# Exercises

PhD Course Finite Fields 2012

Aalborg University

**Exercise 1** Compute the composition table for the sum and the multiplication of $\mathbb{F}_7$.

**Exercise 2** Find a primitive element of $\mathbb{F}_{17}$, find a command in Sage to compute a primitive element. Use such element to find all the primitive elements of $\mathbb{F}_{17}$.

**Exercise 3** What is the characteristic of $\mathbb{F}_{p^n}$?

**Exercise 4** Divide $2X^5 + X^4 + 4X + 3 \in \mathbb{F}_5[X]$ by $3X^2 + 1 \in \mathbb{F}_5[X]$.

**Exercise 5** Show that $X^4+X^2+1 \in \mathbb{F}_2$ does not have any roots but it is not irreducible.

**Exercise 6** Compute $X^{-1}$ in $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$. Compute $X^{-1}$ in $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)$ (Using the Extended Euclidean Algorithm and using a command in Maple/Sage).

**Exercise 7** Write all the elements of $\mathbb{F}_{16}$ using the polynomial notation and the multiplicative notation.

**Exercise 8** Verify that the remainder of $2^{340}$ after division by 341 is 1 using the repeat squaring algorithm.

**Exercise 9** Compute $\lambda$ and $\mu$ such that $\lambda 89 + \mu 55 = \gcd(89, 55)$.

**Exercise 10** Learn how to consider finite fields in Sage/Maple. List all the elements of $\mathbb{F}_{16}$.

**Exercise 11** Construct $\mathbb{F}_{16}$ in Sage/Maple considering the construction $\mathbb{F}_2[X]/(f)$ (i.e. using PolynomialRing and quotient or quotient_ring).

**Exercise 12** Let $p$ prime, $a \in \mathbb{F}_p$ and $b \in \mathbb{Z}$ (you choose them). Compute $a^b \in \mathbb{F}_p$ with Maple/Sage using the repeated squaring algorithm. Write an example that shows that Maple/Sage cannot perform this computation without using the repeated squaring algorithm .

**Exercise 13** Construct $\mathbb{F}_9$ using the companion matrix of $X^2+1 \in \mathbb{F}_3[X]$. List all the elements and consider a sum and a multiplication.

**Exercise 14** Compute the inverse of 12345 in the finite field with 12347 elements using Maple/Sage and using the Extended Euclidean Algorithm.

**Exercise 15** Show that the polynomial $f = X^3+X+1 \in \mathbb{F}_2$ is irreducible and compute the inverse of all non-zero elements in $\mathbb{F}_8 = \mathbb{F}_2[X]/(f)$ using the extended euclidean algorithm.

**Exercise 16** Which elements of $\mathbb{F}_3[X]/\langle X^3 + X + 1\rangle$ are units and compute their inverse?, solve it using Sage.

**Exercise 17**

1. Write a program in Maple/Sage that computes a the Conway polynomial $C_{p,n}$ by (improve) exhaustive search, for $p$ prime and $n \geq 1$.

2. Compute an example with your program.

3. Find a command in Sage for computing a Conway polynomial and check your result.

4. Consider your own example for $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ and map an irreducible element of $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^{n'}}$.

5. Map every element of $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^{n'}}$

**Exercise 18** Find the command for computing $\varphi()$ in Sage (Euler $\varphi$ function). Compute an example.

**Exercise 19** Try the implementations and commands for finite fields in Sage. http://sagemath.org/help.html. You may also have a look to the following OLD pages and try some of the commands with your own examples: [Link1] and [Link2]

**Exercise 20** Find the commands for computing the factorization of a polynomial and for checking if a polynomial is irreducible in Sage. Compute several examples.

**Exercise 21**

1. Compute a polynomial $f \in \mathbb{F}_5$ such that $f(0) = 1$, $f(1) = 4$, $f(2) = 5$, $f(3) = 3$, $f(4) = 2$ (using the Lagrange interpolants).

2. Can you compute such polynomial with a command in Maple/Sage?

3. What can you say about the degree of the Lagrange interpolation polynomial?

4. How many polynomials of degree $n-1$ interpolate $n$ points?, How many polynomials of degree $n$ interpolate $n$ points?, How many polynomials of degree $n+1$ interpolate $n$ points? Can you interpolate $n-1$ points with a polynomial of degree less than $n-1$?

**Exercise 22** *(you do not have to do this exercise)* Let $F = \mathbb{F}_{17}$ and $f = 5X^3 + 3X^2 - 4X + 3$, $g = 2X^3 - 5X^2 + 7X - 2 \in F[X]$.

1. Show that $\omega = 2$ is a primitive 8-th root of unity in $F$ and compute $2^{-1}$ in $F$.

2. Compute $h = fg \in F[X]$

3. For $0 \leq j < 8$, compute $\alpha_j = f(\omega^j)$, $\beta_j = g(\omega^j)$ and $\gamma_j = \alpha_j \cdot \beta_j$. Compare $\gamma_j$ to $h(\omega^j)$.

4. Trace the FFT multiplication algorithm to multiply $f$ and $g$.

**Exercise 23** Write a program that will allow $w$ players to share a secret $K$ in a such a way that $t-1$ players cannot recover it but $t$ players can recover it. Consider now the same problem where $K$ is a 20-digits bank account (hint: is any $p$ valid?).

**Exercise 24** Let $F$ be a field, $f \in F[X]$ of degree lower than $t$ and $x_1, \ldots, x_w \in F \setminus \{0\}$ distinct. Determine the set of all interpolation polynomials $g \in F[X]$ of degree less than $t$ with $g(x_i) = f(x_i)$ for $i \in I$ with $I \subset \{1, \ldots, t\}$ with $\#I = t-1$. Let $c \in F$, How many of these $g$ have constant coefficient $c$? (Your answer should imply that the secret sharing scheme is secure).

*Hints for exercises 25–28: check the bibliography, you can find the answers there.*

**Exercise 25** Consider F5 (as in the slides or as in the bibliography) Check that $\mathrm{rec}(\mathrm{emb}(c, m)) = m$ for all $c, m$. Relate F5 with a well-known error correcting code, note that the recovering map is linear. Compute its matrix. What is the code? What can be said about the embedding and recovering process?

**Exercise 26** Implement F5 in Sage/Maple. Consider your own examples.

**Exercise 27** Prove the propositions: "From stegoschemes to codes" and "From codes to stegoschemes ".

**Exercise 28** Let $(\mathrm{emb}, \mathrm{rec})$ be a steganographic scheme of type $[n, k]$. Show that there exists a proper stegoscheme $(\mathrm{emb}', \mathrm{rec})$ fo the same type $[n, k]$ and such that $R_a(\mathrm{emb}', \mathrm{rec}) \leq R_a(\mathrm{emb}, \mathrm{rec})$

**Exercise 29** Explain what is a code and the distance of two elements in $\mathcal{P}(W)$ (in section III-A) in [Kötter-Kschischang].

**Exercise 30** Explain the construction of the Reed-Solomon like codes (or Gabidulin codes) and their parameters in section V-B of [Kötter-Kschischang]. You may implement them in Sage and/or consider an example.

**Exercise 31** Explain the decoding algorithm of Reed-Solomon like codes (or Gabidulin codes) in section V-C of [Kötter-Kschischang]. You may implement it in Sage and/or consider an example.

**Exercise 32** Prove Theorem 8 and Theorem 9 in [Kötter-Kschischang].