

Math 497A Homework 6
Fall 2008
Due: Friday, October 17

- (1) Let E be an elliptic curve defined over a field K of characteristic $\neq 2$ with equation $E : y^2 = x^3 + ax + b$. Let \overline{K} be an algebraic closure of K . By an **endomorphism** of E we mean a homomorphism $\alpha : E(\overline{K}) \rightarrow E(\overline{K})$ that is given by rational functions. In other words, $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ and there are rational functions (quotients of polynomials) $R_1(x, y), R_2(x, y)$ with coefficients in \overline{K} such that

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)).$$

Let $\text{End}(E)$ be the set of all endomorphisms of E .

- (a) Prove that the addition and multiplication rules

$$(\phi_1 + \phi_2)(P) = \phi_1(P) + \phi_2(P) \quad \text{and} \quad (\phi_1\phi_2)(P) = \phi_1(\phi_2(P))$$

make $\text{End}(E)$ into a ring.

- (b) Explain how $\text{End}(E)$ is different from the endomorphism ring of $E(\overline{K})$ when $E(\overline{K})$ is considered as an abelian group.
(c) Show that the multiplication-by- m map is an endomorphism of E .
(d) Show that any (nontrivial) endomorphism α of E can be written in the form

$$\alpha(x, y) = (r_1(x), r_2(x) \cdot y),$$

with $r_1(x), r_2(x)$ rational functions in x .

- (2) Let E, K be as in Problem 1. Let α be a nontrivial endomorphism of E . By Problem 1(d) we can write $\alpha(x, y)$ as $\alpha(x, y) = (r_1(x), r_2(x)y)$. Write $r_1(x)$ as

$$r_1(x) = p(x)/q(x),$$

with polynomials $p(x)$ and $q(x)$ that do not have a common factor. (If $q(x) = 0$ for some point (x, y) on E , then we assume that $\alpha(x, y) = \mathcal{O}$.) We define the **degree** of α to be

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}.$$

- (a) Now assume that E is defined over a field \mathbb{F}_q , where q is a power of an odd prime. Let $\phi_q(x, y) = (x^q, y^q)$. The map ϕ_q is called the **Frobenius** map. Which points on $E(\overline{K})$ are fixed under ϕ_q ?
(b) Show that ϕ_q is an endomorphism of E of degree q .
(3) Let E, K be as in Problem 1 and let α be a nontrivial endomorphism of E , $\alpha(x, y) = (r_1(x), r_2(x)y)$ with r_1, r_2 rational functions in x . We say that α is **separable** if the derivative $r_1'(x)$ is not identically zero.

Now assume that α is a nonzero separable endomorphism of E . Show that

$$\deg(\alpha) = \# \ker(\alpha),$$

where $\ker(\alpha)$ is the kernel of the homomorphism $\alpha : E(\overline{K}) \rightarrow E(\overline{K})$.

- (4) Using the methods developed in class, find the rank of each of the following elliptic curves:
(a) $y^2 = x^3 + 3x$;
(b) $y^2 = x^3 + 7x$.