23MAC260 Problem Sheet 7

Week 7 Lectures

Last updated: March 15, 2024

1. Prove that if E is an elliptic curve given by an integral model

$$y^2 = x^3 + ax + b \quad a,\ b \in \mathbb{Z}$$

then the coordinates of any point $(x, y) \in E(\mathbb{Q})$ must be of the form

$$x = \frac{m}{d^2} \quad y = \frac{n}{d^3}$$

for some integers m, n, d with $\gcd(m, d) = \gcd(n, d) = 1$.

2. On the elliptic curve E given by

$$y^2 = x^3 - x + 1$$

find:

(a) a point P with $h_x(P) > 0$;

(b) a point Q with $h_x(Q) > 1$;

(c) a point R with $h_x(R) > 10$.

(Hint: keep doubling!)

3. (Non-examinable) Prove that for an elliptic curve E given by an equation

$$y^2 = x(x^2 + ax + b) \quad (a,\ b \in \mathbb{Q})$$

the Kummer map

$$\delta \ :\ E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

is a group homomorphism. (Remember that the group operation on the right-hand side is multiplication.)