Teorie kódování

LS 2021/22, FJFI ČVUT

2. domací úlohy

---

1) Ukažte, že $(3, 2)$-Hammingův kód, tj. lineární kód nad tělesem $\mathbb{Z}_3 = \{-1, 0, 1\}$ délky 4, dimenze 2 a min. vzdáleností 3, není cyklickým kódem.

2) Dokažte, že pro každé liché prvočíslo p existuje n takové, že p dělí $2^n - 1$.

2⋆) Těžší varianta: dokažte, že pro každé liché číslo m existuje n takové, že m dělí $2^n - 1$.

3a) Buď $n \geq 2$, $s \geq 1$ a $r \geq 1$ tři přirozená čísla. Dokažte, že $(n^s - 1)$ dělí $(n^r - 1)$ právě tehdy když s dělí r.

3b) Buď $\mathbb{F}$ těleso, $s \geq 1$ a $r \geq 1$ dvě přirozená čísla. Dokažte, že v okruhu polynomů $\mathbb{F}[x]$ polynom $(x^s - 1)$ dělí polynom $(x^r - 1)$ právě tehdy když s dělí r.

4) Buď p je prvočíslo a nechť a_m značí počet ireducibilních polynomů stupně m z okruhu $\mathbb{Z}_p[x]$. S použitím Gaussovy věty dokažte, že $a_m \geq 1$ pro každé $m \in \mathbb{N}$.

Připomeňme, že Gaussova věta říká pro všechna prvočísla p a $m \in \mathbb{N}$ následující:

$$p^m = \sum_{d|m} d a_d \qquad \text{(součet přes všechny dělitele } d \text{ čísla } m\text{)}.$$

⋆) Dokažte Gaussovu větu.