Math 5020 - Elliptic Curves
Homework 5

Problem 1. (Silverman's VIII: 8.1, 8.2)

(a) Let K be a number field, E/K and elliptic curve, $m \geq 2$ and integer, $\mathrm{Cl}(K)$ the ideal class group of K and

$$S = \{\nu \in M_K^0 : E \text{ has bad reduction at } \nu\} \cup \{\nu \in M_K^0 : \nu(m) \neq 0\} \cup M_K^\infty.$$

Assuming that $E[m] \subset E(K)$, prove the following quantitative version of the weak Mordell-Weil theorem:

$$\mathrm{rank}_{\mathbb{Z}/m\mathbb{Z}}(E(K)/mE(K)) \leq 2\#S + 2\,\mathrm{rank}_{\mathbb{Z}/m\mathbb{Z}}\left(\mathrm{Cl}(K)[m]\right).$$

(b) For each integer $d \geq 1$, let $E_d/\mathbb{Q}$ be the elliptic curve given by $y^2 = x^3 - d^2x$. Prove that $E_d(\mathbb{Q}) \cong T \times \mathbb{Z}^r$, where T is a finite abelian group and $r = \mathrm{rank}_{\mathbb{Z}}(E_d(\mathbb{Q})) \leq 2\nu(2d)$, where $\nu(N)$ is the number of distinct prime divisors of N.

Problem 2. (a) Let $E/\mathbb{Q}$ be an elliptic curve and let $R \in E(\mathbb{Q})$ be a point of infinite order. Show that if p is a prime of good reduction for E then there is $N > 0$ such that p appears in the denominator of $[N]R$. (Hint: if p is not already in the denominator of R, then $\tilde{R} = R \bmod p$ is well defined in $E(\mathbb{F}_p)$, but $E(\mathbb{F}_p)$ is a finite group.) (Note: Siegel's theorem shows that $E(\mathbb{Z}[\frac{1}{p_1}, \frac{1}{p_2}, \ldots, \frac{1}{p_t}])$ is finite, for any primes $p_1, \ldots, p_t$.)

(b) Let $E/\mathbb{Q} : y^2 = x^3 + 3$ and let $R = (1, 2)$. Find N_1 and N_2 such that 5 appears in the denominators of $[N_1]R$ and 7 appears in the denominators of $[N_2]R$. Verify this with SAGE.

Problem 3. Let $E/\mathbb{Q}$ be an elliptic curve and let $P_1, P_2, \ldots, P_r \in E(\mathbb{Q})$ be rational points. Let $\mathcal{H}$ be the elliptic height matrix associated to $\{P_i\}$, i.e.:

$$\mathcal{H} = (\langle P_i, P_j \rangle)_{1 \leq i \leq r,\ 1 \leq j \leq r}$$

where $\langle P, Q \rangle$ is the Néron-Tate pairing, i.e.

$$\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

and $\hat{h}$ is the canonical height on $E/\mathbb{Q}$. Show the following:

(a) Suppose $\det(\mathcal{H}) = 0$ and $u = (u_1, \ldots, u_r) \in \mathrm{Ker}(\mathcal{H})$. Then the points $\{P_i\}$ are linearly dependent and $\sum_{k=1,r} [u_k] P_k = \mathcal{O}$.

(b) If $\det(\mathcal{H}) \neq 0$ then the points $\{P_i\}$ are linearly independent and $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \geq r$.

(c) Let $E : y^2 = x^3 - 10081x$. Use SAGE (or Magma) to find a minimal set of generators for the subgroup that is spanned by all these points on E:

$$(0,0),\ (-100,90),\ \left(\frac{10081}{100}, \frac{90729}{1000}\right),\ \left(\frac{907137}{6889}, -\frac{559000596}{571787}\right),\ (-17,408),\ \left(\frac{1681}{16}, \frac{20295}{64}\right)$$

$$\left(-\frac{161296}{1681}, \frac{19960380}{68921}\right), \left(\frac{833}{4}, \frac{21063}{8}\right), \left(-\frac{6790208}{168921}, -\frac{40498852616}{69426531}\right).$$