

Řešené příklady: Konečná tělesa

Připomenutí: tělesa kterých řádů existují?

Věta 34.3 Řádem konečného tělesa musí být mocnina prvočísla, tedy číslo zapsatelné jako p^n , kde p je prvočíslu a n je kladné celé číslo.

Navíc platí, že všechna tělesa řádu p^n jsou **navzájem izomorfní**.

Definice 34.4 Těleso s p^n prvky nazýváme *Galois field* a značíme ho $GF(p^n)$. Prvočíslu p se nazývá **charakteristikou** tělesa $GF(p^n)$.

Konstrukce konečného tělesa řádu p^n

Bud $p(x) \in \mathbb{Z}_p[x]$ ireducibilní polynom nad \mathbb{Z}_p stupně n .

Trojice

$$\left(\{q(x) \in \mathbb{Z}_p[x] : \deg(q(x)) \text{ je menší než } n \text{ nebo není definován} \}, +, \cdot \text{ mod } p(x) \right),$$

kde $+$ a \cdot jsou operace sčítání a násobení polynomů (z okruhu polynomů $\mathbb{Z}_p[x]$), je konečným tělesem řádu p^n (tedy $GF(p^n)$).

$GF(p^n)$: **aditivní grupa**

Co víme o aditivní grupě tělesa $GF(p^n)$:

- Má řád p^n .
- Neutrální prvek je $0 = 00 \cdots 0 = 0^n$.
- Inverze k prvku $b_1 b_2 \cdots b_n$ je $(p - b_1)(p - b_2) \cdots (p - b_n)$.
- Pro $n > 1$ není cyklická, dokonce pro každý prvek v platí, že $(p + 1) \times v = v$, resp. $p \times v = 0$.

$GF(p^n)$: **multiplikativní grupa**

Co víme o multiplikativní grupě tělesa $GF(p^n)$:

- Má řád $p^n - 1$.
- Neutrální prvek je $00 \cdots 1 = 0^{n-1}1$.
- Je vždy cyklická (důkaz není moc složitý, ale zabral by nám moc času).

Konečná tělesa – příklady

Základní cvičení 23.1

Základní cvičení 23.1

V tělese \mathbb{Z}_{263} najděte multiplikatívni inverzi k prvku 112.

Základní cvičení 23.2

Základní cvičení 23.2

Rozhodněte, zda je polynom $P(x)$ ireducibilní nad tělesem \mathbb{Z}_5 , kde

(a) $P_a(x) = x^3 + 2x + 1$;

(b) $P_b(x) = x^2 + 2x + 2$;

Základní cvičení 23.3

Základní cvičení 23.3

Rozhodněte, zda je polynom $P(x)$ ireducibilní nad tělesem \mathbb{Z}_3 , kde

(a) $P_a(x) = 2x^4 + x^3 + 2x + 1$;

(b) $P_b(x) = x^4 + x^3 + x + 2$;

(c) $P_c(x) = x^4 + x + 2$.

Základní cvičení 23.7

Základní cvičení 23.7

V tělese $GF(3^2)$, kde se násobí modulo ireducibilní polynom $x^2 + 2x + 2$, najděte

(a) všechna y taková, aby $21(y + 11) = 01 + y$,

(b) najděte všechny generátory multiplikatívni grupy tohoto tělesa.

Základní cvičení 23.16

Základní cvičení 23.16

Mějme těleso $GF(5^3)$, kde se násobí modulo ireducibilní polynom $x^3 + 3x + 3$.

(a) Nalezněte inverzní prvek vzhledem k násobení k prvku $x^2 + 2x$.

(b) Nalezněte všechna $y \in GF(5^3)$, která splňují $120 \cdot y^2 = 111$.

ChangeLog

Verze	Datum	Autor	Log
1.1	20.10.2019	ŠS	Opravda: stupeň je deg.
1.0	14.10.2019	ŠS	Výchozí verze.