Congruent Numbers and the Factor of 2

The Area Condition as an Arithmetic Requirement

Dunstan Low

A Philosophy of Time, Space and Gravity

ontologia.co.uk

March 31, 2026

Abstract

A positive integer n is congruent if it is the area of a right triangle with rational sides. We observe that the area formula $\frac{1}{2}ab = n$ forces a factor of 2: the rational sides must satisfy $ab = 2n$. This factor is shown to be equivalent to the condition that the associated elliptic curve $E_n : y^2 = x^3 - n^2x$ has positive rank over $\mathbb{Q}$, which by the Birch and Swinnerton-Dyer conjecture (proved for ranks 0 and 1 by Kolyvagin–Gross–Zagier) is equivalent to $L(E_n, 1) = 0$. The congruent number condition therefore reduces to the presence of a factor of 2 at two levels: in the area formula and in the arithmetic of the elliptic curve. The same factor of 2 appears explicitly in Tunnell's criterion. The argument uses only the classical equivalence between congruent numbers and elliptic curves, the known cases of BSD, and Tunnell's criterion.

1 Introduction

A positive integer n is a *congruent number* if there exists a right triangle with all three sides rational and area exactly n. The problem of determining which integers are congruent is one of the oldest unsolved problems in number theory.

The area of a right triangle with legs a, b and hypotenuse c is $\frac{1}{2}ab$. For the area to equal n:

$$\frac{1}{2}ab = n, \qquad a^2 + b^2 = c^2, \qquad a, b, c \in \mathbb{Q}. \tag{1}$$

The factor of $\frac{1}{2}$ is the first observation of this paper. It is not incidental: for $a, b \in \mathbb{Q}$ and $n \in \mathbb{Z}$, the product ab must equal $2n$, forcing a factor of 2 into the rational arithmetic of the triangle's sides. A right triangle of integer area with rational sides cannot bypass this halving.

The main observation is that this factor of 2 reappears at every level of the classical theory: in the area formula, in the elliptic curve's rank condition, in the L-function at $s = 1$, and explicitly in Tunnell's criterion. The congruent number condition is, in each formulation, a condition on the presence of a factor of 2.

2 The Elliptic Curve Connection

The classical connection between congruent numbers and elliptic curves was established by Birch, Stephens, and others [2]:

Theorem 1 (Equivalence with Elliptic Curve Rank)**.** *A positive integer n is congruent if and only if the elliptic curve*

$$E_n : \quad y^2 = x^3 - n^2 x \tag{2}$$

has at least one rational point of infinite order, i.e. $\operatorname{rank}(E_n(\mathbb{Q})) \geq 1$.

Sketch. Suppose n is congruent, realised by a rational right triangle with legs a, b and hypotenuse c satisfying $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = n$. Set

$$x = \left(\frac{c}{2}\right)^2, \qquad y = \frac{c(b^2 - a^2)}{8}. \tag{3}$$

One verifies directly that (x, y) satisfies $y^2 = x^3 - n^2 x$:

$$x^3 - n^2 x = \frac{c^6}{8} - n^2 \cdot \frac{c^2}{4} = \frac{c^2}{4}\left(\frac{c^4}{4} - n^2\right) = \frac{c^2}{4} \cdot \frac{c^4 - 4n^2}{4}. \tag{4}$$

Since $ab = 2n$ and $a^2 + b^2 = c^2$, one computes $c^4 - 4n^2 = c^4 - (ab)^2 = (c^2 - ab)(c^2 + ab) = (a-b)^2(a+b)^2/4 \cdot 4$, giving $y^2 = x^3 - n^2 x$ after simplification. This point has infinite order because the torsion subgroup of $E_n(\mathbb{Q})$ consists of the four points $\{O, (0,0), (\pm n, 0)\}$, none of which corresponds to a triangle [3].

Conversely, given a rational point (x, y) of infinite order on E_n with $x > 0$ and $y \neq 0$, set

$$a = \frac{n + y/x}{2} + \frac{n - y/x}{2}, \quad b = \left|\frac{n + y/x}{2} - \frac{n - y/x}{2}\right|, \quad c = 2\sqrt{x}. \tag{5}$$

One verifies $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = n$. See [2] Chapter 1 for the complete verification. □

Remark 1 (The Factor of 2 in the Correspondence)**.** *The standard map uses $x = (c/2)^2$ — dividing the hypotenuse by 2 is the central step. The factor of $\frac{1}{2}$ in the area formula and the halving of the hypotenuse in the correspondence are the same arithmetic operation.*

3 The Factor of 2 at Each Level

Proposition 2 (The Area Formula Forces a Factor of 2)**.** *If n is a congruent number realised by a rational right triangle with legs $a, b \in \mathbb{Q}$, then $ab = 2n$. In particular, the rational arithmetic of a and b necessarily includes a factor of 2.*

Proof. From $\frac{1}{2}ab = n$ we get $ab = 2n$ directly. Since $n \in \mathbb{Z}$, the product ab of the rational legs must be an even integer. This forces at least one factor of 2 in the numerator of ab after reducing to lowest terms. There is no rational right triangle of integer area for which this factor of 2 is absent. □

Proposition 3 (The Canonical Height Iterates Along Powers of 2)**.** *For a rational point P of infinite order on E_n, the canonical height is defined by the limit*

$$\hat{h}(P) = \lim_{k \to \infty} \frac{h([2^k]P)}{4^k}, \tag{6}$$

where h is the naïve height and $[2^k]P$ denotes the k-fold doubling of P under the group law. The canonical height is positive for points of infinite order.

Proof. Standard; see [3] Chapter VIII. The key point is that the limit is taken along the sequence of doublings $P, [2]P, [4]P, [8]P, \ldots$ — successive powers of 2 applied to the rational point. □

Remark 2 (Powers of 2 in the Height Definition)**.** *The canonical height is defined precisely by iterating multiplication by* 2 *on the elliptic curve. That the factor of* 2 *from the area formula reappears as the natural iteration direction for the height is the central observation of this paper. The arithmetic that forces* $ab = 2n$ *in the geometry of the triangle is the same arithmetic that drives the height along the sequence* $\{[2^k]P\}$ *on the curve.*

Proposition 4 (The L-Function at $s = 1$ and the Factor of 2)**.** *The completed L-function* $\Lambda(E_n, s) = (N/4\pi^2)^{s/2}\Gamma(s)L(E_n, s)$*, where* N *is the conductor of* E_n*, satisfies the functional equation*

$$\Lambda(E_n, s) = \varepsilon \cdot \Lambda(E_n, 2 - s), \qquad \varepsilon = \pm 1. \tag{7}$$

The symmetry is $s \mapsto 2-s$*, whose fixed point is* $s = 1$ *— the midpoint of* $[0, 2]$*, obtained by dividing the interval length by* 2*. The central value* $L(E_n, 1)$ *is the value at this midpoint.*

Proof. The functional equation is standard; see [4] Appendix C. The midpoint $s = 1$ is fixed by $s \mapsto 2 - s$ since $2 - 1 = 1$, and equals $\frac{0+2}{2}$ — half the sum of the endpoints. □

4 The BSD Condition

The Birch and Swinnerton-Dyer conjecture, in the case of congruent numbers, states:

Theorem 5 (BSD for E_n)**.** $\operatorname{rank}(E_n(\mathbb{Q})) \geq 1$ *if and only if* $L(E_n, 1) = 0$*.*

Remark 3 (Known Cases)**.** *Theorem 5 is proved for rank* 0 *(Coates–Wiles [7] for CM curves; Kolyvagin [6] in general when* $L(E, 1) \neq 0$*) and for rank* 1 *(Gross–Zagier [5] combined with Kolyvagin). For higher ranks the conjecture remains open. The congruent number results below that depend on BSD are stated with this qualification.*

Combining Theorem 1 and Theorem 5:

Corollary 6 (Congruent Number Condition via L-Function)**.** *Assuming BSD:* n *is congruent if and only if* $L(E_n, 1) = 0$*. Unconditionally: if* $L(E_n, 1) \neq 0$ *then* n *is not congruent (by Kolyvagin). If* $\operatorname{rank}(E_n(\mathbb{Q})) = 1$ *and* $L'(E_n, 1) \neq 0$ *then* n *is congruent (by Gross–Zagier and Kolyvagin).*

5 Tunnell's Criterion

Theorem 7 (Tunnell [1])**.** *Define:*

$$A_n = \#\{(x, y, z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = n\}, \tag{8}$$
$$B_n = \#\{(x, y, z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 32z^2 = n\}, \tag{9}$$
$$C_n = \#\{(x, y, z) \in \mathbb{Z}^3 : 8x^2 + 2y^2 + 64z^2 = n\}, \tag{10}$$
$$D_n = \#\{(x, y, z) \in \mathbb{Z}^3 : 8x^2 + 2y^2 + 16z^2 = n\}. \tag{11}$$

If n *is congruent then* $A_n = 2B_n$ *(for* n *odd) and* $C_n = 2D_n$ *(for* n *even). Assuming BSD, the converse holds.*

Remark 4 (The Factor of 2 in Tunnell's Criterion)**.** *The conditions $A_n = 2B_n$ and $C_n = 2D_n$ are explicit factor-of-2 conditions: the ratio of the two quadratic form counts must equal exactly 2. The quadratic forms B_n and D_n differ from A_n and C_n respectively by replacing $8z^2$ with $32z^2$ and $64z^2$ with $16z^2$ — a factor of 4 and a factor of $\frac{1}{4}$ respectively, both powers of 2. The congruent number condition is, at the level of Tunnell's explicit criterion, a condition on the ratio of two quadratic form counts being exactly a power of 2.*

6 The Factor of 2 at Every Level

We summarise the unified picture:

Theorem 8 (The Factor of 2 is the Congruent Number Condition)**.** *The following are equivalent (the last two assuming BSD):*

1. *n is the area of a right triangle with rational sides a, b, c; the area formula gives $ab = 2n$.*
2. *$\operatorname{rank}(E_n(\mathbb{Q})) \geq 1$; the canonical height of a generator is defined by doubling iteration $\{[2^k]P\}$.*
3. *$L(E_n, 1) = 0$; the vanishing occurs at the midpoint $s = 1 = \frac{0+2}{2}$ of the functional equation's reflection interval, obtained by dividing by 2.*
4. *$A_n = 2B_n$ (for n odd) or $C_n = 2D_n$ (for n even); the ratio of quadratic form counts equals 2.*

In every formulation, the congruent number condition is the presence of a specific factor of 2.

Proof. (1) $\Leftrightarrow$ (2): Theorem 1.
(2) $\Leftrightarrow$ (3): BSD (Theorem 5); unconditionally in the direction (3) $\Rightarrow \neg$(2) by Kolyvagin, and (2) $\Rightarrow$ (3) for rank 1 by Gross–Zagier–Kolyvagin.
(3) $\Leftrightarrow$ (4): Tunnell's theorem [1] via the theory of modular forms of weight $\frac{3}{2}$.
The factor of 2 in each formulation is identified in Propositions 2, 3, and 4, and Remark 5. □

Remark 5 (Connection to Perfect Numbers)**.** *A similar factor-of-2 obstruction appears in the theory of perfect numbers. For even perfect numbers $N = 2^{p-1}(2^p - 1)$, the sigma function satisfies $\sigma(2^{p-1}) = 2^p$ — the divisor sum closes through a power of 2. For odd perfect numbers, no sigma factor can be a power of 2 (by Euler's constraint and the Mersenne mod 4 observation), which provides a structural obstruction to their existence. In both cases, the factor of 2 serves as the criterion for a number-theoretic self-consistency condition.*

7 Status of This Paper

Remark 6 (What This Paper Proves and What It Assumes)**.** *The equivalence* (1) $\Leftrightarrow$ (2) *(Theorem 1) is classical and unconditional.*

The equivalence (2) $\Leftrightarrow$ (3) *depends on the Birch and Swinnerton-Dyer conjecture in full generality. In one direction — $L(E_n, 1) \neq 0$ implies $\mathrm{rank}(E_n) = 0$ implies n is not congruent — this is unconditional (Kolyvagin). In the other direction — n congruent implies $L(E_n, 1) = 0$ — this requires BSD.*

The equivalence (3) $\Leftrightarrow$ (4) *is Tunnell's theorem, proved unconditionally in one direction and conditionally on BSD in the other.*

The main observation of this paper — that the factor of 2 *appears explicitly at every level of the theory — is an observation about the classical results, not an additional conjecture. It does not require any new axioms or framework. The argument is complete as a structural observation. Whether it yields a new proof strategy for BSD or the congruent number conjecture is a separate question.*

References

[1] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983) 323–334.

[2] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, New York (1984).

[3] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York (1986).

[4] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York (1994).

[5] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986) 225–320.

[6] V. A. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $\mathrm{Sha}(E, \mathbb{Q})$ *for a class of Weil curves*, Math. USSR Izv. **32** (1989) 523–541.

[7] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977) 223–251.