EXERCISES FOR WEEK 4

AURORE GUILLEVIC

Exercises

Exercise 1 (3.4)**.** Let M and N be 2×2 matrices with $N = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$. Define $\tilde{N} = \begin{pmatrix} z & -x \\ -y & w \end{pmatrix}$ (this is the adjoint matrix).

(a) Show that $\mathrm{Trace}(M\tilde{N}) = \det(M+N) - \det(M) - \det(N)$.

(b) Use 1 to show that

$$\det(aM + bN) - a^2 \det M - b^2 \det N = ab(\det(M+N) - \det M - \det N)$$

for all scalars a, b. This is the relation used in the proof of Proposition 3.16.

Exercise 2. Consider the elliptic curves

$$E\colon y^2 = x^3 \pm x \text{ over } \mathbb{F}_p \text{ where } p \geq 5 \text{ and with } p \equiv 3 \bmod 4\ .$$

Prove that the order of the curves is $p+1$.

Hint: For $E_+\colon y^2 = x^3 + x$, Define the three sets

$$\begin{aligned} S_1 &= \{x \in \mathbb{F}_p,\ x^3 + x \text{ is a non-zero square}\}, \\ S_2 &= \{x \in \mathbb{F}_p,\ x^3 + x = 0\}, \\ S_3 &= \{x \in \mathbb{F}_p,\ x^3 + x \text{ is not a square}\}. \end{aligned}$$

What can you say about the curve order in terms of the orders of S_1, S_2, S_3? What can you say about the order of S_1 with respect to the order of S_3? Consider $x^3 - x$ instead of $x^3 + x$ for the second curve.

Exercise 3. Consider the elliptic curve

$$E\colon y^2 = x^3 + b \text{ over } \mathbb{F}_p \text{ where } b \neq 0,\ p \geq 5 \text{ and with } p \equiv 2 \bmod 3\ .$$

Prove that the order of the curve is $p+1$.

Hint: In a prime finite field $\mathbb{F}_p$ with $p \equiv 2 \bmod 3$, the order of the multiplicative subgroup $\mathbb{F}_p^*$ is $p-1$ and observe that $3 \nmid p-1$ (3 does not divide $p-1$). There is no subgroup of order 3, and the kernel of the endomorphism $x \mapsto x^3$ in $\mathbb{F}_p^*$ is $\{1\}$. It means that any non-zero element of $\mathbb{F}_p^*$ has exactly one cube root. Moreover $x^3 = 0$ has one root $x = 0$, so finally, $x^3 = c$ has only one root for any $c \in \mathbb{F}_p$.

Rewrite the curve equation as

$$E\colon y^2 - b = x^3\ .$$

Consider the pairs $(y, -y)$ of opposite y-coordinates, with $y \neq 0$ so that $y \neq -y$. How many pairs are they? How many solutions $x \in \mathbb{F}_p$ are they for each pair $(y, -y)$?

Consider $y = 0$ separately.

E-mail address: aurore.guillevic@inria.fr

Date: Week 4.