

Math 497A Homework 8
Fall 2008
Due: Friday, October 31

- (1) This exercise gives a proof that the multiplication-by- m map has degree m^2 . We will assume $\text{char}(K) \neq 2, 3$, and take an elliptic curve

$$E : y^2 = x^3 + Ax + B.$$

Define division polynomials $\psi_m \in \mathbb{Z}[A, B, x, y]$ inductively as follows:

$$\begin{aligned} \psi_1 &= 1, \psi_2 = 2y, \\ \psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\ \psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad (m \geq 2) \\ 2y\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad (m \geq 3). \end{aligned}$$

It is easy to check that the ψ_{2m} 's are polynomials. Further define polynomials ϕ_m and ω_m by

$$\begin{aligned} \phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\ 4y\omega_m &= \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2. \end{aligned}$$

- (a) Prove that $\psi_m, \phi_m, y^{-1}\omega_m$ (for m odd) and $(2y)^{-1}\psi_m, \phi_m, \omega_m$ (for m even) are polynomials in $\mathbb{Z}[A, B, x, y^2]$. Hence replacing y^2 by $x^3 + Ax + B$, we will treat them as polynomials in $\mathbb{Z}[A, B, x]$.
- (b) As polynomials in x , show that

$$\begin{aligned} \phi_m(x) &= x^{m^2} + \text{lower order terms}, \\ \psi_m(x)^2 &= m^2x^{m^2-1} + \text{lower order terms}. \end{aligned}$$

- (c) Show that $\phi_m(x)$ and $\psi_m(x)^2$ are relatively prime polynomials in $K[x]$ when $-4A^3 - 27B^2 \neq 0$.
- (d) Again assume $-4A^3 - 27B^2 \neq 0$, so E is an elliptic curve. Let $P = (x_0, y_0) \in E$. Show that

$$mP = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3} \right).$$

- (e) Show that multiplication-by- m has degree m^2 .

- (2) Let E be an elliptic curve defined over a field K . Assume $\text{char}(K) \neq 2, 3$, and assume that E is given by

$$E : y^2 = x^3 + Ax + B.$$

Let m be an integer that is coprime to the characteristic of K . Show that

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

- (3) Let E be an elliptic curve defined over a field K of characteristic $p > 3$. Assume that E is given by

$$E : y^2 = x^3 + Ax + B.$$

Show that $E[p^k]$ is isomorphic either to $\mathbb{Z}/p^k\mathbb{Z}$ for all $k \geq 1$ or to $\{\mathcal{O}\}$ for all $k \geq 1$.