

Véges testek

Feladatsor

Diszkrét modellek alkalmazásai

Matematikai kérdések

1. Számítsuk ki:

- a) $\mathbb{Q}(\sqrt{2})$ -ben $(2 + 3\sqrt{2})/(3 - 2\sqrt{2})$ értékét (azaz írjuk fel $a + b\sqrt{2}$ alakban);
- b) $\mathbb{Q}(\sqrt{3})$ -ben $-3 + 2\sqrt{3}$ multiplikatív inverzét;
- c) $\mathbb{Q}(\sqrt{5})$ -ben $(1 + \sqrt{5})^n$ -t $n = 1, 2, 3, 4$ -re.

2. Számítsuk ki $\mathbb{Q}(\sqrt[3]{2})$ -ben a következő értéket: $(1 + \sqrt[3]{2} - \sqrt[3]{2}^2)(3 + \sqrt[3]{2} + 2\sqrt[3]{2}^2)$.

3. Soroljuk fel az összes legfeljebb 20 elemből álló véges testet.

4. Soroljuk fel $\mathbb{F}_9$ összes elemét a θ primitív elem segítségével.

5. Hány eleme van $\mathbb{Z}_3(\theta)$ -nak, ha θ minimálpolinomja $x^4 + x + \bar{2} \in \mathbb{Z}_3[x]$?

6. Számítsuk ki a megadott véges testekben az alábbi értékeket $a + b\theta$ alakban, ahol θ a test primitív eleme, amelynek minimálpolinomja az adott m polinom:

- a) $(\bar{1} + \bar{2}\theta)(\bar{2} + \bar{3}\theta)$ értékét $\mathbb{F}_{25} = \mathbb{Z}_5(\theta)$ -ban ($m = x^2 - \bar{2}$);
- b) $(\bar{4} + \bar{2}\theta)$ multiplikatív inverzét $\mathbb{F}_{25}$ -ben ($m = x^2 - \bar{2}$);
- c) $(\bar{4} + \bar{2}\theta)$ multiplikatív inverzét $\mathbb{F}_{25}$ -ben ($m = x^2 - \bar{3}$);
- d) $(\bar{5} + \bar{3}\theta)^2/(\bar{6} + \bar{4}\theta)$ értékét $\mathbb{F}_{49}$ -ben ($m = x^2 - \bar{5}$).

Programozási feladatok

7. A Sage műveletei segítségével oldjuk meg a következő feladatokat:

- a) Számítsuk ki $\bar{1} + \bar{3}\theta \in \mathbb{F}_{25} = \mathbb{Z}_5(\theta)$ multiplikatív inverzét, ahol θ az $x^2 - \bar{2}$ polinom gyöke.
- b) Az $\mathbb{F}_{3^4} = \mathbb{Z}_3(\theta)$ testben, ahol θ minimálpolinomja $x^4 + x + \bar{2}$, számítsuk ki a következőt:

$$\frac{(1 + \theta)^3}{1 + \theta + \theta^2 + \theta^3}.$$

- c) Írassuk ki az $\mathbb{F}_4$ test (minimálpolinomja: $m = x^2 + x + \bar{1} \in \mathbb{Z}_2[x]$) primitív elemének első kilenc hatványát: $\theta, \theta^2, \theta^3, \dots, \theta^9$. (Mit veszünk észre?)
- d) Az a) feladatban lévő $\mathbb{F}_{25}$ fölött számítsuk ki a következő polinom gyökeit:

$$x^{33} + \theta x^{32} + \theta x^{31} + \dots + \theta x^2 + \theta x + \theta \in \mathbb{F}_{25}[x].$$

8. a) Írjunk függvényt, amely kap egy byte-ot, azaz egy 0 és 255 közötti egész számot, és azt konvertálja az AES-ben szereplő $\mathbb{F}_{256}$ testbe, például $75 = 1001011_2 \rightarrow \theta^6 + \theta^3 + \theta + 1 \in \mathbb{F}_{256}$.
- b) Írjuk meg az a)-beli transzformáció inverzét, pl. $\theta^6 + \theta^3 + \theta + 1 \in \mathbb{F}_{256} \rightarrow 1001011_2 = 75$.

9. a) Írjunk függvényt, amely elvégzi az AES *SubBytes* transzformációját egy adott byte-ra. A bemenet és a kimenet egész szám legyen (0 és 255 között).
- b) Írassuk ki az eredményt mind a 256 lehetőségre egy 16×16 -os táblázatba (sorfolytonosan). Ellenőrizzük az eredményt az Internet segítségével (keressünk rá: "Rijndael S-box").
- c) Invertálható a transzformáció? (Azaz minden érték pontosan egyszer fordul elő?)
- d) Van a transzformációnak fixpontja? (Azaz olyan érték, amelynek a képe önmaga?)

10. Implementáljuk a $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ test műveleteit a következők szerint. Az elemeket az együtthatók listájával ábrázoljuk: $a + b\sqrt{2} \rightarrow [\mathbf{a}, \mathbf{b}]$. A függvényeket úgy írjuk meg, hogy ne csak $\mathbb{Q}(\sqrt{2})$ -re, hanem más olyan testbővítésre is működjenek, ahol a primitív elem $\sqrt{2}$ -ként viselkedik, például a fenti 6/a)-ban szereplő $\mathbb{F}_{25}$ -re is. (Attól függően, hogy együtthatólista elemei milyen típusúak.)

- a) Írjunk függvényt, amely kiszámítja két $\mathbb{Q}(\sqrt{2})$ -beli szám összegét, például:

$$(1 + 3\sqrt{2}) + (3 - 2\sqrt{2}) = 4 + \sqrt{2} \quad \longrightarrow \quad \text{sqrt2_add}([1, 3], [3, -2]) == [4, 1].$$

- b) Írjunk függvényt, amely kiszámítja két $\mathbb{Q}(\sqrt{2})$ -beli szám szorzatát.
- c) Írjunk függvényt, amely kiszámítja egy $\mathbb{Q}(\sqrt{2})$ -beli nemnulla szám multiplikatív inverzét.