MATH 5020 - Elliptic Curves

Homework 4a

Problem 1 Let $E/\mathbb{Q} : y^2 = x^3 + 3$. Find all the points of $\widetilde{E}(\mathbb{F}_7)$ and verify that N_7 satisfies Hasse's bound.

Problem 2 Let $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ and let $p \geq 3$ be a prime of bad reduction for $E/\mathbb{Q}$. Show that $E(\mathbb{F}_p)$ has a unique singular point.

Problem 3 Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in \mathbb{Q}$, distinct, and such that $e_1 + e_2 + e_3 = 0$. Additionally, suppose that $e_1 - e_2 = n^2$ and $e_1 - e_3 = m^2$ are squares. This exercise shows that, under these assumptions, there is a point $P = (x_0, y_0)$ such that $2P = (e_1, 0)$, i.e., P is a point of exact order 4.

(a) Show that $e_1 = \frac{n^2+m^2}{3}$, $e_2 = \frac{m^2-2n^2}{3}$, $e_3 = \frac{n^2-2m^2}{3}$.

(b) Find A and B, in terms of n and m, such that $x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$. (Hint: Sage or PARI can be of great help here.)

(c) Let $p(x) = x^4 - 2Ax^2 - 8Bx + A^2 - 4(x^3 + Ax + B)e_1$. Show that $p(x_0) = 0$ if and only if $x(2P) = e_1$, and therefore $2P = (e_1, 0)$. (Hint: use the multiplication-by-2 formula.)

(d) Express all the coefficients of $p(x)$ in terms of n and m. (Hint: use Sage or PARI.)

(e) Factor $p(x)$ for $(n, m) = (3, 6),\ (3, 12),\ (9, 12), \ldots$.

(f) Guess that $p(x) = (x - a)^2(x - b)^2$ for some a and b. Express all the coefficients of $p(x)$ in terms of a and b.

(g) Finally, compare the coefficients of $p(x)$ in terms of a, b and n, m and find the roots of $p(x)$ in terms of n, m. (Hint: compare first the coefficient of x^3 and then the coefficient of x^2.)

(h) Write $P = (x_0, y_0)$ in terms of n and m.

Problem 4 In this exercise we study the structure of the quotient $G/2G$, where G is a finite abelian group.

(a) Let $p \geq 2$ be a prime and let $G = \mathbb{Z}/p^e\mathbb{Z}$, with $e \geq 1$. Prove that $G/2G$ is trivial if and only if $p > 2$.

(b) Prove that, if $G = \mathbb{Z}/2^e\mathbb{Z}$ and $e \geq 1$, then $G/2G \cong \mathbb{Z}/2\mathbb{Z}$.

(c) Finally, let G be an arbitrary finite abelian group. We define $G[2^\infty]$ to be the 2-primary component of G, i.e.,

$$G[2^\infty] = \{g \in G : 2^n \cdot g = 0 \text{ for some } n \geq 1\}.$$

In other words, $G[2^\infty]$ is the subgroup of G formed by those elements of G whose order is a power of 2. Prove that

$$G[2^\infty] \cong \mathbb{Z}/2^{e_1}\mathbb{Z} \oplus \mathbb{Z}/2^{e_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2^{e_r}\mathbb{Z}$$

for some $r \geq 0$ and $e_i \geq 1$ (here $r = 0$ means $G[2^\infty]$ is trivial). Also show that $G/2G \cong (\mathbb{Z}/2\mathbb{Z})^r$.