Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

6 Počítání modulo polynom

1. V $\mathbb{Z}_2[x]$ najděte největší společný dělitel $d(x)$ polynomů $p(x) = x^7 + x^6 + x^5 + x^4 + x$ a $q(x) = x^3 + 1$.
2. Řešte rovnici $(x+1)r(x) = x + 2$ v okruhu $A = \mathbb{Z}_3[x]/q(x)$, kde $q(x) = x^2 + 2x + 2$. Tvoří tento okruh těleso? Kolik prvků má okruh A?
3. Rozhodněte, zda je okruh $B = \mathbb{Z}_3[x]/q(x)$, kde $q(x) = x^3 + 1$, těleso. Najděte inverzní prvek k prvku $x^2 + 1$ a vypište všechny prvky, které nemají v okruhu B inverzní prvek.

POČET STRAN: 1 + 4

JMÉNO: Radoslava JANDOVÁ

PODPIS: Jandora

DATUM: 19. 5. 2011

Zpracovala: **Radoslava Jandová, jandora1**
Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

6 POČÍTÁNÍ MODULO POLYNOM

6.1. V $Z_2[x]$ najděte GCD dvou polynomů

$p(x) = x^7 + x^6 + x^5 + x^4 + x$

$q(x) = x^3 + 1$

$GCD\left(p(x), q(x)\right)$

$$x^7 + x^6 + x^5 + x^4 + x = \left(x^4 + x^3 + x^2 + 1\right)\cdot\left(x^3 + 1\right) + \left(x^2 + x + 1\right)$$

$$-x^7 \qquad -x^4$$

$$0 + x^6 + x^5 + 0 + x$$

$$-x^6 \qquad -x^3$$

$$0 + x^5 - x^3 + x$$

$$-x^5 \qquad -x^2$$

$$0 - x^3 - x^2 + x = x^3 + x^2 + x$$

$$-x^3 \qquad +1$$

$$0 \quad x^2 + x + 1$$

$GCD\ d(x) = \left(x^2 + x + 1\right)$

Kontrola:

$$\left(x^3 + 1\right)\left(x^4 + x^3 + x^2 + 1\right) = x^7 + x^6 + x^5 + x^3 + x^4 + x^3 + x^2 + 1$$

$$= x^7 + x^6 + x^5 + x^4 + 2x^3 + x^2 + 1$$

$$+ \qquad x^2 + x + 1$$

$$= x^7 + x^6 + x^5 + x^4 + 2x^2 + x + 1$$

$$= x^7 + x^6 + x^5 + x^4 + x$$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**
Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(2)

6.2. Řešte rovnici $(x+1)\,r(x) = x+2$ v okruhu $A = \mathbb{Z}_3[x] / q(x)$, kde

$q(x) = x^2 + 2x + 2$.

Prvků tohoto okruhu bude?
Kolik prvků má okruh A?

Nejprve zjistím, zda má polynom $(x+1)$ v $\mathbb{Z}_3[x]/q(x)$ inverzi

$$GCD\left(\overbrace{x^2+2x+2}^{n}, \overbrace{x+1}^{a}\right)$$

$x^2 + 2x + 2 = (x+1)(x+1) + 1 \longrightarrow GCD$

$-x^2 - x$

$0 \quad x+2$

$-x-1$

1

$1 = (x^2+2x+2) - (x+1)(x+1)$

$1 = n - (x+1)a$

$x+1 = (x+1) \cdot 1 + 0$

$GCD = 1 \rightarrow$ inverzní prvek existuje

$(x+1)^{-1} = -(x+1)$

Nyní vypočtu hodnotu polynomu $r(x)$

$(x+1) \cdot r(x) = x+2 \quad / \cdot -(x+1)$

$(x+1) \cdot -(x+1) \cdot r(x) = (x+2) \cdot -(x+1)$

$r(x) = -x^2 - x - 2x - 2$

$r(x) = -x^2 - 3x - 2$

$r(x) = 2x^2 + 0 + 1$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(3)

Je okruh A těleso?

Z_3 těleso je, protože 3 je prvočíslo.
$q(x)$ je těleso, pokud je ireducibilní → nyní ověřím zda je polynom $q(x)$ rozložitelný nebo ne

$q(x) = x^2 + 2x + 2$
těleso Z_3 má 3 prvky 0, 1, 2 - tyto prvky postupně doplním do $q(x)$

$x^2 + 2x + 2$

$0 \to 0+0+2$
$1 \to 1+2+2$
$2 \to 4+4+2$

$\neq 0 \to q(x)$ nemá reálné kořeny, je ireducibilní

ověřila jsem, že $q(x)$ je také těleso
→ okruh A je těleso.

Počet prvků v okruhu A

$|A| = p^k = 3^2 = 9$

Z_3 ← → stupeň polynomu $q(x)$

prvky v okruhu A:
$A = \{ ax + b, \quad a, b \in Z_3 \}$

a \ b	0	1	2
0	0	1	2
1	x	$x+1$	$x+2$
2	$2x$	$2x+1$	$2x+2$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

4

Nakonec ještě ověřím, zda rovnice operandu leží v obruči A.

$$(x+1) \cdot r(x) = (x+2)$$

$(x+1)$ a $(x+2)$ jsou prvky obruče A.

$r(x) = 2x^2 + 1 \rightarrow$ nyní ještě zbývá vydělit $q(x)$

$$(2x^2+1) : (x^2+2x+2) = 2$$
$$-2x^2-4x-4$$
$$0 \quad -4x-3 \rightarrow 2x+0$$

$r(x) = 2x \rightarrow$ toto je již prvek obruče A

Zkouška:

$$(x+1) \cdot 2x = 2x^2 + 2x \quad \text{mod } q$$

$$(2x^2+2x) : (x^2+2x+2) = 2$$
$$-2x^2-4x-4$$
$$0 \quad -2x-4 \rightarrow \underline{\underline{x+2}}$$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

5

6.3 Rozhodněte, zda je okruh $B = \mathbb{Z}_3[x] / q(x)$, kde $q(x) = x^3 + 1$, těleso. Najděte inverzní prvek k prvku $x^2 + 1$ a vypište všechny prvky, které nemají v okruhu B inverzní prvek.

Předpoklad: $\mathbb{Z}_3$ je těleso.
$q(x)$ je těleso, pokud je ireducibilní → to ověříme postupným dosazením prvků $\mathbb{Z}_3$ do $q(x)$

$x^3 + 1$ $\quad 0 \to 0+1$ $\quad \} \neq 0$
$\quad 1 \to 1+1$ $\quad \}$
$\quad 2 \to 8+1 = 9 \mod 3 = 0 \to 2$ je kořen

→ $q(x)$ lze rozložit → $q(x)$ není těleso → ~~$\mathbb{Z}_3$~~ $\mathbb{Z}_3[x] / q(x)$ není těleso

Zkouška:

$$(x^3 + 1) : (x - 2) = x^2 + 2x - 4$$
$$-x^3 - 2x^2$$
$$0 + 2x^2 + 1$$
$$-2x^2 + 4x$$
$$0 + 4x + 1$$
$$-4x + 8$$
$$0 + 9 \mod 3 = 0$$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(6)

Nyní hledám inverzní prvek k x^2+1.

$$GCD\left(\overbrace{x^3+1}^{n},\ \overbrace{x^2+1}^{a}\right)$$

$$x^3+1 = x\left(x^2+1\right)+(2x+1)$$
$$-x^3-x$$
$$0 \quad -x+1 \qquad \text{mod } 3 = 2x+1$$

$$2x+1 = x^3+1-x\left(x^2+1\right)$$
$$= n - x \cdot a$$

$$\left(x^2+1\right) = (2x+2)(2x+1)+2$$
$$-x^2-2x$$
$$0 \quad -2x+1 \rightarrow x+1$$
$$-x-2$$
$$0 \quad -1 \rightarrow 2$$

$$2 = \left(x^2+1\right)-(2x+2)(2x+1)$$
$$= a-(2x+2)(n-xa)$$

$$2x+1 = x \cdot 2 + \boxed{1} \rightarrow GCD$$
$$-2x$$
$$0 \quad +1$$

$$1 = (2x+1)-2x$$
$$= n-xa-\left(a-(2x+2)(n-xa)\right)x$$

$$2 = 2 \cdot 1 + 0$$

Vzhledem k tomu, že vyjádření hodnoty 1 je velmi složité, použiji k výpočtu GCD = 1 hodnotu 2 takto:

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(4)

$$1 = a - (2x+2)(x - xa) \quad / \cdot 2 \text{ v } \mathbb{Z}_3$$

$$\begin{aligned} 1 &= 2a - (x+1)(x - xa) \\ &= 2a - (xx - x^2a + x - xa) \\ &= -xx - x + x^2a + xa + 2a \\ &= 2xx + 2x + x^2a + xa + 2a \\ 1 &= x(2x+2) + a(x^2 + x + 2) \end{aligned}$$

$$(x^2+1)^{-1} = x^2 + x + 2$$

Zkouška:

$$\begin{aligned} (x^2+1)(x^2+x+2) &= x^4 + x^3 + 2x^2 + x^2 + x + 2 \\ &= x^4 + x^3 + x + 2 \mod q(x) \end{aligned}$$

$$(x^4 + x^3 + x + 2) : (x^3 + 1) = x + 1$$

$$\begin{array}{rr} -x^4 & -x \\ \hline 0 + x^3 & +2 \\ -x^3 & -1 \\ \hline & 1 \end{array}$$

Prvky okruhu $\mathbb{Z}_3$, které nemají inverzi jsou prvky, které jsou
- soudělné přes $(x^2 + x + 2)$
- soudělné přes $(x+1)$
- hledáme prvky nejvýše st. 2

$$\begin{aligned} k(x)\ (x^2 + x + 2) &= a(x^2 + x + 2) \quad a \in \mathbb{Z}_3 \\ k(x)\ (x+1) &= bx + c\ (x+1) \quad b, c \in \mathbb{Z}_3 \end{aligned}$$