Kryptography Sheet 12

hhu Düsseldorf
Winter term 23/24

Hand in: until monday 22.1.2024, before the lecture starts

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

Exercise 1: Points of order 3

What is a geometric condition on P having order 3?

Let E be the elliptic curve with affine equation $y^2 = x^3+ax+b$ over a field k with $\mathrm{char}(k) \neq 2, 3$. Prove: A point $P = (x, y) \in E(k)$ has order 3 if and only if $3x^4 + 6ax^2 + 12bx - a^2 = 0$ holds.

Exercise 2: Number of points on elliptic curves over finite fields

Let $p > 2$, $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}_p$ and

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a = 0, \\ 1, & \exists\, b \in \mathbb{F}_p,\ b \neq 0 :\ b^2 = a, \\ -1, & \text{else} \end{cases}$$

the generalized Legendre symbol. Prove:

(a) $\#E(\mathbb{F}_p) \leq 2p + 1$.

(b) $\#E(\mathbb{F}_p) = p + 1 + \sum\limits_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right)$.

(c) Consider the elliptic curve $E : y^2 = x^3 + x + 1$ over $\mathbb{F}_7$. Compute $\#E(\mathbb{F}_7)$ by using (b).

Exercise 3: Bisection points

Let k be a field with $\mathrm{char}(k) \neq 2, 3$ and $E(k)$ the elliptic curve with affine equation $y^2 = f(x) := x^3 + ax + b$. A point $P \in E(k)$ is called bisection point, if $2P = O$ holds.
Prove: $E(k)$ has one, two or four bisection points.
Is the case of having exactly one bisection point actually occuring?