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.