Math 573 Problem Set 7

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

It is clear that $y^2 = x^3 - 41^2 x$ is of the appropriate form, so it only remains to show this curve is nonsingular. Let $f(x, y) = y^2 - x^3 + 41^2 x$. We must show there are no points on the curve where both partial derivatives vanish. We have

$$\frac{\partial f}{\partial y} = 2y$$
$$\frac{\partial f}{\partial x} = 3x^2 - 41^2.$$

Thus, the only possible singular points are $(\pm\sqrt{41/3}, 0)$. However, it is easy to check that these points do not actually lie on our curve by plugging them into the equation. Thus the curve is nonsingular and so is an elliptic curve.

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

Using SAGE we compute that $P \oplus P = (0 : 1 : 0) = 0_{E_{41}}$. Alternatively, you could show this using geometry as in class and observing that the tangent line here is vertical so gives a torsion point of order 2.

(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!)

To check that the point is on the curve you just make sure that $24360^2 = 841^3 - 41^2(841)$, which it does. You should use the equations derived in class to compute $P \oplus Q$. It just boils down to plugging in numbers. The answer is $\left(\frac{18081}{400}, -\frac{1023729}{8000}\right)$.

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.

Proof: Let $x, y \in A$ with $f(x) = f(y)$. Applying g to both sides we obtain $x = y$ and so f is injective. Let $b \in B$. We have $f(g(b)) = b$ and so $g(b)$ maps to b under f and thus f is surjective. Hence, 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

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

Proof: One must just check that $f(g(x, y)) = (x, y)$ and $g(f(X, Y, Z)) = (X, Y, Z)$. Both of these are basic calculations using the properties of the sets A and B.

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

Proof: Assume the rank of $E_N > 0$. Recall that this means there is a point $P \in E_N(\mathbb{Q})$ with $P \notin E_N(\mathbb{Q})_{\text{tors}}$. We can use the bijection from part (b) as long as the y-coordinate of P is not 0. Suppose the y-coordinate is 0. Then we have $0 = x(x^2 - N^2)$, i.e., $x = 0$ or $x = \pm N$. But this implies $P \in E_N(\mathbb{Q})_{\text{tors}}$, a contradiction. ■

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

Again, this just amounts to plugging in the value $x = -16$ and $y = 120$ into the equation for E_{34} and verifying it is satisfied.

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

Using the previous problem we see this point corresponds to the triangle with area 34 and sides $\frac{15}{2}, \frac{136}{15}, \frac{353}{20}$.

(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?

To see the point is on the curve one proceeds as above. This point corresponds to the triangle 24, $\frac{17}{6}$, $\frac{145}{6}$ with area 34.

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

The number 34 is a congruent number because in part (b) we have a triangle with rational sides and area 34.

4. (a) Let $(G, \oplus)$ be an abelian 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.

Proof: We begin by observing that $0_G \in G[n]$ since $n0_G = 0_G$ by definition of 0_G. Let $x, y \in G[n]$. Then we have $n(x \oplus y) = (x \oplus y) \oplus \cdots \oplus (x \oplus y) = nx \oplus ny = 0_G$. Thus, $x \oplus y \in G[n]$. Note we needed G abelian here to be able to move the x and y around to group them together. If $x \in G[n]$, then $-x \in G[n]$ since $x \oplus (-x) = 0_G$ and so $nx \oplus n(-x) = n0_G$, i.e., $0_G \oplus n(-x) = 0_G$. The statement about $E_N(\mathbb{Q})[n]$ follows from what we just proved along with the definition of $E_N(\mathbb{Q})[n]$. ■

(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.)

Proof: Recall that we defined $\langle P \rangle = \{nP : n \in \mathbb{Z}\}$. Define a map ϕ from $\langle P \rangle$ to $\mathbb{Z}$ by $nP \mapsto n$. This is clearly a surjective map. It is injective precisely because P is not a torsion point and so if $nP = mP$, then $(n-m)P = 0_G$ which implies $n = m$ (P not torsion). To see the map is a homomorphism, observe that $\phi(0_G P) = 0$ and $\phi(mP \oplus nP) = \phi((m+n)P) = m + n = \phi(nP) + \phi(mP)$. ■

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

Proof: First, recall we are studying whether the equations $2y = 0$ and $3x^2 - N^2 = 0$ have simultaneous solutions when reduced modulo p.
Suppose that $p \mid 2N$. Then either $p = 2$ or $p \mid N$. If $p = 2$, then $\overline{2}y = \overline{0}$

always and so the point $(\overline{0},\overline{0})$ is a singular point. If $p \mid N$, then the equations become $\overline{2}y = \overline{0}$ and $\overline{3}x^2 = \overline{0}$ and again the point $(\overline{0},\overline{0})$ is a singular point. Thus, if $p \mid 2N$ then reduction of E_N is a singular curve.
Suppose now that the reduction of the elliptic curve modulo p is a singular curve modulo p and let (x, y) be a singular point. We must show that $p \mid 2N$. If $p \nmid 2N$ then we must have $y = \overline{0}$ for $\overline{2}y = \overline{0}$, i.e., $p \nmid y$. Thus, $x^3 - N^2x \equiv 0 (\mathrm{mod}\, p)$, i.e., $p \mid x$ or $p \mid (x^2 - N^2$. Since we have a singular point, we also have that $3x^2 - N^2 \equiv 0 (\mathrm{mod}\, p)$. If $p \mid x$, then we obtain that $N^2 \equiv 0 (\mathrm{mod}\, p)$, i.e., $p \mid N$. If $p \mid (x^2 - N^2)$, then we obtain $3N^2 - N^2 \equiv 0 (\mathrm{mod}\, p)$, i.e., $p \mid 2N$. Thus if the reduction is singular, then $p \mid 2N$. ■

6. Suppose that for all but finitely many primes p with $p \equiv 3 (\mathrm{mod}\, 4)$ we have that $p \equiv -1 (\mathrm{mod}\, n)$ 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.

The values listed in the form $(p, a_{E_{53},p})$ are: $(2,0), (3,0), (5,2), (7,0), (11,0), (13,6), (17,2), (19,0), (23,0), (29,-10), (31,0), (37,-2), (41,-10), (43,0), (47,0)$.

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

Proof: Recall that when defining $a_{E_N,n}$ for n not a prime, we specified that $a_{E_N,mn} = a_{E_N,m}a_{E_N,n}$ if $\gcd(m, n) = 1$. Given a prime p with $a_{E_N,p} \neq 0$, we have $a_{E_N,p} = a_{E_N,1\cdot p} = a_{E_N,1}a_{E_N,p}$. Thus, we have $a_{E_N,1} = 1$ for this equation to hold. ■

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

The nonzero values we get are (listed as above): $(1,1), (5,2), (9,-3), (13,6), (17,2)$.
Thus, our approximation is

$$\begin{aligned} L(E_{53},1) &\approx 1 + \frac{2}{5} + \frac{-3}{9} + \frac{6}{13} + \frac{2}{17} \\ &\approx 1.6458. \end{aligned}$$

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

The value SAGE gives is 0.00000000000000.

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

The number 53 is a congruent number because $L(E_{53}, 1) = 0$, so if we believe the Birch and Swinnerton-Dyer conjecture (which we do) we can conclude that 53 is a congruent number.

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

SAGE gives the rank as 2.

(b) Is 41 a congruent number?

Yes, 41 is a congruent number because the rank of $E_{41} > 0$.

(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 $E_N(\mathbb{Q}) \cong E_N(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$.)
Using the point search command we have that the first generator is $(-9, 120)$ and the second generator is $(841, 24360)$.