Congruent Number Problem

Jayadev Ghanta

August 2024

1 Introduction

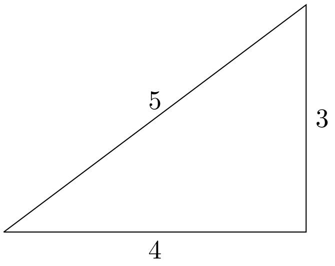
As one of the biggest classical problems in number theory, the congruent number problem has fascinated mathematicians for centuries. This problem has been popularly phrased as how a given positive integer n can be the area of a right-angled triangle with rational side lengths, a question that intertwines the geometry of triangles with the arithmetic of numbers. A positive integer n is called a congruent number if there exists a right-angled triangle with rational sides whose area is exactly n.

In this paper, we will begin by exploring the concept of congruent numbers and the associated Congruent Number Problem. We will introduce the basic definitions and provide examples to illustrate the significance of this problem in number theory. Following this, we will delve into the role of elliptic curves in solving congruent number problems, explaining why they are central to this field of study. We will outline the fundamental aspects of elliptic curves, including their definitions, properties, and the concept of point addition.

Next, we will discuss the correspondence between elliptic curves and congruent numbers, focusing on how elliptic curves can be used to address the Congruent Number Problem. Key theorems such as the Nagell-Lutz Theorem and the Mordell-Weil Theorem will be examined to provide a deeper understanding of the structure of elliptic curves over the rationals and their torsion points. By analyzing these theorems, we will gain insights into the specific examples of congruent numbers and demonstrate how these mathematical tools contribute to solving the problem.

2 Congruent Numbers

A congruent number is a positive integer that can be the area of a right-angled triangle with all three sides having rational lengths. In other words, n is congruent if there exist rational numbers a, b, and c such that $a^2 + b^2 = c^2$ and the area of the triangle is $\frac{1}{2}ab = n$.



$$\text{Area} = \frac{1}{2} \times 3 \times 4 = 6$$

2.1 Congruent Number Problem

Given a whole number N, does there exist a right-angled triangle with rational side lengths and an area of N?

2.1.1 Example

Identifying whether a number is congruent by searching for the side lengths of right-angled triangles is a complex task. As an example, take the congruent number $N = 157$. It can be the area of a right triangle with the following rational side lengths:

$$\alpha = \frac{411340519227716149383203}{21666555693714761309610}$$

$$\beta = \frac{6803298487826435051217540}{411340519227716149383203}$$

This is the "simplest" known triangle corresponding to the congruent number 157.

2.1.2 Simplification

Suppose N represents the area of a rational right-angled triangle with sides α, β, and hypotenuse γ, where $\alpha, \beta, \gamma \in \mathbb{Q}$ and satisfy $\alpha^2 + \beta^2 = \gamma^2$ with $N = \frac{1}{2}\alpha\beta$. When N is multiplied by 4, the following equations hold:

$$(\alpha + \beta)^2 = \gamma^2 - 4N$$

$$(\alpha - \beta)^2 = \gamma^2 + 4N$$

By multiplying the equations together, we get:

$$\left(\frac{\alpha^2-\beta^2}{4}\right)^2 = \gamma^2 - 4N$$

Define $v = \frac{\alpha^2-\beta^2}{4}$ and $u = \gamma^2$. This gives us:

$$v^2 = u - N^2$$

Next, multiply both sides by u^2:

$$(uv)^2 = u^3 - N^2u^2$$

Set $x = u^2 = (\gamma^2)^2$ and $y = uv = \frac{\gamma(\alpha^2-\beta^2)}{8}$. This results in:

$$y^2 = x^3 - N^2x$$

which represents the equation of an elliptic curve.

2.1.3 Why elliptic curves?

By transforming the problem into an elliptic curve equation, the Congruent Number Problem is recast into a question about the rational points on the elliptic curve E_N. Specifically, N is a congruent number if and only if the elliptic curve E_N has a rational point (x, y) with $y \neq 0$. This connection allows us to use the tools and theorems from the theory of elliptic curves, such as the Mordell-Weil theorem, descent methods, and modern computational techniques, to approach and potentially solve the problem.

2.2 Elliptic Curve Correspondence

According to https://kconrad.math.uconn.edu/articles/congruentnumber.pdf, there is a one to one correspondence between an elliptic curve and the sides of a right triangle α, β, γ. Specifically for $n > 0$, there is a one-to-one correspondence between the following two sets:

$$\{(a, b, c) \mid a^2 + b^2 = c^2, \frac{1}{2}ab = n\}$$

and

$$\{(x, y) \mid y^2 = x^3 - n^2x, y \neq 0\}.$$

Mutually inverse correspondences between these sets are:

$$(a, b, c) \mapsto \left(\frac{nb}{c-a}, \frac{2n}{2c-a}\right),$$

$$(x, y) \mapsto \left(\frac{x^2 - n^2 y}{y}, \frac{2nx}{y}, \frac{x^2 + n^2 y}{y} \right).$$

. We can use this information to find these side lengths when we find a corresponding point on the elliptic curve.

3 Elliptic Curves

Now that we have converted the problem into an elliptic curve, let us rephrase the problem into a new one.

For a whole number N, does there exist a rational point (x, y) with $y \neq 0$ on the elliptic curve $E_N : y^2 = x^3 - N^2 x$?

3.1 Intro to Elliptic Curves

An elliptic curve is a type of cubic curve defined by a specific kind of equation in two variables, typically denoted x and y, with the form:

$$y^2 = x^3 + ax + b$$

where a and b are constants, and the curve is defined over a particular field, such as the real numbers $\mathbb{R}$ or the rational numbers $\mathbb{Q}$.

Elliptic curves have a rich structure and are of profound interest in number theory, algebraic geometry, and cryptography. One of the most striking features of elliptic curves is that the set of points on an elliptic curve, together with a special point called the "point at infinity," forms a group under a particular addition operation. This group structure is key to many of the deep results in number theory related to elliptic curves.

3.2 $(E(\mathbb{Q}), +)$ is an Abelian group

Commutativity
For any two points P_1 and P_2 on $E(\mathbb{Q})$, we have:

$$P_1 + P_2 = P_2 + P_1.$$

This follows from the fact that the line through P_1 and P_2 intersects the curve at the same third point, regardless of the order of P_1 and P_2.

Closure
The set $E(\mathbb{Q})$ is closed under the addition operation $+$. For any points P_1 and P_2 in $E(\mathbb{Q})$, their sum $P_1 + P_2$ is also in $E(\mathbb{Q})$.

Identity Element
The identity element with respect to the addition operation $+$ is the point at

infinity, denoted O. For any points P_1 and P_2 on the elliptic curve $E(\mathbb{Q})$, we have:

$$P_1 + P_2 = O \star (P_1 \star P_2).$$

Thus, for any point P on the elliptic curve:

$$O + P = O \star (O \star P) = P,$$

since if $P = (x, y)$, then $O \star P = -P = (x, -y)$, and hence $O \star (O \star P) = (x, y) = P$. Therefore, the point at infinity serves as the identity element.

Inverse Element
For every point P on the elliptic curve, there exists an inverse point $-P$ such that:

$$P + (-P) = O.$$

Define the inverse of P as:

$$-P := P \star (O \star O).$$

Then:

$$P + (-P) = O \star (P \star (-P)) = O \star (P \star (P \star (O \star O))) = O.$$

This indicates that there is no third point on E where the line through P and $-P$ intersects the curve.

Associativity
For any points P_1, P_2, and P_3 on the curve, the addition operation satisfies:

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3).$$

This property has a complex proof that is outside the scope of the paper.

3.3 Point Addition in Elliptic Curves

The equation of the elliptic curve E_N indicates that any line intersecting the curve will intersect it at a third point. We can define an addition operation for points on an elliptic curve by using this third point as the sum of the initial two points. Although this operation is not associative on its own, reflecting the third point over the x-axis provides a well-defined addition operation for elliptic curves. This geometric approach also has an algebraic foundation. An elliptic curve includes a point at infinity, which is considered a rational point.

The set of rational points on the elliptic curve, denoted $E(\mathbb{Q})$, forms an Abelian group, with the point at infinity O serving as the identity element. For two distinct points P_1 and P_2 on the curve, the line through P_1 and P_2 intersects the curve at a third point, denoted $P_1 \star P_2$.

We then draw the vertical line through $P_1 \star P_2$ and intersect it with the curve again to find the reflection of $P_1 \star P_2$ across the x-axis. We define the binary operation $\star$ such that $P_1 \star P_2$ is this reflection. The addition of points on the elliptic curve is then given by:

$$P_1 + P_2 = O \star (P_1 \star P_2)$$

If the points are the same, we use the tangent line to define this addition. Since $P_1 + P_1 = 2P_1 := P$, we draw the tangent line to P and then find the third point of intersection with the curve and reflect it about the x-axis.

3.4 Torsion Points

In the context of elliptic curves, a **torsion point** is a point on the curve that, when added to itself a certain number of times, results in the identity element, which is the point at infinity O. More formally, a point P on an elliptic curve E is called a torsion point if there exists a positive integer n such that:

$$nP = O.$$

The smallest such n is referred to as the **order** of the torsion point P. Torsion points play a crucial role in the study of elliptic curves and are central to many aspects of their theory.

3.4.1 Example of Torsion Points

Consider the elliptic curve E given by the equation:

$$y^2 = x^3 - x$$

defined over $\mathbb{Q}$. To find the torsion points, we look for points (x, y) such that:

$$n(x, y) = (O)$$

for some integer n. For this specific curve, it can be shown that the torsion points include the point at infinity and other points of finite order. For instance, the point $(0, 0)$ is a torsion point of order 2, as:

$$2(0,0) = O$$

Similarly, other torsion points can be computed, giving insight into the structure of the torsion subgroup of E.

3.4.2 Example Theorem

Suppose that P is a 2-torsion point on an elliptic curve E, and that P is not the point at infinity. Show that the y-coordinate of P is 0.

The equation for an elliptic curve is given by $y^2 = x^3 + ax + b$. A point P on an elliptic curve is a 2-torsion point if $2P = \mathcal{O}$. For clarification, an elliptic curve forms an abelian group where the operation of addition for two distinct points P and Q are done as the following:

- Find the line that intersects both P and Q.
- Find the third point where this line intersects the elliptic curve, R.
- Calculate the reflection of this point R, which we will call R'.
- Now we have $P + Q = R'$ as our operation definition, with the identity element being the point at infinity.

Since we are only dealing with one point P, we must take the tangent line of the elliptic curve. Doing some basic implicit differentiation, we find that the slope of the line λ must be $\frac{3x_1^2+a}{2y_1}$, where the coordinates of P are (x_1, y_1). Since we are doing the operation $P+P$, we have that the line is $y = \lambda x + b$. We can find b by plugging in x_1 and y_1. Now the updated line is $y = \lambda(x - x_1) + y_1$. Since the line intersects the elliptic curve at a third point to complete the operation, we can plug in the line equation into the elliptic curve equation: $(\lambda(x-x_1)+y_1)^2 = x^3 + ax + b$. The following is the rest of my algebra for the problem.

$$(\lambda(x - x_1) + y_1)^2 = x^3 + ax + b$$

Moving everything to one side, we can get the following:

$$x^3 - \lambda^2(x - x_1)^2 + \square x + \square$$

We can set $\lambda^2 = x_3 + 2x_1$, which makes $x_3 = \lambda^2 - 2x_1$. We can stop here before we solve for y_3. Since we know that x_3 must equal to infinity in order to form the group, we must find a way to make x_3 to be infinite. Since the denominator of λ is $2y_1$, y_1 must equal to 0.

3.5 Nagell-Lutz Theorem

Let $A, B \in \mathbb{Z}$ be integers, and let $\Delta_{A,B}$ denote the discriminant of the elliptic curve given by the equation

$$\Delta_{A,B} = -16 \cdot (4A^3 + 27B^2)$$

Assume that $\Delta_{A,B} \neq 0$, which ensures that the elliptic curve is nonsingular (i.e., it has no cusps or self-intersections). Consider the elliptic curve E over the rational numbers $\mathbb{Q}$ given by the affine Weierstrass equation:

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

Let (x, y) be a point on E with rational coordinates $x, y \in \mathbb{Q}$, and suppose that this point has finite order under the group law on the elliptic curve. The Nagell-Lutz theorem then states the following:

- **Integer Coordinates:** If (x, y) is a rational point of finite order, then both x and y must actually be integers, i.e., $x, y \in \mathbb{Z}$.
- **Condition on y^2:** Furthermore, the value of y^2 must either be zero or must divide the discriminant $\Delta_{A,B}$ precisely. That is, y^2 must satisfy:

  $$y^2 \mid \Delta_{A,B}$$

  This means that if $y \neq 0$, then the square of y must be a divisor of the discriminant $\Delta_{A,B}$. If $y = 0$, the point $(x, 0)$ corresponds to a point of finite order on the elliptic curve, specifically a point of order 2.

Proof. Let E be an elliptic curve defined over $\mathbb{Z}$, and let $P = (x_0, y_0)$ be a rational point on E. Let's show that if P is not an integral point, then P must have infinite order. Suppose, for contradiction, that P has finite order n. This would imply that $nP = O$, where O is the identity point on the elliptic curve. If P had finite order, it would mean P is a torsion point of the elliptic curve. However, torsion points on elliptic curves defined over $\mathbb{Z}$ are known to be integral points. This follows because the coordinates of torsion points satisfy polynomial equations with integer coefficients, which necessitates that both coordinates must be integers. Since P is given to be a rational point but not an integral point (meaning at least one of x_0 or y_0 is not an integer), it contradicts the fact that a torsion point must be integral. Therefore, the assumption that P has finite order leads to a contradiction. Hence, if P is a rational point but not an integral point, P must have infinite order. □

The Nagell-Lutz theorem is significant because it allows us to classify the torsion points (points of finite order) on an elliptic curve in a very concrete way. By checking which integer points satisfy these conditions, one can determine all the torsion points on a given elliptic curve. This theorem is particularly useful in computational aspects of elliptic curves, where identifying torsion points is a key step in many algorithms.

3.6 Mordell-Weil Theorem

(Mordell–Weil) Let E be an elliptic curve over $\mathbb{Q}$. There is a nonnegative integer r and a finite abelian group T such that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times T.$$

We call r the rank and T the torsion subgroup.

The Mordell-Weil Theorem provides important insights into the structure of elliptic curves over the rational numbers $\mathbb{Q}$. It tells us that the set of rational points on an elliptic curve can be decomposed into two distinct parts. Specifically, any point on the curve can be expressed as a combination of a finite number of special points plus a finite repeating pattern. In simpler terms, this means that every point on the curve can be written as a sum of certain "generator" points with integer coefficients and a finite set of torsion points, where the coefficients of the torsion points are restricted to specific ranges.

To formalize this, the theorem identifies two key components: the rank r and the torsion subgroup T. The rank r represents the number of independent ways to combine these generator points, which essentially gives us an infinite set of combinations. The torsion subgroup T describes a finite set of repeating patterns in the curve's points. This means that the set of rational points on the curve is a blend of a freely combinable infinite part and a finite, periodic part.

Mazur later extended this theorem by detailing the possible structures of these finite repeating patterns, further refining our understanding of the elliptic curve's rational points.

4 Congruent Problem Example

The right triangle with sides 3, 4, and 5 has area 6. Using elliptic curves, find three more right triangles with rational sides and area 6.

We start by introducing the concept of a congruent number. An integer N is defined as a *Congruent Number* if there exist rational numbers α, β, and γ such that $\gamma^2 = \alpha^2 + \beta^2$ and $N = \frac{1}{2}\alpha\beta$. Given that N is our target area, multiplying N by 4 yields the relations $(\alpha + \beta)^2 = \gamma^2 - 4N$ and $(\alpha - \beta)^2 = \gamma^2 + 4N$. Dividing these equations by 4, we derive the identities $\left(\frac{\alpha+\beta}{2}\right)^2 = \left(\frac{\gamma^2}{2}\right) - N$ and $\left(\frac{\alpha-\beta}{2}\right)^2 = \left(\frac{\gamma^2}{2}\right) + N$.

By multiplying these equations, we obtain $\left(\frac{\alpha^2-\beta^2}{4}\right)^2 = \left(\frac{\gamma^2}{4}\right)^2 + N^2$. Introducing the substitutions $v = \frac{\alpha^2-\beta^2}{4}$ and $u = \frac{\gamma^2}{2}$, we arrive at the equation $v^2 = u^4 - N^2$. Further manipulation by multiplying by u^2 leads to $(uv)^2 = u^6 - N^2u^2$. Setting

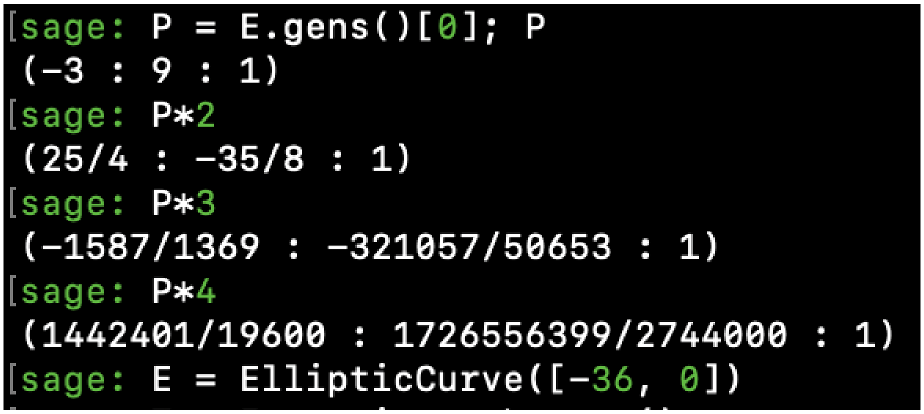
$x = u^2 = \left(\frac{\gamma^2}{2}\right)^2$ and $y = uv = \frac{\gamma(\alpha^2-\beta^2)}{8}$, the resulting equation is $y^2 = x^3 - N^2x$, which describes an elliptic curve.

For $N > 0$, there is a one-to-one correspondence between the set of right triangles with rational sides (α, β, γ) and area N, and the set of rational points (x, y) on the elliptic curve $y^2 = x^3 - N^2x$ with $y \neq 0$. The mutually inverse correspondences between these sets are given by $(\alpha, \beta, \gamma) \mapsto \left(\frac{N\beta}{\gamma-\alpha}, \frac{2N^2}{\gamma-\alpha}\right)$ and $(x, y) \mapsto \left(\frac{x^2-N^2}{y}, \frac{2Nx}{y}, \frac{x^2+N^2}{y}\right)$.

This elliptic curve formulation connects to the classic Congruent Number Problem (CNP) through the question: For a whole number N, does there exist a rational point (x, y) with $y \neq 0$ on the elliptic curve $E_N : y^2 = x^3 - N^2x$? Notice that given a right triangle with rational sides and area N, a corresponding rational point (x, y) can be found on the curve E_N.

Applying the Nagell–Lutz Theorem, consider an elliptic curve E in short Weierstrass normal form $E : y^2 = x^3 + Ax + B$, with integral coefficients $A, B \in \mathbb{Z}$. Let $O \neq P = (x, y) \in E(\mathbb{Q}_{\text{tors}})$. Then $x, y \in \mathbb{Z}$, and either $2P = O$ or y^2 divides $\Delta_0 = -\frac{\Delta}{16} = 4A^3 + 27B^2$. Specifically, for the family of elliptic curves of the form $E_N : y^2 = x^3 - N^2x$, where $\Delta_0 = 4N^6$, the torsion points of E_N are either $y = 0$ or y^2 divides $4N^6$.

Finally, using computational tools such as Sage, these theoretical insights can be applied to find explicit examples of right triangles with rational sides and area 6.



```
[sage: P = E.gens()[0]; P
 (-3 : 9 : 1)
[sage: P*2
 (25/4 : -35/8 : 1)
[sage: P*3
 (-1587/1369 : -321057/50653 : 1)
[sage: P*4
 (1442401/19600 : 1726556399/2744000 : 1)
[sage: E = EllipticCurve([-36, 0])
```

The three right triangles with rational sides and area 6, found using the elliptic curve method, have the following sets of sides: $\frac{120}{7}, \frac{7}{10}, \frac{1201}{70}$; $\frac{4653}{851}, \frac{3404}{1551}, \frac{7776485}{1319901}$; and $\frac{1437599}{168140}, \frac{2017680}{1437599}, \frac{2094350404801}{241717895860}$. I found these side lengths by plugging in the rational points found in the elliptic curve into the mutually inverse correspondence that we have calculated before.