

Math 497A Homework 4
Fall 2008
Due: Friday, September 26

- (1) Let E be an elliptic curve with equation $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{Z}$, and let p be a prime. Show that $E(p^k)/E(p^{5k})$ is a finite p -group. (A p -group is a group in which every element has p -power order.)
- (2) Let E be an elliptic curve given by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Let p be an odd prime and assume that p does not divide $-4a^3 - 27b^2$.
- (a) Show that by considering a, b modulo p , the curve E becomes an elliptic curve defined over \mathbb{F}_p , the field with p elements.
- (b) Let

$$\rho_p : E(\mathbb{Q}) \rightarrow E(\mathbb{F}_p)$$

be the following map: given a point $(\tilde{x}, \tilde{y}) \in E(\mathbb{Q})$, clear denominators to obtain a point $(x : y : z)$ in projective coordinates with $x, y, z \in \mathbb{Z}$ and such that x, y, z do not have a common divisor > 1 . Then $\rho_p((\tilde{x}, \tilde{y}))$ is defined to be

$$(x \bmod p : y \bmod p : z \bmod p).$$

Also map \mathcal{O} to \mathcal{O} . (The map ρ_p is in fact a homomorphism. You may assume this in this exercise.) Compute the kernel of the map ρ_p .

- (c) Give an example of an elliptic curve (and a prime p) where the kernel of ρ_p is nontrivial. Give an example that shows that ρ_p is not necessarily onto.
- (d) Show that if $P \in E(\mathbb{Q})$ is a point of infinite order, then some multiple of P is in the kernel of ρ_p .
- (3) Let E, p, ρ_p be as in the previous exercise. Restrict the map ρ_p to the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of $E(\mathbb{Q})$. Call the restriction ρ_p again.
- (a) Show that $\rho_p : E_{\text{tors}}(\mathbb{Q}) \rightarrow E(\mathbb{F}_p)$ is a homomorphism.
- (b) Show that if p is an odd prime that does not divide the discriminant $-4a^3 - 27b^2$, then ρ_p is one-to-one.
- (c) Use part (b) to find the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of

$$E : y^2 = x^3 - 219x + 1654.$$

- (4) Let E be the elliptic curve given by the equation

$$E : y^2 = x^3 - 5x$$

What can you say about the cardinality of the following groups/sets:

- (a) $E_{\text{tors}}(\mathbb{Q})$, (b) $E(\mathbb{Q})$, (c) $E(p)$, (d) $E(\mathbb{Q}) - E(p)$, (e) $E(p)/E(p^3)$, (f) $E(\mathbb{Q})/3E(\mathbb{Q})$.
- (5) (a) Let E be the elliptic curve $y^2 = x^3 + 1$. For each prime $p \geq 5$, let $E(\mathbb{F}_p)$ be the group of points having coordinates in the finite field with p elements (together with the point at infinity). Let M_p be the number of points in $E(\mathbb{F}_p)$. Make a general conjecture for the value of M_p when $p \equiv 2 \pmod{3}$, and prove that your conjecture is correct.
- (b) Do the same problem for the elliptic curve $y^2 = x^3 + x$. (You will need a different congruence condition.)