

OpenAI Math Digest

CATALOGUE 004

Hilbert's tenth problem over $\mathbb{Q}$

Catalogue synthesis & 2 proof overviews

Independent reading guide · English edition

Edition: 2026-10-15

Created by: Masataka Iwai · Osaka University

AI-generated explanations may contain errors. Check important claims and proofs against the original manuscripts. This booklet collects the website's explanations, not the original papers. Expert review and formal verification have not been performed.

Contents

The synthesis comes first, followed by all 2 overviews in official catalogue order. The contents and citations are clickable. Wide tables are arranged as entries for print; the claims and source references are retained.

00 · Catalogue synthesis	3
01 · Hilbert’s tenth problem over the rational numbers	10
02 · A pointwise 2-converse for elliptic curves with rational two-torsion	22

Original-manuscript snapshot: 1581d4cbdd69a0faf34b2089614fe2a814316a6a

Catalogue 004 · Synthesis

[Read on the website ↗](#)

CATALOGUE 004

Hilbert's tenth problem over $\mathbb{Q}$

Catalogue 004 contains a manuscript on undecidability of rational solvability and a pointwise 2-converse for elliptic curves used to construct its local conditions. The final logical step is a Turing reduction from integer solvability to rational solvability; it does not establish an existential definition of the integers.

1. Papers in official catalogue order

These summaries give the principal scope; consult the cited original results for the complete hypotheses and statements.

Catalogue 004 · 2026-10-15 checked source snapshot

#

01

Manuscript and overview

Hilbert's tenth problem over the rational numbers →

Short name: Hilbert's tenth problem over the rational numbers

October 6, 2026 · 62 pages

Original paper (GitHub) ↗

Principal claim

Rational solvability of integer-coefficient polynomials is undecidable when the number of variables is part of the input. Its Turing degree is $0'$, also for degree at most four and sums of squares of quadratic polynomials.

Theorem 1.1 · p. 3; Corollary 7.1 · pp. 56–57 ↗

Role and available overview

Recovers an integer zero from recursive finite rational tests. Elliptic index comparisons, pole parity and a five-point contact-height bound combine with parallel searches for an integer zero and a failed test.

Read the proof overview →

#

02

Manuscript and overview

A pointwise 2-converse for elliptic curves with rational two-torsion →

Short name: A pointwise 2-converse for elliptic curves with rational two-torsion

October 7, 2026 · 91 pages

[Original paper \(GitHub\)](#) ↗

Principal claim

For $E/\mathbb{Q}$ with nonzero rational two-torsion and full 2^∞ -Selmer corank zero or one, analytic and Mordell–Weil ranks equal that corank and $\text{Sha}(E/\mathbb{Q})$ is finite, with arbitrary reduction at 2.

[Theorem 1.1 · p. 2](#) ↗

Role and available overview

Integral interpolation recovers the central value or derivative at a fixed curve from nonzero addresses in finite twist families. The preceding manuscript uses the Sha-finiteness conclusion in Lemma 3.4 to obtain a rational point in a prescribed square class.

[Read the proof overview](#) →

References on the arrows

The following keys distinguish the two manuscripts. The diagram separates the direct input between manuscripts from subsequent uses within a single manuscript.

- **OpenAI26H:** OpenAI, Hilbert’s tenth problem over the rational numbers, October 6, 2026. Supplies finite rational tests, pole parity, the five-point contact-height bound and undecidability.

[\[OpenAI26H, Theorem 1.1, p. 3\]](#)

- **OpenAI26P:** OpenAI, A pointwise 2-converse for elliptic curves with rational two-torsion, October 7, 2026. Supplies analytic and Mordell–Weil rank equality and finiteness of **Sha** when the full 2^∞ -Selmer corank is zero or one.

[\[OpenAI26P, Theorem 1.1, p. 2\]](#)

Printed pages agree with PDF positions. GitHub previews do not automatically jump to a cited page.

2. From a pointwise 2-converse to finite tests



How rational points from the pointwise 2-converse join height bounds and local comparisons in finite rational tests

Open figure ↗ TeX source ↓

1. Realizing a Selmer class by a prescribed rational point

The pointwise 2-converse directly enters Lemma 3.4 of the Hilbert manuscript. The curve is $E_l : y^2 = x(x - l)(x + 3l)$, and two-descent gives

$$r + \dim_{\mathbf{F}_2} \text{Sha}(E_l/\mathbf{Q})[2] = 1.$$

The proof first checks that the full 2^∞ -Selmer corank is at most one. It then uses the finiteness of Sha supplied by the converse. Alternation of the Cassels–Tate pairing on the finite 2-primary group makes $\dim \text{Sha}[2]$ even, giving $r = 1$ and $\text{Sha}[2] = 0$. The selected Selmer class $\gamma = (\beta, 1)$ is therefore represented by a rational point.

[OpenAI26H, Lemma 3.4, pp. 23–24]

Lemma 3.6 supplies one parameter for two twists. Applying the rational-point conclusion to both gives a positive existential condition Φ that holds on every integer. Outside finitely many exceptional primes, Φ excludes poles of odd order but allows poles of even order. This one-sided condition is not a definition of $\mathbf{Z}$. See the Hilbert article and the 2-converse article.

[OpenAI26H, Proposition 2.8, p. 12]

[OpenAI26H, §3.4, pp. 24–26]

2. Combining local comparisons and heights in one model

If all finite tests succeed, compactness produces a ring R with a root in an elementary extension of the rational field. Its elliptic index map $\eta : R \hookrightarrow {}^*\mathbf{Z}$ is additive; multiplicativity has not been established. Pole parity selects an appropriate tested local branch at a contact prime, and paired elliptic local tests give congruences between ring values and their indices.

[OpenAI26H, Lemma 2.10; Proposition 2.11, pp. 14–15]

Applying these congruences to the fixed root coordinates makes the K th power of each slope's contact radical divide the same $\delta = f(\eta(a))$. Together with the five-point estimate $h(s) \leq HM(s)^c$, this yields a uniform height bound for all ring values when $\delta \neq 0$. Quadratic growth of the elliptic canonical height forces the root indices into an ordinary finite interval; additivity and injectivity then recover an ordinary integer root. The prime-pattern construction supplies the ordinary model for the opposite implication: an integer root passes every test.

[OpenAI26H, Theorem 2.4, p. 9]

[OpenAI26H, §2.4; Proposition 2.12, pp. 12–17]

3. Turning a hypothetical decision procedure into a contradiction

Assume a rational-solvability decider exists. Each finite test uses finitely many rational-solvability queries, so parallel searches for an integer zero and for a failed test would decide integer solvability. The proof distinguishes hardcoding finitely many fixed arithmetic data from computing them afresh for each input polynomial. The reduction and normalization to degree at most four are covered in the [Hilbert article](#).

[OpenAI26H, Corollary 7.1, pp. 56–57]

3. The direct input and its subsequent uses

Input result

Pointwise 2-converse, Theorem 1.1

Used at

Hilbert, Lemma 3.4

Role and conditions

Nonzero rational two-torsion and full Selmer corank ≤ 1 are checked before using finiteness of **Sha**

Checking scope

Statements and application passages checked in both sources

The continuation through Proposition 2.8, local-branch selection and finite tests is a transitive route within the Hilbert manuscript. The 2-converse alone does not supply the height bound or effectiveness of the tests. Remark 3.5 of the Hilbert manuscript records replacement by a converse without the rational-two-torsion hypothesis; that alternative proof route is not checked here.

[OpenAI26H, Lemma 3.4, pp. 23–24]

4. Sources and checking scope

The official subject is **Number theory**, covering entries 001–031. Entry 004 appears on p.2 of the OpenAI Research Catalog, in the manuscript order shown above. The official repository is fixed at commit 1581d4cbdd69a0faf34b2089614fe2a814316a6a. The manuscript versions are October 6, 2026 and October 7, 2026 respectively.

- Hilbert manuscript: read §§2.4–2.7 for finite tests and recovery of an integer root, §§3.3–3.4 for the pointwise-converse application and simultaneous realization on two twists, and §7 for the Turing degree and normalization.
- Pointwise manuscript: check the full Selmer hypothesis of Theorem 1.1, then follow §9 through corank-zero interpolation, uniform odd normalization, and return to a corank-one curve using a fixed negative twist.

This guide checks the principal statements and connections against the proof text. It does not independently verify every integral interpolation and uniform estimate in the Pointwise manuscript, every height and sieve estimate in the Hilbert manuscript, or the complete proofs of external inputs. Each article records its reading and unresolved scope at the end.

Hilbert's tenth problem over the rational numbers

Finite rational tests, additive elliptic indices, and a uniform height contradiction

The manuscript claims undecidability of rational polynomial solvability by a Turing reduction from integer solvability. Its argument does not construct an existential definition of the integers or a Diophantine model preserving multiplication. We distinguish the manuscript's assertions from the inputs and applications checked for this account.

Manuscript author: OpenAI · October 6, 2026 · 62 pages, including references

[Read the manuscript on GitHub ↗](#)

1. Main results

Theorem 1.1 — Undecidability of rational solvability

There is no algorithm that, given $f \in \mathbb{Z}[X_1, \dots, X_n]$, decides whether it has a zero in $\mathbb{Q}^n$. The number of variables n is part of the input. The manuscript states this as a theorem without an additional conjectural assumption.

[Theorem 1.1 · p. 3](#)

Corollary 7.1 — Turing degree and a quartic normal form

Under the usual effective coding, the set $H10(\mathbb{Q})$ of integral polynomials with a rational zero has Turing degree $\mathbf{0}'$, the degree of the halting problem. The same holds for both restricted input problems:

1. Rational solvability of integral polynomials of total degree at most four.

2. Given a nonempty finite list $q_1, \dots, q_s \in \mathbb{Z}[X_1, \dots, X_N]$, each of total degree at most two, whether $\sum_{i=1}^s q_i^2$ has a rational zero.

There is no bound on the number of variables, the number of summands in (2), or coefficient heights.

Corollary 7.1 · p. 56

References on the arrows

Unprefixed theorem, lemma, section and equation numbers refer to [Hilbert's tenth problem over the rational numbers](#). External inputs use the following keys.

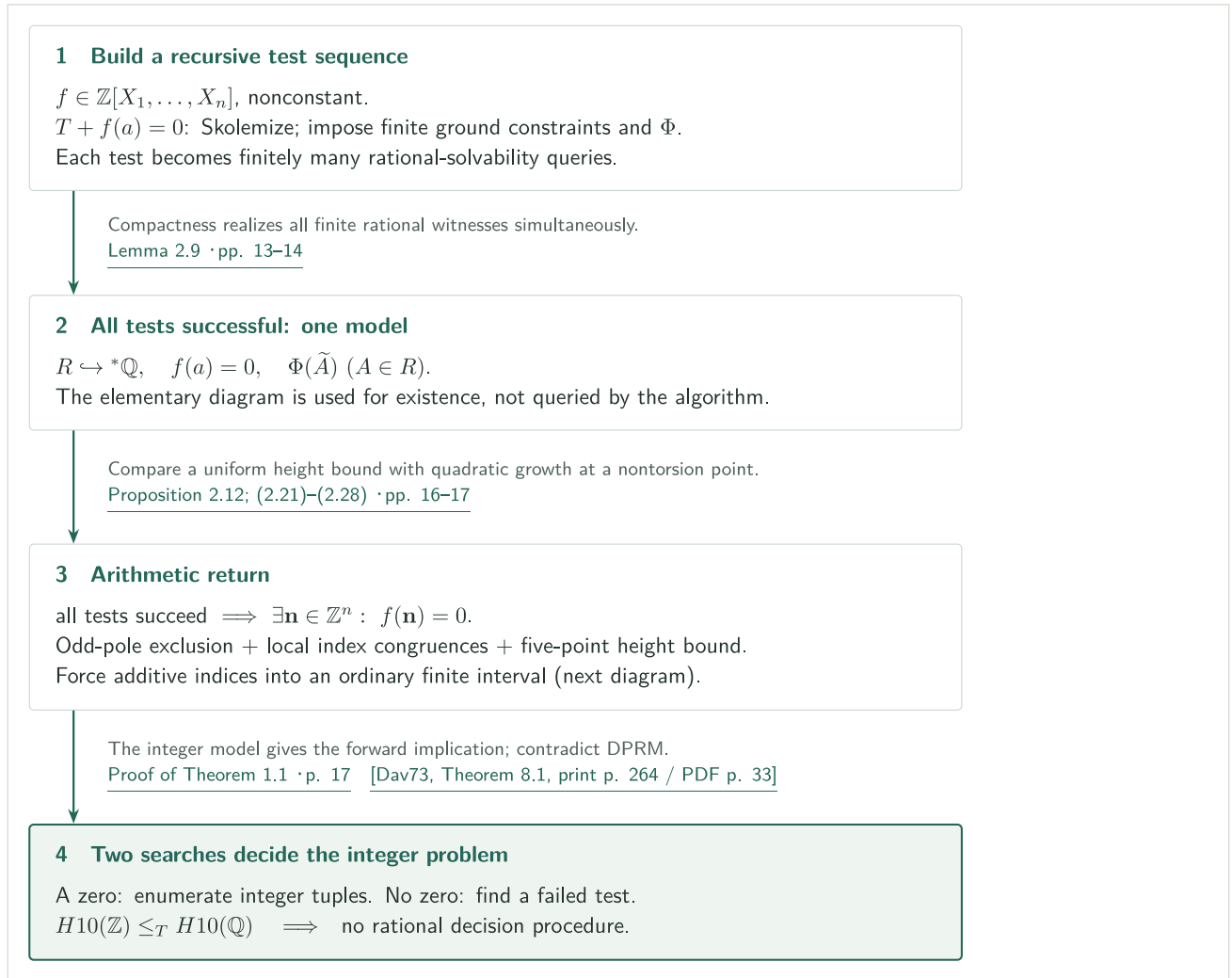
- [OpenAI26P](#) OpenAI — A pointwise 2-converse for elliptic curves with rational two-torsion: Finiteness of Sha from rational two-torsion and full 2-primary Selmer corank zero or one; direct input to Lemma 3.4. October 7, 2026; fixed commit 1581d4cbdd69a0faf34b2089614fe2a814316a6a.
- [OpenAI26F](#) OpenAI — Fontaine–Mazur modularity at the prime 2: Modularity of the odd regular two-dimensional 2-adic representation in §4.7, without residual-image restrictions. October 6, 2026; fixed commit 1581d4cbdd69a0faf34b2089614fe2a814316a6a.
- [Dav73](#) Martin Davis — Hilbert's tenth problem is unsolvable: DPRM representation theorem used for undecidability and the degree of the integer problem. The American Mathematical Monthly 80(3) (1973), 233–269; source scan includes a leading JSTOR cover page.
- [PS99](#) Bjorn Poonen; Michael Stoll — The Cassels–Tate pairing on polarized abelian varieties: Perfect alternating pairing on finite Sha and the rational-divisor condition on the polarization. Author version: November 6, 1998; minor correction August 23, 2014; published Annals of Mathematics 150 (1999), 1109–1149.

Each citation gives the result and pages. When printed pagination differs from the PDF position, both are shown. GitHub previews do not automatically jump to the cited page.

2. Proof of Theorem 1.1 — Two searches through finite tests

Proof target : [Theorem 1.1](#) · p. 3

Proof route. For nonconstant f , construct a recursive sequence of finite tests such that integer solvability is equivalent to success of every test. Proposition 2.12, explained next, is the arithmetic core of the reverse implication. An oracle for rational solvability would decide each test; running integer-zero enumeration alongside a search for a failed test would then decide integer solvability.



The integer model, finite tests, compactness, and the return to an integer zero

[Open figure ↗](#) [TeX source ↓](#)

1. Separate a first-order theory into finite existential queries

For fixed $F = \mathbb{Q}(\sqrt{2})$, $d = 75 - 53\sqrt{2}$, and $E : y^2 = x^3 - d^2x$, Proposition 2.1 supplies $m > 0$ and a nontorsion point P with $mE(F) = \mathbb{Z}P$. The theory T requires a characteristic-zero integral domain R with $\sqrt{2} \notin \text{Frac}(R)$, assigning to each $a \in R$ a point $T_a \in mE(\text{Frac}(R)(\sqrt{2}))$. It imposes $T_0 = O, T_1 = P, T_{a+a'} = T_a + T_{a'}$, and finite, nonzero coordinate conditions for nonzero a . Six R -valued functions record coordinate numerators and denominators.

For each ordinary integer $K \geq 1$ and each $A \in R$, the theory also requires a three-slope representation $A = (u_1 + u_2 + u_3)/v$ and paired local comparisons at factors of the contact forms. The theory itself contains universal quantifiers; it does not define R inside the rationals by one existential formula. The fixed finite data are independent of the input f and can be hardcoded. Lemma 2.7 supplies an integer model with $T_a = aP$.

[Proposition 2.1; §2.3; Lemma 2.7 · pp. 7, 11–12](#)

Adjoin $f(a) = 0$, Skolemize, and enumerate ground terms. Assign rational variables to their values, and impose finite collections of constraints for ring operations, functionality on equal inputs, ground instances of universal axioms, and the positive existential condition Φ on every term value. Each finite collection is an existential Boolean combination of polynomial equations and inequations. Replacing $g \neq 0$ by $gy = 1$ and conjunctions by sums of squares reduces it to finitely many rational-solvability queries for integral polynomials. Auxiliary witnesses for Φ and inverse variables used in this translation are not added as new ground terms of the term-generated ring.

§2.4 · pp. 12–13

2. Obtain a model from all successful tests and complete the failure search

An integer zero gives an integer model whose term values all satisfy Φ , so every test succeeds. Conversely, if all tests succeed, compactness gives $R \hookrightarrow {}^*\mathbb{Q}$ and $f(a) = 0$ inside one elementary extension of the ordinary structure carrying arithmetic, valuations, heights, and finite products. The elementary diagram is used only in this existence argument; the algorithm neither enumerates nor queries all true arithmetic sentences.

Proposition 2.12 extracts an ordinary integer zero from this model. Hence, when no integer zero exists, a finite test fails. Alternating the integer-zero enumeration with the failure search turns a hypothetical rational decision procedure into an integer decision procedure, contradicting DPRM. Constant polynomials are handled directly.

Lemma 2.9 · pp. 13–14

Proof of Theorem 1.1 · p. 17

[Dav73, Theorem 8.1, print p. 264 / PDF p. 33]

3. Proof of Proposition 2.12 — One error for every ring element

Proof target : Proposition 2.12; (2.21)–(2.28) · pp. 16–17

Proposition 2.12 — From all successful finite tests to an integer zero

Let $f \in \mathbb{Z}[X_1, \dots, X_n]$ be nonconstant. If every finite system of rational constraints constructed for f in §2.4 is solvable, then f has a zero in $\mathbb{Z}^n$.

Proposition 2.12; (2.21)–(2.28) · pp. 16–17

Tildes denote images in the elementary extension. The rule $\tilde{T}_a = \eta(a)P$ defines an injective additive map $\eta : R \rightarrow {}^*\mathbb{Z}$ with $\eta(1) = 1$, but multiplication is not yet preserved. For the fixed root $a = (a_j)$ put

$$\delta = f(\eta(a_1), \dots, \eta(a_n)), \quad B = \max(1, |\eta(a_1)|, \dots, |\eta(a_n)|), \quad D = \max(1, \deg f).$$

If $\delta = 0$, elementarity already gives an ordinary integer zero. The diagram treats $\delta \neq 0$.



Odd contact yields index congruences, a height bound on the entire ring, and comparison with quadratic elliptic growth

[Open figure ↗](#) [TeX source ↓](#)

1. Connect odd contact to a tested localization

Theorem 2.4 supplies five fixed points $C \subset \mathbb{P}^1(\mathbb{Q})$ including infinity, a finite exceptional prime set S , and $H, c > 0$. Choose primitive integral linear forms L_b vanishing at these points. For $s = (u : v) \notin C$ set

$$M_S(s) = \prod_{q \notin S : \exists b \in C, v_q(L_b(u,v)) - \min(v_q(u), v_q(v)) \text{ odd}} q, \quad h(s) \leq HM_S(s)^c.$$

Here h is logarithmic Weil height and the product has no repetitions. Enlarging the exceptional set changes only the constant, not c . Fix one ordinary $K \geq cD$ and choose representations for every $A \in R$ at this precision. Contact-form values have the shape $\varepsilon k r$, with k in a fixed finite set; a contact prime q makes the valuation of some $\tilde{r}$ odd.

Theorem 2.4; Corollary 2.5 · pp. 9–10

The condition Φ holds on all integers and makes negative valuations outside S_1 even; it does not define integrality. Since every ring value satisfies Φ , every ring valuation lying in the convex subgroup $J \subset {}^*\mathbb{Z}$ generated by negative ring valuations is even. Thus the odd value $v_q(\tilde{r})$ lies outside J and is positive in the quotient valuation. Its center is one of the two branches of $R_F/rR_F \simeq (R/rR)^2$. Lemma 2.10 converts divisibility by r^l in that tested localization into the actual extended-valuation bound $v^* \geq l$. The ring is not assumed to be q -integral at the start.

Lemma 2.10; Proposition 2.11 · pp. 14–15

2. Use the conjugate comparison to establish integrality of the index ratio first

At the selected branch, the same nonzero $h, j_0 \in R$ work for every $a \in R$. The formal-parameter comparison on the conjugate curve gives

$$\eta(ha) - 4\eta(a) \equiv 0 \pmod{q^K}, \quad \eta(h) \equiv 4 \pmod{q^K}.$$

As $q \neq 2$, the denominator $\eta(h)$ is a unit: $\eta(ha)/\eta(h)$ is integral and congruent to $\eta(a)$. Only after obtaining this integrality can one apply Proposition 2.2 to the truncated formal logarithm ℓ_K on the primary curve. Combining its estimate with the tested condition yields

$$v_q(\tilde{a} - \eta(a)) \geq K \quad (a \in R)$$

and integrality of $\tilde{a}$. One never substitutes $\eta(ha) = \eta(h)\eta(a)$ by assuming multiplicativity. Transfer concerns evaluations of the fixed-degree polynomial ℓ_K , not an infinite series in the elementary extension.

Proposition 2.2; Lemma 2.3 · pp. 8–9

3. Fix the root error and bound heights uniformly

Apply these congruences to the root coordinates at every contact prime of each slope

$s_i = (\tilde{u}_i : \tilde{v})$. They give $v_q(\delta) \geq K$, and transfer of finite-product divisibility gives $M_K(s_i)^K \mid \delta$. Since $|\delta| \leq C_f B^D$,

$$h(s_i) \leq H_K |\delta|^{c/K} \ll_f B, \quad h(\tilde{A}) \leq \sum_{i=1}^3 h(s_i) + \log 3 \ll_f B \quad (A \in R).$$

The constant is independent of A and uniform in the root tuple. Apply the bound to the three ring values in $x(T_{a_j}) = (x_0(a_j) + \sqrt{2}x_1(a_j))/x_2(a_j)$. For nonzero a_j this gives

$h(x(\eta(a_j)P)) \ll_f B$. On the other hand, the canonical-height comparison at the fixed nontorsion point gives $h(x(nP)) = 2\hat{h}(P)n^2 + O(1)$ with $\hat{h}(P) > 0$. If $B > 1$, choose a maximizing index to obtain $B^2 \ll_f B + 1$; the case $B = 1$ is immediate. All indices therefore lie in an ordinary finite interval, so $\eta(a_j) = n_j \in \mathbb{Z}$. Additivity, $\eta(1) = 1$, and injectivity force $a_j = n_j$, producing the ordinary integer zero.

Proposition 2.12; (2.21)–(2.28) · pp. 16–17

4. Proof of Corollary 7.1 — Oracle reduction and arithmetic circuits

Proof target : Corollary 7.1 · p. 56

We address the three conclusions of Corollary 7.1 in order. The parallel search above runs as a single machine with an $H10(\mathbb{Q})$ oracle. The normal-form conversion is allowed to introduce more variables.

1 Turing degree of rational solvability

$$\mathbf{0}' \leq_T H10(\mathbb{Z}) \leq_T H10(\mathbb{Q}) \leq_T \mathbf{0}'.$$

Upper bound: enumerate rational tuples and evaluate exactly.

The lower bound uses DPRM and finite tests; the circuit is effective.

[\[Dav73, Theorem 8.1, print p. 264 / PDF p. 33\]](#) [Proof of Corollary 7.1 · pp. 56–57](#)

2 Arithmetic circuit to quadratic list

$$Y_v - X_j, \quad Y_v - c, \quad Y_v - Y_u - Y_w, \quad Y_v - Y_u Y_w, \quad Y_{\text{out}}.$$

Call these $q_1, \dots, q_s$: $s \geq 1$, $\deg q_i \leq 2$.

Each input has a unique extension through the circuit.

Rational squares are nonnegative; the sum has total degree at most four.

[§7, arithmetic-circuit conversion · p. 57](#)

3 One sum of squares encodes the system

$$\exists x \in \mathbb{Q}^n : f(x) = 0 \iff \exists z \in \mathbb{Q}^N : \sum_i q_i(z)^2 = 0.$$

$$H10(\mathbb{Q}) \leq_m S_2 \leq_m H_{\leq 4}.$$

Both restricted problems are computably enumerable by rational-tuple enumeration.

[Corollary 7.1 · p. 56](#)

4 Both restrictions have degree $\mathbf{0}'$

Variables, summands, and coefficient heights remain unbounded.

The reduction from integer solvability remains a Turing reduction.

No existential definition of $\mathbb{Z}$ or many-one completeness of $H10(\mathbb{Q})$ follows.

The Turing reduction from integer solvability and the many-one reductions to sums of squares of quadratics

[Open figure ↗](#) [TeX source ↓](#)

1. Bound the degree of rational solvability in both directions

DPRM makes the halting set Diophantine over the positive integers. Replace positive-integer witnesses by $1 + u_1^2 + u_2^2 + u_3^2 + u_4^2$ to obtain $\mathbf{0}' \leq_T H10(\mathbb{Z})$. The previous argument gives $H10(\mathbb{Z}) \leq_T H10(\mathbb{Q})$. Rational-tuple enumeration makes $H10(\mathbb{Q})$ computably enumerable, giving the opposite upper bound. The arithmetic constants are hardcoded in one oracle machine, not chosen separately for each f .

[\[Dav73, Theorem 8.1, print p. 264 / PDF p. 33\]](#)

[Proof of Corollary 7.1 · pp. 56–57](#)

2. Record each operation by a quadratic equation

For every node in an arithmetic circuit for f , introduce a variable Y_v . Input, constant, sum, and product nodes give equations $Y_v - X_j = 0$, $Y_v - c = 0$, $Y_v - Y_u - Y_w = 0$, and $Y_v - Y_u Y_w = 0$, respectively. Impose $Y_{\text{out}} = 0$ at the output. The resulting nonempty quadratic list (q_i) uniquely extends every rational input tuple through the circuit equations. Nonnegativity of rational squares gives

$$\exists x \in \mathbb{Q}^n : f(x) = 0 \iff \exists z \in \mathbb{Q}^N : \bigwedge_i q_i(z) = 0 \iff \exists z \in \mathbb{Q}^N : \sum_i q_i(z)^2 = 0.$$

Consequently $H10(\mathbb{Q}) \leq_m S_2 \leq_m H_{\leq 4}$. Both restricted problems are also computably enumerable and hence have degree $\mathbf{0}'$. The arrow from the integer problem to the rational problem remains a Turing reduction: neither many-one completeness of $H10(\mathbb{Q})$ nor a single existential definition of $\mathbb{Z} \subset \mathbb{Q}$ follows. In S_2 , the list presenting the sum of squares is part of the input, so recognizing such a presentation is unnecessary.

§7, arithmetic-circuit conversion · p. 57

5. Which papers supply which steps

Source and result

Pointwise 2-converse: citation below

Used at

Lemma 3.4; Proposition 2.8

Role and required hypotheses

Full rational two-torsion of $E_l : y^2 = x(x-l)(x+3l)$ and $s_2(E_l) \leq 1$ give finiteness of the whole Sha

Checking scope

Input Theorem 1.1 and the application on pp. 23–24 checked; its proof belongs to a separate article

Source and result

Poonen–Stoll: citation below

Used at

Lemma 3.4

Role and required hypotheses

Alternation for the principal polarization from the rational divisor (O); a perfect alternating pairing on the finite 2-primary group forces $\dim \text{Sha}[2]$ even

Checking scope

Author version §1 and the application hypotheses checked

Source and result

Fontaine–Mazur at 2: citation below

Used at

§4.7

Role and required hypotheses

Modularity of continuous, irreducible, odd, finitely ramified two-dimensional representations that are de Rham at 2 with distinct weights

Checking scope

Input Theorem 1.1 and hypothesis checks on p. 39 compared; no residual-image assumption

Source and result

Davis: citation below

Used at

End of Theorem 1.1; Corollary 7.1

Role and required hypotheses

Diophantine representation of computably enumerable sets and the degree of integer solvability

Checking scope

Theorem 8.1 and the change from positive-integer to integer witnesses checked

[OpenAI26P, Theorem 1.1, p. 2]

[PS99, §1, p. 2]

[OpenAI26F, Theorem 1.1, p. 1]

[Dav73, Theorem 8.1, print p. 264 / PDF p. 33]

Integer witnesses for Proposition 2.8 realize one square class on two twists. The Selmer calculation in §3 gives $r + \dim_{\mathbb{F}_2} \text{Sha}(E_l)[2] = 1$. If the divisible part has corank t , then $t \leq \dim \text{Sha}[2]$, so $s_2 = r + t \leq 1$ **before assuming finiteness**. The pointwise 2-converse then gives finiteness; the perfect alternating pairing forces $r = 1$ and $\text{Sha}[2] = 0$, lifting the chosen Selmer class to a rational point. Apply the prime and square-class construction of Lemma 3.6 to both twists to obtain integer completeness of Φ . Exclusion of negative odd valuations is the local calculation of Lemma 3.1. The unrestricted 2-converse is an alternative input in Remark 3.5, not an additional premise of the selected route.

Proposition 2.8; Lemmas 3.1, 3.4, 3.6 · pp. 12, 18–19, 23–26

For Theorem 2.4, a cover ramified to order two at five points carries a family of quaternionic abelian surfaces. The odd-contact product M controls ramification of the fiber. CM fibers have uniformly bounded height. In the non-CM case, resolving an isogeny descent obstruction produces a two-dimensional representation. Section 4.7 verifies irreducibility, oddness, and the de Rham condition before applying Fontaine–Mazur; the weights force weight two and Tate shift zero. Bounds $N \leq CM^a$, $[L' : \mathbb{Q}] \leq CM$, the factorization $J_1(N) \sim_{L'} A \times D_0$, Jacobian-height bounds, and a quantitative isogeny estimate yield $h_F(A) \leq CM^C$. Comparison with base height gives the required $h(s) \leq HM^c$. This article does not independently verify all external theorems and constant estimates in that section.

§4.7; Lemma 4.8; completion of Theorem 2.4 · pp. 39, 42–44

Representations in the integer model come from the prime patterns of Lemma 6.1 and Corollary 6.2. For reduction-group orders d_1, d_2 , the conditions $\gcd(d_1, d_2) \mid 4$ and $r \nmid d_1 d_2$ make $h \equiv 0 \pmod{d_1}$ and $h \equiv 4 \pmod{d_2 r^K}$ compatible. They explain why the same $h, j_0 = d_2$ work for every integer a . The full prime-pattern lower bound and the uniform sieve removing bad primes lie outside the checked scope.

Lemma 6.1; Corollary 6.2 · pp. 47–48

6. Return to the sources

- §2.4 · pp. 12–13 — Effectivity of finite tests and the scope of witness variables.
- Proposition 2.2; Lemma 2.3 · pp. 8–9 — Why the conjugate comparison first makes the index ratio integral.
- Lemma 2.10; Proposition 2.11 · pp. 14–15 — Select a tested branch using odd valuation and the center of a coarsening.

- Proposition 2.12; (2.21)–(2.28) · pp. 16–17 — Use one error δ for all ring values and compare with quadratic height growth.
- Proposition 2.8; Lemmas 3.1, 3.4, 3.6 · pp. 12, 18–19, 23–26 — Separate integer completeness from odd-pole exclusion.
- §4.7; Lemma 4.8; completion of Theorem 2.4 · pp. 39, 42–44 — The modularity, level, isogeny and base-height connections.
- Lemma 6.1; Corollary 6.2 · pp. 47–48 — The CRT construction of local witnesses working for all integers.
- Proof of Corollary 7.1 · pp. 56–57 — The different starting points of the Turing and many-one reductions.

The checked passages comprise the hypotheses and all conclusions of the main results; the finite tests, compactness, branch selection, index congruences, and height contradiction in §2; the Selmer-corank bound before the 2-converse in §3; the modularity connection in §4.7; the rank-one calculation and formal logarithm in §5; simultaneous local witnesses in §6; and each reduction direction in §7. The stated inputs from Pointwise 2-converse, Fontaine–Mazur, Davis, and Poonen–Stoll were compared with their source texts.

The complete Selmer-matrix calculations in §3; all external results and constants for the cover, descent, conductors, and heights in §4; the full prime-pattern and uniform-sieve proofs in §6; and a fresh source check of textbook inputs such as Silverman’s canonical-height comparison remain incomplete. Complete external proofs, expert peer review, and formal verification have not been undertaken. This account maps the manuscript’s argument and its checked scope; it does not independently certify the main claim.

A pointwise 2-converse for elliptic curves with rational two-torsion

Recovering a missing vertex by integral interpolation on binary cubes

The manuscript determines the analytic rank of each elliptic curve with rational two-torsion from its low 2^∞ -Selmer corank. It constructs auxiliary quadratic twists with simultaneous nonvanishing at every nonzero vertex, bounds their normalized valuations uniformly, and transfers this information to the prescribed curve. This account organizes the manuscript's argument and its direct inputs; it is not an independent verification of the entire new integral construction.

Manuscript author: OpenAI · October 7, 2026 · 91 pages, including references

[Read the manuscript on GitHub ↗](#)

1. Main results

Theorem 1.1 — The rational-two-torsion pointwise 2-converse

Let $E/\mathbb{Q}$ satisfy $E(\mathbb{Q})[2] \neq 0$. For the full Selmer group with the usual local Kummer conditions at every place, assume

$$s_2(E) = \text{corank}_{\mathbb{Z}_2} \text{Sel}_{2^\infty}(E/\mathbb{Q}) \in \{0, 1\}.$$

The manuscript proves

$$\text{ord}_{s=1} L(E, s) = \text{rank}_{\mathbb{Z}} E(\mathbb{Q}) = s_2(E), \quad \text{Sha}(E/\mathbb{Q}) \text{ is finite.}$$

There is no reduction restriction at 2. The result includes one rational two-torsion line, full rational two-torsion, and CM curves. The BSD leading-coefficient formula is not part of the conclusion.

[Theorem 1.1 · p. 2](#)

Neither $\text{rank } E(\mathbb{Q}) \leq 1$ nor a finite 2-Selmer dimension can replace the hypothesis. The Kummer exact sequence gives

$$s_2(E) = \text{rank}_{\mathbb{Z}} E(\mathbb{Q}) + \text{corank}_{\mathbb{Z}_2} \text{Sha}(E/\mathbb{Q})[2^\infty].$$

In particular, corank one does not already supply a nontorsion rational point. Corank zero initially gives finiteness of $\text{Sha}[2^\infty]$; finiteness of the whole group follows after determining the analytic rank.

Lemma 2.1; §2 · pp. 4–6

References on the arrows

Unprefixed theorem, lemma, section and equation numbers refer to [A pointwise 2-converse for elliptic curves with rational two-torsion](#). External inputs use the following keys.

- [Kat04](#) Kazuya Kato — p-adic Hodge theory and values of zeta functions of modular forms: Trace to the fixed eigenform lattice, explicit reciprocity, and divisibility after inverting 2. *Astérisque* 295 (2004), pp. 117–290; NUMDAM scan with cover.
- [BT25](#) Ashay A. Burungale; Ye Tian — A rank zero p-converse to a theorem of Gross–Zagier, Kolyvagin and Rubin: Rational main conjecture for CM newforms at every prime; not an integral version. [arXiv:2506.03465v1](#), 4 June 2025 (numbering cited by the manuscript).
- [CST14](#) Li Cai; Jie Shu; Ye Tian — Explicit Gross–Zagier and Waldspurger formulae: Height formula and conductor-factor comparison under split Heegner conditions. *Algebra & Number Theory* 8(10) (2014), pp. 2523–2572; publisher PDF with cover.
- [Sk20](#) Christopher Skinner — A converse to a theorem of Gross, Zagier, and Kolyvagin: The forward Gross–Zagier–Kolyvagin statement recorded in the introduction; not its converse theorem. *Annals of Mathematics* 191(2) (2020), pp. 329–354; published version.

Each citation gives the result and pages. When printed pagination differs from the PDF position, both are shown. GitHub previews do not automatically jump to the cited page.

2. Theorem 1.1 — Proof overview of the main theorem

Proof target : [Theorem 1.1](#) · p. 2

Proof route. The even-sign coefficient system first proves the corank-zero case and a uniform central-value estimate. That estimate then normalizes the odd-sign Heegner-point detector, allowing interpolation over a fixed imaginary quadratic field. In the diagram, $a(E)$ denotes analytic rank and $r(E)$ denotes Mordell–Weil rank.



The even construction branches to the odd normalization; the analytic-rank conclusions then merge into full Sha finiteness

[Open figure ↗](#) [TeX source ↓](#)

1. The even construction has two outputs

Arrange quadratic twists as $h_x = h_0 \prod_q (q^*)^{\lambda_q(x)}$ for $x \in \mathbb{F}_2^b$, with linear forms λ_q . Here $q^* = (-1/q)q$, the new primes avoid a fixed finite support, and all vertices have the same sign and fixed local squareclasses. Binary tests at minimum normalized coefficient depth, together with finite prime networks, provide nonvanishing and a uniform valuation upper bound at every $x \neq 0$. Theorem 3.2 returns them to the base. Proposition 9.7 handles $h_0 = 1$ with $s_2(E) = 0$; Proposition 9.6 supplies a uniform estimate for twists having an appropriate partition certificate, needed later on the odd side.

Propositions 9.6–9.7 · p. 78

2. The order of the odd-side companion choices matters

The fixed h_* defines the Heegner-point detector P_h . The varying $k'(h)$, with uniformly bounded prime count, is used only to prove a divisibility lower bound for P_h . Afterwards, a separate k is fixed once and for all for the final interpolation over $K = \mathbb{Q}(\sqrt{k})$. Treating h_* , $k'(h)$, and k as interchangeable auxiliary twists would use the estimate needed for odd normalization circularly. See the sections on [Proposition 9.10](#) and [Proposition 9.14](#).

[Proposition 9.10](#) · pp. 80–81

3. Rank equality and finiteness of the entire Shafarevich–Tate group

The two interpolation arguments first give $a(E) = s_2(E) \in \{0, 1\}$. The established Gross–Zagier–Kolyvagin forward implication then yields $r(E) = a(E)$ and finiteness of the **whole** group $\text{Sha}(E/\mathbb{Q})$. The forward statement recorded in Skinner’s introduction adds no reduction restriction here. The semistability and other conditions in that paper’s converse theorem are not hypotheses of this forward step.

[Sk20, §1, Gross–Zagier–Kolyvagin implication, print p. 330 / PDF p. 2]

[Proof of Theorem 1.1](#); [Remark 9.15](#) · pp. 87–88

3. Theorem 3.2 — Recovering the central value by cyclotomic interpolation

Proof target : [Theorem 3.2](#) · p. 7

Theorem 3.2 — Transfer to the missing vertex

Fix E , the local squareclasses at $2N$, and the real sign. Let h be a product of distinct signed good odd primes q^* , and put

$$t_q = \dim_{\mathbb{F}_2} E[2]^{\text{Fr}_q}, \quad w(h) = \frac{1}{2} \sum_{q|h} t_q, \quad L^*(h) = \frac{\sqrt{|h|} L(E^{(h)}, 1)}{\Omega_E^{\text{sgn}(h)}}.$$

Write $s(h) = \text{length}_{\mathbb{Z}_2} \text{Sha}(E^{(h)}/\mathbb{Q})[2^\infty]$ when finite, distinguishing this length from s_2 .

Normalize $v(2) = 1$, and set $D(h) = v(L^*(h)) - 2w(h) - s(h)$ when the value is nonzero.

Suppose an allowed h_0 satisfies $s_2(E^{(h_0)}) = 0$. Assume that for arbitrarily large b there are families of the above form, using distinct $q \nmid 2Nh_0$ and linear forms λ_q , all vertices retaining the fixed local classes and sign, such that a family-independent B satisfies

$$L(E^{(h_x)}, 1) \neq 0, \quad D(h_x) \leq B \quad (x \neq 0).$$

Then $L(E^{(h_0)}, 1) \neq 0$ and $D(h_0) \leq B + C_E$. The constant C_E is independent of h_0 , the prime set, and b . The required dimension threshold may depend on the precision being tested.

Theorem 3.2 · p. 7

1 Fixed-lattice Kato classes and rational divisibility

$$u_x \in \Lambda[1/2], \quad 2^{C_{\text{int}}} u \in \mathcal{O}[G]$$

For CM constituents, use the rational main conjecture

Combine characterwise rationality with uniform integrality
[Lemmas 3.3–3.4 · pp. 7–8](#)

2 Recover integrality in the group basis

$$\mathcal{O} \cap \Lambda[1/2] = \Lambda \implies 2^{C_{\text{int}}} u \in \Lambda[G]$$

Apply binary congruences to the integral constant coefficient
[§3.6 · p. 16](#)

3 A nonzero vertex matches finitely many base digits

$$b > 2^M - 1 \implies v(u_x(0) - u_0(0)) \geq M - C_{\text{int}}$$

$$x \neq 0, \quad v(u_x(0)) \leq B + C_{\text{loc}}$$

Fix $M - C_{\text{int}} > B + C_{\text{loc}}$ and obtain a contradiction
[Theorem 3.2 · p. 7](#)

4 Base nonvanishing and valuation bound

$$L(E^{(h_0)}, 1) \neq 0, \quad D(h_0) \leq B + C_E$$

Kato classes in a fixed lattice produce an integral family; binary congruences recover the base central value

[Open figure ↗](#) [TeX source ↓](#)

1. Separate rational divisibility from uniform integrality

Put $\Lambda = \mathbb{Z}_2[[t]]$, $\mathcal{O} = \widehat{\Lambda_{(2)}}$, and $G = (\mathbb{Z}/2)^b$. The manuscript writes the wedge of the real-place class and a Kato class as a scalar u in the determinant of the positive global complex. Tracing into the lattice of one fixed weight-two eigenform constructs $2^{C_{\text{int}}} u \in \mathcal{O}[G]$ with an exponent independent of the number of auxiliary primes. This does not uniformly identify the integral lattices of varying twisted eigenforms.

Kato's Theorem 12.5(3) supplies height-one divisibility after inverting 2; Burungale–Tian's Theorem 2.6 supplies the CM case. Including corrections at the fixed bad primes gives $u_x \in \Lambda[1/2]$ for every character constituent. Kato's stronger integral statement 12.5(4), which requires $p \neq 2$ and an image condition, is not used. Finally Lemma 3.3 applies $\mathcal{O} \cap \Lambda[1/2] = \Lambda$ to each group-basis coefficient, with no additional $|G|$ loss, to obtain

$$2^{C_{\text{int}}}u \in \Lambda[G].$$

Central evaluation is performed on $\Lambda[1/2]$ first; there is no evaluation at $t = 0$ on the whole completed localization $\mathcal{O}$.

[Kat04, §§8.9–8.12, print pp. 185–186 / PDF pp. 70–71]

[Kat04, Theorem 12.5(3)–(4), print p. 222 / PDF p. 107]

[BT25, Theorem 2.6; Remark 2.7, p. 5]

§§3.3–3.5; Proposition 3.7 · pp. 10–15

2. A sufficiently large cube has another vertex with the base's finite digits

At a corank-zero constituent, Proposition 3.7 identifies the vanishing of $u_x(0)$ with that of $L^*(h_x)$ and gives $|v(u_x(0)) - D(h_x)| \leq C_{\text{loc}}$. The nonzero vertices have corank zero by the known analytic-rank-zero theorem; the base has it by hypothesis. Fix $M - C_{\text{int}} > B + C_{\text{loc}}$ and apply Lemma 3.4 to the constant coefficient of $2^{C_{\text{int}}}u$. For $b > 2^M - 1$, some $x \neq 0$ satisfies

$$v(u_x(0) - u_0(0)) \geq M - C_{\text{int}}.$$

If $u_0(0) = 0$, or if its valuation exceeds the upper bound, this contradicts $v(u_x(0)) \leq B + C_{\text{loc}}$. Thus the base is nonvanishing too. Uniformity concerns $C_{\text{int}}, C_{\text{loc}}, B$, not the prime sizes or the precision needed to realize a family.

Lemmas 3.3–3.4 · pp. 7–8

§3.6 · p. 16

3. Supplying the upper bound at all nonzero vertices

Proposition 7.1 compares central values with squares of weight- $3/2$ coefficients; Theorem 3.1 supplies the lower bound that fixes their minimum normalized depth. A unit test gives $L^*(h) \neq 0$ and $v(L^*(h)) \leq 2w(h) + C$. The finite networks of Proposition 7.9 and Theorem 8.3 turn differences in quadratic-residue edge bits into contractions of prime labels and make the test equal to one at every nonzero address. Subtracting $s(h_x) \geq 0$ gives the required upper bound for $D(h_x)$. No prescribed curve is discarded into a density-zero exceptional set.

Proposition 7.1 · pp. 53–54; Lemma 7.5 · pp. 60–61

Theorem 8.3 · pp. 68–69

4. Proposition 9.10 — A uniform lower bound for odd normalization

Proof target : Proposition 9.10 · pp. 80–81

Proposition 9.10 — Two-divisibility of the Heegner-point detector

Fix the prepared positive odd-sign filter of Lemma 9.8. It includes the finite coefficient and class-group support; a negative genus partner h_* with $L(E^{(h_*)}, 1) \neq 0$ has been fixed and its prime divisors excluded. Let P_h denote the conductor-one genus-character Heegner sum over $\mathbb{Q}(\sqrt{hh_*})$, and let $j(P_h)$ be its 2-adic index in the corresponding free rank-one lattice. There is a constant C , independent of h and its prime count, such that, for every analytically rank-one h in this filter,

$$2j(P_h) \geq 2w(h) + s(h) - C.$$

In particular, $j(P_h) \geq w(h) - C'$ uniformly.

Proposition 9.10 · pp. 80–81

1 A bounded-factor companion for a known simple zero

$$a(E^{(h)}) = 1, \quad \omega(k'(h)) \leq A, \quad L(E^{(hk')}, 1) \neq 0$$

$$v(L^*(hk')) \leq 2w(hk') + s(hk') + C$$

The companion is square at $2Nh$ with bounded prime count
[Corollary 4.1 · p. 17](#)

2 Lower-bound the ring-class index

$$2J_h(k') \geq 4w(h) + s(h) + s(hk') - C$$

Cancel the derivative and regulator in two height formulas
[Lemma 9.9 · p. 80](#)

[\[CST14, Theorem 1.1 and Heegner hypotheses, print pp. 2524–2525 / PDF pp. 3–4\]](#)

3 Compare with the fixed-genus-partner detector

$$2J_h(k') - 2j(P_h) = v(L^*(hk')) + O(1)$$

Insert the even estimate and cancel $s(hk')$
[Proposition 9.10 · pp. 80–81](#)
[Proposition 7.4; Lemma 7.5 · pp. 59–61](#)

4 Prove the lower bound before fixing odd minimum depth

$$2j(P_h) \geq 2w(h) + s(h) - C', \quad w(k') \leq A$$

$$\text{Unit test: } a(E^{(h)}) = 1, \quad j(P_h) \leq w(h) + C$$

A varying companion with bounded prime count compares two indices and yields the lower bound for the odd detector

[Open figure ↗](#) [TeX source ↓](#)

1. A varying companion supplies an already nonvanishing central value

For each h already known to have analytic rank one, Lemma 9.8 chooses a negative odd fundamental discriminant $k' = k'(h)$. It satisfies $(k', 2Nh) = 1$, is a square at all places dividing $2Nh$, has $\omega(k') \leq A$, and defines neither an extra-unit field nor the CM field of E . Bounded-factor completion in Proposition 6.2 and finite label preparations control this prime count. Apply Proposition 9.6 to the nonvanishing parameter hk' to obtain

$$v(L^*(hk')) \leq 2w(hk') + s(hk') + C.$$

The actual prime sizes may depend on h . No odd minimum-depth normalization has been used at this point.

[Lemma 9.8 · pp. 79–80; Proposition 6.2 · p. 48](#)

2. Height comparison cancels the additional Sha term

Write $J_h(k')$ for the index of the conductor- $|h|$ ring-class sum over $\mathbb{Q}(\sqrt{k'})$. Corollary 4.1 and Lemma 9.9 give

$$\begin{aligned} 2J_h(k') &\geq 4w(h) + s(h) + s(hk') - C, \\ 2J_h(k') - 2j(P_h) &= v(L^*(hk')) + O(1). \end{aligned}$$

The second identity applies Cai–Shu–Tian’s Theorem 1.1 to the two sums. The level primes split and the conductor is coprime to the level. The original formula’s $c\sqrt{|D|}$ factor differs precisely between conductor $|h|$ and conductor one. Cancelling the derivative and common rank-one regulator leaves the variable factor already included in the normalization of $L^*(hk')$. Excluding extra-unit fields fixes the unit factor as well.

Combine the three inequalities using $w(hk') = w(h) + w(k')$ and $w(k') \leq A$:

$$2j(P_h) \geq 2w(h) + s(h) - 2w(k') - C \geq 2w(h) + s(h) - C'.$$

Only now apply Lemma 7.5. An odd unit simultaneously detects analytic rank one and the upper bound $j(P_h) \leq w(h) + C$.

Corollary 4.1 · p. 17

Lemma 9.9 · p. 80

[CST14, Theorem 1.1 and Heegner hypotheses, print pp. 2524–2525 / PDF pp. 3–4]

Proposition 7.4; Lemma 7.5 · pp. 59–61

5. Proposition 9.14 — Returning from a fixed imaginary quadratic field to corank one

Proof target : Proposition 9.14 · pp. 85–87

Proposition 9.14 — The odd original base

Let $E/\mathbb{Q}$ satisfy $E(\mathbb{Q})[2] \neq 0$ and $s_2(E) = 1$. Then $a(E) = 1$. Again the Selmer group uses Kummer local conditions everywhere; neither Mordell–Weil rank one nor finiteness of Sha at the base is assumed.

Proposition 9.14 · pp. 85–87

1 Fix the final companion once

$$L(E^{(k)}, 1) \neq 0, \quad K = \mathbb{Q}(\sqrt{k}), \quad s_2(E/K) = 1$$

Turn separate nonzero polynomials into simultaneous units
[Theorem 8.3 · pp. 68–69](#)

2 Make both tests one at every nonzero vertex

$$a(E^{(h_x)}) = 1, \quad a(E^{(h_x k)}) = 0 \quad (x \neq 0)$$

All new primes split in K ; $h_0 = 1$

Use both unit bounds in the height comparison
[Lemma 9.9 · p. 80](#)
[Proposition 9.14 · pp. 85–87](#)

3 Bound the index over the fixed field

$$2J_{h_x}(k) - 4w(h_x) - s(h_x) - s(h_x k) \leq C$$

The bound is independent of cube dimension and new support

Transfer using full Selmer corank one and a bounded clearing factor
[Theorem 4.2 · p. 17](#)
[Propositions 5.14–5.15; Lemmas 5.16–5.17; proof of Theorem 4.2 · pp. 45–47](#)

4 Recover the derivative at the missing base

$$\text{ord}_{s=1}(L(E, s)L(E^{(k)}, s)) = 1 \implies a(E) = 1$$

Two simultaneous unit tests over fixed K provide the ring-class upper bound and return a simple zero to the base

[Open figure ↗](#) [TeX source ↓](#)

1. Fix the final companion before the cube dimension

If the prepared odd detector detects the base, the argument is finished. Otherwise take its nonempty minimum seed. A separate even test selects a negative discriminant k with $L(E^{(k)}, 1) \neq 0$. It is a square at $2N$, avoids the old support and required torsion ramification, and excludes the exceptional imaginary fields. Keep $K = \mathbb{Q}(\sqrt{k})$ fixed thereafter. Require every new prime in h to split in K . The forward theorem gives $s_2(E^{(k)}) = 0$, so the quadratic corank identity yields

$$s_2(E/K) = s_2(E) + s_2(E^{(k)}) = 1.$$

This is not an integral direct-sum decomposition of Selmer groups.

Lemma 2.2 · p. 5

2. Make separately nonzero polynomials units at the same vertex

The even test reads hk , while the odd test reads h . Separate nonzero terminal polynomials at an address need not admit the same nonzero assignment of residue symbols. Theorem 8.3 adds primary prime networks and makes both tests equal to one on the same finite graph. No new prime is active at $x = 0$.

When the residual fields are quadratic, the two sides of a rational 2-isogeny supply good simple primes and donors. Full rational two-torsion needs a separate argument: Lemma 9.12 ensures a nonempty witness for the even test restricted to K -split primes, and Lemma 9.13 corrects the oriented total. These are substantive steps beyond generic prime selection.

After choosing b and the networks, select an actual stage of the odd coefficients realizing the required test tables and precision on that finite weight range. The moving detecting prime ℓ and the precision may change; the minimum normalized depth, fixed k , and valuation bound do not. A single stage for all cube dimensions is unnecessary.

Theorem 8.3 · pp. 68–69

Lemmas 9.12–9.13 · pp. 82–85

§§9.5–9.7 · pp. 81–87

3. Feed the index upper bound into ring-class interpolation

At every nonzero vertex, $a(E^{(h)}) = 1$ and $a(E^{(hk)}) = 0$. The two unit bounds and the height comparison for fixed k give

$$2J_h(k) \leq 4w(h) + C.$$

The finite lengths $s(h), s(hk)$ are nonnegative, so $2J_h(k) - 4w(h) - s(h) - s(hk) \leq C$. These are the inputs of Theorem 4.2: for a fixed nonexceptional K satisfying the split Heegner condition at $2N$, full Selmer corank one at the base, and arbitrarily large cubes whose nonzero vertices have a simple product zero and this uniform upper bound, the base product $L(E, s)L(E^{(k)}, s)$ has a simple zero.

The interpolation uses complexes retaining full Kummer conditions and actual maps to Galois cochains to produce an integral family with a bounded clearing factor, $f_x u_x = d_x$. Proposition 5.14 uniformly controls the valuation of $f_0(0) \neq 0$ and the negative Laurent degrees at finite precision. Lemma 5.17 matches finitely many coefficient digits with the base. A vanishing base derivative would give $u_0(0) = 0$, contradicting the known valuation bound at a nonzero vertex. As the manuscript emphasizes, general Selmer duality or the Gross–Zagier formula alone does not supply this simultaneous integral family.

Finally $L(E^{(k)}, 1) \neq 0$ gives $a(E) = 1$. The passage to finiteness of all of Sha is the last step of the main theorem.

Theorem 4.2 · p. 17

Propositions 5.14–5.15; Lemmas 5.16–5.17; proof of Theorem 4.2 · pp. 45–47

6. External inputs and their scope

Source

Kato's fixed-lattice trace, explicit reciprocity, rational divisibility

Used at

§§3.3–3.5

Content and applicability

Weight two, $r = r' = 1$; trace from auxiliary level to the fixed eigenform. Distinguish rational 12.5(3) from integral 12.5(4)

Checked here

Statements in §§8.9–8.12, Theorems 9.7 and 12.5(3)–(4), and the manuscript's use. Uniform integrality for varying support is an additional construction in this manuscript

Source

Burungale–Tian

Used at

§3.4

Content and applicability

The main conjecture over $\Lambda \otimes \mathbb{Q}$ for CM newforms, at every prime including 2

Checked here

Theorem 2.6 and Remark 2.7; no integral version is quoted from them

Source

Cai-Shu-Tian

Used at

Lemma 9.9 and the proof of Theorem 4.2

Content and applicability

Primitive ring-class character, $(c, N) = 1$, split level primes, and $\pi(\infty) = 0$; index comparison and vanishing of the base derivative

Checked here

Formula and assumptions of Theorem 1.1. Not an independent verification of every local comparison

Source

Gross-Zagier-Kolyvagin, in Skinner's combined formulation

Used at

Lemma 2.1 and the final main-theorem step

Content and applicability

Analytic rank zero or one implies rank equality and finiteness of all of Sha

Checked here

Forward statement and its use; proofs not recursively verified

[Kat04, Theorem 9.7, print p. 189 / PDF p. 74]

[BT25, Theorem 2.6; Remark 2.7, p. 5]

[CST14, Theorem 1.1 and Heegner hypotheses, print pp. 2524–2525 / PDF pp. 3–4]

[Sk20, §1, Gross-Zagier-Kolyvagin implication, print p. 330 / PDF p. 2]

The manuscript mentions the broader Goldfeld's analytic density conjecture and the 2-converse for elliptic curves as background, explicitly stating that its converse is not an input. No direct dependency from another paper in catalogue 004 was identified in the principal routes and bibliography examined here. This does not mean that all potential relationships have been investigated.

7. Return to the sources

- Theorem 1.1 · p. 2 — Read the full Selmer hypothesis and the conclusion for all of Sha
- §§3.3–3.5; Proposition 3.7 · pp. 10–15 — Separate rational divisibility from uniform integrality
- §3.6 · p. 16 — See how finite-digit congruences force base nonvanishing
- Propositions 5.14–5.15; Lemmas 5.16–5.17; proof of Theorem 4.2 · pp. 45–47 — Follow the simultaneous arithmetic construction and bounded clearing factor
- Lemma 9.8 · pp. 79–80; Proposition 6.2 · p. 48 — Check the uniform prime-count bound versus variable prime sizes
- Lemma 9.9 · p. 80 — Compare the conductor-one and conductor- $|h|$ sums
- §§9.5–9.7 · pp. 81–87 — Follow normalization, the fixed- K choice and simultaneous tests
- Proof of Theorem 1.1; Remark 9.15 · pp. 87–88 — Pass from both analytic-rank cases to rank equality and full finiteness

For the October 7, 2026 version, the reading covered the main statement; the interpolation route in §§2–3; the interfaces and final transfer in §§4–5; the normalization hypotheses in §7; the address-lemma statement and forest construction in §8; and the assembly in §9. Valuation conventions, the three companions, the order of fixed and varying choices, CM and full rational two-torsion, and the scope of final finiteness were compared with the source.

Outstanding work includes an independent construction of all cochain limits, simultaneous evaluation maps and determinant switches in §§4–5; all uniform moment and sieve estimates in §6; the complete theta weights and local trace identities in §7; and every network coefficient calculation in §8. For Ferrero–Washington’s residual cyclotomic input, Monsky’s parity theorem, Nekovář’s duality, and the Waldspurger and related coefficient inputs, the manuscript’s citations and roles were examined, but the relevant external source passages were not rechecked here. This account therefore does not certify the correctness of the full proof including these connections.