Arithmetic dependencies of the construction with 29 variables

8 November 2026

Abstract

We identify the arithmetic results used by the finite-algebra construction with 29 total variables. Its four stated arithmetic inputs follow from the specified elliptic-group, height and pole theorems in the source manuscript and Sun's simultaneous prime-pattern theorem. In particular, the required avoidance at seven, compatibility with an arbitrary fixed congruence progression, and realization with zero preparation parameters require no stronger global existence assertion. The deductions are given explicitly. The deep arithmetic theorems themselves remain cited inputs.

1 The statements being used

Fix

$$K = \mathbb{Q}(\sqrt{2}), \quad D = 11 - 6\sqrt{2}, \quad E : y^2 = x^3 - Dx, \qquad P = \left(\frac{57 - 28\sqrt{2}}{8}, \frac{-660 + 417\sqrt{2}}{32} \right).$$

Heights are absolute logarithmic Weil heights, and rational valuations are normalized by $v_p(p) = 1$. We count the distinguished rational input as one of the variables of a polynomial.

The source manuscript used here is Version 9 of [1], at commit

`14e8f601fe0d9173d4a5f084aedc3e07066a7688`.

The relevant file is `manuscripts/quartic_v9.tex`. Sun's theorem is Theorem 4.1 of the explicitly versioned preprint [3], arXiv:2610.20691v2. File hashes and theorem identifiers are recorded in the accompanying source certificate. These pins fix the statements whose implications are proved below. For the underlying restricted-converse argument we incorporate the Version 11 correction [2]: the Kato classes are defined on the full index set needed by the 1999 theorem, and their norms are identified with the retained cyclotomic class. This correction changes the proof supporting an inherited input, not the statement of the input used here.

1. The elliptic source gives $2E(K) = \mathbb{Z}P$ and $h(x([n]P)) \geq n^2 - 6$ for $n \neq 0$. The relevant source identifiers are `subsec:v5-point-source` and `eq:o8-indexheight`.

2. Put
$$B_* = \prod_{p \leq 76176} p, \qquad H_{19} = 2^{110} 210^{1800} B_*^{19} + 128.$$
For $t = u/v$ in lowest terms, $v > 0$, and $t \notin \{0, 1, 2401, -343/32\}$, let $M_5(t)$ be the product of primes $p > 76176$ for which at least one of
$$v_p(v), \quad v_p(u), \quad v_p(u - v), \quad v_p(u - 2401v), \quad v_p(32u + 343v)$$
is positive and odd. The source theorem `thm:quartic-height19` gives $h(t) \leq H_{19} M_5(t)^{19}$.

3. The pole results are the source obstruction, simultaneous realization and zero-preparation lemmas, respectively:

   `hyp:o8-pole`,
   `lem:original-seven-simultaneous-realization`,
   `v5:preparation-zero-bridge`.

   The last of these has exactly the zero-preparation conclusion used in Section 3.

4. The prime-pattern result is Sun's Theorem 4.1, whose implications for the prescribed congruences and the elliptic reduction orders are proved in Section 2. The same quantified statement appears as `thm:v5-simultaneous-primes` in the source manuscript.

The first two entries involve the identical normalized point and the identical height constant. The exact integer calculation

$$2^{2093447} < H_{19} < 2^{2093448}$$

is a sharper evaluation of this fixed constant; it does not strengthen the source height inequality. Likewise the implication with exponent 24 follows from the exponent-19 result because $M_5(t) \geq 1$.

2 Finite avoidance and the common congruence progression

For a Gaussian integer π, set

$$d_-(\pi) = N_{\mathbb{Q}(i)/\mathbb{Q}}(\pi - 1), \qquad d_+(\pi) = N_{\mathbb{Q}(i)/\mathbb{Q}}(\pi + 1).$$

Sun's theorem permits any fixed finite list of distinct integral coefficients, any fixed divisibility of the square-denominator parameter, and any fixed lower bounds for the prime values and for the slope. Its avoidance modulus is odd, squarefree, and prime to seven. The fixed Gaussian residues are 9 modulo 16 and $1 + 3i$ modulo seven; at every prime dividing the avoidance modulus the residue is i. The theorem excludes every odd common divisor between the two order norms at the same position and between any two order norms at distinct positions.

Lemma 2.1. *Let $L \geq 1$ be divisible by 64, and fix distinct integers $c_1, \ldots, c_k$, with $k \geq 2$. Prescribe $q \geq 1$ and real numbers $Y, H_0 > 0$. Sun's Theorem 4.1 supplies positive integers u, w such that*

$$q \mid w, \qquad u/w^2 > H_0, \qquad p_j = u + c_j w^2 > Y$$

are primes, with Gaussian generators whose order norms satisfy

$$v_2(d_-(\pi_j)) = 6, \qquad v_2(d_+(\pi_j)) = 2,$$
$$\gcd(d_-(\pi_j), d_+(\pi_h)) = 4 \qquad (1 \leq j, h \leq k),$$

and are all prime to the odd part of L. The primes may simultaneously be required to satisfy $p_j \equiv 1 \pmod{8 \cdot 3 \cdot 17}$.

Proof. Take the avoidance modulus to be the product of the odd primes dividing $3 \cdot 17 \cdot L$, with seven omitted. It is squarefree and prime to seven, as required by Sun's theorem. At each of its prime factors, the two adjacent norms of i are both two. They are therefore units. At seven the fixed residue $1 + 3i$ instead gives

$$d_-(1 + 3i) = 9 \equiv 2 \pmod 7, \qquad d_+(1 + 3i) = 13 \equiv 6 \pmod 7.$$

Thus seven is avoided even when it divides L.

Write $\pi = 9 + 16a + 16bi$. Direct calculation gives

$$d_+(\pi) \equiv 4 \pmod 8, \qquad d_-(\pi) \equiv 64 \pmod{128}.$$

The exact powers of two in the statement follow. The exclusion of odd common factors supplied by Sun's theorem then gives every stated cross-sign gcd, including a position paired with itself. Finally the Gaussian norm is one modulo eight, and its residues at three and seventeen are the norm of i, namely one. These are precisely the required congruences on p_j. □

Corollary 2.2. *In the situation of Lemma 2.1, put*

$$U = \operatorname{lcm}_j(d_-(\pi_j)/4), \qquad V = \operatorname{lcm}_j(d_+(\pi_j)/4).$$

Then

$$\gcd(U, V) = 1, \qquad \gcd(U, L) = 16, \qquad \gcd(V, L) = 1.$$

For every integer h_* divisible by 64, the congruences

$$h \equiv 0 \pmod U, \qquad h \equiv 1 \pmod V, \qquad h \equiv h_* \pmod L$$

have an arithmetic progression of solutions.

Proof. Division by four makes every minus order have two-adic valuation four and every plus order odd. The cross-sign gcds make their least common multiples coprime. Lemma 2.1 excludes all odd factors of L from both least common multiples. The displayed gcds follow. The only nontrivial pairwise compatibility condition is $h_* \equiv 0 \pmod{16}$, which holds. The generalized Chinese remainder theorem now supplies the progression. □

The reduction orders at the two places of K above p_j are the unordered pair $d_-(\pi_j), d_+(\pi_j)$, by the source lemma `lem:v5-two-reductions`. Both reductions have full rational two-torsion. For a finite group of elliptic-curve points of order d, full two-torsion implies that the subgroup of doubles has order $d/4$. Every double is therefore killed by $d/4$. This justifies the divisions by four in Corollary 2.2; the source point P is itself a double.

Lemma 2.3. *The preceding statements also apply to any fixed finite list of rational contact coefficients, with a common square denominator for the slope and with arbitrarily deep fixed denominator divisibility.*

Proof. For coefficients $\gamma_j \in \mathbb{Q}$, choose a positive integer D_0 so that $D_0^2\gamma_j$ are integers, and remove repeated coefficients. Apply Lemma 2.1 with $c_j = D_0^2\gamma_j$ and put $v = D_0^2 w^2$. Then $u + c_j w^2 = u + \gamma_j v$ and $u/v > D_0^{-2} H_0$. Enlarge the prescribed lower bound before applying the lemma to obtain any desired slope bound. By choosing q divisible by suitable powers of a fixed finite set of primes, one obtains any prescribed lower bounds on their valuations in v. Enlarge Y to exclude any fixed finite list of primes. None of these choices changes the quantified form of Sun's theorem. □

Lemma 2.4. *Let G be the closure of a cyclic subgroup generated by a point Q in a compact real Lie group, and let G^0 be its identity component. Suppose L is divisible by the order of G/G^0. Any arithmetic progression $h \equiv h_* \pmod L$, with an additional compatible finite collection of congruences, is dense after multiplication by Q in the component $h_*Q + G^0$. Arbitrarily large positive indices can be used.*

Proof. The compatible congruences give one coset modulo an integer L' divisible by L. A compact connected abelian Lie group is a torus, and multiplication by any nonzero integer is onto it. It follows that $[L']G = G^0$. Thus the two-sided progression has the stated closure. In a compact group, the closure of a positive cyclic orbit is also a group: positive return times approach the identity and consequently approximate the negative multiples. Removing a finite initial segment does not change the closure. This proves the positive-index assertion. □

For the construction, apply this lemma to the closure of (P, P^σ) in the product of the two real elliptic groups. The scalar point, the four integer root labels, the real compact neighborhoods, all contact coefficients, and the modulus L are fixed before the prime-pattern theorem is used. Corollary 2.2 then supplies the final shared index without disturbing those neighborhoods. No estimate uniform in the coefficients, q, L, or the number of contact positions is required.

3 Pole realization with zero preparation

For $b \in \mathbb{Q}^\times$, put $B = 17b$. The zero-preparation predicate is

$$\begin{aligned} p^2 &= B(1-e)(1+3e), \\ h_0 &= e(B-b^2), \\ Bq^2 &= (s^2 - Bh_0)(s^2 + 3Bh_0), \end{aligned}$$

with rational e, p, q, s; h_0 is the displayed expression. No nonzero condition is imposed on these four witnesses.

The source lemma `v5:preparation-zero-bridge` states exactly the following two implications. A solution excludes negative odd valuations of b outside $\{2, 3, 17\}$. Conversely a solution exists if the reduced denominator of b is a square and

$$\begin{aligned} &0 < b < 17, \qquad b \in \mathbb{Q}_2^{\times 2} \cap \mathbb{Q}_3^{\times 2} \cap \mathbb{Q}_{17}^{\times 2}, \\ &v_2(b) \geq 3, \qquad v_3(b) \geq 1, \qquad v_{17}(b) \geq 2. \end{aligned}$$

These are precisely the hypotheses verified for each of the four normalized pole inputs in the finite-algebra construction.

The special role of zero preparation can also be checked directly in the source argument. With preparation parameter zero, the auxiliary quantity there is

$$B(B - b^2) = B^2(1 - b/17).$$

It is positive and is a square in the three specified completions, by the displayed bounds. If μ, θ are the positive squarefree representatives of B and this quantity, their supports are disjoint, $\mu \equiv 17 \pmod{24}$, $\theta \equiv 1 \pmod{24}$, and each is a local square at primes dividing the other. To see the last condition, an odd prime in the support of μ has positive odd valuation on b, so $1 - b/17$ is a square unit; a prime in the support of θ outside $2, 3, 17$ must have $v_p(b) = 0$ and $b \equiv 17 \pmod{p}$, making $B \equiv 17^2 \pmod{p}$. The conditions at $2, 3, 17$ were already imposed. The source simultaneous-realization lemma therefore applies without an additional hypothesis. Its deep restricted-converse and rank dependencies are retained in this use.

Lemma 3.1. *For $B \in \mathbb{Q}^\times$, the first conic is covered by the two formulas*

$$e = \frac{\tau^2 + (4\varepsilon - 1)B}{\tau^2 + 3B}, \qquad p = \frac{-4B\tau(1-\varepsilon)}{\tau^2 + 3B}, \qquad \varepsilon \in \{0, 1\}, \quad \tau^2 + 3B \neq 0.$$

Thus its parametrization imposes no additional restriction on the pole-realization theorem.

Proof. Substitution verifies the conic equation. If $e \neq 1$, take $\varepsilon = 0$ and $\tau = p/(e-1)$. The conic equation gives $\tau^2 + 3B = 4B/(1-e) \neq 0$ and recovers the displayed point. If $e = 1$, then $p = 0$, and $\varepsilon = 1, \tau = 0$ works. The case $e = -1/3, p = 0$ is included in the first chart. □

The two structural coordinates attached to different pole inputs are independent. Once all four inputs satisfy the source hypotheses, choose each rational certificate separately and use Lemma 3.1. Zero second-square roots are included by the explicit finite support split in the finite-algebra construction. No common structural witness for distinct pole inputs is asserted or needed.

4 The resulting implication

Theorem 4.1. *Assume the cited elliptic-group, index-height, contact-height and pole-realization theorems of the pinned source manuscript, and Sun's Theorem 4.1. Then the four arithmetic inputs of the construction with 29 variables hold. Consequently its proved rational-source argument and finite-algebra compilation give a polynomial P such that*

$$t \in \mathbb{Z} \quad \Longleftrightarrow \quad \exists \mathbf{y} \in \mathbb{Q}^{28} : P(t, \mathbf{y}) = 0.$$

No additional global arithmetic existence theorem is required.

Proof. The normalized group and index height are identical to those in the source. The contact-height constant is the same integer, evaluated exactly. Section 3 identifies the needed pole theorem and checks its parametrization and independent simultaneous use. Section 2 supplies the prescribed prime choices, all fixed odd avoidance, the exact congruence compatibility and the unchanged real closure. These are all four arithmetic inputs.

The remaining steps are proved within the finite-algebra construction: the odd-product height identity, the two-parameter point charts, the scalar input normalization, the elementary Lucas growth estimate, the fixed-prime scalar size condition, and the one-coordinate elimination of the finite roots and nonzero guards. Their soundness and completeness therefore apply with precisely the arithmetic inputs just verified. □

The fixed-prime scalar normalization only adds its prime and the finitely many denominator primes to the fixed avoidance set. The preceding argument permits precisely this enlargement before Sun's theorem is applied. It therefore does not alter the arithmetic dependency list.

The theorem is an implication from explicitly identified mathematical results. It does not replace proofs of those deep source results by finite computation, and it does not claim an independent verification of the restricted converse, contact-height theorem, or analytic prime-pattern theorem. The computational certificates verify the literal formulas, source bindings, and finite numerical deductions.

References

[1] E. Glazer and contributors, *Diophantine definition of the integers in the rationals*, Version 9, 7 November 2026, source commit `14e8f601fe0d9173d4a5f084aedc3e07066a7688`. https://github.com/elliotglazer/diophantine-z-q/tree/14e8f601fe0d9173d4a5f084aedc3e07066a7688.

[2] E. Glazer and contributors, *Diophantine definition of the integers in the rationals*, Version 11, Kato index-set and norm-identification correction, source commit `650b298a2a18fa956f8859f3ca80e9d7c8cedd82`. https://github.com/elliotglazer/diophantine-z-q/tree/650b298a2a18fa956f8859f3ca80e9d7c8cedd82/docs/manuscript-revisions/version11.

[3] Z.-W. Sun, *86 unknowns for Hilbert's tenth problem over the rationals*, arXiv:2610.20691v2, 19 October 2026, especially Theorem 4.1. https://arxiv.org/abs/2610.20691v2.