Teorie kódování

LS 2023/24, FJFI ČVUT

2. domací úlohy

1) Ukažte, že každý lineární kód nad tělesem $\mathbb{Z}_3 = \{-1, 0, 1\}$ délky 4, dimenze 2 a minimální vzdáleností 3, není ekvivalentní cyklickému kódu.

   Poznámka: lin. kód nad $\mathbb{Z}_3$ *délky* 4*, dim.* 2 *a min. vzdáleností* 3 *je* $(3, 2)$*-Hammingův kód.*

2a) 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.

2b) 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.

3) Buď p 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 $m \in \mathbb{N}$.

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

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

⋆) Bonus: Dokažte / nastudujte si důkaz pro Gaussovu větu.