

MAS 6396 Elliptic Curves

Homework #1

Please hand in your solutions by 09/29/09, 3:37 p.m. Solutions that are handed in later will be graded with 0 points.

Problem 1 (Multiplication by p^p , 5P)

Prove or give a counter-example: if \mathbb{F}_p is a finite prime field and E an elliptic curve defined over \mathbb{F}_p , then $p^p \cdot P = \infty$ for all points $P \in E(\mathbb{F}_{p^p})$. Here ∞ is the point of infinity, i. e. the neutral element in the group $E(\mathbb{F}_{p^p})$.

Problem 2 (Automorphisms, 10P)

Let $E : y^2 = x^3 + B$ be an elliptic curve defined over a field K containing a non-trivial cube root ζ of 1. Show that $(x, y) \mapsto (\zeta x, -y)$ defines an automorphism of E .

Problem 3 (Legendre equation, 10P) Let $\lambda \in \mathbb{C}$ and

$$y^2 = x(x-1)(x-\lambda)$$

be a Legendre equation, defining an elliptic curve E_λ over the complex numbers \mathbb{C} . Compute the j -invariant $j(E_\lambda)$ of E_λ , and find all λ -values for which the $j(E_\lambda) = 0$.

Problem 4 (Torsion points 10P)

Let E be an elliptic curve in characteristic 2. Show that $E[3] \simeq \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$.