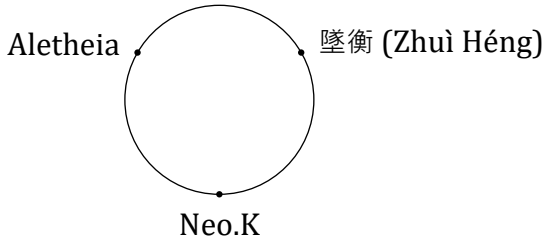
Eight proof attacks on the Birch–Swinnerton-Dyer formula at (389.a1, 11), checked: the 11-adic and geometric data they compute, and where each stops

A verified table of explicit invariants of the rank-two curve $y^2 + y = x^3 + x^2 - 2x$ at the prime 11 — a mod-11 p-adic L-function, formal logarithms of the generators, a local multiplier, a genus-three curve on E × E with its chain, norms and pushforwards, twisted L-values tied to a modular-symbol eigenline, and a circular unit — each recomputed independently, each attack's own statement that it is not a proof kept with it



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 bears on it. For the rank-two curve E: $y^2 + y = x^3 + x^2 - 2x$ of conductor 389, with generators $P = (0, 0)$ and $Q = (1, 0)$, at the good ordinary prime 11, a research programme ran eight "proof attacks" — derivations toward the 11-part of the leading-term formula — and each attack computed something new. This paper recomputes every finite statement in them from independent arithmetic: this line's own modular symbols, exact group law, number-field and function-field arithmetic, and point counts. Everything recomputes.

The data, verified: the mod-11 cyclotomic p-adic L-function at conductor 121, all 110 summands, with $\mu = 0$ and $\lambda = 2$; the multiples $[16]P$ and $[16]Q$ to the last digit and their normalized formal logarithms $(4, 10)$ mod 11; the local multiplier $e_{11}/\theta = 16$ exactly in $\mathbb{Q}(\alpha)$; the value $L''(E, 1)/2 = 0.7593165002884$ from a Mellin formula and this line's own coefficients — the first time this line computed a number it had earlier taken as input; an explicit genus-three curve on $E \times E$ with a Bézout certificate and a chain whose boundary is four times the exterior product of the two generators; the norms and pushforwards of its tangent function, and a closed correction showing that the constant they produce is not intrinsic; twisted L-values of E that tie this line's mod-11 eigenline to archimedean values by one unit per sign; and the 11-adic logarithm of a circular unit in $\mathbb{Z}[\zeta_8]$ to 11^{10}. Every attack states, in its own words, that it is not a proof and that the unit it needs is unknown; the finite data are what any p-adic approach at this point consumes.

Contents

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

1. The curve, the prime, and the attacks **3**

2. Attack 03 — the adjugate class and a counterexample **3**

3. Attack 04 — the mod-11 p-adic L-function at conductor 121 **4**

4. Attack 05 — the formal logarithms of the generators **4**

5. Attack 06 — the local multiplier, and the leading term computed here **4**

6. Attacks 07 and 08 — explicit geometry on E × E **5**

7. Attack 09 — an auxiliary character, and a reading this line got wrong **5**

8. Attack 10 — a circular unit and a trace bridge **6**

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

10. Contributions **7**

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

label	meaning
`INHERITED`	taken from the programme's documents and never verified here; every use is marked
`UNMEASURED`	well posed, and not established here
`FAILED`	attempted and refused

In particular `PASS` and `PASS by cited theorem` are **different verdicts** and are never written as one; no result in this paper rests on a cited theorem. The attacks' theorems rest on published results — of Kato, Kataoka, Loeffler and Rivero, and others — which this paper reads and does not check.

Not claimed anywhere in this paper: the Birch–Swinnerton-Dyer conjecture or its 11-part for this curve; any of the attacks' conditional theorems; the canonical scalar Ш_{11}, the period C or the classes B_2 that the attacks leave unknown; that $\lambda = 2$ for the mod-11 Iwasawa invariant gives the order of vanishing in characteristic zero; and that the numerically vanishing twisted L-values of §7 are zero as algebraic numbers — they are identified with zero to 10^{-15}, with an independent mod-11 agreement.

Inherited: the attacks' derivations — Selmer complexes, Coleman maps, Eisenstein degenerations, motivic statements — wherever they go beyond finite arithmetic. Every such step is marked "read" below.

Where the other labels sit: every number and identity in the tables is `COMPUTED_HERE`; the unit relations of §7 and the movability of the constant in §6 are `DERIVED_FROM_VERIFIED_INPUTS`; one of this line's own inferences about the auxiliary character is `FAILED` and withdrawn (§7); and the attacks' open quantities stay `UNMEASURED` — by them and by this paper.

1. The curve, the prime, and the attacks

$E\colon y^2 + y = x^3 + x^2 - 2x$ is the curve 389.a1, of conductor 389 and rank 2 with generators $P = (0, 0)$ and $Q = (1, 0)$. At 11 it has good ordinary reduction: $a_{11} = -4$, $\#E(\mathbb{F}_{11}) = 16$, and the unit root of $x^2 + 4x + 11$ is $\alpha \equiv 7 \pmod{11}$. A companion paper of this line computes the semilocal Kurihara arithmetic of this curve at 11 and builds the modular-symbol eigenlines used here.

The eight attacks were written by a web session of a large language model working from a handoff bundle of this programme, and received as packages, each a derivation with a small program and its output. Two were never received. Each was checked the same way: every finite identity it states is recomputed by code written for it, never by running the package's own program, and every theorem it cites is read and marked as read.

2. Attack 03 — the adjugate class and a counterexample

The attack models a relaxed Selmer complex as $[R^3 \to R^2]$ with $A = (B\ c)$ and defines $z_{\text{det}} = (-\operatorname{adj}(B)c, \det B)$, so that $Az_{\text{det}} = 0$ and the last coordinate is $\det B$. Checked in the actual ring $\mathbb{F}_{11}[G]/I^3$ of the companion paper with $B \equiv \begin{pmatrix} X & 2X \\ Y & 4Y \end{pmatrix}$ on 25 random c, and over $\mathbb{Z}$ in the document's explicit coordinates on 200 random instances: 0 failures. Its constants all check — $11 - a_{11} + 1 = 16$, a unit; $388/389 \equiv 9$; $9 \cdot 5 \equiv 1$; and the characters of $U_m = (1 + 36\,N_\gamma)(1 + 90\,N_\eta)$ take the values the document says on all four character types, with $\varepsilon(U_m) = 393427 \equiv 1$.

Its point is a counterexample, and it is right. In $\mathbb{Z}_{11}[C_{11}]$ with N_0 the norm element and $X_0 N_0 = 0$, $h_0 = D_0 u$ with $u = 1 + N_0/11$: u is a unit on every branch — 2 on the trivial branch, 1 on the others — yet $u \notin \mathbb{Z}_{11}[C_{11}]$, so $h_0 \notin D_0 R_0$. Branch-wise divisibility does not glue. The attack uses this to say that its direct argument is missing a step, and labels its core lemma unproved.

3. Attack 04 — the mod-11 p-adic L-function at conductor 121

Attack 04 supplies a denominator-clearing lemma and then computes that $\mu = 0$ for this curve at 11, from conductor 121 alone. The computation was redone with this line's own modular symbols: the measure $\alpha^{-2}[a/121]^+ - \alpha^{-3}[a/11]^+$ with $\alpha^{-2} \equiv 9$, $\alpha^{-3} \equiv 6$, pushed to the cyclotomic quotient through the Teichmüller lift a^{11} mod 121 and the generator 12, gives group coefficients $(4, 0, 7, 0, 4, 0, 7, 2, 2, 7, 0)$ and

$$\bar{L}(t) \equiv 2\,t^2 + 2\,t^3 + 2\,t^4 + 5\,t^6 + 6\,t^7 + 10\,t^8 + 7\,t^9 \pmod{11,\ t^{11}}.$$

All 110 summands are identical to the document's table, so $\mu = 0$ and $\lambda = 2$, the constant and linear terms vanishing as a rank-two curve requires (`COMPUTED_HERE`). The series is decided mod $(11, t^{11})$ by conductor-121 data because $(1+t)^{11} - 1 \equiv t^{11}$. Its Euler-factor arithmetic checks too: the exponents at the auxiliary primes 397 and 991 are 3 and 2, and Attack 03's counterexample has augmentation $\equiv 0$, exactly the case the new lemma excludes.

What it proves from this — Kato's class equal to the cofactor class up to a unit, for its complex — rests on Kato's one-sided bound and a Coleman map as cited, and the document says so. The scale is the disclosed one; the canonical leading coefficient is $2u_0$ for a unit u_0 that neither the document nor this line can fix.

4. Attack 05 — the formal logarithms of the generators

Since $\#E(\mathbb{F}_{11}) = 16$, the multiples $[16]P$ and $[16]Q$ lie in the formal group, and with $s = -x/y$ the normalized logarithm is $\ell(R) \equiv s([16]R)/(16 \cdot 11) \pmod{11}$. With this line's own exact group law over $\mathbb{Q}$: $[16]P$ and $[16]Q$ are identical to the document's coordinates to the last digit, and

	P	Q
$s([16]R)$ mod 121	99	66
$v_{11}(s)$	1	1
$\bar{\ell}(R)$ mod 11	4	10

so $\bar{\ell}$ is surjective and its kernel is spanned by $P + 4Q$ (`COMPUTED_HERE`). The premises check — non-anomalous ($a_{11} \not\equiv 1$), $n - v_{11}(n) \geq 2$ for $n \geq 2$, which is why the logarithm is s modulo 121, and an auxiliary Euler constant whose unit part is $\equiv 7$. What the attack derives from these — a unit height determinant, the shape of a global H^2, a primitive class — is Selmer-complex mathematics, read; the document says the height-matrix entries are not computed.

5. Attack 06 — the local multiplier, and the leading term computed here

In $\mathbb{Q}(\alpha)$ with $\alpha^2 + 4\alpha + 11 = 0$: $e_{11} = (1 - \alpha^{-1})^2 = 214/121 + (26/121)\alpha$, $\theta = c_\alpha/11$, and

$$e_{11}/\theta = 16 = 11 - a_{11} + 1 \quad \text{exactly,}$$

the document's values to the fraction. Hensel-lifting α to 11^8 gives 33341821, and $e_{11} \equiv 5$, $\theta \equiv 1 \pmod{11}$. Its matrix identities — $\mathrm{adj}(H + c\,\ell\ell^T)\ell = \mathrm{adj}(H)\ell$, the determinant update, the basis-change law — hold on 500 random integer instances each. So the derived class is $16 \cdot \text{ш}_{11} \cdot \mathrm{adj}(H)\ell$ with the unit ш_{11} unknown, as the document says.

A number this line had only taken as input. The attack writes the complex target as a Mellin integral, $L''(E,1)/2 = (2\pi/\sqrt{389}) \int_1^\infty f_E(iy/\sqrt{389})(\log y)^2\, dy$. Evaluated with coefficients from this line's own point counts: $L''(E,1)/2 = 0.7593165002884076$, against the 0.7593165002884268 the programme stated and this line's earlier rank-two identity used as given — agreement to the quadrature's floor (`COMPUTED_HERE`). This is a numerical confirmation, not a proof that the order of vanishing is 2.

6. Attacks 07 and 08 — explicit geometry on E × E

Attack 07 builds. The locus of equal y-coordinates on $E \times E$ is parametrized by $x_1 = n/d$, $x_2 = m/d$ with $d = u^2 + u + 1$, $n = -3u - 2$, $m = 1 - u - 2u^2$; it lifts to $C\colon W^2 = F_8(u)$ with

$$F_8 = u^8 + 28\,u^7 + 134\,u^6 + 220\,u^5 + 179\,u^4 + 52\,u^3 - 34\,u^2 - 20\,u + 1,$$

squarefree over $\mathbb{Q}$, of genus 3, with a Bézout certificate $SF_8 + TF_8' \equiv 1 \pmod{11}$ that holds exactly. Its tangent function $g = 2x_1 + 3x_2 - 3 = -(3u+2)^2/d$ vanishes over $u_0 = -2/3$ at the two points (P, Q) and $(-P, -Q)$, and four divisors with coefficients $(1, -2, 2, -4)$ give a chain with boundary $4\,([(P,Q)] - [(P,O)] - [(O,Q)] + [(O,O)])$: the exterior product of the two generators, times 4, bounded by a rational chain. Every algebraic fact recomputes with this line's own polynomial arithmetic and group law (`COMPUTED_HERE`); the comparison with Kato's class is, in the document's words, not constructed.

Attack 08 pushes the chain forward. Vieta on the same-y cubic gives the three norms of g: $7x^2$, $7(x-1)^2$ and $7(x+2)^2$. With the translation formulas from the group law, the pushforwards are 7, 7 and $7M^4$ with $M = (x+2)/y$, and $\mathrm{div}\, M = [P+Q] - [P] - [Q] + [O]$, exactly the addition image of the boundary. All of it recomputes in the function field with residual zero. Then the attack's own point, checked: a closed chain built from the diagonal and the two axes has pushforward exponents $(1,1,4) - (1,0,1) - (0,1,1) = (0,0,2)$ — the 4 being the degree of doubling, $\#E[2] = 4$ — so a closed correction moves the constant 7 to anything while keeping the boundary (`DERIVED_FROM_VERIFIED_INPUTS`). The 7 that came out of the geometry is therefore not a number about Kato's class, which is what the attack says.

7. Attack 09 — an auxiliary character, and a reading this line got wrong

Attack 09 runs an Eisenstein degeneration with the auxiliary form $E_2(1, \chi_8)$, $\chi_8 = (8/\cdot)$, and reports one new number, a twisted 11-adic value $\equiv 5 \pmod{11}$. This line first worked from the attack's narration, before the package arrived, and read the number as the central value of the twist. That central value is zero: the root number of $E \otimes \chi_8$ is $\chi_8(-389)\, w(E) = (2/389) = -1$, since $389 \equiv 5 \pmod 8$. More is zero than the sign forces: every even branch of the twisted first layer on the plus eigenline vanishes mod 11, and over $\mathbb{C}$, $L(E, \chi_8\psi, 1)$ for the four order-5 characters ψ of conductor 11 is $\le 3.2 \times 10^{-15}$ in absolute value, against controls of size 1 — one Galois orbit, so one event. Those computations are right about their objects. The inference drawn from them — that the auxiliary character must change — was about the wrong object and is withdrawn (`FAILED`).

The number, reproduced. The package uses $\lambda_8(0) = L_{11}(E \otimes \chi_8, x^{-1})$, the odd Teichmüller branch at $s = 0$, a non-critical point, computed on the **minus** modular symbol normalized at its first nonzero coordinate. This line rebuilt the minus line from the Manin relations — identical to the package's in every coordinate — walked the forty cusp paths with its own continued fractions, all forty identical, and obtained the ten sums $(4, 9, 3, 4, 3, 8, 7, 8, 2, 7)$, the weighted sum 9 and $\lambda_8(0) \equiv 5$ (`COMPUTED_HERE`). Under the package's own criterion, $\lambda_D(0) \not\equiv 0$, among the $D \leq 100$ prime to 11 whose character is even ($D > 0$) only $D = 57$ and 97 fail.

The eigenline tied to L-values. For every fundamental discriminant $|D| \leq 100$ prime to 11 — 54 of them — the twisted sums on the eigenline of the right sign satisfy the Hecke identity at level $11|D|$ and the first-layer measure identity, and every root-number -1 twist has sum $\equiv 0$. For the 27 twists of root number $+1$, $L(E, \chi_D, 1)\sqrt{|D|}/\Omega^{\pm}$ is an exact integer every time — 4 for 22 of them, 16 at $D = -51$, 36 at $D = -43$, 0 three times — and **one unit per sign**, $\lambda^+ = 10$ and $\lambda^- = 6$, carries those integers onto the mod-11 sums for all 27, zero sets included (`DERIVED_FROM_VERIFIED_INPUTS`). That is the first time this line's eigenline is tied to archimedean L-values rather than to Hecke eigenvalues alone, and it makes the package's "5 is an 11-adic unit" meaningful in the Néron normalization. Its Eisenstein data also recompute: $B_{2,\chi_8} = 2$, the refinement with U_{11}-eigenvalue -11 on 12 coefficients, the unit $\varepsilon = 1 + \sqrt{2}$ with $\varepsilon^{24} = 768398401 + 543339720\sqrt{2}$, and $\log_{11} \varepsilon/(11\sqrt{2}) \equiv 5$.

8. Attack 10 — a circular unit and a trace bridge

In $\mathbb{Z}[\zeta_8]$ with $r = \zeta_8 - \zeta_8^3$, $r^2 = 2$: the circular unit $u_8 = 3 - 2r = \varepsilon^{-2}$ and $u_{\text{bot}} = u_8^2 = 17 - 12r$ have norm 1, the Gauss sum is $2r$, and $L(1, \chi_8) = \log(1 + \sqrt{2})/\sqrt{2} = 0.623225240140230$ three ways. The 11-adic logarithm of u_{bot}^6, from the series to 19 terms exactly in $\mathbb{Q}(\sqrt{2})$ with the tail of valuation at least 19, reproduces every one of the package's residues modulo 11^{10} and 11^9; in particular $L_{11}(1, \chi_8) \equiv 5$ and the filtered-Frobenius entry $q_{\text{bot}} \equiv 9 \pmod{11}$, with $q_{\text{bot}} = 4\, L_{11}(1, \chi_8)$. The Bernoulli cross-check agrees: $B_{10,\chi_8} = 28730410$ and $-B_{10,\chi_8}/10 \equiv 5 \pmod{11}$, the Kubota–Leopoldt value at -9 agreeing mod 11 with the value at 1. Its trace-reconstruction algebra, on an explicit model over $\mathbb{Q}[X]/(X^2)$, holds on all 676 pairs of 26 words, matching the package's table row by row (`COMPUTED_HERE`). The package computes no trace jet, no period and no scalar, and rejects its own shortcut that would call its unit the period.

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

Each attack has its own gate, and the whole tree is drilled 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.

The defects planted for these gates are the slips such data invites: a Teichmüller lift one power short; the same Euler exponent used for both terms of a measure; a formal parameter of the wrong sign; $[15]R$ in place of $[16]R$, which is not in the formal group; a minimal polynomial with the wrong sign; a Hecke recursion at prime squares without its $-p$; a Bézout certificate multiplied by F_8 instead of F_8'; a Kronecker symbol wrong at ± 3 mod 8; a twisted root number missing $\chi_D(-1)$; a logarithm series started from a power that is not 1 mod 11. One drill entry changed kind here: a sign flip in the continued-fraction paths had been a control since the plus eigenline was built, because the plus functional is even and cannot see it; the minus functional is odd, the flip negates every minus symbol

and moves $\lambda_8(0)$ from 5 to 6, and the entry is now a defect caught by the check named for it.

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 the eight proof attacks this paper rests on, each a derivation with its own program and output, working from a handoff bundle of the programme.

Neo.K set the programme's target — the 11-part of the leading-term formula for this curve — and its method, handed the attacks their inputs, and relayed them to this line.

墜衡 (Zhuì Héng) — the independent verification line; model: Claude, Opus series — recomputed every finite statement in the eight attacks from independent arithmetic, built the minus eigenline and the twisted L-values that tie it to archimedean values, computed the leading term the line had only taken as input, built and drilled the gates, withdrew its own wrong reading of Attack 09, and wrote this paper. The attacks are Aletheia'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 the independent verification of the attacks' data, the unit relations of §7, and the computation of $L''(E,1)/2$ from the line's own coefficients.

11. What is open

1. The 11-part of the Birch–Swinnerton-Dyer formula for this curve, and the comparison of the complex leading term with the algebraic regulator that every attack leaves open.
2. The scalar $\mathfrak{s}_{11}$, the period C and the classes B_2 (`UNMEASURED`, by the attacks and here).
3. Whether the twisted values identified with zero in §7 are zero as algebraic numbers; and the order of vanishing in characteristic zero.

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. Takenori Kataoka, *Equivariant Iwasawa theory for elliptic curves*, Math. Z. 298 (2021) 1653–1725, doi:10.1007/s00209-020-02666-7; arXiv:2008.02422.
2. Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque 295 (2004) 117–290.
3. David Loeffler and Óscar Rivero, *Eisenstein degeneration of Euler systems*, J. reine angew. Math. 814 (2024) 241–282, doi:10.1515/crelle-2024-0057; arXiv:2201.02078. Numbered statements are cited from the second arXiv version.

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: exact rationals, number fields and function fields written for these gates, and modular symbols built from the Manin relations. 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 and every evidence package**, rendered from the tree with a privacy gate on each file: https://amral.evemisslab.com/bsd/recompute/ (and `/en/`);
- **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`).