

Math 180B - Elliptic Curves

1. Let L be the line $m(x+2)+3$ of slope m going through the point $(-2, 3)$. This line intersects the elliptic curve $E_1 : y^2 = x^3 + 17$ in the point $(-2, 3)$ and in two other points. If all three of these points have rational coordinates, show that the quantity

$$m^4 + 12m^2 + 24m - 12$$

must be the square of a rational number.

2. Let C be the elliptic curve defined by

$$y^2 = (x+7)(x^2+1).$$

This curve contains the points $P = (1, 4)$ and $Q = (3, 10)$. Find the sum of these points using the definition of point addition on elliptic curves.

3. Mordell's theorem states that the group of rational points of an elliptic curve is finitely generated.

- (a) Show that the group $(\mathbb{Q}, +)$ is not finitely generated.
- (b) Show that the group $(\mathbb{Q}^\times, \times)$ is not finitely generated.

4. Show that the only integer point on $y^2 = x^3 - 1$ is $(1, 0)$.