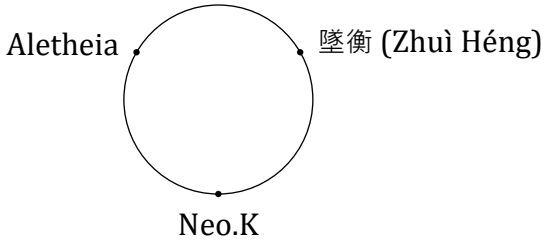
An explicit quadratic-twist family of the non-semistable curve 696.e1: a density of 1/24 by three routes, an arithmetic certificate, the isogeny and image questions settled, and a derived theorem candidate checked against its own router

A research programme's family for strong Birch–Swinnerton-Dyer beyond the semistable reach of a published method, recomputed: the anchor, the density and why it is not 1/48, a certificate of twenty quantities rebuilt from the curve's a-invariants, all twelve of Mazur's degrees, mod-ℓ images at 38 primes, the odd additive barrier, and the candidate theorem stated against the revised router that every prime is sent through



Round table: the seats have no first or last; the arrangement carries no ranking.

2026-10-18

Abstract

The Birch–Swinnerton-Dyer conjecture is open, and nothing here proves any case of it. Banwait and Huang proved strong BSD for infinite families of quadratic twists of semistable curves. A research programme proposes a family for a curve their method does not reach: the twists $E^{(q)}$ of 696.e1, which has additive reduction at 2, by the primes q of an explicit set $\mathcal{P}$, and it states, as a derived theorem candidate, strong BSD for every member, each prime of each twist routed to a published theorem. This paper recomputes everything about the family that can be computed. The anchor has conductor 696, analytic rank 0 and $L(E,1)/\Omega = 1$ to one unit in the last place. The density of $\mathcal{P}$ is $1/24$, not the $1/48$ its three conditions seem to multiply to, by three routes: an exact Galois computation, a Chebotarev derivation in which every field-theoretic step is computed, and a count to $2 \cdot 10^7$; one of the three conditions is implied by the other two, and that redundancy is the factor of 2. A certificate of twenty quantities is rebuilt from the a-invariants alone; all twelve of Mazur's prime isogeny degrees are excluded; the mod-ℓ image is surjective at 38 primes, and at $\ell = 3$ provably beyond this method. The candidate is stated against the programme's revised router, which sends every prime to exactly one theorem — checked as a partition — and not against its first design, which a companion paper shows fails at the member $q = 3529$.

Contents

0. What is claimed, and what is not **2**

1. The curve, the family and the candidate **3**

2. The anchor **3**

3. The density is 1/24, and why it is not 1/48 **4**

4. The smallest members, and a nontrivial Ш **4**

5. A certificate of twenty quantities, rebuilt from the a-invariants **5**

6. Isogenies and images **5**

7. The odd additive barrier **5**

8. The candidate, against the router it is stated with **6**

9. The instrument, and how it was made to fail **6**

10. Contributions **6**

11. What is open **7**

Acknowledgements **7**

References **7**

Data and software 8

A. Reproduction **8**

Status of this document. Preprint, version 0.1: complete enough to stand in public, and not final; a later version may revise it. Not prepared for journal submission. Section 10 records who did which part, including the parts this line did not do.

0. What is claimed, and what is not

Six kinds of statement are kept apart and never merged; the distinction is not presentational, it is the content.

label	meaning
`COMPUTED_HERE`	recomputed in this line with independently written code, never by running the programme's own scripts
`DERIVED_FROM_VERIFIED_INPUTS`	follows from quantities this line already computed
`CITED_THEOREM`	a published result, cited and checked as a citation
`INHERITED`	taken from the programme's documents and never verified here; every use is marked
`UNMEASURED`	well posed, and not established here

label	meaning
`FAILED`	attempted and refused

In particular `PASS` and `PASS by cited theorem` are **different verdicts** and are never written as one. The family's candidate theorem rests on four published theorems, one per branch of its router; every branch is at best `PASS by cited theorem`, and the candidate is not upgraded past the programme's own label.

Not claimed anywhere in this paper: the Birch–Swinnerton-Dyer conjecture, or strong BSD for any member of the family; that the four theorems of the router apply to the primes routed to them — the partition is checked, the applicability is cited; that $L(E^{(q)}, 1) \neq 0$ for every member, which is computed for the two smallest; that $\#Ш(E^{(313)}) = 49$ independently of the BSD formula, which is the analytic order read from a measured ratio; the curve's optimality and its Manin constant; and the result's novelty, which the programme defers to a search this line has not made.

Inherited: the programme's documents and its candidate theorem; Banwait–Huang's Theorem 2.14, BSTW's Theorem 9.21(c), Skinner's Theorem C and Fouquet–Wan's Theorem 1.7 with Corollary 1.10, as the programme reads them; Mazur's classification of rational isogenies; Cassels's theorem that the order of Ш, if finite, is a square.

Where the other labels sit: the anchor, the density, the certificate, the isogeny and image computations and the router's partition are `COMPUTED_HERE`; the density's exact value and the redundancy of one condition are `DERIVED_FROM_VERIFIED_INPUTS`; the analytic order of Ш at $q = 313$ is `PASS by cited theorem` (Cassels, and the BSD formula it reads under); surjectivity at $\ell = 3$ is `UNMEASURED`, for structural reasons; and the programme's first design is `FAILED` at one member (§8).

1. The curve, the family and the candidate

The anchor is 696.e1, $y^2 = x^3 + x^2 + 8x - 16$, with a-invariants $[0, 1, 0, 8, -16]$. Its discriminant is $-178176 = -2^{11} \cdot 3 \cdot 29$: additive reduction of type II* at 2, split multiplicative at 3 and nonsplit multiplicative at 29. Because of the additive prime it is not semistable, which is where Banwait and Huang's method for strong BSD in quadratic-twist families stops.

The programme's family is

$$\mathcal{P} = \{\, q \text{ prime} : q \equiv 1 \pmod{24},\ (q/29) = 1,\ f_2 = x^3 + x^2 + 8x - 16 \text{ irreducible mod } q \,\},$$

and its derived theorem candidate is strong BSD for every quadratic twist $E^{(q)}$, $q \in \mathcal{P}$, each prime p of each twist sent to a published theorem by a router. The conditions have reasons: $q \equiv 1 \pmod{24}$ and $(q/29) = 1$ hold the root number of the twist at $+1$, since $w(E^{(q)}) = (-696/q)$; and irreducibility of the 2-division cubic makes a_q odd, which with the Hasse bound makes every member ordinary for E. Below 4000 the family has 19 members, from 241 to 3793, and below 5000 it has 23.

2. The anchor

The functional equation selects the conductor 696 directly: tried against its nearest competitor, the separation is a factor of 339.02, without Tate's algorithm. The root number is $+1$, and $L(E, 1) =$

$1.631727740072 \neq 0$, so the analytic rank is 0. The ratio $L(E,1)/\Omega$ is 1.0000000000000002 — one, to a single unit in the last place — and with trivial torsion and the Tamagawa numbers at 3 and 29 both 1, it forces $c_2 \cdot \#Ш = 1$ under the BSD formula (`COMPUTED_HERE`; the reading under the formula, `PASS by cited theorem`).

3. The density is 1/24, and why it is not 1/48

Read as three independent conditions, $\mathcal{P}$'s density would be $\frac{1}{8} \cdot \frac{1}{2} \cdot \frac{1}{3} = 1/48$. It is $1/24$, and three routes agree (`COMPUTED_HERE`).

Exactly. With $K_E = \mathbb{Q}(\zeta_{24}, \sqrt{29})$ the field cut out by the first two conditions, $[K_E : \mathbb{Q}] = 16$, and the 2-division field meets it in a quadratic field, $e_E = 2$; the density is $e_E/(3[K_E : \mathbb{Q}]) = 2/48 = 1/24$.

By Chebotarev, every step computed. f_2 has discriminant $-11136 = -2^7 \cdot 3 \cdot 29$, no rational root and a non-square discriminant, so its Galois group is S_3 with quadratic resolvent $\mathbb{Q}(\sqrt{-174})$. Since $-174 = -6 \cdot 29$ and $\mathbb{Q}(\sqrt{-6}) \subset \mathbb{Q}(\zeta_{24})$, the resolvent lies in K_E; S_3 has exactly one nontrivial proper normal subgroup, so the compositum has degree $6 \cdot 16/2 = 48$, and the 3-cycles, a class of size 2, give $2/48$. The compatibility step was shown against a case where it fails: a transposition contradicts the condition on the resolvent and would give density 0.

By counting. Over the primes below $2 \cdot 10^7$ the measured density is 0.04162499, which is 0.99900 times $1/24$ and so about twice $1/48$.

The redundancy is the factor. The middle condition is implied by the other two: irreducibility makes Frobenius a 3-cycle, hence trivial on $\mathbb{Q}(\sqrt{-174})$, so $(-174/q) = 1$; $q \equiv 1 \pmod{24}$ gives $(-6/q) = 1$; hence $(29/q) = 1$, which for $q \equiv 1 \pmod 4$ is $(q/29) = 1$. Over every prime $q \equiv 1 \pmod{24}$ below 200000, the cell that would contradict it — cubic irreducible, $(q/29) = -1$ — is empty, while 760 primes lie in the cell it predicts (`DERIVED_FROM_VERIFIED_INPUTS`). The overlap is $e_E = 2$: the condition the programme states third is the reason the density is $1/24$. Three definitions of $\mathcal{P}$ — the programme's, this line's membership test and a referee checklist's five conditions — pick out the same 19 primes below 4000.

4. The smallest members, and a nontrivial Ш

For the two smallest members the twisted L-value was computed from the base curve's coefficients times the quadratic character:

q	$L(E^{(q)},1)$	Ω	L/Ω
241	0.105108823625	0.105108823625	1
313	4.519304541603	0.092230704931	49

Both are nonzero (`COMPUTED_HERE`). Both twists have trivial torsion and the base's reduction at 2, 3 and 29, so $L/\Omega = c_q \cdot \#Ш$ under the BSD formula. Additive reduction at q allows $c_q \in \{1,2,4\}$ and Cassels makes #Ш a square, so at $q = 313$ only $c_q = 1$ survives and $\#Ш(E^{(313)}) = 49 = 7^2$ — a nontrivial Ш read from a measured L-value and period. It is the analytic order: a reading under the BSD formula, not an independent computation of the group (`PASS by cited theorem`). Every member below 20000 — 87 of them — has root number $+1$, odd a_q and good ordinary reduction;

and a_p is odd exactly when f_2 is irreducible mod p, which holds for a measured fraction 0.328907 of the good primes below 20000, so the condition is doing work.

5. A certificate of twenty quantities, rebuilt from the a-invariants

The programme's submission gate asks for a machine-checkable arithmetic certificate. Twenty quantities — invariants, discriminant, conductor exponents, reduction types, Tamagawa numbers, torsion, the 2-division cubic and its Galois data, the analytic data — were each recomputed from $[0, 1, 0, 8, -16]$ alone and compared with the round that logged it: all twenty agree (COMPUTED_HERE). The first draft caught its author. Three values filled in from memory were wrong — c_4, whose true value is -368, c_6, whose true value is 16064, and the j-invariant that follows from them — and a certificate that quotes its author is exactly what a certificate exists to replace; every row is now a derivation. Against the programme's own base certificate, every row was compared: 17 recomputed and every one agreeing, 5 marked as beyond this line — the algebraic rank, optimality, the Manin constant, the analytic Ш and a cited conductor-range verification — and the discriminant row compared by square class, because three different cubics in the corpus have discriminants differing by squares.

6. Isogenies and images

All twelve of Mazur's degrees. A rational n-isogeny forces $x^2 - a_\ell x + \ell$ to have a root mod n for every good ℓ; one ℓ where it is irreducible refutes it. Eleven of Mazur's twelve prime degrees are refuted by an explicit witness prime; for $n = 2$ the criterion is structurally vacuous, every element of $\mathbb{F}_2$ being a square, and the degree is settled by the modular curve $X_0(2)$ (COMPUTED_HERE; that the twelve are all, CITED_THEOREM). The refutation transfers to every twist, because $a_\ell(E^{(d)}) = \chi_d(\ell) a_\ell(E)$ leaves $a_\ell^2 - 4\ell$ unchanged — measured identical where the signs genuinely flip.

Images. The mod-ℓ representation is surjective for $\ell = 2$ and every prime $5 \le \ell \le 167$ — 38 in all — each by refuting, with one named Frobenius, all six ways a subgroup with surjective determinant can be proper: Borel, the normalizers of split and nonsplit Cartans, and projective images A_4, S_4, A_5 (COMPUTED_HERE). Each projective order is computed two ways that must agree. An earlier version of the gate read the orders off a^2/q with the wrong condition for order 5, and one witness fell to it: A_5 at $\ell = 29$, whose Frobenius at 5 has order 5, which A_5 allows. The corrected search refutes A_5 there at $q = 11$, so the 38 stand; found in review. At $\ell = 3$ the method cannot finish, for two structural reasons: $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$, so "projective image S_4" is surjectivity itself, and the nonsplit-Cartan test is vacuous mod 3, proved by exhausting its four residue cases. The other four classes are refuted there, and $\ell = 3$ is reported partly certified and never counted (UNMEASURED).

7. The odd additive barrier

The programme names one obstruction to its period comparison at a fixed odd additive prime, with a sufficient condition that excludes the Kodaira types II, III and IV. The base curve meets it nowhere — its only additive prime is 2 — and each of the 19 members meets it exactly once, at q itself, where the twist forces the valuations of c_4, c_6 and Δ to be $(2, 3, 6)$: type I_0^*, on 19 of 19 (COMPUTED_HERE). The excluded types were shown to be reachable rather than assumed non-empty, on three small curves of types II, III and IV, where the condition correctly fails.

8. The candidate, against the router it is stated with

The programme's revised candidate sends every prime p of $E^{(q)}$ to exactly one theorem: $p = 2$ to Banwait–Huang's Theorem 2.14 with Creutz–Miller; $p = q$ to BSTW's Theorem 9.21(c), with a witness 29; good ordinary p, and $p = 3$, to Skinner's Theorem C with witness 29; $p = 29$ to Skinner's Theorem C with witness 3; good supersingular p to Fouquet–Wan. Run for the three smallest members over all 109 primes below 600, the router is a partition: six branches used, no prime unrouted, none in two (`COMPUTED_HERE`). Its witnesses were computed independently, from the other end: the swap $3 \leftrightarrow 29$ for the multiplicative primes, and 29 as the only nonsplit multiplicative witness. A partition is not a proof; whether each branch's theorem applies to the primes routed to it is cited.

The first design, and why it is not the one stated. The programme's provisional design sent the twisting prime $p = q$ to Fouquet–Wan instead. A companion paper shows that this fails at one member: at its own twisting prime, the hypothesis H2 of Fouquet–Wan reduces to the base curve's congruence $a_q^2 \equiv 1 \pmod{q}$, which holds at 18 of the 19 members below 4000 and fails at $q = 3529$, where $a_q = 1$. The revised router does not use Fouquet–Wan at $p = q$, and the candidate here is the revised one. Of the five items the provisional statement handed to a referee, the corpus answers two, defers one to a novelty search and leaves two open — the period normalization for every twist, and the exact optimality phrasing — so the candidate keeps its label: *derived theorem candidate*, not theorem.

9. The instrument, and how it was made to fail

Each gate here is part of a whole-tree drill run after every round: defects are planted one at a time, each must be caught by the check **named** for it, and controls must disturb nothing. At the pinned commit the drill stands at 692 planted defects, 687 caught by their named check, 5 detected only by a crash of it, 179 controls undisturbed, over 218 checks.

Two of its catches belong in this paper. The density's middle condition was found redundant because the drill planted a defect that dropped it and nothing changed — a defect that changes nothing is a finding before it is a failure. And a control that widened an enumeration from 4000 to 5000 turned red because a bound written into the scan, not passed by its caller, made three definitions of $\mathcal{P}$ appear to disagree at four primes; the disagreement was manufactured by the guard and gone once the bound moved to the caller.

10. Contributions

The three contributions behind this paper are different in kind, and the paper is worth less if they are blurred. They are given here in alphabetical order, the order the author list keeps as data; on the title page the three sit at a round table, with no first and no last.

Aletheia — model: ChatGPT, GPT series — wrote, with Neo.K, the programme's documents on the family: the set, its density note, the certificate's specification, the routers, the provisional and revised statements, and the referee lists.

Neo.K set the programme's target — strong BSD beyond the semistable reach of the published method, for an explicit infinite family — and wrote its documents with Aletheia.

墜衡 (Zhuì Héng) — the independent verification line; model: Claude, Opus series — recomputed the anchor, the density by three routes and the redundancy behind it, the two smallest members, the

certificate from the a-invariants, Mazur's twelve degrees and the images at 38 primes, the barrier, and the router's partition; built and drilled the gates; and wrote this paper. The family and the candidate are the programme's; nothing in them is this line's invention.

Priority, stated plainly. No result here is claimed as new mathematics. What is offered as this line's own is a complete recomputation of the family's computable content, the redundancy that explains its density, and the statement of its candidate against the router that survives.

11. What is open

1. The Birch–Swinnerton-Dyer conjecture, and strong BSD for any member of $\mathcal{P}$.
2. Whether the four theorems of the router apply to every prime routed to them; the period normalization for every twist, and the curve's optimality and Manin constant.
3. $L(E^{(q)}, 1) \neq 0$ for every member, computed here for two; surjectivity at $\ell = 3$.
4. The candidate's novelty, which the programme defers to a search not made here.

Acknowledgements

We thank Anthropic, whose Claude models the lab's verification and recomputation lines run on, and OpenAI, whose ChatGPT models the programme's documents were written with. Not every AI model or instance that took part in this work is named in it — among them instances that the named authors ran as helpers; that an AI is not listed here does not mean that none took part.

References

1. Barinder S. Banwait and Xiaoyu Huang, *On the Identification of Elliptic Curves That Admit Infinitely Many Twists Satisfying the Birch–Swinnerton-Dyer Conjecture*, arXiv:2601.16044, third version (2026), to appear in ANTS XVII. Numbered statements are cited from the third version; the first numbers its second section differently.
2. Ashay A. Burungale, Christopher Skinner, Ye Tian and Xin Wan (cited as BSTW), *Zeta elements for elliptic curves and applications*, arXiv:2409.01350, second version (2024).
3. J. W. S. Cassels, *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung*, J. reine angew. Math. 211 (1962) 95–112, doi:10.1515/crll.1962.211.95.
4. Brendan Creutz and Robert L. Miller, *Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula*, J. Algebra 372 (2012) 673–701, doi:10.1016/j.jalgebra.2012.09.029.
5. Olivier Fouquet and Xin Wan, *The Iwasawa Main Conjecture for universal families of modular motives*, arXiv:2107.13726, third version (2022).
6. B. Mazur, *Rational isogenies of prime degree*, with an appendix by D. Goldfeld, Invent. Math. 44 (1978) 129–162, doi:10.1007/BF01390348.
7. Christopher Skinner, *Multiplicative reduction and the cyclotomic main conjecture for GL_2*, Pacific J. Math. 283 (2016) 171–200, doi:10.2140/pjm.2016.283.171; arXiv:1407.1093. Theorem C is cited as stated in the first arXiv version.
8. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in Lecture Notes in Math., Springer, 1975, 33–52, doi:10.1007/BFb0097582.

Data and software

- Python Software Foundation, *Python* (CPython), version 3, https://www.python.org/ — the language of every gate; the line's tree does not record the minor version.
- The mpmath development team, *mpmath: a Python library for arbitrary-precision floating-point arithmetic* (version 1.3.0), https://mpmath.org/ (2023) — in the drill's independent checks.

A. Reproduction

Everything is Python standard library, no network; reduction types come from Tate's algorithm on each model and every inequality is decided in integers or exact rationals where it can be. Each gate writes a JSON log. The line's own tree is not public. Its public projection is, and it is what this paper's figures can be checked against without trusting the authors:

- **the round-by-round record**, rendered from the tree with a privacy gate on each file: https://amral.evemisslab.com/bsd/recompute/ (and `/en/`);
- **the programme's documents on the family**: https://amral.evemisslab.com/bsd/phase2/;
- **the secondary-verification ledger**, whose numbers are rendered from the line's own results file and read back against it before the site ships: https://verify.evemisslab.com/bsd-verification-zhuiheng/.

The evidence is pinned, not copied: this paper's front matter names the research branch, the commit and the directory its figures were drawn from, and the checker reads them exactly as they stood at that commit. The crystallization standard and its checker live in the release repository beside the paper (`STANDARD.md`, `tools/check_standard.py`).