Number theory in cryptography

– Exercise set 10 –

The exercises T10.1 a), T10.3 have to be handed in on Tuesday, 7th May 2024, 8:30 at latest.

Theoretical questions

T 10.1 Assume that an elliptic curve E is given by $y^2 = f(x)$ where $f \in k[x]$ is some cubic polynomial and k is some finite field. If we want to count the number of points in $E(k)$ naively, one can loop over every $x \in k$ and check whether $f(x) \in k$ is a square in k.

This exercise explains why detecting squares in finite fields is easy. Namely, given a finite field k with q elements, prove that (Hint: you can use the results seen in the lecture notes, §3.4.1) :

a) If q is odd, then for any element $t \in k^\times$, we have

$$t \text{ is a square} \iff t^{\frac{q-1}{2}} = 1 \in k$$

(and then one can use fast exponentiation as seen at the beginning of the semester).

b) If q is even, then any element $t \in k^\times$ is a square.

T 10.2

a) The projective space of dimension n over a field K, denoted $\mathbb{P}^n_K$, is the set of equivalence classes $[X_0 : \cdots : X_n]$ of tuples $(X_0, \ldots, X_n) \neq (0, ..., 0)$, where we identify scalar multiples: $(X_0, \ldots X_n) \sim (\lambda X_0, \ldots, \lambda X_n)$ for $\lambda \in K^\times$. Such an equivalence class with coordinates in K is called a projective point in $\mathbb{P}^n(K)$. Show that we have a bijection $\mathbb{P}^n(K) \simeq K^n \sqcup \mathbb{P}^{n-1}(K)$. *(Hint: the two pieces can be obtained as $X_n \neq 0$ by taking new coordinates $x_j = X_j/X_n$ and as $X_n = 0$.)*

b) Use this to show that the solutions in the projective plane $\mathbb{P}^2(K)$ of the homogeneous cubic

$$Y^2 Z = X^3 + aXZ^2 + bZ^3$$

correspond to solutions $(x, y) \in K^2$ of the equation $E : y^2 = x^3 + ax + b$ together with a point at infinity $O_E = [0 : 1 : 0] \in \mathbb{P}^2(K)$.

T 10.3 Fix an elliptic curve E over a field k given by an (affine) Weierstrass equation $y^2 = x^3 + ax + b$ (where $a, b \in k$). Assume that $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are two points in $E(k) \setminus \{O_E\}$ (that is, all coordinates belong to k), such that $x_P \neq x_Q$. Let $L_{P,Q}$ be the line going through P, Q.

Then prove directly that $L_{P,Q}$ intersects E in a third[1] point $R = (x_R, y_R)$ which also lies in $E(k)$ (i.e., x_R, y_R both belong to k) and find a formula for x_R in terms of x_P, y_P, x_Q, y_Q, a and b. Hint: you may want to use one of the Viète's formulas.

Programming exercises

P 10.1 Familiarize yourself with the various Sage commands for elliptic curves, see `https://doc.sagemath.org/html/en/reference/arithmetic_curves/index.html`. You should be able to define elliptic curves over finite fields, the real numbers, the complex numbers,

[1] When we count the number of intersection points, we always count the multiplicities.

and the rationals, add points on them, and compute the discriminant; over finite fields $\mathbb{F}_q$, you should be able to compute the number of elements in $E(\mathbb{F}_q)$.