

# CONGRUENT NUMBERS AND ELLIPTIC CURVES

JIM BROWN

ABSTRACT. These are essentially the lecture notes from a section on congruent numbers and elliptic curves taught in my introductory number theory class at the Ohio State University spring term of 2007. The students in this class were assumed to only have a basic background in proof theory (such as sets and induction) and the material we had covered up to this point in the term (primes, congruences, and quadratic reciprocity). These notes are self-contained modulo basic facts from those subjects and do not assume a background of abstract algebra. Any abstract algebra that is needed is introduced. Calculations used in these notes were performed with SAGE ([6]) as the students in this class used this program throughout the term. Homework exercises are contained in the notes as well. These notes owe a great deal to the wonderful treatment of the subject by Koblitz ([3]).

## 1. INTRODUCTION

One of the traits that sets number theory apart from many other branches of mathematics is the fact that many of the most difficult problems are very easy to state. In fact, the statement of many of these problems can be understood by a student in a high school mathematics class. The beauty of these problems is the modern mathematics that flows from their study. The problem these notes focus on is finding an efficient way to determine if an integer is a congruent number.

**Definition 1.1.** An integer  $N$  is a *congruent number* if there exists a right triangle with rational sides so that the area of the triangle is  $N$ .

**Example 1.2.** The number  $N = 6$  is a congruent number as one sees by considering the  $3 - 4 - 5$  triangle.

Given a positive integer  $N$ , we would like a criterion that is easy to check telling us whether or not  $N$  is a congruent number. We begin our study of congruent numbers in the natural place, namely, right triangles. This is the focus of the following section.

---

*Key words and phrases.* Congruent numbers, elliptic curves.

## 2. PYTHAGOREAN TRIPLES

In this section we study what information we can obtain on congruent numbers from a basic study of right triangles.

**Definition 2.1.** Let  $X$ ,  $Y$ , and  $Z$  be rational numbers. We say  $(X, Y, Z)$  is a *Pythagorean triple* if  $X^2 + Y^2 = Z^2$ . If  $X, Y, Z \in \mathbb{Z}$  and  $\gcd(X, Y, Z) = 1$  we say  $(X, Y, Z)$  is a *primitive Pythagorean triple*.

We begin our study of Pythagorean triples by looking at those triples with  $X, Y, Z \in \mathbb{Z}$ .

**Theorem 2.2.** *Let  $(X, Y, Z)$  be a primitive Pythagorean triple. Then there exists  $m, n \in \mathbb{N}$  so that  $X = 2mn$ ,  $Y = m^2 - n^2$  and  $Z = m^2 + n^2$ . Conversely, any  $m, n \in \mathbb{N}$  with  $m > n$  define a right triangle.*

*Proof.* It is clear that given  $m$  and  $n$  in  $\mathbb{N}$  we obtain a right triangle with integer sides using the given formulas. We need to show that given a right triangle with integer sides  $X$ ,  $Y$ , and  $Z$  that we can find such an  $m$  and  $n$ . Observe that we have  $X^2 + Y^2 = Z^2$  by the Pythagorean theorem. Suppose  $X$  and  $Y$  are both odd. In this case we have  $X^2 \equiv Y^2 \equiv 1 \pmod{4}$  and so  $Z^2 \equiv 2 \pmod{4}$ . However, the squares modulo 4 are 0 and 1. Thus it must be that  $X$  or  $Y$  is even. If both were even we would also obtain that  $2 \mid Z$  which would contradict  $\gcd(X, Y, Z) = 1$ . Assume without loss of generality that  $X$  is even so that  $\frac{X}{2}$  is an integer. Write

$$\left(\frac{X}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 - \left(\frac{Y}{2}\right)^2 = \left(\frac{Z-Y}{2}\right)\left(\frac{Z+Y}{2}\right).$$

If  $p$  is a prime that divides  $\frac{X}{2}$ , then  $p^2 \mid \left(\frac{X}{2}\right)^2$ . Since  $p$  is prime, we have that  $p \mid \left(\frac{Z-Y}{2}\right)$  or  $p \mid \left(\frac{Z+Y}{2}\right)$ . Note that  $p$  cannot divide both for if it did we would have  $p \mid \left(\left(\frac{Z-Y}{2}\right) + \left(\frac{Z+Y}{2}\right)\right) = Z$  and  $p \mid \left(\left(\frac{Z+Y}{2}\right) - \left(\frac{Z-Y}{2}\right)\right) = Y$  which would contradict  $\gcd(X, Y, Z) = 1$ . Thus we obtain that  $p^2 \mid \left(\frac{Z-Y}{2}\right)^2$  or  $p^2 \mid \left(\frac{Z+Y}{2}\right)^2$ . Running through all the primes that divide  $\frac{X}{2}$ , we see that we can write  $\left(\frac{X}{2}\right)^2 = m^2 n^2$  where  $m$  is composed of those primes that divide  $\left(\frac{Z+Y}{2}\right)$  and  $n$  is composed of those primes that divide  $\left(\frac{Z-Y}{2}\right)$ . This gives that  $X = 2mn$ ,  $Y = m^2 - n^2$ , and  $Z = m^2 + n^2$ , as desired.  $\square$

This theorem allows us to construct as many congruent numbers as we want. Namely, for any  $m, n \in \mathbb{N}$  we have that  $N = \frac{1}{2}(2mn)(m^2 - n^2)$  is a congruent number. The following table gives examples of congruent numbers obtained from this process.

TABLE 1. Congruent numbers from Pythagorean triples

m	n	X	Y	Z	N
2	1	4	3	5	6
3	1	6	8	10	24
3	2	12	5	13	30
4	1	8	15	17	60
4	3	24	7	25	84
4	2	16	12	20	96
5	1	10	24	26	120
5	4	40	9	41	180

**Exercise 1.** Prove there are infinitely many distinct congruent numbers.

Of course, we want to deal with triangles with rational sides as well. Suppose we have a right triangle with sides  $X, Y, Z \in \mathbb{Q}$  and area  $N$ . It is easy to see that we can clear denominators and obtain a right triangle with integer sides and congruent number  $a^2N$  where  $a$  is the least common multiple of the denominators of  $X$  and  $Y$ . Thus, we can go from a right triangle with rational sides to a right triangle with integer sides and a new congruent number that is divisible by a square. Conversely, given a right triangle with integer sides  $X, Y$ , and  $Z$  and congruent number  $N = a^2N_0$ , we can form a right triangle with rational sides and congruent number  $N_0$  by merely dividing  $X$  and  $Y$  by  $a$ . Thus, in order to classify congruent numbers it is enough to study positive integers  $N$  that are square-free.

**Example 2.3.** Consider the  $40 - 9 - 41$  triangle given by  $m = 5$  and  $n = 4$ . This triangle has area  $180 = 5 \cdot 6^2$ . Thus, 5 is a congruent number given by a triangle with sides  $\frac{3}{2}$ ,  $\frac{20}{3}$ , and  $\frac{41}{6}$ .

Some further examples are given in the following table.

TABLE 2. Congruent numbers from rational right triangles

X	Y	Z	N
$\frac{3}{2}$	$\frac{20}{3}$	$\frac{41}{6}$	5
$\frac{4}{9}$	$\frac{7}{4}$	$\frac{65}{36}$	14
4	$\frac{15}{2}$	$\frac{17}{2}$	15
$\frac{7}{2}$	12	$\frac{25}{2}$	21
4	$\frac{17}{36}$	$\frac{145}{36}$	34

This method allows us to use the Pythagorean triples given in Theorem 2.2 to produce congruent numbers arising from triangles with rational sides. The difficulty is not in producing lots and lots of congruent numbers, the difficulty is determining if a given integer  $N$  is a congruent number. Using the method described thus far, if we cannot find a triangle with area  $N$ , it does not mean  $N$  is not congruent. It may just be that we have not looked hard enough to find the triangle. For example, the integer 157 is a congruent number. However, the simplest triangle giving area 157 has sides given by

$$X = \frac{6803298487826435051217540}{411340519227716149383203}, Y = \frac{411340519227716149383203}{21666555693714761309610}.$$

Clearly we are going to need a new method to solve this problem.

Before we embark on a new method of attack, we note that we have yet to see why such an  $N$  is called a congruent number. The following theorem answers this question. It says that if  $N$  is a congruent number we obtain three squares of rational numbers that are congruent modulo  $N$ .

**Theorem 2.4.** *Let  $N$  be a square-free positive integer. Let  $X, Y, Z$  be positive rational numbers with  $X < Y < Z$ . There is a 1-1 correspondence between right triangles with sides  $X, Y, Z$  and area  $N$  and numbers  $x \in \mathbb{Q}$  so that  $x, x + N, x - N$  are all squares of rational numbers.*

**Exercise 2.** Prove theorem 2.4.

### 3. FROM CONGRUENT NUMBERS TO ELLIPTIC CURVES

The goal of this section is to see that a triangle with area  $N$  and rational sides  $X, Y, Z$  gives rise to a rational point on an elliptic curve. The terms “rational point” and “elliptic curve” will be defined. Note that  $N$  being a congruent number is equivalent to the existence of rational numbers  $X, Y, Z$  so that

$$(1) \quad Z^2 = X^2 + Y^2$$

$$(2) \quad N = \frac{1}{2}XY.$$

As is often the case when we are stuck on a problem involving finding solutions to equations, we play around with the equations and see where it leads us. If we multiply equation (2) by 4 and add and subtract it from equation (1) we obtain the equations

$$(X + Y)^2 = Z^2 + 4N$$

and

$$(X - Y)^2 = Z^2 - 4N,$$

i.e., we have equations

$$(3) \quad \left(\frac{X + Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 + N$$

and

$$(4) \quad \left(\frac{X - Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 - N.$$

Multiplying equations (3) and (4) together we obtain

$$\left(\frac{X^2 - Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - N^2.$$

Thus, a rational right triangle with area  $N$  produces a rational solution to the equation

$$(5) \quad v^2 = u^4 - N^2,$$

namely  $v = \left(\frac{X^2 - Y^2}{4}\right)$  and  $u = \left(\frac{Z}{2}\right)$ . Multiplying equation (5) by  $u^2$  we obtain

$$(uv)^2 = u^6 - N^2u^2.$$

If we set  $x = u^2 = \left(\frac{Z}{2}\right)^2$  and  $y = uv = \frac{Z(X^2 - Y^2)}{8}$ , then we find that a rational right triangle with area  $N$  produces a rational solution to the equation

$$(6) \quad E_N : y^2 = x^3 - N^2x.$$

This curve is an example of type of curve known as an elliptic curve. We will come back to these curves in subsequent sections. For now we have the following result stating that this process can be reversed and we can use certain points on elliptic curves of the form  $E_N$  to show that  $N$  is a congruent number.

**Proposition 3.1.** *Let  $x_0, y_0 \in \mathbb{Q}$  so that*

$$y_0^2 = x_0^3 - N^2x_0.$$

*Suppose  $x_0$  satisfies:*

- (1)  $x_0$  is the square of a rational number
- (2)  $x_0$  has even denominator
- (3) the numerator of  $x_0$  is relatively prime to  $N$ .

*There exists a right triangle with rational sides and area  $N$  which corresponds to  $x_0$ .*

*Proof.* Let  $x_0 = u^2$  with  $u \in \mathbb{Q}$ . We now reverse the steps used to arrive at the equation  $y^2 = x^3 - N^2x$ . Set  $v = y_0/u$  so that  $v^2 = (x_0^3 - N^2x_0)/x_0 = x_0^2 - N^2$ . Thus,

$$(7) \quad x_0^2 = N^2 + v^2.$$

Let  $t$  be the denominator of  $u$ . Since  $u^2 = x_0$  and  $x_0$  has even denominator, we must have  $2 \mid t$ . It is not difficult to see that  $v^2$  and  $x_0^2$  have the same denominator. Multiplying equation (7) by  $t^2$  we obtain that  $t^2N, t^2v, t^2x_0$  is a Pythagorean triple of integers. In fact, since the numerator of  $x_0$  and  $N$  have no common factor we can conclude that  $\gcd(t^2N, t^2v, t^2x_0) = 1$ . We can now apply Theorem 2.2 to conclude that there exists  $m, n \in \mathbb{N}$  so that  $t^2N = 2mn, t^2v = m^2 - n^2$ , and  $t^2x_0 = m^2 + n^2$ .

Consider now the triple  $X = \frac{2m}{t}, Y = \frac{2n}{t}, Z = 2u$ . This determines a right triangle:

$$\begin{aligned} X^2 + Y^2 &= \frac{4}{t^2}(m^2 + n^2) \\ &= \frac{4}{t^2}(t^2x_0) \\ &= 4x_0 \\ &= (2u)^2 \\ &= Z^2. \end{aligned}$$

The area of this triangle is given by

$$\begin{aligned} \frac{1}{2}XY &= \frac{1}{2} \frac{4mn}{t^2} \\ &= \frac{2mn}{t^2} \\ &= N. \end{aligned}$$

Thus, we have a triangle with rational sides and area  $N$  as claimed.  $\square$

Though we will need the above proposition for a future proof, the following exercise is much easier to prove and is more useful for actually turning points  $x_0, y_0 \in \mathbb{Q}$  satisfying  $y_0^2 = x_0^3 - N^2x_0$  into a triangle with rational sides and area  $N$ .

**Exercise 3.** Define sets  $A$  and  $B$  by

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

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

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

#### 4. A QUICK TOUR OF THE PROJECTIVE PLANE

To properly work with the elliptic curves  $E_N$  we will need what is known as the “point at infinity”. In order to introduce this point at infinity, we require a brief introduction to the projective plane.

Consider the tuples of complex numbers  $(x, y, z)$  with  $(x, y, z) \neq (0, 0, 0)$ . Define an equivalence relation on these tuples by  $(x, y, z) \sim (a, b, c)$  if  $x = \lambda a$ ,  $y = \lambda b$ ,  $z = \lambda c$  for some nonzero  $\lambda \in \mathbb{C}$ . We denote the equivalence class containing  $(x, y, z)$  by  $(x : y : z)$ . The set of equivalence classes of tuples is the projective plane  $\mathbb{P}_{\mathbb{C}}^2$ , i.e.,

$$\mathbb{P}_{\mathbb{C}}^2 = \{(x : y : z) : x, y, z \in \mathbb{C}, (x, y, z) \neq (0, 0, 0)\}.$$

We add and multiply in the projective plane coordinate-wise, i.e., for  $(x_1 : y_1 : z_1), (x_2 : y_2 : z_2) \in \mathbb{P}_{\mathbb{C}}^2$ , one has

$$(x_1 : y_1 : z_1) + (x_2 : y_2 : z_2) = (x_1 + x_2 : y_1 + y_2 : z_1 + z_2)$$

and

$$(x_1 : y_1 : z_1)(x_2 : y_2 : z_2) = (x_1x_2 : y_1y_2 : z_1z_2).$$

**Exercise 4.** Check that componentwise addition and multiplication are well-defined on  $\mathbb{P}_{\mathbb{C}}^2$ .

**Remark 4.1.** Projective planes can be constructed over sets other than the complex numbers. For example,  $\mathbb{P}_{\mathbb{R}}^2$  and  $\mathbb{P}_{\mathbb{Q}}^2$  are both defined analogously to  $\mathbb{P}_{\mathbb{C}}^2$ .

The projective plane is a generalization of the ordinary  $xy$ -plane. If we set  $z = 1$ , then we regain the familiar points  $(x, y)$ . This follows from the fact that in each equivalence class where  $z \neq 0$ , there is a unique point  $(x, y, 1)$  that is obtained by normalizing by multiplication by  $z^{-1}$ . The new points we gain are the ones where  $z = 0$ , i.e., the line at infinity. It is the point  $(0 : 1 : 0)$  on this line that we are interested in as it will be the only point on the line at infinity that lies on the elliptic curve  $E_N$ .

Given a curve  $f(x, y) = 0$ , we can associate to this a curve in the projective plane. A monomial  $x^i y^j$  is said to be of degree  $i + j$ . The degree of  $f(x, y)$  is the maximum of the degrees of all the monomials

occurring in  $f(x, y)$ . Let  $n$  be the degree of  $f(x, y)$ . The homogeneous polynomial  $F(x, y, z)$  associated to  $f(x, y)$  is the polynomial obtained by multiplying each monomial  $x^i y^j$  of  $f(x, y)$  by  $z^{n-i-j}$ . Note each monomial of  $F(x, y, z)$  has degree  $n$ . Given a homogeneous polynomial  $F(x, y, z)$  of degree  $n$ , we obtain a polynomial  $f(x, y)$  by setting  $z = 1$ .

**Example 4.2.** Let  $f(x, y) = y^2 - x^3 + N^2x$ . The associated homogeneous polynomial is given by  $F(x, y, z) = y^2z - x^3 + N^2xz^2$ .

One would like to consider our homogeneous polynomials as functions on the projective plane. Unfortunately this is not well-defined as for  $\lambda \neq 0$ , one has  $(x : y : z) = (\lambda x : \lambda y : \lambda z)$  but  $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z) \neq F(x, y, z)$ . However, we do have  $F(x, y, z) = 0$  if and only if  $F(\lambda x, \lambda y, \lambda z) = 0$ . Thus, we can consider the curves  $F(x, y, z) = 0$  as curves in the projective plane.

**Definition 4.3.** A point  $P = (x_0 : y_0 : z_0)$  is said to be *on the curve*  $F(x, y, z) = 0$  if  $F(x_0, y_0, z_0) = 0$ . We say  $P$  is a *rational point on the curve*  $F(x, y, z) = 0$  if  $P$  is on the curve and  $x_0, y_0, z_0 \in \mathbb{Q}$ . If we write  $C : F(x, y, z) = 0$  for the curve, the set of rational points is denoted  $C(\mathbb{Q})$ .

**Example 4.4.** The points  $(0 : 0 : 1)$  and  $(0 : 1 : 0)$  are on the curve  $E_N : y^2z - x^3 + N^2xz^2 = 0$ .

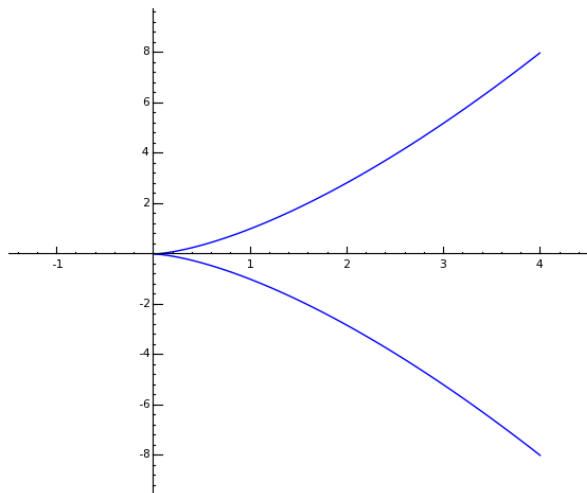
## 5. GENERALITIES ON ELLIPTIC CURVES

In this section we study elliptic curves. We will restrict ourselves to elliptic curves of the form we are interested in for the most part. We begin with a few general definitions before restricting to the case of interest.

**Definition 5.1.** A curve  $F(x, y, z) = 0$  is said to be *singular at a point*  $P = (x_0 : y_0 : z_0)$  if  $P$  is on the curve and  $\frac{\partial F}{\partial x}(x_0, y_0, z_0) = 0$ ,  $\frac{\partial F}{\partial y}(x_0, y_0, z_0) = 0$ , and  $\frac{\partial F}{\partial z}(x_0, y_0, z_0) = 0$ . If  $P$  is on the curve but the curve is not singular at  $P$  it is said to be *nonsingular at  $P$* . A curve that is nonsingular at all the points on the curve is said to be *nonsingular*.

For the curves we are interested in, most of the action will take place in the familiar  $xy$ -plane with only a single point at infinity. In this case one should think of the concept of nonsingular at a point as the familiar concept from calculus of there being a well-defined tangent line at the point.

**Example 5.2.** Consider the curve  $F(x, y, z) = y^2z - x^3 = 0$ . In the  $xy$ -plane we have the following graph:



From the graph of the curve one would expect that it is singular at the point  $(0 : 0 : 1)$  as there is no well-defined tangent line there and nonsingular everywhere else. We now verify this. Observe that  $\frac{\partial F}{\partial x} = -3x^2$  and  $\frac{\partial F}{\partial y} = 2yz$ . The only point on the curve in the  $xy$ -plane where both of these partials vanish is  $(0 : 0 : 1)$ . Thus, the curve is singular at the point  $(0 : 0 : 1)$  and nonsingular at all other points in the  $xy$ -plane. The points on the curve that are not in the  $xy$ -plane occur when  $z = 0$ . Thus, we have only the projective point  $(0 : 1 : 0)$ . We see that  $\frac{\partial F}{\partial z} = y^2$  and since we are looking at the point  $(0 : 1 : 0)$ , we see the curve is nonsingular at the point  $(0 : 1 : 0)$ . Thus,  $F$  is nonsingular at every point except the point  $(0 : 0 : 1)$ .

**Exercise 5.** Let  $N$  be a positive integer and consider the curve  $F(x, y, z) = y^2z - x^3 + N^2xz^2$ . Prove that  $F(x, y, z) = 0$  is a nonsingular curve.

**Definition 5.3.** An *elliptic curve over  $\mathbb{Q}$*  is a nonsingular curve of the form

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_5z^3$$

with  $a_i \in \mathbb{Q}$  for  $1 \leq i \leq 5$ .

We will only be interested in the elliptic curves

$$E_N : y^2z = x^3 - N^2xz^2$$

for  $N$  a positive square-free integer. Note that the exercise above shows that these curves are actually elliptic curves. In fact, you should have seen in that exercise that the only point not in the familiar  $xy$ -plane is the point  $(0 : 1 : 0)$ , which we refer to as the point at infinity. This allows us to work primarily in the  $xy$ -plane with  $z = 1$ . As we will be doing numerous calculations with SAGE for elliptic curves, it is important to note here that the SAGE command to construct the elliptic curve  $E_N$  is as follows:

```
sage: E=EllipticCurve([-N^2,0]); E
Elliptic Curve defined by  $y^2 = x^3 - N^2x$  over Rational
Field
```

One of the reasons that elliptic curves are so special in the world of curves is the fact that we can define an addition on the points of the curve. In particular, we can define an operation  $\oplus$  so that if  $P, Q \in E_N(\mathbb{Q})$  then  $P \oplus Q \in E_N(\mathbb{Q})$ . (This is true for any elliptic curve, but we restrict ourselves to the curves of interest.) In particular, this will make the set  $E_N(\mathbb{Q})$  into an abelian group! We will come back to the notion of an abelian group and give a definition, but first we define the addition on  $E_N(\mathbb{Q})$  and show some basic properties.

The fact that the equation defining  $E_N$  is a cubic implies that any line that intersects the curve must intersect it at exactly three points if we include the point at infinity as well and count a tangent as a double intersection point. This would lead one to guess that defining the point  $P \oplus Q$  is as simple as setting it equal to the third intersection point of the line through  $P$  and  $Q$ . Unfortunately, defining addition in this way would miss the important property of associativity!

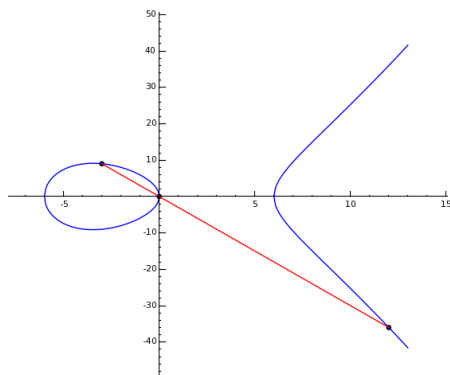


FIGURE 1. Graphical representation that on  $E_6$  one has  $P \oplus Q = (12, -36)$  for  $P = (-3, 9)$  and  $Q = (0, 0)$ .

**Exercise 6.** Define an operation on the points on the curve  $E_N$  by  $P \boxplus Q = R$  where  $R$  is the third intersection point of the line through  $P$  and  $Q$  with  $E_N$  as pictured above. Show with pictures that this addition is not associative. In other words, show that given points  $P_1, P_2, P_3$  on the curve  $E_N$ , that  $P_1 \boxplus (P_2 \boxplus P_3)$  is not necessarily equal to  $(P_1 \boxplus P_2) \boxplus P_3$ .

What turns out to be the correct addition  $P \oplus Q$  is to take the third point of intersection  $R$  of the line through  $P$  and  $Q$  and the elliptic curve and reflect it over the  $x$ -axis as pictured below.

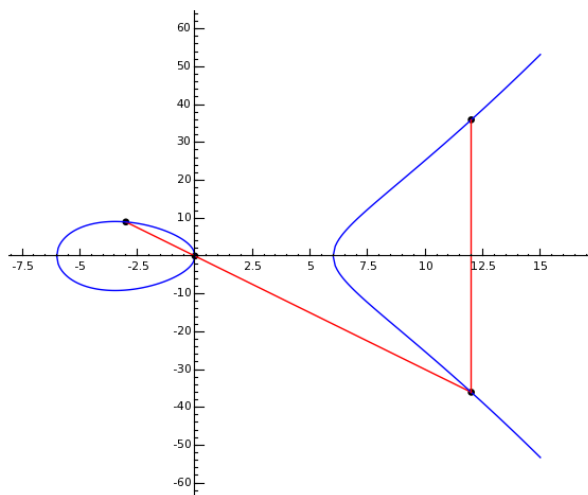


FIGURE 2. Graphical representation that on  $E_6$  one has  $P \oplus Q = (12, 36)$  for  $P = (-3, 9)$  and  $Q = (0, 0)$ .

Note that what we are really doing is finding the point  $R$  and then taking another line through  $R$  and the point at infinity and taking the third intersection point with  $E_N$  as  $P \oplus Q$ . This makes it easy to see that the point at infinity acts as the 0 element. In the future we will often write  $0_{E_N}$  for the point at infinity to reflect this fact.

**Exercise 7.** Convince yourself with pictures that  $P \oplus Q = Q \oplus P$ ,  $P \oplus 0_{E_N} = P$ , and if  $P = (x, y)$ , then  $-P = (x, -y)$ , i.e,  $P \oplus (-P) = 0_{E_N}$ . If you are really brave try to see that the addition is associative as well!

This method shows that given two points  $P$  and  $Q$  on  $E_N$  we get a third point  $P \oplus Q$  on  $E_N$ . What we have not shown yet is given  $P, Q \in E_N(\mathbb{Q})$  that  $P \oplus Q \in E_N(\mathbb{Q})$ . In order to show this we compute

the coordinates of  $P \oplus Q$  in terms of those of  $P$  and  $Q$ . Write  $P = (x(P), y(P))$  and similarly for  $Q$  and  $P \oplus Q$ . Note that if we define  $R$  as above being the third intersection point of the line through  $P$  and  $Q$  with  $E_N$ , then  $x(R) = x(P \oplus Q)$  and  $y(R) = -y(P \oplus Q)$ , so it is enough to determine  $x(R)$  and  $y(R)$  in terms of  $x(P), x(Q), y(P)$  and  $y(Q)$ . We deal with the case  $P \neq Q$  and leave the case of  $P = Q$  as an exercise. Let  $\ell$  be the line through  $P$  and  $Q$ , i.e.,  $\ell$  is the equation  $y - y(P) = m(x - x(P))$  where  $m = \frac{y(P) - y(Q)}{x(P) - x(Q)}$ . Define

$$f(x) = x^3 - N^2x - (m(x - x(P)) + y(P))^2.$$

From the definition of  $\ell$  we see that  $f(x(P)) = f(x(Q)) = f(x(R)) = 0$ . Since  $f(x)$  is a degree three polynomial in  $x$  and we have three roots of  $f(x)$  these are necessarily all the roots. Recall the following basic result from algebra.

**Theorem 5.4.** *Let  $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ . Let  $\alpha_1, \dots, \alpha_n$  be the roots of  $g(x)$ . Then*

$$-a_{n-1} = \sum_{i=1}^n \alpha_i.$$

**Exercise 8.** Prove Theorem 5.4. (Hint:  $g(x) = \prod_{i=1}^n (x - \alpha_i)$ .)

Theorem 5.4 allows us to conclude that

$$x(P) + x(Q) + x(R) = m^2.$$

Thus,  $x(R) = m^2 - x(P) - x(Q)$ . The fact that  $P, Q \in E_N(\mathbb{Q})$  shows that  $m, x(P), x(Q) \in \mathbb{Q}$  and so  $x(P \oplus Q) = x(R) \in \mathbb{Q}$  as well. It remains to calculate  $y(R)$ . For this, we merely plug  $y(R)$  in for  $y$  in the equation of  $\ell$  giving

$$y(R) = m(x(R) - x(P)) + y(P).$$

Since everything on the right hand side of this equation is in  $\mathbb{Q}$ , so is  $y(R)$  and hence  $y(P \oplus Q) = -y(R) \in \mathbb{Q}$ .

**Exercise 9.** Calculate  $2P = P \oplus P$  in terms of  $x(P)$  and  $y(P)$ . Note that the only difference from the above calculation is that in this case  $\ell$  will need to be the tangent line.

**Example 5.5.** Consider the elliptic curve  $E_6$ . It is easy to see that the points  $(0 : 0 : 1)$  and  $(\pm 6 : 0 : 1)$  are on this curve. We can use SAGE to find other nontrivial points. Define the elliptic curve in SAGE as above labelling it as  $E$ . To find points one uses the command:

```
sage: E.point_search(10)
```

The 10 in this command is telling it how many points to search; essentially it is checking all points up to a certain “height”. The only thing we need to remember is that the bigger the number we put in, the longer the process takes. Staying under 20 is generally a good idea. Upon executing this command you will receive a large amount of information. At this point all we are interested in are the points it gives us. Some points it gives us are  $(-2 : 8 : 1)$ ,  $(12 : 36 : 1)$ ,  $(18 : 72 : 1)$ ,  $(50 : 35 : 8)$ , etc. Note that the last point is equivalent to the point  $(\frac{50}{8} : \frac{35}{8} : 1)$  upon normalizing so that  $z = 1$ . We can now use SAGE to add any of these points for us.

```
sage: P = E([-2, 8]); Q = E([12, 36]), R = E([50, 35, 8])
sage: P + Q
(-6 : 0 : 1)
sage: Q + R
(-12 : 36 : 1)
sage: 5 * P
(-1074902978 : 394955797978664 : 1)
(-2015740609 : 90500706122273 : 1)
```

You should compute a couple of these by hand to make sure you are comfortable working with the formulas derived above!

## 6. A SHORT INTERLUDE ON ABSTRACT ALGEBRA

Those familiar with abstract algebra can safely skip this section. For those not familiar we give a brief introduction so that we have a rudimentary vocabulary. In the future if you do study abstract algebra you will be able to come back and see how this theory fits in with what you learn.

**Definition 6.1.** A *group* is a nonempty set  $G$  together with a binary operation  $\oplus$  so that

- (1)  $g \oplus h \in G$  for every  $g, h \in G$ ,
- (2) There exists an element  $0_G \in G$  so that  $g \oplus 0_G = g = 0_G \oplus g$  for every  $g \in G$ ,
- (3) For every  $g \in G$ , there exists  $-g \in G$  so that  $g \oplus (-g) = 0_G = (-g) \oplus g$ ,
- (4)  $(g \oplus h) \oplus k = g \oplus (h \oplus k)$  for every  $g, h, k \in G$ .

If in addition one has that  $g \oplus h = h \oplus g$  for every  $g, h \in G$  we say that  $G$  is an *abelian group*.

**Example 6.2.** (1) The sets  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$  are each abelian groups under the operation  $\oplus = +$  and the identity  $0_G = 0$ .

- (2) The sets  $\mathbb{Q} - \{0\}$ ,  $\mathbb{R} - \{0\}$ , and  $\mathbb{C} - \{0\}$  are all abelian groups with the operation  $\oplus$  being multiplication and the identity  $0_G = 1$ . Note that  $\mathbb{Z} - \{0\}$  is not a group under multiplication as it does not satisfy property (3). For example, 2 would have inverse  $\frac{1}{2} \notin \mathbb{Z}$ .
- (3) Define  $G$  by

$$G = \text{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}.$$

This set is a group under matrix multiplication with identity given by the matrix  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ .

- (4) The set  $G = E_N(\mathbb{Q})$  with  $\oplus$  defined as above is an abelian group with identity element the point at infinity.

As it will be necessary for us to compare groups, we define the appropriate type of map used to study groups.

**Definition 6.3.** A map  $f : G \rightarrow H$  between groups  $(G, \oplus_G)$  and  $(H, \oplus_H)$  is said to be a *group homomorphism* if  $f(g_1 \oplus_G g_2) = f(g_1) \oplus_H f(g_2)$  for every  $g_1, g_2 \in G$ . If  $f$  is also bijective we say that  $f$  is a *group isomorphism*. If there is an isomorphism between two groups  $G$  and  $H$  we say the groups are *isomorphic* and write  $G \cong H$ .

Essentially a group homomorphism is a map that respects the operations of the groups. Two groups that are isomorphic can be thought of as the same group in disguise.

**Definition 6.4.** A subset  $H \subset G$  of a group  $(G, \oplus_G)$  is a *subgroup* if it is also a group under the operation  $\oplus_G$ .

**Exercise 10.** Let  $(G, \oplus)$  be a group and  $H \subset G$ . Show it is enough to prove that  $H$  is nonempty and  $h_1 \oplus (-h_2) \in H$  for every  $h_1, h_2 \in H$  to conclude that  $H$  is a subgroup of  $G$ .

In our study of elliptic curves we will need the following result.

**Theorem 6.5.** *Let  $G$  be a finite group, i.e.,  $\#G < \infty$  and  $H$  a subgroup of  $G$ . Then necessarily  $\#H \mid \#G$ .*

We do not give a proof as it would take us too far astray. However, you can think of it as the generalization of the result that  $\text{ord}_n(a) \mid \phi(n)$ .

**Exercise 11.** If one thinks of Theorem 6.5 as a generalization of the fact that  $\text{ord}_n(a) \mid \phi(n)$ , what is the group  $G$  and what is the subgroup  $H$ ?

**Exercise 12.** Show that the set

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

is a subgroup of  $\mathrm{GL}_2(\mathbb{R})$ .

**Exercise 13.** Let  $(G, \oplus)$  be an abelian group. Let  $n$  be an integer and for  $g \in G$  write  $ng$  to denote the element  $g \oplus g \oplus \cdots \oplus g$  where the addition occurs  $n$  times. Of course if  $n < 0$  we mean the additive inverse of  $g$  is added to itself  $n$  times and if  $n = 0$  we mean the element  $0_G$ . Prove that the set

$$G[n] = \{g \in G : ng = 0_G\}$$

is a subgroup of  $G$ . Define

$$G_{\mathrm{tors}} = \{g \in G : ng = 0_G \text{ for some } n \in \mathbb{Z}\}.$$

Prove that  $G_{\mathrm{tors}}$  is a subgroup of  $G$ .

We will also need the notion of a field. This is a generalization of the familiar sets  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$ .

**Definition 6.6.** Let  $F$  be a nonempty set with two operations  $\oplus$  and  $\odot$  so that the following properties hold:

- (1) The set  $F$  is an abelian group under  $\oplus$ ,
- (2) For every  $a, b \in F$  one has  $a \odot b \in F$ ,
- (3) There exists an element  $1_F \in F$  not equal to  $0_F$  so that for every  $a \in F$  one has  $a \odot 1_F = a = 1_F \odot a$ ,
- (4) For every  $a, b, c \in F$  one has  $(a \odot b) \odot c = a \odot (b \odot c)$ ,
- (5) For every  $a, b \in F$  one has  $a \odot b = b \odot a$ ,
- (6) For every  $a, b, c \in F$  one has  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ .

We then say that  $F$  is a *commutative ring with identity*. If in addition  $F$  satisfies the property that for every element  $a \in F$  not equal to  $0_F$  there exists an element  $a^{-1} \in F$  so that  $a \odot a^{-1} = 1_F$  we say  $F$  is a *field*.

**Example 6.7.** The sets  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$  are all fields under the operations of ordinary addition and multiplication. The set  $\mathbb{Z}$  is a commutative ring with identity but not a field.

**Definition 6.8.** Let  $(R, \oplus_R, \odot_R)$  and  $(S, \oplus_S, \odot_S)$  be commutative rings with identities. A map  $f : R \rightarrow S$  is a *ring homomorphism* if it satisfies the following properties:

- (1)  $f(1_R) = 1_S$ ,
- (2) For every  $r_1, r_2 \in R$  one has  $f(r_1 \oplus_R r_2) = f(r_1) \oplus_S f(r_2)$ ,
- (3) For every  $r_1, r_2 \in R$  one has  $f(r_1 \odot_R r_2) = f(r_1) \odot_S f(r_2)$ .

If in addition  $f$  is bijective we say  $f$  is a *ring isomorphism*. If there is a ring isomorphism between two rings  $R$  and  $S$  we say they are *isomorphic* and write  $R \cong S$ .

The most important example for us will be the field  $\mathbb{Z}/p\mathbb{Z}$  where  $p$  is a prime. We now introduce this set. It is expected that you are familiar with congruence class arithmetic. Let

$$\mathbb{Z}/p\mathbb{Z} = \{\bar{i} : 0 \leq i \leq p-1\}$$

where  $\bar{i} = \{m \in \mathbb{Z} : m \equiv i \pmod{p}\}$ . One can add and multiply these congruence classes by  $\bar{i} \oplus \bar{j} = \overline{i+j}$  and  $\bar{i} \odot \bar{j} = \overline{ij}$ . From now on we use normal multiplication and addition notation for these operations.

**Exercise 14.** Write out addition and multiplication tables for  $\mathbb{Z}/5\mathbb{Z}$ . In other words, write out the results for all possible additions and multiplications of the five elements  $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ , and  $\bar{4}$  of  $\mathbb{Z}/5\mathbb{Z}$ .

The properties showing that  $\mathbb{Z}/p\mathbb{Z}$  is a field follow directly from the properties of congruence class arithmetic. We highlight the only one that requires that we use a prime in our definition.

**Proposition 6.9.** *Let  $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$  with  $\bar{a} \neq \bar{0}$ . There exists  $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$  with  $\bar{b} \neq \bar{0}$  and  $\bar{a}\bar{b} = \bar{1}$ .*

*Proof.* The fact that  $\bar{a} \neq \bar{0}$  implies that  $p \nmid a$ . Thus, it must be the case that  $\gcd(a, p) = 1$ . Hence there exists  $m, n \in \mathbb{Z}$  so that  $am + pn = 1$ . Observe that  $am \equiv 1 \pmod{p}$ . Thus, if we set  $\bar{b} = \bar{m}$  we have the result.  $\square$

The fields  $\mathbb{Z}/p\mathbb{Z}$  are also groups under addition (as all fields are!) It is customary to write  $\mathbb{F}_p$  instead of  $\mathbb{Z}/p\mathbb{Z}$  when we are thinking of  $\mathbb{Z}/p\mathbb{Z}$  as a field instead of just a group. We follow this notation throughout these notes.

## 7. BACK TO ELLIPTIC CURVES

We are now finally able to gather our work thus far and start getting results on congruent numbers.

**Definition 7.1.** Let  $P \in E_N(\mathbb{Q})$ . We say  $P$  is a *torsion point* if there exists  $n \in \mathbb{Z}$  so that  $nP = 0_{E_N}$ . The set of all torsion points is denoted  $E_N(\mathbb{Q})_{\text{tors}}$ . For a particular integer  $n$ , we write  $E_N(\mathbb{Q})[n]$  to denote the set  $\{P \in E_N(\mathbb{Q}) : nP = 0_{E_N}\}$ . If  $P$  is a torsion point and  $n$  is the smallest positive integer so that  $nP = 0_{E_N}$  we say that  $P$  has *order*  $n$ .

Note that exercise 13 shows that  $E_N(\mathbb{Q})[n]$  and  $E_N(\mathbb{Q})_{\text{tors}}$  are both subgroups of  $E_N(\mathbb{Q})$ .

**Exercise 15.** The points in  $E_N(\mathbb{Q})[2]$  are the points so that  $2P = 0_{E_N}$ . Give a geometric description of these points. Use this description to find all such points.

Our goal is to completely determine the group  $E_N(\mathbb{Q})_{\text{tors}}$ . To this end we will prove the following theorem.

**Theorem 7.2.** *For  $N$  a positive square-free integer, one has*

$$E_N(\mathbb{Q})_{\text{tors}} = \{(0 : 1 : 0), (0 : 0 : 1), (\pm N : 0 : 1)\}.$$

The proof of this theorem, and the subsequent results on congruent numbers require us to consider elliptic curves not just defined over  $\mathbb{Q}$  but also elliptic curves defined over the field  $\mathbb{F}_p$ . To accomplish this, we consider the curve

$$\overline{E}_N : y^2 = x^3 - \overline{N}^2 x.$$

We call this the *reduction* of the curve  $E_N$  modulo  $p$ . Note that the  $p$  does not show up in the notation for the reduction. This is standard notation and it is assumed the reader can keep track of what  $p$  is being used.

**Example 7.3.** Consider the curve  $E_7$ . We reduce this curve modulo 3 to obtain  $\overline{E}_7$ . By checking all of the points  $(\bar{i} : \bar{j} : \bar{1})$  and  $(\bar{i} : \bar{j} : \bar{0})$  for  $0 \leq i, j \leq 2$  we find that

$$\overline{E}_7(\mathbb{F}_3) = \{(\bar{0} : \bar{1} : \bar{0}), (\bar{0} : \bar{0} : \bar{1}), (\bar{1} : \bar{0} : \bar{1}), (\bar{2} : \bar{0} : \bar{1})\}.$$

We do need to be careful here as for some primes  $p$  the curve  $\overline{E}_N$  may have singular points!

**Exercise 16.** Show that  $\overline{E}_N$  is nonsingular if and only if  $p \nmid 2N$ .

We also need to make sure that we still have an addition on  $\overline{E}_N$  in order to consider it as an elliptic curve over  $\mathbb{F}_p$ . Let  $P = (x(P), y(P))$  and  $Q = (x(Q), y(Q))$  be points in  $\overline{E}_N(\mathbb{F}_p)$  for  $p$  a prime with  $p \nmid 2N$ . We can define the point  $P \oplus Q = (x(P \oplus Q), y(P \oplus Q))$  by the same formulas used before. Namely, for  $x(P) \neq x(Q)$  we define

$$\begin{aligned} x(P \oplus Q) &= m^2 - x(P) - x(Q) \\ y(P \oplus Q) &= m(x(Q) - x(P)) + y(P) \end{aligned}$$

where we note that  $m = (y(P) - y(Q))(x(P) - x(Q))^{-1}$  makes sense since  $\mathbb{F}_p$  is a field and  $x(P) - x(Q) \neq 0$ . If  $x(P) = x(Q)$  we define  $P \oplus Q = (\bar{0} : \bar{1} : \bar{0})$  as was the case before (this condition forces  $y(P) = -y(Q)$ .)

**Exercise 17.** Check that the equations defining  $2P$  make sense when considered on  $\overline{E}_N(\mathbb{F}_p)$ .

If one wants to work with the reduction  $\overline{E}_N$  in SAGE, one uses the command

```
sage: E= EllipticCurve(FiniteField(p), [-N^2, 0]); E
Elliptic Curve defined by  $y^2 = x^3 - N^2x$  over the finite
field of size  $p$ .
```

Once the curve is defined this way one can work as before with the curve.

Since we are interested in information about  $E_N(\mathbb{Q})$  it may seem pointless to study  $\overline{E}_N(\mathbb{F}_p)$ . However, while we cannot count the number of points in  $E_N(\mathbb{Q})$  easily, we can count the number of points in  $\overline{E}_N(\mathbb{F}_p)$  by merely checking all of the points since there are now only finitely many possibilities! Thus, it is much easier to study  $\overline{E}_N(\mathbb{F}_p)$  and we can use this information at primes  $p \nmid 2N$  to piece information together about  $E_N(\mathbb{Q})$ .

We can define a map from  $\mathbb{P}_{\mathbb{Q}}^2$  to  $\mathbb{P}_{\mathbb{F}_p}^2$  as follows. Let  $(x : y : z) \in \mathbb{P}_{\mathbb{Q}}^2$ . By multiplying by an appropriate integer we can clear the denominators and arrange so that  $\gcd(x, y, z) = 1$ . Thus, we have  $x, y, z \in \mathbb{Z}$  so that  $(x_1 : y_1 : z_1) = (x : y : z)$  and  $\gcd(x_1, y_1, z_1) = 1$ . This means we can always choose  $(x : y : z)$  so that  $x, y, z \in \mathbb{Z}$  and  $\gcd(x, y, z) = 1$ . Define the map by  $(x : y : z) \mapsto (\overline{x} : \overline{y} : \overline{z})$ . Note that this is well defined since we cannot have  $\overline{x}, \overline{y}$ , and  $\overline{z}$  all equal to  $\overline{0}$  since  $\gcd(x, y, z) = 1$ . It is important here that we are able to work in projective coordinates so that we can clear denominators and define this map. Note that by our above definition of addition on  $\overline{E}_N(\mathbb{F}_p)$  we have that the map  $\mathbb{P}_{\mathbb{Q}}^2 \rightarrow \mathbb{P}_{\mathbb{F}_p}^2$  restricts to a group homomorphism  $E_N(\mathbb{Q}) \rightarrow \overline{E}_N(\mathbb{F}_p)$ .

In general one does not have that the map  $\mathbb{P}_{\mathbb{Q}}^2 \rightarrow \mathbb{P}_{\mathbb{F}_p}^2$  is an injection. We have the following proposition determining when two points map to the same point under this map.

**Proposition 7.4.** *Let  $P = (x_1 : y_1 : z_1)$  and  $Q = (x_2 : y_2 : z_2)$ . Then  $P$  and  $Q$  map to the same point in  $\mathbb{P}_{\mathbb{F}_p}^2$  if and only if  $p \mid x_1y_2 - x_2y_1$ ,  $p \mid x_2z_1 - x_1z_2$ , and  $p \mid y_1z_2 - y_2z_1$ .*

*Proof.* First suppose that  $P$  and  $Q$  map to the same point, i.e.,  $\overline{P} = (\overline{x}_1 : \overline{y}_1 : \overline{z}_1) = (\overline{x}_2 : \overline{y}_2 : \overline{z}_2) = \overline{Q}$ . Necessarily we have that  $p$  cannot divide  $x_1, y_1$ , and  $z_1$ . Without loss of generality we assume  $p \nmid x_1$ .

Since  $\overline{P} = \overline{Q}$  we also get that  $p \nmid x_2$ . We then have

$$\begin{aligned} (\overline{x_1 x_2} : \overline{x_1 y_2} : \overline{x_1 z_2}) &= (\overline{x_2} : \overline{y_2} : \overline{z_2}) \\ &= \overline{Q} \\ &= \overline{P} \\ &= (\overline{x_1} : \overline{y_1} : \overline{z_1}) \\ &= (\overline{x_2 x_1} : \overline{x_2 y_1} : \overline{x_2 z_1}). \end{aligned}$$

Since the first  $x$ -coordinates are equal, we must have the  $y$  and  $z$ -coordinates equal as well. Thus,  $p \mid (x_1 y_2 - x_2 y_1)$  and  $p \mid (x_1 z_2 - x_2 z_1)$ . If  $p \mid y_1$ , then  $p \mid y_2$  and so clearly  $p \mid (y_1 z_2 - y_2 z_1)$ . If  $p \nmid y_1$ , we can replace  $x_1$  with  $y_1$  in the above argument to obtain that  $p \mid (y_1 z_2 - y_2 z_1)$ . Suppose now that  $p \mid x_1 y_2 - x_2 y_1$ ,  $p \mid x_2 z_1 - x_1 z_2$ , and  $p \mid y_1 z_2 - y_2 z_1$ . If  $p \nmid x_1$ , then

$$\begin{aligned} \overline{Q} &= (\overline{x_2} : \overline{y_2} : \overline{z_2}) \\ &= (\overline{x_1 x_2} : \overline{x_1 y_2} : \overline{x_1 z_2}) \\ &= (\overline{x_2 x_1} : \overline{x_2 y_1} : \overline{x_2 z_1}) \\ &= \overline{P} \end{aligned}$$

where we have used for example that  $\overline{x_1 y_2} = \overline{x_2 y_1}$  by our assumption. Now assume that  $p \mid x_1$ . Then we must have either  $p \nmid y_1$  or  $p \nmid z_1$ . However, our assumption gives that  $x_2 z_1 \equiv 0 \pmod{p}$  and  $x_2 y_1 \equiv 0 \pmod{p}$ . Since either  $y_1$  or  $z_1$  is nonzero modulo  $p$ , we must have  $x_2 \equiv 0 \pmod{p}$ . Now assume without loss of generality that  $y_1 \not\equiv 0 \pmod{p}$ . Then we have

$$\begin{aligned} \overline{Q} &= (\overline{0} : \overline{y_1 y_2} : \overline{y_1 z_2}) \\ &= (\overline{0} : \overline{y_1 y_2} : \overline{y_2 z_1}) \\ &= \overline{P} \end{aligned}$$

where we have used that  $\overline{y_1 z_2} = \overline{y_2 z_1}$ .  $\square$

**Example 7.5.** It is not true in general that the map  $E_N(\mathbb{Q}) \rightarrow \overline{E}_N(\mathbb{F}_p)$  is a surjection. Consider the reduction of the elliptic curve  $E_{21}$  modulo 5. One can verify that the point  $(\overline{2}, \overline{4})$  is in  $\overline{E}_{21}(\mathbb{F}_5)$  but  $(2, 4)$  is not in  $E_{21}(\mathbb{Q})$ .

**Exercise 18.** Let  $p$  be a prime with  $p \nmid 2N$ . The only 2-torsion points in  $\overline{E}_N(\mathbb{F}_p)$  are the points  $(\overline{0} : \overline{1} : \overline{0})$ ,  $(\overline{0} : \overline{0} : \overline{1})$ , and  $(\pm \overline{N} : \overline{0} : \overline{1})$ .

For  $p \nmid 2N$ , we write  $a_{E_N}(p) = p + 1 - \#\overline{E}_N(\mathbb{F}_p)$ . We can extend the definition by the following rules. Set  $a_{E_N}(p^r) = a_{E_N}(p^{r-1})a_{E_N}(p) -$

$p a_{E_N}(p^{r-2})$  for  $r \geq 2$  and  $p$  a prime with  $p \nmid 2N$  and  $a_{E_N}(mn) = a_{E_N}(m)a_{E_N}(n)$  for relatively prime  $m$  and  $n$  with  $\gcd(mn, 2N) = 1$ .

**Lemma 7.6.** *Let  $p$  be a prime with  $p \nmid 2N$  and  $p \equiv 3 \pmod{4}$ . Then  $a_{E_N}(p) = 0$ .*

*Proof.* We begin by noting that  $(\bar{0} : \bar{1} : \bar{0}), (\bar{0} : \bar{0} : \bar{1}), (\pm\bar{N} : \bar{0} : \bar{1})$  are all in  $\overline{E}_N(\mathbb{F}_p)$  by exercise 18. These points are all distinct because of the fact that  $p \nmid 2N$ . We now count the points  $(x, y) \in \overline{E}_N(\mathbb{F}_p)$  with  $x \neq \bar{0}, \pm\bar{N}$ . Note that this is enough as the only point  $(x : y : z)$  in  $\overline{E}_N(\mathbb{F}_p)$  with  $z = \bar{0}$  is  $(\bar{0} : \bar{1} : \bar{0})$ . Thus there are  $p - 3$  possible values for  $x$ . We pair the remaining values of  $x$  off as  $\{x, -x\}$ . We claim that  $x \neq -x$ . It is at this point that we use that  $x \neq \bar{0}, \pm\bar{N}$  for if  $x = -x$ , then  $2x = \bar{0}$  which implies that  $x$  must be a 2-torsion point. By exercise 18 we must have  $x = \bar{0}, \pm\bar{N}$ , a contradiction. Thus we have that each set  $\{x, -x\}$  has cardinality 2. Let  $f(x) = x^3 - \bar{N}^2 x$ . It is clear that  $f(x)$  is an odd function, i.e.,  $f(x) = -f(-x)$  for all  $x$ . The fact that  $p \equiv 3 \pmod{4}$  gives that  $\left(\frac{-1}{p}\right) = -1$ , i.e.,  $-1$  is not a quadratic residue modulo  $p$ . Suppose  $f(x)$  is not a square modulo  $p$ , i.e.,  $\left(\frac{f(x)}{p}\right) = -1$ . Thus,  $\left(\frac{-f(x)}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{f(x)}{p}\right) = 1$ , so  $-f(x)$  is a square modulo  $p$ . Similarly, if  $f(x)$  is a square then  $-f(x)$  is not a square. This shows that for each pair  $\{x, -x\}$  we obtain a pair of points in  $\overline{E}_N(\mathbb{F}_p)$ , either  $(x, \pm\sqrt{f(x)})$  or  $(-x, \pm\sqrt{-f(x)})$  depending upon whether  $f(x)$  or  $-f(x)$  is a quadratic residue modulo  $p$ . Thus, for the  $p - 3$  different values of  $x$  we obtain  $(p - 3)/2$  pairs of points  $\{x, -x\}$  which give rise to  $p - 3$  distinct points in  $\overline{E}_N(\mathbb{F}_p)$ . Combining these with the four 2-torsion points we already had gives  $a_{E_N}(p) = (p + 1) - (p + 1) = 0$ , as claimed.  $\square$

This lemma as well as Proposition 7.4 are both key ingredients in the proof of Theorem 7.2. We will also need the following theorem known as Dirichlet's theorem on primes in arithmetic progressions.

**Theorem 7.7.** *Let  $a, b \in \mathbb{Z}$  with  $\gcd(a, b) = 1$ . The arithmetic progression*

$$a, a + b, a + 2b, \dots$$

*contains infinitely many primes.*

*Proof.* (of Theorem 7.2) Let  $P$  be a point of  $E_N(\mathbb{Q})_{\text{tors}}$  that is not  $\{(0 : 1 : 0), (0 : 0 : 1), (\pm N : 0 : 1)\}$ . Using Exercise 18 we see that  $P$  cannot have order 2. Let  $m$  be the order of  $P$ .

We claim that  $E_N(\mathbb{Q})_{\text{tors}}$  either has a subgroup of odd order or a subgroup of order 8. First, if  $m$  is odd then clearly  $\langle P \rangle$  is a subgroup

of  $E_N(\mathbb{Q})_{\text{tors}}$  of odd order. So we can assume that  $m$  is even. If  $m$  is not a power of 2, say  $m = 2^a b$  with  $a, b \in \mathbb{Z}$ ,  $b > 1$  and odd, then  $\langle aP \rangle$  is a subgroup of  $E_N(\mathbb{Q})_{\text{tors}}$  of order  $b$ , i.e., of odd order. Thus we can assume that  $m$  is a power of 2. Since  $P$  does not have order 2 we know that  $m = 2^j$  with  $j \geq 2$ . Suppose  $P$  has order 4 and let  $Q = (N : 0 : 1)$ . One can check that the set  $\{(0 : 1 : 0), Q, P, 2P, 3P, P \oplus Q, 2P \oplus Q, 3P \oplus Q\}$  is a subgroup of  $E_N(\mathbb{Q})_{\text{tors}}$  and has order 8. (Note you must show this is a subgroup and none of the elements are equal to each other!) If  $j \geq 3$ , then we can write  $m = 8b$  with  $b \geq 1$ . In this case we have that  $\langle bP \rangle$  is a subgroup of  $E_N(\mathbb{Q})_{\text{tors}}$  of order 8. Thus, in all cases we see that  $E_N(\mathbb{Q})_{\text{tors}}$  contains either a subgroup of odd order or a subgroup of order 8. Denote this subgroup by  $\mathcal{S}$  and enumerate the points as  $\mathcal{S} = \{P_1, \dots, P_{\#\mathcal{S}}\}$ .

Our goal is to show that  $\mathcal{S}$  injects into  $\overline{E}_N(\mathbb{F}_p)$  for all but finitely many primes  $p$ . Write the points of  $\langle P \rangle$  as  $P_i = (x_i : y_i : z_i)$  for  $1 \leq i \leq \#\mathcal{S}$ . Consider two points  $P_i$  and  $P_j$  in  $\langle P \rangle$  with  $i \neq j$ . In order to determine when  $\mathcal{S}$  injects into  $\overline{E}_N(\mathbb{F}_p)$ , we need to determine when  $\overline{P}_i = \overline{P}_j$ . Proposition 7.4 shows that  $\overline{P}_i = \overline{P}_j$  if and only if  $p \mid x_i y_j - x_j y_i$ ,  $p \mid x_j z_i - x_i z_j$ , and  $p \mid y_i z_j - y_j z_i$ . The fact that  $P_i$  and  $P_j$  are distinct points shows that if we consider them as vectors in  $\mathbb{R}^3$  they are not proportional. Thus, the cross product is not the zero vector which implies that  $(x_i y_j - x_j y_i, x_j z_i - x_i z_j, y_i z_j - y_j z_i)$  is not the zero vector. Let

$$d_{i,j} = \gcd(x_i y_j - x_j y_i, x_j z_i - x_i z_j, y_i z_j - y_j z_i).$$

Thus we have that  $\overline{P}_i = \overline{P}_j$  if and only if  $p \mid d_{i,j}$ . If we let  $D = \text{lcm}(d_{i,j})$ , then for  $p > D$  we have that  $\overline{P}_i \neq \overline{P}_j$  for all  $i \neq j$ . This shows that for all but finitely many primes, namely for all the primes larger than  $D$  we have that  $\mathcal{S}$  injects into  $E_N(\mathbb{Q})_{\text{tors}}$ . Thus, for all but finitely many  $p$  we must have that  $\#\mathcal{S} \mid \#\overline{E}_N(\mathbb{F}_p)$ . We now use this to reach a contradiction.

Lemma 7.6 combined with the fact that  $\#\mathcal{S} \mid \#\overline{E}_N(\mathbb{F}_p)$  for all but finitely many  $p$  implies that  $p \equiv -1 \pmod{\#\mathcal{S}}$  for all but finitely many primes  $p$  with  $p \equiv 3 \pmod{4}$ . If  $\#\mathcal{S} = 8$ , then we have that there are only finitely many primes of the form  $3 + 8k$ , contradicting Theorem 7.7. If  $\#\mathcal{S}$  is odd and  $3 \nmid \#\mathcal{S}$ , then this gives only finitely many primes of the form  $4(\#\mathcal{S})k + 3$ , contradicting Theorem 7.7 again. Finally, if  $3 \mid \#\mathcal{S}$ , then we get that there are only finitely many primes of the form  $12k + 7$ , again contradicting Theorem 7.7. Since we have obtained a contradiction in all possible cases, it must be that there can be no such  $P$ .  $\square$

**Exercise 19.** With the set-up as in the proof of Theorem 7.2, prove that  $\{(0 : 1 : 0), Q, P, 2P, 3P, P \oplus Q, 2P \oplus Q, 3P \oplus Q\}$  is a subgroup of  $E_N(\mathbb{Q})_{\text{tors}}$  and has order 8.

Given a point  $P \in E_N(\mathbb{Q})$  so that  $P \notin \{(0 : 1 : 0), (0 : 0 : 1), (\pm N : 0 : 1)\}$  Theorem 7.2 implies that  $P$  has infinite order.

**Corollary 7.8.** *Let  $P \in E_N(\mathbb{Q})$  with  $P \notin \{(0 : 1 : 0), (0 : 0 : 1), (\pm N : 0 : 1)\}$ . Then*

$$\langle P \rangle = \{nP : n \in \mathbb{Z}\} \cong \mathbb{Z}.$$

*Proof.* Define a map  $\varphi : \mathbb{Z} \rightarrow \langle P \rangle$  by  $\varphi(n) = nP$ . This map is surjective by definition of  $\langle P \rangle$ . Suppose  $\varphi(m) = \varphi(n)$ . Then we have  $mP = nP$ , i.e.,  $(m - n)P = 0_{E_N}$ . The fact that  $P$  is not a torsion point implies  $m = n$  and so  $\varphi$  is injective. It only remains to show that  $\varphi$  is a homomorphism. To see this observe that we have

$$\begin{aligned} \varphi(m + n) &= (m + n)P \\ &= mP \oplus nP \\ &= \varphi(m) \oplus \varphi(n), \end{aligned}$$

as required.  $\square$

If there is such a point  $P$  with  $P \notin E_N(\mathbb{Q})_{\text{tors}}$  then we say that the rank of  $E_N(\mathbb{Q})$  is positive. The rank essentially measures how many “independent” such points there are, namely, if  $Q$  is another point with  $Q \notin E_N(\mathbb{Q})_{\text{tors}}$  and  $Q \notin \langle P \rangle$  then  $Q$  is independent of  $P$ . The rank of the elliptic curve is how many independent points there are not in  $E_N(\mathbb{Q})_{\text{tors}}$ . More algebraically we have the Mordell-Weil theorem.

**Theorem 7.9.** *One has the following isomorphism of groups*

$$E_N(\mathbb{Q}) \cong E_N(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

where in this case  $\oplus$  refers to a direct sum and  $r$  is the rank of the elliptic curve  $E_N$ .

We are finally able to relate this material back to congruent numbers via the following theorem.

**Theorem 7.10.** *Let  $N$  be a positive square-free integer. Then  $N$  is a congruent number if and only if the rank of  $E_N$  is positive.*

*Proof.* Let  $N$  be a congruent number. We saw in Proposition 3.1 that  $N$  leads to a point  $x \in E_N(\mathbb{Q})$  so that  $x(P) \in (\mathbb{Q}_{>0})^2$ . Since  $N$  is square-free, we have that  $x(P) \neq 0, \pm N$ . Thus, the point  $P$  cannot be in  $E_N(\mathbb{Q})_{\text{tors}}$ . This proves one direction of the theorem.

Suppose now that the rank of  $E_N$  is positive. This implies that there exists  $P \in E_N(\mathbb{Q})$  with  $y(P) \neq 0$ . This shows that  $P$  is in the set  $B$  of exercise 3 and so corresponds to a triangle with area  $N$ .  $\square$

**Exercise 20.** Prove that if the rank of  $E_N$  is positive then  $N$  is a congruent number.

We have now reduced the problem of determining when a number  $N$  is a congruent number to determining the rank of the elliptic curve  $E_N$ . This will be the subject of the following section.

## 8. A MILLION DOLLAR PROBLEM

As we have reduced determining if  $N$  is a congruent number down to determining if the rank of  $E_N$  is positive, we would like to have an easy way to determine the rank of  $E_N$ . Unfortunately, determining the rank of an elliptic curve is not an easy problem at all! We will see how the rank of  $E_N$  is related to the value at 1 of the  $L$ -function of the elliptic curve.

Recall that we defined  $a_{E_N}(p)$  by

$$a_{E_N}(p) = p + 1 - \#\overline{E}_N(\mathbb{F}_p)$$

for all primes  $p \nmid 2N$ . The  $L$ -function of the elliptic curve  $E_N$  is defined by

$$L(s, E_N) = \prod_{p \nmid 2N} (1 - a_{E_N}(p)p^{-s} + p^{1-2s})^{-1}$$

where  $s$  is a complex number with real part suitably large. This function can be analytically continued to the entire complex plane, so we do not spend time worrying about where it converges. Our interest in this function is the conjecture of Birch and Swinnerton-Dyer. This conjecture is one of the Clay Mathematics Institute's Millenium problems. What this means is that it was deemed an interesting enough problem that the institute has offered 1 million dollars to anyone who can prove or disprove the conjecture. (The conjecture is certainly believed to be true based on lots of evidence in its favor!) We will refer to the conjecture as the BSD conjecture from now on.

**Conjecture 8.1.** (Birch and Swinnerton-Dyer) There are infinitely many rational points on the elliptic curve  $E_N$  if and only if  $L(1, E_N) \neq 0$ .

The conjecture is much more general than stated here and actually gives more information about the  $L$ -function at  $s = 1$ , but this form of the conjecture is enough for our purposes.

**Proposition 8.2.** (Assuming BSD) *The integer  $N$  is a congruent number if and only if  $L(1, E_N) = 0$ .*

*Proof.* This follows immediately from the work in the previous section as well the conjecture.  $\square$

The work of [1], [2], [9], and [7], show that for  $E_N$  one has if  $r > 0$  then  $L(1, E_N) = 0$ . (In fact, this is true of any elliptic curve with complex multiplication.) The other direction is still an open problem. Though determining if  $L(1, E_N) = 0$  is not necessarily an easy problem, it is not difficult to at least do some numerical approximations to get a very good idea if  $L(1, E_N) = 0$  or not.

As was done in the previous section, we can extend the definition of  $a_{E_N}(n)$  to include values of  $n$  that are not prime. Recall we set

$$a_{E_N}(p^r) = a_{E_N}(p^{r-1})a_{E_N}(p) - pa_{E_N}(p^{r-2})$$

for  $p \nmid 2N$  and  $r \geq 2$  and

$$a_{E_N}(mn) = a_{E_N}(m)a_{E_N}(n)$$

for relatively prime  $m$  and  $n$  with  $\gcd(mn, 2N) = 1$ .

**Exercise 21.** Prove that  $a_{E_N}(1) = 1$  for all  $N$ .

This allows us to write  $L(s, E_N)$  as a summation instead of a product:

$$L(s, E_N) = \sum_{\substack{n \geq 0 \\ \gcd(n, 2N) = 1}} a_{E_N}(n)n^{-s}.$$

One can now calculate as many values for  $a_{E_N}(n)$  as one would like and use the resulting finite sum upon substituting  $s = 1$  as an approximation for  $L(1, E_N)$ . We can do computations to this end via SAGE. Suppose we have defined  $E$  as our elliptic curve in SAGE. The command

```
sage: E.ap(q)
```

returns the value  $a_{E_N}(q)$  for the prime  $q$ . If one would like a list of the values for the primes between 2 and 100 instead the command is:

```
sage: for q in primes(2,100):
      print q, E.ap(q)
```

If one would like the first 100 values of  $a_{E_N}(n)$  the command is

```
sage: E.anlist(100)
```

These commands can be used to construct finite sum approximations to  $L(1, E_N)$ . Of course, SAGE has a built in command to do this as well:

```
sage: E.Lseries(1)
```

**Exercise 22.** Is 56 a congruent number? If so, give a triangle with rational side lengths and area 56. If not, prove it is not. (You may assume BSD is true).

It is still desirable to have a criterion that does not involve resorting to elliptic curves to compute if  $N$  is a congruent number. Assuming the validity of *BSD*, Tunnell was able to prove the following theorem which reduces the problem of determining if  $N$  is a congruent number to comparing the orders of finite sets. This theorem uses modular forms and as such is too far afield to cover in these notes. It should be observed though that since these are relatively small finite sets one can compute the orders of these sets in cases where computing with elliptic curves is too time consuming.

**Theorem 8.3.** ([8]) *If  $N$  is square-free and odd (respectively even) and  $N$  is the area of a rational right triangle, then*

$$\#\{x, y, z \in \mathbb{Z} \mid N = 2x^2 + 2y^2 + 32z^2\} = \frac{1}{2} \#\{x, y, z \in \mathbb{Z} \mid N = 2x^2 + y^2 + 8z^2\}$$

(respectively

$$\#\{x, y, z \in \mathbb{Z} \mid N/2 = 4x^2 + y^2 + 32z^2\} = \frac{1}{2} \#\{x, y, z \in \mathbb{Z} \mid N/2 = 4x^2 + y^2 + 8z^2\}).$$

*If BSD is true for  $E_N$ , then the equality implies  $N$  is a congruent number.*

**Exercise 23.** Determine if 2006 is a congruent number. What about 2007? You may assume BSD holds true.

Thus, we have come full circle in our discussion of congruent numbers. We began with an innocent looking problem about areas of triangles with rational side lengths. We then saw how elliptic curves arise naturally in the study of congruent numbers. From here we saw that a million dollar open conjecture actually arises in the study of congruent numbers. Finally, we see that if this million dollar conjecture is true, determining if a number is a congruent number comes down to determining the cardinality of a finite set, a simple counting problem.

#### REFERENCES

- [1] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over  $\mathbb{Q}$ : wild 3-adic exercises*, J. Amer. Math. Soc. 14 no.4, 843-939 (2001).
- [2] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39, 223-251 (1977).
- [3] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer GTM 97, (1993).

- [4] B. Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. 47, 33-186 (1977).
- [5] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44, 129-162 (1978).
- [6] W. Stein, SAGE: *Software for Algebra and Geometry Exploration*, <http://modular.math.washington.edu/sage>.
- [7] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) 141 no. 3, 553-572 (1995).
- [8] J. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. 72 (2), 323-334 (1983).
- [9] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141 no. 3, 443-551 (1995).

DEPARTMENT OF MATHEMATICS, THE OHIO STATE UNIVERSITY, COLUMBUS,  
OH 43210

*E-mail address:* `jimlb@math.ohio-state.edu`