1. cvičení

Připomeňme rozšířený Eukleidův algoritmus hledání největšího společného dělitele čísel a a b:

`VSTUP:` $a, b \in \mathbb{N}$, $a \geq b$
`VÝSTUP:` $\mathrm{NSD}(a,b), x, y \in \mathbb{Z}$, `pro které` $\mathrm{NSD}(a,b) = x \cdot a + y \cdot b$

`0.` $i := 1$, $(a_0, a_1) := (a, b)$; $(x_0, x_1) := (1, 0)$; $(y_0, y_1) := (0, 1)$;

`1.` `while`$(a_i > 0)$ `do`
$\{a_{i+1} := (a_{i-1}) \mathrm{mod}\ a_i$; $q_i := (a_{i-1}) \mathrm{div}\ a_i$; %`tj.` $a_{i-1} = q_i a_i + a_{i+1}$
$x_{i+1} := x_{i-1} - x_i \cdot q_i$; $y_{i+1} := y_{i-1} - y_i \cdot q_i$; $i := i + 1;\}$

`2.` `return` $a_{i-1}, x_{i-1}, y_{i-1}$.

1. Spočítejte největší společný dělitel a příslušné Bézoutovy koeficienty v celých číslech

(a) čísel 539 a 84,

(b) čísel 256 a 27,

(c) čísel $2^{92} - 1$ a $2^{31} - 1$.

2. Spočtěte 23^{-1} v tělese $\mathbb{Z}_{37}$.

3. Dokažte pro hodnoty běhu Eukleidova algoritmu, že

(a) $\mathrm{NSD}(a_{i-1}, a_i) = \mathrm{NSD}(a_i, a_{i+1})$,

(b) $a_i = x_i \cdot a + y_i \cdot b$,

(c) $\mathrm{NSD}(a, b) = x \cdot a + y \cdot b$.

Řešení:

1. (a) $\text{NSD}(539, 84) = 7 = 5 \cdot 539 - 32 \cdot 84$,

   (b) $\text{NSD}(256, 27) = 1 = -2 \cdot 256 + 19 \cdot 27$,

   (c) $\text{NSD}(2^{92} - 1, 2^{31} - 1) = 1 = (-2)(2^{92} - 1) + (1 + 2^{31} + 2^{62})(2^{31} - 1)$.

2. Spočítáme Bezoutův koeficient $y = -8$ ve vztahu

$$37x + 23y = \text{NSD}(37, 23) = 1$$

   , potom $23^{-1} = (-8) \text{mod } 37 = 29$.

3. (a) Při využití vztahů $a_{i-1} = a_{i+1} + q_i \cdot a_i$ a $a_{i+1} = a_{i-1} - q_i \cdot a_i$ uvážíme, že

$$c/a_{i-1}, a_i \Rightarrow c/a_{i+1} = a_{i-1} - q_i \cdot a_i,$$

$$d/a_i, a_{i+1} \Rightarrow d/a_{i-1} = a_{i-1} + q_i \cdot a_i.$$

   (b) Dokážeme indukcí: Tvrzení platí pro $i = 0$ a $i = 1$ a předpokládejme, že tvrzení platí pro i a $i - 1$, tedy $a_i = x_i \cdot a_0 + y_i \cdot a_1$ a $a_{i-1} = x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1$. Dokážeme rovnost pro $i + 1$ dosazením za a_i a a_{i-1} do vztahu:

$$a_{i+1} = a_{i-1} - a_i \cdot q_i = (x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1) - (x_i \cdot a_0 + y_i \cdot a_1) \cdot q_i =$$

$$= (x_{i-1} - x_i \cdot q_i) \cdot a_0 + (y_{i-1} - y_i \cdot q_i) \cdot a_1 = x_{i+1} \cdot a_0 + y_{i+1} \cdot a_1.$$

   (c) Plyne z (a) a (b).

2. cvičení

Ve škole:

1. Popište všechny invertibilní prvky okruhu $\mathbb{Z}_n$ s operacemi modulo n a rozhodněte, pro která n je $\mathbb{Z}_n$ obor integrity a pro která je těleso. Najděte v $\mathbb{Z}_{100}$ inverz k prvku 77.

2. Dokažte, že je konečný obor nutně těleso.

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

$$\{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}, \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}, \{a+b\sqrt[3]{2} \mid a,b \in \mathbb{Z}\}, \{a+b\omega \mid a,b \in \mathbb{Z}\},$$

$$\{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,b,c \in \mathbb{Q}\}, \quad \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d \in \mathbb{Z}\},$$

kde $\omega = e^{2\pi i/3}$. Které z podokruhů tvoří tělesa? (Všimněte si, že $\omega^2 = -1-\omega$.)

4. Popište nejmenší podokruh s jednotkou maticového okruhu $M_2(\mathbb{Z})$, který obsahuje prvek $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Tvoří tento podokruh komutativní okruh?

Úloha pro samostatné počítání:

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

Řešení:

1. Invertibilní jsou právě prvky nesoudělné s n. $77^{-1} = 13$.

   $\mathbb{Z}_n$ je obor integrity $\Leftrightarrow$ je těleso $\Leftrightarrow$ je n prvočíslo.

2. Nechť R je konečný obor. Uvážíme pro každý nenulový prvek $a \in R$ zobrazení $\tau_a : R \to R$ dan0 vyta $\tau(r) = a \cdot r$. Jestliže $\tau(r) = \tau(s)$, pak $a \cdot (r - s) = 0$, a proto $r = s$. Tedy τ_a je prosté zobrazení konečné množiny do sebe, a tudíž i zobrazení na. Tudíž $a^{-1} = \tau_a^{-1}(1)$.

3. $\{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Z}\}$ není podokruh, ostatní množiny jsou, z toho $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b \in \mathbb{Q}\}$ a $\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$ tvoří tělesa

4. $\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} | \ | \ a, b \in \mathbb{Z}\}$, tento podokruh tvoří komutativní okruh.

5. $\{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Z}\}$ není podokruh, ostatní množiny jsou, z toho $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b \in \mathbb{Q}\}$ a $\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$ tvoří tělesa

6. $\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} | \ | \ a, b \in \mathbb{Z}\}$, tento podokruh tvoří komutativní okruh.

7. 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.

3. cvičení

Ve škole:

1. Ověřte, že polynomy s reálnými koeficienty $\mathbb{R}[x]$ chápané jako reálné funkce tvoří s obvyklými operacemi $+$, $-$, $\cdot$ a konstantami 0 a 1 obor integrity a polynomy s racionálními koeficienty $\mathbb{Q}[x]$ a s celočíselnými koeficienty $\mathbb{Z}[x]$ jsou jeho podobory. Určete prvokruh a charakteristiku všech oborů.

2. Je-li $\mathbb{Q}[\pi]$ nejmenší podokruh tělesa $\mathbb{R}$ obsahující $\mathbb{Q} \cup \{\pi\}$, dokažte, že jsou okruhy $\mathbb{Q}[\pi]$ a $\mathbb{Q}[x]$ izomorfní. (Využijte faktu, že π není kořenem žádného nenulového racionálního polynomu).

3. Dokažte, že žádné dva z okruhů $\mathbb{Q}$, $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$ nejsou izomorfní.

Úloha pro samostatné počítání:

4. Uvažujme podokruhy

$$R_1 := \mathbb{Z}[i] \leq \mathbb{C},$$

$$R_2 := \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}\} \leq M_2(\mathbb{Q}),$$

$$R_3 := \{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}\} \leq M_2(\mathbb{Q})$$

. Rozhodněte, které dvojice okruhů R_i a R_j jsou izomorfní.

Řešení:

1. Protože je sčítání i násobení v $\mathbb{R}$ komutativní a asociativní a sčítání je vzhledem k násobení v $\mathbb{R}$ distributivní, mají stejné vlastnosti tyto operace definované po složkách na množině reálných funkcí, tedy i na polynomech. Navíc platí $p + 0 = p$, $p + (-p) = 0$ a $p \cdot 1 = p$ pro každý polynom p. Protože je součet i součin reálných polynomů a opačný polynom k reálnému polynomu opět reálný polynom, jedná se o dobře definované okruhové operace. Z matematické analýzy víme, že součin dvou nenulových polynomů je nenulový, $\mathbb{R}[x]$ je tedy obor.

   Je-li $p = \sum_n p_n x^n, q = \sum_n q_n x^n \in \mathbb{Q}[x](\mathbb{Z}[x])$, pak

$$p + q = \sum_n (p_n + q_n) x^n \in \mathbb{Q}[x](\mathbb{Z}[x]),$$

$$p \cdot q = \sum_n (\sum_{i=0}^{n} p_i \cdot q_{n-i}) x^n \in \mathbb{Q}[x](\mathbb{Z}[x]),$$

$$-p = \sum_n -p_n x^n \mathbb{Q}[x](\mathbb{Z}[x]).$$

   Protože $0, 1 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ tvoří $\mathbb{Q}[x]$ i $\mathbb{Z}[x]$ podobory. Prvookruhem všech těchto oborů je $\mathbb{Z}$ a jedná se tudíž o okruh charakteristiky 0.

2. Stačí uvážit dosazení $\Omega_\pi : p \to p(\pi)$. Snadno nahlédneme, že jde o zobrazení a $\mathbb{Q}[x]$ na $\mathbb{Q}[\pi]$. Pokud $p(\pi) = q(\pi)$, pak je π kořenem polynomu $p - q$, proto $p = q$ a zobrazení Ω_π je i prosté. Přímočaře ukážeme, že $(p + q)(\pi) = p(\pi) + q(\pi)$, $(p \cdot q)(\pi) = p(\pi) \cdot q(\pi)$ a $\Omega_\pi(1) = 1$.

3. Ke sporu předpokádejme, že existuje izomorfismus $\varphi : \mathbb{Q}[i] \to \mathbb{Q}$. Pak

$$-1 = \varphi(-1) = \varphi(i \cdot i) = \varphi(i) \cdot \varphi(i),$$

   tedy v $\mathbb{Q}$ máme prvek $a = \varphi(i)$ splňující podmínku $a^2 = -1$, spor. Ze stejného důvodu neexistuje izomorfismus $\mathbb{Q}[i] \to \mathbb{Q}[\sqrt{2}]$ (ani do žádného jiného podokruhu tělesa $\mathbb{R}$).

   Nechť existuje izomorfismus $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}$, pak

$$2 = \varphi(2) = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(\sqrt{2}) \cdot \varphi(\sqrt{2})$$

   a $\mathbb{Q}$ by tak muselo obsahovat $\sqrt{2}$, což je opět spor.

4. $a + bi \to \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ určuje izomorfismus R_1 a R_2.

   R_3 není izomorfní ani R_1 ani R_2, neboť $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, tedy R_3 není obor zatímco R_1 a R_2 obory jsou. Izomorfismus by musel netriviální dělitele nuly zobrazit opět na netriviální dělitele nuly.

4. cvičení

Ve škole:

Algoritmus dělení se zbytkem polynomů:
`VSTUP:` $a, b = \sum b_n x^n \in R[x]$, `kde` R `je obor a` $b_{\deg b}$ `invertibilní`
`VÝSTUP:` $q,\ r \in R[x]$, `pro které` $a = q \cdot b + r,\ \deg r < \deg b$
`0.` $m := \deg b$; $n := \deg a - m$;
`1. if` $n < 0$ `then return` $0, a$ `else` $r := a$;
`2. for` $i := n$ `downto` 0 `do` $\{q_i := r_{i+m} b_m^{-1}; r := r - q_i x^i b;\}$
`3. return` $\sum_i q_i x^i,\ r$.

1. Vydělte se zbytkem polynomy

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

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

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

Eukleidův algoritmus pro nalezemí největšího společného dělitele (tj. společného dělitele nejvyššího stupně) polynomů nad tělesem T a Bézoutových koeficientů:
`VSTUP:` $a_0,\ a_1 \in T[x] \setminus \{0\}$
`VÝSTUP:` $\mathrm{NSD}(a_0, a_1)$, u, v, `pro které` $u_n \cdot a_0 + v_n \cdot a_1 = \mathrm{NSD}(a_0, a_1)$
`0.` $(u_0, v_1) := (1, 0)$; $(u_0, v_1) := (0, 1)$; $i := 1$
`1. while` $a_i \neq 0$ `do` $\{$`zvol` $a_{i+1}, q_i \in T[x]$ `taková, že`
$a_{i-1} = a_i \cdot q_i + a_{i+1}$ `a` $\deg(a_{i+1}) < \deg(a_i)$;
$u_{i+1} := u_{i-1} - u_i \cdot q_i;\ v_{i+1} := v_{i-1} - v_i \cdot q_i;\ i := i + 1\}$
`2. return` $a_{i-1}, u_{i-1}, v_{i-1}$.

2. Spočítejte největší společný dělitel a příslušné Bézoutovy koeficienty pro polynomy

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

(b) $x^3 - x^2 - x - 2$ a $x^3 - 2x^2 + 3x - 6$ v okruhu $\mathbb{Q}[x]$.

Úlohy pro samostatné počítání:

3. Dokažte, že algoritmus dělení se zbytkem polynomů pracuje správně a nalezené polynomy $q,\ r$ jsou jediné, které splňují podmínky $a = q \cdot b + r$ a $\deg r < \deg b$.

4. Dokažte s využitím úvah o Eukleidově algoritmu nad celými čísly z prvního cvičení správnost Eukleidova algoritmus pro polynomy.

Řešení:

1. (a) $x^4+3x^3+4x^2+x+3 = (x^2+2)(x^2+3x+2)+(-5x-1)$ v $\mathbb{Z}[x]$,
   $x^4+3x^3+4x^2+x+3 = (x^2+2)(x^2+3x+2)+4$ $\mathbb{Z}_5[x]$.
   (b) $x^4+x^2+x = (x^2+x+1)(x^2-x+1)+(x-1)$ v $\mathbb{Z}[x]$,
   $x^4+x^2+x = (x^2+x+1)(x^2+x+1)+(x+1)$ v $\mathbb{Z}_2[x]$.
   (c) $x^{10}+x^9+x^7+x^5+x^3+x^2+x = (x+1)(x^9+x^6+x^5+x^2+1)+1$.

2. (a) $\mathrm{NSD}(x^3+x^2+x+1, x^2+2x+2) =$
   $= 2 = (2x+1)(x^3+x^2+x+1)+(x^2+x+2)(x^2+2x+2)$ v $\mathbb{Z}_3[x]$,
   $= x+3 = 1(x^3+x^2+x+1)+(4x+1)(x^2+2x+2)$ v $\mathbb{Z}_5[x]$.
   (b) $\mathrm{NSD}(x^3-x^2-x-2, x^3-2x^2+3x-6) =$
   $= 7x-14 = (-x-2)(x^3-x^2-x-2)+(x+3)(x^3-2x^2+3x-6)$.

3. Protože $\deg(r-q_ix^ib) < i+m$ pro každé i ve for-cyklu, platí, že má zbytek menší stupeň než m. Indukcí podle i nahlédneme, že $a = q\cdot b+r$, tedy algoritmus pracuje správně.

   Zbývá ukázat jednoznačnost. Předpokládejme, že $a = b\cdot q'+r'$ a $\deg r' < \deg b$. Potom $b\cdot(q-q') = r'-r$ a protože $\deg(r'-r) < \deg b$, dostáváme $r'-r = 0$, a proto i $q-q' = 0$

4. Algoritmus skončí, protože v každém kroku snížíme stupeň zbytku. Zbylá argumentace je obdobná jako v 3.úloze prvního cvičení.

5. cvičení

Ve škole:

1. Nechť p a q jsou dva nenulové polynomy nad tělesem T. Dokažte tvrzení:

(a) Jestliže p dělí q a zároveň q dělí p, pak existuje nenulový prvek v tělesa T, pro který $p = vq$.

(b) Největší společný dělitel p a q je určen jednoznačně až na násobek nenulovým prvkem tělesa.

2. Uvažujme obor integrity $(R, +, \cdot, -, 0, 1)$ a označme $(Q, +, \cdot, -, \frac{0}{1}, \frac{1}{1})$ 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 podílovém tělese dobře definované.

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

Úlohy pro samostatné počítání:

4. Dokažte, že je podílové těleso $(Q, +, \cdot, -, \frac{0}{1}, \frac{1}{1})$ opravdu těleso.

5. 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) Protože p dělí q existuje polynom u, pro který $q = up$, a podobně protože q dělí p existuje polynom v, pro který $p = vq$. Dosadíme-li do druhého vztahu za q dostáváme $p = vup$, proto $p(1 - vu) = 0$ a tudíž $1 - vu = 0$, neboť $T[x]$ je obor. Protože $1 = vu$, musí být u i v nutně polynomy stupně nula, tedy $u, v \in T^*$.

   (b) Nechť a je nějaký největší společný dělitel p a q a b je největší společný dělitel p a q získaný Eukleidovým algoritmem. Protože $b = up + vq$, kde u a v jsou Bézoutovy koeficienty, musí a dělit b, tedy $b = ua$ pro vhodný polynom u. Protože z definice jsou polynomy a a b z definice stejného stupně, musí být u nutně stupně nula, tedy $u \in T \setminus \{0\}$.

2. (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 $\frac{a_1}{b_1} \cdot \frac{c_1}{d_1} = \frac{a_1 c_1}{b_1 d_1} = \frac{a_1 c_1 b_2 d_2}{b_1 d_1 b_2 d_2} = \frac{a_2}{b_2} \cdot \frac{c_2}{d_2}$ a $\frac{a_1}{b_1} + \frac{c_1}{d_1} = \frac{a_1 d_1 + b_1 c_1}{b_1 d_1} = = \frac{a_1 b_2 d_1 d_2 + b_1 b_2 d_2 c_1}{b_1 d_1 b_2 d_2} = \frac{a_2 b_1 d_1 d_2 + b_1 b_2 d_1 c_2}{b_1 d_1 b_2 d_2} = \frac{a_2}{b_2} + \frac{c_2}{d_2}$.

3. 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

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2} i \in \mathbb{Q}[i] \subseteq \mathbb{C}$$

   je izomorfismus podílového tělesa oboru $\mathbb{Z}[i]$ a tělesa $\mathbb{Q}[i]$.

4. $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}$,
   $\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{adf + b(cf+de)}{bdf} = \frac{(ad+bc)f + bde}{bdf} = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f}$,
   $\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = \frac{a(ce)}{bdf} = \frac{(ac)e}{bdf} = (\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f}$,
   $\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b} = \frac{a}{b}$, $\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b} = \frac{a}{b}$, $\frac{a}{b} + \frac{-a}{b} = \frac{a+(-a)}{bb} = \frac{0}{bb} = \frac{0}{1}$,
   $\frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} = \frac{acbf + bdae}{bdbf} = \frac{acf + ade}{bdf} = \frac{a}{b} \cdot \frac{cf+de}{df} = \frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f})$.

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

6. cvičení

Ve škole:

1. Určete násobnost kořenu 2 polynomu

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

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

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

2. Najděte všechny kořeny polynomu $x^2 + x \in \mathbb{Z}_6[x]$ v okruhu $\mathbb{Z}_6$ a napište všechny jeho rozklady na součin kořenových činitelů.

3. Najděte všechna taková $a, b \in \mathbb{R}$, pro která má reálný polynom $x^4 - ax^3 + b$ násobný kořen (tj. aspoň dvojnásobný).

Úlohy pro samostatné počítání:

4. Najděte polynom s racionálními koeficienty stupně 4, jehož kořenem je číslo $\sqrt{2} + \sqrt{3}$

5. Nechť f je polynom kladného stupně nad oborem integrity. Dokažte, že jsou-li polynomy f, f' nesoudělné, pak f nemá žádný násobný kořen.

Řešení:

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

2. Kořenem jsou prvky $0, 2, 3, 5$,
   $x^2 + x = x(x+1) = (x+4)(x+3)$.

3. $(a, b) \in \{(a, 0) \mid a \in \mathbb{R}\} \cup \{(a, \frac{27}{256}a^4) \mid a \in \mathbb{R}\}$.

4. $(\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6}$ a $(\sqrt{2}+\sqrt{3})^4 = (5+2\sqrt{6})^2 = 49 + 20\sqrt{6}$, proto $(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 = -1$, tudíž $\sqrt{2}+\sqrt{3}$ je kořeneme polynomu $x^4 - 10x^2 + 1$.

5. Má-li f násobný kořen α, pak existuje g, pro který $f = (x-\alpha)^2 g$, 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.

7. cvičení

Ve škole:

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

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

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

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

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

3. Spočtěte (a) $3^{3^{3^{3^3}}}$ modulo 28, (b) $14^{14^{14}} + 15^{15^{15}} + 16^{16^{16}}$ modulo 17.

4. Dokažte, že
(a) 13 dělí $23^{32} + 29^{33} + 36^{34}$,
(b) 11 dělí $n^{33} + 5n^{21} + 3n^{13} + 7n^3 + 6n$ pro všechna celá n.

Úlohy pro samostatné počítání:

5. Spočítejte poslední dvě cifry čísla $81^{83^{85}}$

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. (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) $x \in \{19z |\ z \in \mathbb{Z}\} \cup \{14 + 19z |\ z \in \mathbb{Z}\}$,

2. $x \not\equiv 0 \pmod{7}, y \equiv -1 \pmod{7}$.

3. Budeme využívat Eulerovu větu.
   (a) $3^{3^{3^{3^3}}} \equiv 3^{(3^{3^{3^3}})\bmod 12} \equiv 3^{3\cdot(3^{3^{3^3}}-1)\bmod 4} \equiv 3^{3\cdot((-1)^{3^{3^3}}-1)\bmod 4} \equiv 3^3 \equiv 27 \pmod{28}$,
   (b) $14^{14^{14}}+15^{15^{15}}+16^{16^{16}} \equiv (-3)^{14^{14}\bmod 16}+(-2)^{15^{15}\bmod 16}+(-1)^{16^{16}\bmod 16} \equiv (-3)^0 + (-2)^{(-1)^{15}\bmod 16} + (-1)^0 \equiv 1 - (2)^{15} + (-1)^0 \equiv 1 - 9 + 1 \equiv 10 \pmod{17}$, protože $2^{15} = 2^{-1} = 9$ v tělese $\mathbb{Z}_{17}$.

4. (a) $23^{32} + 29^{33} + 36^{34} \equiv (-3)^{(32)\bmod 12} + 3^{(33)\bmod 12} + (-3)^{(34)\bmod 12} \equiv 3^8 + 3^9 + 3^{10} \equiv 3^8(1 + 3 + 9) \equiv 0 \pmod{13}$,
   (b) je-li n násobek 11, pak není co dokazovat, v opačném případě jsou n a 11 besoudělná a opět využijeme Eulerovu větu: $n^{33} + 5n^{21} + 3n^{13} + 7n^3 + 6n \equiv n^3 + 5n + 3n^3 + 7n^3 + 6n \equiv 11n^3 + 11n^1 \equiv 0 \pmod{11}$.

5. $81^{83^{85}} \equiv (-19)^{(83^{85})\bmod 40} \equiv (-19)^{(3^{(85)\bmod 16})\bmod 40} \equiv (-19)^3 \equiv 41 \pmod{100}$.

6. Nutná podmínka: $x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{8}$. Protože pro každé a liché $a^2 \equiv 1 \pmod{8}$ a pro a sudé $a^2 \equiv 0$ nebo $4 \pmod{8}$, musí být nutně x, y, z, w sudé. Nyní vytkneme ze všech neznámých číslo 2 a vykrátíme číslem 4 a řešíme stejnou kongruenci. Odtud plyne, že x, y, z, w jsou násobkem 2^n pro všechna přirozená n, proto $x = y = z = w = 0$.

8. cvičení

Ve škole:

1. 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) $2x + 1 \equiv 2 \pmod 3$, $3x + 2 \equiv 3 \pmod 4$, $4x + 3 \equiv 2 \pmod 5$,
(c) $10x \equiv 6 \pmod{32}$ a $3x \equiv 1 \pmod 5$,
(d) $x^{11} \equiv 2 \pmod 5$ a $x^8 \equiv 1 \pmod 7$.

2. Spočítejte všechna $x \in \mathbb{Z}$ splňující
(a) $x^2 \equiv 1 \pmod 3$ a $x^2 \equiv 1 \pmod 7$,
(b) $x^2 \equiv -1 \pmod{65}$,
(c) $x^2 \equiv 36 \pmod{45}$.

3. Najděte všechny kořeny polynomů
(a) $x^2 - 1$ nad $\mathbb{Z}_{21}$, (b) $x^2 + 1$ nad $\mathbb{Z}_{65}$, (c) $x^2 + 3x + 2$ nad $\mathbb{Z}_{14}$.

Úloha pro samostatné počítání:

4. Nechť jsou p a q dvě různá lichá prvočísla.
(a) Dokažte, že má polynom $x^3 + 3x^2 + 2x$ v okruhu $\mathbb{Z}_{pq}$ právě 9 kořenů.
(b) Rozhodněte, zda existují $a, b \in \mathbb{Z}_{pq}$, aby měl polynom $x^2 + ax + b$ v okruhu $\mathbb{Z}_{pq}$ právě 3 kořeny.

Řešení:

1. Počítáme pomocí dosazovacího (Garnerova) algoritmu na výpočet vzorů Čínské věty o zbytcích:

   (a) $x \equiv 236 \pmod{504}$, (b) $x \equiv 11 \pmod{60}$, (c) $x \equiv 7 \pmod{80}$.

   (d) Všimneme si, že pro $5/x$ nebo $7/x$ kongruence splněny nejsou. Za předpokladu, že 5 ani 7 nedělí x ekvivalentně upravíme kongruence pomocí Eulerovy věty na

   $$1 \equiv 2x \pmod{5}, \quad x^2 \equiv 1 \pmod{7},$$

   druhá z kongruencí je díky kořenovým vlastnostem polynomu $x^2 - 1$ ekvivalentní podmínce $x \equiv \pm 1 \pmod{7}$, odtud už stejným postupem jako v (a)-(c) dostaneme, že $x \equiv 8 \pmod{35}$ nebo $x \equiv 13 \pmod{35}$.

2. (a) $x \in \{\pm 1 + 21k |\ k \in \mathbb{Z}\} \cup \{8 + 21k |\ k \in \mathbb{Z}\} \cup \{13 + 21k |\ k \in \mathbb{Z}\}$

   (b) $x \equiv \pm 8 \pmod{65}$ nebo $x \equiv \pm 18 \pmod{65}$,

   (c) $x \equiv \pm 6 \pmod{15}$, tj. $x \in \{\pm 6 + 15k |\ k \in \mathbb{Z}\}$.

3. Využijeme opět Čínskou větu o zbytcích. Polynomiální rovnice pro (a) a (b) jsme vyřešili už v předchozí úloze.

   (a) $x^2 - 1$ má kořeny $1, 8, 13, 20$,

   (b) $x^2 + 1$ má kořeny $8, 18, 47, 57$,

   (c) $x^2 + 3x + 2 = (x + 1)(x + 2)$ má kořeny $5, 6, 12, 13$.

4. (a) Označme $F_p : \mathbb{Z}_{pq} \to \mathbb{Z}_p$ $F_q : \mathbb{Z}_{pq} \to \mathbb{Z}_q$ zobrazení daná předpisem

   $$F_p(a) = (a) \text{mod } p, \quad F_q(a) = (a) \text{mod } q$$

   a nechť $f = x^3 + 3x^2 + 2x = x(x + 1)(x + 2)$. Pak je podle Čínské věty o zbytcích zobrazení $a \to (F_p(a), F_q(a))$ bijekce množin $\mathbb{Z}_{pq}$ a $\mathbb{Z}_p \times \mathbb{Z}_q$, navíc $a \in \mathbb{Z}_{pq}$ je kořenem polynomu f nad okruhem $\mathbb{Z}_{pq}$, právě když je $F_p(a)$ kořenem polynomu f nad tělesem $\mathbb{Z}_p$ a zároveň je $F_q(a)$ kořenem polynomu f nad tělesem $\mathbb{Z}_q$. Protože má f nad tělesem $\mathbb{Z}_p$ i nad tělesem nad tělesem $\mathbb{Z}_q$ právě 3 kořeny a každá dvojice těchto kořenů odpovídá právě jednomu kořenu nad $\mathbb{Z}_{pq}$, má f nad okruhem $\mathbb{Z}_{pq}$ právě $3 \cdot 3 = 9$ kořenů.

   (b) Ne. Podle předchozí úvahy by musel mít polynom $x^2 + ax + b$ nad tělesem $\mathbb{Z}_p$ nebo $\mathbb{Z}_q$ právě 3 kořeny (a nad druhým tělesem nutně právě jeden), což pro polynom stupně dva nad žádným tělesem není možné.

9. cvičení

Ve škole:

1. Najděte všechny polynomy $f \in \mathbb{R}[x]$, pro které platí:
(a) $f(0) = 2$, $f(1) = 1$, $f(-1) = 3$,
(b) $f(0) = 2$, $f(1) = 1$, $f(-1) = 3$, $f(2) = 6$,
(c) $f(0) = 1$, $f(1) = 2$, $f(-1) = 3$,
(d) $f(0) = 1$, $f(1) = 2$, $f(-1) = 3$, $f(2) = 6$,

2. Najděte všechny polynomy $f \in \mathbb{Z}_3[x]$, pro které platí:
(a) $f \equiv x + 2 \pmod{x^2 + 1}$ a $f \equiv 1 \pmod{x^2 + x + 1}$,
(b) $f \equiv 2 \pmod{x^2 + 1}$ a $f \equiv 2x \pmod{x^2 + x + 1}$.

3. Ověřte, že je $\mathbb{Z}_3[\alpha]/(\alpha^2 + 1)$ těleso a spočítejte
(a) α^{-1}, (b) $(\alpha + 1)^{-1}$, (c) $2\alpha \cdot (2\alpha + 1)$, (d) $\alpha^{-1} \cdot (\alpha + 2)$.

4. Zkonstruujte šestnáctiprvkové těleso.

Úlohy pro samostatné počítání:

5. Dokažte, že existuje izomorfismus mezi okruhy $\mathbb{Z}_5[x]/(x^4 - 1)$ a $\mathbb{Z}_5^4$.

6. Ověřte, že je $\mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$ těleso a najděte v něm všechny kořeny polynomu $x^7 + 1$.

Řešení:

1. (a) Například pomocí Lagrangeova interpolačního polynomu dostaneme $-x+2 = 2 \cdot \frac{(x+1)(x-1)}{-1} + 1 \cdot \frac{x(x+1)}{2} + 3 \cdot \frac{x(x-1)}{2}$, proto $f \in \{-x+2+g(x^3-x) \mid g \in \mathbb{R}[x]\}$.

   (b) Řešíme kongruence $f \equiv -x+2 \pmod{x^3-x}$, $f \equiv 6 \pmod{x-2}$, proto

   $f \in \{x^3-2x+2+g(x^3-x)(x-2) \mid g \in \mathbb{R}[x]\}$.

   (c) $\frac{3}{2}x^2 - \frac{1}{2}x + 1 = 1 \cdot \frac{(x+1)(x-1)}{-1} + 2 \cdot \frac{x(x+1)}{2} + 3 \cdot \frac{x(x-1)}{2}$, proto

   $f \equiv \frac{3}{2}x^2 - \frac{1}{2}x + 1 \pmod{x^3-x}$.

   (d) $f \equiv \frac{3}{2}x^2 - \frac{1}{2}x + 1 \pmod{(x^3-x)(x-2)}$.

2. Postupujeme obdobně jako při řešení kongruencí v $\mathbb{Z}$:

   (a) $f \equiv 2x^3+2 \pmod{(x^2+x+1)(x^2+1)}$, tj.

   $f \in \{2x^3+2+g(x^2+x+1)(x^2+1) \mid g \in \mathbb{Z}_3[x]\}$.

   (b) $f \equiv x^3+2x^2+x+1 \pmod{(x^2+x+1)(x^2+1)}$, tj.

   $f \in \{x^3+2x^2+x+1+g(x^2+x+1)(x^2+1) \mid g \in \mathbb{Z}_3[x]\}$.

3. Protože polynom x^2+1 nemá v $\mathbb{Z}_3$ kořen, není součinem kořenových činitelů (tedy polynomů stupně 1), a proto je ireducibilní. Tudíž je podle pozorování z přednášky okruh $\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ těleso.

   (a) Řešíme kongruenci $\alpha f \equiv 1 \pmod{\alpha^2+1}$ (všimněme si, že $\alpha^2 \equiv -1 \pmod{\alpha^2+1}$) a dostáváme $\alpha^{-1} = 2\alpha$,

   (b) $(\alpha+1)^{-1} = \alpha+2$, (c) $2\alpha \cdot (2\alpha+1) = 2\alpha+2$, (d) $\alpha^{-1} \cdot (\alpha+2) = \alpha+1$.

4. Stačí najít ireducubilní polynom stupně 4 nad tělesem $\mathbb{Z}_2$, takový polynom nesmí mít kořen 0 ani 1, což znamená, že má absolutní člen 1 a lichý počet členů a dále nemůže být součinem dvou ireducibilních polynomů stupně 2. Protože jediný ireducibilní polynom stupně 2 nad tělesem $\mathbb{Z}_2$ je polynom x^2+x+1 a $(x^2+x+1)^2 = x^4+x^2+1$ je ireducibilní například polynom x^4+x+1. Tudíž $\mathbb{Z}_2[x]/(x^4+x+1)$ je šestnáctiprvkové těleso.

5. Definujeme-li $\varphi(g) = (g(1), g(2), g(3), g(4))$ pro každé $g \in \mathbb{Z}_5[x]/(x^4-1)$ a všimneme-li si, že $x^4-1 = (x-1)(x-2)(x-3)(x-4)$, je zobrazení $\varphi : \mathbb{Z}_5[x]/(x^4-1) \to \mathbb{Z}_5^4$ podle Čínské věty o zbytcích izomorfismus.

6. Protože polynom x^3+x+1 nemá v $\mathbb{Z}_2$ kořen, není násobkem kořenového činitele, tedy součinem tedy polynomu stupně 1 a 2. Proto je ireducibilní a okruh $T = \mathbb{Z}_2[\alpha]/(\alpha^3+\alpha+1)$ je tělesem. Kořenem x^7+1 jsou všechny nenulové prvky tělesa T (ověření je bez dalších znalostí teorie poněkud pracné), tedy $x^7+1 = \prod_{t \in T \setminus \{0\}} (x-t)$.

10. cvičení

Ve škole:

1. Dokažte, že algoritmus dělení se zbytkem v oboru $\mathbb{Z}[i]$, který pro $u, v \in \mathbb{Z}[i] \setminus 0$ nejprve najde $a, b \in \mathbb{Q}$ splňující $\frac{u}{v} = a + bi$ a na výstupu předloží hodnoty $q = [a] + [b]i \in \mathbb{Z}[i]$ a $z = u - qv$, splňuje podmínku $\nu(z) < \nu(v)$.

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

3. Dokažte, že je prvočíslo p splňující $p \equiv 3 \pmod 4$ ireducibilním prvkem oboru $\mathbb{Z}[i]$.

4. Spočítejte v oboru $\mathbb{Z}[i]$ ireducibilní rozklady 3, 5, 6, 7, $10 - 6i$, $9 + 3i$,

Úlohy pro samostatné počítání:

5. Spočítejte v oborech $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}_3[x], \mathbb{Z}_5[x]$ ireducibilní rozklady polynomů (a) $x^3 - 2$ a (b) $x^4 - x^2 - 2$.

6. Dokažte, že v oborech $\mathbb{Z}[\sqrt{s}]$ pro $s = -2, 2, 3$ funguje obdoba algoritmu dělení se zbytkem z 1.úlohy. Proč totéž nemůže fungovat pro $s = -3, 5$?

Řešení:

1. $\frac{\|z\|^2}{\|v\|^2} = \|\frac{z}{v}\|^2 = \|\frac{u-qv}{v}\|^2 = \|\frac{u}{v} - q\|^2 = (a-[a])^2 + (b-[b])^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2}$
   $\Rightarrow \nu(z) = \|z\|^2 \leq \frac{1}{2}\|v\|^2 = \frac{1}{2}\nu(v) \Rightarrow \nu(z) < \nu(v)$.

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

   (b) $(3+2i) = 2i\cdot(1-2i) - 1$

   (c) $(3+2i) = 2\cdot(1+i) + 1 = 3\cdot(1+i) - i = (2-i)\cdot(1+i) + i = (3-i)\cdot(1+i) - 1$

3. Je-li p liché prvočíslo, které není ireducibilní v $\mathbb{Z}[i]$, pak lze napsat jako součin $p = (a-bi)(c+di)$ pro $a+bi, c+di \in \mathbb{Z}[i]$, které nejsou invertibilní, tedy $\nu(a-bi) \neq 1 \neq \nu(c+di)$. Protože $p^2 = \nu(p) = \nu(a-bi)\nu(c+di) = (a^2+b^2)(c^2+d^2)$, platí, že $p = a^2+b^2 = c^2+d^2$, a tudíž $a = c$ a $b = d$. Protože je p liché, je právě jedno z čísel a, b liché, tedy existují celá k, l, pro něž $p = (2k)^2 + (2l+1)^2 \equiv 1 \pmod 4$.

   To znamená, že pokud $p \equiv 3 \pmod 4$, je p ireducibilní.

4. 3, $5 = (2+i)(2-i)$, $6 = (1+i)(1-i)\cdot 3$, 7, $10-6i = -(1+i)^3\cdot(4+i)$, $9+3i = 3\cdot(1+i)\cdot(2-i)$,

5. (a) $x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}e^{\frac{2\pi i}{3}})(x + \sqrt[3]{2}e^{\frac{2\pi i}{3}})$ 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 $\mathbb{Z}_5[x]$.
   (b) $x^4 - x^2 - 2 = (x+i)(x-i)(x+\sqrt{2})(x-\sqrt{2})$ 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 $\mathbb{Z}_5[x]$.

6. Obdobným výpočtem zjistíme, že $\nu(r) \leq \frac{3}{4}\nu(v), \frac{1}{2}\nu(v), \frac{3}{4}\nu(v)$, a proto $\nu(r) < \nu(v)$ pro čísla $s = -2, 2, 3$.

   Pro $s = -3, 5$ podobný odhad provést nelze.

11. cvičení

Ve škole:

1. Spočítejte ireducibilní rozklady:
(a) 17, $11 + 2i$ v $\mathbb{Z}[i]$,
(b) $x^4 - 4$ v $\mathbb{Z}[x], \mathbb{R}[x], \mathbb{C}[x]$,
(c) $3 - i\sqrt{2}, 1 - 2i\sqrt{2}, 2$ v $\mathbb{Z}[i\sqrt{2}]$

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

3. Najděte v $\mathbb{Z}[i]$ NSD$(6 - 7i, 7 + i)$ a příslušné Bezoutovy koeficienty.

4. V oboru $\mathbb{Z}[i\sqrt{5}]$ dokažte, že neexistuje žádný prvek s normou 2 ani 3, a určete nějaký ireducibilní rozklad prvku 6. Jedná se o rozklad na prvočinitele?

Úlohy pro samostatné počítání:

5. Najděte všechna celočíselná řešení rovnice $35x + 8y = 7$.

Řešení:

1. (a) $17 = 1 + 4^2 = (1 + 4i)(1 - 4i)$, $11 + 2i = -(1 + 2i)^3$,
   (b) $x^4 - 4 = (x^2 - 2)(x^2 + 2)$ v $\mathbb{Z}[x]$,
   $x^4 - 4 = (x + \sqrt{2})(x - \sqrt{2})(x^2 + 2)$ v $\mathbb{R}[x]$,
   $x^4 - 4 = (x + \sqrt{2})(x - \sqrt{2})(x + i\sqrt{2})(x - i\sqrt{2})$ v $\mathbb{C}[x]$
   (c) $3 - i\sqrt{2}$ je ireducibilní, $1 - 2i\sqrt{2} = -(1 + i\sqrt{2})^2$, $2 = -(i\sqrt{2})^2$.

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

3. $\mathrm{NSD}(6 - 7i, 7 + i) = -2 - i = (6 - 7i) + (-1 + i)(7 + i)$.

4. Kdyby $\nu(a + bi\sqrt{5}) = a^2 + 5b^2 = 2, 3$, pak by $b = 0$ a tedy 2 či 3 by byla druhá mocnina, což neplatí.

   Například $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ jsou ireducibilní rozklady, kde žádný z členů rozkladu není prvočinitel.

5. $(x, y) \in \{(21 - 8k, -91 + 35k) \mid k \in Z\} = \{(-3 - 8k, 14 + 35k) \mid k \in Z\}$.

12. cvičení

Ve škole:

1. (Eisensteinovo kriterium) Nechť $a = \sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x]$ splňuje podmínku $\mathrm{NSD}(a_0, \ldots, a_n) = 1$ a nechť prvočíslo p dělí a_i pro všechna $i = 0, \ldots, n-1$ a p^2 nedělí a_0. Dokažte, že je polynom a v $\mathbb{Z}[x]$ ireducibilní.

2. Dokažte, že jsou v $\mathbb{Z}[x]$ ireducibilní polynomy
(a) $x^8 - 12$, (b) $2x^5 + 9x^3 - 6$, (c) $x^6 + 10x^5 - 4x^3 + 8x^2 - 2$.

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

4. Dokažte, že jsou v $\mathbb{Z}[x]$ ireducibilní polynomy
(a) $x^6 + x^3 + 1$, (b) $x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p - 1}{x - 1}$ pro prvočíslo p.

Úlohy pro samostatné počítání:

5. Najděte generátor u všech ideálů, které jsou hlavní:
(a) $15\mathbb{Z} + 24\mathbb{Z}$ v $\mathbb{Z}$,
(b) $15\mathbb{Z} \cap 24\mathbb{Z}$ v $\mathbb{Z}$,
(c) $3\mathbb{Z}[x] + x\mathbb{Z}[x]$ v $\mathbb{Z}[x]$,
(d) $3\mathbb{Z}[x] \cap x\mathbb{Z}[x]$ v $\mathbb{Z}[x]$.

6. 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?

Řešení:

1. Nechť $a = b \cdot c$, kde $b = \sum_{i=1}^{r} b_i x^i, c = \sum_{i=1}^{s} c_i x^i \in \mathbb{Z}[x]$. Pokud $\deg b = 0$, pak $b = b_0 x^0$ a $a = \sum_{i=1}^{s} b_0 c_i x^i$, proto b_0 dělí $\mathrm{NSD}(a_1, \ldots, a_n) = 1$, tedy $b = \pm 1$ je invertibilní polynom (symetricky pro c).

   Předpokládejme, že $\deg b > 0$ a $\deg c > 0$. Potom $\deg c < n$ a $\deg b < n$, a protože p dělí $a_0 = b_0 c_0$ a p^2 nedělí $a_0 = b_0 c_0$ platí, že buď p dělí b_0 a nedělí c_0 nebo p dělí c_0 a nedělí b_0, bez újmy na obecnosti předpokládejme, že p dělí b_0 a nedělí c_0. Indukcí dokážeme, že p dělí b_i pro všechna $i = 0, \ldots, r < n$. Pro $i = 0$ tvrzení předpokládáme. Nechť $i < n$ a p dělí b_j pro všechna $j = 0, \ldots, i-1$. Protože $a_i = \sum_{j=0}^{i} b_j c_{i-j}$ a p dělí a_i podle předpokladu, platí, že

   $$p \text{ dělí } (a_i - \sum_{j=0}^{i-1} b_j c_{i-j}) = b_i c_0.$$

   Protože p podle předpokladu nedělí c_0, musí dělit b_i. Protože p dělí všechy koeficienty b, dělí i všechny koeficienty $a = b \cdot c$, což je spor s předpokladem $\mathrm{NSD}(a_1, \ldots, a_n) = 1$.

2. Použijeme Eisensteinovo kriterium pro (a),(b) $p = 3$, (c) $p = 2$

3. Dokazujeme nepřímo: nechť $f(x) = g(x)h(x)$ pro neinvertibilní polynomy g a h, pak $f(x+a) = g(x+a)h(x+a)$. Obrácenou implikaci dostaneme použitím dokázaného tvrzení pro polynom $g(x) := f(x+a)$ a $g(x + (-a))$.

4. (a) 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,

   (b) použijeme Eisensteinovo kriterium pro $\frac{(x+1)^p - 1}{(x+1)-1} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}$ a prvočíslo p,

5. (a) $3 = \mathrm{NSD}(15, 24)$,

   (b) $120 = \mathrm{NSN}(15, 24)$,

   (c) Není hlavní: případný generátor hlavního ideálu by byl společný dělitel 3 a x v oboru $\mathbb{Z}[x]$, tedy 1 nebo -1, ovšem $\pm 1 \notin 3\mathbb{Z}[x] + x\mathbb{Z}[x]$,

   (d) $3x$.

6. Nejprve si všimněme, že $u/v \Leftrightarrow v\mathbb{Z} \subseteq u\mathbb{Z}$. 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).

13. cvičení

Ve škole:

1. Najděte generátor u všech ideálů, které jsou hlavní:
(a) $15\mathbb{Z} + 24\mathbb{Z}$ v $\mathbb{Z}$,
(b) $15\mathbb{Z} \cap 24\mathbb{Z}$ v $\mathbb{Z}$,
(c) $3\mathbb{Z}[x] + x\mathbb{Z}[x]$ v $\mathbb{Z}[x]$,
(d) $3\mathbb{Z}[x] \cap x\mathbb{Z}[x]$ v $\mathbb{Z}[x]$.

2. Pro $p(y) \in \mathbb{C}[y]$ dokažte, že $x - p(y)$ je ireducibilní v $\mathbb{C}[x, y]$.

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) $x^2 + y^2$, (d) $x^2 + 2y^2$.

4. Určete v $\mathbb{Z}[i\sqrt{2}]$ ireducibilní rozklady prvků (a) 3, (b) $5 - i\sqrt{2}$.

Úlohy pro samostatné počítání:

5. Musí v $\mathbb{Z}[i\sqrt{2}]$ ireducibilní rozklady existovat a do jaké míry jsou určeny jednoznačně?

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

Řešení:

1. (a) $3 = \mathrm{NSD}(15, 24)$,

   (b) $120 = \mathrm{NSN}(15, 24)$,

   (c) Není hlavní: případný generátor hlavního ideálu by byl společný dělitel 3 a x v oboru $\mathbb{Z}[x]$, tedy 1 nebo -1, ovšem $\pm 1 \notin 3\mathbb{Z}[x] + x\mathbb{Z}[x]$,

   (d) $3x$.

2. 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 $\mathbb{C}[x, y]$,

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

4. $3 = (1 + i\sqrt{2})(1 - i\sqrt{2})$, $5 - i\sqrt{2} = -(1 + i\sqrt{2})^3$.

5. Jedná se Eukleidův obor, neboť norma je zde Eukleidova, tedy je to Gaussův obor. V něm jsou ireducibilní rozklady určeny jednoznačně až na pořadí a násobek invertibilním prvkem. Protože jsou invertibilní prvky $\mathbb{Z}[i\sqrt{2}]$ jen ± 1, jsou ireducibilní rozklady určeny jednoznačně až na pořadí a znaménko.

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

   (b) $x^2 + xy + y - 1 = (x + 1)(x + y - 1)$,

   (c) $2y^3 + y^2x + yx^2 + x^2 + 7y^2 + 3y - x - 2 =$

$$\begin{aligned} &= (y + 1)x^2 + (y^2 - 1)x + (2y^3 + 7y^2 + 3y - 2) \\ &= (y + 1)(x^2 + (y - 1)x + (2y^2 + 5y - 2)) \\ &= (y + 1)(x - y - 2)(x + 2y + 1) \end{aligned}$$