

Elliptic Curves. MT 2025. Sheet 1.

Section A

1. (a) Find a birational transformation over $\mathbb{Q}$ between the curves

$$2X^2 - Y^2 = 1$$

and

$$X^2 + Y^2 - 6XY = 1.$$

Hint: both curves are birational to a line.

- (b) Find a birational transformation over $\mathbb{Q}$ between the curves

$$Y^2 = (X + 2)^6(X^3 + 1)$$

and

$$Y^2 = X^3 + 1.$$

- (c) Find a birational transformation over $\mathbb{C}$ between the curves

$$Y^2 = 2X^2$$

and

$$Y^2 = X^2.$$

Is there a birational transformation over $\mathbb{Q}$?

2. For each of the following elliptic curves, find all the points (including, as always, the point at infinity) over $\mathbb{F}_5$. Draw a complete group table in each case and describe each group as a product of cyclic groups.

(a) $Y^2 = X^3 + 2X$. (b) $Y^2 = X^3 + 1$.

3. Show that the point $(2, 4)$ is of order 4 on $Y^2 = X^3 + 4X$, defined over $\mathbb{Q}$.

Section B

4. (a) Let $m \in \mathbb{N}$ be odd or $f_m \in (\mathbb{Q}^*)^2$ (or both). Show that the curve $Y^2 = f_m X^m + f_{m-1} X^{m-1} + \dots + f_0$, where all $f_i \in \mathbb{Q}$ and $f_m \neq 0$,

can be birationally transformed over $\mathbb{Q}$ to a curve of the form

$$Y^2 = X^m + g_{m-1} X^{m-1} + \dots + g_0, \text{ with all } g_i \in \mathbb{Z}.$$

- (b) Birationally transform over $\mathbb{Q}$ the curve $Y^2 = \frac{1}{5}X^3 + 3X^2 + 1$ to a curve of the form $Y^2 = X^3 + AX + B$, where $A, B \in \mathbb{Z}$.

5. Consider the elliptic curve with projective equation

$$X^3 + Y^3 + aZ^3 = 0$$

for some $a \in \mathbb{Q}^\times$ and identity point $(1, -1, 0)$.

Show that the group law satisfies

$$-(x, y, z) = (y, x, z)$$

and

$$[2](x, y, z) = (y(x^3 - az^3), -x(y^3 - az^3), z(y^3 - x^3)).$$

(You might find Lemma 1.43 in lecture notes helpful.)

6. (a) Let $p \equiv 2 \pmod{3}$ be prime and let $A \in \mathbb{F}_p^*$. Show that the number of points (including the point at infinity) on the curve $Y^2 = X^3 + A$ over $\mathbb{F}_p$ is exactly $p + 1$.
- (b) Let $p \equiv 3 \pmod{4}$ be prime and let $B \in \mathbb{F}_p^*$. Show that the number of points (including the point at infinity) on the curve $Y^2 = X(X^2 + B)$ over $\mathbb{F}_p$ is exactly $p + 1$.
7. (a) Show that the point $(2, 0)$ is of order 2 on $Y^2 = (X - 2)(X^2 + X + 1)$.
- (b) Find all $\mathbb{Q}$ -rational points of order 2 and all $\mathbb{C}$ -rational points of order 2 on each of the following elliptic curves: $Y^2 = X(X^2 - 3)$, $Y^2 = X^3 - 7$ and $Y^2 = X(X - 1)(X - 7)$. In each case, find the group structure (expressed as a product of cyclic groups) of the $\mathbb{Q}$ -rational 2-torsion group (that is, the group of all $\mathbb{Q}$ -rational points P such that $2P = \mathbf{o}$).
8. Show that the point $(0, 2)$ is of order 3 on $Y^2 = X^3 + 4$.

Section C

9. Let K be any field with $\text{Char } K \neq 2, 3$, and let $\mathcal{E} : F(X_0, X_1, X_2) = X_1^2 X_2 - (X_0^3 + AX_0 X_2^2 + BX_2^3)$, with $A, B \in K$, be an elliptic curve (N.B. This is just the standard projective form, but with X, Y, Z replaced by X_0, X_1, X_2). Let P be a point on $\mathcal{E}$.
- (a) Show that $3P = \mathbf{o}$ iff. the tangent line to $\mathcal{E}$ at P intersects $\mathcal{E}$ only at P .
- (b) Show that if $3P = \mathbf{o}$ then the 3×3 matrix $(\partial^2 F / \partial X_i \partial X_j(P))$ has determinant 0. [This matrix is called the Hessian matrix].
- (c) Show that there are at most nine 3-torsion points over K .