Př.: $n = 5$ jaké cyklické kódy $C \subseteq \mathbb{Z}_2^5$ existují?

Víme $g(x)$ dělí $x^5 - 1$

$$x^5 - 1 = (\quad)(\quad)$$

$g_1$ $g_2$

ireduk. reduk

$$C_1 := \{ g_1(x) \cdot a(x) \quad \forall a(x) \in \mathbb{Z}_2^5[x]/x^5 - 1 \}$$

$$x^5 + 1 = x^5 - 1 = \underbrace{(x+1)}_{\text{ireduk}} \underbrace{(x^4 + x^3 + x^2 + x + 1)}_{\text{ireduk.}}$$

$g_1(x) = x + 1$

$C = \{ 0\cdot(x+1),\ 1\cdot(x+1),\ x(x+1),\ (x+1)^2,\ x^2(x+1),\ (x^2+1)(x+1),\ (x^2+x)(x+1),$
$(x^2+x+1)\cdot(x+1),\ x^3(x+1),\ (x^3+1)(x+1),\ (x^3+x)(x+1),\ (x^3+x+1)(x+1),$
$(x^3+x^2)(x+1),\ (x^3+x^2+1)(x+1),\ (x^3+x^2+x)(x+1),\ (x^3+x^2+x+1)(x+1) \}$

co násobky $(x^4 + \underbrace{p(x)}_{\text{st} \le 3})(x+1) = x^5 + x\cdot p(x) + p(x) + x^4$
$= \underbrace{x^4 + 1}_{\cdot} + p(x)(x+1)$

$= (x+1)(x^3+x^2+x+1) + p(x)(x+1) = (x+1)\cdot(\underbrace{p(x) + x^3 + x^2 + x + 1}_{\text{st} \le 3})$

$C = \{ \emptyset,\ x+1,\ x^2+x,\ x^2+1,\ x^3+x^2,\ x^3+x^2+x+1,\ x^3+x,\ x^3+1,$
$x^4+x^3,\ x^4+x^3+x+1,\ x^4+x^3+x^2+x,\ x^4+x^3+x^2+1,\ x^4+x^3+x^2+x+1,$
$x^4+x^2+x+1,\ x^4+x,\ x^4+1 \}$

$|C| = 16$

kód paritní slova $w$ délky 5 t.ž.
$w = w_1 w_2 w_3 w_4 w_5$

$$\sum w_i \equiv 0$$

---

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

$$C = \{\emptyset, x^4 + x^3 + x^2 + x + 1\}$$

00000
11111

---

$x^n - 1 = (g_1)(g_2)\dots(g_k)$

rozklad na ireducibilní polynomy v $\mathbb{Z}_2[x]$

potom $g_i$ jsou jediné možnosti na volbu generujícího polynomu

Def: $q(x)$ ireducibilní polynom v $\mathbb{Z}_2[x]$.

Pro $b(z) \in \mathbb{Z}_2[z]/q(z)$ (konečné těleso) nazýváme MINIMÁLNÍ POLYNOM (jednoznačný)

$\mathbb{Z}_2[x] \Rightarrow f(x)$ s koef. v $\mathbb{Z}_2$ t.ž. $f(b) \equiv 0$ v $\mathbb{Z}_2[z]/q(z)$
s nejmenším možným stupněm

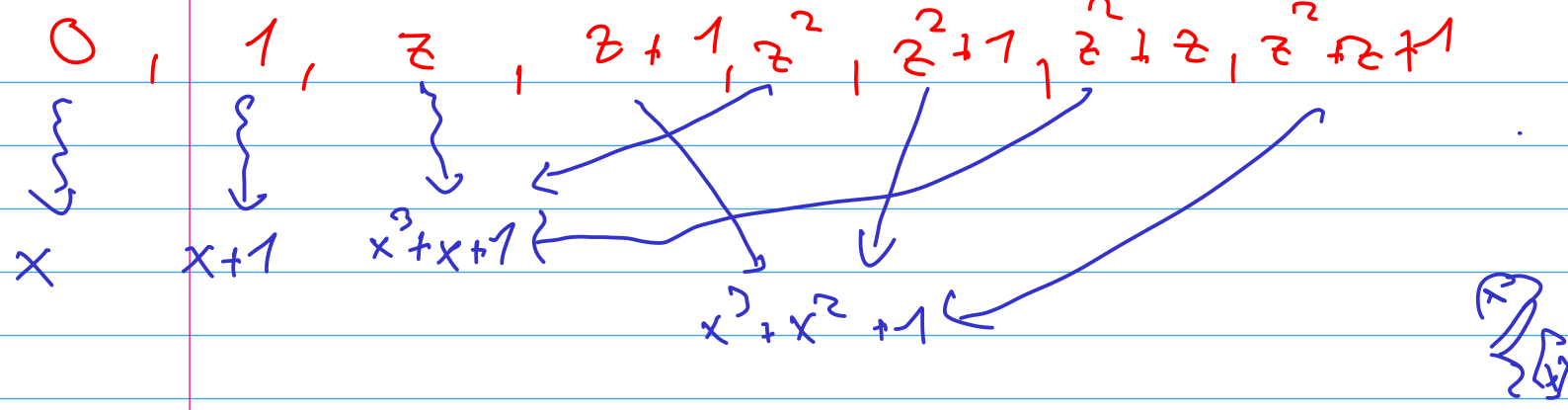
Př: $\mathbb{Z}_2[x]/x^3+x+1$ [aka $GF(8)$ - 8 prvkové konečné těleso]

Pozn: $\mathbb{Z}_p$ mod $p$, $GF(4) \cong \mathbb{Z}_2[z]/x^2+x+1$

$2 \cdot 2 = 0 \pmod 4$

FAKT. až na isomorfismus $\exists$ právě jedno konečné těleso velikosti $p^k$

$\mathbb{Z}_2[z]/z^3+z+1$ má celkem 8 prvků AKA 7 netriviálních prvků




hledáme $f(x) \in \mathbb{Z}_2[x]$ $\quad f = x^3+x+1$

$f(z) \equiv 0$ v $\mathbb{Z}_2[z]/z^3+z+1$

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

$f(z+1) = (z+1)^3 + (z+1)^2 + 1$

$z^3+z^2+z+1 \quad z^2+1 \quad +1 = z^3+z+1 \equiv 0$

$\Rightarrow$ minimální polynomy netriviálních prvků $\mathbb{Z}_2[x]/x^3+x+1$ jsou

1) $x$
2) $x+1$
3) $x^3+x+1$
4) $x^3+x^2+1$

$x(x+1)(x^3+x+1)(x^3+x^2+1) = x(x^7-1)$

$\mathcal{M} = \{ M(x) : M(x)$ je min. polynom $b \neq 0 \}$

$x^7-1 = \prod_{M \in \mathcal{M}} M(x)$

irr. $\forall b \in \mathbb{Z}_2[x]/q(x)$, kde $q$ ireducibilní

$\exists$ polynom $f_b(x)$ t.ž. $f_b(b) \equiv 0$

Def.: $m := \text{stupeň } q$

univerzální $f(x) := x^{2^m} - x$ pořád $f(b) \equiv 0$

$\forall b \in \mathbb{Z}_2[x]/q(x)$

konečné těleso

speciálně nenulové prvky tvoří multip. grupu, která je cyklická

z teorie konečných těles

$GF(2^m) \setminus \{0\} = \{\alpha_1, \alpha^2, \alpha^3, \dots, \alpha^{2^m-1}\}$ pro nějaké $\alpha_1 \in GF(2^m)$

(Př.: $p=3$, $\alpha=3$: $3^1, 3^2, 3^3, 3^4$ $\{3, 4, 2, 1\}$)

Víme, $\forall b \in \mathbb{Z}_2[x]/q(x) \setminus \{0\}$ lze $\alpha^l$ $l \in \mathbb{N}$, $0 \le l \le 2^m - 2$

$$(b)^{2^m-1} \equiv (\alpha^l)^{2^m-1} = \alpha^{(2^m-1)l} = (\alpha^{2^m-1})^l \equiv 1$$

$$f(x) := x\left(x^{2^m-1} - 1\right) = x^{2^m} - x$$

$\forall b \in \mathbb{Z}_2[x]/q(x)$ je kořen $f(x)$ ☒

Věta: $q(x)$ ireducibilní, $b \in \mathbb{Z}_2[x]/q(x)$

existuje právě jeden minimální polynom pro $b$

Dk.: mějme $f_1(x)$ a $f_2(x)$ různé polynomy stejného stupně $m$ s koef. v $\mathbb{Z}_2$ t.ž. $b$ je kořen

CÍL: $f_1(x)$ ani $f_2(x)$ nejsou minimálním polynomem $b$

$$f(x) := f_1(x) - f_2(x) = p_1(x) - p_2(x)$$

$st < m$ (= $m$)

$b$ kořen $f(x)$ $\quad (x^m + p_1(x)) - (x^m + p_2(x))$

$st < m$ $\quad$ $st < m$

$\blacksquare$