EXERCISES FOR TUTORIAL 3

AURORE GUILLEVIC

Exercises

- 2.13 on Legendre form $y^2 = x(x-1)(x-\lambda)$
- 2.17 on automorphisms of curves
- 2.19 on endomorphisms being well-defined
- 2.23 on twists of curves
- 2.18 on curves in characteristic 3
- 2.24 on curves in characteristic 2
- 3.1
- 3.2
- 3.4
- 3.5
- 3.7 points of order 3 are inflexion points
- 3.8

Exercise 1 (2.13)**.**

(a) Put the Legendre equation $y^2 = x(x-1)(x-\lambda)$ into Weierstrass form and use this to show that the j-invariant is

$$j = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} .$$

(b) Show that if $j \neq 0, 1728$, then there are six distinct values of λ giving this j, and that if λ is one such value then the full set is

$$\left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\right\}.$$

(c) Show that if $j = 1728$ then $\lambda \in \{-1, 2, 1/2\}$, and if $j = 0$ then $\lambda^2 - \lambda + 1 = 0$.

Exercise 2 (2.17)**.**

(a) Show that $(x, y) \mapsto (x, -y)$ is a group homomorphism from E to itself, for any elliptic curve in Weierstrass form.

(b) Show that $(x, y) \mapsto (\zeta x, -y)$ where ζ is a nontrivial cube root of unity, is an automorphism of the elliptic curve $y^2 = x^3 + B$.

(c) Show that $(x, y) \mapsto (-x, iy)$ where $i^2 = -1$, is an automorphism of the elliptic curve $y^2 = x^3 + Ax$.

Exercise 3 (2.19)**.** Let $\alpha(x, y) = (p(x)/q(x), y \cdot s(x)/t(x))$ be an endomorphism of the elliptic curve E given by $y^2 = x^3 + Ax + B$, where p, q, s, t are polynomials such that p and q have no common root and s and t have no common root.

(a) Using the fact that (x, y) and $\alpha(x, y)$ lie on E, show that

$$\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}$$

for some polynomial $u(x)$ such that q and u have no common root. (Hint: Show that a common root of u and q must also be a root of p.)

(b) Suppose $t(x_0) = 0$. Use the facts that $x^3 + Ax + B$ has no multiple roots and all roots of t^2 are multiple roots to show that $q(x_0) = 0$. This shows that if $q(x_0) \neq 0$ then $\alpha(x_0, y_0)$ is defined.

Exercise 4 (2.23)**.** Let E be given by $y^2 = x^3 + Ax + B$ over a field K and let $d \in K^\times$. The *twist* of E by d is the elliptic curve $E^{(d)}$ given by $y^2 = x^3 + Ad^2x + Bd^3$.

(a) Show that $j(E^{(d)}) = j(E)$.

(b) Show that $E^{(d)}$ can be transformed into E over $K(\sqrt{d})$.

(c) Show that $E^{(d)}$ can be transformed over K to the form $dy_1^2 = x_1^3 + Ax_1 + B$.

Exercise 5 (2.18)**.** Let $\mathbb{K}$ have characteristic 3 and let E be defined by $y^2 = x^3 + a_2x^2 + a_4x + a_6$. The j-invariant in this case is defined to be

$$j = \frac{a_2^6}{a_2^2a_4^2 - a_2^3a_6 - a_4^3}$$

Date: Week 3.

(this formula is false if the characteristic is not 3).

```
F3 = GF(3)
F3a.<a2,a4,a6> = F3[]
E = EllipticCurve(F3a, [0,a2,0,a4,a6])
E.j_invariant().factor()
```

(a) Show that either $a_2 \neq 0$ or $a_4 \neq 0$ (otherwise, the cubic has a triple root, which is not allowed).
(b) Show that if $a_2 \neq 0$, then the change of variables $x_1 = x - (a_4/a_2)$ yields an equation of the form $y_1^2 = x_1^3 + a_2' x_1^2 + a_6'$. This means that we may always assume that exactly one of a_2 and a_4 is 0.
(c) Show that if two elliptic curves $y^2 = x^3 + a_2 x^2 + a_6$ and $y^2 = x^3 + a_2' x^2 + a_6'$ have the same j-invariant, then there exists $\mu \in \overline{\mathbb{K}}^\times$ such that $a_2' = \mu^2 a_2$ and $a_6' = \mu^6 a_6$.
(d) Show that if $y^2 = x^3 + a_4 x + a_6$ and $y^2 = x^3 + a_4' x + a_6'$ are two elliptic curves (in characteristic 3), then there is a change of variables $y \mapsto ay$, $x \mapsto bx + c$, with $a, b \in \overline{\mathbb{K}}^\times$ and $c \in \overline{\mathbb{K}}$, that changes one equation into the other. Note that this is $a_4' x$, not $a_4' x^2$, in the second curve equation.
(e) Observe that if $a_2 = 0$ then $j = 0$ and if $a_4 = 0$ then $j = -a_2^3/a_6$. Show that every element of $\mathbb{K}$ appears as the j-invariant of a curve defined over $\mathbb{K}$.
(f) Show that if two curves have the same j-invariant then there is a change of variables over $\overline{\mathbb{K}}$ that changes one into the other.

Exercise 6 (2.24)**.** Let $\alpha, \beta \in \mathbb{Z}$ be such that $\gcd(\alpha, \beta) = 1$. Assume that $\alpha \equiv -1 \pmod 4$ and $\beta \equiv 0 \pmod 3$2. Let E be given by $y^2 = x(x-\alpha)(x-\beta)$.

(a) Let p be prime. Show that the cubic polynomial $x(x-\alpha)(x-\beta)$ cannot have a triple root mod p.
(b) Show that the substitution

$$x = 4x_1, \;\; y = 8y_1 + 4x_1$$

changes E into E_1, given by

$$E_1 \colon y_1^2 + x_1 y_1 = x_1^3 + \frac{-\beta - \alpha - 1}{4} x_1^2 + \frac{\alpha\beta}{16} x_1 \; .$$

(c) Show that the reduction mod 2 of the equation for E_1 is $y_1^2 + x_1 y_1 = x_1^3 + e x_1^2$ for some $e \in \mathbb{F}_2$. This curve is singular at $(0,0)$.
(d) Let γ be a constant and consider the line $y_1 = \gamma x_1$. Show that if $\gamma^2 + \gamma = e$, then the line intersects the curve in part 3 to order 3, and if $\gamma^2 + \gamma \neq e$ then this line intersects the curve to order 2.
(e) Show that there are two distinct values of $\gamma \in \overline{\mathbb{F}_2}$ such that $\gamma^2 + \gamma = 2$. This implies that there are two distinct tangent lines to the curve E_1 mod 2 at $(0,0)$, as in Exercise 2.20.

Exercise 7 (3.1)**.** Let E be the elliptic curve $y^2 = x^3 + 1$ mod 5.

(a) Compute the division polynomial $\psi_3(x)$.
(b) Show that $\gcd(x^5 - x, \psi_3(x)) = x$.
(c) Use the result of part 2 to show that the 3-torsion points in $E(\mathbb{F}_5)$ are $\{P_\infty, (0,1), (0,-1)\}$.

Exercise 8 (3.2)**.** Let E be an elliptic curve in characteristic 2. Show that $E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$. (Hint: Use the formulas at the end of Section 2.8.)

Exercise 9 (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 10 (3.5)**.** Show that part (6) of Theorem 3.9 holds when α is the endomorphism given by multiplication by an integer m.

Exercise 11 (3.7)**.** Write the equation of the elliptic curve E as $F(x,y,z) = y^2 z - x^3 - Axz^2 - Bz^3 = 0$. Show that a point P on E is in $E[3]$ if and only if

$$\det \begin{pmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_{zx} & F_{zy} & F_{zz} \end{pmatrix} = 0$$

at the point P, where F_{ab} denotes the 2nd partial derivative with respect to a, b. The determinant is called the *Hessian*. For a curve in $\mathbb{P}^2$ defined by an equation $F = 0$, a point where the Hessian is zero is called a *flex* of the curve.

Exercise 12 (3.8)**.** The division polynomials ψ_n were defined for $n \geq 0$. Show that if we let $\psi_{-n} = -\psi_n$, then the recurrence relations preceding Lemma 3.3, which are stated only for $m \geq 2$, hold for all integers m. (Note that this requires verifying the relations for $m \leq -2$ and for $m = -1, 0, 1$.)

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