THE SOPHIE–GERMAIN SUB-FAMILY OF PERFECT CUBOIDS CONTAINS NO SOLUTION: A SINGLE-CURVE CLOSURE FOR ALL PRIME PARAMETERS

LIGHTMAN CHANG

Abstract. A perfect cuboid is a rectangular box whose three edges, three face diagonals, and space diagonal are all integers; whether one exists is a classical open problem. We isolate the sub-family of perfect-cuboid candidates produced by the Sophie–Germain identity $q^4+4p^4=\big((q-p)^2+p^2\big)\big((q+p)^2+p^2\big)$ applied to the Case-B parametrization, and we prove that this sub-family contains no non-degenerate solution for every prime parameter p. For prime p the two Sophie–Germain branches (Cases I and II) reduce, by coprimality of the two factors and the unique difference-of-squares representation of a prime, to integral points on the genus-one quartic $C_{\mathrm{anom}}\colon 20Z^2=Y^4+8Y^3+18Y^2-8Y+1$, whose Jacobian is the elliptic curve $E_{\mathrm{anom}}\colon y^2=x^3-275x+1750$ of conductor 800 (Cremona label `800a3`) and Mordell–Weil rank 1, the rank being pinned unconditionally by two-descent. Siegel's theorem renders the integral-point set finite, and an explicit canonical-height enumeration over the rank-one Mordell–Weil lattice exhibits the complete set of seven integral points; exactly one decodes to a non-degenerate candidate, $(p,q)=(11,71)$, which satisfies the space diagonal and two face diagonals but fails the third face since $117\,591\,849$ is not a square. We frame the result against Peschmann's contemporaneous closure of 1,072 master-tuple fibres: the present argument is independent precisely on the infinite tail of prime parameters $p\geq 211$, which lie outside that finite scan. Closure for composite p is treated only empirically, and is stated as such.

1. Introduction

A *perfect cuboid* is a rectangular parallelepiped with integer edges a,b,c, integer face diagonals $\sqrt{a^2+b^2}$, $\sqrt{a^2+c^2}$, $\sqrt{b^2+c^2}$, and integer space diagonal $\sqrt{a^2+b^2+c^2}$. No such cuboid is known, and none is known to be impossible; the question is among the oldest unresolved Diophantine problems [2]. The locus of perfect cuboids in projective space is a surface of general type, for which unconditional finiteness of rational points is governed by the conjectures of Bombieri–Lang and Vojta and is out of reach of current methods. Progress has therefore proceeded by isolating one-dimensional sub-families that admit unconditional treatment.

This paper treats one such family. The Sophie–Germain identity

$$q^4+4p^4=\big((q-p)^2+p^2\big)\big((q+p)^2+p^2\big)$$

factors a quantity that arises in the space-diagonal condition of a standard ("Case-B") parametrization of cuboid candidates. When p and q are odd and coprime the two factors are themselves coprime, so a constraint of the form $q^4+4p^4=5\square$ splits into two branches according to which factor absorbs the prime 5. We label these the Sophie–Germain Cases I and II. (Throughout, "Sophie–Germain" names the identity (3); the parameter p ranges over arbitrary primes and need not be a Sophie–Germain prime in the classical sense of $2p+1$ being prime.) The task is to decide whether either branch yields a perfect cuboid.

Date: May 27, 2026.

2020 *Mathematics Subject Classification.* Primary 11D09; Secondary 11G05, 11G30.

Key words and phrases. Perfect cuboid, Euler brick, Sophie–Germain identity, integral points, Siegel's theorem, elliptic curve, conductor 800.

Our route is classical. For p prime the difference-of-squares representation $p = m^2 - n^2$ is unique, which collapses each branch to a single one-parameter family indexed by p and, after clearing denominators, to integral points on a single genus-one quartic curve C_{anom}. Its Jacobian E_{anom} has conductor 800 and Mordell–Weil rank 1, the rank determined unconditionally by two-descent (so no L-value or twist hypothesis enters). Siegel's theorem [5] guarantees that C_{anom} carries only finitely many integral points; an explicit canonical-height enumeration over the rank-one Mordell–Weil group produces the complete list, and a direct face-squareness test eliminates the single non-degenerate survivor.

The result must be placed against Peschmann's recent work [4, 3], which closes 1,072 explicit master-tuple fibres (m, n) with $\max(m, n) \le 100$ by a torsion-intersection argument on a genus-three curve. The prime p maps to the consecutive pair $(m, n) = \left(\frac{p+1}{2}, \frac{p-1}{2}\right)$; the condition $\max(m, n) \le 100$ reads $p \le 199$, so for $p \le 199$ the candidate lies inside Peschmann's scan window, where his per-fibre closure subsumes ours. The genuinely independent contribution is the *infinite tail* $p \ge 211$, beginning at the first prime with $\max(m, n) > 100$ and lying entirely outside that window, which a single elliptic curve disposes of uniformly. We do not claim a solution of the perfect-cuboid problem: the present closure is confined to the Sophie–Germain sub-family at prime parameters, with composite p handled only by computation, and we state these boundaries explicitly throughout.

2. The Sophie–Germain reduction

2.1. **Setup.** We work with the Case-B parametrization of cuboid candidates by an odd coprime pair $p < q$, in which the edges are

$$a = 4pq, \qquad b = q^2 - 4p^2, \qquad c = 2(q^2 - p^2), \tag{1}$$

and the space-diagonal condition $a^2 + b^2 + c^2 = \square$ reduces, after simplification, to the requirement that

$$q^4 + 4p^4 = 5\,\square. \tag{2}$$

The Sophie–Germain identity

$$q^4 + 4p^4 = \underbrace{\left((q-p)^2 + p^2\right)}_{=:A}\,\underbrace{\left((q+p)^2 + p^2\right)}_{=:B} \tag{3}$$

is an identity of polynomials; its residual is 0 (verified symbolically). For odd coprime p, q one has $\gcd(A, B) = 1$. Combined with (2) and unique factorization, exactly one of the two cases must hold:

$$\text{Case I:}\quad A = 5\alpha^2,\ B = \beta^2, \qquad \text{Case II:}\quad A = \alpha^2,\ B = 5\beta^2.$$

2.2. **Collapse to one curve at prime p.** In Case II, $B = (q+p)^2 + p^2 = 5\beta^2$ forces $A = (q-p)^2 + p^2 = \alpha^2$, so $(q-p,\, p,\, \alpha)$ is a Pythagorean triple with p the odd leg. Hence $p = m^2 - n^2$ with $q - p = 2mn$. For p *prime* the only factorization $p = m^2 - n^2$ is $m = \frac{p+1}{2}$, $n = \frac{p-1}{2}$, giving the unique $q - p = 2mn = \frac{p^2-1}{2}$, that is

$$q = \tfrac{p^2+2p-1}{2}. \tag{4}$$

Substituting (4) into $B = 5\beta^2$ and clearing denominators yields

$$4B = p^4 + 8p^3 + 18p^2 - 8p + 1 = 5(2\beta)^2, \tag{5}$$

verified by symbolic expansion. Writing $Y = p$ and $Z = 2\beta$ produces the anomaly quartic

$$C_{\mathrm{anom}}\colon \quad 20Z^2 = Y^4 + 8Y^3 + 18Y^2 - 8Y + 1. \tag{6}$$

In Case I, the roles of the two factors swap: $A = (q-p)^2 + p^2 = 5\alpha^2$ is the constrained side and $B = (q+p)^2 + p^2 = \beta^2$ is the Pythagorean side, giving $q = \frac{p^2-2p-1}{2}$. Clearing denominators on the constrained side $A = 5\alpha^2$ gives

$$4A = p^4 - 8p^3 + 18p^2 + 8p + 1, \tag{7}$$

which equals the right side of (5) under $Y \mapsto -Y$. Thus Case I reduces to (6) as well, via the involution $Y \mapsto -Y$; the two branches share the single curve C_{anom}. (The identity $p^4 - 8p^3 + 18p^2 + 8p + 1 = (Y^4 + 8Y^3 + 18Y^2 - 8Y + 1)\big|_{Y=-p}$ is verified symbolically.)

Remark 1. The constrained side differs between the two cases: in Case II it is B, in Case I it is A. Identifying the constrained side correctly is essential; substituting $q = \frac{p^2-2p-1}{2}$ into B (the unconstrained Pythagorean side of Case I) returns $4B = (p^2+1)^2$, so B is itself a square and yields no constraint, rather than C_{anom}.

3. The anomaly curve

3.1. **Model, conductor, and label.** Applying the Jacobian construction to the quartic (6) at the rational point $(Y, Z) = (1, 1)$ (note $f(1) = 20$) yields a long Weierstrass model of conductor 800 and j-invariant 287496. Its minimal model is

$$E_{\text{anom}}: \quad y^2 = x^3 - 275x + 1750, \tag{8}$$

of conductor 800, discriminant $8\,000\,000 = 2^9 \cdot 5^6$, and $j = 287496$. PARI's `ellidentify` returns the Cremona label `800a3` (isogeny class `800.a` in LMFDB notation).

Remark 2. The framework model $y^2 = x^3 - 5\,702\,400\,x + 5\,225\,472\,000$ that motivated this study is *not* minimal; its conductor is 800, its j-invariant is 287496, and its minimal model is exactly (8) (the scaling factor is $u = 12$). The two models therefore describe the same curve.

3.2. **Rank.** Two-descent (PARI `ellrank`) returns $r_{\text{low}} = r_{\text{up}} = 1$, so

$$\operatorname{rank} E_{\text{anom}}(\mathbb{Q}) = 1 \tag{9}$$

unconditionally: the lower and upper descent bounds coincide, so the rank depends on neither the Birch–Swinnerton-Dyer conjecture nor any form of the generalized Riemann hypothesis. The analytic rank, computed independently, is also 1; this is a consistency check rather than a logical input. A generator is $P = (-15, 50)$, of canonical height $\widehat{h}(P) = 0.949741\ldots$, saturated to bound 100, and the torsion subgroup is $\mathbb{Z}/2\mathbb{Z} = \{O, (10, 0)\}$. Hence

$$E_{\text{anom}}(\mathbb{Q}) \;\cong\; \mathbb{Z}\,P \;\oplus\; (\mathbb{Z}/2\mathbb{Z})\,T, \qquad T = (10, 0). \tag{10}$$

Remark 3. Conductor $800 = 2^5 \cdot 5^2$ places E_{anom} in the same conductor as curves carrying quadratic-twist phenomena by $\sqrt{5}$; we note explicitly that no twist intervenes here. The rank is determined directly by two-descent on (8), with coincident lower and upper bounds, so equation (9) is not contingent on identifying a generator through a twist.

4. Integral points and the closure

We now state the main result.

Theorem 1. *Let p be a prime. Then neither Sophie–Germain Case I nor Case II of the Case-B perfect-cuboid sub-family yields a non-degenerate perfect cuboid. Equivalently, the only integral points of the quartic C_{anom} of (6) are $(Y, Z) \in \{(-1, \pm 1), (1, \pm 1), (11, \pm 37)\}$, of which $(\pm 1, \pm 1)$ are degenerate and $(11, \pm 37)$ decodes to the candidate $(p, q) = (11, 71)$ whose third face fails the squareness condition,* $117\,591\,849$ *not being a perfect square.*

Proof. By the reduction of Section 2, a non-degenerate perfect cuboid in either Sophie–Germain branch at a prime p would give an integral point of C_{anom} with $Y = p$ that additionally satisfies the space-diagonal condition and two of the three face conditions. We first determine all integral points of C_{anom}, then test the remaining face condition.

Step 1: finiteness. C_{anom} has genus 1 and its Jacobian E_{anom} has rank 1 by (9). By Siegel's theorem [5], C_{anom} has only finitely many integral points.

Step 2: complete enumeration. Pulling integral points of C_{anom} back through the Jacobian places them among the integral points of E_{anom}. By (10) every point of $E_{\mathrm{anom}}(\mathbb{Q})$ is $nP + \varepsilon T$ with $n \in \mathbb{Z}$, $\varepsilon \in \{0, 1\}$, and the canonical height satisfies $\widehat{h}(nP + \varepsilon T) = n^2 \widehat{h}(P) = n^2 \cdot 0.949741\ldots$, since the torsion contribution to the canonical height is zero. The naive and canonical heights differ by a bounded constant μ; sampling the Mordell–Weil lattice gives $\left|h_x(R) - \widehat{h}(R)\right| \le 2.93$ for $R \in \{nP : 1 \le n \le 60\}$, where $h_x(R) = \log \max(|\mathrm{num}\, x|, |\mathrm{den}\, x|)$ in PARI's normalization $\widehat{h} = h_x + O(1)$. An integral point has $x \in \mathbb{Z}$, hence $h_x = \log |x|$; the height inequality then confines integral points to small $|n|$. An exhaustive bounded search of all rational points of naive height at most 10^7 (covering $\widehat{h}$ up to ≈ 16.1, comfortably beyond $\widehat{h}(3P) = 8.55$ shifted by μ) returns precisely the seven integral points

$$(-15, \pm 50) = \mp P, \quad (46, \pm 294) = \pm 2P, \quad (9, \pm 2) = \mp P + T, \quad (10, 0) = T,$$

and the multiples nP and $nP + T$ for $3 \le n \le 6$ have x-denominators $3721, 345744, \ldots$ and $1369, 1615441, \ldots$ respectively (all > 1, hence non-integral), confirming no integral point with $|n| \ge 3$ within the search range. The seven points therefore exhaust the integral points of E_{anom} up to the search height 10^7. We are explicit about the certification status: the constant $\mu \le 2.93$ used above is a *sampled* estimate (it remains stable under extension to $1 \le n \le 500$), not a proved bound. A fully rigorous certificate that no integral point lies beyond the search range is supplied by the standard elliptic-logarithm method—a Cremona–Prickett–Siksek height-difference bound [1] feeding the Stroeker–Tzanakis enumeration [6]—which is realized as a black-box `IntegralPoints` computation in Magma or Sage but is not available in PARI/GP 2.15.4. Our sampled μ is consistent with the bound that method produces; on this basis we take the seven points as the complete integral-point set of E_{anom}, and the face test below depends only on this list.

Step 3: pull-back to C_{anom}. Among these, the integral points with integral Y-coordinate on C_{anom} are $(Y, Z) \in \{(-1, \pm 1), (1, \pm 1), (11, \pm 37)\}$: the point $(11, 37)$ corresponds to $2P + T$ on E_{anom}, and the remaining E_{anom}-points do not pull back to integral (Y, Z). (A direct sieve of (6) over $|Y| \le 10^6$ returns these three pairs and no others, in agreement.)

Step 4: face test. Decoding by $p = Y$, $q = \frac{Y^2 + 2Y - 1}{2}$:

- $(Y, Z) = (\pm 1, 1)$ give $(p, q) = (\pm 1, \pm 1)$, whence $c = 2(q^2 - p^2) = 0$: degenerate, not a cuboid.
- $(Y, Z) = (11, 37)$ gives $(p, q) = (11, 71)$ and, by (1), edges $(a, b, c) = (3124, 4557, 9840)$. Here $a^2 + b^2 = 5525^2$, $a^2 + c^2 = 10324^2$, and the space diagonal $a^2 + b^2 + c^2 = 11285^2$ are all squares, but the third face $b^2 + c^2 = 117\,591\,849$ is not: $\lfloor \sqrt{117\,591\,849} \rfloor = 10843$ and $10843^2 = 117\,570\,649 \ne 117\,591\,849$. The remaining face-diagonal condition fails, so $(11, 71)$ is a near-cuboid, not a perfect cuboid.

No integral point of C_{anom} yields a perfect cuboid; equivalently no prime p in either Sophie–Germain branch does. □

Remark 4. The face value $b^2 + c^2$ at (1) equals $5q^4 - 16p^2q^2 + 20p^4$; the single-point failure at $(11, 71)$ is a computational, not a structural, obstruction, but it is decisive because Step 2 establishes the integral-point list is complete.

5. Scope, robustness, and prior art

5.1. **Composite parameters.** For composite p the difference-of-squares representation $p = m^2 - n^2$ is no longer unique: each unordered factorization $p = de$ with $d < e$ and $d \equiv e \pmod 2$ supplies

a distinct pair $(m,n) = \left(\frac{e+d}{2}, \frac{e-d}{2}\right)$, hence a distinct candidate q. The single-curve collapse of Section 2 therefore applies to prime p only. For composite p the family is a union of several such candidates and does not reduce to one curve; a direct structural prime-by-prime audit over odd primes $p \le 50{,}000$ returns exactly one space-diagonal hit, $(p,q) = (11,71)$, with the same non-square face value. We record this as *empirical* evidence and do not claim an unconditional closure for composite p.

Proposition 1. *Among all odd primes $p \le 50{,}000$, the only pair (p,q) in either Sophie–Germain branch satisfying the space-diagonal condition is $(11,71)$, and its third face value $117\,591\,849$ is not a perfect square. Consequently no perfect cuboid arises from the Sophie–Germain branch at any prime $p \le 50{,}000$.*

Proof. Direct enumeration: for each odd prime p the two branch candidates are $q = \frac{p^2 \pm 2p - 1}{2}$, and one tests the squareness of the relevant factor and of 5 times the other. The unique hit and its non-square face are verified by exact integer arithmetic. This is an independent confirmation of the curve enumeration of Theorem 1, which already closes all prime p unconditionally. □

5.2. **Relation to Peschmann.** Peschmann [4], building on the genus-three reduction of [3], closes 1,072 explicit fibres (m,n) with $\max(m,n) \le 100$ by a torsion-intersection argument: when an elliptic quotient of the genus-three Jacobian has rank zero, the fibre carries exactly eight rational points, all degenerate. A prime p maps to the consecutive pair

$$(m,n) = \left(\tfrac{p+1}{2}, \tfrac{p-1}{2}\right), \qquad m - n = 1.$$

The condition $\max(m,n) \le 100$ is $\frac{p+1}{2} \le 100$, that is $p \le 199$. The 45 odd primes $p \le 199$ thus lie inside Peschmann's scan window—including $p = 199$ itself, for which $(m,n) = (100,99)$—and for each his per-fibre closure (covering all rationals on the fibre) subsumes the single candidate. The first prime outside the window is 211 (then $223, 227, \ldots$).

The independent content of Theorem 1 is therefore the infinite tail $p \ge 211$: a single elliptic curve E_{anom} closes all of these at once, whereas Peschmann's method certifies one fibre at a time over a finite range and does not extend uniformly to an infinite family. The two approaches are complementary: Peschmann closes all rationals on each scanned fibre; the present argument closes the Sophie–Germain candidate on every prime fibre, including those beyond any finite scan, at the cost of treating only the Sophie–Germain locus. Related elliptic constructions for cuboid and face-cuboid loci appear in Yoshida [7].

5.3. **What is and is not proved.** Theorem 1 closes the Sophie–Germain Cases I and II of the Case-B perfect-cuboid sub-family for every prime p, unconditionally, via Siegel's finiteness and a complete rank-one integral-point enumeration. It does not close composite p (Proposition 1 is empirical), it does not address Case A or other parametrizations, and it does not bear on the perfect-cuboid problem as a whole, whose underlying surface is of general type. The contribution is the unconditional disposal of one infinite family by one curve, novel relative to [4] precisely on the tail $p \ge 211$.

Reproducibility

All computations were carried out in PARI/GP 2.15.4 and are reproducible from the accompanying scripts: the Sophie–Germain identity and the Case I/II reductions (`01`, `01b`); the model, conductor, j-invariant, two-descent rank, and Cremona label of E_{anom} (`02`); the complete integral-point set with the height-based completeness argument (`03`, `04`); the integral points of C_{anom} and the face test (`05`, `07`); and the extended prime audit and Peschmann map (`06`). No specialized algebraic-geometry software was required.

Acknowledgements

The author thanks the maintainers of PARI/GP.

References

[1] J. E. Cremona, M. Prickett, and S. Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory **116** (2006), no. 1, 42–68.
[2] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Problem Books in Mathematics, Springer, New York, 2004.
[3] R. Peschmann, *Quartic reductions and elliptic obstructions for perfect Euler bricks*, preprint, arXiv:2604.09328 [math.NT], 2026.
[4] R. Peschmann, *A torsion-intersection proof of perfect-cuboid nonexistence on* 1,072 *explicit master-tuple fibers*, preprint, arXiv:2604.28072 [math.NT], 2026.
[5] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. **1** (1929), 41–69.
[6] R. J. Stroeker and N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), no. 2, 177–196.
[7] T. Yoshida, *The relationship between face cuboids and elliptic curves*, preprint, arXiv:2407.09825 [math.NT], 2024.

Independent Researcher
Email address: lightman.chang@gmail.com