Math 573 Problem Set 7

1. (a) Show that the curve E_{41} is actually an elliptic curve.

(b) Show that $P = (41, 0)$ is a torsion point of order 2 on E_{41}.

(c) Show that $Q = (841, 24360)$ is on E_{41}. Compute $P \oplus Q$ by hand. (Of course check you are correct by using SAGE!)

2. (a) Let A and B be sets and let $f : A \to B$ be a function. Prove that if there exists a function $g : B \to A$ so that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$, then f is a bijection.

(b) Define sets A and B by

$$A = \left\{ (X, Y, Z) \in \mathbb{Q}^3 : \frac{1}{2}XY = N, X^2 + Y^2 = Z^2 \right\}$$
$$B = \left\{ (x, y) \in \mathbb{Q}^2 : y^2 = x^3 - N^2 x, y \neq 0 \right\}.$$

Prove that there is a bijection between A and B given by maps

$$f(X, Y, Z) = \left(-\frac{NY}{X+Z}, \frac{2N^2}{X+Z} \right)$$

and

$$g(x, y) = \left(\frac{N^2 - x^2}{y}, -\frac{2xN}{y}, \frac{N^2 + x^2}{y} \right).$$

(c) Let r be the rank of the elliptic curve E_N. Prove that if $r > 0$ then N must be a congruent number.

3. (a) Show that the point $(-16, 120)$ lies on the curve E_{34}

(b) What triangle does the point $(-16, 120)$ correspond to? What is the area of the triangle?

(c) Show that the point $(-2, 48)$ lies on the curve E_{34}. What triangle does this point correspond to? What is the area of this triangle?

(d) Is 34 a congruent number? Why or why not?

4. **(a)** Let $(G, \oplus)$ be a group and let n be an integer. Prove that the set $G[n] = \{g \in G : nG = 0_G\}$ is a subgroup of G. (Recall, you only need to check this set is nonempty, closed under addition and contains inverses to conclude it is a subgroup!) Conclude that the set $E_N(\mathbb{Q})[n]$ is a subgroup of $E_N(\mathbb{Q})$ for any integer n.

(b) Let P be a rational point on the elliptic curve E_N with $P \notin \{0_{E_N}, (0,0), (\pm N, 0)\}$. Prove that the set $\langle P \rangle = \{nP : n \in \mathbb{Z}\}$ is a subgroup of $E_n(\mathbb{Q})$. Prove that $\langle P \rangle \cong \mathbb{Z}$. (Recall, this means you must define a map from $\langle P \rangle$ to $\mathbb{Z}$ that is a group homomorphism and is bijective.)

5. Prove that the reduction of the elliptic curve E_N modulo p is a nonsingular curve if and only if $p \nmid 2N$.

6. Suppose that for all but finitely many primes p with $p \equiv 3 (\operatorname{mod} 4)$ we have that $p \equiv -1 (\operatorname{mod} n)$ for n an odd number with $3 \nmid n$. Show how this contradicts Dirichlet's theorem on primes in arithmetic progression.

7. Consider the elliptic curve E_{53}.
(a) Compute $a_{E_{53},p}$ for the first 15 primes. You can use SAGE to do this, but be sure you know how to do it by hand if asked.

(b) Prove that we must have $a_{E_N,1} = 1$ for any N.

(c) Use the values computed in part (a) to obtain values for $a_{E_{53},n}$ for $1 \le n \le 20$. Use this to obtain an approximation for $L(E_{53}, 1)$.

(d) Use SAGE to obtain the value of $L(E_N, 1)$. (Note that SAGE is really just giving you a much better approximation!)

(e) Is 53 a congruent number? Be sure to justify your answer.

8. **(a)** Use SAGE to calculate the rank of the elliptic curve E_{41}.

(b) Is 41 a congruent number?

(c) Use SAGE to compute 2 points P and Q on $E_{41}(\mathbb{Q})$ so that $P \notin \langle Q \rangle$. You do not have to prove this fact! (It may be helpful to note that under the command $E.point\_search(n)$, the points you are looking for are referred to as generators. These are the ones that correspond to the copies of "$\mathbb{Z}$" that arise in $E_N(\mathbb{Q})$ when we write $E_N(\mathbb{Q}) \cong E_N(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$.)