2018/19

Cvičení z algebry

1

Úloha 1.1. Rozhodněte, zda je

(a) množina $\mathbb{Z} \times \mathbb{Z}$ se standardními operacemi $+, -, \cdot$ po složkách,

(b) množina $\mathbb{Z}$ se standardními operacemi $+, -$ a s operací $x \cdot y = 0$,

(c) množina $P(X) = (\{Y : Y \subseteq X\}, \triangle, -, \cap, \emptyset)$ s operacemi symetrické diference $\triangle$, průniku $\cap$ a s odčítáním $-Y = Y$,

(d) $(\mathbb{Q}^+, \cdot, ^{-1}, +, 1)$, kde $\mathbb{Q}^+ = \{a \in \mathbb{Q} : a > 0\}$,

komutativním okruhem s jednotkou, oborem integrity nebo tělesem.

Úloha 1.2. Rozhodněte, zda následující podmnožiny tvoří podokruh tělesa $\mathbb{C}$:

$$\{a + b\sqrt{2} : \ a, b \in \mathbb{Z}\}, \quad \{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Z}\}, \quad \{a + b\zeta : \ a, b \in \mathbb{Z}\},$$
$$\{a + b\omega : \ a, b \in \mathbb{Z}\}, \quad \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : \ a, b, c, d \in \mathbb{Z}\},$$

kde $\zeta = e^{\pi i/4}$ a $\omega = e^{2\pi i/3}$.

Návod: Všimněte si, že $\omega^2 = -1 - \omega$.

Úloha 1.3. Rozhodněte, zda následující podmnožiny tvoří podtěleso tělesa $\mathbb{C}$:

$$\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}, \quad \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b \in \mathbb{Q}\}, \quad \{a + b\omega : \ a, b \in \mathbb{Q}\},$$

kde $\omega = e^{2\pi i/3}$.

Úloha 1.4. Dokažte, že komutativita sčítání plyne z ostatních axiomů komutativních okruhů s jednotkou.

Úloha 1.5. Dokažte pro libovolnou asociativní operaci $*$ na množině A, že hodnota výrazu $a_1 * a_2 * \cdots * a_n$ pro $a_1, \ldots, a_n \in A$ nezáleží na uzávorkování.

Řešení:

1. (a), (c) jsou okruhy, nikoli obory ani tělesa (s výjimkou $|X| = 1$ v (c)),
   (b),(d) nejsou ani okruhy (neexistuje jednotka).

2. $\{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Z}\}$ ani $\{a + b\zeta : \ a, b \in \mathbb{Z}\}$ nejsou podokruhy, ostatní množiny jsou.

3. všechny tři množiny jsou podtělesa tělesa $\mathbb{C}$.

4. Využijeme-li distributivity dostaneme:
   $$(1 + a)(1 + b) = (1 + a)1 + (1 + a)b = 1 + a + b + ab,$$
   $$(1 + b)(1 + a) = (1 + b)1 + (1 + b)a = 1 + b + a + ba,$$
   Díky komutativitě násobení platí, že
   $$1 + a + b + ab = 1 + b + a + ab$$
   a zbývá odečíst prvek 1 zleva a prvek ab zprava.

5. Indukcí podle n dokážeme, že každý výraz s hodnotami $a_1, \ldots, a_n \in A$ je roven výrazu $a_1 * (a_2 * (a_3 * (\cdots * a_n) \ldots))$. Pro $n \leq 3$ to zřejmě platí. Nechť $n > 3$. Máme-li výraz tvaru $a_1 * u$, kde u je výraz délky $n - 1$, pak u je roven požadovanému tvaru podle indukčního předpokladu, a tudíž tvrzení platí. V opačném případě lze výraz napsat ve tvaru $(u * v) * w$, kde u jsou výrazy kratší než n, tedy $u = a_1 * z$ pro vhodný výraz z podle indukčního předpokladu, proto z asociativity plyne
   $$(u * v) * w = u * (v * w) = (a_1 * z) * (v * w) = a_1 * (z * (v * w)).$$
   Závěr nyní dostaneme úvahou z první části důkazu.

2

Úloha 2.1. Uvažujme obor integrity $(R, +, -, \cdot, 0)$ a označme $(Q, +, -, \cdot, \frac{0}{1})$ jeho podílové těleso. Ověřte, že

(a) $\frac{a\cdot x}{b\cdot x} = \frac{a\cdot y}{b\cdot y}$ pro každé $\frac{a}{b} \in Q$ a $x, y \in R \setminus 0$,

(b) jsou operace na podílové tělese dobře definované,

(c) je $(Q, +, -, \cdot, \frac{0}{1})$ opravdu těleso.

Úloha 2.2. Dokažte, že podílové těleso oboru $\mathbb{Z}[i]$ lze ztotožnit s tělesem $\mathbb{Q}[i]$ (nejprve tvrzení přesně zformulujte!).

Úloha 2.3. Ověřte, že operace s polynomy splňují axiomy komutativního okruhu.

Úloha 2.4. Kdybychom symbolem $\frac{a}{b}$ označili nikoli třídu ekvivalence, nýbrž dvojici $(a, b) \in R\times(R\setminus\{0\})$ a kdybychom operace $+, -, \cdot$ zavedli stejně jako u podílových těles, které axiomy oboru integrity by pro $R \times (R \setminus \{0\})$ neplatily?

Řešení:

1. (a) $\frac{a\cdot x}{b\cdot x} = \frac{a\cdot y}{b\cdot y} \Leftrightarrow (a \cdot x, b \cdot x) \sim (a \cdot y, b \cdot y) \Leftrightarrow axby = bxay$, což plyne z komutativity násobení.
   (b) nechť $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ a $\frac{c_1}{d_1} = \frac{c_2}{d_2}$, pak $\frac{a_1}{b_1} \cdot \frac{c_1}{d_1} = \frac{a_1c_1}{b_1d_1} = \frac{a_1c_1b_2d_2}{b_1d_1b_2d_2} = \frac{a_2}{b_2} \cdot \frac{c_2}{d_2}$ a $\frac{a_1}{b_1} + \frac{c_1}{d_1} = \frac{a_1d_1+b_1c_1}{b_1d_1} = = \frac{a_1b_2d_1d_2+b_1b_2d_2c_1}{b_1d_1b_2d_2} = \frac{a_2b_1d_1d_2+b_1b_2d_1c_2}{b_1d_1b_2d_2} = \frac{a_2}{b_2} + \frac{c_2}{d_2}$.
   (c) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}$,
   $\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{adf+b(cf+de)}{bdf} = \frac{(ad+bc)f+bde}{bdf} = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f}$,
   $\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = \frac{a(ce)}{bdf} = \frac{(ac)e}{bdf} = (\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f}$,
   $\frac{a}{b} + \frac{0}{1} = \frac{a\cdot1+b\cdot0}{b} = \frac{a}{b}$, $\frac{a}{b} \cdot \frac{1}{1} = \frac{a\cdot1}{b} = \frac{a}{b}$, $\frac{a}{b} + \frac{-a}{b} = \frac{a+(-a)}{bb} = \frac{0}{bb} = \frac{0}{1}$,
   $\frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} = \frac{acbf+bdae}{bdbf} = \frac{acf+ade}{bdf} = \frac{a}{b} \cdot \frac{cf+de}{df} = \frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f})$.

2. zobrazení, které formálnímu zlomku $\frac{a+bi}{c+di}$, kde $a, b, c, d \in \mathbb{Z}$, $b \neq 0 \neq d$, přiřadí jeho komplexní vyhodnocení $\frac{a+bi}{c+di} = (a + bi)(c - di)c^2 + d^2 \in \mathbb{Q}[i]$ je bijekce převádějící operace + a · v podílovém tělese oboru $\mathbb{Z}[i]$ na operace + a · v tělese $\mathbb{Q}[i]$.

3. Máme-li $p = \sum_n p_n x^n$, $q = \sum_n q_n x^n$, $r = \sum_n r_n x^n \in R[x]$, pak
   $p + q = \sum_n (p_n + q_n)x^n = \sum_n (q_n + p_n)x^n = q + p$,
   $p \cdot q = \sum_n (\sum_{i+j=n} p_i \cdot q_j)x^n = \sum_n (\sum_{i+j=n} q_i \cdot p_j)x^n = p \cdot q$,
   $(p+q)+r = \sum_n ((p_n+q_n)+r_n)x^n = \sum_n (p_n+(q_n+r_n))x^n = p+(q+r)$. $(p\cdot q)\cdot r = \sum_n (\sum_{i+j=n} p_i \cdot q_j)x^n \cdot r = \sum_n (\sum_{i+j+k=n} p_i \cdot q_j \cdot r_k)x^n = p \cdot (q \cdot r)$,
   $p + 0 = p$, $p \cdot 1 = p$, $p + (-p) = 0$,
   $r \cdot (p + q) = r \cdot \sum_n (p_n + q_n)x^n = \sum_n (\sum_{i=0}^n r_i \cdot (p_{n-i} + q_{n-i}))x^n = = \sum_n (\sum_{i=0}^n r_i \cdot p_{n-i})x^n + \sum_n (\sum_{i=0}^n r_i \cdot q_{n-i})x^n = p \cdot r + q \cdot r$,

4. Platily by všechny axiomy kromě axiomu opačného prvku a axiomu distributivity.

3

Úloha 3.1. Vydělte se zbytkem polynomy

(a) $x^4+3x^3+4x^2+x+3 \ : \ x^2+2$ v okruhu $\mathbb{R}[x]$ a $\mathbb{Z}_5[x]$,

(b) $x^4+x^2+x \ : \ x^2+x+1$ v okruhu $\mathbb{Q}[x]$ a okruhu $\mathbb{Z}_2[x]$,

(c) $x^{10}+x^9+x^7+x^5+x^3+x^2+x \ : \ x+1$ v okruhu $\mathbb{Z}_2[x]$,

(d) $x^n-1 \ : \ x^k-1$ v okruhu polynomů nad libovolným oborem.

Úloha 3.2. Určete násobnost kořenu 2 polynomu

(a) $x^5-6x^4+11x^3-2x^2-12x+8$ v okruhu $\mathbb{R}[x]$

(b) $x^5+x^4+4x^3+5x^2+2x+1$ v okruhu $\mathbb{Z}_7[x]$,

(c) $x^5+2x^3+x^2+2$ v okruhu $\mathbb{Z}_3[x]$.

Úloha 3.3. Dokažte, že pro každé dva polynomy f, g nad libovolným oborem platí Leibnitzovo pravidlo $(f\cdot g)' = f'\cdot g + f\cdot g'$.

Úloha 3.4. Uvažujme zobrazení $D : R[x] \to R[x]$, kde R je obor, splňující pro každé $c \in R$ a $f, g \in R[x]$ podmínky $D(c) = 0$, $D(x) = 1$, $D(f+g) = D(f) + D(g)$, $D(f+g) = D(f) + D(g)$ a $D(f\cdot g) = D(f)\cdot g + f\cdot D(g)$. Dokažte postupně pro každé $c \in R$ $n \in \mathbb{N}$, že
(a) $D(c\cdot f) = c\cdot D(f)$, (b) $D(x^n) = n\cdot x^{n-1}$, (c) D je nutně právě derivace.

Úloha 3.5. Dokažte, že jsou-li polynomy f, f' nesoudělné, pak f nemá vícenásobný kořen.

Řešení:

1. (a) $x^4+3x^3+4x^2+x+3 = (x^2+2)(x^2+3x+2)+(-5x-1)$ v $\mathbb{R}[x]$ a
   $x^4+3x^3+4x^2+x+3 = (x^2+2)(x^2+3x+2)+4$ $\mathbb{Z}_5[x]$
   (b) $x^4+x^2+x = (x^2+x+1)(x^2-x+1)+(x-1)$ v $\mathbb{Q}[x]$ a $x^4+x^2+x = (x^2+x+1)(x^2+x+1)+(x+1)$ v $\mathbb{Z}_2[x]$
   (c) $x^{10}+x^9+x^7+x^5+x^3+x^2+x = (x+1)(x^9+x^6+x^5+x^2+1)+1$,
   (d) Vydělíme-li se zbytkem $n = qk+r$, kde $0 \le r < k$, pak
   $x^n-1 = \sum_{i=0}^{q-1} x^{ik+r}\cdot(x^k-1)+(x^r-1)$

2. (a) 3, (b) 3, (c) 4.

3. Stačí si všimnout, že
$$(x^i)'\cdot x^j + x^i\cdot(x^j)' = nx^{i+j-1} + mx^{i+j-1} = (i+j)x^{i+j-1} = (x^{i+j})' = (x^i\cdot x^j)',$$
$$(f\cdot g)' = (\sum_i f_i x^i \sum_j g_j x^j)' = \sum_{i,j} f_i g_j((x^i)'x^j + x^i(x^j)') =$$
$$= (\sum_i f_i x^i)'\cdot\sum_j g_j x^j + \sum_i f_i x^i\cdot(\sum_j g_j x^j)' = f'\cdot g + f\cdot g'$$

4. (a) $D(c\cdot f) = D(c)\cdot f + c\cdot D(f) = 0\cdot f + c\cdot D(f) = c\cdot D(f)$,
   (b) indukcí: $D(x) = 1 = 1x^0$ a pokud $D(x^{n-1}) = (n-1)x^{n-2}$, pak $D(x^n) = D(x\cdot x^{n-1}) = D(x)\cdot x^{n-1} + x\cdot D(x^{n-1}) = x^{n-1} + (n-1)x\cdot x^{n-2} = n\cdot x^{n-1}$,
   (c) $D(\sum_i f_i x^i) = \sum_i f_i D(x^i) = \sum_i f_i i x^{i-1}) = (\sum_i f_i x^i)'$.

5. Má-li f vícenásobný kořen α, pak existuje g, pro kter $f = (x-\alpha)^2 g$, a protože $f' = ((x-\alpha)^2 g)' = 2(x-\alpha)g + (x-\alpha)^2 g'$ je $(x-\alpha)$ společný dělitel f, tudíž f, f' jsou soudělné.

4

Úloha 4.1. Spočítejte největší společný dělitel a příslušné Bézoutovy koeficienty

(a) čísel 539 a 84 v $\mathbb{Z}$,

(b) čísel 256 a 27 v $\mathbb{Z}$,

(c) čísel $2^{92}-1$ a $2^{31}-1$ v $\mathbb{Z}$,

(d) polynomů x^3+x^2+x+1 a x^2+2x+2 v okruhu $\mathbb{Z}_3[x]$ a v okruhu $\mathbb{Z}_5[x]$.

Úloha 4.2. Spočtěte 23^{-1} v tělese $\mathbb{Z}_{37}$ a v okruhu $\mathbb{Z}_{39}$.

Úloha 4.3. Najděte všechna $x \in \mathbb{Z}$ splňující

(a) $5x+3 \equiv 9x+13 \pmod{17}$,

(b) $10x+5 \equiv 7 \pmod{14}$,

(c) $x^2+5x \equiv 0 \pmod{19}$,

(d) $x^2+10x \equiv 11 \pmod{17}$.

Úloha 4.4. Najděte všechna $x, y, z \in \mathbb{Z}$ splňující $x^2+y^2+z^2 = 15w^2$ (návod: řešte nejprve kongruenci modulo 8).

Řešení:

1. (a) $\mathrm{NSD}(539, 84) = 7 = 5 \cdot 539 - 32 \cdot 84$,
   (b) $\mathrm{NSD}(256, 27) = 1 = -2 \cdot 256 + 19 \cdot 27$,
   (c) $\mathrm{NSD}(2^{92}-1, 2^{31}-1) = 1 = (-2)(2^{92}-1) + (1+2^{31}+2^{62})(2^{31}-1)$,
   (d) $\mathrm{NSD}(x^3+x^2+x+1, x^2+2x+2) =$
   $= 2 = (2x+1)(x^3+x^2+x+1) + (x^2+x+2)(x^2+2x+2)$ v $\mathbb{Z}_3[x]$,
   $= x+3 = 1(x^3+x^2+x+1) + (4x+1)(x^2+2x+2)$ v $\mathbb{Z}_5[x]$.
2. $23^{-1} = 29$ v $\mathbb{Z}_{37}$ a $23^{-1} = 17$ v $\mathbb{Z}_{39}$.
3. (a) $x \equiv 6 \pmod{17}$, tj. $x \in \{6+17z |\ z \in \mathbb{Z}\}$,
   (b) $x \equiv 3 \pmod{7}$, tj. $x \in \{3+7z |\ z \in \mathbb{Z}\}$,
   (c) $x \in \{19z |\ z \in \mathbb{Z}\} \cup \{14+19z |\ z \in \mathbb{Z}\}$,
   (d) $x \in \{1+17z |\ z \in \mathbb{Z}\} \cup \{6+17z |\ z \in \mathbb{Z}\}$,
4. nutná podmínka: $x^2+y^2+z^2+w^2 \equiv 0 \pmod{8}$ a $a^2 \equiv 1 \pmod{8}$ pro a liché $a^2 \equiv 0$ nebo $4 \pmod{8}$ pro a sudé $\Rightarrow x, y, z, w$ sudé. Nyní vytkneme ze všech neznámých číslo 2 a vykrátíme číslem 4 a řešíme stejnou rovnici $\Rightarrow x = y = z = w = 0$.

5

Úloha 5.1. Spočtěte (a) $3^{3^{3^{3^3}}}$ modulo 28 a (b) $100^{99^{98}}$ modulo 39 a modulo 40.

Úloha 5.2. Najděte všechna $x, y \in \mathbb{Z}$ splňující $x^6 + x + xy \equiv 1 \pmod 7$.

Úloha 5.3. Najděte všechna $x \in \mathbb{Z}$, pro která platí
(a) $x \equiv 5 \pmod 7$, $x \equiv 4 \pmod 8$, $x \equiv 2 \pmod 9$,
(b) $10x \equiv 6 \pmod{32}$ a $3x \equiv 1 \pmod 5$.

Úloha 5.4. Najděte všechna $x \in \mathbb{Z}$ splňující
(a) $x^2 \equiv 36 \pmod{45}$ (b) $x^2 \equiv -1 \pmod{65}$.

Úloha 5.5. Dokažte vzoreček $\varphi(\prod_{i=1}^{k} p_i^{r_i}) = \prod_{i=1}^{k} \varphi(p_i^{r_i}) = \prod_{i=1}^{k}(p_i - 1)p_i^{r_i - 1}$ pro Eulerovu funkci, kde $p_1 < p_2 < \cdots < p_k$ jsou prvočísla.

Řešení:

1. (a) $3^{3^{3^{3^3}}} \equiv 27 \pmod{28}$,
   (b) $100^{99^{98}} \equiv 1 \pmod{39}$, $100^{99^{98}} \equiv 0 \pmod{40}$
2. $x \not\equiv 0 \pmod 7, y \equiv -1 \pmod 7$.
3. (a) $x \equiv 236 \pmod{504}$, (b) $x \equiv 7 \pmod{80}$.
4. (a) $x \equiv \pm 6 \pmod{15}$, tj. $x \in \{\pm 6 + 15k |\ k \in \mathbb{Z}\}$,
   (b) $x \equiv \pm 8 \pmod{65}$ nebo $x \equiv \pm 18 \pmod{65}$.

6

Úloha 6.1. Srovnejte obory inkluzí a popište všechny jejich prvky
(a) $\mathbb{Z}[\sqrt{6}]$, $\mathbb{Z}[\sqrt{24}]$ a $\mathbb{Z}[\sqrt{2},\sqrt{3}]$,
(b) $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{24}]$ a $\mathbb{Q}[\sqrt{2},\sqrt{3}]$,
(c) $\mathbb{Q}[\sqrt[3]{s}]$ a $\mathbb{Q}(\sqrt[3]{s})$ pro libovolné $s \in \mathbb{N}$.

Úloha 6.2. Najděte celočíselný polynom stupně 4, jehož kořenem je číslo $\sqrt{2}+\sqrt{3}$ a dokažte, že $\mathbb{Z}[\sqrt{2}+\sqrt{3}] =$

$$= \{p(\sqrt{2}+\sqrt{3}) |\ p \in \mathbb{Z}[x], \deg p \leq 3\} = \{a+b\sqrt{2}+(b+2c)\sqrt{3}+2d\sqrt{6} |\ a,b,c,d \in \mathbb{Z}\}.$$

Úloha 6.3. Rozhodněte, zda platí rovnosti
(a) $\mathbb{Z}[\sqrt{2},\sqrt{3}] = \mathbb{Z}[\sqrt{2}+\sqrt{3}]$, (b) $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$.

Úloha 6.4. Dokažte, že algoritmus dělení se zbytkem v oboru $\mathbb{Z}[i]$ pracuje správně, tj. pokud pro $u, v \in \mathbb{Z}[i] \setminus 0$ najdeme $a, b \in \mathbb{Q}$, pro která $\frac{u}{v} = a + bi$, a položíme $q = [a] + [b]i \in \mathbb{Z}[i]$ a $z = v - qu$, pak $\nu(z) < \nu(v)$.

Řešení:

1. (a) $\mathbb{Z}[\sqrt{6}] = \{a+b\sqrt{6} |\ a,b \in \mathbb{Z}\}$, $\mathbb{Z}[\sqrt{24}] = \{a+2b\sqrt{6} |\ a,b \in \mathbb{Z}\}$, $\mathbb{Z}[\sqrt{2},\sqrt{3}] = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} |\ a,b,c,d \in \mathbb{Z}\}$,
   $\mathbb{Z}[\sqrt{24}] \subsetneq \mathbb{Z}[\sqrt{6}] \subsetneq \mathbb{Z}[\sqrt{2},\sqrt{3}]$,
   (b) $\mathbb{Q}[\sqrt{6}] = \mathbb{Q}[\sqrt{24}] = \{a+b\sqrt{6} |\ a,b \in \mathbb{Q}\} \subsetneq \mathbb{Q}[\sqrt{2},\sqrt{3}] =$
   $= \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} |\ a,b,c,d \in \mathbb{Q}\}$
   (c) $\mathbb{Q}[\sqrt[3]{s}] = \mathbb{Q}(\sqrt[3]{s}) = \{a+b\sqrt[3]{s}+c\sqrt[3]{s^2} |\ a,b,c \in \mathbb{Q}\}$
2. $x^4 - 10x^2 + 1 \Rightarrow \mathbb{Z}[\sqrt{2}+\sqrt{3}] = \{p(\sqrt{2}+\sqrt{3}) |\ p \in \mathbb{Z}[x], \deg p \leq 3\}$,
   $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$, $(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}$
   $\Rightarrow \mathbb{Z}[\sqrt{2}+\sqrt{3}] \subseteq \{a+b\sqrt{2}+(b+2c)\sqrt{3}+2d\sqrt{6} |\ a,b,c,d \in \mathbb{Z}\}$,
   $2c\sqrt{3} = 11c(\sqrt{2}+\sqrt{3}) - c(11\sqrt{2}+9\sqrt{3}) \in \mathbb{Z}[\sqrt{2}+\sqrt{3}], b(\sqrt{2}+\sqrt{3}) \in \mathbb{Z}[\sqrt{2}+\sqrt{3}] \Rightarrow b\sqrt{2}+(b+2c)\sqrt{3} \in \mathbb{Z}[\sqrt{2}+\sqrt{3}]$,
   $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6} \in \mathbb{Z}[\sqrt{2}+\sqrt{3}] \Rightarrow 2d\sqrt{6} \in \mathbb{Z}[\sqrt{2}+\sqrt{3}]$
   $\Rightarrow \{a+b\sqrt{2}+(b+2c)\sqrt{3}+2d\sqrt{6} |\ a,b,c,d \in \mathbb{Z}\} \subseteq \mathbb{Z}[\sqrt{2}+\sqrt{3}]$.
3. (a) ne, (b) ano.
4. $\frac{\|r\|^2}{\|v\|^2} = \|\frac{r}{v}\|^2 = \|\frac{u-qv}{v}\|^2 = \|\frac{u}{v} - q\|^2 = (a-[a])^2 + (b-[b])^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2}$
   $\Rightarrow \nu(r) = \|r\|^2 \leq \frac{1}{2}\|v\|^2 = \nu(v) \Rightarrow \nu(r) < \nu(v)$.

7

Úloha 7.1. Vydělte v oboru $\mathbb{Z}[i]$ se zbytkem
(a) $(5+7i) : (3-i)$, (b) $(3+2i) : (1-2i)$, (c) $(3+2i) : (1+i)$.

Úloha 7.2. Spočítejte v $\mathbb{Z}[i]$ (pomocí Eukleidova algoritmu nebo normy)
(a) $\mathrm{NSD}(5+7i, 3-i)$, (b) $\mathrm{NSD}(6-7i, 7+i)$, (c) $\mathrm{NSD}(8+5i, 4+i)$.

Úloha 7.3. Dokažte pro prvočíslo p, že
(a) je prvočinitelem v oboru $\mathbb{Z}[i]$, právě když $p \equiv 3 \pmod 4$,
(b) je-li $p \equiv 1 \pmod 4$, pak existují prvočinitele $a+bi, a-bi \in \mathbb{Z}[i]$, pro které $p = (a+bi)(a-bi)$.
(Návod: dokažte a využijte tvrzení $(p-1)! \equiv -1 \pmod p$)

Úloha 7.4. Určete v oboru $\mathbb{Z}[i]$ rozklad čísel $3, 5, 6, 7, 20, 21, 101, 157$ na prvočintele.

Řešení:

1. (a) $(5+7i) = (1+3i) \cdot (3-i) - 1 - i$,
   (b) $(3+2i) = 2i \cdot (1-2i) - 1$
   (c) $(3+2i) = 2 \cdot (1+i) + 1 = 3 \cdot (1+i) - i = (2-i) \cdot (1+i) + i = (3-i) \cdot (1+i) - 1$

2. (a) $1+i$, (b) $2+i$, (c) 1

3. Pokud $p = (a+bi)(a-bi) = a^2 + b^2$, pak je právě jedno z čísel, například a liché, proto $p \equiv 1 \pmod 4$. Protože $\nu(p) = p^2$, je prvočíslo součinem nejvýše dvou prvočinitelů (s normou p), proto pokud $p \equiv 3 \pmod 4$, je p prvočinitel.

   Jestliže $p \equiv 1 \pmod 4$, pak je $\frac{p-1}{2}$ sudé a proto

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

   tedy existuje c splňující $p/c^2 + 1 = (c+i)(c-i)$. Hledané $a+bi$ je $\mathrm{NSD}(p, c+i)$ v $\mathbb{Z}[i]$.

4. 3, $5 = (2+i)(2-i)$, $6 = (1+i)(1-i) \cdot 3$, 7, $20 = (1+i)^2(1-i)^2(2+i)(2-i)$, $21 = 3 \cdot 7$, $101 = (10+i)(10-i)$, $157 = (11+6i)(11-6i)$

8

Úloha 8.1. Spočítejte ireducibilní rozklady
(a) $10-6i$, $9+3i$ a $11+2i$ v oboru $\mathbb{Z}[i]$,
(b) x^3-2 a x^4-x^2-2 v oborech $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}_3[x], \mathbb{Z}_5[x]$.

Úloha 8.2. Popište všechny ireducibilní polynomy (a) v $\mathbb{C}[x]$, (b) v $\mathbb{R}[x]$.

Úloha 8.3. Určete v $\mathbb{Z}[i\sqrt{2}]$ ireducibilní rozklady $3-i\sqrt{2}, 1-2i\sqrt{2}, 2, 3, 5-i\sqrt{2}$.

Úloha 8.4. Dokažte, že správnost obdoby algoritmu dělení se zbytkem v oborech $\mathbb{Z}[\sqrt{s}]$ pro $s=-2,2,3$. Proč totéž nemůže fungovat pro $s=-3,5$?

Řešení:

1. (a) $10-6i=-(1+i)^3\cdot(4+i)$, $9+3i=3\cdot(1+i)\cdot(2-i)$ a $11+2i=-(1+2i)^3$,
   (b) $x^3-2=(x-\sqrt[3]{2})(x-\sqrt[3]{2}e^{\frac{2\pi i}{3}})(x+\sqrt[3]{2}e^{\frac{2\pi i}{3}})$ v $\mathbb{C}[x]$,
   $x^3-2=(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$ v $\mathbb{R}[x]$ x^3-2 je ireducibilní v $\mathbb{Q}[x]$,
   $x^3-2=x^3+1=(x+1)^3$ v $\mathbb{Z}_3[x]$ a $x^3-2=(x+2)(x^2+3x+4)$ v $\mathbb{Z}_5[x]$.
   $x^4-x^2-2=(x^2+1)(x^2-2)=(x+i)(x-i)(x+\sqrt{2})(x-\sqrt{2})$ v $\mathbb{C}[x]$,
   $x^4-x^2-2=(x^2+1)(x+\sqrt{2})(x-\sqrt{2})$ v $\mathbb{R}[x]$,
   $x^4-x^2-2=(x^2+1)(x^2-2)$ v $\mathbb{Q}[x]$,
   $x^4-x^2-2=(x^2+1)^2$ v $\mathbb{Z}_3[x]$,
   $x^4-x^2-2=(x+2)(x-2)(x^2-2)$ v $\mathbb{Z}_5[x]$.
2. (a) nenulové komplexní násobky $x+a$ (b) nenulové reálné násobky $x+a$ a $(x-b)(x-\overline{b})=x^2-Re(b)+|b|^2$ pro $b\in\mathbb{C}\setminus\mathbb{R}$.
3. $3-i\sqrt{2}$ je ireducibilní, $1-2i\sqrt{2}=-(1+i\sqrt{2})^2$, $2=-(i\sqrt{2})^2$,
   $3=(1+i\sqrt{2})(1-i\sqrt{2})$, $5-i\sqrt{2}=-(1+i\sqrt{2})^3$.

9

Úloha 9.1. Pro každé $a, b \in \mathbb{Z}$ dokažte, že $\mathrm{NSD}(a,b)\mathbb{Z}$ je vzhledem k inkluzi nejmenší ideál okruhu celých čísel $\mathbb{Z}$ obsahující ideály $a\mathbb{Z}$ i $b\mathbb{Z}$ a že $\mathrm{NSN}(a,b)\mathbb{Z}$ je největší ideál okruhu $\mathbb{Z}$ obsažený v ideálech $a\mathbb{Z}$ i $b\mathbb{Z}$. Platí obdobné tvrzení v každém eukleidovském oboru?

Úloha 9.2. Nechť I a J jsou ideály nějakého komutativního okruhu. Dokažte, že $I + J := \{i + j |\ i \in I, j \in J\}$ je nejmenší ideál obsahující I i J a že $I \cap J$ je největší ideál obsažený I i J (vzhledem k uspořádání inkluzí). Kdy je ideálem $I \cup J$?

Úloha 9.3. Nechť $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ je posloupnost ideálů nějakého komutativního okruhu. Dokažte, že $I = \bigcup_n I_n$ je opět ideál. Kdy je I hlavní?

Úloha 9.4. Najděte v okruhu $\mathbb{Z}$ generátory hlavních ideálů:
(a) $15\mathbb{Z} + 24\mathbb{Z}$, (b) $15\mathbb{Z} \cap 24\mathbb{Z}$, (c)$(100\mathbb{Z} + 60\mathbb{Z} + 16\mathbb{Z}) \cap 21\mathbb{Z} \cap 9\mathbb{Z}$.

Úloha 9.5. Ověřte, že (a) $2\mathbb{Z}[x] + x\mathbb{Z}[x]$ v oboru $\mathbb{Z}[x]$, (b) $x\mathbb{Q}[x,y] + y\mathbb{Q}[x,y]$ v oboru $\mathbb{Q}[x,y]$ nejsou hlavní ideály.

Řešení:

1. Nejprve si v $x/y \Leftrightarrow y\mathbb{Z} \subseteq x\mathbb{Z}$. Je-li $c := \mathrm{NSD}(a,b)$ a $d\mathbb{Z}$ ideál obsahující $a\mathbb{Z} \cup b\mathbb{Z}$ ($\mathbb{Z}$ je obor hlavních ideálů), pak $d/a, b$, a protože je d největší společný dělitel, dostáváme, že d/c, a proto $c\mathbb{Z} \subseteq d\mathbb{Z}$.

   Duálně, jestliže $g := \mathrm{NSN}(a,b)$ a $h\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$, pak $a, b/g$, a protože je h nejmenší společný násobek, dostáváme, že g/h a $h\mathbb{Z} \subseteq g\mathbb{Z}$.

   Úvaha projde v jakémkoli Eukleidovském oboru (dokonce i v OIHI).

2. Využijeme charakterizaci, že M je ideál komutativního okruhu $R \Leftrightarrow \forall a, b \in M, \forall r, s \in R : ar + bs \in M$.

   Pokud $i+j, \widetilde{i}+\widetilde{j} \in I+J$ pro $i, \widetilde{i} \in I$ a $j, \widetilde{j} \in J$ a , $r, s \in R$ pak $(i+j)r+(\widetilde{i}+\widetilde{j})s = (ir+\widetilde{i}s)+(jr+\widetilde{j}s) \in I+J$. Pro každý ideál M obsahující I a J navíc platí, že $\forall i \in I, j \in J : i+j \in M$, tedy $I+J \subseteq M$.

   Pokud $a, b \in I \cap J \subseteq I, J$ a $r, s \in R$, potom $ar + bs \in I$ i $ar + bs \in J$, tudíž $ar + bs \in I \cap J$. pak $(i + j)r + (\widetilde{i} + \widetilde{j})s = (ir + \widetilde{i}s) + (jr + \widetilde{j}s) \in I + J$. Množina $I \cup J$ je zjevně největší obsažená jak v I, tak v J.

   $I + J$ je ideál $\Leftrightarrow I \subseteq J$ nebo $J \subseteq I$.

3. Nechť $a, b \in I$ a $r, s \in R$, pak existuje takové n, že $\forall k \geq n\ a, b \in I_n$, a tedy $ar + bs \in I_k \subseteq I$.

   I je hlavní $\Leftrightarrow I \subseteq J$ nebo $J \subseteq I$ existuje takové n, že $\forall k \geq n\ I_k = I_n = I$ je hlavní ideál.

4. (a) $3\mathbb{Z}$, (b) $120\mathbb{Z}$, (c)$252\mathbb{Z}$

5. Sporem:

   (a) případný generátor hlavního ideálu by byl společný dělitel 2 a x v oboru $\mathbb{Z}[x]$, tedy 1 nebo -1, ovšem $\pm 1 \notin \mathbb{Z}[x] + x\mathbb{Z}[x]$

   (b) případný generátor hlavního ideálu by byl společný dělitel x a y v oboru $\mathbb{Q}[x]$, tedy nenulový konstantní polynom $q \in \mathbb{Q} \setminus \{0\}$, ovšem $q \notin x\mathbb{Q}[x,y] + y\mathbb{Q}[x,y]$.

10

Úloha 10.1. Pro $\alpha, \beta \in \mathbb{C}$ označme $I = \{p(x,y) \in \mathbb{C}[x,y] |\ p(\alpha,\beta) = 0\}$.
(a) Ověřte, že je I ideál oboru $\mathbb{C}[x,y]$,
(b) dokažte, že $I = (x-\alpha)\mathbb{C}[x,y] + (y-\beta)\mathbb{C}[x,y]$,
(c) rozhodněte, zda je I hlavní.

Úloha 10.2. Pro $p(y) \in \mathbb{C}[y]$ a $h(x,y) \in \mathbb{C}[x,y]$ dokažte, že
(a) $(x - p(y))|h(x,y)$ v $\mathbb{C}[x,y] \Leftrightarrow h(p(y),y) = 0$,
(b) $x - p(y)$ je ireducibilní v $\mathbb{C}[x,y]$.

Úloha 10.3. Určete v oborech $\mathbb{Z}[x,y]$, $\mathbb{R}[x,y]$, $\mathbb{C}[x,y]$ ireducibilní rozklad polynomů
(a) $x^2 - y + 2$, (b) $2x^2 - 4y^2$, (c) $x^2 + y^2$.

Řešení:

1. (a) Nechť $p, q \in I$ a $a, b \in I\mathbb{C}[x,y]$, pak $[ap + bq](\alpha,\beta) = a(\alpha,\beta)p(\alpha,\beta) + b(\alpha,\beta)q(\alpha,\beta) = a(\alpha,\beta) \cdot 0 + b(\alpha,\beta) \cdot 0 = 0$,

   (b) $(x-\alpha), (y-\beta) \in I \Rightarrow (x-\alpha)\mathbb{C}[x,y] + (y-\beta)\mathbb{C}[x,y] \subseteq I$.

   Využijem dělení se zbytkem v $(\mathbb{C}[x])[y]$ polynomem $y-\beta$ a v $\mathbb{C}[x]$ polynomem $x-\alpha$. Nechť $h \in I$, pak

   $\exists q \in (\mathbb{C}[x])[y]$ a $r \in (\mathbb{C}[x])[y]$: $h = q(y-\beta) + r$, $\deg_y r < 1 \Rightarrow r \in \mathbb{C}[x]$,

   $\exists s \in \mathbb{C}[x]$ a $c \in \mathbb{C}[x]$: $r = s(x-\alpha) + c$, $\deg_x c < 1 \Rightarrow r \in \mathbb{C}$.

   Nyní $h = q(y-\beta) + s(x-\alpha) + c$, a protože $0 = h(\alpha,\beta) = c$, dostáváme $h \in (x-\alpha)\mathbb{C}[x,y] + (y-\beta)\mathbb{C}[x,y]$.

   (c) Kdyby $p\mathbb{C}[x,y] = I$, pak by $(x-\alpha)|p$ a $(y-\alpha)|p \Rightarrow p \in \mathbb{C}^*$, tedy $I = \mathbb{C}[x,y]$, což je spor.

2. (a) Dosazení $R := \mathbb{C}[y]$ a $\alpha := p(y)$ do Tvrzení 10.1 ze skript.

   (b) Je-li $a \cdot b = x - p(y)$, pak BÚNO $b \in \mathbb{C}[y]$ a existují $c, d \in \mathbb{C}[y]$ $a = cx + d \Rightarrow x - p(y) = bcx + bd$ $\Rightarrow b \in \mathbb{C}^*$.

3. (a) $x^2 - y + 2$ je ireducibilní dle 2(b) v $\mathbb{C}[x,y]$ a tedy i v $\mathbb{Z}[x,y]$, $\mathbb{R}[x,y]$,

   (b) $2x^2 - 4y^2 = 2 \cdot (x^2 - 2y^2)$ v $\mathbb{Z}[x,y]$ a $2x^2 - 4y^2 = (2x - 2\sqrt{2}y)(x + \sqrt{2}y)$ v $\mathbb{R}[x,y]$ a $\mathbb{C}[x,y]$.

   (c) $x^2 + y^2$ je ireducibilní v $\mathbb{Z}[x,y]$, $\mathbb{R}[x,y]$ a $x^2 + y^2 = (x + iy)(x - iy)$ v $\mathbb{C}[x,y]$.

11

Úloha 11.1. Určete v $\mathbb{Z}[x,y]$, $\mathbb{R}[x,y]$, $\mathbb{C}[x,y]$ ireducibilní rozklad polynomů
(a) x^2-2y^2,
(b) x^2-y^3,
(c) $x^2+xy+y-1$,
(d) $2y^3+y^2x+yx^2+x^2+7y^2+7y-x-2$.

Úloha 11.2. Buď $f \in R[x]$ a $a \in R$. Dokažte, že je polynom f ireducibilní v $\mathbf{R}[x]$ právě tehdy, když je polynom $f(x+a)$ ireducibilní v $\mathbf{R}[x]$.

Úloha 11.3. Dokažte pomocí Eisensteinova kriteria a předchozího tvrzení ireducibilitu polynomů v $\mathbb{Z}[x]$:
(a) $x^6+10x^5-4x^3+8x^2-2$,
(b) x^6+x^3+1,
(c) $x^{p-1}+x^{p-2}+\ldots+x+1=\frac{x^p-1}{x-1}$ pro každé prvočíslo p.

Úloha 11.4. Napište všechny racionální kořeny polynomu $2x^4+x^3-x^2+3x+3$.

Řešení:

1. (a) x^2-2y^2 je ireducibilní v $\mathbb{Z}[x,y]$, $x^2+y^2=(x+\sqrt{2}y)(x-\sqrt{2}y)$ v $\mathbb{R}[x,y]$ a $\mathbb{C}[x,y]$.
   (b) x^2-y^3 je ireducibilní v $\mathbb{C}[x,y]$ a tedy i v $\mathbb{Z}[x,y]$, $\mathbb{R}[x,y]$,
   (c) $x^2+xy+y-1=(x+1)(x+y-1)$,
   (d) $2y^3+y^2x+yx^2+x^2+7y^2+3y-x-2=$
   $$\begin{aligned}&=(y+1)x^2+(y^2-1)x+(2y^3+7y^2+3y-2)\\&=(y+1)(x^2+(y-1)x+(2y^2+5y-2))\\&=(y+1)(x-y-2)(x+2y+1)\end{aligned}$$

2. Stačí dokázat $f(x+a)$ je ireducibilní $\Rightarrow$ $f(x)$ je ireducibilní, obrácenou implikaci dostaneme použitím tvrzení pro $g(x):=f(x+a)$ a $g(x+(-a))$.
   Dokazujeme nepřímo: nechť $f(x)=g(x)h(x)$ pro nekonstantní g a h, pak $f(x+a)=g(x+a)h(x+a)$.

3. (a) plyne přímo z Eisensteinova kriteria,
   (b) použijeme Eisensteinovo kriterium pro $(x+1)^6+(x+1)^3+1=x^6+6x^5+15x^4+21x^3+18x^2+9x+3$ a prvočíslo 3,
   (c) použijeme Eisensteinovo kriterium pro $\frac{(x+1)^p-1}{(x+1)-1}$ prvočíslo p,

4. -1.

12

Úloha 12.1. Najděte všechny polynomy $f \in \mathbb{Q}[x]$ stupně < 4 splňující
(a) $f(0) = 1$, $f(1) = 0$, $f(2) = 2$,
(b) $f \equiv x + 1 \pmod{x^2 + 1}$ a $f(0) = 3$,
(c) $f \equiv 1 \pmod{x^2 - 1}$ a $f \equiv x + 1 \pmod{x^2 + 1}$.

Úloha 12.2. V tělese $\mathbb{F}_{125} = \{a_0 + a_1\alpha + a_2\alpha^2 |\ a_i \in \mathbb{Z}_5\}$ s počítáním modulo $\alpha^3 + \alpha + 1$ v $\mathbb{Z}_5[\alpha]$ spočtěte
(a) $(3\alpha^2 + 4\alpha + 1) + (2\alpha^2 + 4)$,
(b) $(3\alpha^2 + 4\alpha + 1) \cdot (2\alpha^2 + 4)$,
(c) α^{-1}, $(\alpha^2)^{-1}$, $(\alpha^2 + 1)^{-1}$,
(d) řešení lineární rovnice $\alpha \cdot x + (\alpha + 1) = \alpha^2$.

Úloha 12.3. V tělese $\mathbb{F}_4 = \{a_0 + a_1\alpha |\ a_i \in \mathbb{Z}_2\}$ s počítáním modulo $\alpha^2 + \alpha + 1$ v $\mathbb{Z}_2[\alpha]$ spočtěte řešení soustavy lineárních rovnic zadané maticí

$$\left(\begin{array}{cc|c} \alpha & 1 & \alpha + 1 \\ \alpha + 1 & \alpha + 1 & \alpha \end{array}\right)$$

Úloha 12.4. Najděte v tělese $\mathbb{F}_9 = \{a_0 + a_1\alpha |\ a_i \in \mathbb{Z}_3\}$ s počítáním modulo $\alpha^2 + 1$ v $\mathbb{Z}_3[\alpha]$ prvek u s vlastností, že každý prvek $v \in \mathbb{F}_9 \setminus \{0\}$ lze napsat jako mocnina u a Najděte ireducibilní rozklad polynomů $x^8 - 1$ v $\mathbb{F}_9[x]$.

Řešení:

1. (a) $\frac{3}{2}x^2 - \frac{5}{2}x + 1 + cx(x-1)(x-2)$ pro libovolné $c \in \mathbb{Q}$,
   (b) $2x^2 + x + 3 + bx(x^2 + 1)$ pro libovolné $b \in \mathbb{Q}$,
   (c) $-\frac{1}{2}x^3 + \frac{1}{2}x + 1$
2. (a) $(3\alpha^2 + 4\alpha + 1) + (2\alpha^2 + 4) = 4\alpha$,
   (b) $(3\alpha^2 + 4\alpha + 1) \cdot (2\alpha^2 + 4) = 3\alpha^2 + 2\alpha + 1$,
   (c) $\alpha^{-1} = 4\alpha^2 + 4$, $(\alpha^2)^{-1} = \alpha^2 + 4\alpha + 1$, $(\alpha^2 + 1)^{-1} = 4\alpha$,
   (d) $x = \alpha^2 + \alpha$
3. $(0, \alpha + 1)^T$
4. Například $\alpha + 1$, $x^8 - 1 = \prod_{\gamma \in \mathbb{F}_9 \setminus \{0\}} (x - \gamma)$.

13

Úloha 13.1. Je polynom $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$ symetrický?

Úloha 13.2. Dokažte, že druhá mocnina determinantu Vandermondovy matice

$$V(x_1, \ldots, x_n) = (x_i^{j-1})_{i,j=1,\ldots,n}$$

je symetrický polynom vzhledem k proměnným $x_1, \ldots, x_n$.

Úloha 13.3. Vyjádřete symetrické polynomy

$$\text{(a) } 3x^2yz + 3xy^2z + 3xyz^2, \quad \text{(b) } x^3(y+z) + y^3(x+z) + z^3(x+y)$$

jako součet součinů elementárních symetrických polynomů.

Úloha 13.4. Uvažujme monický polynom $f = \sum a_i x^i \in R[x]$, který se v R rozkládá na lineární činitele $(x-u_1)\cdot\ldots\cdot(x-u_n)$. Vyjádřete součet čtverců jeho kořenů $u_1^2+\ldots+u_n^2$ pomocí koeficientů $a_0, \ldots, a_{n-1}$.

Řešení:

1. Ano.
2. $\det V(x_1, \ldots, x_n)^2 = \prod_{i>j}(x_i - x_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(x_i - x_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(x_\sigma(i) - x_\sigma(i))^2$ pro všechna $\sigma \in S_n$.
3. (a) $3x^2yz + 3xy^2z + 3xyz^2 = 3s_1s_3$,
   (b) $x^3(y+z) + y^3(x+z) + z^3(x+y) = s_1^2s_2 - 2s_2^2 - s_1s_3$.
4. $u_1^2 + \ldots + u_n^2 = a_{n-1}^2 - 2a_{n-2}$.

14 *To nejlepší z celého semestru*

Úloha 14.1. Najděte všechna $x \in \mathbb{Z}$, pro která platí $x \equiv 5 \pmod 7$, $x \equiv 4 \pmod 8$, $x \equiv 2 \pmod 9$.

Úloha 14.2. Spočítejte ireducibilní rozklad prvku $9 + 3i$ v oboru $\mathbb{Z}[i]$.

Úloha 14.3. Najděte v okruhu $\mathbb{Z}$ generátor hlavního ideálu $(100\mathbb{Z} + 60\mathbb{Z} + 16\mathbb{Z}) \cap 21\mathbb{Z} \cap 9\mathbb{Z}$.

Úloha 14.4. Dokažte (pomocí Eisensteinova kriteria) ireducibilitu polynomu $x^6 + x^3 + 1$ v oboru $\mathbb{Z}[x]$.

Úloha 14.5. Uvažujme monický polynom $f = \sum a_i x^i \in R[x]$, který se v R rozkládá na lineární činitele $(x-u_1)\cdot\ldots\cdot(x-u_n)$. Vyjádřete součet čtverců jeho kořenů $u_1^2+\ldots+u_n^2$ pomocí koeficientů $a_0, \ldots, a_{n-1}$.

Úloha 14.6. Najděte všechna $x, y, z \in \mathbb{Z}$ splňující $x^2+y^2+z^2 = 15w^2$ (návod: řešte nejprve kongruenci modulo 8).

Řešení:

1. $x \equiv 236 \pmod{504}$, , tj. $x \in \{236 + 504k |\ k \in \mathbb{Z}\}$.
2. $9 + 3i = 3 \cdot (1 + i) \cdot (2 - i)$
3. $252\mathbb{Z}$.
4. Použijeme Eisensteinovo kriterium pro $(x+1)^6+(x+1)^3+1 = x^6+6x^5+15x^4+21x^3+18x^2+9x+3$ a prvočíslo 3.
5. $u_1^2 + \ldots + u_n^2 = a_{n-1}^2 - 2a_{n-2}$.
6. nutná podmínka: $x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod 8$ a $a^2 \equiv 1 \pmod 8$ pro a liché $a^2 \equiv 0$ nebo $4 \pmod 8$ pro a sudé $\Rightarrow x, y, z, w$ sudé. Nyní vytkneme ze všech neznámých číslo 2 a vykrátíme číslem 4 a řešíme stejnou rovnici $\Rightarrow x = y = z = w = 0$

□