The Congruent Number Problem and Its Connection with Elliptic Curves

Palash Khanra

Dept. of Mathematics, Ramakrishna Mission Vidyamandira, Belur Math, 711202, West Bengal, India, Email: palash1729@vidyamandira.ac.in .

Abstract

Number theory, a mathematical domain, centers on integers and their patterns. It often requires advanced methods to solve even simple problems. The Congruent Number Problem, unsolved for centuries, exemplifies this challenge. This survey article highlights how studying congruent numbers motivates exploring elliptic curves and how insights from these curves advance solving the Congruent Number Problem. The elegant connections between these subjects are striking.

Keywords: Congruent Numbers, Elliptic Curves, Connections

AMS subject classification: 11H52 , 97F10 , 14Gxx

1 Introduction

The congruent number problem (CNP) involves determining whether a natural number n is congruent. In number theory, congruent numbers usually denote two numbers sharing the same remainder when divided by a third number (congruent modulo an integer). However, in this article, we'll employ the term 'congruent numbers' differently. A natural number n is a congruent number if it forms the area of a right triangle with rational sides: $n = \frac{ab}{2}$. and $a^2 + b^2 = c^2$; $a, b, c \in \mathbb{Q}$. This is attributed to the Greek Mathematician Diophantus and is referred to as the 'Triangular version' of the congruent6 number problem.
The CNP's initial mention is in the Arab manuscript '*AL-Kitab-al-Fakhri*', written by Persian mathematician Al-Karaji (c.953 - c.1029).. In his '*Introduction to Elliptic Curves and Modular Forms*', N. Koblitz mentioned that, "*the problem of studying whole numbers N which occur as areas of rational right triangles were of interest to Greeks in special cases, it seems that the congruent number problem was first systematically studied by Arab scholars of the*

tenth century. The Arab scholars used to rephrase the problem in terms of rational square numbers: given N, can one find a rational number x such that $x^2 + N$ and $x^2 - N$ are both squares of rational numbers?"[1]. Arabs identified these congruent numbers: 5, 6, 14, 15, 21, 30, 65, 70, 110, 154, 190, and so on [2]. Diophantus (c.210 - c.290) also mentioned similar problems long before the Arab scholar's work. L. E. Dickson, in his '*History of the Theory of Numbers, Vol-2 (Diophantine Analysis)*' mentioned Woepeck's view that there is no sign that Arabs knew Diophantus before the translation by Aboul Wafi (c.998), but they probably come to know about the problem from the Hindus who were acquainted with his work [3].
In the 11_{th} century, Fibonacci, challenged by King Frederic-II's scholars, sought three rational numbers whose squared values formed an arithmetic progression with no common difference 5. In 1225, in his book '*Liber Quadratorum*[1]' (Book of Squares), he defined an integer N as '*Congruum*' if it is served as the common difference in an arithmetic progression of three squares: $x^2 - N$, x^2 and $x^2 + N$. This marks the 'original version' of the CNP. Both terms 'congruum' and 'congruence' come from the Latin 'congruere', meaning "*to meet together*" [4]. Fibonacci demonstrated that 5 and 7 are congruent numbers ($\frac{3}{2}$, $\frac{20}{3}$, $\frac{41}{6}$ and $\frac{35}{12}$, $\frac{24}{5}$, $\frac{337}{6}$ are rational sides of respective triangles). He also asserted, without proof, that no congruent number can be a square, effectively implying that 1 is not a congruent number [2]. The equivalence of the original and triangular versions can be easily established. In 1659, Fermat provided proof for this and additionally stated that 2 and 3 are not congruent numbers [4]. Fermat introduced his method of infinite descent, first applied it to the CNP. A. Weil stated that "*Fortunately, just for once, he (Fermat) had found room for this mystery (i.e. the method) in the margin of the very last proposition of Diophantus*". [2].
Imagine a right triangle with sides a,b, and c. Using the concept of Pythagorean triplets, the area of such a triangle with rational sides is an integer, given by $ab(b^2 - a^2)$. The key question is, for positive integers a,b, which integers can rise as $ab(b^2 - a^2)$ when adjusted for a rational square factor? This query is essentially the congruent number problem. If we express a positive integer n as $n = a^2b$, where b is a squarefree integer, then n is congruent if and only if b is congruent. On September 22, 2009 – Mathematicians successfully tackled the first trillion cases of the congruent number problem, revealing numbers like- 5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47, 52, 53, 54, 55, 56, 60, 61, 62, 63, 65, 69, 70, 71, 77, 78, 79, 80, 84, 85, 86, 87, 88, 92, 93, 94, 95, 96, 101, ..., 2022, **2023**, 2029, ...[5]
For more comprehensive list of squarefree congruent numbers below < 1000, refer to [6] by Alter and Curtz. For further exploration, [7] by F. R. Nemenzo offers insight into determining all congruent numbers under 40000.

An elliptic curve, defined over any field $\mathbb{K}$ (finite or infinite), is a smooth cubic curve with a fixed point at infinity. If $\mathbb{K}$ is an algebraic number field, then with some change of variables, it can be transformed into the Weierstrass equation. The classical Weierstrass equation, $y^2 = x^3 + Ax + B$, suits fields except those with characteristic 2 or 3. The general Weierstrass equation, $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_0$, applies to all number fields, even those with characteristic 2 and 3. While cubic curves weren't extensively explored until the late 1600s, their roots trace back to ancient number theory. The First challenge arises from Diophantus of Alexandria's '*Arithmetica*' (c.210- c.290), where he mentionned that dividing a number into two, yielding a product that's a cube minus a side: $Y(a - Y) = X^3 - X$

[1]Prince Boncompaign found this lost book and published it in the year 1856.[2]

for a given a. The second issue concerns congruent numbers, involving contributions from various mathematicians including Bachet, Fermat, Newton, Euler, Legendre, Maclaurin, and others [8]. Though 'ellipses' and 'elliptic curves' sound alike, they have distinct structures. Ellipses are quadratic, whereas elliptic curves are cubic. However, a subtle link between them is forged through bridges like elliptic integrals and functions. Consider an ellipse $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ with $a > b > 0$. Taking the positive value, we have, $y = f(x) = \frac{b}{a}\sqrt{a^2 - x^2}$. Then $f'(x) = \frac{-rx}{\sqrt{a^2-x^2}}$, where $r = \frac{b}{a} < 1$. Using the arc length formula, the circumference is, $L = \int_a^b \sqrt{1 + (f'(x))^2}dx = 4\int_0^a \sqrt{1 + \frac{r^2x^2}{a^2-x^2}}dx$. With the substitution $x = at$, this becomes $L = 4a\int_0^1 \sqrt{\frac{1-e^2t^2}{1-t^2}}dt$, where, $e = \sqrt{1 - r^2}$ is the ellipse's eccentricity. This is an elliptic integral. Let $u(t) = \sqrt{\frac{1-e^2t^2}{1-t^2}}$. This implies $u^2(1 - t^2) = 1 - e^2t^2$. Setting $e = \frac{1}{a}$, we have, $u^2 + (\frac{t}{a})^2 = 1 + a^2u^2(\frac{t}{a})^2$, which resemmbles the Edward curve, $x^2 + y^2 = 1 + dx^2y^2, d \neq 0$. By substituting $z = y(1 - dx^2)$ into $x^2 + y^2 = 1 + dx^2y^2$, we obtain $z^2 = 1 - (d+1)x^2 + dx^4$. For the Edwards curve to describe an elliptic curve, the polynomial must have distinct roots, which is true if and only if the discriminant $(d + 1)^2 - 4d \neq 0$ i.e. $(d - 1)^2 \neq 0$ i.e. $d \neq 1$. This implies that $x^2 + y^2 = 1 + dx^2y^2$ defines an elliptic curve when $d \neq 1$. Hence, $u^2(1 - t^2) = 1 - e^2t^2$ with $e = \frac{1}{a}$, defines an elliptic curve. This u(t) is sometimes referred to as the *elliptic function* [9]. A more elegant connection can be established using the Weierstrass-$\mathscr{P}$ function. Throughout this article, we consider the classical Weierstrass equation $y^2 = x^3 + Ax + B$ as defineing an elliptic curve. Let E be an elliptic curve over the field $\mathbb{Q}$. In 1901, Henri Poincare proved that, $E(\mathbb{Q}) = \{(x, y) \in E\colon x, y \in \mathbb{Q}\} \bigcup \{\mathbb{O}\}$ is a commutative group under '+', where $P + Q = \mathbb{O} * (P * Q)$. Poincare conjectured that all the rational-coordinate points on an elliptic curve E can be generated by adding finitely many starting points, a conjecture later proven by Louis J. Mordell in 1922 and generalized by Andre Weil in 1928. They established that $E(\mathbb{Q})$ is a finitely generated abelian group. [10]. Andrew Ogg introduced an idea about the possible torsion subgroup of $E(\mathbb{Q})$, and Barry Mazur subsequently demonstrated 15 possible structures for the torsion (all abelian). Mazur's theorem additionally ensures that the order must be infinite for a rational point $P \in E(\mathbb{Q})$ with an order exceeding 12.

Let's define, $t = c - a$. Using the triangular version of the CNP, we get, $\frac{n^3b^3}{t^3} - \frac{n^3b}{t} = \frac{4n^4}{t^2}$. Now introduce $Y = \frac{2n^2}{t} = \frac{2n^2}{c-a} \neq 0$ and $X = \frac{nb}{t}$. Thus we have, $Y^2 = X^3 - n^2X$. Notably, there are three evident rational solutions to this equation: (0,0), (n,0), and (-n,0), along with other solutions. The reverse is also true. Suppose there exist rational points (u,v) on the elliptic curve $Y^2 = X^3 - n^2X$ where $u, v \neq 0$ simultaneously. Define, $a = \frac{v}{u}$ and $b = \frac{2n}{a}$. So, $a, b > 0$. Now, we obtain, $a^2 + b^2 = \frac{(u^2+n^2)^2}{v^2} = c^2$. Thus a triangle with sides a,b, and c is formed, satisfying $a^2 + b^2 = c^2$ and $n = \frac{ab}{2}$. This implies that n is a congruent number [4]. Hence, the congruent number problem aligns with seeking non-trivial rational solutions for the elliptic curve $E_n : Y^2 = X^3 - n^2X$. These E_n's are known as **congruent number elliptic curves**, constituting a distinct class and being quadratic twists[2] of E_1. All congruent number elliptic curves share a consistent structure: an egg-shaped segment for $x \in [-n, 0]$ and an unbounded portion for $x \in [n, \infty)$. Our focus in this article centers on exploring

[2]The isomorphic state over a quadratic extension of $\mathbb{Q}$, but not over $\mathbb{Q}$.

the interconnections between the Congruent number problem (CNP) and this special class of elliptic curves.

2 Connections

The below theorem connects CNP to elliptic curves, Define,
$C_n = \{(a,b,c) : a^2 + b^2 = c^2, n = \frac{ab}{2}\}$,and $E_n = \{(x,y) : y^2 = x^3 - n^2x, y \neq 0\}$.
Theorem 1. *The number $n > 0$ is congruent if and only if. the curve $y^2 = x^3 - n^2x$ has a point $(x,y) \in \mathbb{Q}\times\mathbb{Q} : y \neq 0$. More precisely, there is a one-one correspondence $C_n \longleftrightarrow E_n$. The mappings $f : C_n \longrightarrow E_n$ and $g : E_n \longrightarrow C_n$ are defined by, $f(a,b,c) = (\frac{nb}{c-a}, \frac{2n^2}{c-a})$, and $g(x,y) = (\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y})$.*

Let $y^2 = x^3 - n^2x$ be an elliptic curve and its' discriminant is $\triangle = 4n^6$. By Nugell-Lutz theorem, the torsion points are $P(x,y)$, where either $y = 0$ or, $y^2|4n^6$. But since n is a congruent number, $y^2 = x^3 - n^2x$ has no rational solution with $y \neq 0$ and $y^2|4n^6$. Hence we have, $E_n(Q)_{tor} = \{O, (0,0), (n,0), (-n,0)\}$.

2.1 Geometry of congruent number elliptic curves

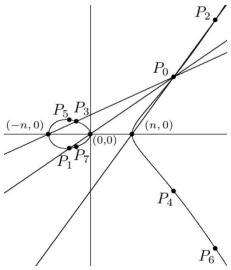

Fig. 1 Intersecting points on the congruent number elliptic curve

Let, $(a,b,c) \in C_n$. Then it motivates for another seven new points $\in C_n$. Four points, (a, b, c), (-a, -b, -c), (-a, -b, c), and (a, b, -c). The other four points are, (b, a, c), (-b, -a, -c), (-b, -a, c), and (b, a, -c), obtained just by interchanging the right-angled sides a,b in the previous four points. These relationships hold a geometric significance by generating new points from the old ones on the congruent number elliptic curve $y^2 = x^3 - n^2x$ using the cord-tangent method. $(a,b,c) \in C_n$ corresponds to $(x,y) \in E_n$. The point (x, -y) corresponds to (-a, -b, -c). Three evident solutions to the elliptic curve are (0, 0), (n, 0), and (-n, 0). The cord joining (0, 0) and (x, y) intersects the elliptic curve at $(\frac{-n^2}{x}, \frac{-n^2y}{x^2})$, correspoding to $(a,b,-c) \in C_n$. Reflectig $(\frac{-n^2}{x}, \frac{-n^2y}{x^2})$ results in $(\frac{-n^2}{x}, \frac{n^2y}{x^2})$, corresponding to $(-a,-b,c) \in C_n$.

Connecting (x, y) to the other two points (n, 0) and (-n, 0) yields the other four points. The geometry of the elliptic curve $y^2 = x^3 - n^2x$, helps us to obtain a new rational right triangle with area n using two known triangles of the same area and we can repeat this process. A new rational right triangle can even be obtained from a single such triangle by using a tangent line. A rational point (x,y) on $y^2 = x^3 - n^2x$ with $y \neq 0$ produces a tangent line that intersects the curve, allowing derivation of a new rational right triangle with area n using Theorem 1. The cord method adds points, while the tangent method doubles the points.

2.2 Correspondence: Rational points on circle

The connection between rational triangles with sides a,b,and c, and area $n = \frac{ab}{2}$, and rational solutions to the curve $y^2 = x^3 - n^2x$, can be established through rational points on the unit circle $x^2 + y^2 = 1$. Let's explore this relationship. The line joining (-1,0) and (0,t) has the

equation $y = t(x+1)$ with slope t. The point X(u,v) lies both on this line (denoted as L) and on the circle $x^2+y^2 = 1$. For a fixed value of t, we obtain the quadratic equation, $1-u^2 = v^2 = t^2(1+u)^2$. The root $u = -1$ corresponds to the point $(-1, 0)$ lying on both L and the circle. To find another root $u \neq -1$, we divide both sides by (1+u), resulting in $(1-u) = t^2(1+u)$, which simplifies to $u = \frac{1-t^2}{1+t^2}$. Substituting the value of u into $u^2 + v^2 = 1$, we get $v = \sqrt{1-\left(\frac{1-t^2}{1+t^2}\right)^2} = \frac{2t}{1+t^2}$. This yields a rational parametrization $(u, v) = (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ of the circle. This implies that x and y are rational if and only if t is rational, allowing us to find rational points on the unit circle. Consider a rational right triangle with sides a,b, and c, and area $n = \frac{ab}{2}$. If a,b, and c shares a common factor, it can be factored out. Triangles without a common factor are primitive. If b,c has prime factor then, it divides a due to $a^2 = c^2 - b^2$. Assuming a,b, and c have no common factor, we get $\left(\frac{a}{c}\right)^2 + \left(\frac{a}{c}\right)^2 = 1$. Pair (u,v) is a rational point on circle $x^2 + y^2 = 1$, where $u = \frac{a}{c}$ and $v = \frac{b}{c}$. As a and b lack a common factor, at least one is odd. Two cases emerge: (Case-1) One of a or b is odd, resulting in $a^2 + b^2 \equiv 1 \pmod 4$. (Case-2) Both a and b are odd, leading to $a^2 + b^2 \equiv 2 \pmod 4$. However, $a^2 + b^2 \equiv 0$ or $1 \pmod 4$, a contradiction in Case-2. Thus, one must be odd. Assuming a is odd and b is even, define $t = \frac{p}{q}$. $\frac{a}{c} = u = \frac{q^2-p^2}{q^2+p^2}$ and $\frac{b}{c} = v = \frac{2pq}{q^2+p^2}$. Let $q^2 + p^2 = \beta c$. This leads to $\beta a = q^2 - p^2$ and $\beta b = 2pq$. **Claim:** $\beta = 1$.

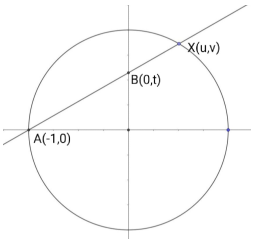

Fig. 2 The line $y = t(x+1)$ with slope t

Proof. Since $\beta \mid (q^2 + p^2)$ and $\beta \mid (q^2 - p^2)$, $\beta \mid 2q^2$ and $\beta \mid 2p^2$. As p and q are co-prime, $\beta \mid 2$. Therefore, β is only 1, as $\beta \nmid 4$. This establishes the claim. □

All primitive triangles can be obtained with $p, q \in \mathbb{Z}$: $a = q^2 - p^2$, $b = 2qp$, and $c = q^2+p^2$, where a+b is odd. Define, $S = \{(u, v) : u^2+v^2 = 1\}$. The triplet (a,b,c) corresponds to the pair (u,v) through the parametrization form of u and v, achieved by selecting $t = \frac{p}{q}$. Thus, for $(u, v) \in S$, we have $(a, b, c) \in C_n$ and $(x, y) \in E_n$ with

$$(u, v) \longleftrightarrow (a, b, c) \longleftrightarrow \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right).$$

2.3 Generalization: CNP (θ - Congruency)

This generalization broadens the conditions for a Congruent Number Problem (CNP) by considering wider angle ranges. Let θ be an angle within $[\frac{\pi}{3}, \pi]$. An integer n is termed 'θ-congruent' if there exists a rational-sided triangle with a maximum angle of θ and an area equal to n. In mathematical terms, this translates to the existence of rational values for a,b, and c that satisfy $a^2+b^2-2ab\cos\theta = c^2$, $n = \frac{ab\sin\theta}{2}$. We classify $\theta \in [\frac{\pi}{3}, \pi]$ as 'admissible' if both $\sin\theta$ and $\cos\theta$ lies in $\mathbb{Q}$. This requirement is fundamental. For rational points (u,v) on the unit circle, the parametric equations are $u = \frac{1-t^2}{1+t^2}$, and $v = \frac{2t}{1+t^2}$. Here, t represents the slope of the line connecting (-1,0) and $(u, v) = (\cos\theta, \sin\theta)$. By defining $u = \cos\theta = \frac{1-t^2}{1+t^2}$, and $v = \sin\theta = \frac{2t}{1+t^2}$, we establish the relationship Now we have, $\tan\frac{\theta}{2} = \frac{\sin\theta}{1+\cos\theta} = t$.

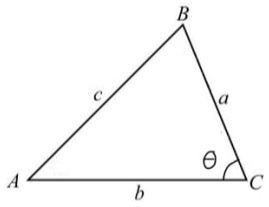

Fig. 3

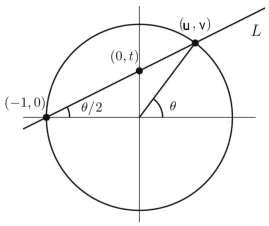

Fig. 4

Therefore, for every $\theta \geq \frac{\pi}{3}$ or equivalently $t \geq \frac{1}{\sqrt{3}}$, a distinct generalized congruent number problem arises. The case where $\theta = \frac{\pi}{2}$, or $t = 1$, corresponds to the classical congruent problem. L. Rolen's paper [11] introduces the concept of aberrant (where $m^2 + 1 \in \mathbb{Q}$) and 'generic' pairs (where this condition is not met). For each aberrant m, there is a unique square-free natural number n such that $mn \in \mathbb{Q}$ and the pair (n,m) is also aberrant. An associated elliptic curve, denoted by $E_{n,\theta_m} : y^2 = x(x - \frac{n}{m})(x + nm)$, corresponds to a triangle with sides $a = b = \sqrt{\frac{n}{m}.(m^2 + 1)}$ and $c = 2.\sqrt{\frac{n}{m}}$. This triangle has an angle θ_m and area n, provided (n,m) is aberrant.

2.4 Birch and Swinnerton-Dyer (BSD) conjecture

The rank of an elliptic curve, denoted as r, quantifies the size of its set of rational points. While we have some understanding of the rank's properties, its determination remains challenging. Computation of the rank is feasible for small values of r, but for larger r, we can often only establish a lower bound. In 1967, Tate and Shafarevich demonstrated that the rank r can grow unbounded in function fields, although this remains an open question for number fields. Noam Elkies discovered the largest known example, an elliptic curve with $r = 28$, in 2006. Numerous inquiries about elliptic curve ranks remain unanswered, including whether there exists an upper bound. Currently, no algorithm exists to ascertain the rank, and the possible integer values in this context are unknown. The Birch and Swinnerton-Dyer (BSD) conjecture addresses matters related to both the algebraic rank and analytic rank. The former refers to the rank r in the Mordell-Weil theorem, while the latter will be defined later. The formulation of BSD starts by considering the solutions to the Weierstrass equation $y^2 = x^3 + Ax + B$ (mod p), where p is a prime. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with integer coefficients A and B. Through reduction modulo a prime p, we can derive a new elliptic curve E', expressed as $E' : y^2 = x^3 + A'x + B'$ with coefficients A' and B' in the finite field $\mathbb{F}p$. However, it is crucial to ensure that the new discriminant remains nonzero in $\mathbb{F}p$. A good reduction at prime p occurs when p does not divide $\triangle$, while a bad reduction happens when p divides $\triangle$. The Birch and Swinnerton-Dyer conjecture proposes that if the rank of an elliptic curve E is sizable, then on average, E should possess more than p points (mod p) [18].

Theorem 2 (Due to Hasse)**.** *Let E be an elliptic curve, $y^2 = x^3 - Ax + B$ with $A, B \in \mathbb{F}_p$. Then $\mid (\#E(\mathbb{F}_p) = N_p) - p + 1 \mid \leq 2\sqrt{p}$, for every prime number p not dividing $\triangle$.*

In the 1960s at Cambridge University, Birch and Swinnerton-Dyer used EDSAC-2 to compute $\prod_{p \leq X} \frac{N_p}{p}$, leading to the conjecture.

Conjecture (weak BSD):

Let E be an elliptic curve over $\mathbb{Q}$, let r be its' rank, and let N_p denotes the number of points

on E (mod p). Then as $X \to \infty$ for some constant C depending only on E, we have

$$\prod_{p \leq X} \frac{N_p}{p} \sim C.(logX)^r.$$

A more refined version will be discussed later. The modern form of BSD conjecture involves L-functions of elliptic curves. The L -function $L(E, s)$ for an elliptic curve $E(\mathbb{Q})$ is given by:

$$L(E, s) = \prod_{p \nmid 2\triangle} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

where $a_p = p + 1 - N_p$ and $\triangle$ is the curve's discriminant. [12]. This product converges only when $s \in \mathbb{C}$ satisfying $Re(s) > \frac{3}{2}$.

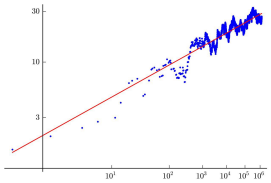

Fig. 5 Graph of $\prod_{p \leq X} \frac{N_p}{p}$ for E: $y^2 = x^3 - 5x$, with X ranging up to the first 10^6 primes. X-axis: log(log(X)), Y-axis: log scale. The conjecture predicts a linear pattern with a slope equal to the curve's rank (here, 1). The line is drawn accordingly.

A conjecture due to Hasse: *$L(E, s)$ should have a holomorphic continuation as a function of s to the entire complex plane!* [13].

It's relevant to consider the value and order of vanishing at $s = 1$.

Theorem 3 (Wiles et al, 1995)**.** *For any elliptic curve E, the L-function $L(E, s)$ has a holomorphic continuation to the entire complex plane.*

At $s = 1$, $\frac{1}{1-a_p p^{-s}+p^{1-2s}}$ becomes $\frac{1}{1-a_p p^{-1}+p^{-1}} = \frac{p}{p+1-a_p} = \frac{p}{N_p}$. Thus we have, $L(E, 1) = \prod_{p \nmid 2\triangle} \frac{1}{1-a_p p^{-s}+p^{1-2s}} = \prod_{p \nmid 2\triangle} \frac{p}{N_p}$. Another equivalent form of the earlier weak BSD conjecture is that *the holomorphic function $L(E, s)$ has a zero of order r ($r_{Analytic}$) at $s = 1$*, which is succinctly expressed as *for any $E(\mathbb{Q})$, $r_{Algebraic} = r_{Analytic}$.*

Conjecture (strong BSD):

The Taylor series expansion of $L(E, s)$ at $s = 1$ has the following form,

$$L(E, s) = c_E(s - 1)^r + \textit{higher order terms}$$

, where $c_E = \frac{1}{r!} L^{(r)}(E, 1)$ with $r = r_{Analytic}$ and $r_{Algebraic} = r_{Analytic}$.

Originally posed for $\mathbb{Q}$, this conjecture was later extended to all abelian varieties over global fields by J. Tate and refined by Gross, Deligne, Beilinson, Bloch, and Kato. [19] Another version of the stronger BSD conjecture relates to the finiteness of the *Tate-Shafarevich* group and other complex factors. However, this variation won't be discussed in this article.

Theorem 4 (Coates and Wiles, 1977)**.** *If E be an elliptic curve of the form $y^2 = x^3 + Ax$ or $y^2 = x^3 + B$ and if $r_{Analytic} = 0$, then BSD conjecture is true for E.*

Theorem 5 (Gross, Zagier, and Kolyvagin, 1989)**.** *If $r_{Analytic} = 0$ or 1 for an elliptic curve E, then the BSD conjecture is true for E.*

Theorem 6 (Skinner, Urban, and Zhang, 2013)**.** *If $r_{Algebraic} = 0$ or 1 for an elliptic curve E, and if E satisfies some further conditions*[3] *then BSD is true.*

Theorem 7 (Bhargava and Sankar, 2013)**.** *At least 83% of elliptic curves have $r_{Algebraic} = 0$ or 1.*

[3] For some prime $p \geq 5$, E has *p-Selmer* rank 0 or 1, E has good ordinary or multiplicative reduction at p, etc.

Theorem 8 (Bhargava, Skinner, and Zhang, 2014)**.** *The Birch and Swinnerton-Dyer conjecture is true for than* 66% *of all elliptic curves* $E(\mathbb{Q})$ *(when ordered by height).*

- Many mathematicians speculate that a substantial number of elliptic curves probably possess an analytic or algebraic rank of 0 or 1, although this remains unproven.
- In 2010-2012, Bhargava- Sankar showed that the average rank of all elliptic curves over $\mathbb{Q}$ is less than 1.
- Goldfeld-Katz-Sarnak conjectured that the average rank is to be exactly 0.5.

Via elliptic curves, the Birch and Swinnerton-Dyer (BSD) conjecture also plays a very important role in the progress of the congruent number problem.

2.5 Tunnell's work and few developements

J. B. Tunnell made a significant contribution to the CNP in 1983. By utilizing elliptic curve arithmetic, he identified a necessary condition for the problem and demonstrated its sufficiency under the assumption of the weak Birch and Swinnerton-Dyer conjecture. [14]

Theorem 9 (Tunnell, 1983)**.** *Let n be a square-free positive integer. Define* $a(n)$*,* $b(n)$*,* $a'(n)$*,* $b'(n)$ *as follows:*

$$\begin{aligned} a(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = n\}, \\ b(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 32z^2 = n\}, \\ a'(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 : 8x^2 + 2y^2 + 16z^2 = n\}, \\ b'(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 : 8x^2 + 2y^2 + 64z^2 = n\} \end{aligned}$$

For odd n, if n is a congruent number, then $a(n) = 2b(n)$*; for even n, if n is a congruent number, then* $a'(n) = 2b'(n)$*. Moreover, if the weak Birch and Swinnerton-Dyer conjecture is true for the elliptic curve* $E_n : y^2 = x^3 - n^2x$*, then the conditions are also sufficient.*

Remark: Tunnell's theorem offers an unconditional approach to establish the non-congruence of a square-free integer n. It also provides a conditional method to demonstrate the congruence of n, contingent upon the validity of the BSD conjecture.

1. If n is odd and $a(n) \neq 2b(n)$, then n is not a congruent number. If n is even, and $a'(n) \neq 2b'(n)$, then n is not a congruent number.
2. Let the weak Birch Swinnerton-Dyer conjecture is true for the elliptic curve $E_n : y^2 = x^3 - n^2x$. If n is odd and $a(n) = 2b(n)$, then n is a congruent number. If n is even, and $a'(n) = 2b'(n)$, then n is a congruent number.
3. To each $E_n : y^2 = x^3 - n^2x$, there is a associated L-function $L(E_n, s)$.

Theorem 10 (Coates and Wiles)**.** *If* E_n *has infinitely many rational solutions, then* $L(E_n, s = 1) = 0$.

The converse of this theorem has also been demonstrated. If the L-function $L(E_n, 1)$ equals 0, it implies a positive analytic rank. Following the Birch and Swinnerton-Dyer conjecture, a positive algebraic rank is anticipated. In simpler terms, the elliptic curve E_n is expected to have an infinite number of rational points [13]. We can thus conclude that n is congruent if and only if there exist an infinite number of rational solutions (x,y) on the elliptic curve E_n, which can be stated as n being congruent if and only if $L(E_n, 1) = 0$. Consequently, when $L(E_n, 1) \neq 0$, n is a non-congruent number.

Examples:

1. For n=1,

$$a(1) = \#\{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = 1\}$$
$$= \{(0, \pm 1, 0)\} = \#\{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 32z^2 = 1\} = b(1).$$

So, $a(1) \neq 2b(1)$. Thus, 1 is not a congruent number.

2. For n=2,

$$a'(2) = \#\{(x,y,z) \in \mathbb{Z}^3 : 8x^2 + 2y^2 + 16z^2 = 2\}$$
$$= \{(0, \pm 1, 0)\} = \#\{(x,y,z) \in \mathbb{Z}^3 : 8x^2 + 2y^2 + 64z^2 = 2\} = b'(2).$$

So, $a'(2) \neq 2b'(2)$. Thus, 2 is not a congruent number. Similarly for n=3,

$$a(3) = \#\{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = 3\}$$
$$= \{(\pm 1, \pm 1, 0)\} = \#\{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 32z^2 = 3\} = b(3).$$

So, $a(3) \neq 2b(3)$. Thus, 3 is not a congruent number.

So, Tunnell's Theorem is really helpful.

Theorem 11 (Stephen, 1975)**.** *If the weak Birch and Swinnerton-Dyer conjecture is true, then any positive integer $n \equiv 5, 6, 7$ (mod 8) is a congruent number.*

Proof. Suppose, $n \equiv 5, 6, 7$ (mod 8) is a positive integer. Let $n = a^2b$ where b is the square-free part. If a is even, then $n = 4m^2b$ for some positive integer m. Which implies that $n \equiv 0$ (mod8). So we consider a is odd. Therefore for some positive integer m, $n = (2m+1)^2b$ (mod 8) $= 4m^2b + 4mb + b$ (mod 8) $\equiv b$ (mod 8). Thus we may assume n is square-free. n can not be even as well as $\equiv 5, 7$ (mod 8), thus it must be odd. If $n \equiv 5, 7$(mod 8) is odd, then we need to check solutions to $2x^2 + y^2 + 8z^2 \equiv 5, 7$(mod 8) and $2x^2 + y^2 + 32z^2 \equiv 5, 7$(mod 8) i.e. solutions to the equation $2x^2+y^2 \equiv 5, 7$ (mod 8). There is no integer solution to this equation. So we have, $a(n) = 0 = b(n)$. Hence $a(n) = 2b(n)$. If the weak Birch and Swinnerton-Dyer conjecture is true, then Tunnell's theorem implies that n is a congruent number. n can not be odd as well as $\equiv 6$ (mod 8), thus it must be even. If $n \equiv 6$(mod 8) is even, then we need to check solutions to $2y^2 \equiv 6$(mod 8). Then this equation has no integer solution. So we have, $a'(n) = 0 = b'(n)$. Hence $a'(n) = 2b'(n)$. If the weak Birch and Swinnerton-Dyer conjecture is true, then Tunnell's theorem implies that n is a congruent number. □

Example:

The prime number $n = 157 \equiv 5$ (mod 8), indicating that it is a congruent number. Don Zagier computed the sides of the smallest right triangle with an area of 157. The sides X, Y, and hypotenuse Z are given by:

$$X = \frac{6803298487826435051217540}{411340519227716149383203}, \quad Y = \frac{411340519227716149383203}{21666555693714761309610},$$
$$Z = \frac{224403351770433696992455751309067486316094847204 1}{8912332268928859588025535178967165700164808 30}$$

J.S. Chahal [15] disproved the converse of the aforementioned theorem. He demonstrated that a square-free number a is not admissible if $a \equiv 0, 4$ (mod 8).

Theorem 12 (J. S. Chahal)**.** *Every(permissible) residue class modulo eight contains infinitely many congruent numbers.*

Recently M. A. Bennett [16], showed that one can replace the *"modulo 8"* term in the above theorem with *"modulo m"*, for any integer $m > 1$.

Theorem 13 (M. A. Bennett)**.** *If m is a positive integer and x is any integer, then $\exists$ infinitely many (not necessarily squarefree) congruent numbers n with $n \equiv x$ (mod m). If further,*

$gcd(x, m)$ is squarefree, then $\exists$ infinitely many (squarefree) congruent numbers with $n \equiv x$ (mod m).

3 Discussion

To quote John Coates (PNAS, 2012), "*The Congruent Number Problem, the written history of which can be traced back at least a millennium, is the oldest unsolved major problem in number theory, and perhaps in the whole of mathematics*". Throughout the previous section, we explored the diverse connections of the congruent number problem. A notable breakthrough in this area was achieved by J. Tunnell. His findings can be summarized as follows: for odd n, the value of $L(E_n, 1)$ is a nonzero constant multiple of $(a(n) - 2b(n))$, and for even n, the value of $L(E_n, 1)$ is a nonzero constant multiple of $(a'(n) - 2b'(n))$. In essence, Tunnell's theorem provides a method to confirm the non-congruence of a given number. The converse part of Tunnell's theorem holds true if the weak BSD conjecture is valid.

Hasse- Weil conjecture:

Let E be an elliptic curve over $\mathbb{Q}$. Then $L(E, s)$ has an holomorphic continuation to a meromorphic function on $\mathbb{C}$, and $L^*(E, s) = N_E^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E, s)$ satisfies the functional equation, $L^*(E, s) = w_E L^*(E, 2 - s)$ where, $w_E = \pm 1$ (the root number) and N_E is the conductor of the curve.

If $w_E = -1$, the functional equation implies a zero at $s = 1$ for both $L^*(E, s)$ and $L(E, s)$. On the other hand, $w_E = +1$ if and only if $L(E, s)$ has an even-order zero at $s = 1$. The Birch and Swinnerton-Dyer conjecture establishes a connection between the algebraic rank of an elliptic curve and its analytic rank. A Parity conjecture also links the root number w_E to the parity of $r_{Analytic}$.

Parity conjecture:

Let $E(\mathbb{Q})$ be an elliptic curve of rank r. Then $w_E = (-1)^{r_{Analytic}}$.

The algebraic rank is even for $w_E = +1$ and odd for $w_E = -1$. In his paper [19], T. Dokchitser mentioned, elliptic curves with root number $w_E = -1$ must possess an infinite number of rational points. The Parity conjecture is an arithmetic statement independent of L-functions, often serving as the sole method to predict the existence of infinitely-ordered points on any elliptic curve. The Parity conjecture is applicable to $E_n(\mathbb{Q})$ since this set is a specific subset of $E(\mathbb{Q})$.

Stephens initially employed the Parity conjecture in the context of the congruent number problem, demonstrating that Selmer's second conjecture implies the congruence of positive integers $n \equiv 5, 6, 7$ (mod 8) as congruent numbers [20].

The modularity theorem (formerly called the Taniyama–Shimura conjecture, Taniyama-Weil conjecture, or modularity conjecture for elliptic curves) states that *elliptic curve $E(\mathbb{Q})$ is modular*, which can be simply stated as *the L-function of the modular form is the L-function of the elliptic curve.* By the modularity theorem both L-functions extend analytically to all of $\mathbb{C}$. [17] In the preceding section, we established a link between congruent numbers and a special class of elliptic curves over $\mathbb{Q}$. Using the modularity theorem we can establish a connection between congruent numbers and modular forms. This relationship is intricately tied to the Galois representations associated with both elliptic curves and modular forms, which are, in fact, identical for a congruent number elliptic curve and a modular form. Tunnell's Theorem is a significant result of Waldspurger's Theorem. Waldspurger's Theorem relates

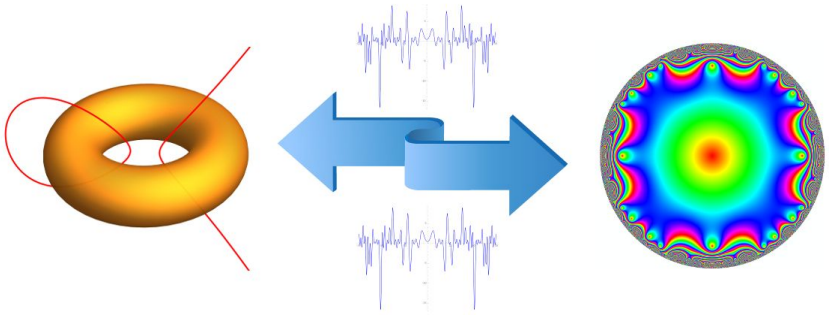

Fig. 6 Connection of elliptic curves and modular forms using their L-functions. This picture is due to Prof. Andrew Sutherland (MIT, USA).

the critical value of the $L - function$ of a cusp form Φ to the n_{th} coefficient of a modular form of half-integral weight. In explicit applications, such as Tunnell's Theorem, it is necessary to compute the space of cusp forms that are "Shimura equivalent" to a new form of even integral weight. Shimura's decomposition theorem allows for decomposition into irreducible components, enabling explicit computation and application.

4 Conclusion

This article illustrates how the investigation of congruent numbers serves as inspiration for exploring elliptic curves, showcasing the reciprocal impact between the two fields. This dynamic interplay underscores a compelling and intellectually enriching dual progression. Looking ahead, my research pursuits will center around Number Theory and Arithmetic Geometry.

Acknowledgement

This article is a product of the author's MSc thesis. The author expresses gratitude to their family, with special recognition to Supervisor Prof. Stephan Baier, for unwavering support and guidance. The author acknowledges Dr. Sajith G. for motivating the publication of their thesis work and extends thanks to other supporters.

References

[1] N. Koblitz, *An Introduction to Elliptic Curves and Modular Forms*, 2_{nd} edition, Graduate Texts In Mathematics 97, Springer-Verlag, Newyork, 1993.

[2] V. Chandrasekar, *The Congruent Number Problem*, Resonance 3 (2007) 33-45.

[3] L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, *Diophantine Analysis*, New York, 1952.

[4] K. Conrad, Faculty Featured Article: *The Congruent Number Problem*, [online accessed].

[5] Bill Hart, *A trillion triangles*, 2009, [Online accessed].

[6] R. Alter and T. B. Curtz, *A note on congruent numbers*, Math. Comp. 28 (1974) 303–305 and 30 (1976), 198.

[7] F. R. Nemenzo, *All congruent numbers less than 40000*, Proc. Japan Acad. Ser. A, Math. Sci. 74 (1998), 29-31.

[8] A. Rice and E. Brown, *Why Ellipses Are Not Elliptic Curves*, Mathematics Magazine 85, Mathematical Association of America, (2012), 163-176.

[9] H. M. Edwards, *A Normal Form for Elliptic Curves*, Bulletin of the American Mathematical Society 44 (2007), 393-422.

[10] A. L. Robledo, *Elliptic Curves, Modular Forms, and Their L-functions*, Student Mathematical Library, AMS, (1998), Vol-58.

[11] L. Rolen, *A Generalisation of the Congruent Number Problem*, International Journal of Number Theory 8 (2011).

[12] R.K. Ansah, R.K. Boadi, W.O. Denteh, A.Y. Sasu (2016), *Review of the Birch and Swinnerton-Dyer Conjecture*, American Journal of Mathematics and Statistics, 182-189.

[13] A. Wiles, the Birch and Swinjnerton-Dyer conjecture, [Online Accessed].

[14] J. B. Tunnell, *A classical diophantine problem and modular forms of weight* $\frac{3}{2}$, Inventiones Mathematicae 72 (1983), 323-334.

[15] J. S. Chahal, *Congruent numbers and elliptic curves*, The American Mathematical Monthly 113, (2006), 308-317.

[16] M. A. Bennett, *Lucas' square pyramid problem revisited*, Acta Arith. 105 (2002), 341-347.

[17] Fred Diamond, Jerry Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics 228, Springer.

[18] M. Bhargava, C. Skinner, W. Zhang, *A majority of elliptic curves over Q satisfy the Birch and Swinjnerton-Dyer conjecture*, arXiv, [Online Accessed].

[19] T. Dokchitser, Notes on the Parity conjecture, arXiv, [Online Accessed].

[20] L. C. Kellock and V. Dokchitser, Root Numbers and Parity Phenomena, arXiv, [Online Accessed].

[21] P. Khanra, *A Survey on the Congruent Number Problem and Its Connection with Elliptic Curves*, MSc thesis work, [Online Accessed].