ROZKLAD POLYNOMŮ

Tvrzení: $c \in \mathbb{Z}_p$ je kořen polynomu $q(x) \in \mathbb{Z}_p[x]$ jestliže $q(x) = (x-c) \cdot L(x)$

Tvrzení: Polynom st. k nad $\mathbb{Z}_p$ má v $\mathbb{Z}_p$ nejvýše k kořenů.

Pozn.: To neplatí v $\mathbb{Z}_n[x]$, $n \neq p$

např. $q(x) = x^2 - 1 \in \mathbb{Z}_8[x]$

má 4 kořeny a to $1, 3, 5, 7 \in \mathbb{Z}_8$

a má nejednoznačný rozklad

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

DEF. Polynom $q(x)$ je IREDUCIBILNÍ (= nerozkladný) v $\mathbb{Z}_p[x]$, jestliže nelze rozložit na součin dvou polynomů nižších stupňů.

Pozn.: Vždy lze $q(x) = a \cdot (a^{-1} \cdot q(x))$

(a: st. 0; $a^{-1} \cdot q(x)$: st. = st. q)

ANALOGIE $p = 1 \cdot p$

TEST IREDUCIBILITY

$q(x)$ je ireducib. právě když $q(x)$ není dělitelný žádným ireducib. polyn. st. $\leq \frac{\text{st } q}{2}$

Spec.: $q(x)$ polyn. st. ≤ 3 je ireducib. jestliže není dělitelný žádným polyn. st. 1

$q(x)$ polyn. st. $\leq$ je ireducib. v $\mathbb{Z}_p[x]$ jestliže

$q(x)$ nemá kořen v $\mathbb{Z}_p$.

(PŘ) $\mathbb{Z}_2[x]$ najdi ireducib. polyn. st. 2 a 3

st. 2 $x^2 + x + 1$

nemá kořen v $\mathbb{Z}_2$ 0 ... abs. člen = 1

1 .... lichý počet sčítanců

jediný ireducib. polyn. st. 2 nad $\mathbb{Z}_2$

st. 3 $x^3 + x + 1$

$x^3 + x^2 + 1$

Pozn.: st. 4 $x^4 + x^2 + 1$ - nemá kořen $\Rightarrow$

nelze napsat jako

$(x - c)(x^3 + \dots) =$ ~~$\dots$~~

$\hookrightarrow = (x^2 + x + 1)^2 \Rightarrow$ je rozložitelný

(V) okruh polynomů nad $\mathbb{Z}_p[x]/q(x)$ je těleso, jestliže $q(x)$ je ireducib. v $\mathbb{Z}_p[x]$.

(Dk) $a(x) \in \mathbb{Z}_p[x]/q(x)$

kdyby po dělení $q(x) \Rightarrow$ st. $a(x) <$ st $q(x)$

$q(x)$ je ireducib. v $\mathbb{Z}_p[x] \rightarrow$ nesoudělný

se všemi polyn. nižšího stupně kromě 0

$\rightarrow$ všechny $a(x) \neq 0$ mají inverzi

Jako tělesa se nazývají GALOISOVA TĚLESA

$GF(p^k)$

Galois field $\hookrightarrow$ p^k = počet prvků

(k = st. polynomu)

(PŘ) z minula

$A = \mathbb{Z}_3[x] / x^2+1$

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

$q(0) = 1$
$q(1) = 2$
$q(2) = 2$

→ $q(x)$ nemá kořen v $\mathbb{Z}_3$.
(q je st. 2) → q je ireducib.
A je těleso $GF(3^2) = GF(9)$

(PŘ) $B = \mathbb{Z}_3[x] / x^2-1$

$q(1) = 0$ → má kořen → $q(x)$ je rozložitelný
→ B není těleso

Které prvky nemají inverz? → jsou soudělné s $q(x)$

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

---

v $\mathbb{Z}_{12}$ - a soudělné s 12 $\quad 12 = 2^2 \cdot 3$
soudělné přes 2 $\quad k \cdot 2, \quad k < 6$
— " — přes 3 $\quad k \cdot 3, \quad k < 4$

$q(x) = (x-1)(x+1)$

$\mathbb{Z}_3[x]$ $q(x) : (x-1) = x+1$

soudělné přes $(x-1)$ $\quad k(x) \cdot (x-1) = a(x-1) \in B$
— " — přes $(x+2)$ $\quad k(x) \cdot (x+1) = b(x+1)$
$a, b \in \mathbb{Z}_3$

zbytky sl. nejvýše 1

pro $a = 0$ a $b = 0$ vyjde
$a(x-1) = 0$ → celem
$3+3-1 = 5$ prvků nemá inverz

PŘ $C = \mathbb{Z}_2[x] \Big/ x^4 + x^2 + 1$

$q(0) = 1$
$q(1) = 1$
$\Big\}$ → bez kořene

ALE $st = 4$ → lze rozložit ireducib. polynomem
$st\ 2 \left(= \frac{st\ q}{2}\right)$

ho je jen $x^2 + x + 1$

nad $\mathbb{Z}_2$ $\left(x^4 + x^2 + 1\right) : \left(x^2 + x + 1\right) = x^2 + x + 1$

→ $q(x)$ je rozložitelný → C není těleso

Prvky

$C = \{ ax^3 + bx^2 + cx + d, \quad koef. \in \mathbb{Z}_2 \}$

inverze nemají – součiny $\circ\ q(x) = \left(x^2 + x + 1\right)^2$

$a(x) = k(x)\left(x^2 + x + 1\right) \quad st \leq 3$

→ $a(x) = \left(bx + c\right)\left(x^2 + x + 1\right)$

$b, c \in \mathbb{Z}_2$ → 4 prvky