MATH 5020 - Elliptic Curves
Homework 4b

Problem 1 As you know, the elliptic curve $y^2 = x^3+2x^2-3x$ satisfies $E(\mathbb{Q})[4] = \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. In previous exercises, it has been shown that $\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt{3})$ and $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In the rest of the exercise, you may also assume the following fact: $E(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, i.e. there are no points of infinite order defined over $\mathbb{Q}$, and the only rational points are in $E(\mathbb{Q})[4]$. (The goal of this exercise is to provide an example for the method of proof of the Weak Mordell-Weil Theorem.)

(a) Let $L = \mathbb{Q}([2]^{-1}E(\mathbb{Q}))$. Show (or notice) that (i) $\mathbb{Q}(E[4]) \subseteq L$ and (ii) there is a point T of order 8 defined over L. In fact, $L = \mathbb{Q}(E[4], T)$.

(b) Show that $\mathbb{Q}(E[4])/\mathbb{Q}$ is a Galois extension, with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, unramified outside 2, 3 and ∞. (You may use the results of Hw 3).

(c) Let $T = (\alpha, \beta)$ and put $F = \mathbb{Q}(T) = \mathbb{Q}(\alpha, \beta)$. Then α is a root of a quartic polynomial (see solutions to Hw 3, part 7) and $\beta^2 = \alpha^3 + 2\alpha^2 - 3\alpha$. Show that, in fact, $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, \beta)$. Conclude that $F/\mathbb{Q}$ is Galois, $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, and the only ramified (finite) primes in $F/\mathbb{Q}$ are 2 and 3. (You may do this using SAGE, PARI, or otherwise).

(d) Let $K = \mathbb{Q}(E[2])$ (which, in this case, is simply $K = \mathbb{Q}$) and put $L = \mathbb{Q}([2]^{-1}E(\mathbb{Q}))$ as before. Show directly (i.e. without using the Weak Mordell Weil Theorem or the Kummer Pairing) that L/K is a finite abelian extension of exponent 2 unramified outside

$$S = \{ \text{ primes of bad reduction for } E/\mathbb{Q} \ \} \cup \{2\} \cup \{\infty\}.$$

Problem 2 Let $E : y^2 = x^3+3$. We have seen in class that $E(\mathbb{Q})_{\text{torsion}} = \{\mathcal{O}\}$, and therefore, $P = (1, 2) \in E(\mathbb{Q})$ is a point of infinite order. (The goal of this exercise is to provide yet another example of the method in the proof of the Weak Mordell-Weil Theorem.)

(a) Let Θ be the subgroup generated by P, i.e. $\Theta = \{[n]P : n \in \mathbb{Z}\}$. Show that $\mathbb{Q}([2]^{-1}\Theta) = \mathbb{Q}([2]^{-1}\{P, \mathcal{O}\})$ and, therefore, $\mathbb{Q}([2]^{-1}\Theta)/\mathbb{Q}$ is a finite extension.

(b) Let $K = \mathbb{Q}(E[2])$. Show that $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$, the symmetric group in three letters.

(c) Let $T = (\gamma, \delta) \in E(\bar{\mathbb{Q}})$ be a point such that $2T = P$. Show that $\mathbb{Q}(T) = \mathbb{Q}(\gamma, \delta) = \mathbb{Q}(\gamma)$. (Use SAGE or PARI).

(d) Let $F = \mathbb{Q}(T)$. Show that $F/\mathbb{Q}$ is not Galois, and the Galois closure of F is a field L such that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_4$, the symmetric group in four letters. Show that $K \subseteq L$. In fact, show that $L = K([2]^{-1}\Theta) = \mathbb{Q}(E[2], T)$. (You may use SAGE, PARI, or other software. For instance, in SAGE you can show that a field K can be embedded in a field L, using the command K.embeddings(L)).

(e) Show that there is a unique normal subgroup H of S_4 such that $|H| = 4$ and S_4/H is isomorphic to S_3. Show that L^H must be K. Hence, L/K is Galois and $\mathrm{Gal}(L/K) \cong H$. Conclude that L/K is a finite abelian extension of exponent 2.

(f) Finally, show that $K([2]^{-1}\Theta)/K$ is unramified outside the primes of bad reduction of $E/\mathbb{Q}$, 2 and ∞. (It suffices to show that $L/\mathbb{Q}$ is only ramified at the appropriate primes. Thus, simply find the discriminant of $L/\mathbb{Q}$.)