## 1. Základní algebraické struktury a dělitelnost

Připomeňme, že (asociativním) *okruhem* (s jednotkou) rozumíme nějakou množinu $R$ opatřenou dvojicí binárních operací $+$ a $\cdot$, jednou unární operaci $-$ a dvěma význačnými prvky 0 a 1, které splňují podmínky

(1) $(R, +, -, 0)$ je komutativní grupa,
(2) operace $\cdot$ je asociativní a $a \cdot 1 = 1 \cdot a = a$ pro všechna $a \in R$,
(3) $a \cdot (b + c) = a \cdot b + a \cdot c$ a $(b + c) \cdot a = b \cdot a + c \cdot a$ pro všechna $a, b, c \in R$.

Je-li operace $\cdot$ komutativní, mluvíme o *komutativním okruhu*. Konkrétní zápis okruhu jako (univerzální) algebry není ustálen, my zvolíme například zápis $(R, +, \cdot, -, 0, 1)$.

Je-li $(R, +, \cdot, -, 0, 1)$ komutativní okruh, nazveme množinu $I \subseteq R$ ideálem, jestliže

(1) I je podgrupou grupy $(R, +, -, 0)$ a
(2) $i \cdot r \in I$ pro všechna $i \in I$ a $r \in R$.

Komutativní okruh $(R, +, -, 0, \cdot, 1)$ nazveme *oborem integrity*, platí-li pro každou dvojici nenulových prvků $a, b \in R$, že $a \cdot b \neq 0$. O oboru integrity hlavních ideálů mluvíme v případě, že jsou všechny jeho ideály hlavní, tj. tvaru $iR = \{i \cdot r | \ r \in R\}$. Dobře známými příklady oborů integrity hlavních ideálů jsou okruhy celých čísel $(\mathbf{Z}, +, -, 0, \cdot, 1)$ či polynomů o jedné neznámé nad libovolným komutativním tělesem

Buď $(R, +, -, 0, \cdot, 1)$ obor integrity a $a, b \in R$. V souladu s pojmem dělitelnosti na celých číslech nebo reálných polynomech řekneme, že $a$ *dělí* $b$ (píšeme $a/b$), existuje-li takové $c \in R$, že $b = a \cdot c$. Dále řekneme, že je $a$ *asociováno s* $b$ (píšeme $a \| b$), jestliže $a/b$ a $b/a$.

Všimněme si, že v oboru integrity 0 dělí pouze opět 0 (a tedy s 0 je asociována jen 0), obvykle ji proto z našich úvah budeme vypouštět. V následujícívh úvahách si nejprve uvědomíme, jak vyjádřit otázky dělitelnosti pomocí ideálů.

**1.1.** Nechť $(R, +, -, 0, \cdot, 1)$ je obor integrity a $a, b \in R \setminus \{0\}$.

(1) Dokažte, že $a/b$, právě když $bR \subseteq aR$.
(2) Dokažte, že $a \| b$, právě když $aR = bR$.
(3) Dokažte, že $a \| b$, právě když existuje invertibilní $u \in R$, pro které $b = a \cdot u$.

(1) ($\Rightarrow$) Existuje-li $c \in R$, pro které $b = a \cdot c$, pak $b \in aR$, a proto i $b \cdot s \in aR$ pro každé $s \in R$.

($\Leftarrow$) Máme-li $bR \subseteq aR$, potom $b = b \cdot 1 \in bR \subseteq aR$, tedy existuje takové $c \in R$, že $b = a \cdot c$

(2) Stačí dvakrát použít (1).

(3) ($\Rightarrow$) Protože $a/b$, existuje $u \in R$, pro něž $b = a \cdot u$, a protože také $b/a$ existuje takové $v \in R$, že $a = b \cdot v$, Dosadíme-li do první rovnosti, dostaneme

$$b = a \cdot u = (b \cdot v) \cdot u = b \cdot (v \cdot u),$$

a proto $b \cdot (1 - v \cdot u) = 0$. Z definice oboru integrity je $1 - v \cdot u = 0$, tedy $v \cdot u = 1$ a $u$ je invertibilní prvek.

($\Leftarrow$) Okamžitě z předpokladu $b = a \cdot u$ máme $a/b$. Protože $a = b \cdot u^{-1}$, vidíme, že $b/a$. □

**1.2.** Je-li $\mathcal{R} = (R, +, \cdot, -, 0, 1)$ komutativní okruh, dokažte následující tvrzení.

(a) Jsou-li $I$ a $J$ dva ideály okruhu $\mathcal{R}$, pak $I + J = \{i + j |\ i \in I, j \in J\}$ je nejmenší ideál okruhu obsahující ideály $I$ a $J$.
(b) Je-li $I_0, I_1, \ldots$ posloupnost ideálů okruhu $\mathcal{R}$, pro které platí, že $I_i \subseteq I_{i+1}$, pak $\bigcup_i I_i$ je rovněž ideál.
(c) Je-li $S_0, S_1, \ldots$ posloupnost okruhů, pro které platí, že $S_i$ je podokruh okruhu $S_{i+1}$, pak $\bigcup_i S_i$ je okruh s takovými operacemi, že všechny okruhy $S_i$ jsou jeho podokruhy.

(a) Nejprve ukážeme, že množina $I + J$ tvoří ideál. Předně $0 = 0 + 0 \in I + J$. Zvolme $r \in R$ a $x_1, x_2 \in I + J$ libovolně. Potom existuje $i_1, i_2 \in I$ a $j_1, j_2 \in I$, pro něž $x_\nu = i_\nu + j_\nu$, kde $\nu = 1, 2$, a proto $-x_1 = -i_\nu + (-j_\nu) \in I + J$, dále $x_1 + x_2 = (i_1 + i_2) + (j_1 + j_2) \in I + J$ a $x_1 \cdot u = a \cdot (r_1 \cdot u) + b \cdot (s_1 \cdot u) \in aR + bR$.
(b) Opět vezměme $r \in R$ a $a, b \in \bigcup_i I_i$ libovolně. Potom existuje $n$, pro něž $a, b \in I_n$, tudíž $0, -a, a \cdot r, a + b \in I_n \subseteq \bigcup_i I_i$.
(c) Úvaha je obdobná jako v úloze (b), stačí si opět uvědomit, že pro každá dvojici prvků $a, b \in \bigcup_i S_i$ existuje $n$, pro které $a, b \in S_n$. □

Obor integrity $\mathcal{R}$ je *noetherovský*, jestliže neobsahuje žádný nekonečný ostře rostoucí řetězec ideálů. Jestliže jsou v oboru všechny ideály hlavní, mluvíme o *oboru integrity hlavních ideálů*.

**1.3.** Je-li $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ obor integrity hlavních ideálů, dokažte tvrzení:

(a) Pro každé $a, b \in R \setminus \{0\}$ $aR + bR = cR$ právě tehdy, když $c$ je NSD$(a, b)$.
(b) $\mathcal{R}$ je noetherovský.

(a) ($\Rightarrow$) Předpokládejme, že $aR + bR = cR$. Potom podle 1.2 máme $aR, bR \subseteq cR$, a proto podle 1.1 je $c/a$ a $c/b$. Vezmeme-li $d \in R$, pro něž $d/a$ a $d/b$, tedy díky 1.1 $aR, bR \subseteq dR$. Z minimality $aR + bR = cR$, potom dostáváme, že $cR = aR + bR \subseteq dR$, tedy $d/c$.
($\Leftarrow$) Je-li $c$ je NSD$(a, b)$ a vezmeme-li takové $d \in R$, že $aR + bR = dR$ (to musí existovat, protože každý ideál $(R, +, -, 0, \cdot, 1)$ je hlavní), pak i $d$ je NSD$(a, b)$, proto jsou podle definice NSD prvky $c$ a $d$ asociovány a 1.1 říká, že $aR + bR = dR = cR$.
(b) Předpokládejme, že obor není neoetherovský, tedy existuje nekonečný ostře rostoucí řetězec ideálů $I_0, I_1, \ldots$, tj. platí, že $I_i \subseteq I_{i+1}$ a $I_i \neq I_{i+1}$. V 1.2(b) jsme dokázali, že je $I = \bigcup_i I_i$ rovněž ideál. Kdyby existovalo $c \in R$, pro něž $cR = I$, pak by $c \in I_n$ pro nějaké $n$, proto $I_{n+1} \subseteq I = cR \subseteq I_n$, což je spor. Tedy ideál $I$ není hlavní. □

Připomeňme, že oborem integrity hlavních ideálů je každé těleso, okruh celých čísel a okruh polynomů jedné neurčité nad tělesem. Jde tedy podle dokázaného tvrzení o noetherovské obory.

*25.2.*

Okruh polynomů jedné neurčité s celočíselnými koeficienty $\mathbf{Z}[x]$ je (například podle Hilbertovy věty o bázi) noetherovský, ovšem ideál $x\mathbf{Z}[x] + 2\mathbf{Z}[x]$ by v oboru integrity hlavních ideálů musel být generován největším společným dělitelem prvků $x$ a 2, tedy prvkem 1, což zjevně neplatí, tedy $\mathbf{Z}[x]$ není obor integrity hlavních ideálů.

**1.4.** Uvažujme podokruh $R = \{\sum_i p_i x^i \in \mathbf{Q}[x] |\ p_0 \in \mathbf{Z}\}$ okruhu $\mathbf{Q}[x]$.

(a) Rozhodněte, zda $R$ obsahuje nekonečnou posloupnost $a_i$ vlastních dělitelů, tj. $a_{i+1}/a_i$ a $a_i$ není s $a_{i+1}$ asociován,
(b) rozhodněte, zda je $R$ noetherovský,
(c) rozhodněte, zda v $R$ existují ireducibilní rozklady každého neninvertibilního nenulového prvku.

(a) Uvědomme si, že $2^{-n}x \in R$, $2^{-n}xR \subseteq 2^{-(n+1)}xR$, protože $2^{-n}x = 2 \cdot 2^{-(n+1)}x$, a $2^{-n}xR \neq 2^{-(n+1)}xR$, protože $2^{-(n+1)}x \notin 2^{-n}xR$, čímž jsme našli nekonečnou posloupnost vlastních dělitelů $x/2^{-1}x/\ldots/2^{-n}x/2^{-(n+1)}x\ldots$.

(b) V (a) jsme našli rostoucí posloupnost ideálů, tedy $R$ není noetherovský.

(c) Kdyby existoval ireducibilní rozklad $x = p_1 \cdot \cdots \cdot p_n$, pak by právě jeden z polynomů $p_i = \frac{1}{c}x$ a součin ostatních by byl roven $c$, kde $c \in \mathbf{Z}$. Ovšem polynom $\frac{1}{c}x$ umíme napsat jako součin $\frac{1}{c}x = 2 \cdot \frac{1}{2c}x$, kde $2, \frac{1}{2c}x \in R$ nejsou invertibilní, tedy $\frac{1}{c}x$ není inreducibilní a polynom $x$ nelze ireducibilně rozložit. □

Připomeňme, že podokruhy tělesa komplexních čísel $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{2}]$ a $\mathbf{Z}[\sqrt{3}]$ jsou eukleidovské s euklidovskými normami $\nu_{-1}(a+bi) = a^2+b^2$, $\nu_2(a+b\sqrt{2}) = |a^2 - 2b^2|$ a $\nu_3(a+b\sqrt{2}) = |a^2-2b^2|$. Dále poznamenejme, že jsou všechny tři normy mulriplikativní, tedy platí $\nu_s(\alpha\cdot\beta) = \nu_s(\alpha)\cdot\nu_s(\beta)$ (důkaz je zcela přímočarý).

**1.5.** Najděte všechny invertibilní prvky okruhu $\mathbf{Z}[i]$ a ukažte, že okruh $\mathbf{Z}[\sqrt{2}]$ obsahuje nekonečně invertibilních prvků.

Protože prvek $\alpha \in \mathbf{Z}[i]$ je invertibilní existuje-li $\beta \in \mathbf{Z}[i]$, pro nkteré $\alpha\cdot\beta = 1$, proto $\nu(\alpha\cdot\beta) = 1$, tedy $\nu(\alpha) = 1$. Vidíme, že $\alpha \in \{1, -1, i, -i\}$.

Všimneme si, že invertibilní je právě prvek $a+b\sqrt{2} \in \mathbf{Z}[\sqrt{2}]$, pro který $\mu(a+b\sqrt{2}) = 1$. Jakmile $a^2-2b^2 = -1$, potom $(a+b\sqrt{2})\cdot(-a+b\sqrt{2}) = 2b^2-a^2 = 1$, a v případě, kdy $a^2-2b^2 = 1$, pak $(a+b\sqrt{2})\cdot(a-b\sqrt{2}) = a^2-2b^2 = 1$. Protože $\mu(1+\sqrt{2}) = 1$, je i $\mu((1+\sqrt{2})^n) = 1^n = 1$ pro každé $n$, tedy prvky $(1+\sqrt{2})^n$ jsou invertibilní. Přitm $1+\sqrt{2} > 1$, proto $(1+\sqrt{2})^n < (1+\sqrt{2})^{n+1}$, tedy jsme našli nekonečnou množinu $\{(1+\sqrt{2})^n |\ n \in \mathbf{N}\}$ invertibilních prvků oboru $(\mathbf{Z}[\sqrt{2}], +, -, 0, \cdot, 1)$. □

**1.6.** Dokažte, že okruh $\mathbf{Z}[\sqrt{5}]$ není Gaussův.

Stačí uvážit dva rozklady čísla $4 = 2\cdot 2 = (\sqrt{5}+1)\cdot(\sqrt{5}-1)$, o nichž snadno dokážeme, že jsou ireducibilní, ovšem číslo 2 zřejmě není v $\mathbf{Z}[\sqrt{5}]$ asociováno s číslem $\sqrt{5}-1$ ani s číslem $\sqrt{5}+1$ □

Všimněme si, že pomocí čísel 2, $\sqrt{5}-1$, $\sqrt{5}+1$ můžeme vytvořit dvojici prvků, která nemá v $\mathbf{Z}[\sqrt{5}]$ největší společný dělitel, konkrétně lze vzít dvojici $2(\sqrt{5}+1)$ 4. To samozřejmě nutně znamená, že $\mathbf{Z}[\sqrt{5}]$ není obor integrity hlavních ideálů. Dále poznamenejme, že okruh $\mathbf{Z}[\sqrt{5}]$ je noetherovský, protože tuto vlastnost splňuje okruh $\mathbf{Z}[x]$ a náš obor $\mathbf{Z}[\sqrt{5}]$ je izomorfní faktoru $\mathbf{Z}[x]/(x^2-5)\mathbf{Z}[x]$.

**1.7.** Je-li $\mathbf{Q}[x_1] \subseteq \mathbf{Q}[x_1, x_2] \subseteq \dots$ nekonečný řetězec okruhů (okruh méně neurčitých lze vždy přirozeně chápat jako podokruh okruhu více neurčitých), uvažujme množinu $\mathbf{Q}[\mathbb{X}] = \bigcup_i \mathbf{Q}[x_1, \dots, x_i]$, kde $\mathbb{X} = \{x_1, x_2, \dots\}$. Dokažte následující tvrzení.

(a) $\mathbf{Q}[\mathbb{X}]$ je obor integrity, jehož jsou všechny obory $\bigcup_i Q[x_1, \dots, x_i]$ podokruhy,
(b) $\mathbf{Q}[\mathbb{X}]$ není noetherovský,
(c) jestliže $a \in \mathbf{Q}[x_1, \dots, x_n]$ a $a = b \cdot c$, kde $b, c \in \mathbf{Q}[\mathbb{X}] \setminus \{0\}$, pak $b, c \in \mathbf{Q}[x_1, \dots, x_n]$,
(d) v $\mathbf{Q}[\mathbb{X}]$ neexistuje nekonečná posloupnost vlastních dělitelů (tj. taková, že by každý následující prvek dělil předchozí, ale nebyl by s ním asociován),
(e) v $\mathbf{Q}[\mathbb{X}]$ neexistuje nekonečný ostře rostoucí řetězec hlavních ideálů,
(f) existují NSD každé dvojice (nenulových a neinvertibilních prvků).
(g) $\mathbf{Q}[\mathbb{X}]$ je Gaussův.

(a) Plyne okamžitě z 1.2(c).

(b) Položíme $I_0 = \{0\}$ a indukcí definujme množinu $I_{n+1} = I_n + x_{n+1}\mathbf{Q}[\mathbb{X}]$. Zřejmě $I_{n+1} \subseteq I_n$, a protože $x_{n+1} \notin I_n$ máme $I_{n+1} \neq I_n$. Navíc $I_n$ je pro každé $n$ podle 1.2(a) ideál, tedy $\mathbf{Q}[\mathbb{X}]$ není noetherovský.

(c) Uvažme, že pro každé $m$ lze na každý prvek okruhu $\mathbf{Q}[\mathbb{X}]$ nahlížet jako na polynom $S_m[x_m]$, kde $S_m$ je podokruh $\mathbf{Q}[\mathbb{X}]$, který sestává z polynomů neobsahujících (s nenulovým koeficientem) proměnnou $x_m$. Všimněme se, že je $S_m$ jako podokruh oboru integrity opět oborem integity. Vezmeme-li $b, c \in \mathbf{Q}[\mathbb{X}] \setminus \{0\}$ a předpokládejme, že $b \notin \mathbf{Q}[x_1, \dots, x_n]$, pak existuje $m > n$, pro které $b$ obsahuje neznámou $x_m$, tedy $b$ má jako polynom z oboru $S_m[x_m]$ kladný stupeň. Tudíž i $b \cdot c$ má jako polynom z oboru $S_m[x_m]$ má kladný stupeň, a proto $b \cdot c \notin \mathbf{Q}[x_1, \dots, x_n]$.

(d) Předpokládejme, že máme posloupnost dělitelů, tj. prvky $a_i \in \mathbf{Q}[\mathbb{X}]$, pro které $a_{i+1}/a_i$. Protože existuje $n$, pro něž $a_1 \in \mathbf{Q}[x_1, \dots, x_n]$, a $a_i/a_1$ , platí podle (c), že $a_i \in \mathbf{Q}[x_1, \dots, x_n]$ pro všechna $i$. Díky Gaussově větě víme, že je obor $\mathbf{Q}[x_1, \dots, x_n]$ Gaussův, proto existje takové $m$, že $a_i \| a_m$ pro všechna $i > m$ v okruhu $\mathbf{Q}[x_1, \dots, x_n]$. Konečně z pozorování, že prvky asociované v $\mathbf{Q}[x_1, \dots, x_n]$ jsou nutně asociované i v $\mathbf{Q}[\mathbb{X}]$ plyne závěr.

(e) Jedná se jen o reformulaci (d) z jazyka dělitelnosti do aritmetiky ideálů (viz tvrzení úlohy 1.1).

(f) Vezmeme-li $p, q \in \mathbf{Q}[\mathbb{X}]$, existuje $n$, pro které $p, q \in \mathbf{Q}[x_1, \dots, x_n]$. Protože je obor $\mathbf{Q}[x_1, \dots, x_n]$ Gaussův, existje v něm $\mathrm{NSD}(p, q)$, označme ho $d$. Zřejmě $d$ dělí $p$ i $q$ v oboru $\mathbf{Q}[\mathbb{X}]$. Vezmeme-li $e$, které dělí $p$ i $q$ v oboru $\mathbf{Q}[\mathbb{X}]$, potom $e \in \mathbf{Q}[x_1, \dots, x_n]$ podle (c). Protože $d$ je $\mathrm{NSD}(p, q)$ v $\mathbf{Q}[x_1, \dots, x_n]$, nutně $e/d$ v $d$ v oboru $\mathbf{Q}[x_1, \dots, x_n]$, a tudíž i $e/d$ v oboru $\mathbf{Q}[\mathbb{X}]$.

(g) Plyne z bodů (d) a (f). □

## 2. Homomorfismy cyklických grup a řády prvků

Připomeňme, že zobrazení $f : G \to H$ grupy $(G, \cdot, ^{-1}, 1)$ do grupy $(H, \cdot, ^{-1}, 1)$ se nazývá homomorfismus, jestliže pro všechna $a, b \in G$ platí $f(a \cdot b) = f(a) \cdot f(b)$, $f(a^{-1}) = (f(a))^{-1}$ a $f(1) = 1$. a

**2.1.** Dokažte, že zobrazení $f : G \to H$ grupy $(G, \cdot, ^{-1}, 1)$ do $(H, \cdot, ^{-1}, 1)$, které splňuje $f(a \cdot b) = f(a) \cdot f(b)$ pro všechna $a, b \in G$, je homomorfismus.

Protože $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$, stačí rovnost $f(1) = f(1) \cdot f(1)$ přenásobit prvkem $f(1)^{-1}$, abychom dostali $1 = f(1) \cdot f(1)^{-1} = f(1) \cdot f(1) \cdot f(1)^{-1} = f(1)$. Dále $1 = f(1) = f(a^{-1} \cdot a) = f(a^{-1}) \cdot f(a)$ a podobně $1 = f(a) \cdot f(a^{-1})$, proto $f(a^{-1}) = (f(a))^{-1}$. □

*17.3.*

Jsou-li $G$, $H$ grupy, označme $\mathrm{Hom}(G, H)$ množinu všech homomorfismů $G$ do $H$.

**2.2.** Popište všchny prvky množiny

(a) $\mathrm{Hom}(\mathbf{Z}_{30}, \mathbf{Z}_{49})$,
(b) $\mathrm{Hom}(\mathbf{Z}_{30}, \mathbf{Z}_{30})$,
(c) $\mathrm{Hom}(\mathbf{Z}_{30}, \mathbf{Z}_{600})$,
(d) $\mathrm{Hom}(\mathbf{Z}_{30}, \mathbf{Z}_{6})$,
(e) $\mathrm{Hom}(\mathbf{Z}_{30}, \mathbf{Z}_{800})$.

Uvažujeme-li homomorfismus $\varphi : \mathbf{Z}_{30} \to H$ pro libovolnou konečnou grupu $H$, všimneme si, že $\varphi(\mathbf{Z}_{30})$ je podgrupa grupy $H$, tedy podle Lagrangeovy věty $|\varphi(\mathbf{Z}_{30})|/|H|$. Využijeme-li 1. větu o izomorfismu, vidíme, že $\varphi(\mathbf{Z}_{30}) \cong \mathbf{Z}_{30}/\mathrm{Ker}\varphi$, proto opět díky Lagrangeově Větě $|\varphi(\mathbf{Z}_{30})| \cdot \mathrm{Ker}\varphi = |\mathbf{Z}_{30}| = 30$, tudíž $|\varphi(\mathbf{Z}_{30})|/30$.

(a) Je-li $\varphi : \mathbf{Z}_{30} \to \mathbf{Z}_{49}$ homomorfismus, z předchozího pozorování vyplývá, že $|\varphi(\mathbf{Z}_{30})|$ dělí číslo 30 i číslo 49, tedy $|\varphi(\mathbf{Z}_{30})| = 1$. To zamená, že $\mathrm{Hom}(\mathbf{Z}_{30}, \mathbf{Z}_{49})$ obsahuje pouze nulový homomorfismus. Poznamenejme, že bychom dostali stejný výsledek i kdybychom uvažovali obecné grupy řádu 30 a 49.

(b) Uvažujme homomorfismus $\varphi : \mathbf{Z}_{30} \to \mathbf{Z}_{30}$. Jestliže $\varphi(1) = k$, snadno nahlédneme, že $\varphi(1+1) = \varphi(1) + \varphi(1) = (2k)\mathrm{mod}\ 30$, $\varphi(2+1) = \varphi(2) + \varphi(1) = (3k)\mathrm{mod}\ 30, \ldots$, tedy $\varphi(a) = (ak)\mathrm{mod}\ 30$ pro každé $a \in \mathbf{Z}_{30}$. Uvědomili jsme si, že homomorfismus je dán obrazem prvku 1 (nebo jiného generátoru). Naopak, definujeme-li pro libovolné $k \in \mathbf{Z}_{30}$ zobrazení $\varphi_k : \mathbf{Z}_{30} \to \mathbf{Z}_{30}$ předpisem $\varphi_k(a) = (ak)\mathrm{mod}\ 30$, vidíme, že

$$\varphi_k(a+b) = ((a+b)k)\mathrm{mod}\ 30 = ((ak)\mathrm{mod}\ 30 + (bk)\mathrm{mod}\ 30)\mathrm{mod}\ 30 = \varphi_k(a) + \varphi_k(b),$$

tedy jedná se o homomorfismus. Ukázali jsme , že $\mathrm{Hom}(\mathbf{Z}_{30}, \mathbf{Z}_{30}) = \{\varphi_k |\ k \in \mathbf{Z}_{30}\}$.

(c) Opět mějme homomorfismus $\varphi : \mathbf{Z}_{30} \to \mathbf{Z}_{600}$. Všimněme si, že $30/600$, tedy existuje právě jedna třicetiprvková podgrupa grupy $\mathbf{Z}_{600}$ řádu 30, konkrétně jde o podgrupu

$$\langle 20 \rangle = 20\mathbf{Z}_{600} = \{0, 20, 40, \ldots, 560, 580\}.$$

Obdobně nahlédneme, že i pro každý dělitel $d$ čísla 30 existuje jednoznačně určená podgrupa $\langle \frac{600}{d} \rangle$ řádu $d$, která je zřejmě obsažena v grupě $\langle 20 \rangle$. Označíme-li $d = |\varphi(\mathbf{Z}_{30})|$, vidíme, že $\varphi(\mathbf{Z}_{30}) = \langle \frac{600}{d} \rangle \subseteq \langle 20 \rangle$, tedy $\varphi(1) \in \langle 20 \rangle$. Naopak, zvolíme-li $k \in \mathbf{Z}_{30}$ definujeme-li zobrazení $\varphi_k : \mathbf{Z}_{30} \to \mathbf{Z}_{600}$ předpisem $\varphi_k(a) = (20ka)\mathrm{mod}\ 30$, vidíme, že

$$\varphi_k(a+b) = (20k(a+b)\mathrm{mod}\ 30)\mathrm{mod}\ 600 = ((20ka) + (20kb))\mathrm{mod}\ 600 = \varphi_k(a) + \varphi_k(b),$$

tedy i tentokrát je $\varphi_k$ homomorfismus. Tím jsme ověřili, že $\mathrm{Hom}(\mathbf{Z}_{30}, \mathbf{Z}_{600}) = \{\varphi_k |\ k \in \mathbf{Z}_{30}\}$.

(d) Zvolme libovolně $\varphi : \mathbf{Z}_{30} \to \mathbf{Z}_{6}$. I tentokrát je homomorfismus určen obrazem prvku 1, a protože $6/30$ je zobrazení $\varphi_k : \mathbf{Z}_{30} \to \mathbf{Z}_{6}$ dané předpisem $\varphi_k(a) =$

$(ka)\bmod 6$ homomorfismus, neboť

$$\varphi_k(a+b) = (k(a+b)\bmod 30)\bmod 6 = ((ka)+(kb))\bmod 6 = \varphi_k(a)+\varphi_k(b).$$

Dokázali jsme, že $\mathrm{Hom}(\mathbf{Z}_{30},\mathbf{Z}_6) = \{\varphi_k |\ k \in \mathbf{Z}_6\}$.

(e) Buď $\varphi : \mathbf{Z}_{30} \to \mathbf{Z}_{800}$ homomorfismus a položme $d = |\varphi(\mathbf{Z}_{30})|$. Z úvodního úvahy plyne, že $d/\mathrm{NSD}(30,800) = 10$, proto obdobnou úvahou jako v případě (c), dostáváme, že $\varphi(\mathbf{Z}_{30}) = \langle\frac{800}{d}\rangle \subseteq \langle\frac{800}{10}\rangle\langle 80\rangle$. Zároveň obvyklým argumentem nahlédneme, že je zobrazení $\varphi_k : \mathbf{Z}_{30} \to \mathbf{Z}_{800}$ dané předpisem $\varphi_k(a) = (10ka)\bmod 30$ pro každé $k \in \mathbf{Z}_{10}$ homomorfismus, tedy $\mathrm{Hom}(\mathbf{Z}_{30},\mathbf{Z}_{800}) = \{\varphi_k |\ k \in \mathbf{Z}_{10}\}$. □

**2.3.** Které z homomorfismů uvažovaných v 2.2 jsou prosté a které jsou na?

Uvažujme opět homomorfismus $\varphi : \mathbf{Z}_{30} \to H$ pro libovolnou konečnou grupu $H$. Snadno nahlédneme, že $\varphi$ je prosté, právě když $|\varphi(\mathbf{Z}_{30})| = 30$, a $\varphi$ je na, právě když $\varphi(1)$ je generátor $H$. V konkrérních případech to znamená, že

(a) žádný prostý ani surjektivní homomorfismusu $\mathbf{Z}_{30}$ do $\mathbf{Z}_{49}$ neexistuje;
(b) homomorfismus $\varphi_k : \mathbf{Z}_{30} \to \mathbf{Z}_{30}$ daný předpisem $\varphi_k(a) = (ak)\bmod 30$ je prostý, právě když je na a to nastává právě pro $k \in \mathbf{Z}_{30}^*$ (takových homomorfismů je právě 8);
(c) samozřejmě žádný homomorfismus $\mathbf{Z}_{30}$ na $\mathbf{Z}_{600}$ neexistuje a homomorfismus $\varphi_k : \mathbf{Z}_{30} \to \mathbf{Z}_{600}$ daný předpisem $\varphi_k(a) = (20ka)\bmod 600$ je prostý, právě když $k \in \mathbf{Z}_{30}^*$ (tedy opět máme 8 prostých homomorfismů);
(d) zřejmě neexistuje žádný prostý homomorfismus $\mathbf{Z}_{30}$ na $\mathbf{Z}_6$ a homomorfismus $\varphi_k : \mathbf{Z}_{30} \to \mathbf{Z}_6$ definovaný vztahem $\varphi_k(a) = (ka)\bmod 6$ je na $\mathbf{Z}_6$, právě když $k \in \mathbf{Z}_6^*$ (tedy epimorfismy jsou zobrazení $\varphi_1$ a $\varphi_5$);
(e) žádný monomorfismus ani epimorfismusu $\mathbf{Z}_{30}$ do $\mathbf{Z}_{800}$ neexistuje. □

**2.4.** Určete řád prvku 4 v grupě $(\mathbf{Z}_{3^{10}}^*, \cdot, ^{-1}, 1)$.

Předně připomeňme, že řád grupy $\mathbf{Z}_{3^{10}}^*$ je $\varphi(\mathbf{Z}_{3^{10}}^*) = (3-1)3^9$, kde $\varphi$ značí Eulerovu funkci, tedy podle Lagrangeovy věty musí být řád prvku 4 tvaru $2^\alpha 3^\beta$ pro $\alpha \in \mathbf{Z}_2$ a $\beta \in \mathbf{Z}_9$. Dále poznamenejme, že $4 = 1+3 \in G = \{1+3a |\ a \in \mathbf{Z}_{3^9}\}$ a že je $G$ podgrupa grupy $(\mathbf{Z}_{3^{10}}^*, \cdot, ^{-1}, 1)$ řádu $3^9$ (zřejmě jde o prvky nesoudělné s 3, tedy invertibilní v $(\mathbf{Z}_{3^{10}}, \cdot, 1)$, dále je $G$ uzavřená na součiny, obsahuje 1, a protože je $G$ konečné, musí pro každé $a$ existovat $n$, pro něž $(1+3a)^n = 1$, tedy $(1+3a)^{-1} = (1+3a)^{n-1} \in G$). To znamená, že řád 4 musí dělit řád $G$, a proto $\alpha = 0$.

Nyní si zbývá uvědomit, že podle Tvrzení 2.9 z přednášky pro každé přirozené $e \geq 2$ a každé liché prvočíslo $p$ platí, že $(1+p)^{p^{e-2}} \equiv 1 + p^{e-1} \bmod p^e$, proto $1+3$ není řádu $3^i$ pro žádné $i = 1,\ldots,8$, tudíž je nutně řádu $3^9$. □

*24.3.*

**2.5.** Najděte generátor cyklické grupy $(\mathbf{Z}_{3^{10}}^*, \cdot, ^{-1}, 1)$.

V úloze 2.4 jsme zjistili, že podgrupa $\langle 4\rangle$ je řádu $3^9$, proto snandno pomocí Lagrangeovy věty spočítáme, že $[\mathbf{Z}_{3^{10}}^* : \langle 4\rangle] = \frac{|\mathbf{Z}_{3^{10}}^*|}{|\langle 4\rangle|} = \frac{2\cdot 3^9}{3^9} = 2$. Najdeme-li tedy prvek $a \in \mathbf{Z}_{3^{10}}^*$, pro který platí, že $a \notin \langle 4\rangle$ a $\langle 4\rangle \subseteq \langle a\rangle$, potom to už nutně musí být prvek řádu řádu $2\cdot 3^9$, tedy generátor grupy $\mathbf{Z}_{3^{10}}^*$.

Vidíme, že $2 \notin \langle 4\rangle = \{1+3a |\ a \in \mathbf{Z}_{3^9}\}$ a $2^2 = 4$, proto $\langle 4\rangle \subseteq \langle 2\rangle$. Hledaným generátorem je tedy například prvek 2. □

**2.6.** Rozhodněte, zda je prvek $b$ generátorem cyklické grupy $(\mathbf{Z}^*_{3^{10}}, \cdot, ^{-1}, 1)$, jestliže

(a) $b = 2^{15}$,
(b) $b = 2^{16}$,
(c) $b = 2^{17}$,
(d) $b = 13$,
(e) $b = 3^{10} - 2$.

(a) - (c) Máme-li generátor 2 cyklické grupy $(\mathbf{Z}^*_{3^{10}}, \cdot, ^{-1}, 1)$, víme, že zobrazení $\psi : \mathbf{Z}_{2\cdot 3^9} \to \mathbf{Z}^*_{3^{10}}$ dané předpisem $\psi(k) = 2^k$ je izomorfismem grup $(\mathbf{Z}_{2\cdot 3^9}, +, -, 0)$ a $(\mathbf{Z}^*_{3^{10}}, \cdot, ^{-1}, 1)$. Rozhodujeme-li otázku, zda je $2^k$ generátorem multiplikativní grupy $(\mathbf{Z}^*_{3^{10}}, \cdot, ^{-1}, 1)$, stačí tedy abychom zjistili, zda je prvek $k$ generátorem aditivní grupy $(\mathbf{Z}_{2\cdot 3^9}, +, -, 0)$, tedy zda je číslo $k$ nesoudělné s číslem $2 \cdot 3^9$. To znamená, že $2^{15}$ ani $2^{16}$ generátorem nejsou, neboť $\mathrm{NSD}(15, 2\cdot 3^9) = 3$ a $\mathrm{NSD}(16, 2\cdot 3^9) = 2$, zatímco $2^{17}$ je generátorem, protože $\mathrm{NSD}(17, 2\cdot 3^9) = 1$.

(d), (e) Předně vidíme, že $\mathrm{NSD}(13, 2\cdot 3^9) = 1$ a $\mathrm{NSD}(3^{10}-2, 2\cdot 3^9) = 1$, proto $13, 3^{10}-2 \in \mathbf{Z}^*_{3^{10}}$. Protože $3^{10} - 2 = 1 + 3(3^9 - 1) \in \langle 4\rangle$ a $13 = 1 + 3 \cdot 4 \in \langle 4\rangle$, prvek 13 ani prvek $3^{10} - 2$ negenerují grupu $\mathbf{Z}^*_{3^{10}}$. □

**2.7.** Spočítejte řády prvků $2^{15}$, $2^{16}$ a $3^{10} - 2$ grupy $(\mathbf{Z}^*_{3^{10}}, \cdot, ^{-1}, 1)$.

U čísel $2^{15}$, $2^{16}$ stačí díky izomorfismu $\psi$ určit řád prvku 15 a 16 v grupě $(\mathbf{Z}_{2\cdot 3^9}, +, -, 0)$, tedy $|\langle 2^{15}\rangle| = \frac{2\cdot 3^9}{\mathrm{NSD}(15, 2\cdot 3^9)} = 2 \cdot 3^8$, a $|\langle 2^{16}\rangle| = \frac{2\cdot 3^9}{\mathrm{NSD}(16, 2\cdot 3^9)} = 3^9$.

Uvědomíme-li si, že $(3^{10} - 2)^2 = 4$ v grupě $(\mathbf{Z}^*_{3^{10}}, \cdot, ^{-1}, 1)$ a že $3^{10} - 2 \in \langle 4\rangle$, vidíme, že $\langle 3^{10} - 2\rangle = \langle 4\rangle$, tedy řád prvku $3^{10} - 2$ je $3^9$. □

**2.8.** Uvažujme v grupě $(\mathbf{Z}^*_{5^8}, \cdot, ^{-1}, 1)$ prvek $a$ řádu $5^7$ a prvek $b$ řádu $4 \cdot 5^\beta$, kde $0 \le \beta < 7$. Dokažte, že $a \cdot b$ generuje $\mathbf{Z}^*_{5^8}$.

Z Lagrangeovy věty víme, že řád prvku $a \cdot b$ je $2^\alpha \cdot 5^\gamma$ pro nějaká $\alpha \in \mathbf{Z}_3$ a $\gamma \in \mathbf{Z}_8$. Nejprve nahlédneme, že $(a \cdot b)^{5^7} = a^{5^7} \cdot b^{5^7} = b^{5^7}$, tedy s využitím faktu, že zobrazení $k \to b^k$ indukuje izomorfismus cyklických grup $(\mathbf{Z}_{4\cdot 5^\beta}, +, -, 0)$ a $(\langle b\rangle, \cdot, ^{-1}, 1)$, dostáváme, že $b^{5^7}$ je prvek řádu 4. Protože $\langle b^{5^7}\rangle \subseteq \langle b\rangle$, dává nám Lagrangeova věta závěr, že $4/2^\alpha \cdot 5^\gamma$, tedy $\alpha = 2$. Obdobným argumentem pro grupu $(\langle a \cdot b\rangle, \cdot, ^{-1}, 1)$ dospějeme k pozorování, že $(a \cdot b)^4$ je prvek řádu $5^\gamma$. Ukážeme, že $\gamma = 7$.

Předpokládejme, že $\gamma < 7$. Protože $(a^4 \cdot b^4)^{5^\beta} = a^{4\cdot 5^\beta} \cdot b^{4\cdot 5^\beta} = a^{4\cdot 5^\beta} \neq 1$, musí $\gamma > \beta$, ovšem potom dostáváme, že $1 = (a^4 \cdot b^4)^{5^\gamma} = a^{4\cdot 5^\gamma} \cdot b^{4\cdot 5^\gamma} = a^{4\cdot 5^\gamma}$, tudíž $\gamma = 7$. Nyní znovu využijeme Lagrangeovu větu, abychom zjistili, že řád prvku $a \cdot b$ je $4 \cdot 5^7$, tedy, že $a \cdot b$ generuje grupu $\mathbf{Z}^*_{5^8}$. □

**2.9.** Najděte generátor cyklické grupy $(\mathbf{Z}^*_{5^8}, \cdot, ^{-1}, 1)$.

Vyžijeme-li výsledek předchozí úlohy, stačí najít prvek řádu $5^7$ a prvek řádu $4\cdot 5^\beta$ pro $\beta < 7$.

Stejným postupem jako v úloze 2.4 (tj. v důsledku Tvrzení 2.10 ze skript) zjistíme, že $6 = 1 + 5$ je prvek řádu $5^7$. Protože $2^2, 2^3 \notin \langle 6\rangle = \{1 + 5a |\ a \in \mathbf{Z}_{5^7}\}$ a $2^4 \in \langle 6\rangle$, je rozkladová třída $2 \cdot \langle 6\rangle$ generátorem čtyřprvkové faktorové grupy $\mathbf{Z}^*_{5^8}/\langle 6\rangle$, tedy opět díky Lagrangeově větě vidíme, že 4 dělí řád prvku 2 v grupě

$\mathbf{Z}_{5^8}^*$. Nevíme ovšem, zda 2 je či není generátorem celé grupy $\mathbf{Z}_{5^8}^*$, zodpovězení této otázky odpovídá nalezení diskrétního logaritmu prvku $2^4$ o základu 6 (což je obecně obtížná úloha). Vezmeme-li ovšem prvek $2^5$, obvyklým způsobem nahlédneme, že je řádu $4 \cdot 5^{\max(0,\beta-1)}$, jakmile $4 \cdot 5^\beta$ je řád prvku 2. Tedy podle pozorování 2.8 je prvek $2^5 \cdot 6 = 192$ generátorem grupy $\mathbf{Z}_{5^8}^*$. □

**2.10.** Najděte v grupě $(\mathbf{Z}_{225}^*, \cdot, ^{-1}, 1)$ prvky řádu 2, 3 a 5.

Nejprve si uvědomme, že prvkem řádu 2, tedy involucí, je zřejmě $225 - 1 = 224$.

Podle Čínské věty o zbytcích je zobrazení $f : \mathbf{Z}_{225} \to \mathbf{Z}_9 \times \mathbf{Z}_{25}$ dané předpisem $f(k) = (k \bmod 9, k \bmod 25)$ okruhový izomorfismus, proto indukuje izomorfismus mezi grupami invertibilních prvků $f_* : \mathbf{Z}_{225}^* \to \mathbf{Z}_9^* \times \mathbf{Z}_{25}^*$. Tvrzení 2.10 ze skript, jehož důkazu jsme věnovali pozornost v úloze 2.4 nám dává prvek 4 řádu 3 v grupě $\mathbf{Z}_9^* = \mathbf{Z}_{3^2}^*$ a prvek 6 řádu 5 v grupě $\mathbf{Z}_{25}^* = \mathbf{Z}_{5^2}^*$. Protože se v grupě $\mathbf{Z}_9^* \times \mathbf{Z}_{25}^*$ násobí po složkách, vidíme, že prvek $(4, 1)$ je zde řádu 3 a prvek $(1, 6)$ je řádu 5, tedy nám zbývá (obecně pomocí rozšířeného Eukleidova algoritmu, zde spíše zkusmo) najít prvky $f_*^{-1}((4, 1))$ a $f_*^{-1}((1, 6))$.

Tedy v prvním případě hledáme $a \in \mathbf{Z}_{225}$, pro které

$$a \equiv 4 (\bmod\ 9), \qquad a \equiv 1 (\bmod\ 25).$$

Vyjádříme-li si z druhé kongruence $a = 1 + 25 \cdot b$ pro vhodné $b \in \mathbf{Z}_9$ a dosadíme do první kongruence, dostáváme

$$\begin{aligned} 1 + 25 \cdot b &\equiv 4 \pmod 9, \\ 7 \cdot b &\equiv 3 \pmod 9, \\ b &\equiv 3 \pmod 9. \end{aligned}$$

Tedy $a = 1 + 25 \cdot 3 = 76$ je prvek grupy $(\mathbf{Z}_{225}^*, \cdot, ^{-1}, 1)$ řádu 3.

Podobně v druhém případě hledáme $a \in \mathbf{Z}_{225}$, pro něž

$$a \equiv 1 (\bmod\ 9), \qquad a \equiv 6 (\bmod\ 25).$$

Upravujme obdobně jako výše: $a = 6 + 25 \cdot b$ pro $b \in \mathbf{Z}_9$ a

$$\begin{aligned} 6 + 25 \cdot b &\equiv 1 \pmod 9, \\ 7 \cdot b &\equiv 4 \pmod 9, \\ b &\equiv 7 \pmod 9. \end{aligned}$$

Spočítali jsme, že $a = 1 + 25 \cdot 7 = 176$ je prvek řádu 5. □

*31.3.*

**2.11.** Určete pro každé přirozené $k$, kolik je v grupě $(\mathbf{Z}_{231}^*, \cdot, ^{-1}, 1)$ prvků řádu $k$.

Nejprve si rozmyslíme, pro která $k$ v grupě $(\mathbf{Z}_{231}^*, \cdot, ^{-1}, 1)$ existuje nějaký prvek řádu $k$. Využijeme několikrát Čínskou větu o zbytcích. Nejprve spočítáme prvočíselný rozklad $231 = 3 \cdot 7 \cdot 11$ a nahlédneme, že jsou izomorfní okruhy $\mathbf{Z}_{231}$ a $\mathbf{Z}_3 \times \mathbf{Z}_7 \times \mathbf{Z}_{11}$, tedy jsou izomorfní i grupy invertibilních prvků $\mathbf{Z}_{231}^*$ a $\mathbf{Z}_3^* \times \mathbf{Z}_7^* \times \mathbf{Z}_{11}^*$. Protože jsou grupy $(\mathbf{Z}_p^*, \cdot, ^{-1}, 1)$ pro všechna prvočísla $p$ cyklické, dostáváme izomorfismus

$$(\mathbf{Z}_3^* \times \mathbf{Z}_7^* \times \mathbf{Z}_{11}^*, \cdot, ^{-1}, (1,1,1)) \cong (\mathbf{Z}_2 \times \mathbf{Z}_6 \times \mathbf{Z}_{10}, +, -, (0,0,0))$$

a využijeme-li Čínskou větu o zbytcích pro aditivní grupy $\mathbf{Z}_6$ a $\mathbf{Z}_{10}$ máme

$$\mathbf{Z}_2 \times \mathbf{Z}_6 \times \mathbf{Z}_{10} \cong \mathbf{Z}_2 \times (\mathbf{Z}_2 \times \mathbf{Z}_3) \times (\mathbf{Z}_2 \times \mathbf{Z}_5) \cong \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5.$$

Protože je grupa $(\mathbf{Z}_{231}^*, \cdot, ^{-1}, 1)$ izomorfní grupě $(\mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5, +, -, ((0,0,0),0,0))$, můžeme otázku řádu prvků v multiplikativní grupě $\mathbf{Z}_{231}^*$ zodpovědět v aditivní grupě $\mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$. Označíme-li $o(g)$ řád prvku $g$ a zvolíme $a \in \mathbf{Z}_2^3$, $b \in \mathbf{Z}_3$ a $c \in \mathbf{Z}_5$, vidíme, že $o((a,b,c)) = \mathrm{nsn}(o(a), o(b), o(c))$, přičemž v grupě $\mathbf{Z}_2^3$ nacházíme 1 prvek řádu 1 a 7 prvků řádu 2, v grupě $\mathbf{Z}_3$ máme 1 prvek řádu 1 a 2 prvky řádu 3 a konečně grupa $\mathbf{Z}_5$ obsahuje právě 1 prvek řádu 1 a 4 prvky řádu 5. To znamená, že grupa $\mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$, a proto i grupa $\mathbf{Z}_{231}^*$ obsahuje prvky řádu $2^\alpha 3^\beta 5^\gamma$ pro $\alpha, \beta, \gamma \in \{0,1\}$.

Nyní už snando určíme počty prvků daného řádu:

k=1 V každé grupě máme zřejmě právě 1 prvek řádu 1.

k=2 Počítáme počet prvků množiny

$$\{(a,b,c) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ \mathrm{nsn}(o(a), o(b), o(c)) = 2\} =$$
$$= \{(a,b,c) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ o(a) = 2, o(b) = 1, o(c) = 1\} =$$
$$= \{(a,0,0) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ a \neq (0,0,0)\},$$

tedy máme 7 prvků řádu 2.

k=3 Počítáme počet prvků množiny

$$\{(a,b,c) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ \mathrm{nsn}(o(a), o(b), o(c)) = 3\} = \{(0,b,0) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ b \neq 0\},$$

tedy máme 2 prvky řádu 3.

k=5 Tentokrát pracujeme s množinou

$$\{(a,b,c) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ \mathrm{nsn}(o(a), o(b), o(c)) = 5\} = \{(0,0,c) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ c \neq 0\},$$

která obsahuje všechny 4 prvky řádu 5.

k=6 Nyní spočítáme $|\{(a,b,c) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ \mathrm{nsn}(o(a), o(b), o(c)) = 6\}| =$ $= |\{(a,b,0) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ a \neq (0,0,0), b \neq 0\}| = 14$ prvků řádu 6.

k=10 Počítáme

$$|\{(a,0,c) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ a \neq (0,0,0), c \neq 0\}|,$$

tudíž máme 28 prvků řádu 10.

k=15 Tentokrát dostáváme právě $|\{(0,b,c) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ b \neq 0, c \neq 0\}| = 8$ prvků řádu 15.

k=30 Konečně $|\{(a,b,c) \in \mathbf{Z}_2^3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 |\ a \neq (0,0,0), b \neq 0, c \neq 0\}| = 56$ je počet prvků řádu 30.

□

**2.12.** Najděte v grupě $(\mathbf{Z}_{231}^*, \cdot, ^{-1}, 1)$ tři involuce a jeden prvek řádu 30.

Označme $f : \mathbf{Z}_{231}^* \to \mathbf{Z}_3^* \times \mathbf{Z}_7^* \times \mathbf{Z}_{11}^*$ izomorfismus daný předpisem $f(k) = ((k)\mathrm{mod}\ 3, (k)\mathrm{mod}\ 7, (k)\mathrm{mod}\ 11)$ a postupujeme stejně jako v 2.10.

Nejprve snadno nahlédneme, že $230 = 231 - 1$ je involuce. Všimněme si, že $f(230) = (2,6,10)$. Nyní potřebujeme najít další prvky řádu 2 v grupě $\mathbf{Z}_3^* \times \mathbf{Z}_7^* \times \mathbf{Z}_{11}^*$, zvolíme například $(2,1,1)$ a $(2,1,10)$ a hledáme $a, b \in \mathbf{Z}_{231}^*$, aby $f(a) = (2,1,1)$ a $f(b) = (2,1,10)$, tedy řešíme kongruence:

$$a \equiv 2(\mathrm{mod}\ 3), \qquad a \equiv 1(\mathrm{mod}\ 7), \qquad a \equiv 1(\mathrm{mod}\ 11),$$
$$b \equiv 2(\mathrm{mod}\ 3), \qquad b \equiv 1(\mathrm{mod}\ 7), \qquad b \equiv 10(\mathrm{mod}\ 11),$$

Vyjádříme $a = 2 + 3c_1$ a upravujme jako v 2.10:

$$\begin{aligned} 2 + 3 \cdot c_1 &\equiv 1 \pmod 7, \\ 3 \cdot c_1 &\equiv 6 \pmod 7, \\ c_1 &\equiv 2 \pmod 7, \end{aligned}$$

tedy $a = 2 + 3 \cdot 2 + 21c_2 = 8 + 21c_2$ a stejným způsobem pokračujeme

$$\begin{aligned} 8 + 21 \cdot c_2 &\equiv 1 \pmod{11}, \\ 10 \cdot c_2 &\equiv 4 \pmod{11}, \\ c_2 &\equiv 7 \pmod{11}, \end{aligned}$$

proto $a = 8 + 21 \cdot 7 = 155$.

První krok druhého výpočtu proběhne stejně, tedy vyjádříme $b = 8 + 21d$ a dosadíme

$$\begin{aligned} 8 + 21 \cdot d &\equiv 10 \pmod{11}, \\ 10 \cdot d &\equiv 2 \pmod{11}, \\ d &\equiv 9 \pmod{11}, \end{aligned}$$

tudíž $b = 8 + 21 \cdot 9 = 197$.

Pro nalezení prvku řádu 30 v grupě $(\mathbf{Z}_{231}^*, \cdot, ^{-1}, 1)$ nejprve najdeme prvek řádu 10 v $(\mathbf{Z}_{11}^*, \cdot, ^{-1}, 1)$ a prvek řádu 3 v grupě $(\mathbf{Z}_7^*, \cdot, ^{-1}, 1)$. V prvním případě tedy hledáme generátor $\mathbf{Z}_{11}^*$ jímž je například prvek 2, neboť $2^2 \not\equiv 1 \not\equiv 2^5 (\mathrm{mod}\ 11)$. V druhé grupě snadno nahlédneme, že 4 je řádu 3, proto tentokrát počítáme soustavu kongruencí

$$x \equiv 1 (\mathrm{mod}\ 3), \qquad x \equiv 4 (\mathrm{mod}\ 7), \qquad x \equiv 2 (\mathrm{mod}\ 11),$$

kterou standardním postupem vyřešíme: položíme $x = 2 + 11c_1$ a upravujme

$$\begin{aligned} 2 + 11 \cdot c_1 &\equiv 4 \pmod 7, \\ 4 \cdot c_1 &\equiv 2 \pmod 7, \\ c_1 &\equiv 4 \pmod 7, \\ x &= 46 + 77c_2 \\ 46 + 77 \cdot c_2 &\equiv 1 \pmod 3, \\ 2 \cdot c_2 &\equiv 0 \pmod 3, \\ x &= 46. \end{aligned}$$

Zjistili jsme, že číslo 46 má v grupě $(\mathbf{Z}_{231}^*, \cdot, ^{-1}, 1)$ řád 30. □

**2.13.** Najděte v grupě $(\mathbf{Z}_{231}^*, \cdot, ^{-1}, 1)$ aspoň 3 prvky $a$, pro která $a^{231-1} = 1$. Kolik takových prvků existuje?

Hledáme tedy 3 Fermatovy lháře, přesněji řečeno 3 báze pseudoprvočísla 231, tj. čísla $a \in \mathbf{Z}_{231}^*$, pro něž $a^{230} \equiv 1 (\mathrm{mod}\ 231)$. Vidíme, že tuto podmínku splňují právě ty prvky grupy $(\mathbf{Z}_{231}^*, \cdot, ^{-1}, 1)$, jejichž řád dělí číslo $231 - 1 = 230 = 2 \cdot 5 \cdot 23$, tedy, jak jsme ukázali v úloze 2.11 právě prvky řádu 1,2, 5 a 10. Zřejmě tedy tuto podmínku splňuje prvek 1 a dále prvky 155 a 197, která jsou podle 2.12 řádu 2. Konečně poznamenejme, že prvků řádu 1,2, 5 a 10 je v grupě $(\mathbf{Z}_{231}^*, \cdot, ^{-1}, 1)$ celkem 40. □

**2.14.** Uvažujme grupu $(\mathbf{Z}_{297}^*, \cdot, ^{-1}, 1)$.

(a) Spočítejte, kolik v grupě $\mathbf{Z}_{297}^*$ existuje bází pseudoprvočísla 297 (tj. Fermatových lhářů),
(b) určete, kolik čísel $a \in \mathbf{Z}_{297}$ nesplní podmínku $a^{296} \equiv 1 \pmod{297}$ (tj. neprojdou Fermatovým testem),
(c) najděte všechny báze pseudoprvočísla 297,
(d) najděte všechny báze silného pseudoprvočísla 297 (tj. čísla, která neprojdou Rabinovým-Millerovým testem).

(a) Protože, $297 = 3^3 \cdot 11$, opět si uvědomíme, že

$$\mathbf{Z}_{297}^* \cong \mathbf{Z}_{3^3}^* \times \mathbf{Z}_{11}^* \cong \mathbf{Z}_{18} \times \mathbf{Z}_{10} \cong \mathbf{Z}_2^2 \times \mathbf{Z}_9 \times \mathbf{Z}_5.$$

(zdůrazněme, že dvě grupy vlevo mají multiplikativní strukturu a dvě grupy vpravo mají aditvní strukturu). Zodpovíme tedy otázku v grupě $\mathbf{Z}_2^2 \times \mathbf{Z}_9 \times \mathbf{Z}_5$, kde hledáme počet prvků, jejichž řád dělí číslo 296. Stejně jako v úloze 2.11 si tedy uvědomíme, že pro prvek $(a,b,c,d) \in \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_5$ platí $x(a,b,c,d) = (xa, xb, xc, xd) = (0,0,0,0)$, právě když $\mathrm{nsn}(o(a), o(b), o(c), o(d))/x$. Protože chceme, aby zároveň $x/296 = 2^3 \cdot 37$, hledáme tedy taková $(a,b,c,d)$, aby $y = \mathrm{nsn}(o(a), o(b), o(c), o(d))/2^3 \cdot 37$. Protože víme, že $y = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$ pro vhodná $\alpha, \gamma \in \mathbf{Z}_2$ a $\beta \in \mathbf{Z}_3$, stačí nám uvažovat dělitele $\mathrm{NSD}(2^1 \cdot 3^2 \cdot 5^1, 2^3 \cdot 37) = 2$. Vidíme, že stačí spočítat prvky exponentu 2 (tedy řádů, které dělí 2), jimiž jsou právě $(a,b,0,0)$, kde $s, b \in \mathbf{Z}_2^2$. Zjistili jsme, že máme právě čtyři Fermatovy lháře.

(b) Platí-li pro nějaké $a \in \mathbf{Z}_{297}$, že $a^m \equiv 1 \pmod{297}$ pro nějaké kladné $m$, potom $(a^{m-1}) \mathrm{mod}\ 297$ je inverz k číslu $a$, a proto $a \in \mathbf{Z}_{297}^*$, To znamená, že pro číslo $a$ soudělné s hodnotou 297 podmínka $a^{296} \equiv 1 \pmod{297}$ nemůže být splněna. Fermatovým testem tedy neprojdou pouze 4 hodnoty z grupy $\mathbf{Z}_{297}^*$ spočítané v příkladu (a).

(c) Díky úvaze z (a) postupujeme stejně jako v příkladu 2.11. Nejprve snadno najdeme (jediné) prvky řádu 2 v grupách $\mathbf{Z}_{11}^*$ a $\mathbf{Z}_{27}^*$, jimiž jsou zřejmě prvky opačné k jedničce, tedy $-1 \equiv 10 \pmod{11}$ a $-1 \equiv 26 \pmod{27}$. Dále bez počítání uvážíme, že jediným prvkem řádu 1 je v grupě $\mathbf{Z}_{297}^*$ prvek 1 a zjevným prvkem řádu 2 je zde $-1 \equiv 296 \pmod{297}$ (přitom zjevně platí, že $-1 \equiv 296 \pmod{11}$ a $-1 \equiv 296 \pmod{27}$). Tedy zbývá najít báze $a, b \in \mathbf{Z}_{297}^*$ splňující

$$a \equiv -1 (\mathrm{mod}\ 11), \quad a \equiv 1 (\mathrm{mod}\ 27), \qquad b \equiv 1 (\mathrm{mod}\ 11), \quad b \equiv -1 (\mathrm{mod}\ 27).$$

Protože $a \equiv -b (\mathrm{mod}\ 297)$, stačí vyřešit pouze jednu z dvojic kongruencí. Obvyklým způsobem vyjádříme $a = 1 + 27c$ a upravujme:

$$\begin{aligned} 1 + 27c &\equiv -1 \pmod{11}, \\ 5c &\equiv -2 \pmod{11}, \\ 10c &\equiv -4 \pmod{11}, \\ -c &\equiv -4 \pmod{11}, \\ c &\equiv 4 \pmod{11}, \end{aligned}$$

proto $a = 1 + 27 \cdot 4 = 109$ a $b = 297 - 109 = 188$. Našli jsme množinu $\{1, 109, 188, 296\}$ všech Fermatových lhářů.

(d) Připomeňme, že pro $N-1=2^e\cdot m$, kde je $m$ liché, je $a\in\mathbf{Z}_N$ bází silného pseudoprvočísla $N$, jestliže buď $a^m\equiv 1 \pmod N$ nebo existuje nezáporné $j<e$, pro něž $a^{2^j\cdot m}\equiv -1 \pmod N$ (a zjišťování, zda platí tato podmínka se nazývá Rabinův-Millerův test prvočíselnosti čísla $N$ v bázi $a$). Pro jakékoli liché $N$ zjevně platí, že $1^m\equiv 1 \pmod N$ a $(-1)^m\equiv -1 \pmod N$, tedy 1 a $-1$ jsou báze pseudoprvočísla $N$. Dále poznamenejme, že číslo, které projde Rabinovým-Millerovým testem nutně splní podmínku $a^{N-1}\equiv 1 \pmod N$, tedy projde i Fermatovým testem.

Zbývá nám Rabinovým-Millerovým testem otestovat čísla 109 a 188 pro $N-1=296=2^3\cdot 37$. Protože můžeme využít Čínskou větu o zbytcích pro kanonický okruhový izomorfismus $f:\mathbf{Z}^*_{297}\to\mathbf{Z}^*_{11}\times\mathbf{Z}^*_{27}$, nebudeme samozřejmě opravdu počítat $(109^{37})\mathrm{mod}\ 297$, protože

$$f(109^{37})=f(109)^{37}=((-1)^{37},1^{37})=(-1,1)=f(109),$$

tedy $(109^{37})\mathrm{mod}\ 297=109$. Podobně $(288^{37})\mathrm{mod}\ 297=288$. Dále

$$f(109^{2^j\cdot 37})=f(109)^{2^j\cdot 37}=(2^j\cdot 37,1^{2^j\cdot 37})=(-1^{2^j},1)=(1,1)=f(1),$$

tedy $(109^{2^j\cdot 37})\mathrm{mod}\ 297=1$ pro každé kladné $j$. Podobnou úvahu můžeme udělat i pro číslo 188. Vidíme, že báze 109 a 188 Rabinovým-Millerovým testem neprojdou. Jedinými bázemi silného pseudoprvočísla 297 jsou čísla 1 a 296. □

**2.15.** Rozhodněte, která z čísel 429, 561, 663, 1105 jsou Carmichaelova.

Máme za úkol pro dané liché $N$ zjistit, zda pro všechna $a\in\mathbf{Z}^*_N$ platí kongruence $a^{N-1}\equiv 1 \pmod N$. Uvažujme prvočíselný rozklad $N=\prod_i p_i^{r_i}$. V úloze 2.14 jsme nahlédli, že potřebujeme zjistit, zda řády všech prvků grupy $\mathbf{Z}^*_N\cong\prod_{i=1}^s\mathbf{Z}^*_{p_i^{r_i}}$, kde $\mathbf{Z}^*_{p_i^{r_i}}$ jsou cyklické grupy řádu $(p_i-1)p_i^{r_i-1}$, dělí číslo $N-1$. Tedy díky cykličnosti grup $\mathbf{Z}^*_{p_i^{r_i}}$ budeme zjišťovat, zda

$$\mathrm{nsn}((p_1-1)p_1^{r_1-1},\ldots,(p_s-1)p_s^{r_s-1})/N-1.$$

Uvažejme nyní jednotlivé případy:

(N=429) Spočítáme-li prvočíselný rozklad $429=3\cdot 11\cdot 13$ a $\mathrm{nsn}(2,10,12)=60$, snadno nahlédneme, že 60 nedělí číslo 428, tedy existuje prvek grupy $\mathbf{Z}^*_{429}$, který není bází pseudoprvočísla 429, proto číslo 429 není Carmichaelovo. Konkrétně si uvědomme, že umíme najít například prvek $a\in\mathbf{Z}^*_{429}$ řádu 5, pro který tudíž platí, že $a^{428}\equiv a^{425}\cdot a^3\equiv a^3\not\equiv 1 \pmod{429}$.

(N=561) Opět spočítáme prvočíselný rozklad $561=3\cdot 11\cdot 17$ a $\mathrm{nsn}(2,10,16)=80$. Nyní vidíme, že $80/560$, proto jsou všechny prvky grupy $\mathbf{Z}^*_{561}$ báze pseudoprvočísla 561 a číslo 561 je Carmichaelovo.

(N=663) Protože $663=3\cdot 13\cdot 17$ a $\mathrm{nsn}(2,12,16)=48$ nedělí číslo 662, číslo 663 není Carmichaelovo.

(N=1105) Tentokrát $1105=5\cdot 13\cdot 17$ a $\mathrm{nsn}(4,12,16)=48$ dělí číslo 1104, číslo 1105 tudíž je Carmichaelovo.

□

*14.4.*

**2.16.** Spočítejte kolik existuje bází silného pseudoprvočísla 561.

Víme, že $560 = 2^4 \cdot 35$ a $561 = 3 \cdot 11 \cdot 17$. Obvyklým způsobem přeložíme otázku počtu čísel $a \in \mathbf{Z}_{561}^*$ splňujících buď $a^{35} \equiv 1 \pmod{561}$ nebo $a^{2^j \cdot 35} \equiv -1 \pmod{561}$ pro nějaké nezáporné $j < 4$ do aditivní grupy $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \times \mathbf{Z}_{16}$, která je izomorfní multiplikativní grupě $\mathbf{Z}_{561}^* \cong \mathbf{Z}_3^* \times \mathbf{Z}_{11}^* \times \mathbf{Z}_{17}^*$.

Nejprve uvážíme, že involuci $-1$ grupy $\mathbf{Z}_{561}^*$ odpovídá při kanonickém izomorfismu Čínské věty o zbytcích prvek $(-1,-1,-1)$ grupy $\mathbf{Z}_3^* \times \mathbf{Z}_{11}^* \times \mathbf{Z}_{17}^*$. Protože je každá z grup $\mathbf{Z}_3^*$, $\mathbf{Z}_{11}^*$ a $\mathbf{Z}_{17}^*$ cyklická, obsahuje jedinou involuci, tedy jsou tyto multiplikativní grupy izomorfní aditivním grupám po řadě $\mathbf{Z}_2$, $\mathbf{Z}_2 \times \mathbf{Z}_5$ a $\mathbf{Z}_{16}$ s involucemi 1, $(1,0)$ a 8. Proto involuci $-1$ z grupy $\mathbf{Z}_{561}^*$ odpovídá v grupě $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \times \mathbf{Z}_{16}$ prvek $(1,1,0,8)$.

Nyní hledáme $\mathbf{a} = (a_1, a_2, a_3, a_4) \in \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \times \mathbf{Z}_{16}$, pro která platí

$$35 \cdot \mathbf{a} = (35a_1, 35a_2, 35a_3, 35a_4) = (a_1, a_2, 0, 3a_4) = (0,0,0,0)$$

nebo pro nějaké nezáporné $j < 4$

$$35 \cdot 2^j \cdot \mathbf{a} = (2^j a_1, 2^j a_2, 0, 3 \cdot 2^j a_4) = (1,1,0,8).$$

Poznamenejme, že $2^j a_1 = 1$ může nastat pouze pro $j = 0$, proto druhá podmínka platí pro $j = 0$, $a_1 = a_2 = 1$, $a_4 = 8$ a $a_3$ libovolné ze $\mathbf{Z}_5$, tedy pro pět různých $\mathbf{a}$. Podobně první podmínka je spolňena pro $a_1 = a_2 = a_4 = 0$ a $a_3 \in \mathbf{Z}_5$, tedy i v tomto případě nacházíme 5 bází. Zjistili jsme, že existuje celkem 10 bází silného pseudoprvočísla 561. □

Závěrem poznamenejme, že je číslo 561 Carmichaelovo, tedy existuje $\varphi(561) = 320$ bází pseudoprvočísla 561, což znamená, že zatímco při Fermatově testu pro náhodně zvolené číslo $a \in \mathbf{Z}_{561} \setminus \{0\}$ máme pravděpodobnost $\frac{320}{560} = \frac{4}{7}$, že neodhalíme, že se nejedná o prvočíslo, v případě Rabinova-Millerova testu bude pravděpodobnost neodhalení neprvočíselnosti pouze $\frac{10}{560} = \frac{1}{56}$.

**Další úlohy**

(1) Rozhodněte, zda je okruh $\mathbf{Z}[i\sqrt{3}]$ Gaussův.
(2) Kolik prostých homomorfismů leží v množině $\mathrm{Hom}(\mathbf{Z}_{7^{10}}, \mathbf{Z}_{7^{20}})$?
(3) Kolik homomorfismů na obsahuje množina $\mathrm{Hom}(\mathbf{Z}_{999}, \mathbf{Z}_{333})$?
(4) Určete řád prvku $4^i$ v grupě $(\mathbf{Z}_{3^{10}}^*, \cdot, ^{-1}, 1)$ pro každé celé $i$.
(5) Najdtěte v grupě $(\mathbf{Z}_{7^3}^*, \cdot, ^{-1}, 1)$ všechny prvky řádu 2,3 a 7.
(6) Najděte generátor cyklické grupy $(\mathbf{Z}_{7^{777}}^*, \cdot, ^{-1}, 1)$.
(7) Najděte v grupě $(\mathbf{Z}_{1323}^*, \cdot, ^{-1}, 1)$ všechny prvky řádu 2, 3, 4, 6, 7 a 9.
(8) Najděte v grupě $(\mathbf{Z}_{1000}^*, \cdot, ^{-1}, 1)$ všechny involuce.
(9) Najděte najmenší přirozené $s$, aby $a^s \equiv 1 (\mathrm{mod}\ 999)$ pro všechna $a \in \mathbf{Z}_{999}^*$.
(10) Najděte v grupě $(\mathbf{Z}_{1000}^*, \cdot, ^{-1}, 1)$ aspoň 3 prvky $a$, pro která $a^{999} = 1$. Kolik takových prvků existuje?
(11) Spočítejte, kolik existuje bází pseudoprvočísla 2465 a najděte nějakou bázi nejvyššího možného řádu.
(12) Rozhodněte, která z čísel 1547 1547, 1729, 2717, 3003 jsou Carmichaelova.
(13) U každého z čísel z předchozí úlohy najděte číslo, které je s ním nesoudělné a není jeho bazí jako silného pseudoprvočísla.