1. série domácích úkolů

Odevzdejte do čtvrtku 31.3., 12:30.

1.1. Uvažujte binární Hammingův kód $\mathcal{H}$ s kontrolní maticí $H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ z proseináře. Dekódujte přijatou zprávu 0011101101101111011000101000001000 1 (sestávající z pěti bloků délky 7) předpokládáte-li, že v každém bloku došlo nejvýše k jedné chybě.

5 bodů

1.2. Sestrojte generující matici nějakého lineárního kódu délky 7 a dimenze 3, který opraví dvě chyby (*Vyžijte Příklad 2.4 z proseináře pro aspoň sedmiprvkové těleso*).

5 bodů

1.3. Najděte řešení (a vysvětlete, jak jste ho našli) varianty Eulerovy úlohy o důstojnících pro 5 regimentů (označte čísly $1, \ldots, 5$) a 5 hodností (označte písmeny P - poručík, N - nadporučík K - kapitán, M - major, G - generál).

5 bodů

1.4. Nechť $(a_{i,j})_{i,j\in I}$ a $(\tilde{a}_{i,j})_{i,j\in I}$ jsou vzájemně ortogonální latinské čtverce na množině I a $(b_{i,j})_{i,j\in J}$ a $(\tilde{b}_{i,j})_{i,j\in J}$ vzájemně ortogonální latinské čtverce na množině J. Dokažte, že $((a_{i,j}, b_{k,l}))_{(i,k),(j,l)\in I\times J}$ a $((\tilde{a}_{i,j}, \tilde{b}_{k,l}))_{(i,k),(j,l)\in I\times J}$ jsou vzájemně ortogonální latinské čtverce na množině $I \times J$.

5 bodů

2. série domácích úkolů

Odevzdejte do čtvrtku 21.4., 12:30.

2.1. Spočítejte násobnost kořenu 1 polynomu $x^6 + x^5 - 2x^4 - 2x^3 - 2x^2 + 2x + 2$ nad tělesem $\mathbb{Z}_5$. Výpočet vysvětlete. Jaká bude násobnost téhož kořenu v témže polynomu nad tělesem o 125 prvcích?

5 bodů

2.2. Najděte pro $w = y^2 - (x^3 + x + 1) \in \mathbb{Z}_5[x, y]$ všechny prvky $\mathbb{E}_w(\mathbb{Z}_5)$, určete prvek opačný pro každý prvek $\mathbb{E}_w(\mathbb{Z}_5)$ a najděte nějakou trojici a, b, c po dvou různých prvků kladného řádu, aby $a + b = c$.

5 bodů

2.3. Uvažujte ElGamalovy protokoly s grupou Z_{29}^*, tajným klíčem $k = 5$ a generátorem $a = 2$ (že se jedná o generátor nemusíte ověřovat). Zašifujte zprávu 13 a digitálně podpište zprávu $m \in M$, jejíž hash je 10. Jako náhodné číslo l zvolte 9.

5 bodů

2.4. Nechť R je obor a K jeho podílové těleso. Pokud pro každé $a \in K \setminus \{0\}$ platí $a \in R$ nebo $a^{-1} \in R$ (takovému oboru se říká valuační), dokažte, že je R lokální. *(Návod: ukažte* $\forall a, b \in R$*, že* $a \cdot b \in R^* \Rightarrow a, b \in R^*$ *a že* $\frac{a}{b} \in R, a + b \in R^* \Rightarrow \frac{1}{b} \in R \Rightarrow b \in R^*$*, což vám umožní dokázat, že je* $R \setminus R^*$ *ideál).*

5 bodů

3. SÉRIE DOMÁCÍCH ÚKOLŮ

Odevzdejte do čtvrtku 19.5., 12:30.

3.1. Uvažte konvoluční kódování nad dvouprvkovým tělesem $\mathbb{F}_2$ dané racionální funkcí $\frac{1+D}{1+D+D^2}$. Napište prvních deset bitů (tj. koeficienty polynomu $\sum_{i=0}^{9} b_i D^i$) zprávy $K(u)$ pro (a) $u = 1001 \sim 1 + D^3$, (b) $u = 10011 \sim 1 + D^3 + D^4$.

5 bodů

3.2. Uvažte orientovaný graf $G = (\mathbb{Z}_8, V)$, kde $V = \{(a, b) \in \mathbb{Z}_8^2 \mid a + 5 \equiv b \bmod 8\}$. Rozhodněte, zda je grupa automorfismů $Aut(G)$ abelovská a kolik má prvků. Svá tvrzení dokažte.

5 bodů

3.3. Dokažte, že ideál $(3, 1 + i\sqrt{5})$ není v okruhu $\mathbb{Z}[i\sqrt{5}]$ hlavní.

5 bodů

3.4. Najděte nějakou věrnou reprezentaci nad tělesem $\mathbb{C}$ symetrické grupy S_3 stupně 3 (tj. prostý homomorfismus $S_3 \to GL_3(\mathbb{C})$). Vysvětlete, proč neexistuje žádná věrná reprezentace S_3 stupně 1.

5 bodů

4. SÉRIE DOMÁCÍCH ÚKOLŮ

Odevzdejte do středy 29.6., 23:59.

4.1. Nechť $(R, +, \cdot, -, 0, 1)$ je (obecně nekomutativní) okruh s jednotkou splňující pro každé $a, b \in R \setminus \{0\}$ podmínku, že $a \cdot b \neq 0$ (tj. jde o "obecně nekomutativní obor"). Pokud je R konečný, dokažte s využitím malé Wedderburnovy věty, že jde nutně o komutativní těleso.

5 bodů

4.2. Popište všechna n, pro něž je n-tý cyklotomický polynom tvaru $\Phi_n = \sum_{i=0}^{n-1} x^i$. Své tvrzení dokažte.

5 bodů

4.3. Kolik existuje různých homomorfismů volné grupy $F_{\{x,y\}}$ o dvou generátorech do grupy S_3. Své tvrzení vysvětlete.

5 bodů

4.4. Ověřte, že je prezentace $\langle x, y \mid x^2, y^3, (xy)^2 \rangle$ izomorfní grupě S_3.

(Návod: ukažte, že má daná prezentace nejvýše 6 prvků, tj. různých rozkladových tříd modulo normální podgrupa $N = \langle\langle x^2, y^3, (xy)^2 \rangle\rangle$, najděte surjektivní homomorfismus $\psi : F_{\{x,y\}} \to S_3$, jehož jádro obsahuje N a využijte první větu o izomorfismu.)

5 bodů