Elliptic Curves.
Exercises

Elisa Lorenzo García

Exercise 0.1. *Compute the discriminant of the curve* $y^2 + 2xy + 2y = x^3 + 3x^3 + 2x + 1$*. Is is an elliptic curve over* $\mathbb{Q}$*? and over* $\mathbb{F}_7$*?*

Exercise 0.2. *Compute a Legendre model for the elliptic curve* $E : y^2 + 2xy + 2y = x^3 + 3x^3 + 2x + 1/\mathbb{Q}$.

Exercise 0.3. *Show that 3 points on an elliptic curve add to* ∞ *if and only if they are collinear.*

Exercise 0.4. *Determine the doubling and addition formulas for an elliptic curve in characteric 2 and 3.*

Exercise 0.5. *Let* E *be given by* $y^2 = x^3 + Ax + B$ *over a field* K *and let* $d \in K^*$*. 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* $dy^2 = x^3 + Ax + B$.

Exercise 0.6. *Let* k *be a field of characteristic different from 2 or 3. Let us consider an elliptic curve* $E : y^2 = x^3 + ax + b$ *given by a simplified Weierstrass model. Prove that the automorphism group* $Aut(E)$ *has only 2 elements if* $j \neq 0, 1728$*, 4 elements if* $j = 1728$ *and 6 elements if* $j = 0$ *(if the characteristic is 2 or 3 the automorphism group may be larger).*

Exercise 0.7. *Let* k *be a field of characteristic different from 2 or 3. Let us consider an elliptic curve* $E : y^2 = x^3 + ax + b$ *given by a simplified Weierstrass model. Find a Legendre model* $y^2 = x(x-1)(x-\lambda)$.

Starting now with a Legendre model $y^2 = x(x-1)(x-\lambda)$*, find a Weierstrass model. Check that the* j*-invariant is given by*

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

and that the values $\frac{1}{\lambda}$, $1-\lambda$, $\frac{1}{1-\lambda}$, $\frac{\lambda}{\lambda-1}$, $\frac{\lambda-1}{\lambda}$ *produce the same* j*-invariant. Can you find a reason for that?*

Exercise 0.8. *(2-torsion) Let E/k be an elliptic curve given by a simplified Weierstrass model $E: y^2 = x^3 + ax + b$. Find $E[2]$.*

(3-torsion) Let E/k be an elliptic curve given by a simplified Weierstrass model $E: y^2 = x^3 + ax + b$. Find $E[3]$.

Exercise 0.9. *Let E be the elliptic curve $y^2 = x^3 + 1$ mod 5.*

(a) Compute the division polynomial $\psi_3(x)$.

(b) Compute gcd$(x^5 - x, \psi_3(x))$.

(c) Use the result of part (b) to show that the 3-torsion points in $E(\mathbb{F}_5)$ are $\{\infty, (0,1), (0,-1)\}$.

Exercise 0.10. *Let E be an elliptic curve in characteristic 2. Show that the $E[3] \simeq C_3 \oplus C_3$.*

Exercise 0.11. *Let E be an elliptic curve over a field K and let $P \neq \infty$ be a point of exact order n (where n is not divisible by the characteristic of K). Let $Q \in E[n]$. Show that there exists an integer k such that $Q = kP$ if and only if $e_n(P, Q) = 1$.*

Exercise 0.12. *Show that each of the following elliptic curves defined over $\mathbb{Q}$ has the stated torsion group:*

- $y^2 = x^3 - 2$; $\{O\}$.
- $y^2 = x^3 + 8$; $\mathbb{Z}/2\mathbb{Z}$;
- $y^2 = x^3 + 4$; $\mathbb{Z}/3\mathbb{Z}$;
- $y^2 = x^3 + 4x$; $\mathbb{Z}/4\mathbb{Z}$;
- $y^2 = x^3 - 432x + 8208$; $\mathbb{Z}/5\mathbb{Z}$;
- $y^2 = x^3 + 1$; $\mathbb{Z}/6\mathbb{Z}$;

Exercise 0.13. *Let $E/\mathbb{Q}: y^2 = x^3 + 2x - 2$. Prove that E is an elliptic curve. Let $P = (1,1) \in E(\mathbb{Q})$. Compute $2P$. Prove that E has infinetely many rational points.*