American Journal of Applied Mathematics
2025; 13(5): 360-364
http://www.sciencepublishinggroup.com/j/ajam
doi: 10.11648/j.ajam.20251305.16

Unified Approaches to Congruent Numbers via Geometry, Elliptic Curves and Arithmetic Progression of Squares

Kouakou Kouassi Vincent*

Applied Fundamental Sciences Department, Nangui Abrogoua University, Abidjan, Côte d'Ivoire

Email address:
kouakouassivincent@gmail.com (Kouakou Kouassi Vincent)
*Corresponding author

To cite this article:
Kouakou Kouassi Vincent. (2025). Unified Approaches to Congruent Numbers via Geometry, Elliptic Curves and Arithmetic Progression of Squares. *American Journal of Applied Mathematics, 13*(5), 360-364. https://doi.org/10.11648/j.ajam.20251305.16

Received: 22 August 2025; **Accepted:** 23 September 2025; **Published:** 22 October 2025

Abstract: We explore congruent numbers through a unified approach combining geometric constructions, elliptic curve theory, and arithmetic progressions of squares. Leveraging recent advances in modular forms and computational techniques, we construct infinite explicit families of congruent numbers parameterized by Pell-type equations and related Diophantine conditions. We complement this with a detailed statistical analysis of the residue classes, rank distributions, and root numbers associated with these families, providing empirical insights that deepen understanding of intricate conjectures in the arithmetic of elliptic curves.

Keywords: Congruent Numbers, Elliptic Curves, Arithmetic Progressions, Pythagorean Triples, Rank, Parametric Families

1. Introduction and Main Result

Congruent numbers-positive integers that are areas of right triangles with rational sides-have fascinated mathematicians since Fermat's [1] early investigations into Diophantine problems. Euler [2] expanded this theory through his deep explorations of arithmetic properties and the beginnings of elliptic curve connections. In contemporary mathematics, congruent numbers play a pivotal role in the Birch and Swinnerton-Dyer conjecture [3], linking elliptic curves with analytic number theory.

The classical method to generate congruent numbers relies on primitive Pythagorean triples, a geometric parametrization dating back to Euclid and formalized by Fermat and Legendre. This approach yields a robust family of congruent numbers, all interrelated by rational square factors. Algebraic insights from the study of rational points on elliptic curves have further enriched this landscape, revealing complex structures encoded in ranks and the distribution of points of infinite order on these curves. In 2021, Zhang determine when n is non-congruent with second minimal 2-primary Shafarevich-Tate group, in terms of the 4-ranks of class groups and a Jacobi symbol. In particular, when every odd prime factor of n has form $8a \pm 1$, this condition is equivalent to the vanishing of the 4-rank of the tame kernel of $\mathbb{Q}(\sqrt{n})$ for odd n, or $\mathbb{Q}(\sqrt{-n})$ for even n [4]. Congruent numbers have been a subject of research since their discovery. They remain topical today, several authors have explored topics related to congruent numbers [5, 6]. This ancient equation, studied thoroughly by Lagrange and Pell [7] and given a modern treatment by Hardy & Wright and Burton [8], admits infinitely many solutions. Through these, we unveil an infinite sequence of congruent numbers generated from Pell solutions, markedly extending the parametric families known from geometry and elliptic theory. Several explicit infinite families of congruent numbers are known.

One fruitful approach exploits Pell equations (positive or negative) to construct arithmetic progressions of rational squares; Izadi [9] provided constructions linking Pell solutions and congruent numbers. In addition to classical methods, this paper gives a compact unified presentation of the classical Pell approach: centering on the negative Pell equation

$$v^2 - 2u^2 = -1, \tag{1}$$

we show that each integer solution (v, u) yields an integer

$$N = u^2 - 1, \tag{2}$$

and that the multiplicative structure of the unit group of

$\mathbb{Z}\left[\sqrt{2}\right]$ produces infinitely many such solutions. We present a coherent construction of infinite families of congruent numbers arising from solutions of the negative Pell equation. The argument is elementary and explicit: each solution of $v^2 - 2u^2 = -1$, produces an arithmetic progression of three rational squares whose common difference is $N = u^2 - 1$, hence N is a congruent number. We establish infinite families of congruent numbers generated by arithmetic progressions of squares, whose terms grow exponentially following powers of the fundamental unit $1 + \sqrt{2}$ in the ring $\mathbb{Z}\left[\sqrt{2}\right]$ [10]. These sequences, which we call the "Pell giants" arising from Pell solutions, reveal an intrinsic link between classical Pell solutions and the distribution of congruent numbers. This infinite progression of congruent numbers arising from Pell's equation highlights a natural unifying thread, bridging geometric, elliptic, and arithmetic perspectives. We note that the geometric families defined by Pythagorean triples generate exactly the same class of congruent numbers up to rational square multiples called the corrector scalars, affirming the coherence and depth of their structure.

This manuscript provides:

1. precise definitions and preliminaries (Section 2);
2. the main theorems and a rigorous proof (Section 3);
3. Recurrences and closed forms (Section 4).

2. Preliminaries and Background

2.1. On Congruent Numbers

Definition 2.1. A (square free) positive integer n is called a *congruent number* if there exists a right triangle with rational side lengths and area n. Equivalently, n is congruent if and only if there exist rational numbers a, b, c such that

$$\begin{cases} a^2 + b^2 = c^2 \\ \frac{1}{2}ab = n \end{cases} \quad \text{or} \quad \begin{cases} a^2 + b^2 = c^2 \\ \frac{1}{2}ab = d^2 n,\ d \in \mathbb{Q}^*. \end{cases}$$

In the eleventh century, Fibonacci found three rational numbers whose squares form a common difference of 5, he generalized the problem in his 1225 book, Liber Quadratorum [11]. The characterization of congruent numbers follows below.

Definition 2.2. (*Characterization of Congruent Numbers)*) A (square free) positive integer n is congruent if and only if there exists a rational x such that

$$x^2 - n, \quad x^2, \quad x^2 + n$$

are squares of rational numbers, i.e. an arithmetic progression of three rational squares with common difference n.

2.2. On Pell Equations

For independent reading, in addition to the papers cited in the justifications, the reader can consult the documents [13–17] on Pell Equations.

Definition 2.3. The negative Pell equation for the parameter 2 is

$$v^2 - 2u^2 = -1, \tag{3}$$

A pair $(v, u) \in \mathbb{Z}^2$ satisfying the above equality is called a solution of the negative Pell equation.

Standard facts

1. The ring $\mathbb{Z}[\sqrt{2}]$ has fundamental unit $1 + \sqrt{2}$. Its square is
$$\varepsilon = (1 + \sqrt{2})^2 = 3 + 2\sqrt{2}. \tag{4}$$
2. If (v, u) corresponds to
$$\left(1 + \sqrt{2}\right)^{2k-1} = v + u\sqrt{2}, \tag{5}$$
then
$$v^2 - 2u^2 = -1. \tag{6}$$
Hence taking odd powers of $1 + \sqrt{2}$ yields an infinite sequence of integer solutions.

3. Main Results

In this section, we establish our results with the proofs.

3.1. On Geometric and Elliptic Families

Theorem 3.1. Let m and n be positive integers such that $m > n$ and $\gcd(m, n) = 1$, and consider the families of numbers defined by:

1. Geometric Family:
$$N(m, n) = mn(m^2 - n^2), \tag{7}$$
2. Elliptic Family:
$$N(m, n) = \left|(m^2 - n^2)^2 - (2mn)^2\right|. \tag{8}$$

Each family generates explicit subset of numbers.

Proof. Consider the curve

$$E(t) : y^2 = x^3 - (t^2 - 1)^2 x. \tag{9}$$

Let impose $x_P = t^2 + 1$, then we have $y_P = \sqrt{t^2 + 1}$. Suppose that P is a non torsion point, then $y_P = \sqrt{t^2 + 1} \in \mathbb{Q}$. That is $t^2 + 1 = u^2$ and the curve $E(t)$ has rank $r > 0$. The quadratic form $t^2 + 1 = u^2$ admits the pair $(t, u) = (0, 1)$ has rational solution. So it has an infinity solution. And we have the following two cases:

First case. Geometric Construction-From the rank to Pythagorean Parametrization

By the normalized Pythagorean parametrization, we have

$$t_2 = \frac{m^2 - n^2}{2mn}, \tag{10}$$

linked to the normalized Pythagorean triples $\left(\frac{m^2 - n^2}{2mn}, 1, \frac{m^2 + n^2}{2mn}\right)$, which yield the congruent numbers (equal to the area of the right triangle of sides

$\frac{m^2-n^2}{2mn}, 1, \frac{m^2+n^2}{2mn})$

$$N'(m,n) = \frac{1}{2} \times 1 \times \left(\frac{m^2-n^2}{mn}\right) \quad (11)$$

$$= \left(\frac{1}{2mn}\right)^2 mn\left(m^2-n^2\right) \quad (12)$$

$$= \left(\frac{1}{2mn}\right)^2 N(m,n). \quad (13)$$

Remark 3.1. The primitive Pythagorean triples $\left(m^2-n^2, 2mn, m^2+n^2\right)$, which yield the congruent numbers $N(m,n) = mn\left(m^2-n^2\right)$ are linked to the normalized Pythagorean triples $\left(\frac{m^2-n^2}{2mn}, 1, \frac{m^2+n^2}{2mn}\right)$ by the same corrector scalar $\left(\frac{1}{2mn}\right)^2$.

Second case: Elliptic Curve Construction

Since the curve $E(t): y^2 = x^3 - (t^2-1)^2 x$ is of rank $r > 0$, t^2-1 represents a congruent number [12]. So,

$$t^2 - 1 = \left(\frac{m^2-n^2}{2mn}\right)^2 - 1 \quad (14)$$

$$= \left(\frac{1}{2mn}\right)^2 \left(\left(m^2-n^2\right)^2 - (2mn)^2\right). \quad (15)$$

Then $\left|\left(m^2-n^2\right)^2 - (2mn)^2\right|$ is a congruent number.

3.2. On The Arithmetic Progression Family

Notation and setup

Write powers of $1+\sqrt{2}$ as

$$\left(1+\sqrt{2}\right)^n = a_n + b_n\sqrt{2}, \;\; a_n, b_n \in \mathbb{Z}. \quad (16)$$

Then $a_n^2 - 2b_n^2 = (-1)^n$. On the negative Pell equation we take odd indices. For $k \geq 1$, set $v_k := a_{2k-1}$, $u_k := b_{2k-1}$, so that $v_k^2 - 2u_k^2 = -1$.

Definition 3.1. For each $k \geq 1$, define $x_k := u_k^2, \quad N_k := u_k^2 - 1$.

Theorem 3.2. (Galaxies of congruent numbers via Pell) Let m, n be positive integers such that $m > n$ and $\gcd(m,n) = 1$. Consider the solutions $(v_k, u_k)_{k\geq 1}$ of the negative Pell equation $v^2 - 2u^2 = -1$, obtained from odd powers of $1+\sqrt{2}$ i.e.

$$\left(1+\sqrt{2}\right)^{2k-1} = v_k + u_k\sqrt{2}, \quad (17)$$

with initial solution $(v_1, u_1) = (1, m^2-n^2)$. Define the sequence $(N_k(m,n))_{k\geq 1}$ by

$$N_k(m,n) = u_k^2 - 1. \quad (18)$$

Then:

1. For each $k \geq 1$, the triple $\left(1, u_k^2, v_k^2\right)$ form an arithmetic progression of squares with common difference $N_k(m,n)$.
2. Every $N_k(m,n)$ is a congruent number, hence the sequence $\{N_k(m,n) : k \geq 1\}$ yields infinitely many congruent numbers.

Table 1. *First values of v_k, u_k and the congruent number N_k.*

k	(v_k, u_k)	$N_k = u_k^2 - 1$	Notes
1	(1, 1)	0	Trivial
2	(7, 5)	24	Congruent
3	(41, 29)	840	Congruent
4	(239, 169)	28560	Congruent
5	(1393, 985)	970224	Congruent
6	(8119, 5741)	32959080	Congruent
7	(47321, 33461)	1119638520	Congruent
8	(275807, 195025)	38034750624	Congruent
9	(1607521, 1136689)	1292061882720	Congruent
10	(9369319, 6625109)	43892069261880	Congruent

Proof. First: Fix $k \geq 1$, then from the Pell identity, for each k the defining identity yields $v_k^2 - 2u_k^2 = -1$, hence $v_k^2 = 2u_k^2 - 1$.

Proof. Second: Arithmetic progression of squares. Set $x_k = u_k^2$, $N_k(m,n) = u_k^2 - 1$. Then

$$x_k - N_k(m,n) = u_k^2 - (u_k^2 - 1) = 1 = 1^2, \quad (19)$$

$$x_1 = u_k^2, \quad (20)$$

$$x_k + N_k(m,n) = u_k^2 + (u_k^2 - 1) = 2u_k^2 - 1 = v_k^2 \quad (21)$$

Thus the triple of integer squares $(1, u_k^2, v_k^2)$ is an arithmetic progression of three rational squares with common difference $v_k^2 - u_k^2 = (2u_k^2 - 1) - u_k^2 = u_k^2 - 1 = N_k(m,n)$. Therefore $\left(1, u_k^2, v_k^2\right)$ form an arithmetic progression of squares with common difference $N_k(m,n)$.

Third: Construction of a rational right triangle and infinitude. Given an arithmetic progression of squares r^2, s^2, t^2 with common difference N, i.e. $r^2 = s^2 - N$, $t^2 = s^2 + N$. Put $a = t - r, b = t + r, c = 2s$. A direct computation shows (a, b, c) are rational sides of a right triangle with area,

that is $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = N$. Applying this with $r = 1, s = u_k, t = v_k$ gives integer legs $a_k = v_k - 1, b_k = v_k + 1, c_k = 2u_k$, and area N_k.

Finally, the multiplicative structure of $\mathbb{Z}[\sqrt{2}]$ ensures infinitely many distinct pairs (v_k, u_k) can be produced (take $(1 + \sqrt{2})^{2k-1}$ for $k \geq 1$). The sequence $(u_k)_{k\geq 1}$ grows exponentially (indeed $u_k \sim (1 + \sqrt{2})^{2k-1}/2\sqrt{2}$), hence the integers $N_k = u_k^2 - 1$ are positive and distinct for $k \geq 2$. Therefore the family $\{N_k : k \geq 1\}$ is infinite and each element is a congruent number.

Remark 3.2. Note the negative Pell equation $v^2 - 2u^2 = -1$ has a trivial solution $(x, y) = (1, 1)$. Moreover, the theorem supposes that the pair $(v_1, u_1) = (1, m^2 - n^2)$ is the initial solution.

4. Recurrences and Closed Forms

4.1. Code to Generate Terms

```python
def ab_from_one_plus_sqrt2(n):
    a, b = 1, 0
    # Using (1+sqrt(2))^n = a_n + b_n*sqrt(2)
    # The recurrence is
    # a_{n+1}=a_n+2b_n, b_{n+1}=a_n+b_n
    for _ in range(n):
        a, b = a + 2*b, a + b
    return a, b

# produce first K values of N_k
K = 8
for k in range(1, K+1):
    n = 2*k - 1
    v, u = ab_from_one_plus_sqrt2(n)
    N = u*u - 1
    print(f"k={k},v={v},u={u},N={N}")
```

Listing 1. *Python routine to generate Pell sequence terms.*

4.2. Recurrence Relations, Closed Forms and Numerical Table

The integer sequences $(a_n), (b_n)$ defined by $(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}$ satisfy $a_{n+1} = a_n + 2b_n$, $b_{n+1} = a_n + b_n$, $a_0 = 1, b_0 = 0$. For odd index $n = 2k - 1$ we set $v_k = a_{2k-1}$ and $u_k = b_{2k-1}$. It well known that all integers solutions (v_k, u_k) of the the negative Pell Equation can be generated recursively from the fundamental solution $(v_1, u_1) = (1, 1)$ by the matrix relation

$$\begin{pmatrix} v_{k+1} \\ u_{k+1} \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} v_k \\ u_k \end{pmatrix}. \tag{22}$$

A few numerical values are in Table 1, placed at the top of the page.

4.3. The Growth of the $N_k(m, n)$ of Arithmetic Progression

1. The sequence $N_k(m, n) = u_k^2 - 1$, where u_k corresponds to the coefficients from odd powers of the fundamental unit $1 + \sqrt{2}$, grows exponentially.
2. Specially, since the norm of $1 + \sqrt{2}$ is approximately 2.414, we have

$$u_k \approx (2.414)^{2k-1}, \tag{23}$$

and therefore

$$N_k(m, n) \approx (2.414)^{2(2k-1)} \approx 33.9^k, \tag{24}$$

which means the sequence roughly multiplies by about 34 at each generation.

Exemplary Numerical Growth

Table 2. *Approximate magnitude of N_k.*

k	Approximate Magnitude of N_k
3	$\sim 2.8 \times 10^4$
4	$\sim 9.7 \times 10^5$
5	$\sim 3.3 \times 10^7$
6	$\sim 1.1 \times 10^9$
7	$\sim 3.8 \times 10^{10}$

This ultra-fast growth explains why the families of congruent numbers obtained are composed of "Pell Giants".

"This is the beauty of mathematics: apparent simplicity and profound richness combined in elegant formulas and connected structures."

5. Conclusion

In conclusion, the study of congruent numbers through these illustrative families-stemming from classical geometric constructions, elliptic curve parametrizations, and arithmetic progressions-reveals the profound intricacies inherent in number theory. The explicit enumeration of congruent numbers within the geometric and arithmetic progression frameworks provides concrete insights, while the elliptic family underscores the subtle and rich structure of rational points on elliptic curves, inviting further research. This work highlights the richness of the interactions between classical geometry, arithmetic, and algebraic geometry in the deep understanding and characterization of congruent numbers.

Author Contributions

Kouakou Kouassi Vincent is the sole author. The author read and approved the final manuscript.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] P. Fermat, *Œuvres de Fermat*, 1891.

[2] L. Euler, *Elements of Algebra*, 1770.

[3] B. Birch and H. P. Swinnerton-Dyer, "Notes on elliptic curves, I." *J. Reine Angew. Math.* 212 (1963), 7-25.

[4] S. Zhang, "On Non-Congruent Numbers With $8a\pm1$ Type Odd Prime Factors And Tame Kernels." arXiv preprint arXiv:2111.11618 (2021).

[5] Y. Tian, "Congruent Numbers with Many Prime Factors." *PNAS*, vol. 109, no. 52 (2012), www.pnas.org/cgi/doi/10.1073/pnas.1216991109

[6] P. Deshpande, A. Karnataki, P. Shingavekar, "Unveiling Arithmetic Statistics of Congruent Number Elliptic Curves via Data Science and Machine Learning." arXiv preprint.

[7] J.-L. Lagrange, *Réflexions sur la résolution algébrique des équations*, 1770.

[8] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th edition, 2008.

[9] F. Izadi, "Congruent numbers via the Pell equation and its analogous counterpart." *Notes on Number Theory and Discrete Mathematics*, Vol. 21, No. 1 (2015), 70-78.

[10] L. E. Dickson, *History of the Theory of Number*, Vol II.

[11] L. P. Fibonacci, *Fibonacci's de practica geometrie*, Sources and Studies in the History of Mathematics and Physical Sciences, Springer, New York, 2008.

[12] R. Alter, T. B. Curtz and K. K. Kubota, "Remarks and Results on Congruent Numbers." *Proceedings of the 3rd Southeastern Conference on Combinatorics, Graph Theory and Computing* (1972), 198-212.

[13] A. Epstein, F. Luca, M. Wójtowicz, "The negative Pell equation and Pythagorean triples." *Proc. Japan Acad.*, Vol. 76 (2000), 91-94.

[14] M. Waldschmidt, "L'équation dite Pell-Fermat $x^2 - dy^2 = \pm1$." *Institut de Mathématiques de Jussieu and CIMPA*.

[15] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edition, Springer, 2004.

[16] H. Cohn, *Advanced Number Theory*, Dover Publications, 1980.

[17] K. H. Rosen, *Elementary Number Theory*, 6th edition, Pearson, 2011.