# Problem Set 4

*Finite Fields*

## Problem I

Let $F$ be a finite field and $P \in F[X]$.

**1.** Can $P$ be irreducible if it has a root in $F$.

**2.** Conversely, suppose that $\forall x \in F,\ P(x) \neq 0$. Can we conclude that $P$ is irreducible?

## Problem II

**1.** Show there are eight polynomials of degree 3 in $(\mathbb{Z}/2\mathbb{Z})[X]$.

**2.** We consider the polynomials found in question 1. If the constant term of the polynomial is zero then the polynomial is reducible. Explain why.

**3.** Prove that $x^3 + 1$ and $x^3 + x^2 + x + 1$ are both reducible.

**4.** Prove that $x^3 + x + 1$ and $x^3 + x^2 + 1$ are both irreducible.

**5.** Use one of the polynomials of the previous question to construct $\mathbb{F}_8$. What are the eight elements?

**6.** Present the $8 \times 8$ multiplication table in this field.

**7.** Can $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ be equipped with a field structure?

## Problem III

Let $n \geq 2$ be an integer and $F$ a set with $n$ elements.

**1.** What requirement on $n$ do we need to impose so $F$ can be equipped with a field structure. From now on, we suppose $n$ satisfies this requirement.

**2.** Let $\varphi$ be the Euler[1]'s totient function. Show that there are $\varphi(q-1)$ generators of the underlying multiplicative groupe to $F$.

[1] Leonhard Euler, 18th-century Swiss mathematician, worked in every area of mathematics, including analytical geometry, trigonometry and calculus. His name is also associated to the line and the circle joining several special points in a triangle, to the Euler constant (0,5772156649...), to the Euler differential equation, etc.

Leonhard Euler (1707-1783)

## Problem IV

Perform this operation in $\mathbb{F}_{2^8}$

$$32 + 1A \times B4$$

## Problem V

Adapt the Euclid Algorithm to compute the GCD of $x^2 - 1$ and $x^2 + x + 1$ in $\mathbb{R}[x]$.

## Problem VI

**1.** Find the inverse of $Z = x^6 + x^4 + x + 1$ in $\mathbb{F}_{2^8}$.

**2.** What are the bytes corresponding to $Z$ and its inverse?