Finite fields

Exercises

Application of discrete models

Mathematical questions

1. Calculate:
a) $(2+3\sqrt{2})/(3-2\sqrt{2})$ in $\mathbb{Q}(\sqrt{2})$ (i.e. write it in $a+b\sqrt{2}$ form);
b) the multiplicative inverse of $-3+2\sqrt{3}$ in $\mathbb{Q}(\sqrt{3})$;
c) $(1+\sqrt{5})^n$ for $n=1,2,3,4$ in $\mathbb{Q}(\sqrt{5})$.

2. Calculate $(1+\sqrt[3]{2}-\sqrt[3]{2}^2)(3+\sqrt[3]{2}+2\sqrt[3]{2}^2)$ in $\mathbb{Q}(\sqrt[3]{2})$.

3. List all finite fields with at most 20 elements.

4. List all elements of $\mathbb{F}_9$, using the primitive element θ.

5. How many elements does $\mathbb{Z}_3(\theta)$ have if the minimal polynomial of θ is $x^4+x+\overline{2}\in\mathbb{Z}_3[x]$?

6. Calculate the following values in the given finite fields in $a+b\theta$ form, where θ is the primitive element of the field, whose minimal polynomial is the given m polynomial:
a) $(\overline{1}+\overline{2}\theta)(\overline{2}+\overline{3}\theta)$ in $\mathbb{F}_{25}=\mathbb{Z}_5(\theta)$ $(m=x^2-\overline{2})$;
b) the multiplicative inverse of $(\overline{4}+\overline{2}\theta)$ in $\mathbb{F}_{25}$ $(m=x^2-\overline{2})$;
c) the multiplicative inverse of $(\overline{4}+\overline{2}\theta)$ in $\mathbb{F}_{25}$ $(m=x^2-\overline{3})$;
d) $(\overline{5}+\overline{3}\theta)^2/(\overline{6}+\overline{4}\theta)$ in $\mathbb{F}_{49}$ $(m=x^2-\overline{5})$.

Programming exercises

7. Solve the following exercises using Sage operations:

a) Calculate the multiplicative inverse of $\overline{1} + \overline{3}\theta \in \mathbb{F}_{25} = \mathbb{Z}_5(\theta)$, where θ is the root of $x^2 - \overline{2}$.

b) Calculate the following value in $\mathbb{F}_{3^4} = \mathbb{Z}_3(\theta)$, where the minimal polynomial of θ is $x^4+x+\overline{2}$:

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

c) In the field $\mathbb{F}_4$ (minimal polynomial: $m = x^2 + x + \overline{1} \in \mathbb{Z}_2[x]$), print the first nine powers of the primitive element: $\theta, \theta^2, \theta^3, \ldots, \theta^9$. (What do we notice?)

d) Calculate the roots of the following polynomial over the field $\mathbb{F}_{25}$ from exercise a) above:

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

8. a) Write a function that receives a byte, i.e. an integer between 0 and 255, and converts it to $\mathbb{F}_{256}$ of AES, e.g. $75 = 1001011_2 \to \theta^6 + \theta^3 + \theta + 1 \in \mathbb{F}_{256}$.

b) Write the inverse of the above transformation, e.g. $\theta^6 + \theta^3 + \theta + 1 \in \mathbb{F}_{256} \to 1001011_2 = 75$.

9. a) Write a function that performs the *SubBytes* transformation of AES for a given byte. The input and output are integers (between 0 and 255).

b) Print all 256 results in a 16×16 table (in row major order). Check the result using the Internet (search for "Rijndael S-box").

c) Is this transformation invertible? (I.e. do all possible values occur exactly once?)

d) Does this transformation have a fixed point? (I.e. a value whose image is itself?)

10. Implement the field operations of the field $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ as follows. The elements are represented by the list of coefficients: $a + b\sqrt{2} \to$ `[a, b]`. Implement them in such a way that they work for not only $\mathbb{Q}(\sqrt{2})$, but for any other field extension where the primitive element works like $\sqrt{2}$, e.g. $\mathbb{F}_{25}$ from exercise 6/a) above. (Depending on what type of coefficients are given to the functions.)

a) Write a function that calculates the sum of two elements of $\mathbb{Q}(\sqrt{2})$, for example:

$$(1 + 3\sqrt{2}) + (3 - 2\sqrt{2}) = 4 + \sqrt{2} \quad \longrightarrow \quad \texttt{sqrt2\_add([1, 3], [3, -2]) == [4, 1]}.$$

b) Write a function that calculates the product of two elements of $\mathbb{Q}(\sqrt{2})$.

c) Write a function that calculates the multiplicative inverse of a nonzero element of $\mathbb{Q}(\sqrt{2})$.