# Kryptography Last Sheet 13

hhu Düsseldorf
Winter term 23/24

**Hand in: until monday 29.1.2024, before the lecture starts**

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

**Exercise 1:** On the number of points on elliptic curves over $\mathbb{F}_p$

Let $E_1, E_2$ be elliptic curves over $\mathbb{F}_p$, $p > 2$, with affine equations $E_1 : y^2 = x^3 + ax + b$, $E_2 : y^2 = x^3 + ax - b$. Show:

(a) If $p \equiv 3 \bmod 4$, then $\#E_1(\mathbb{F}_p) + \#E_2(\mathbb{F}_p) = 2p + 2$.

(b) Let $p \equiv 3 \bmod 4$ and $E(\mathbb{F}_p)$ an elliptic curve with affine equation $y^2 = x^3 + ax$. For each integer $0 < x < p/2$, either $x$ or $p - x$ is the $x$-coordinate of a point of $E(\mathbb{F}_p)$.

**Exercise 2:** Determination of the possible group structure of an elliptic curve

Determine Hasse's interval for $\#E(\mathbb{F}_{73})$.

We consider the elliptic curve $E : y^2 = x^3 - 2x + 2$ over $\mathbb{F}_{73}$. The point $(-36, 24)$ has order 23. Determine $\#E(\mathbb{F}_{73})$ and the possible group structure of $E$.

**Exercise 3:** Cryptographically safe elliptic curve

The website `http://safecurves.cr.yp.to/`
with the title "SafeCurves: choosing safe curves for elliptic-curve cryptography"
collects information on the security of certain elliptic curves.
Choose one of these curves and give its corresponding curve equation. In which way do you consider this curve as cryptographically safe (according to the lecture)?