Elliptic curves / Courbes elliptiques
Cours de M2, mathématiques fondamentales
Université Paris Diderot Paris 7
Marc Hindry (cours), Dominique Bernardi (TD)

EXAMEN DU 6 JANVIER 2016 (ENGLISH VERSION)

The three exercises are independent, apart question 4, exercise 2, where a result from exercise 1 is used.

1. Exercise 1

We consider an isogeny between two elliptic curves $\phi : E_1 \to E_2$ all defined over a field K.

(1) Put $D_\phi := \phi^*(0_{E_2}) - \deg(\phi)(0_{E_1})$. Show that $2D_\phi$ is a principal divisor. Is it true that D_ϕ is always principal?

(2) Suppose now that K is a number field, we denote $\hat{h}$ the Néron-Tate height on E_1 or E_2; show that

$$\hat{h}(\phi(P)) = \deg(\phi)\hat{h}(P).$$

(3) We choose now $E = E_1 = E_2$ defined by $y^2 = x^3+x$ over the field $K = \mathbb{Q}(i)$. Show that

$$\phi(x, y) := (-x, iy)$$

is an automorphism of E. Deduce that $\mathrm{End}(E) = \mathbb{Z}[i]$.
Considering the isogeny $\psi := 1 + \phi$ (i.e. $\psi(P) = P + \phi(P)$), whose degree you will determine, show that the points P and $\phi(P)$ are orthogonal with respect to the Néron-Tate pairing.

2. Exercise 2

Let p be an odd prime number[1]. We consider the elliptic curve E over $\mathbb{F}_p$ with equation

$$y^2 = x^3 + x = f(x)$$

(1) Let $\left(\frac{u}{p}\right)$ denote the Legendre symbol (with value 0 if $u = 0$, value $+1$ if u is a non zero square, and -1 if u is not a square). Recall why

$$|E(\mathbb{F}_p)| = p + 1 + S, \text{ avec } S := \sum_{x\in\mathbb{F}_p} \left(\frac{f(x)}{p}\right) \equiv -A_p \mod p$$

where A_p is the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$.

(2) Show that E is supersingular (resp. ordinary) if $p \equiv 3 \mod 4$ (resp. if $p \equiv 1 \mod 4$). Deduce that, if $p \equiv 3 \mod 4$, then $|E(\mathbb{F}_p)| = p + 1$ and, in particular, $|E(\mathbb{F}_p)| \equiv 0 \mod 4$.

(3) If $p \equiv 1 \mod 4$ show that $E[2] \subset E(\mathbb{F}_p)$ and deduce that $|E(\mathbb{F}_p)| \equiv 0 \mod 4$.

[1] Reminder from algebraic number theory : such a p is the sum of two squares if and only if $p \equiv 1 \mod 4$ and if and only if p is split in the quadratic extension $\mathbb{Q}(i)/\mathbb{Q}$

(4) We know (see exercise 1) that the endomorphism ring of $E/\mathbb{Q}(i)$ is $\mathbb{Z}[i]$. Deduce that, when $p \equiv 1 \mod 4$, the endomorphism ring of $E/\mathbb{F}_p$ is $\mathbb{Z}[i]$. [Indication: use, with justification, the fact that the reduction homomorphism $\mathrm{End}(E/\mathbb{Q}(i)) \to \mathrm{End}(E/\mathbb{F}_p)$ is injective.]
(5) Let Fr_p be the Frobenius of $E/\mathbb{F}_p$, show that it can be identified with $a+bi \in \mathbb{Z}[i] = \mathrm{End}(E)$ such that $a^2+b^2 = p$, with a odd and $|E(\mathbb{F}_p)| = p+1-2a$.
(6) The condition $p = a^2 + b^2$ and a odd détermine a up to sign, can you determine a, specifying, for example, $a \mod 4$?

3. Exercise 3

We study some properties of the elliptic curve E, with origin denoted 0_E and affine equation over $\mathbb{Q}$:

$$y^2 + y = x^3 - 4x$$

(1) Check that the points $P_1 = (0,0)$, $P_2 = (2,0)$ and $P_3 = (-2,0)$ belong to $E(\mathbb{Q})$ and that $P_1 + P_2 + P_3 = 0_E$.
(2) Show that E has good reduction at $p = 2,3,5$ [in fact outside $p = 13$ and 313] and that $\tilde{E}_2(\mathbb{F}_2) \cong \mathbb{Z}/3\mathbb{Z}$, $\tilde{E}_3(\mathbb{F}_3) \cong \mathbb{Z}/7\mathbb{Z}$.
(3) Show that the cardinality of $\tilde{E}_5(\mathbb{F}_5)$ is 9. Do we have $\tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/9\mathbb{Z}$ or $\tilde{E}_5(\mathbb{F}_5) \cong (\mathbb{Z}/3\mathbb{Z})^2$? [[Apologies : the text contained a mistake and was asking : Do we have $\tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/8\mathbb{Z}$ or $\tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\tilde{E}_5(\mathbb{F}_5) \cong (\mathbb{Z}/2\mathbb{Z})^3$?]]
(4) Deduce that $E(\mathbb{Q})_{tor} = \{0_E\}$ and $E(\mathbb{Q}) \cong \mathbb{Z}^r$ with $r \geq 1$.
(5) Show that $E(\mathbb{R})$ has two connected components : the neutral component, which we'll denote $\mathcal{C}_0$ and another component – compact in the affine plane $\mathbb{R}^2$ – which we will denote $\mathcal{C}_1$. Check that P_1 and P_3 belong to $\mathcal{C}_1$ (resp. P_2 to $\mathcal{C}_0$). Deduce that P_1, P_3 do not belong to $2E(\mathbb{Q})$.
(6) Using the duplication formula (which you will justify):

$$x(2P) = \left(\frac{3x^2(P) - 4}{2y(P) + 1}\right)^2 - 2x(P),$$

show that P_2 does not belong to $2E(\mathbb{Q})$. [Indication : you may show that, if $2P = P_2$ then P has integral coordinates, with $x(P)$ even and consider 2-adic valuations.]
(7) Conclude that P_1, P_2, P_3 generate a subgroup isomorphic to $\mathbb{Z}^2$. [Nota : in fact they generate the entire group $E(\mathbb{Q})$ who therefore has rank 2 – but you are not required to show this.]