

Elliptic Curves. Sheet 2. To be handed in during 3rd Week.

1.

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

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

3.

(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. $T_1T_2 = T_2T_1$, $T_1T_2 = T_2T_1$ 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 .

4. Let K be any field with $\text{Char } K \neq 2, 3$, and let

$$\mathcal{E} : F(X_0, X_1, X_2) = X_1^2X_2 - (X_0^3 + AX_0X_2^2 + BX_2^3), \text{ with } A, B \in K,$$

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 .