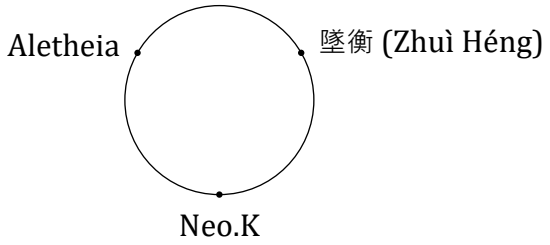
The semilocal Kurihara arithmetic of 389.a1 at p = 11, recomputed

What is canonical and what is a choice: a localization determinant, a local unit, a Kurihara number and a Bockstein determinant, each computed from the group law or from modular symbols built here



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 directly. Explicit instances of Kolyvagin–Kurihara arithmetic in rank 2 are rare; this paper recomputes one completely, for the rank-2 curve 389.a1 at the good ordinary prime $p = 11$ with the two ramified directions $\ell = 397$ and 991, and sorts every figure into what is canonical and what is a choice.

Canonical: the localization determinant is non-zero ($\det M_{\mathrm{loc}} = 2$ in $\mathbf{F}_{11}$), the norm-Selmer group cut out by both directions is zero, the mod-11 Kurihara number at $n = 397 \cdot 991$ is non-zero, and the Bockstein determinant spans the line $\mathbf{F}_{11}XY$ in $\mathbf{F}_{11}[G]/I^3$ with $\mathrm{ord}_I = 2$. A choice: the coefficient on that line, which takes every value in $\mathbf{F}_{11}^{\times}$ under a change of generators; the Kurihara number's value, 5 at the one disclosed scale and 6 in an undisclosed one; the ratio 3 between two normalizations, which a change of primitive roots alone moves through all ten units; the 11-adic valuation of a local unit, which changes by one under a change of Mordell–Weil basis; and the pair $\{397, 991\}$ itself, which is the smallest of 230 pairs below 20,000 that work. Three boxed statements of the programme turn out to be one determinant. Every figure was recomputed with independently written code — the group law over $\mathbf{Q}$ and $\mathbf{F}_\ell$, and mod-11 modular symbols for $\Gamma_0(389)$ built from Manin symbols — and the Kurihara number agrees with two other implementations term by term over 392040 terms.

Contents

0. What is claimed, and what is not 2

1. The curve, the prime and the directions 3

2. The localization determinant 3

3. Three boxed statements, one determinant **4**

4. A local unit, and a valuation that depends on the basis **4**

5. The Kurihara number, a third time **5**

6. The Bockstein determinant, and a ratio that is a coordinate **6**

7. The programme's ledger, read as data **6**

8. The instrument, and how it was made to fail **7**

9. Contributions **7**

10. What is open **8**

Acknowledgements **8**

References **8**
Data and software 8

A. Reproduction **9**

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 9 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
`FAILED`	attempted and refused

In particular `PASS` and `PASS by cited theorem` are **different verdicts** and are never written as one. Every figure in this paper is `COMPUTED_HERE`; the places where a conclusion also needs a theorem or an inherited input are named where they occur.

Not claimed anywhere in this paper: the Birch–Swinnerton-Dyer conjecture or its leading-term formula for this curve; that $Ш(E/\mathbf{Q})[11^\infty] = 0$ — the programme concludes it from a theorem this line has not read, and this paper verifies only the finite input; that the finite Bockstein operator is the Bockstein regulator of any published theory (the programme's own gate `P5-CANON-BocID`, open); the comparison of the complex leading term with the algebraic regulator (`P5-CPLX-GPR`, open); and any canonical value of the Kurihara number at the Néron scale.

Inherited, and marked where used: the rank, $\operatorname{rank} E(\mathbf{Q}) = 2$, with generators P, Q taken from the curve's record (this line has no descent); $Ш(E/\mathbf{Q})[11] = 0$ where a Selmer dimension needs it; the identification of the local norm quotient with $E(\mathbf{F}_\ell)/11\,E(\mathbf{F}_\ell)$ for a tame, totally ramified degree-11 extension, which is the programme's Proposition 4.1, read and with its hypotheses checked on the data; and the programme's identification of the Bockstein determinant with $\det M_{\mathrm{loc}}$. **Cited:** Mazur's isogeny theorem and the rational points of $X_0(11)$; the classification of subgroups of $\mathrm{GL}_2(\mathbf{F}_{11})$ behind a surjectivity certificate; Kim's structure theorem for Selmer groups, whose computable hypotheses are checked and whose statement is not; and the Manin constant, an external record.

1. The curve, the prime and the directions

$E = 389.\mathrm{a}1$ is $y^2 + y = x^3 + x^2 - 2x$, with $\Delta = 389$ prime, $c_4 = 112$ and $c_6 = -856$, so its only bad prime is 389, of type I_1 with Tamagawa number 1. The generators are $P = (0, 0)$ and $Q = (1, 0)$ (inherited); the torsion is trivial, since the gcd of $\#E(\mathbf{F}_q)$ over small good q is 1. Derived from the a-invariants, not copied, the short model is $Y^2 = X^3 - 3024\,X + 46224$, with $P' = (12, 108)$ and $Q' = (48, 108)$.

At $p = 11$, $\#E(\mathbf{F}_{11}) = 16$ and $a_{11} = -4$, so 11 is good and **ordinary, but not anomalous in Mazur's sense**; the programme's word "anomalous" refers to the ramified directions, where $11 \mid \#E(\mathbf{F}_\ell)$ — the opposite of the classical hypothesis — and its own text says so. A **direction** is a prime $\ell \equiv 1 \pmod{11}$ with $11 \parallel \#E(\mathbf{F}_\ell)$, so that $a_\ell \equiv \ell + 1 \pmod{11}$, the Kolyvagin–Kurihara condition, and the norm quotient is one -dimensional. At $\ell = 397$, $\#E(\mathbf{F}_{397}) = 374 = 2 \cdot 11 \cdot 17$ and $a_{397} = 24$; at $\ell = 991$, $\#E(\mathbf{F}_{991}) = 1045 = 5 \cdot 11 \cdot 19$ and $a_{991} = -53$.

2. The localization determinant

For a direction ℓ, the local norm quotient $E(\mathbf{Q}_\ell)/NE(L_\ell)$ is identified with $E(\mathbf{F}_\ell)/11\,E(\mathbf{F}_\ell)$ (inherited, Proposition 4.1), so localizing a global point is reducing it mod ℓ and reading it in a cyclic group of order 11 — through the cofactor $m = \#E(\mathbf{F}_\ell)/11$, since $mR = O$ exactly when $R \in 11\,E(\mathbf{F}_\ell)$. Normalizing each row to $(1, k_\ell)$,

$$M_{\mathrm{loc}} = \begin{pmatrix} 1 & 2 \\ 1 & 4 \end{pmatrix}, \qquad \det M_{\mathrm{loc}} = 2 \neq 0 \text{ in } \mathbf{F}_{11}.$$

This was computed twice, by two implementations of the group law that share no code. The first read the cofactor multiples on the minimal model: $34\,P = (217, 30)$ and $34\,Q = (11, 115)$ at 397, $95\,P = (744, 133)$ and $95\,Q = (822, 620)$ at 991. The second, on the short model, found more than the matrix: P' **generates** both groups — its orders are 374 and 1045 — and the discrete logarithms are $Q' = 244\,P'$ in $E(\mathbf{F}_{397})$ and $Q' = 356\,P'$ in $E(\mathbf{F}_{991})$, found by exhaustive stepping. The slopes 2 and 4 must then be 244 and 356 mod 11, and they are. The four multiples the programme prints — $34\,P' = (281, 236)$, $34\,Q' = (11, 334)$, $95\,P' = (39, 97)$, $95\,Q' = (865, 243)$ — agree exactly.

The simultaneous reduction $\rho(a,b) = (a + 244\,b \bmod 374,\ a + 356\,b \bmod 1045)$ is surjective, with image of size $390830 = 374 \cdot 1045$: the two orders share only the factor 11, and the compatibility condition is solvable for every target because $356 - 244 = 112 \equiv 2$ is a unit modulo 11. The programme's kernel basis $(5742, -22)$, $(-254980, 1045)$ lies in the kernel and has determinant 390830, so it is a basis; the index $[E(\mathbf{Q}) : E^S(\mathbf{Q})]$ is 390830, with 11-adic valuation 2; and the cokernel is trivial.

3. Three boxed statements, one determinant

With rows normalized to $(1, k)$, the norm-Selmer kernels are the lines $\mathbf{F}_{11}(Q - 2P)$ at 397 and $\mathbf{F}_{11}(Q - 4P)$ at 991, and the Selmer cube has dimensions $2 \to 1, 1 \to 0$ and cardinalities $121 \to 11 \to 1$ — exactly as the programme states. (Its top, dim $= 2$, needs rank 2 and $Ш(E/\mathbf{Q})[11] = 0$, both inherited; only the trivial torsion is computed here.)

Then $\det M_{\mathrm{loc}} = k_{991} - k_{397}$, and three statements the programme boxes in two different documents are all the condition $k_{991} \neq k_{397}$:

- the norm-Selmer group cut out by both directions is zero;
- the two rank-one faces of the cube are transverse;
- the Bockstein determinant of §6 is non-zero, by the programme's identification of it with $\det M_{\mathrm{loc}}$ (inherited).

Three boxed statements read as three confirmations, and they are one arithmetic fact; none is evidence for either other. The same shape appears in §4: the truncation factor $L_{11}(E,1)^{-1} = 16/11$ and the point count $\#E(\mathbf{F}_{11}) = 16$ are one computation, since $1 - a_p/p + 1/p = \#E(\mathbf{F}_p)/p$ at a good prime, and their agreement confirms nothing.

The pair is a choice. Among the primes below 20000 with $\ell \equiv 1 \pmod{11}$, 199 have $11 \nmid \#E(\mathbf{F}_\ell)$, one ($\ell = 19867$) has 11^3 dividing it, one ($\ell = 19009$) has both generators in $11\,E(\mathbf{F}_\ell)$ and so imposes no condition, and the remaining 23 give rows of the form $(1, k)$, with ten of the eleven residues occupied. A pair degenerates exactly when its two k agree: 230 of the 253 pairs give a non-zero determinant, 90.9%, and the 23 that degenerate are what uniform k would predict. $\{397, 991\}$ is the smallest pair, not a distinguished one. The first version of this line's own gate had counted 25 directions, mixing two criteria in one log — divisibility by 11 for the list and exact divisibility for the rows; the count above uses the second throughout.

4. A local unit, and a valuation that depends on the basis

The programme isolates the explicitly computable 11-local factors of the rank-2 element and asks whether a hidden 11-denominator survives. Its chain was recomputed link by link: the truncation factor $(16/11)(388/389)$ has 11-adic valuation -1; $\omega'/\omega = 1/6$; and, the load-bearing step, $16\,P'$ lies in the formal group at 11 with $v_{11}(t(16\,P')) = 1$ and $t(16\,P')/11 \equiv 7 \pmod{11}$ — computed by double-and-add over $\mathbf{Q}$ in exact rational arithmetic, on a point whose x-coordinate has a 38-digit numerator. The formal logarithm agrees with t modulo 11^2 on $11\mathbf{Z}_{11}$ (its n-th term has valuation at least $n - v_{11}(n)$, checked to $n = 199$), and the chain closes with $\log_\omega(P)/11 \equiv 4$, so the local unit u_{loc} has valuation 0 and residue 4.

What the programme does not say: since $16 = \#E(\mathbf{F}_{11})$ sends every rational point into the formal group, $\varphi(R) = [t(16\,R)/11]$ is a **homomorphism** $E(\mathbf{Q}) \to \mathbf{Z}/11$, with $\varphi(P) = 7$ and $\varphi(Q) = 1$, so

$\varphi(aP+bQ) = 7a+b$ — checked on all 48 combinations with $|a|, |b| \le 3$. It is surjective, with a kernel of index 11, and **the kernel meets a basis**: $\{3P + Q, P\}$ has determinant -1, and its first vector has $v_{11}(\log) = 2$. In that basis u_{loc} has valuation 1. So the programme's sentence that multiplying by u_{loc} "neither changes the field-of-definition gate nor the 11-valuation" is true of a basis whose first vector is P, and of no other kind: the rationality equivalence it boxes survives any basis (it needs only $u_{\mathrm{loc}} \neq 0$), the valuation clause does not. A sample suggested the opposite — all 16 small integral points with $|x| \le 40$ give valuation 1 — and the homomorphism, not the sample, decides. The programme's own document on the rank-2 scalar draws the same line in general, putting a rationality gate before a valuation gate; here the failure of the second without the first is explicit, and of index 11.

As an independent check that $\{3P + Q, P\}$ is a basis and not an index-k subgroup, whose regulator would be k^2 times larger: the two regulators at doubling depth 8 are 0.152467 and 0.152510, apart by 4.3×10^{-5}, which is the method's precision at that depth.

5. The Kurihara number, a third time

The programme proves $Ш(E/\mathbf{Q})[11^\infty] = 0$ from Kim's theorem — whose input, the Iwasawa main conjecture for E at 11, it cites to Burungale, Castella and Skinner — and one finite fact: the mod-11 Kurihara number at $n = 397 \cdot 991 = 393427$ is non-zero. It reports that number as 6 in a normalization it does not disclose. An independent package elsewhere in the lab had rebuilt the computation at a disclosed scale and found 5. This line built a third implementation sharing no code with either.

Modular symbols mod 11 for $\Gamma_0(389)$, built here. Manin symbols on $\mathbf{P}^1(\mathbf{F}_{389})$ — 390 generators, 780 relation rows from the two- and three-term relations — reduce by sparse elimination over $\mathbf{F}_{11}$ to rank 325 and a quotient of dimension 65, which is $2g + 1$ with $g(X_0(389)) = 32$ from the genus formula, not read. Hecke operators by Merel's matrices of determinant q (4, 7, 15, 25, 63, 93 and 109 of them at $q = 2, 3, 5, 7, 13, 17, 19$), acting on the bottom row, with point-counted $a_2, a_3, a_5 = -2, -2, -3$, cut the space to dimension 2; the plus condition $\lambda(c, d) = \lambda(-c, d)$ to 1. That this eigenline then has the point-counted eigenvalues $-5, -3, -6, 5$ at $7, 13, 17, 19$ is the check that the operators and their action are right; a transposed action does not pass it. The scale is $\lambda(1, 5) = 1$, the first non-zero coordinate.

The sum. Over all $392040 = \varphi(n)$ units, with primitive roots 5 mod 397 and 6 mod 991 and logarithms reduced mod 11, the plus part of $\{\infty, a/n\}$ computed by continued fractions: $\delta_n = 5$, and the integer raw product sum is 43605160 — the other package's figure exactly, which can only happen if the eigenline, the path convention and both logarithm tables agree term by term. Beyond δ, the whole of $\bar{\theta}_n$ modulo I^3 was computed: its constant, X, Y, X^2 and Y^2 coefficients are 0 and its XY coefficient is 5, so $\mathrm{ord}_I \bar{\theta}_n = 2$ and $\bar{\theta}_n \equiv 5X_{397}X_{991} \pmod{I^3}$. The rank-one Kurihara numbers at 397 alone and at 991 alone are both 0, as Kim's theorem requires when the Selmer corank is 2.

Verdict. The theorem's input, $\delta \neq 0$, is `COMPUTED_HERE`, by the third of three implementations that agree. The programme's 6 is not reproduced and is not called wrong: a normalization of a one-dimensional eigenline is a unit away, and the one the programme used is not written down. The implication to $Ш[11^\infty] = 0$ is the programme's, through a theorem this line has not read, and is not claimed here.

6. The Bockstein determinant, and a ratio that is a coordinate

Let $A = \mathbf{F}_{11}[G]$, $G \cong C_{11} \times C_{11}$, with $X = \gamma_{397} - 1$ and $Y = \gamma_{991} - 1$ and augmentation ideal I; modulo I^3 it has six monomials, and $(1+X)^{11} \equiv 1$ holds there automatically. The programme's finite norm-Bockstein operator has matrix $\begin{pmatrix} X & 2X \\ Y & 4Y \end{pmatrix}$, and the ring's own multiplication gives

$$\det B_N = X \cdot 4Y - 2X \cdot Y = 2\,XY \pmod{I^3}.$$

What a change of generators does. Replacing $\gamma_{397} \mapsto \gamma_{397}^{a}$ and $\gamma_{991} \mapsto \gamma_{991}^{b}$ multiplies the determinant's coefficient by ab. Over all 100 pairs (a, b), $\mathrm{ord}_I = 2$ and the line $\mathbf{F}_{11}XY$ are preserved, and the coefficient takes every value in $\mathbf{F}_{11}^{\times}$. Non-vanishing and the line are invariants; the coefficient is a coordinate.

The ratio. The programme observes that $[\bar{\theta}_n]_2 = 6XY$ and $\det B_N = 2XY$ span the same line, and declines to promote $6/2 = 3$ to an invariant. It is right to decline, and the reason is now a computed set. At the disclosed scale the ratio is $5/2 = 8$. And a change of primitive roots alone moves it anywhere: $\log_{g'} = \log_{g'}(g) \cdot \log_g$, and as g' runs over the 120 primitive roots mod 397, $\log_{g'}(5)$ mod 11 runs over all ten units (likewise over the 240 mod 991). So δ, and with it the ratio, reaches every unit. The identity was confirmed on the full 392040-term sum for two other root pairs: $(7, 11)$, with log scales 10 and 10, gives 5 again, and $(13, 7)$, with scales 6 and 7, gives 1. "3" is a coordinate, not a number.

Kim's hypotheses, where computable. $p = 11 \geq 5$; good ordinary; $E(\mathbf{Q}_{11})[11] = 0$, since $11 \nmid 16$ and the formal group has no 11-torsion when $e = 1 < p - 1$; $c_{389} = 1$; trivial torsion; and $\bar{\rho}_{E,11}$ **surjective**, certified by Frobenius witnesses that refute each maximal proper subgroup — the Borel at $q = 2$ ($a_2 = -2$, discriminant a non-residue mod 11), the normalizer of the split Cartan at 2, of the nonsplit Cartan at 3, and the exceptional images by projective orders 4 at 2 and 5 at 3, each computed two ways that must agree. The classification behind the certificate is cited; the witnesses are computed. (An earlier version of the gate, and this paper, gave the order at 3 as 6: the gate read orders off a^2/q with the wrong condition for order 5. The certificate is unchanged, since S_4 has no element of order 5; found in review.) The Manin constant is the one hypothesis left as an external record.

7. The programme's ledger, read as data

The programme's documents declare gate statuses in fenced blocks, and a reader building on them needs to know which `CLOSED` is a computation and which is a citation — the ledgers write both with the same word. Every row of the four documents that carry one was extracted verbatim: 39 distinct gate names, five of them with more than one status, and all five explained, either as a version-ordered move or as the same verdict at different resolution. The blocking graph is acyclic. One edge is genuinely ambiguous: `P5-LAT11 BLOCKED BY BOC-NZ11 + GPR11` names a target that matches three declared gates, and a later version resolves it to the minimal one while marking the full one "stronger than needed" — read the other way, an attack would go after a theorem the chain does not need.

Two gates the ledgers close by citation are closed here on this line's own evidence. `P5-BOC-NZ11` needs $\det(B_N) \neq 0$, which by the programme's identification is $\det M_{\mathrm{loc}} = 2 \neq 0$ (§2). `P5-RESIDUAL-IRR11`, which a ledger closes by "maximal 11-adic image", needs only that E has no rational 11-isogeny, and two routes give it without that stronger claim: $j(E) = 112^3/389 = 1404928/389$ is not an integer, so it is none of the three non-cuspidal j-invariants on $X_0(11)$, -24729001, -32768 and -121; and E

is semistable, so Mazur's isogeny theorem allows a rational p-isogeny only for $p \leq 7$. The arithmetic of both routes is computed; the two theorems are cited, so this verdict is `PASS by cited theorem`. §6's surjectivity certificate is a third, independent route.

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

Each figure above 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. Four things it found are worth stating:

- **A scan that under-reports looks clean.** The first ledger scan matched statuses with a word boundary, and the underscore is a word character, so it silently skipped every status written as `CLOSED_BY_PUBLISHED_COMPUTATION` — about a third of the rows, including both readings of the one gate whose status had moved. The first report therefore showed fewer conflicts and a clean bill on exactly that gate. The drill now pins the row count and specific rows.
- **A symmetry, recorded as a control.** One planted defect — the path written with $(-1)^{i}$ in place of $(-1)^{i-1}$ — could not be caught, and rightly: $(-c : d) = (c : -d)$ projectively, so a functional even in c is even in d, and the plus part does not see the sign. It is a convention the answer is invariant under, and it stays as a control with that reason attached.
- **A defect that recursed.** Two defects first called the very function they replaced, so the check went red on a recursion error rather than on the defect; the harness in use had swallowed the exception. They are now bound to the original function.
- **A classical list pinned.** Dropping one of the three j-invariants of $X_0(11)$ would not have changed today's verdict, since $j(E)$ is in neither list; the list is pinned anyway, because a corrupted input that does not matter today will matter later.

9. Contributions

The 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 authors sit at a round table, with no first and no last.

Aletheia — model: ChatGPT, GPT series — is a standing author of the research programme, seated by Neo.K's decision. The programme's packages record Neo.K's name; which of their parts Aletheia wrote is not recorded in them, and this paper assigns her none of its recomputations.

Neo.K wrote the research programme whose documents this paper recomputes: the curve, the prime, the two directions, the localization matrix, the local-unit chain, the Selmer cube, the Kurihara certificate and the Bockstein formalism are all from its packages, which carry his name.

墜衡 (Zhuì Héng) — the independent verification line; model: Claude, Opus series — recomputed every figure with independently written code, including two implementations of the group law and mod-11 modular symbols for $\Gamma_0(389)$ built from Manin symbols; found that three boxed statements are one determinant, that the local unit's valuation depends on the basis, that the pair of directions is generic, and that the ratio 3 is a coordinate; reconciled the ledger; built and drilled the instruments; and wrote this paper. Nothing in the programme is this line's invention.

Inputs from outside the byline. The Kurihara package of the stress test run by the lab's Witness line,

見證, first reproduced the Kurihara computation at a disclosed scale; this paper uses that scale, and the agreement of its producer and verifier with this line's implementation is the "three implementations" of §5. It is credited here, and its authors are not on this byline. The theorems of Kim, Mazur and Burungale–Castella–Skinner, and the classification of subgroups of $\mathrm{GL}_2(\mathbf{F}_{11})$, are other people's and are cited as such.

Priority, stated plainly. No result here is claimed as new mathematics. What is offered as this line's own is the separation of the canonical from the conventional, and a complete recomputation behind it.

10. What is open

1. Whether the finite Bockstein operator is the Bockstein regulator of a published theory (`P5-CANON-BocID`).
2. The comparison of the complex leading term with the algebraic regulator (`P5-CPLX-GPR`).
3. The Kurihara number at the Néron scale, which would fix the coefficient this paper shows to be a choice.
4. A descent proving rank $E(\mathbf{Q}) = 2$ in this tree, and an independent check of $Ш(E/\mathbf{Q})[11] = 0$, both inherited 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. Ashay Burungale, Francesc Castella and Christopher Skinner, *Base Change and Iwasawa Main Conjectures for GL_2*, Int. Math. Res. Not. IMRN 2025, doi:10.1093/imrn/rnaf082; arXiv:2405.00270.
2. Chan-Ho Kim, *The structure of Selmer groups and the Iwasawa main conjecture for elliptic curves*, Amer. J. Math. 148 (2026) 79–129, doi:10.1353/ajm.2026.a980769; arXiv:2203.12159.
3. B. Mazur, *Rational isogenies of prime degree*, with an appendix by D. Goldfeld, Invent. Math. 44 (1978) 129–162, doi:10.1007/BF01390348.

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.
- The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org — the record of the elliptic curve 389.a1, from which this paper takes its Manin constant; the line's tree does not record when it was read, and it was read again for this version on 2026-10-24.

A. Reproduction

Everything is Python standard library, no network. 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 programme's documents** this paper recomputes: https://amral.evemisslab.com/bsd/p5/;
- **the stress-test line's independent Kurihara package**: https://amral.evemisslab.com/bsd/stress-test/;
- **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`).