Kryptography Sheet 11

hhu Düsseldorf
Winter term 23/24

Hand in: until monday 11.1.2024, before the lecture starts

Website: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Exercise 1: Order of a point on an elliptic curve

Let E be the elliptic curve over $\mathbb{F}_7$ with equation $E : y^2 = x^3 + x + 3$.

(a) Determine the set $E(\mathbb{F}_7)$ of all points on E.

(b) Which order has the point $P = (4, 1) \in E(\mathbb{F}_7)$?

(c) Show that $E(\mathbb{F}_7) \cong \mathbb{Z}_6$, i.e. $E(\mathbb{F}_7)$ is cyclic of order 6.

Exercise 2: Group structure of elliptic curves

Let E_1 and E_2 be the elliptic curves over $\mathbb{F}_{11}$ with equations $E_1 : y^2 = x^3 + x + 1$ and $E_2 : y^2 = x^3 + x$. Determine the group structure of $E_1(\mathbb{F}_{11})$ and $E_2(\mathbb{F}_{11})$.

Exercise 3: The criterion with discriminants

Let $\mathcal{C}$ be a curve over $\mathbb{C}$ with affine equation $y^2 = x^3 + ax^2 + bx + c$.
Compute the discriminant $\Delta(\mathcal{C})$.
For which c defines the equation $y^2 = x^3 - 4x^2 + c$ an elliptic curve $E(\mathbb{C})$?