CONGRUENT NUMBERS AND ELLIPITIC CURVES

GAL PORAT

1 Outline

We discuss congruent numbers and relate them to elliptic curves. We then show how the theory of elliptic curves enables us to answer classical questions regarding congruent numbers.

2 Congruent Numbers

A general reference for this section is [1].

Definition 1. A natural number n is called a congruent number if it is the area of a right triangle with rational sides. In other words, there is a solution in $a, b, c \in \mathbb{Q}$ for

$$a^2 + b^2 = c^2, \frac{ab}{2} = n$$

The name *congruent* is ancient (due to Fibonacci) and has nothing to do with the usual notion of congruence.

Example 2. 6 is a congruent number, since it is the area of the right triangle with sides $(a, b, c) = 3, 4, 5$.

Example 3. 210 is a congruent number, since it is the area of the right triangle with sides $(a, b, c) = 35, 12, 37$. It is also the area of the right triangle with sides $(a, b, c) = 21, 20, 29$, so we see that the triangle involved does not have to be unique.

Example 4. 1 is not a congruent number. In order to show this, we will sketch the proof given in [1, Theorem 2.1], following an original proof of Fermat. The proof uses the method of *infinite descent*.

Suppose by contradiction that 1 is a congruent number, then there is a solution in $a, b, c \in \mathbb{Q}$ for

$$a^2 + b^2 = c^2, \frac{ab}{2} = n$$

This can be homogenized to the set of equations

$$a^2 + b^2 = c^2, \frac{ab}{2} = nd^2$$

And it is enough to show that the latter equation does not admit solutions in $\mathbb{N}$. Assume by contradiction that there is such a solution, then without loss of generality we have that a, b are relatively prime and that a is even. It is then possible to construct another solution $a', b', c', d' \in \mathbb{N}$ with $0 < c' < c$, by setting

$$a' = \frac{\sqrt{\sqrt{\frac{c+b}{2}} + \sqrt{\frac{c-b}{2}}} + \sqrt{\sqrt{\frac{c+b}{2}} - \sqrt{\frac{c-b}{2}}}}{2}, b' = \frac{\sqrt{\sqrt{\frac{c+b}{2}} + \sqrt{\frac{c-b}{2}}} - \sqrt{\sqrt{\frac{c+b}{2}} - \sqrt{\frac{c-b}{2}}}}{2}$$

$$c' = \sqrt[4]{\frac{c+b}{2}}, d' = \frac{1}{2}\sqrt[4]{\frac{c-b}{2}}$$

(these may not look like integers, but they are). This yields a contradiction since the natural numbers are well ordered. □

The last example illustrates the fact that if a number is not congruent, a priori there isn't a simple argument or algorithm which tells us it is not congruent.

These examples raise the following two questions.

Question I. How can we check whether a number is congruent or not?

Question II. Suppose n is congruent. In how many ways is it congruent?

We are going to present a partial solution to the first question and a complete solution to the second question. In order to do this, take another look at the equations describing a congruent number. These are two equations with three variables. In other words, we are looking at the intersection of two surfaces. We therefore expect this intersection be a one dimensional curve. We have the following theorem, for which such a curve has an exceptionally simple form.

Theorem 5. *We have a bijection*

$$\{(a, b, c) \in \mathbb{Q}^3 | a^2 + b^2 = c^2, \frac{ab}{2} = n\} \to \{(x, y) \in \mathbb{Q}^{\times 2} | y^2 = x^3 - n^2 x\}$$

$$\varphi : (a, b, c) \mapsto \left(\frac{bn}{c-a}, \frac{2n^2}{c-a}\right)$$

with inverse given by

$$\psi : (x, y) \mapsto \left(\frac{x_0^2 - n^2}{y_0}, \frac{2nx_0}{y_0}, \frac{x_0^2 + n^2}{y_0}\right)$$

Proof. Put $c = t + a$, then the first equation becomes $b^2 = t^2 + 2ta$, and then plug in $a = \frac{2n}{b}$. Then we have one equation which is

$$b^2 = t^2 + 4t\frac{n}{b} \Longrightarrow b^3 = t^2 b + 4tn$$

Divide by t^3 and multiply by n^3 to get

$$\left(\frac{bn}{t}\right)^3 = \frac{bn^3}{t} + \frac{4n^4}{t^2} = \frac{bn^3}{t} + \left(\frac{2n^2}{t}\right)^2$$

We may rewrite this as

$$\left(\frac{2n^2}{t}\right)^2 = \left(\frac{bn}{t}\right)^3 - n^2\left(\frac{bn}{t}\right)$$

Thus we see that we obtain a solution $(\frac{bn}{t}, \frac{2n^2}{t})$, of $y^2 = x^3 - n^2x$ with both coordinates nonzero.

Conversely, if we start with a rational solution (x_0, y_0) of $y^2 = x^3 - n^2x$ with $x_0, y_0 \neq 0$, we may obtain a solution for the original pair of equations by solving backwards $a = \frac{x_0^2 - n^2}{y_0}, b = \frac{2nx_0}{y_0}, c = \frac{x_0^2 + n^2}{y_0}$. $\square$

Using this theorem, we may translate our original questions about congruent numbers to questions about the curves $y^2 = x^3 - n^2x$.

Question I. Given n, how can we check whether $y^2 = x^3 - n^2x$ has a rational solution with $y \neq 0$?

Question II. Suppose $y^2 = x^3 - n^2x$ has a rational solution with $y \neq 0$. How many rational solutions does it have with $y \neq 0$?

The curves $y^2 = x^3 - n^2x$ is are examples of *elliptic curves*. Fortunately, these objects are well studied, as we will see in the next section.

3 Elliptic curves

Elliptic curves can be defined over any field, but we will focus on the definition for fields of characteristic different than $2, 3$. We will present an elementary definition.

Definition 6. Let F be a field, $charF \neq 2, 3$. An elliptic curve E defined over F is an algebraic curve of the form

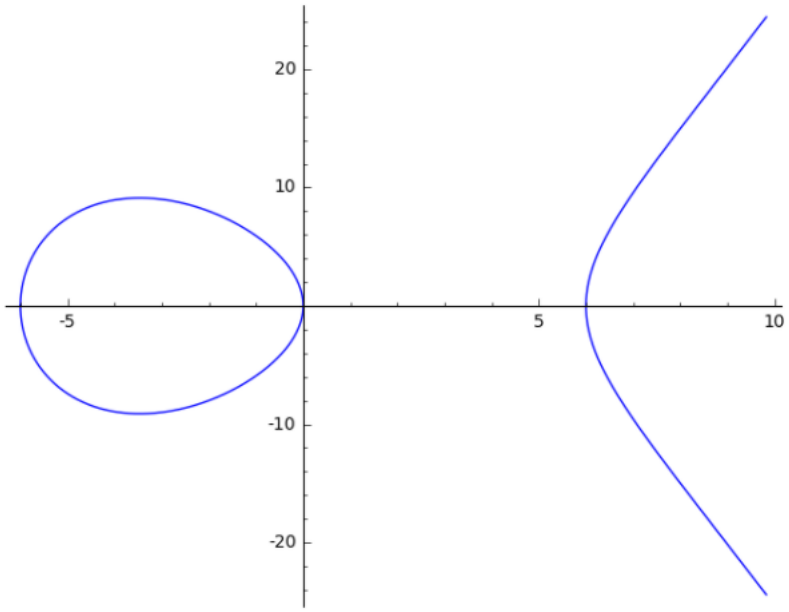
$$y^2 = x^3 + Ax + B$$

For some $A, B \in F$ with $4A^3 + 27B^2 \neq 0$. Given any field $F \subset K$, we define the K-valued points of E as

$$E(K) = \{(x, y) \in K^2 | y^2 = x^3 + Ax + B\} \cup \{O\}$$

Where O is a special point that lies "infinitely high in the y-axis".

Example 7. Take $F = \mathbb{R}$, and let E be the elliptic curve defined by $y^2 = x^3 - 36x$. Its $\mathbb{R}^2$-points can be drawn as follows.



With an additional point lying at infinity.

Adding the point at infinity O to an elliptic curve might seem ad hoc, but it has the following advantage.

Theorem 8. *If E is an elliptic curve defined ovr K, then $E(K)$ has a canonical abelian group structure for which O is the identity.*

A nice aspect of this group law is that it has a geometric interpertation. It is determined by the following property:

$$P + Q + R = O \text{ if and only if } P, Q, R \text{ are collinear}$$

Where we agree that a line intersects O if and only if it is parallel to the y-axis. Also, one needs to count each point with the correct multiplicity for a line tangent to E.

Example 9. Let E be the elliptic curve given by $y^2 = x^3 - 36x$. We have

$$(0, 0) + (-3, 9) + (12, -36) = O$$

Because $(0, 0), (-3, 9), (12, -36)$ lie on the same line. Now the line through $(12, -36), (12, 36)$ is parallel to the y-axis, so

$$(12, -36) + (12, 36) + O = O \Rightarrow (12, -36) = -(12, 36)$$

Hence we conclude that

$$(0,0) + (-3,9) = (12,36)$$

As another example, we compute the 2-torsion subgroup of an elliptic curve.

Example 10. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over F. What is the two-torsion subgroup $E(F)[2]$?

First of all, $O \in E(F)[2]$ because it is the identity element. Now suppose $P = (x, y) \neq O$ is a point of order two. This means that

$$P + P + O = O$$

So we have a line tangent to E at P that is parallel to the y-axis. This happens if and only if P lies on the y axis, i.e. $y = 0$.

Specifically, for $E_n : y^2 = x^3 - n^2 x$ we have

$$E_n(\mathbb{Q})[2] = O \cup \{(x,0) \in E_n(\mathbb{Q})\} = \{O, (0,0), (n,0), (-n,0)\}$$

We will use this fact in the sequel.

Keep in mind that we we want to understand the rational points on an elliptic curve, which is $F = \mathbb{Q}$. In this case, we have the following classical theorem.

Theorem 11. (Mordel-Weil [4, VIII, Theorem 4.1]) *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated abelian group. In other words, there is some $r \in \mathbb{Z}_{\geq 0}$ and an isomorphism*

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$$

With $E(\mathbb{Q})_{tors}$ finite and abelian.

Computing the Mordell-Weil group of an elliptic curve is a nontrivial task. However, computing only the torsion is quite easy. This is illustrated by the following deep fact.

Theorem 12. (**Mazur [2, 3]**) Let E be an elliptic curve defined over $\mathbb{Q}$. Then

$$\#E(\mathbb{Q})_{tors} \leq 16$$

.

In practice, the torsion part can be computed quite easily with the following theorem.

Theorem 13. *[4, VII, Proposition 3.1] Let E be an elliptic curve defined over $\mathbb{Z}$. Then for all but finitely many primes p, there is an injection*

$$E(\mathbb{Q})_{tors} \hookrightarrow E(\mathbb{F}_p)$$

Where $E(\mathbb{F}_p)$ is the curve obtained from the same equation after reducing mod p (which is an elliptic curve for almost all primes).

In other words, finding the torsion subgroup comes down to computing solutions to several mod p equations.

4 Answering Question II

Recall Question II asks how many elements lie in $\{(x,y)|y^2 = x^3 - n^2x, y \neq 0\}$, given that it is nonempty. But actually we have seen in Example 10 that $E_n(\mathbb{Q})[2] = O \cup \{(x,0) \in E_n(\mathbb{Q})\}$, and therefore we are asking equivalently how many elements lie in $E_n(\mathbb{Q})\backslash E_n(\mathbb{Q})[2]$.

It is therefore very convenient that an elementary computation using Theorem 13 shows that in fact $E_n(\mathbb{Q})_{tors} = E_n(\mathbb{Q})[2]$.

In order to do this, we would like to count $E_n(\mathbb{F}_p)$; we can do this in the case $p \equiv 3(4)$.

Lemma 14. *If $p \equiv 3(4)$ and p does not divide n then $E_n(\mathbb{F}_p) = p + 1$.*

Proof. First, we have the four special solutions $O, (0,0), (n,0), (-n,0)$. All the rest of the solutions are of the form (x,y) where $x \neq 0$. Now notice that interchanging $x^3 - n^2x$ by $(-x)^3 - n^2(-x)$ just multiples by (-1). Since $p \equiv 3(4)$, $(-1)^{\frac{p-1}{2}} = -1$ and so the Legendre symbol of $x^3 - n^2x$ changes signs. Thus precisely half of the x's have two solutions for y while the rest have none. Remembering the point at infinity, this implies that $E_n(\mathbb{F}_p) = p + 1$.□

By Theorem 14, $\#E_{n,tors}(\mathbb{Q})$ must divide $p+1$ for almost all primes having $p \equiv 3(4)$. Since primes are evenly distributed among congruency classes, it must hold that $\#E_{n,tors}(\mathbb{Q}) = 4$.

Using the Mordel-Weil theorem, we may now deduce a finer characterization of $E_n(\mathbb{Q})$ as an abelian group.

Theorem 15. *$E_n(\mathbb{Q}) \simeq E_n(\mathbb{Q})[2] \oplus \mathbb{Z}^r$, where $E_n(\mathbb{Q})[2] = \{O, (0,0), (n,0), (-n,0)\}$ and $r \in \mathbb{Z}_{\geq 0}$.*

If n is a congruent number, the above discussion shows that $E_n(\mathbb{Q}) \neq E_n(\mathbb{Q})[2] = E_n(\mathbb{Q})_{tors}$. Since any point in $E_n(\mathbb{Q})\backslash E_n(\mathbb{Q})_{tors}$ has infinite order, we obtain the following answer to question II.

Corollary 16. *If n is a congruent number, it is the area of infinitely many rational triangles.*

In fact, if n is a congruent number, then knowing generators of the free part of $E_n(\mathbb{Q})$ enables us to compute all the different triangles for which n is congruent.

Example 17. Take $n = 6$. Then $E_n(\mathbb{Q})$ is $y^2 = x^3 - 36x$. The point that corresponds to the triangle $(3,4,5)$ is $(12,36)$. One can show that $E_n(\mathbb{Q}) \simeq E_n(\mathbb{Q})[2] \oplus \mathbb{Z}$ and that $(12,36)$ is a generator for the free part. Then 6 is the area of the triangles

$$\psi(\{T + k(12,36)|T = O, (0,0), (6,0), (-6,0), k \in \mathbb{Z}\})$$

For instance, $(6,0) + 3(12,36) = (19602/2209, 2021976/103823)$, so 6 is the area of the triangle with sides $(a,b,c) = (3404/1551, 4653/851, 7776485/1319901)$.

Of course, in general we cannot expect to compute the group of rational points.

5 Answering Question I

Assuming the weak Birch and Swinnerton-Dyer conjecture, Tunnel proved a necessary and sufficient criterion for n being a congruent number. For simplicity we will only describe one case.

Theorem 18. (Tunnel [5]) *Suppose n is square free and odd. If n is congruent then*

$$\#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 8z^2 = n\} = 2\#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 32z^2 = n\}$$

If the weak Birch and Swinnerton-Dyer holds then the converse is also true.

For example, the theorem yields immediately that 1 is not a congruent number.

It is a pleasant fact that the "necessary" part is unconditional and does not depend on any conjecture. Therefore, if we really believe the weak Birch and Swinnerton-Dyer conjecture holds, in theory there is always a finite amount of computation that will determine whether a specific number n is congruent or not, in a way that is *unconditional* on the conjecture.

Indeed, given an n, check the criterion above. If the criterion does not hold, then we know for sure that n is not congruent.

If the criterion does hold, we know that n is supposed to be congruent. Therefore, we can enumerate right triangles with rational sides (orderd by the maximal size of a numerator or denominator). At some point, we will have found a triangle with rational sides and area n.

References

[1] K. Conrad, *The Congruent Number Problem,* The Harvard College Mathematics Review 2, 58-74, 2008.

[2] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes E´tudes Sci. Publ. Math., (47):33–186 (1978), 1977.

[3] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*. Invent. Math., 44(2):129–162, 1978.

[4] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[5] J. Tunnel, *A classical Diophantine problem and modular forms of weight 3/2*, Inventiones Mathematicae. 72 (2) (1983) 323–334.