

MAS 6396 Elliptic Curves

Homework #1

Please hand in your solutions by September 28, 2007,
7 p.m. Solutions that are handed in later will be graded
with 0 points.

Problem 1 (Multiplication by p) 9 P

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 $p \cdot Q = \mathcal{O}$ for all points Q in $E(\mathbb{F}_p)$. Here \mathcal{O} is the point of infinity, i. e. the neutral element in the group $E(\mathbb{F}_p)$.

Problem 2 (Automorphisms 6 P)

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 (Fast addition 10 P)

Let E be an elliptic curve, and P a point on E . Show that there is a constant $\lambda \in \mathbb{N}$ such that for all $k \in \mathbb{N}$ the sum $k \cdot P = \sum_{i=1}^k P$ can be computed with no more than $\lambda \cdot \log_2(k)$ additions on E .

Problem 4 (Twists 10 P)

Let $E : y^2 = x^3 + Ax + B$ and $E^{(d)} : y^2 = x^3 + Ad^2x + Bd^3$ be elliptic curves that are defined over a field K and where $d \in K^*$. We refer to $E^{(d)}$ as a *twist* of E by d . show that E and $E^{(d)}$ have the same j -invariant and that $E^{(d)}$ can be transformed into E over a quadratic extension of K .