Kamil Dareby

(6.1) V $\mathbb{Z}_2[x]$ najděte největší společný dělitel $d(x)$ polynomů

$$p(x) = x^7 + x^6 + x^5 + x^4 + x \quad a \quad q(x) = x^3 + 1$$

použijeme Euklidův algoritmus

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

$$\begin{array}{r} -x^7 \qquad -x^4 \\ \hline x^6 + x^5 + x \\ -x^6 \quad -x^3 \\ \hline x^5 - x^3 + x \\ -x^5 \quad -x^2 \\ \hline x^3 + x^2 + x \\ -x^3 \qquad -1 \\ \hline x^2 + x + 1 \end{array}$$

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

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

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

$$x^3 + 1 = (x+1)(x^2 + x + 1) + 0$$

největší společný dělitel $d(x) = x^2 + x + 1$

Kamil Dareby

(6.2) Řešte rovnici $(x+1)\cdot r(x) = x+2$ 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?

Zjistíme, zda má polynom $(x+1)$ v $\mathbb{Z}_3[x]/q(x)$ inverzní prvek

$\gcd((x^2+2x+2), (x+1))$

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

$-x^2 - x$

$x+2$

$-x-1$

-1

$x^2+2x+2 = (x+1)\cdot(x+1)+1 \qquad 1 = (x^2+2x+2) - (x+1)(x+1)$

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

$\gcd((x^2+2x+2), (x+1)) = 1 \Rightarrow$ existuje inverzní prvek,

který přečteme z Bezoutovy rovnosti.

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

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

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

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

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

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

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

(6.2) pokračování

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

$$\underline{-\,2x^2 - 4x - 4}$$

$$-4x - 3$$

$$r(x) = 2x$$

$\mathbb{Z}_3$ je těleso $q(x) = x^2 + 2x + 2$ je ireducibilní (nemá kořen v $\mathbb{Z}_3$)

proto je okruh $A = \mathbb{Z}_3[x] / q(x)$ těleso.

počet prvků

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

$$A = \{ ax + b,\ a, b \in \mathbb{Z}_3 \}$$

Kamil Dareby

(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.

$\mathbb{Z}_3$ těleso, aby B bylo těleso, musí být $q(x)$ ireducibilní.

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

$-x^3 + 2x^2$

$2x^2 + 1$

$-2x^2 + 4x$

$4x + 1$

$-4x + 8$

$9 = 0$

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

Okruh B není těleso.

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

$\gcd((x^3+1), (x^2+1))$

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

$-x^3 - x$

$2x+1$

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

$n = x^3+1 \quad a = x^2+1$

$(2x+1) = n - x \cdot a$

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

$-x^2 - 2x$

$x+1$

$-x-2$

$2 = a - (2x+2) \cdot (n - xa)$

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

(6.3) pokračování

$$2 = a - (2x+2)(n - xa)$$

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

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

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

$$1 = -(x+1)(x^3+1) + (x^2+1)(x^2+x+2)$$

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

Které prvky nemají inverze?

soudělné s $(x^2+x+2)(x+1)$

hledáme prvky alespoň nejvýše 2

$k(x)(x^2+x+2) = a(x^2+x+2)$ $\quad a \in \mathbb{Z}_3$

$l(x)(x+1) = bx + c(x+1)$ $\quad b, c \in \mathbb{Z}_3$