The congruent number problem, and Goldfeld's conjecture

Bogdan Grechuk • 4 Jan 2026

The just-published first 2026 issue of the *Annals of Mathematics* contains a paper by Burungale and Tian (Burungale and Tian 2026) which, among other results, establishes a striking and accessible theorem related to the classical congruent number problem.

A positive integer n is called a *congruent number* if it is the area of a right triangle with rational side lengths. Equivalently, $n = \frac{1}{2}ab$ for some positive rational numbers a and b such that the hypotenuse

$$c = \sqrt{a^2 + b^2}$$

is also rational. Determining whether a given positive integer is congruent is known as the *congruent number problem*. With a history stretching back more than 1000 years, it is one of the oldest unsolved problems in mathematics.

There is a deep and beautiful connection between congruent numbers and elliptic curves. If $n = \frac{1}{2}ab$ is a congruent number, then the quantities

$$x = \frac{n(a+c)}{b}, \qquad y = \frac{2n^2(a+c)}{b^2}$$

give a nonzero rational solution of the equation

$$y^2 = x^3 - n^2 x. \tag{1}$$

Conversely, if (x, y) is a rational solution of (1) with $y \neq 0$, then n is the area of a right triangle with rational side lengths

$$a = \left|\frac{x^2 - n^2}{y}\right|, \qquad b = \left|\frac{2nx}{y}\right|, \qquad c = \left|\frac{x^2 + n^2}{y}\right|.$$

Thus, the congruent number problem is equivalent to determining whether equation (1) has a rational solution with $y \neq 0$. It is known that if (1) has finitely many rational solutions, then all of them have $y = 0$. Hence, n is a congruent number if and only if equation (1) has infinitely many rational solutions.

Equation (1) is a special case of equation

$$y^2 = x^3 + Ax + B, \tag{2}$$

where $A, B \in \mathbb{Z}$ satisfy $4A^3 + 27B^2 \neq 0$. The curve defined by (2) is called an *elliptic curve*. A special case of famous Birch and Swinnerton-Dyer conjecture predicts that (2) has finitely many rational solutions if and only if its *analytic rank* is equal to 0, where analytic rank is a non-negative integer associated to any given elliptic curve. A special case of this conjecture for family (1) thus implies that n is a congruent number if and only if the analytic rank of (1) is positive.

A remarkable theorem of Tunnell (Tunnell 1983) gives a completely elementary reformulation of this analytic condition. Let $\Sigma(n)$ denote the set of integer solutions to

$$2 \cdot \gcd(n, 2)\, x^2 + y^2 + 8z^2 = \frac{n}{\gcd(n, 2)},$$

where gcd is the greatest common divisor. Then define

$$\mathcal{L}(n) = \#\{(x, y, z) \in \Sigma(n) : 2 \mid z\} - \#\{(x, y, z) \in \Sigma(n) : 2 \nmid z\},$$

where, as usual, $\#A$ is the number of elements in set A. Tunnell (Tunnell 1983) proved that the analytic rank of (1) is positive if and only if $\mathcal{L}(n) = 0$. Assuming the Birch and Swinnerton-Dyer conjecture, Tunnell's work implies that

$$n \text{ is a congruent number } \iff \mathcal{L}(n) = 0.$$

Since $\mathcal{L}(n)$ can be computed efficiently for any given n, this would yield a complete solution to the congruent number problem. Moreover, Tunnell proved unconditionally that if $\mathcal{L}(n) \neq 0$, then n is *not* a congruent number.

Computational data for small values of n suggest the following pattern.

- (a) Every positive integer $n \equiv 5, 6, 7 \pmod 8$ appears to be congruent.
- (b) The set of congruent numbers $n \equiv 1, 2, 3 \pmod 8$ appears to have density zero.

(There is no need to consider $n \equiv 0, 4 \pmod 8$, since one may restrict attention to square-free integers.)

In 2016, Smith (Smith 2016) made major progress on part (a) by proving that a positive proportion of integers congruent to 5, 6, or 7 modulo 8 are congruent numbers. In particular, a positive proportion of all positive integers are congruent. In subsequent work (Smith 2017), Smith established part (b) in full: the set of congruent numbers congruent to 1, 2, or 3 modulo 8 has zero natural density.

Smith's proof does not imply that $\mathcal{L}(n) \neq 0$ for almost all n in the relevant congruence classes. This was achieved by Burungale and Tian in their recent Annals paper (Burungale and Tian 2026).

Theorem 1 *Let $\mathcal{S}$ be the set of positive square-free integers congruent to 1, 2, or 3 modulo 8. There exists a subset $\mathcal{A} \subset \mathcal{S}$ of density one such that $\mathcal{L}(n) \neq 0$ for all $n \in \mathcal{A}$.*

Since $\mathcal{L}(n) \neq 0$ implies that n is not a congruent number, Theorem 1 implies Smith's density-zero result. The converse implication is not known. Recall that the condition $\mathcal{L}(n) \neq 0$ is equivalent to saying that the analytic rank of (1) is zero. A deep conjecture of Goldfeld (Goldfeld 1979), known as "even parity Goldfeld's conjecture" predicts that, in certain natural families of elliptic curves, exactly 50% should have analytic rank 0. Since exactly half of all square-free integers are congruent to 1, 2, or 3 modulo 8, Theorem 1 confirms the even parity Goldfeld conjecture for the family of congruent number curves (1). This is the first family of elliptic curves for which this conjecture has been proved.

References

Burungale, Ashay A., and Ye Tian. 2026. "A Rank Zero p-Converse to a Theorem of Gross–Zagier, Kolyvagin and Rubin." *Ann. Of Math. (2)* 203 (1): 1–13. https://doi.org/10.4007/annals.2026.203.1.1.

Goldfeld, Dorian. 1979. "Conjectures on Elliptic Curves over Quadratic Fields." *Number Theory Carbondale 1979*, 108–18.

Smith, Alexander. 2016. "The Congruent Numbers Have Positive Natural Density." *arXiv Preprint arXiv:1603.08479*.

———. 2017. "Selmer Groups, Class Groups, and Goldfeld's Conjecture." *arXiv Preprint arXiv:1702.02325*.

Tunnell, Jerrold B. 1983. "A Classical Diophantine Problem and Modular Forms of Weight 3/2." *Invent. Math.* 72 (2): 323–34.