

Math 497A Homework 3
Fall 2008
Due: Friday, September 19

- (1) Let E be an elliptic curve defined over \mathbb{Q} , and let R, S be two rational points on E . We will make the rational points on E into a group in two ways: first by choosing R to be the identity element of our group (and applying the group law accordingly), and then by choosing S to be the identity element of our group.

Show that with these two different choices we get isomorphic groups.

- (2) Let E be an elliptic curve with generalized Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where a_1, \dots, a_6 are rational numbers. Show that there is a linear change of variables of the form

$$x' = u_1x + u_2 \quad y' = u_3y + u_4x + u_5$$

with $u_1, \dots, u_5 \in \mathbb{Q}$ such that after the change of variables the new curve equation is of the form

$$(y')^2 = (x')^3 + px' + q \quad \text{with } p, q \in \mathbb{Q}.$$

- (3) (a) Let E be the elliptic curve over \mathbb{Q} given by

$$y^2 + xy = x^3 + x^2 - 11x.$$

Show that the point $P = \left(\frac{11}{4}, -\frac{11}{8}\right)$ has finite order. This shows that the Lutz-Nagell Theorem does not hold for elliptic curves in generalized Weierstrass form.

- (b) Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve in generalized Weierstrass form defined over \mathbb{Q} , and let $P = (x_0, y_0)$ be a rational torsion point on E . Which primes can occur in the denominator of the coordinates of P ?

- (4) Let $p \geq 2$ be a prime and let C be the cubic curve

$$C : y^2 = x^3 + px.$$

Find all points of finite order in $C(\mathbb{Q})$.

- (5) For each of the following elliptic curves determine all of the points of finite order. Also, determine the structure of the group formed by these points and find generators and relations for the group.

(a) $y^2 = x^3 - 2$

(b) $y^2 = x^3 + 8$

(c) $y^2 = x^3 - 33339627x + 73697852646$

(d) $y^2 + xy - 5y = x^3 - 5x^2$

(e) $y^2 = x^3 - 219x + 1654$

(f) $y^2 + 7xy = x^3 + 16x$

- (6) (*) Let E be an elliptic curve over \mathbb{Q} . Show that $E(\mathbb{Q})[3]$ is either the trivial group or cyclic of order 3.