22MAC260 Problem Sheet 6

Week 6 Lectures

Last updated March 11, 2024

1. Let E be the elliptic curve given by
$$y^2 = x^3 + 8.$$
   (a) Find a point of order 2 on E.
   (b) Calculate the discriminant Δ of E, and hence find all primes p for which the curve $\overline{E}_p$ obtained by reducing E mod p is **not** an elliptic curve.
   (c) By reducing E mod p for sufficiently many primes, show that the torsion subgroup $T \subset E(\mathbb{Q})$ has only 2 elements.

2. Use reduction modulo an appropriate prime to compute the torsion subgroup of the curve E given by
$$y^2 = x^3 - 39x + 70.$$

3. Let E be the elliptic curve given by
$$y^2 = x^3 + 3x - 11.$$
   (a) Calculate the order of the point $P = (3, 5)$ on E.
   (b) Use reduction mod 7 and 17 to compute the torsion subgroup $T \subset E(\mathbb{Q})$.

---

4. (Non-examinable) Show that if K is an algebraically closed field of characteristic 2, for any short Weierstrass equation

$$f(x, y) = y^2 - x^3 - ax - b$$

there is a point $(x, y) \in K^2$ where

$$f(x, y) = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0.$$

This explains why we must ignore the prime $p = 2$ in our discussion of reduction mod p.