Pure and Applied Mathematics Journal
2025; 14(5): 157-160
http://www.sciencepublishinggroup.com/j/pamj
doi: 10.11648/j.pamj.20251405.16

On a Family of Congruent Numbers Defined Modulo 72: A Conjectural Study

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). On a Family of Congruent Numbers Defined Modulo 72: A Conjectural Study. *Pure and Applied Mathematics Journal, 14*(5), 157-160. https://doi.org/10.11648/j.pamj.20251405.16

Received: 14 September 2025; **Accepted:** 18 October 2025; **Published:** 22 October 2025

Abstract: We investigate the interplay between the Chinese Remainder Theorem and the theory of congruent numbers through a modular approach to expressing integers as sums of three cubes. By analyzing congruence systems arising from specific residue classes modulo 8 and modulo 9, we classify the possible integers likely to be representable as sums of cubes based on their modular residues. We also explore computational methods applying this modular framework to identify explicit cube decompositions within these classes.

Keywords: Congruent Numbers, Chinese Remainder Theorem, Modular Arithmetic, Sums of Cubes, Diophantine Equations

1. Introduction

Congruent numbers have held a central place in number theory, from ancient mathematicians to modern developments. A positive integer n is called congruent if it is the area of a right triangle with rational side lengths. More formally, n is congruent if there exist rational numbers a, b, c such that

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

The problem of determining whether an integer is congruent is renowned for its difficulty. It translates into the question of existence of rational solutions to certain elliptic curve equations, linking geometry, analysis, and arithmetic. Historically, the study of congruent numbers traces back to ancient mathematicians like Diophantus [17] and Fibonacci [9], with seminal contributions from Fermat [16] in the 17th centuries. In the 20th century, modern breakthroughs by Tunnell [11] connected congruent numbers to elliptic curve theory and conjectures such as Birch and Swinnerton-Dyer [14, 15] enriching the depth and scope of this classical problem. Up to the weak Birch-Swinnerton-Dyer conjecture for the elliptic curve $E(n)$, an elegant characterization of congruent numbers has been obtained by Tunnel (see Koblitz [10], Theorem, p. 221, or Cohen [6], Theorem 6.12.4). Several authors, including Lagrange [12], Abdolmalki and Izadi [1] and Johnstone and Spearman [4] have made contributions to the study of congruent numbers. Hürlimann [2] revisited Tunnel's Congruent Number Criterion. Four elementary characterizations of congruent numbers were reviewed by Hürlimann [3].

The importance of congruent numbers appear in rational geometry, useful in modeling physical phenomena where exact ratios between lengths and areas are important. They help understand algebraic structures in elliptic curve theory, with ramifications in cryptography, mathematical physics, and the modeling of complex systems. The mystery surrounding these numbers means that their study continues to be a vibrant field of theoretical research.

Meanwhile, the problem of expressing integers as sums of three cubes—writing n as $a^3 + b^3 + c^3$ with integers a, b, c—attracts significant interest, particularly concerning modular restrictions. Conditions modulo 8 and modulo 9 impose strong limitations on the integers n that can admit such decompositions. A key step in our study lies in understanding the modular residues of the integers n, especially modulo 8 and modulo 9. In modular arithmetic, two integers are congruent modulo m if they leave the same remainder upon

division by m. This idea groups integers into equivalence classes, simplifying the study of their algebraic properties. For the congruent number conjecture and the sum-of-three-cubes problem, certain residue classes are privileged:

1. Modulo 8, only three residue classes matter: $5, 6, 7 \pmod 8$. These correspond to numbers that can represent the areas of right triangles with rational sides and satisfy particular modular square properties [5, 7, 10, 11].
2. Modulo 9, only residues $0, 1$, and $-1 \equiv 8 \pmod 9$ allow representations as sums of three cubes. This relates to the properties of cube residues modulo 9 and the algebraic structure of the integers modulo 9.

The intersection of these constraints defines nine residue classes modulo 72 (the least common multiple of 8 and 9) where the sum-of-cubes representation problem is focused. This modular stratification is a powerful tool guiding our theoretical and computational investigations. To tackle these challenges, the Chinese Remainder Theorem displays decisive power. It reduces complex modular constraints into simpler systems. Here, the Chinese Remainder Theorem helps classify congruent numbers and candidates for cube sums by their residue classes modulo 72. In this exposition, we explore this modular approach, combining theory and numerical experimentation to better understand congruent numbers and their sum-of-cubes decompositions. We analyze relevant congruence systems, identify meaningful residue classes, and develop methods for finding solutions, illustrated by explicit examples. This approach highlights the rich interplay among modular arithmetic, Diophantine equations, and algorithmic computation.

2. Main Result

Theorem 2.1. Let $a, b, c \in \mathbb{Z}$. If

$$n = |a^3 + b^3 + c^3|$$

is a congruent number, then

$$n \equiv r \pmod{72}$$

with

$$r \in \{37, 45, 46, 53, 54, 55, 62, 63, 71\}.$$

In other words, every congruent number that can be written as the sum of three positive cubes lies in one of these nine residue classes modulo 72.

Proof. A well-known classical conjecture from Alter, Curtz and Kubota [13] says that " an positive integer n is a congruent number if $n \equiv 5, 6, 7 \pmod 8$ (see also [8, 10, 11],). We also find in [5] "$n \equiv 5, 6, 7 \pmod 8$, and if the ii eak Birch Swinnerton Dyer conjecture holds for En then n is a congruent number". Next, consider n expressible as a sum of three cubes,

$$n = |a^3 + b^3 + c^3|,$$

with $a, b, c \in \mathbb{Z}$. Observe that cubes modulo 9 only take values in

$$\{-1, 0, 1\},$$

since for all integers x,

$$x^3 \equiv -1, 0, \text{ or } 1 \pmod 9.$$

Hence,

$$a^3 + b^3 + c^3 \equiv -1, 0, \text{ or } 1 \pmod 9.$$

By combining modulo 8 and modulo 9 congruences through the Chinese Remainder Theorem, since $\operatorname{lcm}(8, 9) = 72$, we have the results shown in Table 1.

Table 1. *Residue classes modulo 72 derived from the Chinese Remainder Theorem.*

Residue $\pmod 8$	Residue $\pmod 9$	Resulting Res. $\pmod{72}$
5	0	45
5	1	37
5	8	53
6	0	54
6	1	46
6	8	62
7	0	63
7	1	55
7	8	71

Thus, any congruent number expressible as a sum of three cubes lies in one of these nine residue classes modulo 72.

3. Statistical Commentary

Among the 322 congruent numbers less than 1000 identified in Lagrange's classical framework [12], our specific family—defined by numbers

$$n = |a^3 + b^3 + c^3|$$

with the modular constraints

$$n \equiv \{5, 6, 7\} \pmod 8$$
$$n \equiv \{-1, 0, 1\} \pmod 9$$
$$n \equiv \{37, ..., 71\} \pmod{72}$$

generates 112 distinct congruent numbers less than 1000.

Table 2 lists these 112 values of n.

Table 2. *List of the 112 congruent numbers $n < 1000$ in the studied family.*

37	45	46	53	54	55	62	63
71	109	117	118	125	126	127	134
135	181	189	190	197	198	199	206
207	215	253	261	262	269	270	271
278	279	287	333	334	341	342	343
350	351	359	397	405	406	413	414

485	486	487	495	503	541	549	550
557	558	559	566	567	575	613	622
629	630	631	638	639	647	685	694
701	702	703	710	711	757	766	775
782	783	791	837	838	845	846	847
854	855	863	901	909	910	917	918
919	927	935	973	981	989	990	991
998	999						

This represents approximately

$$\frac{112}{322} \approx 0.348$$

i.e., 34.8% of the known congruent numbers under 1000. This shows that our modular filter based on sums of cubes captures a substantial and meaningful portion of the congruent number set.

Moreover, these 112 numbers correspond to elliptic curves of rank 1. Rank 1 curves possess rich rational point structures that intimately relate to the congruency problem and the Birch and Swinnerton-Dyer conjecture. This suggests that our modular family not only filters a significant subset but also aligns with important arithmetic properties signaled by elliptic curve theory, reinforcing the deep connections between sums of cubes, modular congruences, and rational solutions on elliptic curves.

This is a significant outcome for computational experimentation and theoretical research, providing a focused framework for studying congruent numbers through the lens of sums of cubes and modular arithmetic.

4. Conclusion

This study highlighted a particular family of congruent numbers defined by stringent modular constraints on sums of three cubes, effectively reducing the search space through modular structures modulo 8 and 9, and then modulo 72. The finding that this family accounts for nearly $34,8\%$ of congruent numbers between 0 and 1000 underscores its richness and fundamental role in the arithmetic understanding of congruent numbers. This modular approach opens promising avenues for finer classification and efficient filtering in algorithmic searches for representations of congruent numbers.

Further work may extend these methods to larger intervals and explore connections with deep conjectures, such as the Birch and Swinnerton-Dyer conjecture, which links number theory and elliptic curves in this context.

Author Contributions

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

Conflicts of Interest

The author declares no conflict of interest.

References

[1] H. R. Abdolmalki and F. Izadi, New methods for obtaining new families of congruent numbers, *Notes on Number Theory and Discrete Mathematics*, 25(1), 14-24, 2019.

[2] W. Hürlimann, Bell's Ternary Quadratic Forms and Tunnel's Congruent Number Criterion Revisited, *Advances in Pure Mathematics*, 5, 267-277, 2015. http://dx.doi.org/10.4236/apm.2015.55027

[3] W. Hürlimann, A Congruent Twin Number Problem, *Pioneer Journal of Algebra, Number Theory and its Applications*, 1(1), 53-66, 2011.

[4] J. A. Johnstone and B. K. Spearman, On the distribution of congruent numbers, *Proceedings of the Japan Academy, Series A*, 2010.

[5] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, 2nd edition, Springer, The Arithmetic of Elliptic Curves. Graduate Texts in Math, 2009.

[6] H. Cohen, *Number Theory, Volume I: Tools and Diophantine Equations*, Graduate Texts in Mathematics, Springer Science + Business Media, LLC, New York, 2007.

[7] S. K. Chahal, Infinitely many congruent numbers in each congruence class modulo 8, *Journal of Number Theory*, 2000.

[8] K. Feng, Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture, *Acta Arithmetica*, 75(1), 71-83, 1996.

[9] L. Pisani, *Liber Quadratorum*, 1225, translation and commentary by L. E. Sigler, Springer, 1987.

[10] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, New York, 1984. https://doi.org/10.1007/978-1-4684-0255-1

[11] J. Tunnel, A Classical Diophantine Problem and Modular Forms of Weight 3/2, *Inventiones Mathematicae*, 72, 323-334, 1983. https://doi.org/10.1007/BF01389327

[12] J. Lagrange, Construction d'une table de nombres congruents, *Mémoires de la S. M. F.*, tome 49-50, 125-130, 1977.

[13] 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*, Boca Raton, 28 February-2 March 1972, 27-35.

[14] J. B. Birch and H. P. F. Swinnerton-Dyer, Notes on Elliptic Curves II, *Journal für die Reine und Angewandte Mathematik (Crelle's Journal)*, 218, 79-108, 1965. https://doi.org/10.1515/crll.1965.218.79

[15] J. B. Birch and H. P. F. Swinnerton-Dyer, Notes on Elliptic Curves I, *Journal für die Reine und Angewandte Mathematik (Crelle's Journal)*, 212, 7-25, 1963. https://doi.org/10.1515/crll.1963.212.7

[16] P. Fermat, *Œuvres de Fermat*, T. I-IV, Gauthier-Villars, 1891-1922.

[17] Diophantus, *Arithmetica*, édition de X. R. Charlier, 1893.