Math 418/818

Assignment 9

Due 26 November 2015

1. Let $E/F$ be the elliptic curve defined by the equation $y^2 = x^3 + ax + b$. Show that:
   (a) If $P = (x, y) \in E(F)$ has order 3, then $x$ is a root of the polynomial $\psi_3(x) = 3x^4 + 6ax^2 + 12bx - a^2$.

   (b) Conversely, if $x$ is a root of $\psi_3(x)$, and if $x^3 + ax + b = y^2$ is a square in $F$, then $P = (x, y)$ is a point of order 3 in $E(F)$.

2. Let $E/F$ be an elliptic curve and let $P \in E(F)$ be a point.
   (a) If $n = \text{ord}(P) > \frac{1}{2}(\sqrt{q} + 1)^2$, prove that $E(F_q)$ is cyclic of order $n$.
   (b) If $n = \text{ord}(P) > \frac{1}{m}(\sqrt{q} + 1)^2$ for some $m \geq 2$, what can you say about $|E(F_q)|$?

3. (a) Let $E/F_p$ be the elliptic curve $y^2 = x^3 - x$. Show that if $p \equiv 3 \pmod{4}$ is a prime and $r$ is an odd integer, then $N_{E/F_p} = p^r + 1$.

   (b) Find the structure of $E(F_q)$ for $q = 11^3$.

   (c)* Find the structure of $E(F_p)$ for $p = 41$.

   [Hint for (c)*: Consider the points $P_1 = (6, 13), P_2 = (16, 12) \in E(F_{41})$.]

4. Let $p \equiv 3 \pmod{4}$ be a prime and let $E/F_{p^r}$ be the elliptic curve $y^2 = x^3 - x$. Find the zeta-function of $E/F_p$ and use it to determine $|E(F_{p^r})|$ for all $r \geq 1$.

5. (a) Write a short MAPLE program $\text{numE}(a, b, p)$ which calculates the number of points on the elliptic curve $E_{a,b} : y^2 = x^3 + ax + b$ over $F_p$. (Use the formula given in class.)

   (b) Test this program for $a = 5, b = 3$ and $p = 773$, and check that Hasse’s inequality holds.

   (c)* Write a program $\text{count}(p)$ which returns a list (or a vector) whose $N$-th entry equals the number of $(a, b)$ for which $N_{E_{a,b}/F_p} = N$. (Exclude those $(a,b)$’s for which $E_{a,b}$ is not an elliptic curve.) Test this for $p = 23$ and for $p = 59$. 