Sügis 2016

Lõplikud korpused I

4. praktikumi ülesanded

Baasid ja elliptilised kõverad.

1. Leida korpuse $\mathbb{F}_{2^5} = \mathbb{F}_2[x]/(x^5+x^3+1)$ kanoonilise baasi $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ duaalbaas.

2. Leida üks korpuse $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/(x^4+x+1)$ eneseduaalne baas üle $\mathbb{F}_2$ ja tõestada, et ükski $\mathbb{F}_{2^4}$ eneseduaalne baas üle $\mathbb{F}_2$ ei ole normaalbaas.

3. Tõestada, et korpuse $\mathbb{F}_{q^n}$ erinevate polünoombaaside arv üle $\mathbb{F}_q$ on $\sum_{d|n} \mu(\frac{n}{d}) q^d$.

4. Olgu $K = \mathbb{F}_q$ ja $L = \mathbb{F}_{q^n}$. Tõestada, et korpusel L on olemas selline normaalbaas $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ üle korpuse K, et $\mathrm{Tr}_{L/K}(\alpha) = 1$.

5. Vaatleme võrrandit $E : y^2 = x^3+2x-1$ üle $\mathbb{F}_5$. Koostada elliptilise kõvera $E(\mathbb{F}_5)$ Cayley tabel.

6. Alice ja Bob kasutavad ühissaladuse jagamiseks elliptilist Diffie-Hellmani võtmevahetusskeemi elliptilise kõvera $E : y^2 = x^3 + 171x + 853$ jaoks üle $\mathbb{F}_{2671}$, fikseerides sellel punkti $P = (1980, 431)$. Alice saadab Bobile sõnumi $(2110, 543)$. Bob otsustab kasutada kordajana arvu $n = 1943$. Mis on nende ühissaladus? Kui Alice saadab välja ainult x-koordinaadi 2 ja Bob kasutab kordajat 875 ning ühissaladuseks on samuti x-koordinaat, siis mis see on?

7. Aita Evel leida eelmise ülesande esimeses pooles vahetatud ühissaladust, st. leida diskreetne logaritm $\log_{(1980,431)}(2110, 543)$ üle $E(\mathbb{F}_{2671})$.

8. Olgu E elliptiline kõver üle $\mathbb{F}_p$ ja kehtigu $Q = nP$ mingite E punktide Q ja P korral. Tähistagu $n_0 = \min\{n \in \mathbb{N} \mid Q = nP\}$ vähimat sellist arvu ja $m_0 = \min\{m \in \mathbb{N} \mid mP = \mathcal{O}\}$ punkti P järku. Tõestada, et iga võrrandi $xP = Q$ lahend x (st. diskreetne logaritm) on kujul $x = n_0 + im_0$, $i \in \mathbb{Z}$.

9*. Leida piisav ja tarvilik tingimus selleks, et lõpliku korpuse $\mathbb{F}_{q^n}$ polünoombaasi (üle $\mathbb{F}_q$) duaalne baas oleks samuti polünoombaas.