Feuille de TD2 :

Sandra Marcello

10 mars 2022

1 Exercice : Elliptic curve

Let E be an elliptic curve over F_{11} defined by $y^2 = x^3 + x + 6$.

1. Find the solution of this equation. Considering also the point at infinity we can now consider we are dealing with an elliptic curve. We consider the addition of points, hence this elliptic curve is a abelian group.
2. Is it a cyclic group ?
3. Let $\alpha = (2, 7)$ be a generator. Compute 2α and 3α.

2 Exercice : El Gamal Cipher applied to the previous Elliptic Curve

We use the previous elliptic curve. Let 7 be the private Key (PrivKey). Let α be the choosen generator.

1. Define the public key (PubKey) associated to the previous private key. The ciphering operation is :

$$Enc((x, k), PubKey) = (k\alpha, x + k.PubKey) = (y_1, y_2),$$

with $x \in E$ and $0 \leq k \leq 12$

$$Dec((y_1, y_2), PrivKey) = y_2 - PrivKey.y_1.$$

2. Let $x = (10, 9)$ and $k = 3$, apply the previous defined operations.

3 Fetmat's little theorem

Compute :$7^{2022}[19]$. (see Shanks algorithm).

4 Finite Fields 1

We are in $\mathbb{F}_2[X]$.

1. List the irreducible polynomials of de degre 3 in $\mathbb{F}_2[X]$?
2. Chose an irreducible polynomial f and hence define $\mathbb{F}_2[X]/(f)$
3. Give the multiplication table of this field.
4. Chose an element of the field and compute the inverse using the extend euclidean algorithm. (you can verify your result thanks to the previous question).

5 Finite Fields 2

We are in $\mathbb{F}_2[X]$.

1. Are the following polynomials irreducible in $\mathbb{F}_2[X]$? x^5+x^4+1, x^5+x^3+1
2. Prove the irreducibility of the following polynomial :$x^5 + x^2 + 1$. Hence $\mathbb{F}_2[X]/(x^5 + x^2 + 1)$ is a finite field.
3. Compute $(x^4 + x^2)(x^3 + x + 1)$
4. Find the inverse of $x^3 + x^2$ in $\mathbb{F}_2[X]/x^5 + x^2 + 1$.