$$

($M_i = \frac{M}{m_i}$, M_i^* je inverzní prvek k M_i v okruhu $\mathbb{Z}_{m_i}$), které je řešením rovnice (1).

Nechť dále b_i^* je také řešení i-té rovnice soustavy (2) a dále nechť

$$x^* \equiv x_0^* = M_1 M_1^* b_1^* + \ldots + M_k M_k^* b_k^* \pmod{m}$$

je odpovídající řešení rovnice (1). Předpokládejme, že jsou tato řešení stejná, tj. že platí $x \equiv x^* \pmod{m}$. Jelikož $m_i | m$, plyne odtud $x \equiv x^* \pmod{m_i}$, a to vzhledem k podmínce $M_k \equiv 0 \pmod{m_j}$ pro $j \neq k$ dává

$$M_i M_i^* b_i \equiv M_i M_i^* b_i^* \pmod{m_i}.$$

Ovšem $M_i M_i^* \equiv 1 \pmod{m_i}$, tedy $b_i \equiv b_i^* \pmod{m_i}$. Dokázali jsme tedy, že různé k-tice řešení rovnic (2) dávají různá řešení rovnice (1), tj. počet řešení rovnice (1) je právě $n_1 \cdot \ldots \cdot n_k$.

Příklad. Řešme rovnici $f(x) = 3x^3 + 6x^2 + x + 10 \equiv 0 \pmod{15}$.
Řešení: Rovnice je ekvivalentní soustavě $f(x) \equiv 0 \pmod{3}$, $f(x) \equiv 0 \pmod{5}$. První rovnice má řešení $x \equiv -1 \pmod{3}$, druhá má tři řešení $x \equiv 0, 1, 2 \pmod{5}$. Platí $M_1 = 5$, $M_2 = 3$, odkud pro M_1^*, M_2^* postupně dostaneme rovnice

$$\begin{aligned} M_1 M_1^* &\equiv 1 \pmod{3} \\ 5 M_1^* &\equiv 1 \pmod{3} \\ M_1^* &\equiv -1 \pmod{3}, \end{aligned}$$

$$\begin{aligned} M_2 M_2^* &\equiv 1 \pmod{5} \\ 3 M_2^* &\equiv 1 \pmod{5} \\ M_2^* &\equiv 2 \pmod{5}. \end{aligned}$$

Proto

$$x \equiv M_1 M_1^* b_1 + M_2 M_2^* b_2 = -5 b_1 + 6 b_2 \pmod{15},$$

tedy rovnice má řešení

$$\begin{aligned} x_1 &\equiv (-5) \cdot (-1) + 6 \cdot 0 = 5 \pmod{15} \\ x_2 &\equiv (-5) \cdot (-1) + 6 \cdot 1 = 11 \pmod{15} \\ x_3 &\equiv (-5) \cdot (-1) + 6 \cdot 2 = 2 \pmod{15}. \end{aligned}$$

Kongruenční rovnice n-tého stupně v modulu p^α

Fundamentální význam pro řešení obecných kongruenčních rovnic mají rovnice tvaru

$$f(x) \equiv 0 \pmod{p^\alpha}, \tag{1}$$

kde p je prvočíslo. Pro velké hodnoty p a α může být číslo p^α velké, proto metoda řešení rovnic (1) postupným dosazováním všech zbytkových tříd modulo p^α za x do polynomu $f(x)$ by nebyla efektivní.

Ukažme, jak je možno ze znalosti řešení rovnice

$$f(x) \equiv 0 \pmod{p} \tag{2}$$

hledat řešení rovnice (1). Je-li totiž nějaké $x \in \mathbb{Z}$ řešením rovnice (1), tím spíše bude i řešením rovnice (2). Buď tedy x_1 řešení rovnice (2), tj. $x \equiv x_1 \pmod{p}$, neboli $x = x_1 + pt_1$, $t_1 \in \mathbb{Z}$. Obecně ne pro všechny hodnoty t_1 je příslušné x řešením rovnice (1). Hledejme nyní ta $t_1 \in \mathbb{Z}$, která vyhovují rovnici

$$f(x) = f(x_1 + pt_1) \equiv 0 \pmod{p^2}.$$

Provedeme Taylorův rozvoj polynomu f rozvineme v bodě x_1, tj.

$$f(x_1 + pt_1) = f(x_1) + \frac{f'(x_1)}{1!}pt_1 + \frac{f''(x_1)}{2!}(pt_1)^2 + \ldots + \frac{f^{(k)}(x_1)}{k!}(pt_1)^k.$$

Snadno se ověří, že všechna čísla

$$\frac{f^{(i)}(x_1)}{i!} \in \mathbb{Z}, \quad \text{pro } i = 1, \ldots, k.$$

Je tedy

$$f(x_1 + pt_1) \equiv f(x_1) + f'(x_1)pt_1 \equiv 0 \pmod{p^2}. \tag{3}$$

Jelikož $f(x_1) \equiv 0 \pmod{p}$, tj. $p|f(x_1)$, dostaneme z (3)

$$f'(x_1)t_1 \equiv -\frac{f(x_1)}{p} \pmod{p}. \tag{4}$$

A) V nejobecnějším případě, kdy $p \nmid f'(x_1)$ (tj. $f'(x_1) \not\equiv 0 \pmod{p}$), má rovnice (4) jediné řešení $t_1 \equiv t' \pmod{p}$ neboli $t_1 = t' + pt_2$, $t_2 \in \mathbb{Z}$.

B) Platí-li v rovnici (4) $p|f'(x_1)$, pak mohou nastat dva případy:

   (i) pravá strana rovnice (4) není dělitelná p. V tomto případě rovnice (4) nemá řešení, a tedy žádné $x \equiv x_1 \pmod{p}$ nebude řešením (1).

   (ii) pravá strana rovnice (4) je dělitelná p. Pak rovnici (4) vyhovují všechna čísla $t_1 \in \mathbb{Z}$ a rovnice (4) má tedy právě p řešení.

V případě A) přejdeme dále k řešení rovnice

$$f(x) = f(x_2 + p^2t_2) \equiv 0 \pmod{p^3}.$$

Opětovným užitím Taylorova rozvoje polynomu f, tentokrát v bodě x_2, dostaneme

$$f(x_2) + p^2t_2f'(x_2) \equiv 0 \pmod{p^3},$$

a jelikož $p^2|f(x_2)$, platí

$$\frac{f(x_2)}{p^2} + t_2f'(x_2) \equiv 0 \pmod{p}. \tag{5}$$

Jelikož $x_1 \equiv x_2 \pmod{p}$, je $f'(x_1) \equiv f'(x_2) \pmod{p}$ (ověřte!). Ale dle předpokladu platí $f'(x_1) \not\equiv 0 \pmod{p}$, tedy také $f'(x_2) \not\equiv 0 \pmod{p}$. Rovnice (5) má tedy jediné řešení

$$t_2 = t_2' + pt_3, \quad t_3 \in \mathbb{Z}.$$

Dosazením za t_2 do vztahu pro x dostaneme

$$x = x_2 + p^2(t_2' + pt_3) = x_3 + p^3 t_3, \quad x \equiv x_3 \pmod{p^3},$$

kde $x_3 = x_2 + p^2 t_2'$.

Uvedený postup dále opakujeme až do příslušné mocniny p^α. Z uvedených úvah je také vidět, že v případě A) dává řešení rovnice (2) jediné řešení rovnice (1).

V případě B)(ii) dosazujeme postupně všechna řešení rovnice (4) do rovnice $f(x) \equiv 0 \pmod{p^3}$ a postupujeme dále stejně jako v případě A).

Příklad. Řešme rovnici $f(x) = 2x^4 + 5x - 1 \equiv 0 \pmod{27}$.

Řešení: Snadno ověříme dosazovací metodou, že rovnice $f(x) \equiv 0 \pmod{3}$ má jediné řešení

$$x \equiv 1 \pmod{3}, \quad x = 1 + 3t_1.$$

Přitom $f'(x) = 8x^3 + 5$, tedy $f'(1) = 13$ a $3 \nmid 13$, což odpovídá případu A). Dle výše uvedeného schématu dle (3) platí

$$f(1) + 3t_1 f'(1) \equiv 0 \pmod{9},$$

tj. $6 + 3t_1 \cdot 13 \equiv 0 \pmod{9}$, $13t_1 \equiv -2 \pmod{3}$, $t_1 \equiv -2 + 3t_2$.

Dosazením za t_1 do vztahu pro x dostaneme

$$x = -5 + 9t_2, \quad x_2 = -5,$$

a tedy

$$f(-5) + 9t_2 \cdot f'(-5) \equiv 0 \pmod{27},$$

$$1224 + 9t_2 \cdot (-995) \equiv 0 \pmod{27},$$

$$t_2 \equiv -1 \pmod{3}, \quad t_2 = -1 + 3t_3,$$

což opětovným dosazením do x dává

$$x = -14 + 27t_3, \quad x \equiv 13 \pmod{27}.$$

Cvičení

65. Řešte kongruence:

    a) $5x^4 + 2x^3 - x + 17 \equiv 0 \pmod{21}$,
    b) $5x^3 - 7x^2 + 3x + 11 \equiv 0 \pmod{33}$,
    c) $2x^2 - 7x + 6 \equiv 0 \pmod{55}$,
    d) $4x^3 - 5x^2 + 7x + 21 \equiv 0 \pmod{105}$,
    e) $3x^2 + 7x + 5 \equiv 0 \pmod{34}$.

66. Řešte kongruence prvního stupně vyšetřením systému rovnic jim ekvivalentních:

    a) $43x \equiv 59 \pmod{112}$,
    b) $37x \equiv 162 \pmod{245}$,
    c) $23x \equiv 11 \pmod{153}$.

67. Řešte kongruence:

    a) $x^2 \equiv 19 \pmod{25}$,
    b) $x^2 \equiv 29 \pmod{49}$,
    c) $x^2 \equiv 31 \pmod{121}$,
    d) $x^2 \equiv 82 \pmod{169}$.

68. Dokažte, že pro žádné celé číslo x výraz $x^2 + 3x + 5$ není dělitelný číslem 121.
69. Řešte kongruence:

    a) $2x^3 + x + 12 \equiv 0 \pmod{25}$,
    b) $4x^3 + 7x + 1 \equiv 0 \pmod{25}$,
    c) $3x^3 - 2x^2 - 2x - 21 \equiv 0 \pmod{49}$,
    d) $5x^3 + 4x^2 - 6x + 5 \equiv 0 \pmod{49}$.

70. Řešte kongruenci
$$2x^3 - 5x - 32 \equiv 0 \pmod{175}.$$

Kapitola 4

Struktura multiplikativních grup okruhů $\mathbb{Z}_m$ a jejich užití

4.1 Obecné vlastnosti grup $\mathbb{Z}_m^*$ a primitivní kořeny

Pro unitární okruh $\mathcal{R} = (R, +, \cdot, 0, 1)$ označme R^* množinu všech jeho invertibilních prvků, tj.

$$R^* = \{x \in R; \exists x^{-1} \in R \colon xx^{-1} = x^{-1}x = 1\}.$$

Snadno se vidí, že $(R^*, \cdot)$ je grupa – tzv. *multiplikativní grupa okruhu* $\mathcal{R}$.

V této kapitole se budeme zabývat strukturou grup $\mathbb{Z}_m^*$ pro $m \in \mathbb{N}$. Získané výsledky později využijeme při řešení některých typů kongruenčních rovnic.

Jsou-li $\mathcal{R}_i = (R_i, +_i, \cdot_i, 0_i)$ okruhy pro $i = 1, \ldots, n$, lze na kartézském součinu množin $\prod R_i$ zavést binární operace $\oplus$ a $\odot$ formulemi

$$(r_1, \ldots, r_n) \oplus (r_1', \cdots, r_n') = (r_1 +_1 r_1', \cdot, r_n +_n r_n'),$$
$$(r_1, \ldots, r_n) \odot (r_1', \cdots, r_n') = (r_1 \cdot_1 r_1', \cdot, r_n \cdot_n r_n'),$$

tj. operace jsou na množině $\prod R_i$ definovány „po složkách“. Vzhledem k těmto operacím je struktura $\prod \mathcal{R}_i = (\prod R_i, \oplus, \odot, \mathbf{0})$ okruhem s nulovým prvkem $\mathbf{0} = (0_1, \ldots, 0_n)$ a nazývá se *direktní součin okruhů* $\mathcal{R}_1, \ldots, \mathcal{R}_n$. Jsou-li navíc 1_i jednotkové prvky okruhů $\mathcal{R}_i$, je $\mathbf{1} = (1_1, \ldots, 1_n)$ jednotkovým prvkem okruhu $\prod \mathcal{R}_i$. Z důvodu stručnosti značení zaveďme úmluvu, že budeme operace ve všech okruzích $\mathcal{R}_i$ a $\prod \mathcal{R}_i$ značit stejně, a to symboly $+, \cdot$, a 0. Na čtenáři ponecháme důkaz následujícího jednoduchého tvrzení:

Věta 4.1. *Platí* $\prod \mathcal{R}_i^* = (\prod \mathcal{R}_i)^*$.

Buďte nyní $m_1, \ldots, m_t$ po dvou nesoudělná přirozená čísla. Označme $I(m_i)$ ideál v $\mathbb{Z}$ generovaný prvkem m_i. Označme dále $\psi_i \colon \mathbb{Z} \to \mathbb{Z}/I(m_i) = \mathbb{Z}_{m_i}$ přirozený homomorfismus okruhu $\mathbb{Z}$ do okruhu $\mathbb{Z}_{m_i}$, tj.

$$\psi_i(x) = \overline{x} = x + I(m_i), \quad x \in \mathbb{Z}.$$

Definujme dále zobrazení $\psi \colon \mathbb{Z} \to \prod \mathbb{Z}_{m_i}$ předpisem

$$\psi(n) = (\psi_1(n), \ldots, \psi_t(n)), \quad n \in \mathbb{Z}.$$

Snadno se ověří, že ψ je okruhový homomorfismus. Zkoumejme, zda je ψ surjekce: nechť $(\overline{b}_1, \ldots, \overline{b}_t) \in \prod \mathbb{Z}_{m_i}$ je libovolný prvek. Má-li pro některé $n \in \mathbb{Z}$ platit $\psi(n) = (\overline{b}_1, \ldots, \overline{b}_t)$, pak $\psi_i(n) = \overline{b}_i$, tedy

$$n \equiv b_i \pmod{m_i}.$$

Čínská věta o zbytcích garantuje, že v případě po dvou nesoudělných modulů m_i takové $n \in \mathbb{Z}$ pro zadané hodnoty b_i existuje. Tedy ψ je surjekce.

Určíme jádro homomorfismu $\operatorname{Ker} \psi$. Nechť pro $n \in \mathbb{Z}$ je $\psi(n) = (\overline{0}, \ldots, \overline{0})$. Pak $n \equiv 0 \pmod{m_i}$ a vzhledem k nesoudělnosti modulů m_i odtud plyne $n \equiv 0 \pmod{m}$ pro $m = m_1 \cdot \ldots \cdot m_t$. To ale znamená, že $n \in I(m)$ a $\operatorname{Ker} \psi = I(m)$.

Z věty o homomorfismu okruhů odtud plyne izomorfismus

$$\mathbb{Z}/\operatorname{Ker} \psi = \mathbb{Z}_m \cong \prod \mathbb{Z}_{m_i}.$$

Z věty 4.1 pak dále dostaneme následující tvrzení.

Věta 4.2. $\mathbb{Z}_m^* \cong \prod \mathbb{Z}_{m_i}^*$.

Buď nyní $m = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$ kanonický rozklad čísla m. Dle tvrzení 4.2 platí $\mathbb{Z}_m^* \cong \prod \mathbb{Z}_{p_i^{\alpha_i}}^*$, a tedy struktura grupy $\mathbb{Z}_m^*$ je plně určena strukturami grup $\mathbb{Z}_{p_i^{\alpha_i}}^*$. Budeme tedy dále studovat pouze grupy tohoto typu.

Struktura grup $\mathbb{Z}_{p_i^{\alpha_i}}^*$

Budeme se zabývat zejména otázkou, které z uvažovaných grup budou cyklické. Uvažujeme-li např. grupu $(\mathbb{Z}/I(5))^* = \mathbb{Z}_5^*$, pak vzhledem k tomu, že $\mathbb{Z}_5$ je těleso, bude platit

$$\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

Grupa $\mathbb{Z}_5^*$ je cyklická, přičemž každý z prvků $\overline{2}$, $\overline{3}$ je jejím generátorem. Obecně platí, že je-li p prvočíslo, pak je $\mathbb{Z}_p$ těleso a $|\mathbb{Z}_p^*| = p - 1$. Víme již také, že prvek $\overline{a}$ je invertibilní v $\mathbb{Z}_m$ právě tehdy když $(a, m) = 1$. Takových prvků je právě $\phi(m)$, a tedy řád grupy $\mathbb{Z}_m^*$ je právě $\phi(m)$.

Jak je známo ze základního kurzu algebry, konečná grupa je cyklická, právě když obsahuje prvek řádu rovného řádu uvažované grupy. Prvek $\overline{a}$ je tedy generátorem grupy $\mathbb{Z}_m^*$ právě když jeho řád je roven $\phi(m)$, tj. právě když $n = \phi(m)$ je nejmenší přirozené číslo vlastnosti $\overline{a}^n = \overline{1} \pmod m$. Navíc pak bude platit

$$\mathbb{Z}_m^* = \{\overline{a}^0, \overline{a}^1, \ldots, \overline{a}^{n-1}\};$$

prvek $\overline{a}$ přitom nazýváme *primitivní kořen modulo* m.

Zabývejme se tedy otázkou, ve kterých grupách $\mathbb{Z}_m^*$ budou existovat primitivní kořeny.

Příklad. Zvolíme-li $m = 8$, pak $\phi(8) = 4$, $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Přitom platí $\overline{3}^2 = \overline{1}$, $\overline{5}^2 = \overline{1}$, $\overline{7}^2 = \overline{1}$, tedy prvky $\overline{3}$, $\overline{5}$, $\overline{7}$ jsou řádu 2. Grupa $\mathbb{Z}_8^*$ tedy nemá prvek řádu 4 a není tedy cyklická.

Věta 4.3. *Buď p prvočíslo a $1 \leq k < p$. Pak $p \Big| \binom{p}{k}$.*

Důkaz: Zřejmě $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, tedy $p! = k!(p-k)!\binom{p}{k}$. Dále $p|p!$, $p \nmid k!(p-k)!$, tedy $p \Big| \binom{p}{k}$, neboť p je prvočíslo. □

Věta 4.4. *Je-li $l \geq 1$, $a \equiv b \pmod{p^l}$, pak $a^p \equiv b^p \pmod{p^{l+1}}$.*

Důkaz: Podmínku $a \equiv b \pmod{p^l}$ lze přepsat do tvaru $a = b + cp^l$, $c \in \mathbb{Z}$. Z binomické věty dostaneme

$$a^p = b^p + \binom{p}{1} b^{p-1} cp^l + A,$$

kde $A \in \mathbb{Z}$ a $p^{l+2}|A$. Přitom $p^{l+1} \Big| \binom{p}{1} b^{p-1} cp^l$, tedy $a^p \equiv b^p \pmod{p^{l+1}}$. □

Věta 4.5. *Je-li $l \geq 2, p \neq 2$, pak pro $a \in \mathbb{Z}$ je*

$$(1 + ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \pmod{p^l}.$$

Důkaz: Pro $l = 2$ tvrzení evidentně platí. Předpokládejme jeho platnost pro $l \geq 2$ a dokažme platnost pro $l + 1$. Dle předchozí věty je

$$\left[(1 + ap)^{p^{l-2}}\right]^p \equiv \left(1 + ap^{l-1}\right)^p \pmod{p^{l+1}}.$$

Z binomické věty dostaneme

$$\left(1 + ap^{l-1}\right)^p = 1 + \binom{p}{1} ap^{l-1} + B,$$

kde $B = \sum_{k=2}^{p} \binom{p}{k} (ap^{l-1})^k$. Z věty 4.3 máme $p \Big| \binom{p}{k}$ pro každé $p \neq k$. Je tedy k-tý člen v sumě B pro $k \neq p$ dělitelný $p^{k(l-1)+1}$ a každý z nich je dělitelný alespoň

členem $p^{2(l-1)+1}$ (pro $k=2$). Jelikož $l \geq 2$, platí $1+2(l-1) \geq l+1$. Poslední člen v B je roven $a^p p^{p(l-1)}$. Pro $p \geq 3$ ale platí $p(l-1) \geq l+1$. Celkem tedy $p^{l+1}|B$, odkud

$$(1+ap)^{p^{l-1}} \equiv 1 + ap^l \pmod{p^{l+1}}.$$

□

Jako důsledek pak dostáváme následující větu.

Věta 4.6. *Je-li $p \neq 2$, $(a,p)=1$, pak p^{l-1} je řád prvku $1+ap$ v grupě $\mathbb{Z}^*_{p^l}$.*

Důkaz: Dle věty 4.5 platí $(1+ap)^{p^{l-1}} \equiv 1 + ap^l \pmod{p^{l+1}}$, odkud

$$(1+ap)^{p^{l-1}} \equiv 1 \pmod{p^l}.$$

Je tedy řád prvku $1+ap$ dělitelný p^{l-1}. Na druhé straně ovšem z $(a,p)=1$ platí

$$(1+ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \not\equiv 1 \pmod{p^l},$$

tedy žádný vlastní dělitel prvku p^{l-1} nemůže být jeho řádem. □

Věta 4.7. *Je-li p liché prvočíslo, $l \in \mathbb{N}$, pak existují primitivní kořeny modulo p^l.*

Důkaz: Pro $l=1$ je $\mathbb{Z}_p$ těleso. Je známo, že multiplikativní grupy konečných těles jsou cyklické a existuje tedy primitivní kořen $g \pmod p$.

Primitivním kořenem (mod p) bude také číslo $g+p$. Kdyby $g^{p-1} \equiv 1 \pmod{p^2}$, pak by

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p \pmod{p^2}.$$

Jelikož $p^2 \nmid (p-1)g^{p-2}p$ (jinak by platilo $p|g^{p-2}$, a tedy $g^{p-2} \equiv 0 \pmod p$ a $g^{p-1} \equiv 0 \pmod{p^2}$, což je spor s $g^{p-1} \equiv 1 \pmod{p^2}$), odkud $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$. Lze tedy předpokládat, že g je primitivní kořen modulo p vlastnosti $g^{p-1} \not\equiv 1 \pmod{p^2}$ (v opačném případě bychom místo prvku g vzali primitivní kořen $g+p$).

Ukažme, že prvek g je je pak již primitivním kořenem modulo p^l pro každé $l \in \mathbb{N}$. K tomu je třeba dokázat, že platí-li $g^n \equiv 1 \pmod{p^l}$ pro některé $n \in \mathbb{N}$, pak $\phi(p^l) = p^{l-1}(p-1)|n$ (tj. že n je násobek řádu grupy $\mathbb{Z}^*_{p^l}$).

Z podmínky $g^{p-1} \equiv 1 \pmod p$ plyne, že $g^{p-1} = 1 + ap$ pro některé $a \in \mathbb{Z}$, a jelikož $g^{p-1} \not\equiv 1 \pmod{p^2}$, máme $(a,p)=1$ a $p \nmid a$. Díky důsledku 4.6 je p^{l-1} řád prvku $1+ap \pmod{p^l}$. Zřejmě

$$(1+ap)^n \equiv (g^{p-1})^n \equiv (g^n)^{p-1} \equiv 1 \pmod{p^l},$$

platí tedy $p^{l-1}|n$.

Položme $n = p^{l-1}n'$. Pak z $g^p \equiv g \pmod p$ plyne $g^{p^{l-1}} \equiv g \pmod p$ a

$$g^n \equiv (g^{p^{l-1}})^{n'} \equiv g^{n'} \equiv 1 \pmod p.$$

Vzhledem k tomu, že g je primitivní kořen modulo p (a tedy řád prvku $g \pmod p$ je $\phi(p) = p-1$), platí $p-1|n'$ a celkem $p^{l-1}(p-1)|n$. □

Předchozí tvrzení platí pouze pro lichá prvočísla. Podívejme se nyní na existenci primitivních kořenů modulo 2^l pro $l \geq 2$.

Věta 4.8. *Primitivní kořeny* $\pmod{2^l}$ *existují pouze pro* $l = 1, 2$, *pro* $l \geq 3$ *neexistují. Je-li* $l \geq 3$, *pak množina* $\{(-1)^a \cdot 5^b; a \in \{0,1\}, 0 \leq b < 2^{l-2}\}$ *tvoří redukovaný systém zbytků* $\pmod{2^l}$, *a tedy grupa* $\mathbb{Z}^*_{2^l}$ *je direktním součinem dvou cyklických grup, jedné řádu* 2 *a druhé řádu* 2^{l-2}.

Důkaz: Snadno se ověří, že 1, resp. 3 je primitivní kořen (mod 2), resp. (mod 4).

Předpokládejme, že $l \geq 3$. Dokážeme, že

$$5^{2^{l-3}} \equiv 1 + 2^{l-1} \pmod{2^l}. \tag{1}$$

Pro $l = 3$ tvrzení zřejmě platí. Postupujme dále matematickou indukcí, tj. předpokládejme platnost (1) pro l a dokažme pro $l+1$. Aplikací věty 4.4. dostaneme

$$(5^{2^{l-3}})^2 = 5^{2^{l-2}} \equiv (1 + 2^{l-1})^2 \pmod{2^{l+1}}.$$

Ovšem

$$\left(1 + 2^{l-1}\right)^2 = 1 + 2^l + 2^{2l-2}$$

a pro $l \geq 3$ je $2l - 2 \geq l + 1$, tedy $(1 + 2^{l-1})^2 \equiv 1 + 2^l \pmod{2^{l+1}}$ a celkem

$$5^{2^{l-2}} \equiv 1 + 2^l \pmod{2^{l+1}}. \tag{2}$$

Tím je formule (1) dokázána.

Ze vztahu (2) ihned plyne kongruence $5^{2^{l-2}} \equiv 1 \pmod{2^l}$, z (1) pak $5^{2^{l-3}} \not\equiv 1 \pmod{2^l}$. To znamená, že 2^{l-2} je řád čísla 5 $\pmod{2^l}$.

Uvažujme nyní množinu $A = \{(-1)^a \cdot 5^b; a \in \{0,1\}, 0 \leq b < 2^{l-2}\}$ mající 2^{l-1} prvků. Ukažme, že žádné dva z nich nejsou kongruentní $\pmod{2^l}$. Kdyby totiž $(-1)^a \cdot 5^b \equiv (-1)^{a'} \cdot 5^{b'} \pmod{2^l}$, $l \geq 3$, pak by $(-1)^a \equiv (-1)^{a'} \pmod 4$, odkud $a \equiv a' \pmod 2$.

Je tedy $a = a'$, neboť $a \in \{0,1\}$. Z $a = a'$ plyne $5^b \equiv 5^{b'} \pmod{2^l}$. Jelikož 2^{l-2} je řád 5 $\pmod{2^l}$, je $b \equiv b' \pmod{2^{l-2}}$, odkud $b = b'$, neboť $0 \leq b, b' < 2^{l-2}$.

Dokázali jsme tedy, že množina A je redukovaný systém zbytků $\pmod{2^l}$. K dokončení důkazu stačí ověřit, že v A není prvek řádu $\phi(2^l) = 2^l - 2^{l-1} = 2^{l-1}$. Zřejmě $((-1)^a \cdot 5^b)^{2^{l-2}} = (-1)^{a \cdot 2^{l-2}} \cdot (5^{2^{l-2}})^b = (5^{2^{l-2}})^b \equiv 1^b = 1 \pmod{2^l}$, tedy řády prvků z A jsou nejvýše rovny 2^{l-2}, čímž je důkaz hotov. □

Předchozí tvrzení dávají úplnou odpověď na otázku struktury grup $\mathbb{Z}^*_m$:

Věta 4.9. *Nechť* $m = 2^a \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_l^{\alpha_l}$ *je kanonický rozklad čísla* m. *Pak*

$$\mathbb{Z}^*_m \cong \mathbb{Z}^*_{2^a} \times \prod \mathbb{Z}^*_{p_i^{\alpha_i}}.$$

Grupy $\mathbb{Z}^*_{p_i^{\alpha_i}}$ jsou přitom cyklické řádů $p_i^{\alpha_i-1}(p_i-1)$, grupa $\mathbb{Z}^*_{2^a}$ je cyklická grupa řádu 1 nebo 2 pro $a=1$ nebo $a=2$, pro $a\geq 3$ je direktním součinem dvou cyklických grup, jedné řádu 2, druhé řádu 2^{a-2}.

Jako bezprostřední důsledek dostaneme, které moduly mají primitivní kořeny:

Věta 4.10. *Primitivní kořeny* $(\mathrm{mod}\ m)$ *existují právě pro* $m=2,4,p^a$ *a* $2p^a$, *kde* $a\in\mathbb{N}$ *a* p *je liché prvočíslo.*

Důkaz: Dle tvrzení 4.8 je $m\neq 2^l$ pro $l\geq 3$. Není-li m žádného z uvažovaných tvarů, pak $m=m_1\cdot m_2$, $(m_1,m_2)=1$ a $m_1,m_2>2$. V tom případě jsou čísla $\phi(m_1)$ a $\phi(m_2)$ sudá a platí $\mathbb{Z}^*_m\cong\mathbb{Z}^*_{m_1}\times\mathbb{Z}^*_{m_2}$. Obě grupy $\mathbb{Z}^*_{m_1},\mathbb{Z}^*_{m_2}$ obsahují prvky řádu 2 (grupy jsou sudých řádů a lze dokázat, že pro každého prvočíselného dělitele q řádu konečné grupy existuje v této grupě prvek řádu q). Jsou-li to prvky a_1,a_2, pak prvky $(a_1,1),(1,a_2)\in\mathbb{Z}^*_m$ jsou navzájem různé prvky řádu 2. Cyklická grupa ovšem nemůže mít dva různé prvky řádu 2 (je-li G cyklická grupa řádu $2l$ a g je její generátor, pak $G=\{g^0,\ldots,g^{2l-1}\}$; nechť $a=g^k$, $b=g^j$, $0\leq k$, $j\leq 2l-1$ jsou prvky řádu 2 v G. Pak $g^{2k}=g^{2j}=1$ implikuje $2l|2k$, $2l|2j$, odkud $l|k$, $l|j$, což vzhledem k volbě k,j znamená $k=j=l$, tedy $a=b$), tedy grupa $\mathbb{Z}^*_m$ není cyklická. Máme již dokázáno, že $2,4,p^a$ mají primitivní kořeny. Jelikož

$$\mathbb{Z}^*_{2p^a}\cong\mathbb{Z}^*_2\times\mathbb{Z}^*_{p^a}\cong\mathbb{Z}^*_{p^a},$$

je grupa $\mathbb{Z}^*_{2p^a}$ cyklická a existují tedy i primitivní kořeny $(\mathrm{mod}\ 2p^a)$. □

Cvičení

71. Určete řád prvku a v modulu m. Je a primitivní kořen v modulu m?
    a) $3,17$, b) $3,19$, c) $4,21$, d) $5,18$, e) $5,23$, f) $7,24$.
    Je a primitivní kořen v modulu m?
72. a) Víte-li, že 12 je řádu 6 v modulu 19, najděte řády prvků 12^3, 12^4, 12^5 v tomto modulu.
    b) Víte-li, že 6 je primitivní kořen v modulu 41, najděte řády prvků 6^{12}, 6^{15}, 6^{16} v tomto modulu.
73. Víte-li, že pro dva navzájem nesoudělné moduly m_1 a m_2 číslo a je řádu δ_1 a δ_2, najděte řád δ prvku a v modulu m_1m_2.
74. Najděte řády pro:
    a) 2 v modulu 35,
    b) 3 v modulu 35
    užitím vlastností vyplývající z předchozích cvičení a nezávisle na nich.
75. Najděte počet tříd primitivních kořenů v modulech:
    a) 17, b) 43, c) 73, d) 89.
76. Najděte počet tříd řádu:
    a) 7 v modulu 29,
    b) 9 v modulu 37.

4.2 Indexy prvků, jejich vlastnosti a užití

Vlastnosti primitivních kořenů umožňují zavést v teorii čísel důležitý pojem, který je analogický pojmu logaritmu.

Je-li g primitivní kořen (mod m), pak $\phi(m)$ je řád prvku g v grupě $\mathbb{Z}_m^*$, tj.

$$g^0, g^1, \ldots, g^{\phi(m)-1} \tag{1}$$

je redukovaný systém zbytků (mod m). Odtud plyne, že pro každé $a \in \mathbb{Z}$, $(a, m) = 1$, existuje jediné γ, $0 \leq \gamma \leq \phi(m) - 1$ tak, že

$$a \equiv g^\gamma \pmod{m}. \tag{2}$$

Číslo γ nazýváme *index prvku a modulo m* pro primitivní kořen g a značíme $\operatorname{ind}_g a$. Je-li zřejmé, který primitivní kořen g uvažujeme, píšeme jen $\operatorname{ind} a$.

Příklad. Pro $m = 7$ je $\mathbb{Z}_7^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$, $g = 3$ je primitivní kořen (mod 7), indexy pro $g = 3$ jsou postupně 0, 2, 1, 4, 5, 3.

Jsou-li $\gamma_1, \gamma_2 \in \mathbb{N}_0$ taková čísla, že $g^{\gamma_1} \equiv g^{\gamma_2} \pmod{m}$, pak pro $\gamma_1 - \gamma_2 \geq 0$ je

$$g^{\gamma_1 - \gamma_2} \equiv 1 \pmod{m}.$$

Jelikož $\phi(m)$ je řád prvku g, platí $\phi(m) | \gamma_1 - \gamma_2$, tedy $\gamma_1 \equiv \gamma_2 \pmod{\phi(m)}$. Odtud tedy plyne, že $a \equiv b \pmod{m}$ implikuje $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{\phi(m)}$. Obrácená implikace se dokáže analogicky, celkem tedy platí

$$a \equiv b \pmod{m} \iff \operatorname{ind} a = \operatorname{ind} b \pmod{\phi(m)}. \tag{3}$$

Příklad. Pro $m = 7$ je $\operatorname{ind}_3 6 = 3$. Z kongruencí $55 \equiv 27 \equiv 6 \pmod{7}$ plyne

$$\operatorname{ind}_3 55 \equiv \operatorname{ind}_3 27 \equiv \operatorname{ind}_3 6 \equiv 3 \pmod{6}.$$

Ukažme, že indexy mají podobné vlastnosti jako logaritmy.

Vlastnosti indexů

Platí

$$\operatorname{ind}(a_1 \cdot \ldots \cdot a_n) \equiv \operatorname{ind} a_1 + \ldots \operatorname{ind} a_n \pmod{\phi(m)} \tag{4}$$

Důkaz: Zřejmě máme $a_i \equiv g^{\operatorname{ind} a_i} \pmod{m}$, proto

$$g^{\operatorname{ind}(a_1 \cdot \ldots \cdot a_n)} \equiv a_1 \cdot \ldots \cdot a_n \equiv g^{\sum \operatorname{ind} a_i} \pmod{m},$$

odkud z vlastnosti (3) plyne

$$\operatorname{ind}(a_1 \cdot \ldots \cdot a_n) \equiv \operatorname{ind} a_1 + \ldots \operatorname{ind} a_n \pmod{\phi(m)}.$$

Vlastnost (4) má zřejmý důsledek:

$$\operatorname{ind} a^n \equiv n \cdot \operatorname{ind} a \pmod{\phi(m)}. \tag{5}$$

Tabulky indexů

K tomu, abychom mohli prakticky pro dané $a \in \mathbb{Z}$ a pro daný primitivní kořen $g \pmod m$ najít hodnotu $\operatorname{ind}_g a$ a zpátky k danému indexu najít odpovídající číslo, jsou sestaveny tzv. *tabulky indexů*.

Příklad. Pro $m = 37$ a $g = 2$ vypadá tabulka indexů takto:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Z tabulky vyčteme , že např. $\operatorname{ind}_2 23 \equiv 15 \pmod{36}$, odkud $23 \equiv 2^{15} \pmod{37}$. Zpátky, je-li $\operatorname{ind}_2 x = 18$, pak $x \equiv 36 \pmod{37}$.

Tabulky indexů pro prvočísla menší než 89 jsou uvedeny v příloze na konci skripta.

Cvičení

77. Víte-li, že 6 je primitivním kořenem v modulu 13, sestavte při základu 6 tabulku indexů v modulu 13.
78. Víte-li, že 5 je primitivním kořenem v modulu 18, sestavte při základu 5 tabulku indexů v modulu 18.
79. Dokažte, že pro lichý prvočíselný modul p platí:
$$\operatorname{ind}(-1) \equiv \operatorname{ind}(p-1) \equiv \frac{p-1}{2} \pmod{p-1}.$$
80. Víte-li, že v modulu 71 je $\operatorname{ind}_7 66 \equiv 63 \pmod{70}$, najděte v tomto modulu $\operatorname{ind}_{13} 66$ (13 je primitivní kořen v modulu 71).

Užití indexů k řešení kongruenčních rovnic

1. Řešení binomických kongruenčních rovnic

Zabývejme se rovnicemi ve tvaru

$$a \cdot x^n \equiv b \pmod m, \quad (m, a) = 1. \tag{1}$$

Budeme řešit rovnice (1) pouze pro případ, kdy existují primitivní kořeny (mod m). Aplikujeme-li na rovnici (1) vlastnosti indexů (3), (4), (5), dostaneme

$$\operatorname{ind} a + n \cdot \operatorname{ind} x \equiv \operatorname{ind} b \pmod{\phi(m)},$$

odkud

$$n \cdot \operatorname{ind} x \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{\phi(m)}. \tag{2}$$

Rovnice (2) je lineární kongruenční rovnice vzhledem k $\operatorname{ind} x$ a v tabulkách indexů nalezneme příslušná x. Mohou nastat následující případy:

1) $(n, \phi(m)) = 1$. Pak má rovnice (2) vzhledem k $\operatorname{ind} x$ jediné řešení, tedy rovnice (1) má *jediné řešení* vzhledem k x;

2) $(n, \phi(m)) = d > 1$. Pak mohou nastat možnosti:

   a) $d \nmid (\operatorname{ind} b - \operatorname{ind} a)$; pak rovnice (2) nemá řešení, a tedy ani rovnice (1) *nemá řešení*;

   b) $d | (\operatorname{ind} b - \operatorname{ind} a)$; pak z rovnice (2) dostaneme

$$\frac{n}{d} \cdot \operatorname{ind} x \equiv \frac{\operatorname{ind} b - \operatorname{ind} a}{d} \quad \left(\mathrm{mod}\ \frac{\phi(m)}{d}\right).$$

   Tato rovnice má jediné řešení v modulu $\frac{\phi(m)}{d}$ a v modulu $\phi(m)$ má právě d řešení, tedy i rovnice (1) má *právě d řešení.*

Příklad. Řešme rovnici $x^3 \equiv 34 \pmod{41}$.
Řešení:

$$\begin{aligned} 3 \cdot \operatorname{ind} x &\equiv \operatorname{ind} 34 \pmod{40} \\ 3 \cdot \operatorname{ind} x &\equiv 19 \pmod{40} \\ \operatorname{ind} x &\equiv 33 \pmod{40}. \end{aligned}$$

Z tabulek indexů zjistíme $x \equiv 17 \pmod{41}$.

Příklad. Řešme rovnici $39x^{21} \equiv 53 \pmod{73}$.
Řešení:

$$\begin{aligned} \operatorname{ind} 39 + 21 \cdot \operatorname{ind} x &\equiv \operatorname{ind} 53 \pmod{72} \\ 21 \cdot \operatorname{ind} x &\equiv \operatorname{ind} 53 - \operatorname{ind} 39 = 53 - 65 = -12 \pmod{72} \\ \operatorname{ind} x &\equiv -4 \pmod{24} \\ \operatorname{ind} x &\equiv 20, 44, 68 \pmod{72} \\ x &\equiv 18, 71, 57 \pmod{73} \end{aligned}$$

Kritérium řešitelnosti rovnice $x^n \equiv a \pmod m$

Z rovnice $x^n \equiv a \pmod m$ plyne

$$n \cdot \operatorname{ind} x \equiv \operatorname{ind} a \pmod{\phi(m)}.$$

Je-li $(n, \phi(m)) = d$, pak je poslední rovnice vzhledem k $\operatorname{ind} x$ řešitelná, právě když $d | \operatorname{ind} a$, tj.

$$\operatorname{ind} a \equiv 0 \pmod d. \tag{1}$$

Vyjádříme podmínku (1) v závislosti na číslech m, d. Rovnost (1) vynásobíme číslem $\frac{\phi(m)}{d}$, tj. dostaneme

$$\frac{\phi(m)}{d} \cdot \operatorname{ind} a \equiv 0 \pmod{\phi(m)},$$

odkud

$$\operatorname{ind} a^{\frac{\phi(m)}{d}} \equiv 0 \pmod{\phi(m)},$$

tedy

$$a^{\frac{\phi(m)}{d}} \equiv 1 \pmod m. \tag{2}$$

Podmínka (2) je nutnou a postačující podmínkou řešitelnosti rovnice (1). Pro případ $n = 2$ a m liché prvočíslo, dostaneme známé Eulerovo kritérium pro kvadratické zbytky.

2. Řešení exponenciálních rovnic

Uvažujme rovnice ve tvaru

$$a^x \equiv b \pmod m.$$

Přechodem k indexům dostaneme

$$x \cdot \operatorname{ind} a \equiv \operatorname{ind} b \pmod{\phi(m)}.$$

Tato rovnice (a tedy i původní) je řešitelná právě když pro $d = (\operatorname{ind} a, \phi(m))$ platí $d | \operatorname{ind} b$.

Příklad. Řešme rovnici $5^x \equiv 17 \pmod{31}$.
Řešení: Dostaneme

$$x \cdot \operatorname{ind} 5 \equiv \operatorname{ind} 17 \pmod{30},$$

$$20x \equiv 7 \pmod{30}.$$

Protože $d = (20, 30) = 10$, $10 \nmid 7$, rovnice není řešitelná.

Příklad. Řešme rovnici $11^x \equiv 17 \pmod{31}$.
Řešení: Dostaneme

$$\begin{aligned} x \cdot \operatorname{ind} 11 &\equiv \operatorname{ind} 17 \pmod{30} \\ 23x &\equiv 7 \pmod{30} \\ x &\equiv -1 \pmod{30}. \end{aligned}$$

Zabývejme se nyní ještě otázkou počtu primitivnich kořenů (pokud existují) (mod m). Pro $a \in \mathbb{Z}$, $(a, m) = 1$, označme $\delta(a)$ řád prvku $\overline{a}$ v grupě $\mathbb{Z}_m^*$.

Věta 4.11. *Řád prvku $\delta(a)$ je definován rovností*

$$(\operatorname{ind} a, \phi(m)) = \frac{\phi(m)}{\delta(a)};$$

speciálně tedy a je primitivní kořen (mod m) *právě když* $(\operatorname{ind} a, \phi(m)) = 1$. *V redukované soustavě zbytků* (mod m) *existuje tedy právě $\phi(\phi(m))$ primitivních kořenů.*

Důkaz: Zřejmě $\delta(a)$ je nejmenší přirozené číslo vlastnosti $a^{\delta(a)} \equiv 1 \pmod{m}$. Tato podmínka je ekvivalentní s rovností

$$\delta(a) \cdot \operatorname{ind} a \equiv 0 \pmod{\phi(m)} \quad \text{nebo} \quad \operatorname{ind} a \equiv 0 \left(\mod \frac{\phi(m)}{\delta(a)}\right).$$

To znamená, že $\delta(a)$ je nejmenší dělitel $\phi(m)$, pro který $\frac{\phi(m)}{\delta(a)}$ dělí $\operatorname{ind} a$, neboli $\frac{\phi(m)}{\delta(a)}$ je největší dělitel $\phi(m)$, dělící $\operatorname{ind} a$. Celkem tedy $(\operatorname{ind} a, \phi(m)) = \frac{\phi(m)}{\delta(a)}$.

Indexy redukované soustavy zbytků (mod m) jsou prvky množiny $\operatorname{ind} a \in \in \{0, 1, \ldots, \phi(m) - 1\}$. Tedy z podmínky pro primitivní kořeny $(\operatorname{ind} a, \phi(m)) = 1$ plyne, že existuje právě tolik primitivních kořenů (mod m), kolik existuje čísel $\operatorname{ind} a$ menších než $\phi(m)$ nesoudělných s $\phi(m)$, což je právě $\phi(\phi(m))$. □

Příklad. V redukované soustavě zbytků (mod 41) jsou primitivními kořeny čísla a, pro která $(\operatorname{ind} a, 40) = 1$, tj. čísla 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35, jejich počet je $\phi(40) = 16$.

Cvičení

81. Řešte kongruence použitím tabulek indexů:

a) $x^5 \equiv 37 \pmod{43}$,
b) $x^8 \equiv 27 \pmod{37}$,
c) $x^{10} \equiv 33 \pmod{37}$,
d) $x^{12} \equiv 27 \pmod{83}$,
e) $x^2 \equiv 61 \pmod{73^2}$,
f) $x^2 \equiv 29 \pmod{59^2}$.

82. Řešte kongruence prvního stupně použitím tabulek indexů:

a) $23x \equiv 9 \pmod{97}$,
b) $47x \equiv 23 \pmod{73}$,
c) $53x \equiv 37 \pmod{79}$,
d) $65x \equiv 38 \pmod{83}$.

83. Řešte kongruence použitím tabulek indexů:

a) $43x^{17} \equiv 35 \pmod{71}$,
b) $45x^{12} \equiv 28 \pmod{67}$,
c) $53x^{21} \equiv 38 \pmod{61}$,
d) $27x^{30} \equiv 41 \pmod{79}$.

84. Najděte zbytek po dělení použitím tabulek indexů:

a) 341^{245} po 89,
b) 244^{408} po 73,
c) 749^{193} po 79,
d) $53^{29}43^{17}$ po 37,
e) 175^{411} po 629.

85. Najděte nejmenší celé kladné řešení exponenciálních kongruencí:

a) $13^x \equiv 42 \pmod{53}$,
b) $18^x \equiv 53 \pmod{79}$,
c) $44^x \equiv 19 \pmod{71}$.

Kapitola 5

Aproximace reálných čísel racionálními čísly

5.1 Řetězové zlomky reálných čísel a jejich vlastnosti

1. Vyjádření iracionálních čísel nekonečnými řetězovými zlomky

V předešlých kapitolách bylo ukázáno, že algoritmem postupného hledání celých částí je možno každé racionální číslo $\alpha = \frac{a}{b}$ vyjádřit jakožto *konečný* řetězový zlomek

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}} = (q_1, \ldots, q_n) \tag{1}$$

a naopak, že každý řetězový zlomek (1) reprezentuje racionální číslo.

Algoritmus postupného hledání celých částí je možno aplikovat i pro reálná čísla obecně. Pro iracionální číslo α ovšem algoritmus musí být nutně nekonečný. Výpočet řetězového zlomku odpovídajícího iracionálnímu číslu α je možno vyjádřit následujícím schématem:

$$\begin{aligned}
\alpha = \alpha_1 &= q_1 + \tfrac{1}{\alpha_2}, \quad \text{kde } q_1 = [\alpha_1], \alpha_2 > 1, \\
\alpha_2 &= q_2 + \tfrac{1}{\alpha_3}, \quad \text{kde } q_2 = [\alpha_2], \alpha_3 > 1, \\
&\vdots \quad \vdots \\
\alpha_k &= q_k + \tfrac{1}{\alpha_{k+1}}, \quad \text{kde } q_k = [\alpha_k], \alpha_{k+1} > 1, \\
&\vdots \quad \vdots
\end{aligned} \tag{2}$$

Je tedy možno psát

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_k + \cfrac{1}{\alpha_{k+1}}}}}. \tag{3}$$

Posloupnost $\alpha = (q_1, q_2, \ldots, q_k, \ldots)$ budeme nazývat *nekonečný řetězový zlomek čísla* α, čísla $q_1, q_2, \ldots, q_k, \ldots$, pak *prvky řetězového zlomku*. Poznamenejme, že každému α odpovídá *jediný* řetězový zlomek, neboť výpočet celých částí je jednoznačný.

Jestliže se nekonečný řetězový zlomek počínaje jistým prvkem začíná opakovat, nazývá se zlomek *periodický*. Opakuje-li se už od 1. prvku, nazývá se *ryze periodický*. V opačném případě hovoříme o *smíšeném periodickém zlomku*.

Ryze periodický zlomek $(q_1, \ldots, q_k, q_1, \ldots, q_k, \ldots)$ zapisujeme zkráceně ve tvaru $((q_1, \ldots, q_k))$, smíšený periodický zlomek $(q_1, \ldots, q_k, q'_1, \ldots, q'_1, q'_1, \ldots, q'_1, \ldots)$ ve tvaru $(q_1, \ldots, q_k, (q'_1, \ldots, q'_1))$.

Příklad. Pro $\alpha = \sqrt{11}$ dostaneme $\alpha = \alpha_1 = 3 + \frac{1}{\alpha_2}$, $\alpha_2 > 1$, dále pak

$$\begin{aligned}
\alpha_2 &= \tfrac{1}{\sqrt{11}-3} = \tfrac{\sqrt{11}+3}{2} = 3 + \tfrac{1}{\alpha_3}, \quad \alpha_3 > 1, \\
\alpha_3 &= \tfrac{2}{\sqrt{11}-3} = \sqrt{11} + 3 = 6 + \tfrac{1}{\alpha_4}, \quad \alpha_4 > 1, \\
\alpha_4 &= \tfrac{1}{\sqrt{11}-3} = \tfrac{\sqrt{11}+3}{2} = 3 + \tfrac{1}{\alpha_5}, \quad \alpha_5 > 1, \ldots
\end{aligned}$$

Celkem tedy $\sqrt{11} = (3, (3, 6))$.

Čísla α_k ve formulích (2) nazýváme *zbytková čísla řádu* k rozkladu čísla α. Pro nekonečný řetězový zlomek $(q_1, \ldots, q_k, \ldots)$ je možno opět uvažovat posloupnost zlomků $\delta_1 = q_1, \delta_2 = (q_1, q_2), \ldots, \delta_k = (q_1, \ldots, q_k), \ldots$ nazývaných *parciální zlomky* rozkladu čísla α.

Je zřejmé, že rekurentní formule pro výpočet zlomků δ_k pomocí zlomků předchozích zůstanou stejné jako v případě konečných řetězových zlomků, neboť jejich výpočet závisí pouze na prvcích $q_1, \ldots, q_k, \ldots$ a nikoliv na tom, zda posloupnost některým prvkem q_k končí. Platí tedy:

1)
$$\delta_k = \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}}, \quad \text{kde}$$

$$\begin{aligned}
P_k &= q_k P_{k-1} + P_{k-2}, \quad P_0 = 1,\ P_1 = q_1, \\
Q_k &= q_k Q_{k-1} + Q_{k-2}, \quad Q_0 = 0,\ Q_1 = 1.
\end{aligned}$$

2) $\Delta_k = P_k Q_{k-1} - Q_k P_{k-1} = (-1)^k$,

3) $\delta_k - \delta_{k-1} = \dfrac{(-1)^k}{Q_k Q_{k-1}}$.

Bereme-li v úvahu formuli (3), je možno podobně psát

$$\alpha = \frac{\alpha_{k+1} P_k + P_{k-1}}{\alpha_{k+1} Q_k + Q_{k-1}}. \tag{4}$$

Zajímavá nyní bude otázka, jak budou parciální zlomky δ_k a číslo α uspořádány na číselné ose.

Věta 5.1. *Číslo α leží vždy mezi sousedními parciálními zlomky δ_k, δ_{k+1} svého rozkladu a je vždy blíže k δ_{k+1} než k δ_k.*

Důkaz: Z formule (4) postupně odvodíme

$$\begin{aligned}
\alpha\alpha_{k+1}Q_k + \alpha Q_{k-1} &= \alpha_{k+1}P_k + P_{k-1},\\
\alpha_{k+1}(\alpha Q_k - P_k) &= P_{k-1} - \alpha Q_{k-1},\\
\alpha_{k+1}Q_k\left(\alpha - \frac{P_k}{Q_k}\right) &= Q_{k-1}\left(\frac{P_{k-1}}{Q_{k-1}} - \alpha\right),\\
\alpha_{k+1}Q_k(\alpha - \delta_k) &= Q_{k-1}(\delta_{k-1} - \alpha).
\end{aligned}$$

Přitom $\alpha_{k+1} > 1$, $Q_k > Q_{k-1} > 0$ (dokáže se snadno indukcí), takže

$$\alpha_{k+1}Q_k > Q_{k-1} > 0.$$

Odtud plyne

1) čísla $\alpha - \delta_k, \delta_{k-1} - \alpha$ mají stejná znaménka, tedy α leží mezi δ_k a δ_{k-1};
2) $|\alpha - \delta_k| < |\delta_{k-1} - \alpha|$, tj. α je blíže δ_k než δ_{k-1}. □

Jelikož $\alpha > \delta_1 = q_1$, je $\alpha < \delta_2$, $\alpha > \delta_3$, ... Odtud dostaneme:

a) α je větší než parciální zlomky lichého řádu a menší než všechny parciální zlomky sudého řádu;

b) parciální zlomky lichého řádu tvoří rostoucí posloupnost a sudého řádu klesající posloupnost, tj.

$$\delta_1 < \delta_3 < \cdots < \alpha < \cdots < \delta_4 < \delta_2.$$

Dále, protože $Q_{k+1} > Q_k$, je $\lim\limits_{k\to\infty} Q_k = \infty$, tj.

$$\lim_{k\to\infty} |\delta_{k+1} - \delta_k| = \lim_{k\to\infty} \frac{1}{Q_k Q_{k-1}} = 0.$$

Jelikož α leží ve všech intervalech (δ_k, δ_{k+1}), je

$$\alpha = \lim_{k\to\infty} \delta_k.$$

Dokázali jsme tedy následující větu.

Věta 5.2. *Nekonečná posloupnost parciálních zlomků δ_k odpovídající iracionálnímu číslu α konverguje k α, přičemž je alternující kolem α.*

Cvičení

86. Najděte rozklad v řetězový zlomek a parciální zlomky pro $\alpha = \frac{\sqrt{5}+1}{2}$. Najděte zákonistosti v posloupnosti jmenovatelů těchto zlomků a ukažte, že tvoří tzv. Fibonacciho posloupnost.

87. Najděte reálné číslo α mající parciální zlomek δ_k a zbytkové číslo α_{k+1} pro:

    a) $\frac{10}{3}, \sqrt{2}$; b) $\frac{43}{17}, \sqrt{5}$.

88. Najděte rozklad reálného čísla α v řetězový zlomek, jestliže α má parciální zlomek δ_k a zbytkové číslo α_{k+1} pro:

    a) $\frac{10}{7}, \sqrt{3}$; b) $\frac{37}{13}, \frac{1+\sqrt{3}}{2}$.

2. Konvergence nekonečných řetězových zlomků

Ukážeme, že pro libovolný nekonečný řetězový zlomek $(q_1, \ldots, q_k, \ldots)$ posloupnost jeho parciálních zlomků konverguje k nějakému iracionálnímu číslu α, tj. také naopak, že každý nekonečný parciální řetězový zlomek reprezentuje jediné iracionální číslo.

Dokázali jsme, že

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \quad \text{a} \quad |\delta_k - \delta_{k-1}| = \frac{1}{Q_k Q_{k-1}}.$$

Tyto formule ukazují, že

1) $\delta_{2k} > \delta_{2k-1}$, $\delta_{2k} > \delta_{2k+1}$ pro libovolné $k \in \mathbb{N}$;

2) $|\delta_{k+1} - \delta_k| = \frac{1}{Q_{k+1}Q_k} < \frac{1}{Q_k Q_{k-1}} = |\delta_k - \delta_{k-1}|$.

Je tedy δ_3 blíže δ_2 než δ_1 a jelikož δ_1 a δ_3 leží vlevo od δ_2, je $\delta_1 < \delta_3$. Podobně $\delta_4 < \delta_2$, atd.

Jelikož dále je $\lim_{k\to\infty}(\delta_k - \delta_{k-1}) = 0$, tvoří délky intervalů (δ_1, δ_2), $(\delta_3, \delta_4), \ldots$ klesající posloupnost. Musí mít tedy jediný společný bod α, který je společnou limitou posloupností $\delta_1, \delta_3, \ldots$, a $\delta_2, \delta_4, \ldots$ Celkem platí

$$\alpha = \lim_{k\to\infty}(q_1, \ldots, q_k).$$

3. Přiblížení reálného čísla zlomky se zadaným ohraničením pro jmenovatele

Jelikož množina všech racionálních čísel je hustá v $\mathbb{R}$, lze ke každému reálnému číslu α a $\varepsilon > 0$ najít racionální číslo $\frac{p}{q}$ tak, že

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon, \tag{1}$$

tj. reálné číslo α lze aproximovat racionálním číslem s libovolnou přesností. Jestliže ovšem budeme na zlomek $\frac{p}{q}$ klást jisté omezující podmínky, už se obecně zlomkem $\frac{p}{q}$ nebudeme zřejmě moci číslu α libovolně přiblížit. Zabývejme se následujícími problémy:

(1) jsou-li dána čísla α a ε, jak velké je nutno vzít q tak, aby platil vztah (1);

(2) jsou-li dána α a q nebo nějaké ohraničení shora pro q, jak malé může být číslo ε, aby ještě platil vztah (1).

Zabývejme se nejprve otázkou, jak „blízko“ jsou parciální zlomky δ_k v rozkladu α k číslu α, tj. zkoumejme rozdíl $|\alpha - \delta_k|$. Jelikož α leží vždy mezi sousedními parciálními zlomky δ_k, δ_{k+1} a je vždy blíže k δ_{k+1}, platí

$$|\alpha - \delta_k| \leq |\delta_{k+1} - \delta_k| = \frac{1}{Q_k Q_{k+1}}.$$

Ovšem $Q_{k+1} = q_{k+1}Q_k + Q_{k-1}$, kde $q_{k+1} \geq 1$, $Q_k, Q_{k-1} > 0$, tedy $Q_{k+1} \geq$ $\geq Q_k + Q_{k-1} > Q_k$, odkud $\frac{1}{Q_k Q_{k+1}} < \frac{1}{Q_k^2}$. Celkem tedy máme

$$|\alpha - \delta_k| < \frac{1}{Q_k^2}.$$

Zkoumání problémů 1) a 2) začněme následujícím motivačním příkladem

Příklad. Holandský astronom, fyzik a matematik *Christian Huygens* (1629–1695) narazil při konstrukci modelu sluneční soustavy pomocí ozubených kol na problém, který ho přivedl k objevu důležitých vlastností nekonečných řetězových zlomků. Předpokládejme, že podíl úhlových rychlostí dvou kol je α. Jelikož úhlové rychlosti jsou nepřímo úměrné počtu zubů, musí být podíl počtu zubů také α. Je-li $\alpha = \frac{N}{n}$ zlomek v základním tvaru s velkými hodnotami N a n (např. $\frac{1261}{881}$), pak vzniká technická obtíž výroby kol s tak velkým počtem zubů. Úlohu je možno technicky zjednodušit omezením počtu zubů, přičemž poměr počtu zubů by měl být přibližně zachován. Chceme tedy např. čísla N a n zaměnit čísly N_1 a n_1 tak, aby $n_1 \leq 100$. Rozložíme $\frac{1261}{881}$ v řetězový zlomek a určíme jeho parciální zlomky:

$$\frac{1261}{881} = (1, 2, 3, 7, 8, 2)$$

q_k		1	2	3	7	8	2
P_k	1	1	3	10	73	594	1261
Q_k	0	1	2	7	51	415	881

Vidíme, že našim podmínkám vyhovuje parciální zlomek $\delta_4 = \frac{73}{51}$, přičemž

$$\left|\frac{1261}{881} - \delta_4\right| < \frac{1}{51 \cdot 415} < 10^{-4}.$$

Úlohu je možno formulovat i jinak: najít zlomek s co nejmenším jmenovatelem tak, aby se nelišil od $\frac{N}{n}$ o více než 10^{-4}. Je tedy nutné vybrat nejmenší k tak, aby $Q_k \cdot Q_{k+1} > 10^4$. Zjistíme, že $k = 4$ a úloze pak vyhovuje zlomek δ_4.

Příklad. Víme, že $\sqrt{11} = (3, (3, 6))$. Nahraďme $\sqrt{11}$ zlomkem s přesností 10^{-3}. Hledáme tedy takový parciální zlomek $\delta_k = \frac{P_k}{Q_k}$ tak, aby $Q_k Q_{k+1} > 10^3$. Parciální zlomky dostaneme z tabulky:

q_k		3	3	6	3	...	...
P_k	1	3	10	63	199	...	...
Q_k	0	1	3	19	60	...	...

Odtud $\delta_3 = \frac{63}{19}$ je parciální zlomek s nejmenším jmenovatelem vyhovující naší úloze, neboť $19 \cdot 60 > 10^3$.

Shora uvedené problémy lze formulovat takto:

1) *najít co nejlepší racionální přiblížení čísla α parciálním zlomkem s jmenovatelem $\leq n$;*
2) *najít racionální přiblížení parciálními zlomky čísla α s co nejmenším jmenovatelem tak, aby odchylka nebyla větší než ε.* V tomto případě hledáme nejmenší $k \in \mathbb{N}$ vlastnosti $Q_k Q_{k+1} > \frac{1}{\varepsilon}$.

Zákon možného přiblížení libovolného reálného čísla α racionálním číslem nezávisle na jeho tvaru vyjadřuje následující věta.

Věta 5.3. (Dirichletova) *Nechť $\alpha, \tau \geq 1$ jsou reálná čísla. Pak existuje zlomek $\frac{a}{b}$ v základním tvaru tak, že*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau}, \quad 0 < b \leq \tau.$$

Jiná formulace: Pro každá reálná čísla $\alpha, \tau \geq 1$ existuje racionální přiblížení $\frac{a}{b}$ čísla α s přesností $\frac{1}{b\tau}$, $0 < b \leq \tau$.

Důkaz: Nechť $\delta_k = \frac{P_k}{Q_k}$ je parciální zlomek čísla α. Vybereme nejmenší Q_k tak, aby $Q_k \leq \tau$ a položíme $\frac{a}{b} = \delta_k$ (uvědomte si, že posloupnost Q_k je rostoucí, tedy takové Q_k vždy existuje). Platí tedy

$$Q_k \leq \tau < Q_{k+1},$$

odkud

$$\left|\alpha - \frac{a}{b}\right| = \left|\alpha - \frac{P_k}{Q_k}\right| \leq \frac{1}{Q_k Q_{k+1}} < \frac{1}{b\tau},$$

neboť $\frac{1}{Q_{k+1}} < \frac{1}{\tau}$, $Q_k = b, 0 < b = Q_k \leq \tau$. □

Příklad. Nalezneme přiblížení čísla $\sqrt{19}$ zlomkem $\frac{a}{b}$ s přesností $\frac{1}{100b}$.

Platí $\sqrt{19} = (4, (2, 1, 3, 1, 2, 8))$, odkud dle tabulky

q_k		4	2	1	3	1	2	8	...
P_k	1	4	9	13	48	61	170		...
Q_k	0	1	2	3	11	14	39		...

je vidět, že největší jmenovatel $Q_k \leq 100$ je 39. Zvolíme tedy $\frac{a}{b} = \frac{170}{39}$.

4. Parciální zlomky jako nejlepší přiblížení

Na uvedených příkladech jsme viděli, že parciální zlomky reálného čísla α jej dobře aproximují. Obecně ukažme, že v jistém smyslu dávají nejlepší možná přiblížení.

Uvažujeme-li např. aproximaci čísla α desetinným číslem až do n-té cifry za desetinnou čárkou, dostaneme zlomek $\frac{p}{q}$ s jmenovatelem $q = 10^n$, přičemž odchylka je rovna $|\alpha - \frac{p}{q}| \leq \frac{1}{2q}$ (zbytek nemůže být větší než polovina čísla 10^{-n}).

Jak jsme odvodili, je-li $\frac{p}{q}$ parciální zlomek čísla α, pak

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2},$$

takže pro dané q je odchylka $\frac{1}{q^2}$ mnohem menší než $\frac{1}{2q}$.

Příklad. Vyjádřete přibližně číslo π zlomkem s jmenovatelem ≤ 100.

Řešení: Pro desetinné přiblížení je $3,14 = \frac{314}{100}$, odkud $|\pi - 3,14| < 0,016$. Užitím desetinného rozvoje čísla π na 35 desetinných míst spočítal *J. Wallis* (1616-1703) v r. 1685 jeho prvních 34 parciálních zlomků:

$$\pi = (\ 3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2,$$
$$2, 2, 2, 1, 84, 2, 1, 1, 15, 3, 13, 1, 4, 2, 6, 6, 1, \dots\ ),$$

odkud

$$\delta_1 = \frac{3}{1} = 3, \quad \delta_2 = \frac{22}{7}, \quad \delta_3 = \frac{333}{106}, \quad \text{atd.}$$

Přitom $|\pi - \frac{22}{7}| < \frac{1}{7 \cdot 106} < 0,0014$. Přiblížení $\frac{22}{7}$ tedy dává mnohem větší přesnost při daleko menším jmenovateli než $\frac{314}{100}$.

Euler jako první odvodil řetězový zlomek pro číslo e:

$$\mathrm{e} = (2, 1, 2, 1, 1, 4, 1, 1, \ldots, 2m, 1, 1, \ldots) = (2, (1, 2m, 1))_{m\geq 1}.$$

Vidíme tedy, že pro číslo e známe (na rozdíl od čísla π) jakýsi vytvořující zákon jeho řetězového zlomku. Relativně jednoduchý Hurwitzův důkaz uvedeného vytváření lze nalézt v knize [8]. Podobnou metodou bylo dokázáno, že

$$\mathrm{e}^2 = (7, 2, 1, 1, 3, 18, 5, 1, 1, 6, 30, 8, 1, 1, 9, 42, \ldots),$$

neboli $\mathrm{e}^2 = (7, (3m-1, 1, 1, 3m, 12m+6))_{m\geq 1}$.

Uveďme pro zajímavost ještě další formuli, odvozenou L. Eulerem (pro $a \geq 1$):

$$\frac{\mathrm{e}^{2/a}+1}{\mathrm{e}^{2/a}-1} = (a, 3a, 5a, 7a, \ldots),$$

speciálně tedy

$$\frac{\mathrm{e}^2+1}{\mathrm{e}^2-1} = (1, 3, 5, 7, \ldots), \qquad \frac{\mathrm{e}+1}{\mathrm{e}-1} = (2, 6, 10, 14, \ldots).$$

Cvičení

89. Použitím aparátu řetězcových zlomků zaměňte zlomek $\frac{N}{n}$ zlomkem $\frac{N_1}{n_1}$ tak, aby $n_1 \leq 100$ a aby $\frac{N_1}{n_1}$ bylo co nejblíže $\frac{N}{n}$. Určete dosaženou chybu ε.
    a) $\frac{1847}{379}$, b) $\frac{857}{149}$, c) $\frac{1499}{647}$, d) $\frac{2099}{593}$.

90. Použitím aparátu řetězových zlomků zaměňte zlomek $\frac{N}{n}$ zlomkem $\frac{N_1}{n_1}$ s co nejmenším jmenovatelem n_1 tak, aby dosažená chyba nebyla větší než ε:
    a) zadání z předchozího příkladu pro $\varepsilon = 0,01$;
    b) $\frac{1741}{293}$, $\varepsilon = 0,01$; c) $\frac{1327}{383}$, $\varepsilon = 0,001$; d) $\frac{1609}{239}$, $\varepsilon = 0,01$.

91. Použitím aparátu řetězových zlomků najděte pro $\sqrt{a}$ racionální přiblížení s největším jmenovatelem $n_1 \leq b$ a určete dosaženou chybu ε:
    a) $a = 15$, $n_1 \leq 10$; b) $a = 17$, $n_1 \leq 10$;
    c) $a = 23$, $n_1 \leq 50$; d) $a = 31$, $n_1 \leq 100$.

92. Mezi parciálními zlomky rozkladu α najděte přiblížení k α s co nejmenším jmenovatelem tak, aby dosažená chyba nepřevyšovala ε:
    a) $\alpha = \sqrt{26}$, $\varepsilon = 0,001$; b) $\alpha = \sqrt{37}$, $\varepsilon = 0,001$;
    c) $\alpha = \sqrt{29}$, $\varepsilon = 0,001$; d) $\alpha = \sqrt{19}$, $\varepsilon = 0,01$.

93. Řešte totéž jako v předchozím příkladě pro:
    a) $\alpha = \frac{\sqrt{5}+2}{2}$, $\varepsilon = 0,01$; b) $\alpha = \frac{\sqrt{401}+18}{11}$, $\varepsilon = 0,01$;
    c) $\alpha = \frac{2\sqrt{39}+11}{7}$, $\varepsilon = 0,01$; d) $\alpha = \frac{\sqrt{101}+9}{5}$, $\varepsilon = 0,01$;
    e) $\alpha = \frac{\sqrt{7}+2}{4}$, $\varepsilon = 0,01$; f) $\alpha = \frac{\sqrt{21}+9}{6}$, $\varepsilon = 0,01$.

94. Najděte parciální zlomek k $\sqrt[3]{10}$ s přesností do 0,01.

Že uvedený výsledek není náhodný, ukazuje následující věta.

Věta 5.4. *Je-li α reálné číslo, $\delta = \frac{P}{Q}$ racionální číslo a platí $\left|\alpha - \frac{P}{Q}\right| < \left|\alpha - \frac{P_k}{Q_k}\right|$ pro nějaké $k > 1$, pak $Q > Q_k$.*

Důkaz: Zřejmě $\alpha \neq \delta_k$ pro každé $k \in \mathbb{N}$. Víme, že α leží mezi zlomky δ_k, δ_{k+1} a přitom α je blíže δ_{k+1} než δ_k. Je-li δ blíže k α než δ_k, pak δ leží mezi δ_{k-1} a δ_k (např. pro k sudé je α blíže δ_k než δ_{k-1}, a tedy $\delta \in (\alpha-\varepsilon, \alpha+\varepsilon)$ pro nějaké $\varepsilon > 0$, $\varepsilon < \delta_k - \alpha$).

Předpokládejme tedy, že k je sudé (pro k liché postupujeme analogicky).
Máme $0 < \delta < \delta_k$, odkud

$$0 < \delta - \delta_{k-1} < \delta_k - \delta_{k-1} = \frac{1}{Q_k Q_{k-1}},$$

tedy

$$0 < \frac{P}{Q} - \frac{P_{k-1}}{Q_{k-1}} < \frac{1}{Q_k Q_{k-1}},$$

$$0 < \frac{PQ_{k-1} - QP_{k-1}}{QQ_{k-1}} < \frac{1}{Q_k Q_{k-1}},$$

$$0 < Q_k(PQ_{k-1} - QP_{k-1}) < Q.$$

Jelikož $PQ_{k-1} - QP_{k-1} > 0$, je $Q_k < Q$. □

Předchozí tvrzení nás vede k následující definici: Přiblížení čísla α zlomkem $\frac{a}{b}$ se nazývá *nejlepší přiblížení*, jestliže platí: je-li $\frac{c}{d}$ racionální číslo a platí

$$\left|\alpha - \frac{c}{d}\right| < \left|\alpha - \frac{a}{b}\right|,$$

pak $d > b$.

Dokázali jsme tedy, že *parciální zlomky* δ_k čísla α jsou *jeho nejlepší přiblížení*. Je třeba si přitom uvědomit, že parciální zlomky *nejsou jediná* nejlepší přiblížení čísla α.

Pro odchylku čísel α a δ_k byl odvozen vztah

$$|\alpha - \delta_k| < \frac{1}{Q_k^2}.$$

Lze tedy tvrdit, že pro číslo $c = 1$ a pro libovolné iracionální číslo α existuje nekonečně mnoho zlomků $\frac{P}{Q}$ v základním tvaru vlastnosti

$$\left|\alpha - \frac{P}{Q}\right| < \frac{c}{Q^2}. \tag{1}$$

Takovými budou například všechny parciální zlomky $\delta_k = \frac{P_k}{Q_k}$ čísla α. Vzniká otázka, zda existuje menší číslo c než 1 tak, aby pro každé iracionální číslo α existovalo nekonečně mnoho zlomků $\frac{P}{Q}$ v základním tvaru vlastnosti (1).

Věta 5.5. *Pro každé iracionální číslo α existuje pro $c = \frac{1}{2}$ nekonečně mnoho zlomků $\frac{P}{Q}$ v základním tvaru s vlastností*

$$\left|\alpha - \frac{P}{Q}\right| < \frac{c}{Q^2}. \tag{2}$$

Takovými zlomky mohou být jen parciální zlomky δ_k čísla α.

Důkaz: Ukažme, že z každých dvou po sobě následujících parciálních zlomků δ_k, δ_{k+1} $(k > 1)$ alespoň jeden splňuje nerovnost (2).

Předpokládejme opak, tj. nechť platí

$$|\alpha - \delta_k| \geq \frac{1}{2Q_k^2}, \quad |\alpha - \delta_{k+1}| \geq \frac{1}{2Q_{k+1}^2}.$$

Pak

$$|\alpha - \delta_k| + |\alpha - \delta_{k+1}| \geq \frac{1}{2}\left(\frac{1}{Q_k^2} + \frac{1}{Q_{k+1}^2}\right).$$

Jelikož α leží mezi δ_k a δ_{k+1}, je

$$|\alpha - \delta_k| + |\alpha - \delta_{k+1}| = |\delta_k - \delta_{k+1}| = \frac{1}{Q_k Q_{k+1}},$$

tj.

$$\frac{1}{2}\left(\frac{1}{Q_k^2} + \frac{1}{Q_{k+1}^2}\right) \leq \frac{1}{Q_k Q_{k+1}},$$

odkud

$$\left(\frac{1}{Q_k} + \frac{1}{Q_{k+1}}\right)^2 \leq 0.$$

To ovšem pro $k > 1$ není možné. □

Předchozí tvrzení dává *postačující* podmínku pro to, aby zlomek δ v základním tvaru byl parciálním zlomkem iracionálního čísla α. Není to však podmínka nutná, neboť existují parciální zlomky, které vlastnost (2) nemají (může jich být dokonce nekonečně mnoho). Jak uvidíme dále, pomocí této podmínky je možno řešit tzv. *Pellovy rovnice*.

Krajní možnost pro číslo c ve shora uvedeném smyslu dává následující věta:

Věta 5.6. (Hurwitz–Borelova) *Pro libovolné iracionální číslo α existuje pro $c = \frac{1}{\sqrt{5}}$ nekonečně mnoho zlomků $\frac{P}{Q}$ v základním tvaru vlastnosti*

$$\left|\alpha - \frac{P}{Q}\right| < \frac{1}{\sqrt{5}Q^2} = \frac{c}{Q^2}. \tag{3}$$

Je-li $c < \frac{1}{\sqrt{5}}$*, pak existuje iracionální číslo* α*, pro nějž existuje jen konečný počet zlomků* $\frac{P}{Q}$ *v základním tvaru vlastnosti* (3)*.*

Důkaz: Provedeme jen náznak důkazu. Nejprve se dokáže, že z tří po sobě následujících parciálních zlomků čísla α má alespoň jeden vlastnost (3). Pro $c < \frac{1}{\sqrt{5}}$ iracionální čísla α, pro něž existuje jen konečný počet zlomků $\frac{P}{Q}$ (dle předešlého tvrzení je $\frac{P}{Q}$ vždy parciální zlomek čísla α) vlastnosti (3), jsou například všechna iracionální čísla, která jsou kořeny některé kvadratické rovnice s koeficienty ze $\mathbb{Z}$ (tzv. kvadratické iracionality). □

Poznamenejme na závěr, že z Hurwitz–Borelovy věty plyne řada zajímavých důsledků pro teorii diofantických nerovnic. Uvažujeme-li totiž pro dané α a $c > 0$ nerovnici

$$\left|\alpha - \frac{y}{x}\right| < \frac{c}{x^2},$$

kde $(x, y) \in \mathbb{N} \times \mathbb{Z}$, pak má tato nerovnice pro $c \geq \frac{1}{\sqrt{5}}$ vždy nekonečně mnoho řešení, kdežto pro $c < \frac{1}{\sqrt{5}}$ jich může mít jen konečně mnoho.

5.2 Kvadratické iracionality a periodické řetězové zlomky, Pellova rovnice

Kvadratickou iracionalitou rozumíme každý iracionální kořen kvadratické rovnice s koeficienty z množiny $\mathbb{Z}$. Obecný tvar takového čísla je

$$\frac{a + \sqrt{b}}{c},$$

kde $a, b, c \in \mathbb{Z}$, $b > 0$, b není kvadrátem žádného přirozeného čísla.

Ukažme vztah mezi kvadratickými iracionalitami a periodickými řetězovými zlomky.

Věta 5.7. *Každý periodický řetězový zlomek je rozkladem některé kvadratické iracionality.*

Důkaz: Nechť α je smíšený periodický zlomek, tj.

$$\alpha = (q_1, \ldots, q_k, \alpha'),$$

kde $\alpha' = ((q'_1, \ldots, q'_l))$ je ryze periodický zlomek.

Označme $\frac{P_i}{Q_i}$, resp. $\frac{P'_i}{Q'_i}$ parciální zlomky čísel α resp. α'. Jelikož $\alpha' = (q'_1, \ldots, q'_l, \alpha')$, platí

$$\alpha' = \frac{P'_l \alpha' + P'_{l-1}}{Q'_l \alpha' + Q'_{l-1}}.$$

Odtud plyne, že α' vyhovuje kvadratické rovnici s celočíselnými koeficienty (ověřte!), je tedy α' kvadratická iracionalita. Podobně

$$\alpha = \frac{P_k\alpha' + P_{k-1}}{Q_k\alpha' + Q_{k-1}},$$

tedy i α je kvadratická iracionalita. □

J. L. Lagrange (1736-1813) dokázal, že platí i věta obrácená:

Věta 5.8. (Lagrangeova) *Řetězový zlomek každé kvadratické iracionality je periodický.*

Důkaz: Nechť α je kořen rovnice

$$a\alpha^2 + b\alpha + c = 0, \tag{1}$$

kde $a, b, c \in \mathbb{Z}$. Při rozkladu čísla α v řetězový zlomek víme, že

$$\alpha = \frac{P_k\alpha' + P_{k-1}}{Q_k\alpha' + Q_{k-1}}, \tag{2}$$

kde α' je zbytek čísla α řádu $k+1$. Dosazením z (2) do (1) dostaneme pro α' rovnici

$$A_k\alpha'^2 + B_k\alpha' + C_k = 0, \tag{3}$$

kde

$$\begin{aligned} A_k &= aP_k^2 + bP_kQ_k + cQ_k^2, \\ B_k &= 2aP_kP_{k-1} + b(P_kQ_{k-1} + P_{k-1}Q_k) + 2cQ_kQ_{k-1}, \\ C_k &= aP_{k-1}^2 + bP_{k-1}Q_{k-1} + cQ_{k-1}^2. \end{aligned} \tag{4}$$

Odtud máme $C_k = A_{k-1}$ a

$$B_k^2 - 4A_kC_k = (b^2 - 4ac)(P_kQ_{k-1} - P_{k-1}Q_k)^2 = b^2 - 4ac. \tag{5}$$

Jsou tedy diskriminanty rovnic (1) a (3) stejné a nezávisí na k. Idea důkazu spočívá v důkazu omezenosti koeficientů A_k, B_k, C_k. Bude-li toto platit, pak koeficienty A_k, B_k, C_k mohou nabývat jen konečně mnoha hodnot (jsou to celá čísla), a tedy i rovnic (3) bude jen konečně mnoho. To ale bude znamenat, že zbytky α' mohou také nabývat jen konečně mnoha hodnot. Pak existují zbytky nabývající stejných hodnot, tj. řetězový zlomek bude periodický.

Stačí ukázat ohraničenost koeficientů A_k, neboť z $C_k = A_{k-1}$ plyne ohraničenost C_k a díky (5) pak i ohraničenost B_k. Platí

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k^2},$$

neboli

$$\alpha - \frac{P_k}{Q_k} = \frac{\varepsilon}{Q_k^2},$$

kde $|\varepsilon| < 1$, tj.

$$\frac{P_k}{Q_k} = \alpha - \frac{\varepsilon}{Q_k^2}.$$

Z první z rovností (4) máme

$$\frac{A_k}{Q_k^2} = a\left(\frac{P_k}{Q_k}\right)^2 + b\left(\frac{P_k}{Q_k}\right) + c = a\left(\alpha - \frac{\varepsilon}{Q_k^2}\right)^2 + b\left(\alpha - \frac{\varepsilon}{Q_k^2}\right) + c =$$
$$= a\alpha^2 + b\alpha + c - 2a\alpha\frac{\varepsilon}{Q_k^2} + a\varepsilon^2\frac{1}{Q_k^4} - b\varepsilon\frac{1}{Q_k^2}.$$

Jelikož $a\alpha^2 + b\alpha + c = 0$, dostaneme

$$|A_k| \leq |2a\alpha\varepsilon| + \left|\frac{a\varepsilon^2}{Q_k^2}\right| + |b\varepsilon| \leq |2a\alpha| + |a| + |b|,$$

tedy koeficienty A_k jsou ohraničené. □

Uveďme ještě bez důkazu následující vlastnosti řetězových zlomků kvadratických iracionalit:

1) perioda řetězového zlomku začíná obecně od jeho druhého členu

2) ryze periodický zlomek dostaneme právě tehdy, když

$$\alpha = \frac{a + \sqrt{b}}{c} > 1 \quad \text{a zároveň} \quad \alpha' = \frac{a - \sqrt{b}}{c} \in (-1, 0).$$

Příklad. Najděte kvadratickou rovnici tak, aby jeden její kořen byl kvadratickou iracionalitou s řetězovým zlomkem $x = ((2, 3, 1))$ a určete číslo x.
Řešení: Zřejmě platí $x = (2, 3, 1, x)$. Sestavíme tabulku pro výpočet parciálních zlomků:

	2	3	1	x
1	2	7	9	$9x + 7$
0	1	3	4	$4x + 3$

Je tedy

$$x = \frac{9x + 7}{4x + 3},$$

tj. $4x^2 - 6x - 7 = 0$. Vyřešením této rovnice dostaneme

$$((2, 3, 1)) = \frac{3 + \sqrt{37}}{4}.$$

Příklad. Najděte kvadratickou iracionalitu pro řetězový zlomek $x = (4, (2, 1))$.
Řešení: Podobně jako v předchozím příkladě bude platit $x = (4, y)$, kde je $y = (2, 1, y)$. Pro y dostaneme následující tabulku:

	2	1	y
1	2	3	$3y + 2$
0	1	1	$y + 1$

Odtud odvodíme

$$y = \frac{3y + 2}{y + 1},$$

tj. $y^2 - 2y - 2 = 0$, a $y = 1 + \sqrt{3}$. Dále $x = 4 + \frac{1}{y}$, odkud $x = \frac{7+\sqrt{3}}{2}$. Pro x tak máme kvadratickou rovnici

$$2x^2 - 14x + 23 = 0.$$

Cvičení

95. Sestavte rovnici tak, aby jeden z jejích kořenů měl rozvoj v řetězový periodický zlomek α, a najděte odpovídající iracionální číslo pro:

a) $\alpha = ((3, 2))$;
b) $\alpha = ((1, 7))$;
c) $\alpha = ((2, 6, 1))$;
d) $\alpha = ((5, 4, 3))$;
e) $\alpha = (3, (2, 1))$;
f) $\alpha = (4, (3, 2))$;
g) $\alpha = (1, 2, (3, 4))$.

Řešení Pellovy rovnice

Lagrangeova věta a postačující podmínka pro parciální zlomky dávají možnost řešit tzv. *Pellovy rovnice*. Jde o neurčité rovnice tvaru

$$x^2 - ay^2 = 1, \tag{1}$$

kde $a > 0$, $\sqrt{a}$ je kvadratická iracionalita, s neznámými $x, y \in \mathbb{Z}$.

Rovnice (1) má vždy řešení $(1, 0)$, které nazýváme *triviální*. Hledejme nějaké kladné řešení rovnice (1), tj. řešení $(x, y) \in \mathbb{N} \times \mathbb{N}$. Z (1) postupnými úpravami dostaneme

$$\frac{x^2}{y^2} - a = \frac{1}{y^2}$$
$$\frac{x}{y} - \sqrt{a} = \frac{1}{y^2\left(\frac{x}{y} + \sqrt{a}\right)}.$$

Odtud $\frac{x}{y} > \sqrt{a}$ (pravá strana poslední rovnosti je kladná), a tedy

$$\frac{x}{y} + \sqrt{a} > 2\sqrt{a} > 2, \qquad 0 < \frac{x}{y} - \sqrt{a} < \frac{1}{2y^2}.$$

Zlomek $\frac{x}{y}$ vyhovuje dle Věty 5.5 postačující podmínce pro parciální zlomky $\sqrt{a}$ (přičemž je evidentně sudého řádu, neboť $\frac{x}{y} > \sqrt{a}$). Všechna kladná řešení rovnice (1) je tedy možno hledat ve tvaru $\frac{P_k}{Q_k}$, kde k je sudé a $\frac{P_k}{Q_k}$ je parciální zlomek čísla $\sqrt{a}$.

Nechť $\sqrt{a} = (q_1, \ldots, q_k, q_{k+1}, \ldots)$. Platí

$$\sqrt{a} = \frac{\alpha_{k+1} P_k + P_{k-1}}{\alpha_{k+1} Q_k + Q_{k-1}},$$

kde $\alpha_{k+1} = (q_{k+1}, \ldots)$ je zbytek $\sqrt{a}$ řádu $k+1$. Odtud pro k sudé platí

$$\alpha_{k+1}(P_k - Q_k\sqrt{a}) = Q_{k-1}\sqrt{a} - P_{k-1},$$

$$\begin{aligned}\alpha_{k+1}(P_k^2 - aQ_k^2) &= (P_k + \sqrt{a}Q_k)(Q_{k-1}\sqrt{a} - P_{k-1}) = \\ &= (P_kQ_{k-1} - Q_kP_{k-1})\sqrt{a} + Q_kQ_{k-1}a - P_kP_{k-1},\end{aligned}$$

$$\alpha_{k+1}(P_k^2 - aQ_k^2) = \sqrt{a} + b,$$

kde $b = Q_kQ_{k-1}a - P_kP_{k-1}$, $P_kQ_{k-1} - Q_kP_{k-1} = (-1)^k = 1$ pro k sudé.

Odtud dále plyne, že parciální zlomek $\frac{P_k}{Q_k} = \frac{x}{y}$ je řešením rovnice (1), právě když

$$\alpha_{k+1} = \sqrt{a} + b. \tag{2}$$

Podmínka (2) je přitom ekvivalentní podmínce

$$\alpha_{k+1} = \sqrt{a} + b = (b + q_1, q_2, \ldots, q_k, \alpha_{k+1}) = (q_{k+1}, q_2, \ldots, q_k, \alpha_{k+1}),$$

(uvědomte si, že celá část čísla α_{k+1} je $q_{k+1} = b + q_1$)

$$\alpha_{k+1} = ((q_{k+1}, q_2, \ldots, q_k, \alpha_{k+1})).$$

To ale znamená, že

$$\sqrt{a} = (q_1, (q_2, \ldots, q_{k+1})). \tag{3}$$

Dvojice (P_k, Q_k) je tedy řešením rovnice (1), je-li $\sqrt{a}$ periodický řetězový zlomek s periodou od 2. členu a číslo k dostaneme jako délku periody. Obecně jsme dokázali, že řetězový zlomek kvadratické iracionality je periodický s periodou od druhého členu, je tedy rovnice (1) vždy řešitelná, přičemž

1) je-li délka periody k, kde k je sudé, jsou jejím řešením dvojice (P_k, Q_k), (P_{2k}, Q_{2k}), atd.;

2) je-li k liché, jsou řešeními rovnice (1) dvojice (P_{2k}, Q_{2k}), (P_{4k}, Q_{4k}) atd.

Nejmenší kladné řešení je v prvním případě (P_k, Q_k), ve druhém případě (P_{2k}, Q_{2k}). Dá se navíc snadno dokázat, že je-li (x_1, y_1) nejmenší kladné řešení rovnice (1), dostaneme každé kladné řešení (x_n, y_n) rovnice (1) z formule

$$x_n + y_n\sqrt{a} = (x_1 + y_1\sqrt{a})^n.$$

Příklad. Řešme Pellovu rovnici $x^2 - 11y^2 = 1$.
Řešení: Platí $\sqrt{11} = (3, (3, 6))$. Je tedy $k = 2$ a nejmenší kladné řešení je $x = P_2 = 10$, $y = Q_2 = 3$.

Příklad. Řešme Pellovu rovnici $x^2 - 41y^2 = 1$.
Řešení: Platí $\sqrt{41} = (6, (2, 2, 12))$. Je tedy $k = 3$ a nejmenší kladné řešení je tvaru $x = P_6 = 2049$, $y = Q_6 = 320$.

Cvičení

96. Najděte nejmenší kladná řešení rovnic:

    a) $x^2 - 26y^2 = 1$,

    b) $x^2 - 37y^2 = 1$,

    c) $x^2 - 19y^2 = 1$,

    d) $x^2 - 29y^2 = 1$.

Kapitola 6

Algebraická a transcendentní čísla

6.1 Iracionální čísla

Racionalita či iracionalita čísla vypovídá o jeho utváření. Zatímco racionální čísla jsou charakterizována *konečnými* nebo *periodickými* desetinnými rozvoji či *konečnými* řetězovými zlomky, čísla iracionální jsou charakterizována rozvoji *neperiodickými* či *nekonečnými*. Tyto vlastnosti mohou být sice kritérii racionality či iracionality čísla, ale ne vždy jsou prakticky použitelná.

Iracionalita čísla $\sqrt{2}$ byla dokázána již Pythagorejci. Toto jednoduché tvrzení lze následovně zobecnit pro libovolné odmocniny:

Věta 6.1. *$\sqrt[k]{n}$ je pro $k \in \mathbb{N}$, $n \in \mathbb{N}$ iracionální číslo, právě když n není k-tou mocninou žádného přirozeného čísla.*

Důkaz: Předpokládejme sporem, že $\sqrt[k]{n} = \frac{a}{b}$ je racionální číslo, kde $(a, b) = 1$. Nutně $b > 1$ (jinak by $\sqrt[k]{n}$ byla k-tou mocninou přirozeného čísla). Pak $a^k = b^k n$, odkud $b|a^k$. Je-li nyní p prvočíselný dělitel b, pak $p|a^k$, tedy nutně $p|a$. Vzhledem k $(a, b) = 1$ máme $b = 1$, což je spor. □

Příklad. Důkazy iracionality některých odmocnin je možno provést i pomocí velmi názorných geometrických úvah. Ukažme takový typ důkazu pro $\sqrt{5}$. Snadno zjistíme, že číslo $x = \frac{1}{2}(\sqrt{5} - 1)$ je řešením kvadratické rovnice $x^2 = 1 - x$. Bude přitom platit, že $\sqrt{5}$ je iracionální číslo právě když je iracionální x.

Geometricky to znamená, že máme-li dánu úsečku AB délky 1, $|AC| = x$, pak platí $|AC|^2 = |AB| \cdot |CB|$ (neboť $x^2 = 1 \cdot (1 - x)$, viz obrázek).

Říkáme také, že bod C dělí úseču AB *zlatým řezem*, tj. platí

$$|AB| : |AC| = |AC| : |CB|.$$

Při dělení úsečky AB je zbytek $|CB| = 1 - x = x^2$. Dále platí

$$x = x^2 \cdot 1 + (x - x^2), \quad \text{kde } x - x^2 = x(1-x) = x^3,$$
$$x^2 = x^3 \cdot 1 + (x^2 - x^3), \quad \text{kde } x^2 - x^3 = x^2(1-x) = x^4, \text{ atd.}$$

Geometricky předchozí rovnosti znamenají toto: sestrojíme-li bod C_1 souměrně sdružený s B dle bodu C, je úsečka AC dělena bodem C_1 opět zlatým řezem, jelikož

$$|AC| : |CC_1| = x : x^2 = x^2 : (x - x^2) = |CC_1| : |AC_1|.$$

Sestrojíme-li dále bod C_2 středově souměrný s A dle bodu C_1, dělí bod C_2 úsečku CC_1 zlatým řezem, neboť

$$|CC_1| : |C_1C_2| = x^2 : x^3 = x^3 : (x^2 - x^3) = |C_1C_2| : |C_2C|.$$

Uvedený algoritmus konstrukce bodů C_i zřejmě neskončí po konečném počtu kroků. Kdyby bylo číslo x racionální, byly by úsečky AB a AC celistvými násobky téhož racionálního čísla δ. Totéž by platilo pro úsečky $|CC_1| = |AB| - |AC|$ a $|C_1C_2| = |AC_1| - |CC_1|$, atd. Zkonstruovali bychom nekonečnou klesající posloupnost celistvých násobků racionálního čísla δ, což není možné.

Předchozí tvrzení je speciálním případem tvrzení:

Věta 6.2. *Je-li α reálný kořen rovnice $x^n + c_1x^{n-1} + \ldots + c_n = 0$ s koeficienty ze $\mathbb{Z}$, pak α je buď číslo celé nebo iracionální.*

Důkaz: Nechť $c_n \neq 0$ a nechť $\frac{a}{b}$ je racionální kořen uvedené rovnice, $(a, b) = 1$ a $b > 1$ (jinak by $\frac{a}{b}$ bylo celé číslo). Pak

$$a^n + c_1a^{n-1}b + \ldots + c_nb^n = 0,$$
$$a^n = -b(c_1a^{n-1} + \ldots + c_nb^{n-1}).$$

Odtud plyne $b|a^n$, a tedy jako v předešlém tvrzení dostaneme spor. □

Příklad. Číslo $x = \sqrt{2} + \sqrt{3}$ je dle předchozího tvrzení iracionální, neboť není celé (proč?) a je kořenem rovnice s celočíselnými koeficienty $x^4 - 10x^2 + 1 = 0$.

Pro zkoumání racionality či iracionality čísel jsou užitečná následující tvrzení:

Věta 6.3. *Pro každé racionální číslo α existuje kladná konstanta c tak, že nerovnost*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q}$$

platí pro libovolné racionální číslo $\frac{p}{q} \neq \alpha$.

Důkaz: Nechť $\alpha = \frac{a}{b} \neq \frac{p}{q}$ (tedy $aq - bp \neq 0$) a $b \geq 1$. Pak dostaneme

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq} = \frac{\frac{1}{b}}{q}.$$

Stačí položit $c = \frac{1}{b}$. □

Z uvedeného tvrzení plyne postačující podmínka iracionality čísla:

Věta 6.4. *Jestliže lze pro libovolné kladné číslo c najít alespoň jednu dvojici celých čísel p, q tak, že*

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{c}{q},$$

pak α je iracionální číslo.

Kromě odmocnin existují další zajímavá iracionální čísla, mající svůj původ v matematické analýze. Uveďme alespoň dvě z nich.

Iracionalita čísel e a π

Je známo, že

$$\mathrm{e} = \sum_{k=0}^{\infty} \frac{1}{k!}.$$

Předpokládejme, že e je racionální, tj. $\mathrm{e} = \frac{a}{b}$. Pro $k \geq b$ uvažujme výraz

$$c = k! \left(\mathrm{e} - 1 - \frac{1}{1!} - \ldots - \frac{1}{k!}\right). \tag{1}$$

Díky $k \geq b$ platí $b|k!$, a tedy $k! \cdot \mathrm{e} = \frac{a}{b} \cdot k! \in \mathbb{Z}$. Je tedy $c \in \mathbb{Z}$, neboť po roznásobení pravé strany v (1) dostaneme celá čísla. Z rovnosti (1) dále máme

$$0 < c = k! \left(\frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \ldots\right) =$$
$$= \frac{1}{(k+1)} + \frac{1}{(k+1)(k+2)} + \ldots < \frac{1}{(k+1)} + \frac{1}{(k+1)^2} + \ldots = \frac{1}{k},$$

tj. $0 < c < \frac{1}{k}$, tedy $c \notin \mathbb{Z}$, což je spor. □

Dokázat iracionalitu čísla π je složitější. Poprvé se to podařilo v r. 1761 Lambertovi pomocí řetězových zlomků obecného typu.

Předpokládejme, že číslo $\pi = \frac{a}{b}$ je racionální. Uvažujme funkce

$$f(x) = \frac{x^n (a - bx)^n}{n!}, \tag{2}$$

$$F(x) = f(x) - f''(x) + f^{(IV)}(x) - \ldots + (-1)^n f^{(2n)}(x). \tag{3}$$

Jelikož se ve funkci $f(x)$ vyskytuje x v mocninách od n do $2n$, lze psát

$$f(x) = \frac{1}{n!} \sum_{i=n}^{2n} a_{i-n} x^i,$$

kde $a_{i-n} \in \mathbb{Z}$. Odtud dostaneme

$$f(0) = f'(0) = \ldots = f^{(n-1)}(0) = 0.$$

Pro derivace k-tého řádu pro $n \leq k \leq 2n$ v bodě 0 bude nenulový pouze člen u k-té mocniny, neboli

$$f^k(0) = \frac{k!}{n!} a_{k-n}.$$

Je tedy $f^{(j)}(0)$ pro $0 \leq j \leq 2n$ celé číslo. Vzhledem k (2) je $f(x) = f(\pi - x)$ a $f^{(j)}(x) = f^{(j)}(\pi - x)$, tj. $f^{(j)}(\pi) = f^{(j)}(0) \in \mathbb{Z}$. Proto dle (3) jsou $F(0)$ a $F(\pi)$ celá čísla. Z definice funkce $F(x)$ dále obdržíme

$$F''(x) = f''(x) - f^{(IV)}(x) + f^{(VI)}(x) - \ldots + (-1)^{n-1} f^{(2n)}(x),$$

odkud

$$F''(x) + F(x) = f(x).$$

Z poslední rovnosti dále plyne vztah

$$\frac{\mathrm{d}}{\mathrm{d}x}(F'(x)\sin x - F(x)\cos x) = f(x)\sin x. \tag{4}$$

Vypočítejme nyní následující integrál užitím rovnosti (4):

$$I = \int_0^\pi f(x)\sin x \mathrm{d}x = [F'(x)\sin x - F(x)\cos x]_0^\pi =$$
$$= F(\pi) + F(0) \in \mathbb{Z}.$$

Na intervalu $(0, \pi)$ ovšem dle (2) platí

$$f(x)\sin x < \frac{\pi^n a^n}{n!}.$$

Pro dostatečně velké n ale výraz na pravé straně nabývá libovolně malých hodnot, tedy integrál I nemůže být celé číslo, což je spor. □

6.2 Liouvillova věta, transcendentní čísla

Iracionální čísla je možno z hlediska jejich kořenových vlastností rozdělit do dvou skupin:

1) *algebraická čísla* – jsou kořeny nějaké algebraické rovnice s koeficienty z $\mathbb{Q}$ (a tedy ze $\mathbb{Z}$);
2) *transcendentní čísla* – nejsou kořenem žádné algebraické rovnice s koeficienty z $\mathbb{Q}$ resp. $\mathbb{Z}$.

Po dlouhou dobu se předpokládalo, že všechna čísla jsou algebraická. Teprve až r. 1844 dokázal francouzský matematik *J. Liouville* (1809-1882), že existují transcendentní čísla, a co bylo nejpřekvapivější, že jich je dokonce nekonečně mnoho.

Pro každé algebraické číslo α existuje polynom stupně n tvaru

$$f_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Q}[x]$$

takový, že α je jeho kořenem, a přitom α není kořenem polynomu nad $\mathbb{Q}$ nižšího stupně. Takový polynom $f_\alpha(x)$ je určen prvkem α jednoznačně a nazývá se *minimální polynom prvku* α. Podle stupně n polynomu f_α nazýváme prvek α *algebraický stupně n*. Je-li potom α kořenem některého polynomu $f(x) \in \mathbb{Q}[x]$, pak $f_\alpha | f$. Navíc platí, že polynom f_α je ireducibilní v $\mathbb{Q}[x]$ (proč?).

Věta 6.5. (Liouvillova) *Pro reálné algebraické číslo α stupně $n \geq 2$ existuje kladná konstanta c tak, že nerovnost*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^n}$$

platí pro libovolný racionální zlomek $\frac{p}{q}$.

Důkaz: Buď $f(x) = x^n + a'_{n-1}x^{n-1} + \ldots + a'_1 x + a'_0 \in \mathbb{Q}[x]$ minimální polynom prvku α. Polynomu f odpovídá polynom $f^*(x)$ s koeficienty ze $\mathbb{Z}$

$$f^*(x) = a_0 x^n + \ldots + a_{n-1}x + a_n.$$

Jelikož α je kořenem $f^*(x)$, je $f^*(x) = (x-\alpha)\cdot\phi(x)$, kde $\phi(x)$ je polynom stupně $n-1$. Položíme-li $x = \frac{p}{q}, q > 0$, pak

$$\left|f^*\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \cdot \left|\phi\left(\frac{p}{q}\right)\right|.$$

Díky nerozložitelnosti polynomu f^* je $f^*(\frac{p}{q}) \neq 0$. Proto

$$\left|f^*\left(\frac{p}{q}\right)\right| = \frac{|a_0 p^n + a_1 p^{n-1}q + \ldots + a_n q^n|}{|q^n|} \geq \frac{1}{q^n},$$

neboť číslo v čitateli je celé číslo různé od nuly.

Předpokládejme, že $\frac{p}{q} \in \langle \alpha-1, \alpha+1 \rangle$ a nechť $\frac{1}{c_1}$ je největší hodnota polynomu $\phi(x)$ v tomto intervalu. Pak $|\phi(\frac{p}{q})| \leq \frac{1}{c_1}$, a tedy

$$\frac{1}{q^n} \leq \left| f^* \left(\frac{p}{q} \right) \right| \leq \frac{1}{c_1} \left| \alpha - \frac{p}{q} \right|,$$

odkud

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c_1}{q^n}.$$

Je-li $\frac{p}{q}$ vně intervalu $\langle \alpha-1, \alpha+1 \rangle$, pak $|\alpha - \frac{p}{q}| > 1$ a jelikož $q \in \mathbb{N}$, $|\alpha - \frac{p}{q}| > 1 > \frac{1}{q^n}$. Vezmeme-li $c = \max(1, c_1)$, bude c hledanou konstantou. □

Povaha iracionálního čísla, nezávisle na jeho algebraičnosti či transcendentnosti, je dána možnostmi jeho aproximace racionálními čísly. Jinak řečeno, pojem aproximace je centrální při studiu iracionálních čísel. V roce 1909 zavedl Thue při studiu jistých typů diofantických rovnic pojem řád aproximace:

Definice. Nechť $\alpha \in \mathbb{R}$ and $\nu \geq 1$. Řekneme, že α je *aproximovatelné racionálními čísly do řádu* ν, existuje-li $c > 0$ (závislé na c, ν) a nekonečně mnoho zlomků v základním tvaru $\frac{p}{q}$ tak, že

$$\left| \alpha - \frac{p}{q} \right| < \frac{c}{q^\nu}.$$

Uveďme několik základních postřehů, týkajících se řádů aproximací:

- Je-li $\nu \geq \nu' \geq 1$, pak aproximovatelnost do řádu ν implikuje také aproximovatelnost do řádu ν';
- Z předchozího je tedy rozumné zavést pojem *řád aproximace čísla* α jakožto (reálné) číslo $\nu(\alpha) = sup\{\nu\,;\, \alpha \text{ je aproximovatelné do řádu } \nu\}$;
- Každé racionální číslo je aproximovatelné racionálními čísly do řádu 1 (pro libovolné $c > 1$), nikoli však do řádu $1 + \varepsilon$ pro $\varepsilon > 0$. Tedy $\nu(\alpha) = 1$ pro každé $\alpha \in \mathbb{Q}$;
- Je-li α reálná iracionalita, pak α je aproximovatelné racionálními čísly do řádu 2 (stačí položit $c = c(\alpha, 2) = 1$). Jak totiž víme, existuje nekonečně mnoho racionálních čísel (např. parciálních zlomků α) tak, že $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$. Tedy pro $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ máme $\nu(\alpha) \geq 2$;

Liouville uvažoval následující čísla: $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ se nazývá *Liouvillovo číslo* existuje-li pro každé $n \in \mathbb{N}, n \geq 2$, zlomek $\frac{p_n}{q_n}$ v základním tvaru vlastnosti

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^n}.$$

Jinak řečeno,

- Reálné číslo α je Liouvillovo právě když je aproximovatelné racionálními čísly do libovolného řádu $\nu \geq 1$, tedy $\nu(\alpha) = \infty$.

Uveďme pro ilustraci, že např. čísla e, π a ln 2 nejsou Liouvillova, není ale známo, zda e^π je Liouvillovo či nikoliv.

Přímo z definice Liouvillova čísla a Liouvillovy věty dostaneme

Věta 6.6. *Každé Liouvillovo číslo je transcendentní.*

Podívejme se dále, jak je možno generovat Liouvillova čísla. Uvažujme čísla ve tvaru

$$a_1 10^{-1!} + a_2 10^{-2!} + a_3 10^{-3!} + \dots ,$$

kde každý z koeficientů a_i je buď 0 nebo 1 a kde nekonečně mnoho koeficientů je rovno 1. Uvedená volba dává dobré aproximace uvedeného čísla racionálními čísly, které vzniknou jakožto součty prvních k sčítanců v uvedené sumě. V důsledku jsou všechna čísla uvedeného typu Liouvillova, a tedy dostaneme

Věta 6.7. *Existuje nekonečně mnoho Liouvillových čísel.*

Přímým důsledkem předchozího tvrzení je následující:

Věta 6.8. *Existuje nekonečně mnoho transcendentních čísel.*

Ukažme nyní jinou konstrukci transcendentních čísel pomocí řetězových zlomků a Liouvillovy věty. Definujme číslo α rekurentně takto: $\alpha = (q_1, \dots, q_k, \dots)$, přičemž jsou-li čísla $q_1, \dots, q_k$ již dána (a tedy jsou dány parciální zlomky $\delta_1 = \frac{P_1}{Q_1}, \dots, \delta_k = \frac{P_k}{Q_k}$), pak zvolme q_{k+1} tak, aby $q_{k+1} > Q_k^k$.

Ukažme, že α je pak transcendentní číslo. Platí

$$\left|\alpha - \frac{P_k}{Q_k}\right| = \frac{1}{Q_k Q_{k+1}} = \frac{1}{Q_k(q_{k+1}Q_k + Q_{k-1})} < \frac{1}{Q_k^2 q_{k+1}} < \frac{1}{Q_k^2 Q_k^k},$$

neboli

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{\frac{1}{Q_k^2}}{Q_k^k}.$$

Nechť nyní $c > 0$ je libovolné reálné číslo a $n \in \mathbb{N}$. Jelikož $Q_k \to \infty$ pro $k \to \infty$, existuje $k \geq n$ takové, že

$$\frac{1}{Q_k^2} < c.$$

Pak dostaneme

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{c}{Q_k^k} \leq \frac{c}{Q_k^n},$$

neboť $Q_k^k \geq Q_k^n$. Dle Liouvillovy věty ovšem číslo α nemůže být algebraické stupně n, a tedy je transcendentní.

Poznámka. V roce 1874 německý matematik *G. Cantor* (1845-1918) v souvislosti s rozvojem teorie množin dokázal novým způsobem existenci transcendentních čísel. Ukázal, že množina $\mathbb{Q}$ všech racionálních čísel je spočetná, tedy i množina polynomů s racionálními koeficienty je spočetná. Odtud plyne, že počet kořenů takovýchto polynomů je spočetný a celkem je tedy *množina algebraických čísel spočetná*. Jelikož množina reálných čísel je ale nespočetná, je nutně *množina transcendentních čísel nespočetná*. Z předešlých úvah o konstrukci Liouvillových čísel lze vyvodit, že dokonce *množina Liouvillových čísel je nespočetná*. Navíc lze dokázat, že *množina Liouvillových čísel je míry* 0, tedy vybereme-li náhodně reálné číslo, pak pravděpodobnost, že bude Liouvillovo, je rovna 0.

Ačkoli je množina Liouvillových čísel míry 0, platí následující skoro paradoxní tvrzení:

Věta 6.9. *Každé reálné číslo je součtem dvou Liouvillových čísel.*

Důkaz: Provedeme jen ideu důkazu. Uvažujme libovolné reálné číslo α. Nezávisle na tom, je-li α racionální či iracionální, lze jej vyjádřit desetinným rozvojem s nekonečně mnoha nenulovými ciframi. Opravdu, máme-li ukončený desetinný rozvoj, např. $0,452$, lze jej nahradit nekonečným rozvojem $0,451999\ldots$. Zapišme nyní desetinný rozvoj α jako

$$I, d_1 d_2 d_3 d_4 \ldots,$$

kde I je celá část α a d_i je jeho i-tá desetinná cifra. Uvažujme dále čísla α_1 a α_2 daná desetinnými rozvoji

$$\begin{aligned}
\alpha_1 &= I,\ 0\ d_2\ d_3\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ d_{10} \ldots d_{33}\ \ 0\ \ \ 0\ \ \ldots\ , \\
\alpha_2 &= 0,\ d_1\ \ 0\ \ 0\ d_4\ d_5\ d_6\ d_7\ d_8\ d_9\ \ 0\ \ \ldots\ \ 0\ \ d_{34}\ d_{35}\ \ldots\ ,
\end{aligned}$$

kde délky s nulami jsou alternačně $1!,\ 2!,\ 3!,\ 4!$ atd. Vidíme, že $\alpha = \alpha_1 + \alpha_2$. Přitom z konstrukce čísel α_1 a α_2 lze vyvodit, že jde o čísla Liouvillova, neboť libolně dlouhé posloupnosti nul v jejich desetinných vyjádřeních dávají dobré racionální aproximace.

□

Jak jsme viděli v předchozím textu, není problém zkonstruovat transcendentní čísla. Mnohem větší problém je ukázat, že dané číslo je transcendentní. Tento problém patří k nejtěžším v teorii čísel. Až v roce 1873 *Ch. Hermite* (1822-1901) dokázal transcendentnost čísla e, v roce 1882 Němec *F. von Lindemann* (1852-1939) transcendentnost čísla π.

Dosud uvažovaná čísla se vyznačovala vlastností, že některé jejich desetinné aproximace byly natolik dobré, že vedly k jejich transcendentnosti. Avšak pro většinu reálných čísel jejich nejlepší racionální aproximace nepocházejí z jejich desetinných rozvojů. Z tohoto důvodu jsou důkazy transcendentnosti čísel obecně dosti složité, podrobnosti lze nalézt např. v knize [2].

Důkazem transcendentnosti π byl řešen problém tzv. *kvadratury kruhu*, tj. zda lze pomocí pravítka a kružítka sestrojit čtverec o stejném obsahu, jako je obsah jednotkového kruhu. Je známo, že pomocí pravítka a kružítka lze zkonstruovat pouze kořeny algebraických rovnic s celočíselnými koeficienty. Jelikož π (a tedy i $\sqrt{\pi}$) je transcendentní, nemůže být takový čtverec uvedenými prostředky sestrojen.

Na mezinárodním matematickém kongresu v r. 1900 *D. Hilbert* (1862-1943) formuloval jako jeden z aktuálních 23 matematických problémů zjistit, zda jsou transcendentní čísla ve tvaru α^β, kde α, β jsou algebraická čísla, $\alpha \neq 0, 1$ a β je iracionální číslo (speciálně, jsou-li $2^{\sqrt{2}}$ a e^π transcendentní). Tento problém byl plně vyřešen nezávisle *A. Gelfondem* (1906-1968) a *T. Schneiderem* (1911-1988) až v r. 1934:

Věta 6.10. (Gelfond–Schneiderova) *Čísla ve tvaru α^β, kde α, β jsou algebraická, $\alpha \neq 0, 1, \beta$ iracionální, jsou transcendentní.*

Z uvedené věty mj. vyplývá, že logaritmy racionálních čísel, pokud nejsou racionálními čísly, jsou transcendentní. Kdyby totiž $\log r = \beta$ bylo algebraické iracionální číslo pro racionální $r \in \mathbb{Q}$, platilo by $r = 10^\beta$ a dle Gelfond–Schneiderovy věty by bylo r transcendentní.

Transcendentní je také číslo e^π, neboť $\mathrm{e}^{i\pi} = -1 = i^2$, odkud $\mathrm{e}^\pi = i^{-2i}$.

Poznamenejme na závěr, že dosud uvažovaná transcendentí čísla se vyznačovala

Racionalita či iracionalita čísel 2^e, π^e, $\pi^{\sqrt{2}}$ zůstává nadále otevřeným problémem. Některé aktuální problémy týkající se iracionality či transcendentnosti čísel jsou uvedeny v poslední kapitole.

Cvičení

97. Dokažte, že čísla

$$\alpha = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \dots$$

$$\beta = \frac{1}{2^{1!}} + \frac{1}{2^{2!}} + \dots$$

jsou transcendentní.

Kapitola 7

Aditivní problémy teorie čísel

Aditivními problémy teorie čísel se rozumějí takové úlohy, v nichž zkoumáme utváření přirozených čísel ze sčítanců daného typu. V takových úlohách se zkoumají vazby mezi vlastnostmi přirozených čísel vzhledem k násobení (multiplikativní vlastnosti) nebo vzhledem ke sčítání (aditivní vlastnosti). Tyto vztahy jsou často velmi složité a jejich zkoumání vedlo k formulaci základních aditivních problémů teorie čísel.

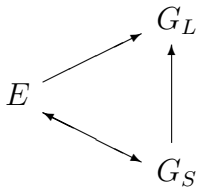
Jedním z nich je tzv. *Goldbachova hypotéza*. Byla vyslovena už v r. 1742 petrohradským matematikem *Ch. Goldbachem* (1690-1764) a říká, že

každé celé číslo ≥ 6 *lze vyjádřit jako součet tří prvočísel.*

Euler jako reakci na Goldbachovu domněnku vyslovil hypotézu, že

každé sudé číslo > 2 *je součet dvou prvočísel.*

Rozdělíme-li Goldbachovu hypotézu na hypotézu pro sudá čísla (G_S) a pro lichá čísla (G_L), pak souvislost mezi nimi a hypotézou Eulera (E) je následující:



1) jestliže ke každému sudému číslu ≥ 4 přičteme prvočíslo 2, dostaneme všechna sudá čísla ≥ 6, tedy $E \Rightarrow G_S$; naopak z platnosti G_S plyne, že jeden ze sčítanců je sudé číslo, tj. 2, odkud $G_S \Rightarrow E$.

2) jestliže ke každému sudému číslu ≥ 4 přičteme prvočíslo 3, dostaneme všechna lichá čísla > 6, a tedy $E \Rightarrow G_L$.

Z uvedeného vyplývá, že Goldbachova hypotéza je ekvivalentní hypotéze G_S (a tedy E). Goldbachovu hypotézu je tedy také možno formulovat tak, že *každé přirozené číslo* > 2 *je součtem nejvýše tří prvočísel.* Téměř dvě století se nepodařilo udělat pokrok v jejím řešení.

Druhým významným problémem v teorii čísel je *Waringův problém.* Formuloval ho v r. 1770 anglický matematik *E. Waring* (1736-1798):

Pro každé přirozené číslo $n \geq 2$ *existuje přirozené číslo* $r(n) = r$ *tak, že každé přirozené* N *je možno vyjádřit ve tvaru*

$$N = x_1^n + x_2^n + \ldots + x_r^n, x_i \geq 0,$$

tj. jako součet nejvýše r *n-tých mocnin čísel z* $\mathbb{N}_0$.

Je třeba poznamenat, že *počet sčítanců závisí pouze na čísle* n *a nezávisí na vyjadřovaném čísle* N.

Na druhé straně Waringův problém (jakožto existenční hypotézu) stačí řešit pro *dostatečně velká* N, neboť jestliže pro vyjádření všech přirozeých čísel $N > N_0$ (tj. dostatečně velkých N) stačí r sčítanců, pak pro vyjádření všech přirozených čísel není třeba více než $r' = \max(N_0, r)$ sčítanců (každé $N \leq N_0$ je totiž možno vyjádřit ve tvaru N sčítanců $N = 1^n + 1^n + \ldots + 1^n$).

Nejzajímavější na problému je určení čísel $r(n)$ pro dané $n \in \mathbb{N}$. Ještě v 18. stol. byl Waringův problém řešen pro $n = 2$ *Lagrangem*:

každé přirozené číslo je součtem nejvýše čtyř kvadrátů, tj. $r(2) = 4$.

V obecném případě byl problém neřešen až do počátku 20. století. Poprvé byla hypotéza dokázána r. 1909 *Hilbertem.*

Další významné problémy aditivní teorie čísel byly formulovány *G.H. Hardym* (1877-1947) a *J. E. Littlewoodem* (1885-1977):

1) *každé dostatečně velké přirozené číslo, které není kvadrátem, je součtem kvadrátů a prvočísla;*
2) *každé dostatečně velké přirozené číslo je součtem dvou kvadrátů a prvočísla.*

Druhý z problémů dokázal Rus *J. V. Linnik* v r. 1959.

7.1 Rozklad na součet kvadrátů

Dříve než dokážeme Lagrangeovu větu o rozkladu přirozených čísel na součet čtyř kvadrátů, prozkoumáme rozklady na součet dvou kvadrátů.

Věta 7.1. *Přirozené číslo* N *lze rozložit na součet dvou kvadrátů* $x^2 + y^2$*, právě když se v kanonickém rozkladu čísla* N *nevyskytuje prvočíslo ve tvaru* $4k+3$ *v liché mocnině.*

Poznámka. Tvrzení dává odpověď na otázku, pro která přirozená čísla N existují na kružnici $x^2 + y^2 = N$ body s celočíselnými souřadnicemi.

Důkaz: ($\Rightarrow$) Nechť $x^2 + y^2 = N$. Je-li $d = (x, y)$, pak $N = d^2(x_1^2 + y_1^2)$, kde $x_1 = \frac{x}{d}, y_1 = \frac{y}{d}$, $(x_1, y_1) = 1$.

Platí-li $p|N_1 = x_1^2 + y_1^2$ pro nějaké liché prvočíslo p, pak vzhledem k $(x_1, y_1) = 1$ plyne z věty 2.25 $p \equiv 1 \pmod 4$. Má tedy číslo N_1 pouze prvočíselné dělitele $\equiv 1 \pmod 4$. Jestliže $p|N$ pro $p \equiv 3 \pmod 4$, pak tedy nutně $p|d$, což vzhledem k $d^2|N$ znamená, že p je dělitel v sudé mocnině.

($\Leftarrow$) Ověřením identit

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 \mp b_1b_2)^2 + (a_1b_2 \pm a_2b_1)^2$$

dostaneme, že součin dvou celých čísel, která jsou součty kvadrátů, je opět součtem kvadrátů. Číslo N uvedené vlastnosti je součinem čísel tvaru: kvadrátů, dvojky, prvočísel ve tvaru $4k+1$. Všechna lze vyjádřit jako součet dvou kvadrátů, tedy i číslo N má tuto vlastnost. □

Ukažme, že prvočísla ve tvaru $4n + 1$ lze charakterizovat pomocí jednoznačnosti rozkladu na součet nesoudělných kvadrátů (jednoznačnost je zde myšlena až na záměnu sčítanců).

Věta 7.2. (Eulerova) *Číslo ve tvaru $4n + 1$ je prvočíslem, právě když jej lze jednoznačně vyjádřit jako součet dvou nesoudělných kvadrátů.*

Důkaz: ($\Rightarrow$) Předpokládejme, že

$$p = x_1^2 + y_1^2 = x_2^2 + y_2^2 \tag{1}$$

je dvojí vyjádření prvočísla p v součet nesoudělných kvadrátů. Pak $x_1^2y_2^2 - y_1^2x_2^2 = p(y_2^2 - y_1^2)$, neboť

$$\begin{aligned} p(y_2^2 - y_1^2) = (x_1^2 + y_1^2)(y_2^2 - y_1^2) = x_1^2y_2^2 - x_1^2y_1^2 + y_1^2y_2^2 - y_1^4 = \\ = x_1^2y_2^2 - y_1^2(x_1^2 + y_1^2 - y_2^2) = x_1^2y_2^2 - y_1^2x_2^2. \end{aligned}$$

Odtud máme

$$p|(x_1y_2 - y_1x_2)(x_1y_2 + y_1x_2).$$

Obě závorky nemohou být současně dělitelné p. V opačném případě by totiž musel být p dělitelný i jejich součet, tedy $p|2x_1y_2$, odkud $p|x_1$ nebo $p|y_2$. To by ale znamenalo dle (1), že pak i $p|y_1$ nebo $p|x_2$, což je spor s $(x_1, y_1) = (x_2, y_2) = 1$.

Vynásobením rovností (1) dostaneme

$$p^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 \pm y_1y_2)^2 + (x_1y_2 \mp y_1x_2)^2. \tag{2}$$

Platí-li $p|(x_1y_2 - y_1x_2)$, pak $p^2|(x_1y_2 - y_1x_2)^2$ a z (2) také $p^2|(x_1x_2 + y_1y_2)^2$. Lze tedy rovnost (2) vydělit p^2, odkud

$$\left(\frac{x_1x_2 + y_1y_2}{p}\right)^2 + \left(\frac{x_1y_2 - y_1x_2}{p}\right)^2 = 1.$$

Pak ale $x_1y_2 - y_1x_2 = 0$, a tedy $x_1y_2 = y_1x_2$. Jelikož $(x_1, y_1) = (x_2, y_2) = 1$, dostaneme $x_1|x_2$, $x_2|x_1$, odkud $x_1 = x_2$, $y_1 = y_2$.

Jestliže $p|(x_1y_2+y_1x_2)$, pak z (2) podobnými úvahami vyplyne $x_1x_2-y_1y_2 = 0$, tj. $x_1x_2 = y_1y_2$, odkud $x_1|y_2$, $y_2|x_1$, $y_2 = x_1$, $y_1 = x_2$. Celkem jsme tedy dokázali jednoznačnost rozkladu.

($\Leftarrow$) Každé číslo ve tvaru $4n + 1$, které lze vyjádřit jako součet kvadrátů, má dle věty 2.25 pouze prvočíselné dělitele $\equiv 1 \pmod 4$. Součin takových prvočísel, např. $p_1 = x_1^2 + y_1^2$, $p_2 = x_2^2 + y_2^2$, kde $x_1 > y_1 > 0$, $x_2 > y_2 > 0$ lze vyjádřit alespoň dvěma způsoby ve tvaru součtu kvadrátů:

$$p_1p_2 = (x_1x_2 \pm y_1y_2)^2 + (x_1y_2 \mp y_1x_2)^2.$$

Stačí ukázat, že $(x_1x_2+y_1y_2)^2 > (x_1x_2-y_1y_2)^2$, $(x_1y_2\mp y_1x_2)^2$, neboli, že rozklady na pravé straně jsou různé.

První nerovnost platí díky nenulovosti čísel x_1, x_2, y_1, y_2; ukážeme, že

$$x_1x_2 + y_1y_2 > x_1y_2 + y_1x_2 > x_1y_2 - y_1x_2.$$

Máme $x_1x_2 + y_1y_2 - x_1y_2 - y_1x_2 = (x_1 - y_1)(x_2 - y_2) > 0$. Budeme-li pokračovat pro další prvočísla $\equiv 1 \pmod 4$, dostaneme opět rozklad alespoň dvěma způsoby. □

Věta 7.3. (Lagrangeova) *Každé přirozené číslo je možno vyjádřit ve tvaru součtu čtyř kvadrátů přirozených čísel nebo nuly.*

Důkaz: Budeme vycházet z identity

$$(a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = A^2 + B^2 + C^2 + D^2, \tag{1}$$

kde

$$\begin{aligned} A &= a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2, \\ B &= -a_1b_2 + b_1a_2 - c_1d_2 + d_1c_2, \\ C &= -a_1c_2 + c_1a_2 - d_1b_2 + b_1d_2, \\ D &= -a_1d_2 + d_1a_2 - b_1c_2 + c_1b_2. \end{aligned} \tag{2}$$

Díky této identitě stačí ukázat, že každé prvočíslo je možno vyjádřit ve tvaru součtu čtyř kvadrátů. Jelikož číslo 2 a každé prvočíslo $p \equiv 1 \pmod 4$ je součtem dvou kvadrátů, je tím spíše součtem čtyř kvadrátů (stačí k nim totiž přičíst součet $0^2 + 0^2$). Uvedenou vlastnost je tedy třeba dokázat pouze pro prvočísla $p \equiv 3 \pmod 4$.

I. Nejprve ukažme, že pro takové prvočíslo p existuje číslo m, $0 < m < p$ tak, že číslo mp je součtem čtyř kvadrátů. K tomu studujme čísla ve tvaru $x^2, -y^2-1$, kde x, y probíhají hodnoty z množiny $M = \{0, 1, \ldots, \frac{1}{2}(p-1)\}$. Platí-li pro prvky $x_1, x_2 \in M$, že $x_1^2 \equiv x_2^2 \pmod p$, pak $(x_1 + x_2)(x_1 - x_2) \equiv 0 \pmod p$. Ovšem $\mathbb{Z}_p$ je těleso, tedy $x_1 \equiv \pm x_2 \pmod p$.

Vzhledem k tomu, že množina $\{0, \pm 1, \ldots, \pm\frac{1}{2}(p-1)\}$ je úplný systém zbytků modulo p, je nutně $x_1 = x_2$. Ze stejného důvodu tedy nejsou kongruentní modulo p žádné dva z prvků $-y^2 - 1$. Po dosazení prvků z M do výrazů x^2 a $-y^2 - 1$ dostaneme $p + 1$ čísel, tj. některé dvě z nich jsou nutně kongruentní modulo p. Existují tedy prvky $x, y \in M$ tak, že

$$x^2 \equiv -y^2 - 1 \pmod p,$$

neboli

$$mp = x^2 + y^2 + 0^2 + 1^2,$$

kde $0 < m < p$, neboť $x^2 + y^2 + 1 > 0$, $x < \frac{1}{2}p$, $y < \frac{1}{2}p$, a tedy

$$m = \frac{x^2 + y^2 + 1}{p} < \frac{\frac{1}{2}p^2 + 1}{p} < p.$$

Celkem tedy platí

$$mp = a_1^2 + b_1^2 + c_1^2 + d_1^2 \tag{3}$$

pro některé prvky $a_1, b_1, c_1, d_1 \in \mathbb{N}_0$.

II. Ukažme, že je možno v předešlém případě volit $m = 1$, tj. že p je součtem čtyř kvadrátů.

Existuje nejmenší $n \in \mathbb{N}$ takové, že číslo mp je součtem čtyř kvadrátů. Připusťme, že $m > 1$. Je možno uvažovat m liché, neboť pro $m = 2m_1$ jsou čísla a_1, b_1, c_1, d_1 buď všechna sudá nebo všechna lichá nebo jedna dvojice je sudá a jedna lichá. Ve všech případech bude platit

$$m_1 p = \left(\frac{a_1 + b_1}{2}\right)^2 + \left(\frac{a_1 - b_1}{2}\right)^2 + \left(\frac{c_1 + d_1}{2}\right)^2 + \left(\frac{c_1 - d_1}{2}\right)^2,$$

tj. $m_1 p$ lze rozložit na součet čtyř kvadrátů.

Označme a_2, b_2, c_2, d_2 absolutně nejmenší zbytky čísel a_1, b_1, c_1, $d_1 \pmod m$, neboli

$$a_1 \equiv a_2,\ b_1 \equiv b_2,\ c_1 \equiv c_2,\ d_1 \equiv d_2 \pmod m, \tag{4}$$

přičemž $|a_2|, |b_2|, |c_2|, |d_2| < \frac{1}{2}m$, ($m$ je liché). Odtud dostaneme

$$mp = a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv a_2^2 + b_2^2 + c_2^2 + d_2^2 \equiv 0 \pmod m.$$

Existuje tedy prvek $k \in \mathbb{N}$ takový, že

$$mk = a_2^2 + b_2^2 + c_2^2 + d_2^2 < 4\Big(\frac{1}{2}m\Big)^2 = m^2. \tag{5}$$

Přitom $0 < k < m$, neboť v případě $k = 0$ by platilo $a_2 = b_2 = c_2 = d_2 = 0$, odkud $m|a_1, b_1, c_1, d_1$, $m^2|mp$, $m|p$, což vzhledem k $0 < m < p$ není možné.

Dále, vynásobením rovností v podmínkách (2) a (5) dostaneme

$$mk \cdot mp = m^2kp = (a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = A^2 + B^2 + C^2 + D^2$$

pro některá A, B, C, D dle (1), přičemž z formulí (2) a (4) vyplyne

$$A \equiv B \equiv C \equiv D \equiv 0 \pmod{m}.$$

Vydělením poslední rovnosti m^2 obdržíme

$$kp = \left(\frac{A}{m}\right)^2 + \left(\frac{B}{m}\right)^2 + \left(\frac{C}{m}\right)^2 + \left(\frac{D}{m}\right)^2,$$

kde $\frac{A}{m}, \frac{B}{m}, \frac{C}{m}, \frac{D}{m} \in \mathbb{Z}$. Je tedy možno číslo kp, $0 < k < m$, vyjádřit ve tvaru součtu čtyř kvadrátů, což je spor s minimalitou čísla m. Dokázali jsme $m = 1$, čímž je důkaz hotov. □

7.2 Schnirelmannova metoda sčítání posloupností

První úspěchy při řešení Goldbachovy hypotézy náleží ruskému matematikovi *L. Schnirelmannovi* (1905-1938), který vybudoval nový aparát v teorii čísel, tzv. *metodu sčítání číselných posloupností*. S její pomocí dokázal, že existuje konstanta c (tzv. *Schirelmannova konstanta*) taková, že *každé přirozené číslo $N > 1$ je součtem nejvýše c prvočísel*.

Vyložme základní principy uvedené metody. Mějme dány nějaké rostoucí posloupnosti přirozených čísel s prvním členem 0, tj.

$$a_0(= 0), a_1, \ldots, a_m, \ldots, \qquad (A)$$

$$b_0(= 0), b_1, \ldots, b_m, \ldots, \qquad (B)$$

$$\vdots$$

$$c_0(= 0), c_1, \ldots, c_m, \ldots. \qquad (C)$$

Vyberme z každé z nich po jednom členu a čísla sečtěme. Množinu všech takovýchto součtů, kde stejné součty uvažujeme pouze jedenkrát, můžeme uspořádat do nové rostoucí posloupnosti

$$n_0(= 0), n_1, \ldots, n_m, \ldots. \qquad (N)$$

Posloupnost N nazveme *součet posloupností A, B, ..., C* a píšeme

$$N = A + B + \ldots + C.$$

Posloupnost N má členy tvaru $a_i + b_j + \ldots + c_l$ a obsahuje všechny členy daných posloupností $A, B, \ldots, C$ (stačí totiž sčítat členy dané posloupnosti s nulovými členy ostatních).

Označíme-li P posloupnost

$$0, 2, 3, 5, 7, 11, 13, \ldots \qquad (P)$$

sestávající se z 0 a všech prvočísel, je možno Goldbachovu hypotézu formulovat takto: *Součet posloupností $P + P + P$ obsahuje všechna přirozená čísla > 1.*

Pak je totiž možno každé přirozené číslo > 1 vyjádřit jako součet nejvýše tří prvočísel.

Jestliže součet k stejných posloupností A obsahuje všechna přirozená čísla, nazýváme A *báze posloupnosti přirozených čísel řádu k* (pak samozřejmě je i bází řádu $k_1 > k$). Řekneme, že je A *báze řádu k pro dostatečně velká přirozená čísla* (tj. pro skoro všechna $n \in \mathbb{N}$), jestliže součet k posloupností A obsahuje skoro všechna přirozená čísla (tj. počínaje jistým členem všechna přirozená $n \in \mathbb{N}$).

Ne každá posloupnost je bází, např. posloupnost všech sudých čísel

$$0, 2, 4, 6. \ldots$$

není bází žádného řádu, neboť sčítáním sudých čísel nelze dostat čísla lichá. Také posloupnost P všech prvočísel není bází, neboť 1 není součtem žádných prvočísel nebo nuly.

Klíčovým pojmem této kapitoly je hustota posloupnosti. Nechť

$$a_0(=0), a_1, \ldots, a_m, \ldots \qquad (A)$$

je uvažovaná posloupnost. Označme $A(n)$ pro $n \in \mathbb{N}$ počet členů posloupnosti A menších nebo rovných n (člen a_0 se nepočítá). Zřejmě pro každé $n \in \mathbb{N}$ platí $0 \leq A(n) \leq n$, odkud

$$0 \leq \frac{A(n)}{n} \leq 1.$$

Jelikož je množina všech čísel $\frac{A(n)}{n}$ ohraničená zdola, má infimum. Označme

$$\alpha = \inf \frac{A(n)}{n},$$

tj. α je takové reálné číslo, že $\alpha \leq \frac{A(n)}{n}$ pro všechna $n \in \mathbb{N}$ a přitom, je-li $\beta \leq \frac{A(n)}{n}$ pro všechna $n \in \mathbb{N}$, je $\beta \leq \alpha$. Číslo α nazýváme (*Schnirelmannova*) *hustota posloupnosti A*. Z definice hustoty přímo plyne, že je-li $a_1 > 1$, pak $\frac{A(1)}{1} = 0$, odkud

$$\alpha = \inf \frac{A(n)}{n} = 0.$$

Je-li hustota posloupnosti $\alpha = 1$, pak A je nutně posloupnost všech přirozených čísel (s prvním členem 1).

Pro hustotu součtu dvou posloupností lze odvodit následující důležitou větu:

Věta 7.4. *Jsou-li α, β hustoty posloupností A, B a γ je hustota posloupnosti $C = A + B$, pak*

$$\gamma \geq \alpha + \beta - \alpha \cdot \beta,$$

neboli

$$1 - \gamma \leq (1 - \alpha)(1 - \beta).$$

Důkaz: Uvažujme v $\mathbb{N}$ interval $\langle 1, n\rangle$ pro $n \in \mathbb{N}$. Ukažme některé prvky tohoto intervalu patřící posloupnosti C:

1) všechna čísla posloupnosti A ležící v tomto intervalu – těch je právě $A(n)$ (stačí vzít v součtu $b_0 = 0$);
2) nechť je mezi sousedními členy a_k, a_{k+1} posloupnosti A právě l_k přirozených čísel $a_k + r_k$, $1 \leq r_k \leq l_k$. Je-li přitom $r_k \in B$, pak $a_k + r_k \in C$. Takových členů posloupnosti C je v intervalu $\langle a_k, a_{k+1}\rangle$ právě $B(l_k)$, a na celém intervalu $\langle 1, n\rangle$ právě $\sum_k B(l_k)$.

Uvedené kategorie čísel z C přitom nevyčerpávají všechny prvky z C na intervalu $\langle 1, n\rangle$, neboť vnitřní body intervalů $\langle a_k, a_{k+1}\rangle$ mohou také patřit C.

Příklad. Uvažujme posloupnosti

$$0, 1^2, 2^2, 3^2, \ldots \tag{A}$$

$$0, 1^3, 2^3, 3^3, \ldots \tag{B}$$

Pak na intervalu $\langle 25; 36\rangle$ lze dle 2) nalézt čísla patřící do posloupnosti $A + B$:

$$25 + 1 = 26, 25 + 8 = 33.$$

Přitom ale také $0 + 27 = 27 \in C$, $1 + 27 = 28 \in C$, $4 + 27 = 31 \in C$.

Pro $n \geq 1$ tedy určitě platí odhad

$$C(n) \leq A(n) + \sum_k B(l_k).$$

Ovšem $B(l_k) \geq \beta \cdot l_k$ (neboť β je hustota B), odkud dostaneme

$$\sum_k B(l_k) \geq \beta \sum_k l_k = \beta(n - A(n)), \tag{1}$$

neboť l_k je počet přirozených čísel v otevřeném intervalu (a_k, a_{k+1}).

Podobně platí také $A(n) \geq \alpha \cdot n$, což po dosazení do vztahu (1) dává

$$C(n) \geq A(n) + \beta(n - A(n)) = A(n)(1 - \beta) + \beta n \geq \alpha(1 - \beta)n + \beta n = (\alpha + \beta - \alpha\beta)n,$$

odkud

$$\gamma = \inf \frac{C(n)}{n} \geq \alpha + \beta - \alpha\beta.$$

Poslední nerovnost je možno přepsat do tvaru

$$1 - \gamma \leq (1 - \alpha)(1 - \beta),$$

který lze zobecnit pro libovolný konečný počet posloupností. □

Pomocí předchozího tvrzení je možno dokázat následující podmínku pro bázi posloupnosti přirozených čísel:

Věta 7.5. *Každá posloupnost kladné hustoty je bází posloupnosti přirozených čísel.*

Důkaz: Nechť A je posloupnost hustoty $\alpha > 0$. Nechť γ je hustota součtu k posloupností A (označme takovou posloupnost A_k), tj. dle předchozího tvrzení

$$1 - \gamma \leq (1 - \alpha)^k.$$

Jelikož $\alpha > 0$, existuje k dostatečně velké tak, že $(1 - \alpha)^k < \frac{1}{2}$, a tedy $\gamma > \frac{1}{2}$. Odtud plyne, že na libovolném intervalu $\langle 1, n\rangle$ je $r_n > \frac{1}{2}n$ členů posloupnosti A_k. Nechť jsou to prvky $c_1, \ldots, c_{r(n)}$. Přidáme-li k nim čísla $0, n - c_1, \ldots, n - c_{r(n)}$, budeme mít celkem $2r_n + 1 > n + 1$ čísel intervalu $\langle 0, n\rangle$. To ale znamená, že alespoň dvě z nich jsou stejná, tj.

$$n - c_i = c_j,$$

$$n = c_i + c_j$$

pro některá i, j. Pak ale libovolné přirozené n je součtem prvků z A_k, tj. A je báze řádu $\leq 2k$. □

Předchozí tvrzení použil Schnirelmann při řešení Goldbachovy hypotézy. Bezprostředně ji však použít nelze, neboť hustota posloupnosti

$$0, 1, 2, 3, 5, 7, 11, 13, \ldots \qquad (P')$$

nuly, jedničky a všech prvočísel je nula. Avšak Schnirelmann dokázal, že

posloupnost $P + P'$ má kladnou hustotu.

Odtud bezprostředně vyplývá, že

posloupnost $P + P'$ (a tedy i P') je bází posloupnosti N,

tedy

každé přirozené číslo $n \neq 1$ je součtem konečného počtu prvočísel nezávisejícího na n.

Uveďme na závěr, že Linnik v r. 1943 vyřešil užitím uvedené metody elementárním způsobem Waringův problém, když dokázal, že

pro libovolné $n \in \mathbb{N}$ tvoří posloupnost

$0, 1^n, 2^n, \ldots, k^n, \ldots$ *bázi posloupnost N.*

Cvičení

98. Ověřte, která z prvočísel p je možno rozložit v součet dvou kvadrátů:

    113, 151, 541, 757, 811, 1091, 1423.

99. Víte-li, že $317 = 11^2 + 14^2$ a $281 = 5^2 + 16^2$, rozložte na součet dvou kvadrátů číslo $N = 317 \cdot 281 = 89077$.

    Podobnou úlohu řešte, víte-li, že $937 = 19^2 + 24^2$ a $746 = 11^2 + 25^2$.

100. Dokažte, že neexistují různé mřížové body stejně vzdálené od bodu o souřadnicích $Q = (\sqrt{2}, \frac{1}{3})$.

101. Dokažte, že pro každé přirozené číslo n existuje takový kruh se středem v bodě $Q = (\sqrt{2}, \frac{1}{3})$, že uvnitř něho leží právě n mřížových bodů.

102. Rozložte v součet čtyř kvadrátů číslo

$$5220 = \left(1^2 + 2^2 + 3^2 + 4^2\right)\left(5^2 + 6^2 + 7^2 + 8^2\right).$$

Kapitola 8

Kvadratická tělesa, celá algebraická čísla

8.1 Základní pojmy

Jak již bylo uvedeno, algebraickým číslem rozumíme každé komplexní číslo α, které je kořenem některého polynomu

$$a_0 x^n + \ldots + a_n \in \mathbb{Q}[x].$$

Celým algebraickým číslem je každé komplexní číslo ω, které je kořenem polynomu

$$x^n + b_1 x^{n-1} + \ldots + b_n, \quad b_1, \ldots, b_n \in \mathbb{Z}. \tag{1}$$

Z definice je přitom zřejmé, že každé celé algebraické číslo je algebraické, opak však obecně neplatí:

Věta 8.1. *Racionální číslo r je celé algebraické, právě když $r \in \mathbb{Z}$.*

Důkaz: Zřejmě každé $r \in \mathbb{Z}$ je celým algebraickým číslem, neboť je kořenem rovnice $x - r = 0$.

Nechť $r \in \mathbb{Q}$ je celé algebraické číslo, nechť je kořenem rovnice (1) a nechť $r = \frac{c}{d}$ pro $c, d \in \mathbb{Z}$, $(c, d) = 1$. Dosazením za r do (1) dostaneme

$$c^n + b_1 d c^{n-1} + \ldots + b_n d^n = 0,$$

odkud $d | c^n$ a jelikož $(c, d) = 1$, je $d = \pm 1$ a $r = \frac{c}{d} \in \mathbb{Z}$. □

Zabývejme se nyní otázkami vlastností množiny algebraických (celých algebraických) čísel vzhledem k operacím sčítání a násobení. K tomu zaveďme nejprve následující užitečné pojmy.

Podmnožina $V \subseteq \mathbb{C}$ komplexních čísel se nazývá $\mathbb{Q}$-*modul*, jestliže platí:

1) $\gamma_1, \gamma_2 \in V \Rightarrow \gamma_1 \pm \gamma_2 \in V$

2) $\gamma \in V, r \in \mathbb{Q} \Rightarrow r\gamma \in V$

3) každý prvek $\gamma \in V$ je $\mathbb{Q}$-lineární kombinací některých prvků $\gamma_1, \ldots, \gamma_n \in V$, tj.

$$\gamma = \sum_{i=1}^{n} r_i \gamma_i$$

pro $r_i \in \mathbb{Q}$.

Jinak řečeno, $V \subseteq \mathbb{C}$ je $\mathbb{Q}$-modul, právě když je V vektorovým prostorem konečné dimenze nad $\mathbb{Q}$.

Pro prvky $\gamma_1, \ldots, \gamma_n \in V$ označme symbolem $[\gamma_1, \ldots, \gamma_n]$ $\mathbb{Q}$-modul generovaný množinou $\{\gamma_1, \ldots, \gamma_n\}$, tj.

$$[\gamma_1, \ldots, \gamma_n] = \left\{ \sum_{i=1}^{n} r_i \gamma_i; r_i \in \mathbb{Q} \right\}.$$

Věta 8.2. *Nechť $V = [\gamma_1, \ldots, \gamma_n] \neq \{0\}$, nechť pro prvek $\alpha \in \mathbb{C}$ platí vlastnost $\alpha\gamma \in V$ pro každé $\gamma \in V$. Pak α je algebraické číslo.*

Důkaz: Dle předpokladu platí $\alpha\gamma_i \in V$ pro $i = 1, \ldots, n$. Pro každé i existují prvky $a_{ij} \in \mathbb{Q}$, $j = 1, \ldots, n$ tak, že

$$\sum_{j=1}^{n} a_{ij}\gamma_j = \alpha\gamma_i = \sum_{j=1}^{n} \delta_{ij}\alpha\gamma_j, \quad \text{tedy} \quad \sum_{j=1}^{n} (a_{ij} - \delta_{ij}\alpha)\gamma_j = 0.$$

Přitom nenulový vektor $(\gamma_1, \ldots, \gamma_n)$ je netriviálním řešením homogenní soustavy s maticí $(a_{ij} - \delta_{ij}\alpha)$, platí tedy

$$\det\,(a_{ij} - \delta_{ij}\alpha) = 0.$$

Výpočtem determinantu zjistíme, že α je kořenem polynomu stupně n s koeficienty z $\mathbb{Q}$, tj. α je algebraické číslo. □

Věta 8.3. *Množina všech algebraických čísel tvoří těleso.*

Důkaz: Nechť α_1, α_2 jsou algebraická čísla. Ukažme, že také $\alpha_1 + \alpha_2$, $\alpha_1\alpha_2$ jsou algebraická čísla. Nechť

$$\alpha_1^n + r_1\alpha_1^{n-1} + \ldots + r_n = 0, \qquad \alpha_2^m + s_1\alpha_2^{m-1} + \ldots + s_m = 0,$$

kde $r_i, s_j \in \mathbb{Q}$. Nechť $V = [\alpha_1^i\alpha_2^j; i \in \{0, \ldots, n-1\}, j \in \{0, \ldots, m-1\}]$. Je-li $\gamma \in V$, pak

$$\gamma = \sum r_{ij}\alpha_1^i\alpha_2^j$$

pro některá $r_{ij} \in \mathbb{Q}$. Dále

$$\alpha_1\gamma = \sum r_{ij}\alpha_1^{i+1}\alpha_2^j \in V, \qquad \alpha_2\gamma = \sum r_{ij}\alpha_1^i\alpha_2^{j+1} \in V.$$

Pak ovšem $\alpha_1\gamma + \alpha_2\gamma = (\alpha_1 + \alpha_2)\gamma \in V$, $(\alpha_1\alpha_2)\gamma \in V$, tedy dle předchozího tvrzení jsou $\alpha_1 + \alpha_2$ a $\alpha_1\alpha_2$ algebraická čísla.

Je třeba ještě dokázat, že α_1^{-1} je algebraické. K tomu si stačí uvědomit, že α_1^{-1} je řešením rovnice $r_n x^n + \ldots + r_1 x + 1 = 0$. □

Podmnožina $W \subseteq \mathbb{C}$ se nazývá $\mathbb{Z}$-*modul*, platí-li podmínky

1') $\gamma_1, \gamma_2 \in W \Rightarrow \gamma_1 \pm \gamma_2 \in W$

2') každý prvek $\gamma \in W$ je $\mathbb{Z}$-lineární kombinací některých prvků $\gamma_1, \ldots, \gamma_n \in$ $\in W$, tj.

$$\gamma = \left\{ \sum_{r=1}^{n} b_i \gamma_i; b_i \in \mathbb{Z} \right\}.$$

Následující tvrzení pro $\mathbb{Z}$-moduly jsou analogická předchozím tvrzením pro $\mathbb{Q}$-moduly:

Věta 8.4. *Nechť $W \neq \{0\}$ je nějaký $\mathbb{Z}$-modul, nechť prvek $\omega \in \mathbb{C}$ má vlastnost $\omega\gamma \in W$ pro každé $\gamma \in W$. Pak ω je celé algebraické číslo.*

Věta 8.5. *Množina všech celých algebraických čísel tvoří okruh.*

Připomeňme ještě některé další vlastnosti algebraických čísel. Je-li α algebraické číslo, existuje normovaný polynom nejnižšího stupně $f(x) \in \mathbb{Q}[x]$ takový, že α je jeho kořenem. Polynom f je určen *jednoznačně* a nazývá se *minimální polynom prvku* α. Dále platí, že je-li α kořenem některého polynomu $g(x) \in \mathbb{Q}[x]$, pak $f(x)|g(x)$ a polynom f je *ireducibilní* v $\mathbb{Q}[x]$.

Označme symbolem $\mathbb{Q}(\alpha)$ těleso vzniklé z $\mathbb{Q}$ adjunkcí algebraického prvku α stupně n (tj. $\mathbb{Q}(\alpha)$ je nejmenší podtěleso $\mathbb{C}$ obsahující množinu $\mathbb{Q} \cup \{\alpha\}$). Lze dokázat, že

$$\mathbb{Q}(\alpha) = \{g(\alpha); g(x) \in \mathbb{Q}[x], \text{ stupeň } g(x) < n\};$$

těleso $\mathbb{Q}(\alpha)$ nazýváme *jednoduché algebraické rozšíření* tělesa $\mathbb{Q}$. Lze jej chápat také jakožto vektorový prostor nad $\mathbb{Q}$, jehož dimenzi $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ nazýváme *stupeň nadtělesa* $\mathbb{Q}(\alpha)$ nad $\mathbb{Q}$. Je-li přitom f minimální polynom prvku α stupně n (tj. α je algebraický stupně n), pak prvky $1, \alpha, \ldots, \alpha^{n-1}$ generují vektorový prostor $\mathbb{Q}(\alpha)$ nad $\mathbb{Q}$ a platí $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.

V této kapitole se budeme dále zabývat algebraickými prvky α stupně 2, tj. prvky, které jsou kořeny nějaké kvadratické rovnice

$$a_0 x^2 + a_1 x + a_2 = 0,$$

kde $a_0 \neq 0$, $a_0, a_1, a_2 \in \mathbb{Q}$. Kořeny takovýchto rovnic mají obecný tvar

$$\alpha = \frac{a + b\sqrt{m}}{c}, \tag{1}$$

kde $a, b, c, m \in \mathbb{Z}$. Můžeme přitom předpokládat, že m nemá žádného dělitele ve tvaru kvadrátu. Tělesa $\mathbb{Q}(\alpha)$ nazýváme *kvadratická tělesa* a jejich celá algebraická čísla $D \subseteq \mathbb{Q}(\alpha)$ nazýváme *celá algebraická čísla* tělesa $\mathbb{Q}(\alpha)$.

Prvním problémem, kterým se budeme zabývat, je nalezení celých algebraických čísel v obecných kvadratických tělesech.

Z rovnosti (1) je zřejmé, že $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{m})$. Úpravou (1) dostaneme vztah

$$(c\alpha - a)^2 = mb^2,$$

tj. α je kořenem rovnice

$$c^2x^2 - 2acx + a^2 - mb^2 = 0. \tag{2}$$

Můžeme navíc předpokládat, že $c > 0$ a $(a, b, c) = 1$. Vydělením rovnice (2) číslem c^2 dostaneme

$$x^2 - \frac{2a}{c}x + \frac{a^2 - mb^2}{c^2} = 0. \tag{3}$$

Celá algebraická čísla D v $\mathbb{Q}(\alpha)$ jsou právě ty prvky, které vyhovují rovnici (3) pro celočíselné koeficienty, tedy pro něž je $\frac{2a}{c} \in \mathbb{Z}$, $\frac{a^2-mb^2}{c^2} \in \mathbb{Z}$, tj. $c|2a$, $c^2|(a^2 - mb^2)$. Je-li $d = (a, c)$, pak $d^2|a^2$, $d^2|c^2$, $d^2|c^2|(a^2 - mb^2)$, odkud $d^2|mb^2$ a $d|b$, neboť m nemá dělitele, který je kvadrátem. Ovšem $(a, b, c) = 1$, tedy $d = 1$. Odtud a z podmínky $c|2a$ plyne $c|2$, a tedy $\underline{c = 1 \text{ nebo } c = 2.}$

Je-li $c = 2$, pak a je liché (jinak by platilo $2|c$, $2|a$ a $(a, c) \neq 1$), a tedy $mb^2 \equiv a^2 \equiv 1 \pmod 4$. To ale znamená, že b je liché (jinak by $mb^2 \equiv 0 \pmod 4$), tj. $b^2 \equiv 1 \pmod 4$, odkud $m \equiv 1 \pmod 4$. Rozlišíme dva případy:

(i) Je-li $\underline{m \not\equiv 1 \pmod 4}$, pak vzhledem k předešlým úvahám je $c = 1$ a celá algebraická čísla tělesa $\mathbb{Q}(\sqrt{m})$ jsou tvaru

$$\alpha = a + b\sqrt{m}, a, b \in \mathbb{Z}.$$

(ii) Je-li $\underline{m \equiv 1 \pmod 4}$ a $c = 2$, jsou a, b lichá, tedy

$$\alpha = \frac{a + b\sqrt{m}}{2} = \frac{a + b}{2} + \frac{1}{2}b(\sqrt{m} - 1),$$

tj. $\alpha = a_1 + b_1\tau$, kde $a_1 = \frac{1}{2}(a + b) \in \mathbb{Z}$, $b_1 = b \in \mathbb{Z}$, $\tau = \frac{1}{2}(-1 + \sqrt{m})$. Pro $c = 1$ dostaneme

$$\alpha = a + b\sqrt{m} = a + b + 2b\tau = a_1 + b_1\tau,$$

kde $a_1, b_1 \in \mathbb{Z}$.

Celkem tedy platí věta:

Věta 8.6. *Celá algebraická čísla $\mathbb{Q}(\sqrt{m})$ jsou čísla $a+b\sqrt{m}$ pro $m \equiv 2, 3 \pmod 4$ a čísla $a + b\tau = a + \frac{1}{2}b(-1 + \sqrt{m})$ pro $m \equiv 1 \pmod 4$, kde $a, b \in \mathbb{Z}$.*

Příklad. Pro $m = -1$ je $m \equiv 3 \pmod 4$, jsou tedy celá algebraická čísla tělesa $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\mathrm{i})$ čísla $a + b\mathrm{i}, a, b \in \mathbb{Z}$ (jsou to právě prvky oboru integrity Gaussových celých čísel). Pro $m = -3$ je $m \equiv 1 \pmod 4$, tedy celá algebraická čísla tělesa $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(3\mathrm{i})$ jsou ve tvaru $a + b\omega$, kde $\omega = \frac{1}{2}(-1 + \sqrt{3}\mathrm{i}), a, b, \in \mathbb{Z}$. Dostaneme tedy Eisensteinova celá čísla.

Cvičení

103. Najděte rozklady v kvadratickém tělese $\mathbb{Z}(\mathrm{i})$ pro:

a) 97; b) 137; c) 181; d) 281; e) 317.

104. Dokažte, že průsečíky kružnice $x^2 + y^2 = 1$ s přímkami $y = kx - 1$, kde $k \in \mathbb{Q}$, jsou všechny racionální body kružnice. Udělejte náčrtek.

Dokázali jsme, že celá algebraická čísla v tělesech $\mathbb{Q}(\sqrt{m})$ tvoří obor integrity – označme je $D(\sqrt{m})$. Prozkoumejme nyní vlastnosti oborů $D(\sqrt{m})$ z hlediska dělitelnosti.

Každý z prvků $D(\sqrt{m})$ je tvaru

$\alpha = r + s\sqrt{m}$, $s, r \in \mathbb{Z}$, pro $m \equiv 2, 3 \pmod 4$

nebo

$\alpha = r + s\tau = (r - \frac{1}{2}s) + \frac{1}{2}s\sqrt{m}$, $r, s \in \mathbb{Z}$, pro $m \equiv 1 \pmod 4$.

V prvním případě označme $\overline{\alpha} = r - s\sqrt{m}$, ve druhém $\overline{\alpha} = (r - \frac{1}{2}s) - \frac{1}{2}s\sqrt{m}$ a nazývejme tyto prvky *konjugované* k prvku α. V obou případech definujeme normu prvku α následovně:

$$N(\alpha) = \alpha\overline{\alpha}.$$

V případě $m \equiv 2, 3 \pmod 4$ je

$$N(a + b\sqrt{m}) = a^2 - mb^2,$$

pro $m \equiv 1 \pmod 4$ je

$$N(a + b\tau) = \left(a - \frac{1}{2}b\right)^2 - \frac{1}{4}mb^2 = a^2 - ab + \frac{1}{4}b^2(1 - m).$$

Normy prvků splňují následující elementární vlastnosti:

1) norma prvku je vždy celé číslo,
2) norma zachovává součin, tj. $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$,
3) α je jednotka dělení v $D(\sqrt{m})$, právě když $N(\alpha) = \pm 1$,
4) $\alpha | \beta$ implikuje $N(\alpha) | N(\beta)$.

Vlastnost 1) je zřejmá, 2) lze ověřit přímým výpočtem. Dokažme vlastnost 3):
Je-li α jednotka, tj. $\alpha | 1$, pak existuje prvek γ tak, že $\alpha\gamma = 1$. Dle 2) pak

$$N(\alpha)N(\gamma) = N(\alpha\gamma) = N(1) = 1,$$

odkud $N(\alpha) | 1, N(\alpha) = \pm 1$. Naopak, pro každý prvek α platí $N(\alpha) = \alpha \cdot \overline{\alpha}$, a tedy $\alpha | N(\alpha)$. Platí-li $N(\alpha) = \pm 1$, pak $\alpha | \pm 1$, tj. α je jednotka.

Vlastnost 4) je přímým důsledkem 2).

Díky vlastnosti 3) je možno popsat všechny jednotky dělení v oborech integrity $D(\sqrt{m})$: je-li $m < 0$, je $m = -y$ pro $y > 0$ a jednotky vyhovují rovnicím

$$a^2 + yb^2 = 1 \quad \text{pro } m \equiv 2, 3 \pmod 4,$$
$$\left(a - \frac{1}{2}b\right)^2 + \frac{1}{4}yb^2 = 1 \quad \text{pro } m \equiv 1 \pmod 4.$$

Tyto rovnice mají vždy pouze *konečný* počet řešení, speciálně pro

- $m = -1$ jsou to prvky $\pm 1, \pm \mathrm{i}$,
- $m = -3$ prvky $\pm 1, \pm\omega, \pm\omega^2$, kde $\omega = \frac{1}{2}(-1 + \mathrm{i}\sqrt{3})$,
- $m < -3$ jen prvky ± 1.

Diametrálně odlišná situace nastane v případě $m > 0$. Je-li např. $m = 2$, pak všechny jednotky vyhovují rovnici

$$a^2 - 2b^2 = \pm 1,$$

mající *nekonečně mnoho* řešení (v prvním případě se jedná o Pellovu rovnici, viz 5.2). Všechny jednotky je pak možno nalézt z rekurentních vztahů

$$a + b\sqrt{2} = \pm(1 + \sqrt{2})^{2n}, \quad a + b\sqrt{2} = \pm(1 + \sqrt{2})^{2n+1}, \quad n \in \mathbb{N}.$$

Jako bezprostřední důsledek vlastností normy dostaneme větu:

Věta 8.7. *Každý prvek α takový, že $N(\alpha)$ je prvočíslo, je ireducibilní v $D(\sqrt{m})$. Obory integrity $D(\sqrt{m})$ splňují podmínku EIR, tj. každý prvek je součinem konečného počtu ireducibilních prvků.*

Ne všechny obory integrity $D(\sqrt{m})$ však splňují podmínku JIR, tj. rozklady na součin ireducibilních prvků nemusejí být jednoznačné:

Příklad. Pro $m = -5$ platí $-5 \equiv 3 \pmod 4$ a $D(\sqrt{-5}) = \{a + b\mathrm{i}\sqrt{5}; a, b \in \mathbb{Z}\}$. Čísla $2, 3, 1 - \mathrm{i}\sqrt{5}, 1 + \mathrm{i}\sqrt{5} \in D(\sqrt{-5})$ jsou ireducibilní, přitom rozklad čísla 6 není jednoznačný:

$$6 = 2 \cdot 3 = (1 - \mathrm{i}\sqrt{5})(1 + \mathrm{i}\sqrt{5}).$$

Podobně v okruhu $D(\sqrt{10})$ nejsou také rozklady jednoznačné, neboť

$$6 = 2 \cdot 3 = (4 - \sqrt{10})(4 + \sqrt{10}).$$

Zkoumejme, které z oborů integrity $D(\sqrt{m})$ jsou eukleidovské s eukleidovskou funkcí $|N(\alpha)|$, tj. kdy splňují podmínku

$$\forall \gamma, \gamma_1 \in D(\sqrt{m}), \gamma_1 \neq 0 \ \exists k, \gamma_2 \in D(\sqrt{m}):$$
$$\gamma = k\gamma_1 + \gamma_2, \text{ kde } \gamma_2 = 0 \text{ nebo } |N(\gamma_2)| < |N(\gamma_1)|. \tag{1}$$

Podmínka (1) je ekvivalentní s podmínkou

$$\forall \delta \in \mathbb{Q}(\sqrt{m})\ \exists k \in D(\sqrt{m})\colon |N(\delta - k)| < 1. \tag{2}$$

Skutečně, definujme pro prvky z $\mathbb{Q}(\sqrt{m})$ normu takto:

je-li $\delta = \frac{\gamma_1}{\gamma_2}$, kde $\gamma_1, \gamma_2 \in D(\sqrt{m})$, pak $N(\delta) = \frac{N(\gamma_1)}{N(\gamma_2)}$.

Z podmínky (1) pak plyne $\frac{\gamma}{\gamma_1} = k + \frac{\gamma_2}{\gamma_1}$, tedy $\frac{\gamma_2}{\gamma_1} = \frac{\gamma}{\gamma_1} - k$. Odtud dostaneme

$$\left| N\left(\frac{\gamma}{\gamma_1} - k\right)\right| = \left| N\left(\frac{\gamma_2}{\gamma_1}\right)\right| = \left|\frac{N(\gamma_2)}{N(\gamma_1)}\right| < 1,$$

neboť $|N(\gamma_2)| < |N(\gamma_1)|$.

Je-li tedy dán prvek $\delta = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, existuje dle (2) vždy prvek $k = x + y\sqrt{m} \in \mathbb{Z}(\sqrt{m})$ takový, že pro

$m \equiv 2, 3 \pmod 4$ je

$$|(r-x)^2 - m(s-y)^2| < 1, \tag{3}$$

$m \equiv 1 \pmod 4$ je

$$\left|\left(r - x - \frac{1}{2}y\right)^2 - m\left(s - \frac{1}{2}y\right)^2\right| < 1. \tag{4}$$

Pro $m = \mu < 0$ je snadné určit všechna $m \in \mathbb{Z}$ tak, aby pro daná $r, s \in \mathbb{Q}$ existovala vhodná čísla $x, y \in \mathbb{Z}$ splňující vztahy (3), resp. (4).

Věta 8.8. *$D(\sqrt{m})$ je pro $m < 0$ eukleidovský obor integrity, právě když*

$$m = -1, -2, -3, -7, -11.$$

Důkaz: Rozlišme dva případy:

1) $m \equiv 2, 3 \pmod 4$. Vezměme $r = s = \frac{1}{2}$ v podmínce (3). Pak

$$\left(\frac{1}{2} - x\right)^2 \geq \frac{1}{4}, \quad -m\left(\frac{1}{2} - y\right)^2 \geq \frac{1}{4}\mu,$$

tedy

$$1 > \left|\left(\frac{1}{2} - x\right)^2 - m\left(\frac{1}{2} - y\right)^2\right| \geq \left|\frac{1}{4} + \frac{1}{4}\mu\right|.$$

Z poslední nerovnosti plyne, že $\mu < 3$, tj. $\underline{m = -1, -2}$. V obou případech zvolíme $x, y \in \mathbb{Z}$ tak, aby platilo

$$|x - r| \leq \frac{1}{2}, |y - r| \leq \frac{1}{2}$$

(takový výběr je vždy možný), tedy

$$(r-x)^2 - m(s-y)^2 \leq \frac{1}{4} + \frac{1}{4}\mu < 1.$$

2) $m \equiv 1 \pmod 4$. V podmínce (4) zvolíme $r = s = \frac{1}{4}$. Dostaneme

$$\left(\frac{1}{4} - x - \frac{1}{2}y\right)^2 \geq \frac{1}{16}, \quad -m\left(s - \frac{1}{2}y\right)^2 \geq \frac{\mu}{16},$$

tedy

$$1 > \left|\left(\frac{1}{4} - x - \frac{1}{2}y\right)^2 - m\left(s - \frac{1}{2}y\right)^2\right| \geq \left|\frac{1}{16} + \frac{\mu}{16}\right|.$$

Poslední nerovnost dává podmínku $\mu < 15$, což vzhledem k $\mu \equiv 3 \pmod 4$ znamená $\mu = 3, 7, 11$ a $\underline{m = -3, -7, -11}$. Pro daná čísla $r, s \in \mathbb{Q}$ vždy existují $x, y \in \mathbb{Z}$ tak, že

$$|2s - y| \leq \frac{1}{2}, \quad \left|r - x - \frac{1}{2}y\right| \leq \frac{1}{2},$$

tedy

$$\left|\left(r - x - \frac{1}{2}\right)^2 - m\left(s - \frac{1}{2}y\right)^2\right| \leq \frac{1}{4} + \frac{\mu}{16} < \frac{1}{4} + \frac{11}{16} = \frac{15}{16} < 1.$$

□

Mnohem obtížnější je najít hodnoty m, pro něž je obor integrity $D(\sqrt{m})$ alespoň Gaussův.

Věta 8.9. *Pro $m < 0$ je obor integrity $D(\sqrt{m})$ Gaussův pro*

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Existuje přitom ještě nejvýše jedno $m < 0$ tak, že $D(\sqrt{m})$ je Gaussův, přičemž $m < 5 \cdot 10^9$.

Pro $m > 0$ platí následující věta:

Věta 8.10. *Pro $m > 0$ je obor integrity $D(\sqrt{m})$ Gaussův, právě když*

$$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Důkaz: Tvrzení nebudeme dokazovat v plné obecnosti, ale pro jednoduchost pouze pro $m = 2, 3, 5, 6, 7, 11, 13, 17, 21, 29$. V případě

- $m \not\equiv 1 \pmod 4$ položme $\lambda = 0$, $n = m$,
- $m \equiv 1 \pmod 4$ položme $\lambda = \frac{1}{2}$, $n = \frac{1}{4}m$.

Vztahy (3) a (4) lze pak zapsat ve společném tvaru

$$|(r - x - \lambda y)^2 - n(s - y)^2| < 1, \tag{5}$$

přičemž v případě $m \equiv 1 \pmod 4$ klademe $s := 2s$.

Není-li $D(\sqrt{m})$ eukleidovský, pak vztah (5) neplatí pro některá $r, s \in \mathbb{Q}$ a každá $x, y \in \mathbb{Z}$. Lze předpokládat, že $0 \leq r \leq \frac{1}{2}$, $0 \leq s \leq \frac{1}{2}$. Pro tato r, s pak pro všechna $x, y \in \mathbb{Z}$ platí jedna z nerovností

$$(r - x - \lambda y)^2 \geq 1 + n(s - y)^2, \qquad P(x, y)$$

$$n(s - y)^2 \geq 1 + (r - x - \lambda y)^2. \qquad N(x, y)$$

Uvažujme speciálně nerovnosti

$P(0,0)$: $r^2 \geq 1 + ns^2$	$N(0,0)$: $ns^2 \geq 1 + r^2$
$P(1,0)$: $(1-r)^2 \geq 1 + ns^2$	$N(1,0)$: $ns^2 \geq 1 + (1-r)^2$
$P(-1,0)$: $(1+r)^2 \geq 1 + ns^2$	$N(-1,0)$: $ns^2 \geq 1 + (1+r)^2$.

Je-li $r = s = 0$, pak nerovnosti $P(0,0)$ a $N(0,0)$ neplatí, tedy platí nutně $N(0,0)$ a $N(1,0)$. Kdyby navíc platilo $P(-1,0)$, pak bychom z $P(-1,0)$ a $N(1,0)$ dostali

$$(1+r)^2 \geq 1 + ns^2 \geq 2 + (1-r)^2,$$

odkud $4r \geq 2, r \geq \frac{1}{2}$. Je tedy $r = \frac{1}{2}$ a $ns^2 = \frac{5}{4}$. Nechť dále $s = \frac{p}{q}$, kde $(p, q) = 1$. V případě $m \not\equiv 1 \pmod 4$ je $m = n$ a

$$4mp^2 = 5q^2.$$

Platí tedy $p^2|5$, tj. $p = 1$ a $q^2|4m$. Jelikož m nemá za dělitele kvadrát a $0 \leq s \leq \frac{1}{2}$, dostaneme $q = 2$, $s = \frac{1}{2}$ a $m = 5 \equiv 1 \pmod 4$, spor.

V případě $m \equiv 1 \pmod 4$ by bylo $m = 4n$, odkud

$$mp^2 = 5q^2.$$

To ale implikuje $p = 1, q = 1, s = 1$, což je opět spor.

Nerovnost $P(-1,0)$ tedy neplatí, a tudíž platí $N(-1,0)$. Celkem dostaneme

$$ns^2 \geq 1 + (1+r)^2 \geq 2, \underline{n \geq 8}.$$

Pro $n < 8$ jsou tedy $D(\sqrt{m})$ eukleidovské obory integrity, tj. pro

$$m = 2, 3, 5, 6, 7, 13, 17, 21, 29.$$

□

Příklad. Ukažme, že obor integrity $D(\sqrt{23})$ není eukleidovský.
Řešení: Položme v podmínce (5) $r = 0, s = \frac{7}{23}$. Vzhledem k tomu, že $23 \equiv 3 \pmod 4$, je $\lambda = 0$, $n = m = 23$ a nerovnost (5) má tvar

$$|23x^2 - (23y - 7)^2| \leq 23.$$

Jelikož $\xi = 23x^2 - (23 - y)^2 \equiv -49 \equiv -3 \pmod{23}$, je $\xi = -3$ nebo $\xi = 20$. Položme $Y = 23y - 7$.

V prvním případě by platilo $\xi = 23x^2 - Y^2 = -3$, tj.

$$2x^2 \equiv Y^2 \pmod 3.$$

Kdyby dále platilo $x \equiv 0$ nebo $Y \equiv 0 \pmod 3$, pak by $9|\xi = -3$, spor.

Je tedy $x, Y \not\equiv 0 \pmod 3$, odkud $x^2, Y^2 \equiv 1 \pmod 3$, tedy

$$\xi = 23 - 1 = 22 \equiv 1 \pmod 3,$$

spor. Podobně ke sporu dojdeme i v případě $\xi = 20$.

Cvičení

105. Dokažte, že neexistují celá čísla x, y tak, že platí

$$23x^2 - (23y - 7)^2 = 20.$$

Kapitola 9

Některé významné problémy v teorii čísel

Mnoho významných problémů v teorii čísel má u matematiků širokou popularitu. V teorii čísel se u problémů více než kde jinde užívá ještě přívlastek „notorický“. Je to proto, že problémy v teorii čísel, ačkoli jsou často snadno formulovatelné a užívají pouze nejelementárnějších pojmů, se dokazují neobyčejně složitě.

Pro zajímavost uveďme několik zajímavých problémů, z nichž některé budou srozumitelné každému, kdo umí sčítat a násobit.

9.1 Velká Fermatova věta (VFV)

Problém 1. Existují pro přirozené číslo $n > 2$ čísla $x, y, z \in \mathbb{N}$ tak, že platí $x^n + y^n = z^n$?

Bylo známo už ve starověku (Pythagorejci), že součet dvou kvadrátů čísel může být opět kvadrátem, dokonce, že takových trojic čísel existuje nekonečně mnoho. Fermat se pokoušel o zobecnění tohoto výsledku. Ve své kopii Diofantovy knihy na okraj strany píše: „Je nemožné dostat třetí, resp. čtvrtou mocninu ze dvou třetích, resp. čtvrtých mocnin; objevil jsem pozoruhodný důkaz, který se však nevejde na okraj této stránky“. Od té doby zůstávala jeho domněnka nedokázána a stala se jedním z „notorických“ problémů teorie čísel. Ukažme vývoj při dokazování negativní odpovědi na problém 1 (viz tabulka 9.1).

Od důkazu Fermata pro $n = 4$ plynula platnost VFV pro všechny násobky čtyř, tj. pro 25 % exponentů. Přesněji, označíme-li pro x symbolem $N(x)$ počet exponentů z $[2, x]$, pro něž VFV platí, pak Fermat dokázal, že asymptoticky $\frac{N(x)}{x} > \frac{1}{4} - \varepsilon$ pro každé $\varepsilon > 0$. Eulerův důkaz pro $n = 3$ znamenal, že asymptoticky

$$\frac{N(x)}{x} > \frac{1}{3} + \frac{1}{4} - \frac{1}{12} - \varepsilon = \frac{1}{2} - \varepsilon,$$

($\frac{1}{12}$ se odečítá, protože tolik je násobků 3 a 4 zároveň), tj. platnost pro 50 % exponentů.

1659	Fermat	$n = 4$
1753	Euler	$n = 3$
1825	Dirichlet, Legendre	$n = 5$
1839	Lamé	$n = 7$
1847	Kummer	$n \leq 100$
1930–7	Vandiver	$n < 617$
1953	Inkeri	je-li (x, y, z) protipříklad VFV s exponentem p, pak $x > \left(\frac{2p^3 + p}{\log 3p}\right)^p$
1954	Lehmer, Vandiver	$n \leq 2500$ (užili počítače)
1976	Wagstaff	$n \leq 125\,000$
1983	Faltings	pro $n \geq 3$ existuje pouze konečně mnoho řešení
1985	Granville, Heath	VFV platí pro skoro všechny exponenty
1987	Tanner, Wagstaff	$n \leq 150\,000$
1991	Buhler, Crandall, Sompolski	$n \leq 1\,000\,000$
1995	Wiles	VFV dokázána

Tabulka: Vývoj řešení VFV

Wagstaffův důkaz pro $n \leq 125\,000$ dával asymptotickou platnost pro 93 % exponentů. Teprve Faltingsův výsledek z roku 1983 umožnil dokázat, že

$$\lim_{x \to \infty} \frac{N(x)}{x} = 1,$$

tj. že VFV platí asymptoticky pro 100 % exponentů.

Důkaz pro $n \leq 1\,000\,000$ spolu s Inkeriho výsledkem znamenal, že protipříklad k VFV by musel být takový, že x^n má alespoň 10^{13} cifer!

Dnes je důkaz VFV minulostí, neboť roku 1995 publikoval A. Wiles 108stránkovou práci, obsahující její úplný důkaz. Zájemce odkazujeme na populární knihu S. Singha [9] nebo velmi zajímavý dokument http://spotter.cz/931699-posledni-fermatova-veta.htm#! věnované osobě A. Wilese a jeho řešení VFV.

Piere de Fermat (1601-1665) byl matematikem s geniální intuicí. V některých případech může být však intuice i scestná. Euler se např. domníval, že lze Fermatovu větu zobecnit na tvrzení: „Součet méně než n n-tých mocnin čísel nemůže být pro $n \geq 3$ n-tou mocninou“. Roku 1966 však byla pomocí počítače dokázána rovnost

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

a později

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

Pro šesté mocniny platnost či neplatnost Eulerovy domněnky není dosud známa:

Problém 2. Může být součet pěti šestých mocnin čísel opět šestou mocninou?

9.2 Dokonalé krabice

Problém 3. Existuje krabice s celočíselnými stranami taková, aby všechny stěnové a tělesové úhlopříčky byly opět celými čísly?

Problém vede k řešení následující soustavy diofantických rovnic:

$$x^2 + y^2 = a^2, \quad x^2 + z^2 = b^2, \quad y^2 + z^2 = c^2, \quad x^2 + y^2 + z^2 = d^2,$$

kde x, y, z reprezentují strany krabice a, b, c stěnové úhlopříčky, d tělesovou úhlopříčku.

Byly řešeny o něco jednodušší modifikace problému 3, a to:

1) nemusí-li být tělesová úhlopříčka d celočíselná,

2) nemusí-li být některá stěnová uhlopříčka celočíselná,

3) nemusí-li být některá hrana celočíselná.

Ve všech případech je známo nekonečně mnoho řešení, přičemž nejmenší z nich jsou v případě

1) $x = 44, y = 117, z = 240$;

2) $x = 104, y = 153, z = 672$;

3) $x = 124, y = 957, z = \sqrt{13852800}$;

Řada neřešených diofantických rovnic pochází z rovinné geometrie:

Problém 4. Existuje obdélník s celočíselnými stranami a bod uvnitř něho mající od všech vrcholů celočíselné vzdálenosti?

Heronův trojúhelník je trojúhelník s celočíselnými stranami a obsahem. Např. trojúhelník o stranách 13, 14, 15 má obsah 84, je tedy Heronův. Následující zobecnění se 7 neznámými je však neřešeno:

Problém 5. Existuje trojúhelník, v němž strany, obsah a délky těžnic jsou celá čísla?

Existují pythagorejské trojúhelníky, např. o stranách 3, 4, 5, v nichž přepona a jedna z odvěsen jsou prvočísla. Není však řešen následující problém:

Problém 6. Existuje nekonečně mnoho pythagorejských trojúhelníků s prvočíselnou přeponou a odvěsnou?

9.3 Egyptské zlomky

Egypťané měli speciální symboly pro značení tzv. jednotkových zlomků, které jsou převrácenými čísly k číslům celým (tj. zlomků s čitatelem rovným 1). Neměli ovšem symboly pro zlomky se jmenovatelem $\neq 1$, např. zlomek $\frac{4}{23}$ reprezentovali jako součet

$$\frac{4}{23} = \frac{1}{23} + \frac{1}{23} + \frac{1}{23} + \frac{1}{23}.$$

Existují však i další možná vyjádření zlomku pomocí jednotkových zlomků. Jedna z cest hledání takových vyjádření je tzv. „hladový algoritmus“. Pro zlomek $\frac{a}{b}$, $a, b \in \mathbb{N}$, najdeme nejmenší přirozené číslo x_1 tak, aby $\frac{1}{x_1} \leq \frac{a}{b}$. Dále najdeme nejmenší číslo $x_2 \neq x_1$ tak, aby $\frac{1}{x_2} \leq (\frac{a}{b} - \frac{1}{x_1})$ atd. Např. pro zlomek

$$\frac{4}{23} = \frac{1}{6} + \frac{1}{138}, \quad \frac{41}{42} = \frac{1}{2} + \frac{1}{3} + \frac{1}{7}.$$

Termín „hladový algoritmus“ se užívá proto, že v každém kroku hledaný zlomek „ujídá“ co nejvíce ze zbylého zlomku. Fibonacci v roce 1202 dokázal, že algoritmus je vždy konečný. Navíc ukázal, že pokud je zlomek < 1, pak počet jednotkových zlomků v součtu není větší než jeho čitatel.

Neřešené problémy se týkají zejména počtu sčítanců ve vyjádření daného zlomku zlomky jednotkovými. Je-li b liché, pak u zlomku $\frac{2}{b}$ vždy stačí dva sčítanci, pro $\frac{3}{b}$ tři sčítanci. Erdös dokázal, že pro celá čísla $\frac{4}{b}$, $b < 10^8$, stačí tři sčítanci. Obecně zůstávají otevřené následující problémy:

Problém 7. Je možno zlomek $\frac{4}{b}$ pro $b > 1$ vyjádřit jako součet nejvýše tří různých jednotkových zlomků?

Problém 8. Je vždy možno pomocí „hladového“ algoritmu vyjádřit zlomek s lichým jmenovatelem jako součet jednotkových zlomků s lichými jmenovateli?

9.4 Dokonalá čísla

O dokonalých číslech jsme již mluvili. Byla vždy spjata s nejrůznějšími číselnými spekulacemi. Např. sv. August tvrdil, že Bůh stvořil zemi a nebe v 6 dnech, neboť 6 je dokonalé číslo, a tím chtěl poukázat na dokonalost své práce. Jak také již víme, jsou těsně spjata s Mersenneovými prvočísly.

Dnes je známo 48 Mersenneových prvočísel.

V roce 1996 vznikl síťový projekt GIMPS (Great Internet Mersenne Prime Search) v němž tisíce matematiků a nadšenců z celého světa hledá s podporou počítačů velká Mersenneova prvočísla. Hledání je založeno na myšlence využití volně šiřitelného softwaru, pomocí něhož jsou Mersenneova prvočísla hledána. Zájemce odkazujeme na adresu projektu www.mersenne.org.

V rámci projektu GIMPS bylo např. v roce 1999 nalezeno první prvočíslo s více než milionem cifer - $M_{6\,972\,593}$.

Číslo $M_{57\,885\,161}$ je dosud největším známým Mersenneovým prvočíslem (leden 2013) a také vůbec dosud největším známým prvočíslem, majícím 17 425 170 cifer.

Problém 9. Existuje nekonečně mnoho Mersenneových prvočísel?

Problém 10. Existuje nekonečně mnoho dokonalých čísel?

Problém 11. Existuje liché dokonalé číslo?

V množině všech prvočísel se objevují dvojice, lišící se pouze o číslo 2. Říkáme jim prvočíselná dvojčata, např. dvojice (5,7) a (11,13). Není však řešen následující problém.

Problém 12. Existuje nekonečně mnoho prvočíselných dvojčat?

Problém 13. Existuje nekonečně mnoho prvočísel ve tvaru $n^2 + 1$?

Problém 14. Existuje pro každé $n \in \mathbb{N}$ prvočíslo mezi n^2 a $(n+1)^2$?

9.5 Prvočíselná faktorizace

Dle fundamentální věty aritmetiky přirozených čísel je možno každé přirozené číslo N vyjádřit v kanonickém rozkladu

$$N = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Prakticky je však obtížné pro velká čísla tento rozklad najít. Jelikož délka čísla N ve dvojkové soustavě je $[\log_2 N] + 1$, hledá se algoritmus, který by určil rozklad čísla N v čase ohraničeném některou mocninou čísla $\log_2 N$ (a tedy $\log N$). Takový algoritmus, který proběhne v čase, který je omezen některou mocninou délky vstupu, nazýváme polynomiální.

Problém 15. Existuje polynomiální algoritmus pro určení prvočíselného rozkladu přirozeného čísla?

Problém 15 lze rozložit na řešení následujících problémů:

Problém 16. Existuje polynomiální algoritmus určující, zda dané číslo je prvočíslo?

Problém 17. Existuje polynomiální algoritmus, který pro dané složené číslo N určí jeho netriviální dělitele?

Nezajímá-li nás pracovní čas počítače, existuje přímý algoritmus pro hledání rozkladu. Jednoduše řečeno, zkusíme všechny možné dělitele. Ve skutečnosti je ovšem k tomuto výpočtu třeba nejvýše $\sqrt{N}$ kroků, ovšem $\sqrt{N}$ není ohraničena žádným polynomem v $\log N$.

Je nutno zdůraznit, že tato metoda není příliš efektivní. Předpokládáme-li, že jsme schopni provést miliardu početních dělení za sekundu, trval by nám rozklad čísla $N = p \cdot q$ pro 30ciferná prvočísla p, q déle, než je stáří Vesmíru. Museli bychom totiž postupně ověřovat dělitelnost čísla N postupně prvočísly nepřevyšujícími

$\sqrt{N}$, tedy $x = 10^{30}$. Takových prvočísel je jak víme $\pi(x)$, což je dle zákona asymptotického rozdělení prvočísel 2.1.14 přibližně

$$\frac{x}{\ln x} = \frac{10^{30}}{30 \ln 10} \approx 1,5 \cdot 10^{28}.$$

Protože rok má $3,2 \cdot 10^7$ sekund a uvažujeme-li stáří Vesmíru $13 \cdot 10^9$ roku, můžeme za dobu trvání Vesmíru učinit $4,2 \cdot 10^{26}$ dělení. Na prozkoumání dělitelnosti uvedeným počtem prvočísel by ovšem bylo třeba zhruba $40\times$ více času.

K důkazu prvočíselnosti 36ciferného čísla bychom potřebovali roky času na nejrychlejších počítačích. Tento algoritmus je znám už přes 2 000 let, moderní algoritmy jsou mnohem rychlejší.

Např. nejrychlejšímu ze známých testovacích algoritmů na nejrychlejších počítačích by trval rozklad 200ciferného čísla staletí. Pro 80ciferná čísla provede rozklad v rozumném čase a v nedávné době byla překonána hranice 100 cifer.

Nechceme-li znát dělitele daného čísla a stačí nám rozhodnout pouze o jeho prvočíselnosti, existují velice rychlé nepolynomiální algoritmy. Např. je známo, že číslo $2^{727} - 1$ není prvočíslem, i když není znám žádný netriviální dělitel tohoto 219ciferného čísla. Podobně pro číslo $2^{511} - 1$ jsou známi dělitelé

$$127, \quad 439, \quad 2\,298\,041, \quad 15\,212\,471, \quad 9\,361\,973\,132\,609,$$

žádní další dělitelé tohoto 123ciferného čísla nejsou známi.

K tomuto testování se používá velice často malá Fermatova věta: je-li N prvočíslo, pak $2^{N-1} \equiv 1 \pmod{N}$. Obrácené tvrzení bohužel neplatí, a tedy malou Fermatovu větu nelze užít k testování prvočíselnosti.

9.6 $3n + 1$ problém

Uvažujme následující jednoduchou situaci: je dána funkce $f\colon \mathbb{N} \to \mathbb{N}$ (tzv. $3n + 1$ funkce) předpisem

$$f(n) = \begin{cases} \frac{1}{2}n & \text{pro } n \text{ sudé} \\ 3n + 1 & \text{pro } n \text{ liché} \end{cases}$$

V roce 1950 byl formulován následující problém.

Problém 18. Jak vypadají funkční hodnoty funkce f, aplikujeme-li postupně f na libovolně zvolené přirozené číslo?

9.7 Zajímavá reálná čísla

Ačkoliv všechna reálná čísla odpovídají bodům číselné přímky, jsou z hlediska jejich vlastností mezi nimi velké rozdíly. Některá byla vytvořena nejstaršími lidmi (1, 2, 3), jiná moudrými Řeky ($\sqrt{2}, \pi$) a další objevením nového kalkulu (e). Jak již víme, základní dělení reálných čísel je na racionální a iracionální, která dále dělíme na algebraická a transcendentní. Moderní vlastnosti splněné některými, ale ne všemi reálnými čísly, jsou normalita a spočitatelnost v reálném čase (RTC). V této kapitole se budeme zabývat vlastnostmi některých zajímavých reálných čísel.

Snad nejzajímavějším reálným číslem je číslo π. Je známo více než 1 000 let, že jde o iracionální transcendentní číslo. Co lze říci o jeho desetinném rozvoji $\pi = 3,14159264\ldots$? Vyskytují se v něm nějaké neočekávané bloky číslic? Vyskytují se všechny cifry nekonečně mnohokrát? To je podstatou otázky normality π, kterou budeme diskutovat později.

Podobně o čísle e je známo, že jde o iracionální transcendentní číslo. Existuje nějaká jednoduchá kombinace čísel e a π tak, aby výsledné číslo bylo racionální? Je např. číslo $\frac{\mathrm{e}}{\pi}$ racionální?

Číslo π se v matematice objevuje v řadě zajímavých formulí, např.

$$\mathrm{e}^{i\pi} = -1 \quad \text{či} \quad \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi}{6}.$$

Vlastnosti čísla π byly studovány po staletí, zejména v souvislosti s problematikou kvadratury kruhu. Tento problém byl řešen plně v roce 1882, kdy Lindemann dokázal transcendentnost čísla π. Není takřka nic známo o vlastnostech desetinného rozvoje čísla π. Uveďme např. pro zajímavost výskyt cifry 7 v prvních 29 milionech cifer čísla $\pi - 3$:

počet cifer	100	1 000	10^4	10^5	10^6	10^7	29 360 000
počet 7	8	95	970	10 025	99 800	1 000 207	2 934 083
% podíl	8 %	9,5 %	9,7 %	10,02 %	9,98 %	10,002 %	9,99 %

Dá se tedy očekávat, že každá z 10 cifer se v rozvoji π vyskytuje s 10% pravděpodobností.

Problém 19. Vyskytují se v dekadickém rozvoji čísla π cifry bez jakéhokoliv vzoru?

Po mnoho staletí bylo nejrychlejším způsobem nalezení cifer čísla π užitím Gaussovy formule:

$$\pi = 48 \operatorname{arctg} \frac{1}{18} + 32 \operatorname{arctg} \frac{1}{57} - 20 \operatorname{arctg} \frac{1}{239}.$$

V roce 1976 Brent a Salamin objevili užitečnost Gaussovy formule pro výpočet π. Definujeme-li dvě posloupnosti (a_n) a (b_n) tak, že $a_0 = a$, $b_0 = b$ a

$$a_{n+1} = \frac{a_n + b_n}{2},\ b_{n+1} = \sqrt{a_n b_n},$$

pak, jak patrno, mají tyto posloupnosti společnou limitu

$$\sqrt{ab} = \frac{a+b}{2},$$

(tzv. aritmeticko-geometrický průměr). Zajímavé na tom je, že uvedené posloupnosti konvergují velice rychle – počet přesných cifer se v každém kroku zdvojnásobuje a je třeba asi jen 19 kroků na přesnost na milion cifer.

Položme tedy $a_0 = 1, b_0 = \frac{1}{\sqrt{2}}$. Sestrojíme posloupnosti $(a_n), (b_n)$ a nechť a je jejich společná limita, $d = a_n^2 - b_n^2$. Brent–Salaminova formule říká, že

$$\pi = \frac{4a^2}{1 - \sum_{j=1}^{\infty} 2^{j+1} d_j}.$$

Posloupnost

$$\pi_n = \frac{4a_{n+1}^2}{1 - \sum_{j=1}^{n} 2^{j+1} d_j}$$

konverguje velmi rychle k π. Číslo π_{19} udává π s přesností na milion cifer, π_{26} na 200 milionů cifer. Dnes je známo π s přesností na bilion cifer.

Podobně jako π, číslo e bylo také intenzivně studováno, i když bylo objeveno o 2 000 let později.

Problém 20. Jsou čísla e, π algebraicky nezávislá? Je jejich podíl racionální číslo?

Podobně obtížný problém o vztahu čísel e a π je, zda čísla $\pi + \mathrm{e}$, $\pi\mathrm{e}$, π^{e}, e^{e}, π^{π} jsou iracionální. Očekává se, že jde o transcendentní čísla a tento problém by byl plně vyřešen při řešení problému 20.

Dnes je již známo, že pokud číslo e $+\pi$ je kořenem polynomu s celočíselnými koeficienty, je tento polynom stupně alespoň 500 milionů.

Z početního hlediska jsou racionální čísla jednodušší než iracionální. Snadno jde ověřit, že pro nalezení jeho prvních n cifer není třeba více než $c \cdot n$ kroků pro nějakou konstantu c. To vede k následující definici.

Definice. Reálné číslo je spočitatelné v reálném čase (RTC), existuje-li algoritmus počítající jeho desetinné cifry a pro který existuje konstanta c tak, že pro každé n algoritmus nepotřebuje více než $c \cdot n$ kroků k výpočtu prvních n cifer.

Jednoduše řečeno, definice říká, že v průměru je třeba na výpočet každé cifry stejné množství času, nezávisející na tom, zda počítáme desátou cifru či cifru řádu 10^6.

Není obtížné zkonstruovat RTC čísla. Např. každé z následujících čísel je RTC:

- $x_1 \ldots$ má 1 na pozicích $n!$ pro $n \in \mathbb{N}$, všude jinde 0 – tzv. Liouvillovo číslo
- $x_2 \ldots$ má 1 na pozicích 2^n pro $n \in \mathbb{N}$, všude jinde 0
- $x_3 \ldots$ má 1 na pozicích n^2 pro $n \in \mathbb{N}$, všude jinde 0
- $x_4 \ldots$ má na desetinných místech za sebou postupně psaná všechna přirozená čísla, tj.
$$x_4 = 0,12345678910111213\ldots$$
tzv. *Mahlerovo* číslo.

Liouvillovo číslo x_1 je historicky zajímavé, neboť šlo o *první známé transcendentní číslo.*

Není známo, která z následujících vlastností platí pro algebraická iracionální čísla:

1) všechna algebraická iracionální čísla jsou RTC,
2) některá algebraická iracionální čísla jsou RTC, některá ne,
3) žádné algebraické iracionální číslo není RTC.

Pro transcendentní čísla je známo, že skoro všechna nejsou RTC. Podívejme se např. na algebraické iracionální číslo $\sqrt{2}$. Dodnes se používá babylonská metoda pro výpočet cifer $\sqrt{2}$. Posloupnost $a_0 = 2$, $a_{r+1} = \frac{1}{2}(a_r + \frac{2}{a_r})$ konverguje k $\sqrt{2}$, a to velice rychle:

$$a_0 = 2; \quad a_1 = 1,5; \quad a_2 = 1{,}41666666\ldots; \quad a_3 = 1{,}414215686274509804\ldots,$$

$$a_4 = 1{,}414213562374689911\ldots, \quad a_5 = 1{,}414213562373095049\ldots.$$

K nalezení prvních n cifer se však potřebuje alespoň n^2 kroků, a jelikož n^2 není omezeno $c \cdot n$ pro žádné c, není to RTC algoritmus. Babylonský algoritmus tedy není dost rychlý. Obecně se předpokládá, že žádné algebraické iracionální číslo není RTC.

9.8 Součty převrácených hodnot mocnin přirozených čísel

Je dobře známo, že je nemožné sečíst převrácená čísla k přirozeným číslům, neboť tvoří harmonickou řadu

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots,$$

která diverguje. Jestliže však z této řady vybereme jen některé členy, může se stát, že příslušná řada už bude konvergovat – např. pro geometrickou řadu

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots$$

platí, že je konvergentní a její součet je 2.

Euler jako první dokázal, že řada

$$\sum_{k=1}^{\infty} \frac{1}{k^2}$$

má součet $\frac{\pi^2}{6}$. Snadno se dá dokázat, že také řady

$$\xi(r) = \sum_{k=1}^{\infty} \frac{1}{k^r}$$

pro $r \geq 2$ konvergují, přičemž

$$\xi(4) = \frac{\pi^4}{90}, \xi(6) = \frac{\pi^6}{945}, \xi(8) = \frac{\pi^8}{9450},$$

atd. Obecně $\xi(2n)$ je racionálním násobkem π^{2n}, uvedená čísla jsou tedy iracionální.

Pomocí formule $\xi(2) = \frac{\pi^2}{6}$ lze snadno nalézt pravděpodobnost, že dvě vybraná přirozená čísla jsou nesoudělná. Prvně určeme pravděpodobnost, že 2 nedělí obě čísla najednou, tj. alespoň jedno z nich je liché. Ta je rovna $1 - \frac{1}{4}$. Podobně pravděpodobnost, že 3 nedělí obě zároveň, je $1 - \frac{1}{9}$ atd. Nyní pravděpodobnost, že obě jsou nesoudělná, znamená, že všechny uvedené eventuality platí najednou, tj. je rovna součinu

$$\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{25}\right)\dots$$

Užitím formule pro součet geometrických posloupností je uvedený součin roven

$$\frac{1}{1 + \frac{1}{4} + \frac{1}{16} + \dots} \cdot \frac{1}{1 + \frac{1}{9} + \frac{1}{81} + \dots} \cdot \dots$$

Vynásobením jmenovatelů dostaneme právě všechny kvadráty přirozených čísel, tj. pravděpodobnost je převrácené číslo k $\sum_{k=1}^{\infty} \frac{1}{k^2}$, tedy $\frac{6}{\pi^2}$.

Velice málo je však známo o číslech $\xi(2n+1)$. Až v roce 1978 bylo dokázáno, že $\xi(3)$ je iracionální číslo.

Problém 21. Je číslo $\xi(5) = 1 + \frac{1}{2^5} + \frac{1}{3^5} + \dots$ iracionální?

Ačkoli harmonická řada diverguje, jsou hodnoty součtu prvních r členů

$$H(r) = 1 + \frac{1}{2} + \ldots + \frac{1}{r}$$

harmonické posloupnosti blízké hodnotě $\ln r$. Platí totiž

$$\int_1^{r+1} \frac{1}{t}\,\mathrm{d}t = \ln(r+1).$$

Je zajímavé, že posloupnost $H(r) - \ln r$ je konvergentní s limitou $\gamma = 0,577215\ldots$ Konstanta γ vypovídá o rychlosti divergence harmonické řady, pro velká r je totiž

$$H(r) \doteq \gamma + \ln r.$$

Problém 22. Je číslo γ iracionální?

Výsledky a návody ke cvičením

1. a) 13, b) 76, c) 87, d) 282

2. číslo 295! stejně jako 299! končí 72 nulami.

3. $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$, $20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

4. 41, je to mocnina čísla 13 v rozkladu $\frac{700!}{200!}$

5. platí $[x] \leq x$, tedy $[x] + [y] \leq x + y$, odkud $[x] + [y] \leq [x + y]$

6. nerovnost stačí dokázat pro případ, že $0 \leq \alpha < 1$, $0 \leq \beta < 1$; ta má pak tvar $[2\alpha] + [2\beta] \geq [\alpha + \beta]$: je-li $[\alpha + \beta] = 0$, jsme hotovi, je-li $[\alpha + \beta] = 1$, pak $\alpha + \beta \geq 1$ a alespoň jeden ze sčítanců $\alpha, \beta \geq \frac{1}{2}$. Odtud $[2\alpha] + [2\beta] \geq 1 = [\alpha + \beta]$

7. uvažujte mocniny prvočísla p v rozkladech čitatele a jmenovatele a užijte předchozího cvičení

8. pro $0 \leq x < \frac{1}{n}$ tvrzení platí, neboť obě strany jsou rovny 0; platí-li rovnost pro některé x, platí také pro $x + \frac{1}{n}$: každý sčítanec vlevo kromě posledního přechází v sousední zprava a poslední v $[x+1] = [x]+1$, pravá strana je rovna $[n(x + \frac{1}{n})] = [nx + 1] = [nx] + 1$; libovolné x lze zapsat ve tvaru $x = \alpha + \frac{m}{n}$ pro některá $0 \leq \alpha < \frac{1}{n}$ a $m \in \mathbb{Z}$: stačí vzít m tak, aby $nx \geq m > nx - 1$

9. $\pi(10^7) \approx 620\,000$, $\pi(10^8) \approx 5\,425\,000$

11. předpokládejte, že prvočísel v uvedeném tvaru je pouze konečně mnoho $\{q_1, \ldots, q_n\}$ a uvažujte číslo $6q_1 \cdot \ldots \cdot q_n - 1$; ukažte, že toto číslo je nutně dělitelné prvočíslem v uvažovaném tvaru

12. postupujte podobně jako ve cvičení 11 pro číslo $4(q_1 \cdot \ldots \cdot q_n)^2 + 3$

18. z $p|ab$ plyne $p|a$ nebo $p|b$, což vzhledem k $p|a + b$ znamená $p|a$ a $p|b$

19. z předpokladů plyne $p|b^2$, tedy $p|b$

21. z $p|ab$, $p|a + b$ plyne $p|a$, $p|b$, což vzhledem k $(a, b) = 1$ znamená $p = 1$

22. z $(a, b) = 1$ plyne $(a + b, ab) = 1$; užijte cvičení 20

23. zřejmě $a^2 - ab + b^2 = (a + b)^2 - 3ab$; platí-li $p|a + b$, $p|(a + b)^2 - 3ab$, pak $p|3ab$; vzhledem k $(a, b) = 1$, nutně $p|3$

26. uvažujte postupně prvočísla ve tvarech $p = 3$, $p = 3k + 1$, $p = 3k + 2$ a dokažte, že nutně $p = 3$

27. $2^n \equiv (-1)^n \pmod 3$, tj. alespoň jedno z čísel $2^n + 1$, $2^n - 1$ je dělitelné třemi

28. ukažte, že $p = 3$; uvažujte p ve tvarech $p = 3k + 1$, $p = 3k + 2$ a dokažte, že pak číslo $8p^2 + 1$ je složené

30. a) $x \equiv 5 \pmod 7$, b) $x \equiv 4 \pmod{11}$, c) $x \equiv 6 \pmod{17}$,
d) $x \equiv 3 \pmod 8$, e) $x \equiv 4, 11, 18, 25, 32 \pmod{35}$, f) není řešitelná,
g) $x \equiv 21 \pmod{36}$, h) $x \equiv 7 \pmod{15}$, i) není řešitelná,
j) $x \equiv 14 \pmod{35}$

31. a) $x \equiv 7 \pmod{25}$, b) $x \equiv 5 \pmod{11}$, c) $x \equiv 5 \pmod{11}$,
d) $x \equiv 11 \pmod{24}$, e) $x \equiv 7 \pmod{31}$, f) $x \equiv 8 \pmod{35}$

32. a) $x \equiv 8 \pmod{17}$, b) $x \equiv 9 \pmod{19}$, c) $x \equiv 11 \pmod{58}$

33. a) 7, $\frac{2}{45}$, b) -48, 0,7, c) 0, 0,73, d) -1, $\frac{8}{23}$

34. a) $[|-\frac{47}{5}|] = 9$, b) $[\frac{103}{5}] = 20$

35. a) $[|-\frac{61}{5}|] = 12$, b) $[\frac{92}{5}] = 18$

36. a) (4, 2, 2, 1, 1, 2), b) (3, 1, 1, 1, 4, 10), c) (3, 2, 1, 24),
d) (−6, 1, 1, 28), e) (0, 2, 2, 3), f) (−1, 1, 1, 1, 1, 1, 1, 2, 6)

37. a) $x \equiv 31 \pmod{183}$, b) $x \equiv 47 \pmod{241}$, c) není řešitelná

38. a) $x \equiv 41, 190, 339 \pmod{447}$, b) $x \equiv 61, 248 \pmod{422}$,
c) $x \equiv 39, 196, 353 \pmod{471}$

39. a) $x \equiv 73 \pmod{177}$, b) $x \equiv 29 \pmod{311}$, c) $x \equiv 48 \pmod{219}$

40. a) $x = -1 + 16t$, $y = -8 + 17t$, b) $x = -7 + 15t$, $y = 12 - 23t$,
c) $x = 9 + 37t$, $y = 3 + 12t$, d) není řešitelná, e) $x = 4 + 16t$, $y = 7 - 11t$

41. 26. dubna

42. $a = 8$, $b = 1$

43. a) $x = -4 + 13t$, $-100 < -4 + 13t < 150$, $-7 \leq t \leq 11$, 19 bodů,
b) 7 bodů, c) 8 bodů

45. užijte cvičení 44, počet bodů je 12

46. přímka $ax + by = c$ má směrnici $-\frac{a}{b}$, přičemž $(a, b) = 1$, tedy $r = \sqrt{a^2 + b^2}$

47. a) $x \equiv 291 \pmod{420}$, b) $x \equiv 251 \pmod{630}$, c) $x \equiv 747 \pmod{840}$,
d) $x \equiv 371 \pmod{462}$

48. a) 89, 209, 329, 449, 569, 689, 809, 929,
b) 244, 559, 874, c) 731, d) 841

49. 299 a 439

50. a) a b) jsou řešitelné, c) a d) nejsou řešitelné

51. plyne z toho, že pro $f(x) = x^2 - a$ je $p \nmid f'(x) = 2x$

52. rovnici mohou vyhovovat pouze lichá čísla $x = 2t + 1$; dosazením za x do rovnice dostaneme $4t(t+1) \equiv a - 1 \pmod 2^\alpha$, odkud plynou nutné podmínky řešitelnosti:

a) pro $\alpha = 1$ je $a \equiv 1 \pmod 2$, tj. $(a, 2) = 1$
b) pro $\alpha = 2$ je $a \equiv 1 \pmod 4$
c) pro $\alpha \geq 3$ je $a \equiv 1 \pmod 8$.

53. nutné podmínky ze cvičení 52 jsou pro $\alpha = 1, 2, 3$ také postačující:

pro $\alpha = 1$ je řešením $x \equiv 1 \pmod 2$,
pro $\alpha = 2$ je řešením $x \equiv 1, 3 \pmod 4$,
pro $\alpha = 3$ je řešením $x \equiv 1, 3, 5, 7 \pmod 8$.

54. 1 v případech a), e), f), j), -1 v ostatních případech

55. v případech a) a c) prochází, b) a d) neprochází

56. a), d), a g) jsou řešitelné, b), c), e), f) nejsou řešitelné

57. a) $a \equiv \pm 8 \pmod{17}$, b) $a \equiv \pm 10 \pmod{23}$, c) neexistuje

58.

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{pro } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{3}\right) & \text{pro } p \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 & \text{pro } p \equiv 1 \pmod 3 \\ \left(\frac{2}{3}\right) & \text{pro } p \equiv 2 \pmod 3 \end{cases}$$

Je tedy $\left(\frac{3}{p}\right) = 1$ právě když

a) $3p \equiv 3 \pmod{12}$ a $4p \equiv 4 \pmod{12}$, tj. $p \equiv 1 \pmod{12}$
nebo
b) $3p \equiv 9 \pmod{12}$ a $4p \equiv 8 \pmod{12}$, tj. $p \equiv -1 \pmod{12}$.

59. $(\frac{-3}{p}) = (\frac{-1}{p}) \cdot (-1)^{\frac{1}{2}(p-1)} \cdot (\frac{p}{3}) = (\frac{p}{3})$, tedy $(\frac{-3}{p}) = 1$ právě když $p \equiv 1 \pmod 3$, tj. p je tvaru $6n + 1$

60. a) $x^2 - 1 \equiv 0 \pmod 3$, $x \equiv \pm 1 \pmod 3$,

b) $x^4 + 2x^3 - 2x^2 + 2x - 1 \equiv 0 \pmod 5$, není řešitelná,

c) $x^6 + 2x^5 - 2x + 3 \equiv 0 \pmod 7$, $x \equiv -2, -3 \pmod 7$

61. a) $(x-2)(x-3)(x-9)$, b) $(x-1)(x+2)(x-13)$, c) $(x+1)(x+3)(x-17)$

62. užijte Wilsonovy věty

63. vynásobte kongruence $a^p \equiv a \pmod p$ a $(p-1)! \equiv -1 \pmod p$

65. a) $x \equiv 11, 20 \pmod{21}$, b) $x \equiv 4, 22 \pmod{33}$, c) $x \equiv 2, 7, 24, 29 \pmod{55}$, d) $x \equiv 3, 26, 28, 49, 63, 73, 84, 94 \pmod{105}$

66. a) $x \equiv 17 \pmod{112}$, b) $x \equiv 11 \pmod{245}$, c) $x \equiv 67 \pmod{153}$

67. a) $x \equiv \pm 12 \pmod{25}$, b) $x \equiv \pm 15 \pmod{49}$, c) $x \equiv \pm 47 \pmod{121}$, d) $x \equiv \pm 63 \pmod{169}$

69. a) $x \equiv 6 \pmod{25}$, b) $x \equiv 14 \pmod{25}$,
c) $x \equiv 5, 12, 19, 26, 33, 40, 47 \pmod{49}$,
d) $x \equiv 2, 9, 16, 23, 30, 37, 44 \pmod{49}$

70. $x \equiv 36, 136 \pmod{175}$

71. a) 16, je primitivním kořenem, b) 18, je, c) 3, není, d) 6, je, e) 22, je, f) 2, není

72. a) $\frac{6}{(6,3)} = 2$, $\frac{6}{(6,4)} = 3$, $\frac{6}{(6,5)} = 6$, b) $\frac{40}{(40,12)} = 10$, $\frac{40}{(40,15)} = 8$, $\frac{40}{(40,16)} = 5$

73. $\delta = [\delta_1, \delta_2]$

74. a) $12 \pmod{35}$, b) $20 \pmod{55}$

75. a) $\phi(16) = 8$, b) $\phi(42) = 12$, c) $\phi(72) = 32$, d) $\phi(88) = 40$

76. a) $\phi(7) = 6$, b) $\phi(9) = 6$

77. redukovaný systém zbytků modulo 13 tvoří čísla $6^0, 6^1, \ldots, 6^{11}$, jejich nejmenší kladné zbytky modulo 13 jsou 1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11

78. redukovaný systém zbytků modulo 18 tvoří čísla $5^0, 5^1, 5^2, 5^3, 5^4, 5^5$, jejich nejmenší kladné zbytky modulo 18 jsou 1, 5, 7, 17, 13, 11

79. primitivní kořen g v lichém prvočíselném modulo p má řád $p-1$, odkud $g^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$, tedy $\frac{1}{2}(p-1) \equiv \mathrm{ind}(-1) \equiv \mathrm{ind}(p-1) \pmod{(p-1)}$

80. $66 \equiv 13^x \equiv 7^{63} \pmod{71}$, přechodem k indexům při základu 6 pak $x \operatorname{ind} 13 \equiv 63 \pmod{70}$ neboli $39x \equiv 63 \pmod{70}$, odkud $x = \operatorname{ind}_{13} 66 \equiv 7 \pmod{70}$

81. a) $x \equiv 7 \pmod{43}$, b) není řešitelná, c) $x \equiv 4, 33 \pmod{37}$, d) $x \equiv 30, 53 \pmod{83}$, e) $x \equiv \pm 253 \pmod{73^2}$, f) $x \equiv \pm 1634 \pmod{59^2}$

82. a) $x \equiv 51 \pmod{97}$, b) $x \equiv 30 \pmod{73}$, c) $x \equiv 32 \pmod{79}$, d) $x \equiv 44 \pmod{83}$

83. a) $x \equiv 59 \pmod{71}$, b) není řešitelná, c) $x \equiv 36, 45, 41 \pmod{61}$, d) $x \equiv 6, 65, 59, 73, 14, 20 \pmod{79}$

84. a) 60, b) 8, c) 8, d) 19, e) 147

85. a) 10, b) není řešitelná, c) 2

86. $\alpha = ((1)) = (1, 1, \ldots)$

87. a) $\delta_k = \frac{10}{3} = (3, 3)$, $\delta_{k-1} = \frac{3}{1}$, $\alpha = \frac{10\sqrt{2}+3}{3\sqrt{2}+1} = \frac{57-\sqrt{2}}{17}$,
b) $\delta_k = \frac{43}{17} = (2, 1, 1, 8)$, $\delta_{k-1} = \frac{5}{2}$, $\alpha = \frac{43\sqrt{5}+5}{17\sqrt{5}+2} = \frac{3645-\sqrt{5}}{1441}$

88. a) $\frac{10}{7} = (1, 2, 3)$, $\sqrt{3} = (1, (1, 2))$, $\alpha = (1, 2, 3, 1, (1, 2))$,
b) $\frac{37}{13} = (2, 1, 5, 2)$, $\frac{\sqrt{3}+1}{2} = (1, (2, 1))$, $\alpha = (2, 1, 5, 2, 1, (2, 1))$

89. a) $\frac{N_1}{n_1} = \delta_6 = \frac{385}{79}$, $\varepsilon < \frac{1}{79 \cdot 150} < 0{,}0001$; b) $\frac{N_1}{n_1} = \delta_3 = \frac{23}{4}$, $\varepsilon < \frac{1}{4 \cdot 149} < 0{,}01$;
c) $\frac{N_1}{n_1} = \delta_6 = \frac{95}{41}$, $\varepsilon < \frac{1}{41 \cdot 101} < 0,001$; d) $\frac{N_1}{n_1} = \delta_6 = \frac{223}{63}$, $\varepsilon < \frac{1}{63 \cdot 265} < 0,0001$.

90. a) $\frac{N_1}{n_1} = \frac{39}{8}, \frac{23}{4}, \frac{44}{19}, \frac{39}{11}$; b) $\frac{N_1}{n_1} = \delta_4 = \frac{101}{17}$; c) $\frac{N_1}{n_1} = \delta_3 = \frac{97}{28}$; d) $\frac{N_1}{n_1} = \delta_5 = \frac{74}{11}$

91. a) $\sqrt{15} = (3, (1, 6)) \approx \delta_4 = \frac{31}{8}$, $\varepsilon < \frac{1}{8 \cdot 55} < 0,01$;
b) $\sqrt{17} = (4, (8)) \approx \delta_2 = \frac{33}{8}$, $\varepsilon < \frac{1}{8 \cdot 65} < 0,01$;
c) $\sqrt{23} = (4, (1, 3, 1, 8)) \approx \delta_6 = \frac{235}{49}$, $\varepsilon < \frac{1}{49 \cdot 191} < 0,001$;
d) $\sqrt{31} = (5, (1, 1, 3, 5, 3, 1, 1, 10)) \approx \delta_5 = \frac{206}{37}$, $\varepsilon < \frac{1}{37 \cdot 118} < 0,001$

92. a) $\sqrt{26} = (5, (10)) \approx \delta_2 = \frac{51}{10}$, b) $\sqrt{37} = (6, (12)) \approx \delta_2 = \frac{73}{12}$,
c) $\sqrt{29} = (5, (2, 1, 1, 2, 10)) \approx \delta_5 = \frac{70}{13}$,
d) $\sqrt{19} = (4, (2, 1, 3, 1, 2, 8)) \approx \delta_4 = \frac{48}{11}$

93. a) $\alpha = ((2, 8)) \approx \delta_3 = \frac{36}{17}$, b) $\alpha = ((3, 2, 5)) \approx \delta_3 = \frac{38}{11}$,
c) $\alpha = ((3, 2, 1, 4)) \approx \delta_4 = \frac{28}{13}$, d) $\alpha = ((3, 1, 4)) \approx \delta_4 = \frac{61}{16}$,
e) $\alpha = ((1, 3, 5, 6)) \approx \delta_2 = \frac{7}{6}$, f) $\alpha = ((2, (3, 1)) \approx \delta_4 = \frac{34}{15}$

94. $\sqrt[3]{10} = (2, 6, 2, \ldots) \approx \delta_6 = \frac{28}{13}$

95. a) $2\alpha^2 - 6\alpha - 3 = 0$, $\alpha = \frac{(3+\sqrt{15})}{2}$, b) $7\alpha^2 - 7\alpha - 1 = 0$, $\alpha = \frac{(7+\sqrt{77})}{14}$, c) $7\alpha^2 - 9\alpha - 13 = 0$, $\alpha = \frac{(9+\sqrt{445})}{14}$, d) $13\alpha^2 - 64\alpha - 21 = 0$, $\alpha = \frac{(32+\sqrt{1297})}{13}$, e) $\alpha^2 - 4\alpha + 1 = 0$, $\alpha = 2 + \sqrt{3}$, f) $3\alpha^2 - 18\alpha + 22 = 0$, $\alpha = \frac{(9+\sqrt{15})}{3}$, g) $16\alpha^2 - 32\alpha + 13 = 0$, $\alpha = \frac{(4+\sqrt{3})}{4}$

96. a) $\sqrt{26} = (5, (10)), x = 51, y = 10$, b) $\sqrt{37} = (6, (12)), x = 73, y = 12$, c) $\sqrt{19} = (4, (2, 1, 3, 1, 2, 8)), x = 170, y = 39$, d) $\sqrt{29} = (5, (2, 1, 1, 2, 10)), x = 9801, y = 1820$

97. nechť

$$\alpha_k = \frac{1}{10^{1!}} + \ldots + \frac{1}{10^{k!}} = \frac{p}{10^{k!}}$$

pro nějaké $p \in \mathbb{N}$, pak

$$\alpha - \alpha_k < \frac{1}{10^{(k+1)!}} \cdot \left(1 + \frac{1}{10} + \frac{1}{10^2} + \ldots\right) < \frac{10}{10^{(k+1)!}};$$

je-li α algebraické číslo stupně n, pak dle Liouvillovy věty existuje kladná konstanta c taková, že

$$|\alpha - \alpha_k| \geq \frac{c}{10^{k!n}};$$

je-li k tak velké, že $10^{k!} > \frac{10}{c}$, pak dle předchozích nerovností je

$$\frac{10}{10^{(k+1)!}} > \frac{10}{10^{k!(n+1)}},$$

tj. $k!(n+1) > (k+1)!$; poslední nerovnost ovšem nemůže platit pro dostatečně velké k při zadaném n, je tedy α transcendentní

99. a) $N = 279^2 + 106^2 = 169^2 + 246^2$, b) $N = 809^2 + 211^2 = 391^2 + 739^2$

100. mají-li body $P_1(x_1, y_1), P_2(x_2, y_2)$ od bodu Q stejné vzdálenosti, pak

$$x_1^2 - x_2^2 + 2(x_1 - x_2)\sqrt{2} + y_1^2 - y_2^2 = \frac{2}{3}(y_1 - y_2),$$

odkud $x_1 = x_2$; ale $y_1 \neq y_2$, tedy $y_1 + y_2 = \frac{2}{3}$, spor

101. nechť K je kruh se středem Q obsahující více než n mřížových bodů (takový jistě existuje); mřížových bodů uvnitř je přitom konečně mnoho; protože mají různé vzdálenosti od Q (viz cvičení 100), je možno je uspořádat do konečné posloupnosti dle rostoucí vzdálenosti, takže kruh K_{n+1} se středem Q jdoucí bodem p_{n+1} má uvnitř právě n mřížových bodů

102. $5220 = 0^2 + 8^2 + 16^2 + 70^2$

103. pomocí norem prvků určete jejich netriviální dělitele

105. užijte předchozího řešeného příkladu

Tabulky indexů

Prvočíslo 3:

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

Prvočíslo 5:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Prvočíslo 7:

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Prvočíslo 11:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

Prvočíslo 13:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

Prvočíslo 17

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	4	12	2	6					

Prvočíslo 19:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Prvočíslo 23:

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

Prvočíslo 29:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Prvočíslo 31:

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21
3										

Prvočíslo 37:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Prvočíslo 41:

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	17	20	38	23	23	15	8	7
4										

Prvočíslo 43:

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Prvočíslo 47:

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

Prvočíslo 53:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5										

Prvočíslo 59:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

Prvočíslo 61:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31
6										

Prvočíslo 67:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

Prvočíslo 71:

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	43	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61
7										

Prvočíslo 73:

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Prvočíslo 79:

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

Prvočíslo 83:

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	43	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

Prvočíslo 89:

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

Literatura

[1] Aigner, M., Ziegler, G.M.: *Proofs from The Book*. Springer Verlag, 3rd edition, Berlin, Heidelberg, New York, 2004.

[2] Burger, E.B., Tubbs R.: *Making Transcendence Transparent*. Springer Verlag, 2004.

[3] Hardy, G. H., Wright, E. M.: *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford, 2008.

[4] Ireland, K., Rosen, M.: *A Classical Introduction to Modern Number Theory*. Graduate texts in Mathematics vol. 84, 2nd edition, Springer Verlag, 1998.

[5] Klee, V., Wagon S.: *Old and New Unsolved Problems in Plane Geometry and Number Theory*. Dolciani Mathematical Expositions (Book 11), 2nd edition, The Mathematical Association of America, 1991.

[6] Křížek, M., Somer, L., Šolcová, A.: *Kouzlo čísel*. Academia, 2011.

[7] Michelovič, Š. Ch.: *Teorie čísel*. Moskva, 1967 (rusky).

[8] Ribenboim, P.: My Numbers, My Friends. Springer Verlag, New York, Berlin, Heidelberg, 2000.

[9] Singh, S.: *Velká Fermatova věta*. Argo a Dokořán, 2010.

[10] Vinogradov, I. M.: *Elements of Number Theory*. Dover Publications, Inc., 1954.