

Elliptic Curves. HT 2018/19. Sheet 1.

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

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

3(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 $A, B \in \mathbb{Z}$.

4(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 $p + 1$.

5(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 $2P = \mathbf{o}$).

6. Show that the point $(0, 2)$ is of order 3 on $Y^2 = X^3 + 4$.

7(a). Let $Y^2 = (X - \alpha)(X^2 + aX + b)$ be an elliptic curve with $a, b, \alpha \in K$ (characteristic $\neq 2$), and \mathbf{o} = point at infinity, as usual. Show that $(\alpha, 0)$ is a point of order 2. Let x', y' be defined by: $(x', y') = (x, y) + (\alpha, 0)$, and define $T : K \rightarrow K : x \mapsto x'$. Find $t_{11}, t_{12}, t_{21}, t_{22}$ in terms of a, b, α such that: $x' = \mu(x) = (t_{11}x + t_{12}) / (t_{21}x + t_{22})$. Check that $\mu^2 : x \mapsto x$.

(b). Consider $Y^2 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$, with $\alpha_1, \alpha_2, \alpha_3$ distinct, and let T_1, T_2, T_3 be as in (a), but with α replaced by $\alpha_1, \alpha_2, \alpha_3$, respectively. Express each T_i in terms of $x, \alpha_1, \alpha_2, \alpha_3$. Show, directly from expressions, that T_1, T_2, T_3 commute (i.e. $T_1T_2 = T_2T_1$, $T_1T_3 = T_3T_1$ and $T_2T_3 = T_3T_2$), and that $T_1T_2T_3 : x \mapsto x$. Find the fixed points of T_1 and show that they are permuted by T_2 .