A split genus-three lift curve in a moving square-sum construction

Yicheng Pan
independent researcher

Draft of 15 July 2026

Abstract

We study a moving square-sum construction arising from the factor-difference problem of Erdős and Rosenfeld. On every fixed nondegenerate fiber, the simultaneous first-lift conditions form a genus-three hyperelliptic curve with a Klein four-group of involutions. We give all three elliptic quotients and prove, by their invariant differentials, that the Jacobian is isogenous over $\mathbb{Q}$ to their product. On two rational fibers exact 2-descent gives factor ranks $(5,3,4)$ and $(5,5,6)$, hence Jacobian ranks 12 and 16. Magma independently confirms both u-quotient rank computations. Good-prime sieves and exact reconstruction exclude nondegenerate second lifts in four explicit finite Mordell–Weil coefficient boxes, including 32,482,404 representations on a rank-three factor. Modular-polynomial certificates rule out cyclic isogenies of every degree at most 10 between any two quotient families at a rational parameter. We also identify a superficially attractive rank-five specialization as the boundary fiber $p = 0$, where two shifts coincide. On the exceptional nondegenerate fiber $m = -13364$, the complete lift is a genus-nine $(\mathbb{Z}/2\mathbb{Z})^3$-cover whose Jacobian splits into nine elliptic curves of total rank 29; a good-prime sieve excludes new points in a 16,016,004-representation coefficient box. A conservative two-cover descent on its rank-five genus-two quotient reduces every rational point to four elliptic square classes of rational ranks $0, 0, 1, 1$; the two rank-zero classes are determined globally, while a forty-prime multiplier sieve leaves only the known points for $|n| \le 10^6$ in the two rank-one classes. The splitting mechanisms are classical, and all search statements are finite and relative to displayed finite-index subgroups. The work neither determines all rational points nor solves Erdős Problem 885 for $k = 5$.

1 Factor differences and the moving construction

For a positive integer N, put

$$D(N) = \{|d - e| : N = de,\ d, e \in \mathbb{Z}_{>0}\}.$$

Erdős and Rosenfeld asked whether, for every $k \ge 1$, there are $N_1 < \cdots < N_k$ for which $\bigcap_i D(N_i)$ has at least k elements [1]. They proved the case $k = 2$; Jiménez-Urroz proved $k = 3$ [2], and Bremner proved $k = 4$ [3]. The case $k = 5$ remains open in the current public record [4].

The elementary equivalence

$$d \in D(N) \quad \Longleftrightarrow \quad d^2 + 4N \text{ is a square}$$

turns the problem into a rectangular square-sum question. A public set of research notes attached to Problem 885 develops a moving deformation from the four-shift packet

$$(0, 79200, 227205, 1258560)$$

and the square abscissae $18, 234, 346, 514$ [5]. We take only the exact equations from that construction as our starting point.

Set $r = 1258560$. The deformation base is

$$\Delta^2 = (m - 1532)(m - 524)(m + 596)(m + 1460), \tag{1}$$

and define

$$p = \frac{m^2 - 1277104 - \Delta}{8}, \qquad q = \frac{m^2 - 1277104 + \Delta}{8}. \tag{2}$$

For a proposed new square abscissa u, the first discriminant condition is

$$W^2 = (u^2 + p)(u^2 + q). \tag{3}$$

The induced second abscissa is

$$v = \frac{9(m + 13364)u + 18W}{u^2 - 324}, \tag{4}$$

with the sign of W accounting for the two quadratic roots. To lift both abscissae through the final shift r, one additionally needs

$$S^2 = u^2 + r, \qquad T^2 = v^2 + r. \tag{5}$$

Equations (1)–(5) are the complete system studied below. A useful point must also avoid the built-in values

$$u^2, v^2 \in \{18^2, 234^2, 514^2\}, \qquad u^2 = v^2. \tag{6}$$

2 The first elliptic quotient

Fix a rational point (m, Δ) of (1). Write

$$a = p + q - 2r, \qquad c = (p - r)(q - r).$$

Proposition 1. *The simultaneous first-lift equations* (3) *and* $S^2 = u^2 + r$ *have the elliptic quotient*

$$E_m : \quad y^2 = (x + a)(x^2 - 4c). \tag{7}$$

More precisely, after eliminating $u^2 = S^2 - r$*, one obtains*

$$W^2 = S^4 + aS^2 + c,$$

and a birational map to (7) *is*

$$x = 2(W + S^2), \qquad y = 2S(x + a). \tag{8}$$

Away from the poles, its inverse is

$$S = \frac{y}{2(x + a)}, \qquad W = \frac{x}{2} - S^2. \tag{9}$$

A point of $E_m(\mathbb{Q})$ *lifts to the original first-lift curve precisely when* $S^2 - r$ *is a rational square.*

Proof. Substitution gives

$$(u^2+p)(u^2+q) = (S^2+p-r)(S^2+q-r) = S^4 + aS^2 + c.$$

For (8), direct expansion gives

$$y^2 - (x+a)(x^2-4c) = 4(x+a)\big(W^2 - S^4 - aS^2 - c\big),$$

so the quartic equation implies (7). Equations (9) follow immediately, and the last assertion is exactly $u^2 = S^2 - r$. □

The quotient is useful because its Mordell–Weil group can be computed before imposing the final square-coordinate condition. It does not reduce the full problem to an elliptic curve: adjoining $u = \sqrt{S^2 - r}$ is a nontrivial double cover.

3 The genus-three curve and its three quotients

Put $t = S - u$. Then

$$S = \frac{t + r/t}{2}, \qquad u = \frac{r/t - t}{2}, \qquad H = 4t^2 W,$$

and the complete simultaneous first-lift curve is birational to

$$C_{p,q,r}: \quad H^2 = \big(t^4 + (4p-2r)t^2 + r^2\big)\big(t^4 + (4q-2r)t^2 + r^2\big). \tag{10}$$

When $0, p, q, r$ are pairwise distinct, the polynomial on the right is squarefree: the discriminant of the first quartic is proportional to $p(p-r)$, similarly for q, and a common root would force $p = q$. Thus the smooth projective model has genus 3.

Theorem 2. *The curve* (10) *has commuting involutions*

$$\sigma(t, H) = (-t, H), \qquad \tau(t, H) = \left(\frac{r}{t}, \frac{r^2 H}{t^4}\right).$$

Its three nontrivial quotients by $\langle \sigma, \tau \rangle$ are elliptic. Writing $z = H/t^2$, two quotient models are

$$E_S: \quad z^2 = (x^2 + 4(p-r))(x^2 + 4(q-r)), \qquad x = t + r/t, \tag{11}$$

$$E_u: \quad z^2 = (x^2 + 4p)(x^2 + 4q), \qquad x = t - r/t. \tag{12}$$

For the third, put

$$B_p = 4p - 2r, \quad B_q = 4q - 2r, \quad D = B_p + B_q, \quad C = B_p B_q + 2r^2, \quad R = r^2.$$

The quotient by σ is

$$H^2 = (v^2 + B_p v + r^2)(v^2 + B_q v + r^2), \qquad v = t^2,$$

and its Weierstrass model is

$$E_t: \quad Y^2 = X^3 + CX^2 + (RD^2 - 4R^2)X + 2R^2(D^2 - 2C). \tag{13}$$

Moreover,

$$\mathrm{Jac}(C_{p,q,r}) \sim_{\mathbb{Q}} E_S \times E_u \times E_t.$$

Proof. Direct substitution gives the three displayed quotient equations. The point $(v, H) = (0, r^2)$ on the third quartic gives (13) by the standard quartic-to-cubic transformation; an exact map is recorded in the companion verifier. A basis of regular differentials on (10) is

$$\frac{dt}{H}, \qquad \frac{t\,dt}{H}, \qquad \frac{t^2\,dt}{H}.$$

Pullbacks of invariant differentials from E_t, E_S, E_u are respectively

$$\frac{2t\,dt}{H}, \qquad \frac{(t^2 - r)\,dt}{H}, \qquad \frac{(t^2 + r)\,dt}{H}.$$

Their coefficient determinant is $4r \neq 0$. Hence the induced homomorphism from the product of the quotient Jacobians has full tangent rank and finite kernel, proving the isogeny. This is also an instance of the classical Kani–Rosen decomposition [6]. □

4 Two nondegenerate fibers

The following fibers arose in an exact base-fiber search. In both cases the four shifts $0, p, q, r$ are pairwise distinct.

Verified computation 3. *For*

$$m_1 = -\frac{1028}{13}, \qquad \Delta_1 = \frac{140743680}{169},$$

one has

$$\{p_1, q_1\} = \left\{-\frac{44439684}{169}, -54756\right\}.$$

The global minimal model of (7) *is*

$$E_1 = [1, -1, 1, -74412615957377, 247067329653364918929]. \tag{14}$$

It has conductor 6268174242540210*, root number* -1*, torsion subgroup* $\mathbb{Z}/4\mathbb{Z}$*, and rank exactly* 5*.*

For

$$m_2 = -\frac{1929164}{559}, \qquad \Delta_2 = \frac{3315921100800}{312481},$$

one has

$$\{p_2, q_2\} = \left\{\frac{4942236}{1849}, \frac{448791516}{169}\right\}.$$

The global minimal model is

$$E_2 = [1, -1, 1, 167142427759082074063, 768755042626092730768753649 61]. \tag{15}$$

It has conductor 49226569982055237300599070*, root number* -1*, torsion subgroup* $\mathbb{Z}/2\mathbb{Z}$*, and rank exactly* 5*.*

The remaining factors in Theorem 2 have the following exact arithmetic. Here the first row in each fiber is the previously displayed E_S.

fiber	factor	conductor	torsion	rank
m_1	E_S	6268174242540210	$\mathbb{Z}/4\mathbb{Z}$	5
	E_u	5671725769710	$\mathbb{Z}/4\mathbb{Z}$	3
	E_t	10144069441183440716343390	$\mathbb{Z}/2\mathbb{Z}$	4
m_2	E_S	49226569982055237300599070	$\mathbb{Z}/2\mathbb{Z}$	5
	E_u	3045060743429815110	$\mathbb{Z}/2\mathbb{Z}$	5
	E_t	88882060445029369326512453236897410	$\mathbb{Z}/2\mathbb{Z}$	6

Thus the two genus-three Jacobians have exact ranks 12 and 16. In particular, neither satisfies the classical Chabauty inequality $\operatorname{rank}\operatorname{Jac}(C)(\mathbb{Q}) < 3$.

Here $[a_1, a_2, a_3, a_4, a_6]$ denotes a generalized Weierstrass model. The five independent points used for E_1 are

$$(-9878563, 4264922106), \quad (5025167, 166396356),$$
$$(-51040553/9, 595716826036/27), \quad (5451479, 1846313172),$$
$$(44084323/9, 8415841612/27),$$

and those used for E_2 are

$$(6479648831, 1196639270739084),$$
$$(13393919831, 2172180680400084),$$
$$(16906815581, 2781245374569834),$$
$$(39886495031, 8378543287353684),$$
$$(1376953199/4, 2933426615291547/8).$$

Verification of Computation 3. PARI/GP 2.17.4 returns $[5, 5, 0, L]$ from `ellrank` for each minimal model, where L is the corresponding displayed list. Thus the unconditional lower and upper rank bounds coincide. The regulators are approximately 739.5059338532833 and 4670.311999119634 respectively. Applying `ellsaturation` at every prime below 1000 changes neither list nor regulator. Hence the generated subgroups have finite index with no prime divisor below 1000; no index-one claim is made.

For E_1, the official University of Sydney Magma V2.29-8 calculator independently returns `RankBounds(E) = 5 5` and torsion $\mathbb{Z}/4\mathbb{Z}$. The corresponding public calculation for E_2 exceeded the service's practical 60-second window, so there is no second-software upper-bound claim for E_2.

The torsion statements also have elementary exact certificates. A point of order four is displayed for E_1, while good reductions at $19, 23, 41$ have orders $24, 32, 44$, whose gcd is 4. For E_2, good reductions at $23, 29$ have orders $32, 36$, bounding rational torsion by 4. The 2-division polynomial has exactly one rational root, and neither rational root of the associated halving polynomial has a rational ordinate. Hence its torsion is exactly $\mathbb{Z}/2\mathbb{Z}$.

For the four additional factors, PARI/GP returns rank intervals $[3, 3], [4, 4], [5, 5], [6, 6]$ in the order shown in the table. Each displayed point list in the companion certificate is unchanged by saturation at every prime below 1000. Magma independently returns rank bounds $3, 3$ and $5, 5$ for the two E_u factors. Both E_t rank calculations exceeded the public calculator's practical 60-second window, so no Magma rank claim is made for them; their torsion groups were independently returned as $\mathbb{Z}/2\mathbb{Z}$ and also have elementary reduction-and-halving certificates. □

5 A finite Mordell–Weil coefficient sieve

Let $P_1, \dots, P_5$ denote the points displayed above, and let T run over the full rational torsion subgroup. We tested every representation

$$n_1P_1 + \cdots + n_5P_5 + T, \qquad |n_i| \le 8. \tag{16}$$

At a good prime, a point is rejected only when the inverse (9) is defined and $S^2 - r$ is a quadratic nonresidue. Points reducing to a pole or a zero denominator are retained. Consequently the modular filters cannot discard a rational point that satisfies the square condition.

The prime list was

$$193, 317, 139, 179, 503, 547, 599, 383, 347, 101, 331, 163, 673, 929, 809, 307,$$
$$557, 827, 859, 691, 617, 263, 277, 739, 563, 223, 523, 919, 367, 349, 577, 727,$$
$$653, 811, 659, 233, 461.$$

The prime 599 is omitted for E_1 because it is not a good usable reduction for this certificate.

Verified computation 4. *For E_1, the box* (16) *contains*

$$4 \cdot 17^5 = 5,679,428$$

coefficient–torsion representations. The 36 *good-prime filters leave* 16 *survivors. Exact rational reconstruction shows that* 14 *satisfy $S^2 - r \in \mathbb{Q}^2$; their* 12 *second lifts through* (4)–(5) *all satisfy the degeneracy condition* (6)*.*

For E_2, the box contains

$$2 \cdot 17^5 = 2,839,714$$

representations. The 37 *filters leave* 18 *survivors. Exactly* 16 *satisfy the rational square-coordinate condition, and all* 16 *resulting second lifts are degenerate. Thus neither box contains a nondegenerate candidate.*

The ordered survivor lists have SHA-256 values

`446e215b70204dcebbc426db2c683f8a07fd7103cfd3111ca7ebbdea4ddf96cb`,
`2b6b1594fb70f8024dfdb9b7e433a70ec311c3bb64fb34a78025064c8638fc81`.

A JavaScript implementation performs the finite-field group operations and produces these lists. A separate Python implementation uses exact rational group arithmetic to reconstruct every survivor, verify the eliminated quadratic, test both signs in (4), and classify the final lifts.

The second quotient (12) supplies an independent search coordinate system. Its Weierstrass model and inverse are

$$y^2 = (x + p + q)(x^2 - 4pq), \qquad u = \frac{y}{2(x + p + q)}, \qquad W = \frac{x}{2} - u^2.$$

Thus the modular square test is now $u^2 + r \in \mathbb{Q}^2$.

Verified computation 5. *For m_1, the factor E_u has rank* 3*. The box*

$$n_1P_1 + n_2P_2 + n_3P_3 + T, \qquad |n_i| \le 100,$$

contains

$$4 \cdot 201^3 = 32,482,404$$

coefficient–torsion representations. The 37 *good-prime filters leave* 16 *survivors. Exact reconstruction leaves* 14 *square-coordinate points; their possible final lifts yield only two built-in square pairs and no candidate. The survivor-list digest is*

`1940fae29b1b3e739449bc058faecba53e5229e1983f084a5597291a24febbdd`.

For m_2*, the rank-five* E_u *coefficient-eight box contains* 2,839,714 *representations. It leaves* 18 *modular survivors, of which* 16 *reconstruct exactly; all* 16 *second lifts are degenerate. Its digest is*

`3f33e03b683983364a1490304e1576e53c73f1bf315b74bd9e62f172b1da6e69`.

These are different finite-index subgroups and coefficient coordinates from Computation 4. Their representation counts therefore must not be interpreted as counts of distinct rational points.

6 The rank-five boundary fiber

The parameter

$$m_0 = -\frac{22484038}{3341}$$

looks attractive because the constant term of the fixed-fiber discriminant vanishes, reducing another auxiliary curve to an elliptic curve of rank 5. It is important, however, that

$$\Delta_0 = \frac{491276571071220}{11162281}, \qquad \{p_0, q_0\} = \left\{0, \frac{122819142767805}{11162281}\right\}.$$

Changing the sign of Δ_0 only exchanges p_0 and q_0. Hence two of the nominal shifts $0, p_0, q_0, r$ coincide. This auxiliary rank-five curve is a boundary degeneration and cannot itself yield a nondegenerate four-shift packet. We record this explicitly because a rank computation alone obscures the loss of distinctness.

7 An exceptional genus-nine full cover

The integral parameter $m = -13364$ behaves differently for a useful reason: the mixed term in (4) vanishes. Choosing

$$\Delta = -177321984$$

gives

$$p = 44330172, \qquad q = -324.$$

Thus $0, q, r, p$ are pairwise distinct, and this is a nondegenerate base fiber. Equation (4) becomes

$$v = \frac{18W}{u^2 - 324}.$$

Put

$$L = r + 324 = 1258884 = 1122^2, \qquad K_0 = 324(p - r) - rL = -1570425844752,$$

and

$$b = \frac{K_0}{L} = -\frac{43622940132}{34969}, \qquad c = p - r = 43071612.$$

Eliminating u, W, v from the two final square conditions gives

$$T^2(S^2 - L) = LS^2 + K_0.$$

Consequently, with $Z = T(S^2 - L)/1122$, one obtains the elliptic quartic

$$Z^2 = (S^2 - L)(S^2 + b). \tag{17}$$

Its cubic model

$$y^2 = (x - L + b)(x^2 + 4Lb), \qquad S = \frac{y}{2(x - L + b)}, \quad Z = \frac{x}{2} - S^2,$$

has exact rank 2 and torsion $\mathbb{Z}/4\mathbb{Z}$.

A genuine complete lift is a rational point on the multiquadratic cover

$$\begin{aligned} U^2 &= S^2 - r, \\ Z^2 &= (S^2 - L)(S^2 + b), \\ W^2 &= (S^2 - L)(S^2 + c). \end{aligned} \tag{18}$$

Proposition 6. *The smooth projective model X of* (18) *has genus* 9. *Over $\mathbb{Q}$, its Jacobian is isogenous to a product of nine elliptic curves. In the character order*

$$Z, W, ZW, UZ^+, UZ^-, UW^+, UW^-, UZW^+, UZW^-,$$

their Mordell–Weil ranks are

$$2, 3, 5, 3, 5, 1, 4, 4, 2,$$

and hence $\operatorname{rank} \mathrm{Jac}(X)(\mathbb{Q}) = 29$.

Proof. The three squareclasses in (18) are independent in $\mathbb{Q}(S)^*/\mathbb{Q}(S)^{*2}$. The degree-eight cover has eight branch points, above the four distinct values $S^2 = r, L, -b, -c$, all with inertia two. Riemann–Hurwitz gives

$$2g(X) - 2 = 8(-2) + 8 \cdot 4 = 16.$$

The seven nontrivial character quotients have squarefree right-hand sides with degrees and genera

$$(2, 4, 4, 4, 6, 6, 6), \qquad (0, 1, 1, 1, 2, 2, 2),$$

respectively. The character idempotents give the corresponding Jacobian decomposition.

Each of the three genus-two factors has the form

$$C_{A,B,C} : Y^2 = (S^2 - A)(S^2 - B)(S^2 - C),$$

for

$$(A, B, C) = (r, L, -b), (r, L, -c), (r, -b, -c).$$

The involutions $(S, Y) \mapsto (-S, Y)$ and $(S, Y) \mapsto (-S, -Y)$ give the elliptic quotients

$$y^2 = (x - A)(x - B)(x - C), \qquad z^2 = x(x - A)(x - B)(x - C).$$

Their pulled-back invariant differentials span $S\,dS/Y$ and dS/Y, so each genus-two Jacobian is isogenous to the product of these two elliptic curves. This yields nine elliptic factors in total. Exact 2-descent in PARI/GP returns the displayed equal lower and upper rank bounds. All returned point lists are unchanged by saturation at primes below 1000; the unified certificate prints every minimal model, conductor, torsion group, and point list. An independent symbolic verifier checks all quotient maps and the trace decomposition at fifteen good-prime instances. □

Verified computation 7. *On the rank-two factor* (17)*, every representation*

$$n_1P_1 + n_2P_2 + T, \qquad |n_1|, |n_2| \le 1000, \quad T \in E(\mathbb{Q})_{\mathrm{tors}},$$

was tested. The box contains 16,016,004 *representations. Sixty good-prime filters, retaining all reductions at map poles, leave twelve: four poles and eight representations of the built-in pairs* $(234, 514)$ *and* $(514, 234)$ *with signs. Exact rational reconstruction gives no nondegenerate point in the box.*

This calculation is not a global point determination. In particular the rank total 29 exceeds the genus, so classical Chabauty is unavailable. The rank-one factor UW^+ is a potentially useful projection because the image of a rational point has square x-coordinate; an effective covering or Mordell–Weil sieve would still require a global height bound.

The rank-five genus-two quotient

$$C_{UW} : Y^2 = (S^2 - 1258560)(S^2 - 1258884)(S^2 + 43071612) \tag{19}$$

admits a sharper covering reduction. Write

$$g(S) = (S^2 - 1258560)(S^2 - 1258884), \qquad h(S) = S^2 + 43071612.$$

Proposition 8. *Every point of* $C_{UW}(\mathbb{Q})$ *lifts, over* $K = \mathbb{Q}(\sqrt{-10767903})$*, to one of the four elliptic quartics*

$$E_\gamma : z^2 = \gamma g(S),$$

where

$$\gamma \in \{1, 9619625497086, 275265700983302798538, 589110732\}.$$

Only $E_\gamma(\mathbb{Q})$ *is relevant to such a lift, and the four rational ranks are respectively* $0, 0, 1, 1$*. The first two classes contribute only the two points at infinity and the points with* $S = \pm 1122$*, respectively.*

Proof. A fake two-Selmer calculation with all good primes through the genus-two Weil cutoff 1153 and bad-prime cutoff 1000 leaves 59 classes. Omitting bad primes can only enlarge this set. Taking the norm associated to the quartic factor g collapses those 59 representatives to the four displayed square classes, so every rational point is covered.

All four γ are positive, and $h(S) > 0$ on the real line. Hence a real point of (19) has $g(S) \ge 0$. If $z \in K$ and $z^2 = \gamma g(S) \in \mathbb{Q}_{\ge 0}$, then $z \in \mathbb{Q}$: writing $z = a + b\sqrt{-10767903}$, rationality of z^2 gives $ab = 0$, and the purely quadratic alternative has nonpositive square. Thus the quadratic-twist summands cannot lift from the real curve.

Exact descent gives rational ranks $0, 0, 1, 1$. The first torsion group is $\mathbb{Z}/4\mathbb{Z}$, with finite S-images ± 1122 and two points above infinity; $h(1122)$ is not a square, so only the two infinity points lift. The second torsion group is $\mathbb{Z}/2\mathbb{Z}$, again with images ± 1122, and

$$\frac{h(1122)}{9619625497086} = \left(\frac{112}{52173}\right)^2.$$

This proves the last assertion. □

Verified computation 9. *For* $\gamma = 275265700983302798538$*, Magma proves that* $E_\gamma(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$*; a free generator has* $S = -1146$*, and its torsion translate has* $S = 1146$*. For* $\gamma = 589110732$*, the known point with* $S = 1234$ *is saturated at every prime below* 1000*. An* 8*-isogeny from its minimal model to*

$$[1, 0, 1, -3378747234189, -1098105753406983989]$$

sends this point to one of canonical height less than 46.071*. The torsion-adjusted Siksek bound on the target is less than* 8.673*. Thus any remaining prime divisor* $p \geq 1009$ *of the index would produce an affine rational point of multiplicative x-height at most* 5844*; exact enumeration of that box is empty. Hence this point is primitive and the fourth group is also* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$*. In both torsion cosets of both rank-one classes, an exact check through* $|n| \leq 50$ *and a forty-prime Mordell–Weil multiplier sieve through* $|n| \leq 10^6$ *leave only* $n = \pm 1$*. Exact reconstruction gives only*

$$S = \pm 1146, \qquad S = \pm 1234,$$

with remaining square roots 1028/2560067433 *and* 52/189*, respectively.*

The multiplier sieve in Computation 9 is finite. The index argument is global, but the sieve supplies no global height bound for the square-coordinate pullback on either rank-one group. The bad prime 2029, omitted by the original cutoff, removes no cover; a direct public-service calculation at the remaining bad prime 3694181 exceeded its memory limit. Thus the 59-cover set is still described conservatively.

7.1 A finite binary-form reduction of the rank-one pullbacks

The two unresolved constants have squarefree kernels

$$27526570098330279853 8 = 42 \cdot 2560067433^2, \qquad 589110732 = 4123 \cdot 378^2.$$

Put $d = 42$ or 4123, and take $(s_0, t_0) = (1146, 1028)$ or $(1234, 104)$ respectively. The conic $S^2 + 43071612 = dT^2$ is parametrized by

$$S = \frac{A}{B}, \qquad A = 2dt_0mn - s_0(n^2 + dm^2), \qquad B = n^2 - dm^2.$$

Indeed, if $U = t_0(n^2 + dm^2) - 2s_0mn$, then

$$A^2 + 43071612B^2 = dU^2.$$

For primitive (m, n), the other square condition is

$$d(A^2 - 1258560B^2)(A^2 - 1258884B^2) \in \mathbb{Q}^2.$$

Verified computation 10. *For* $d = 42$*, exact factorization gives*

$$A^2 - 1258560B^2 = 36Q_2, \qquad A^2 - 1258884B^2 = 2016Q_0Q_1,$$

where

$$Q_0 = 12m^2 - 1028mn + 27n^2, \qquad Q_1 = 3969m^2 - 3598mn + n^2,$$

and

$$Q_2 = 2683044m^4 - 230905248m^3n + 213130708m^2n^2 - 5497744mn^3 + 1521n^4.$$

Thus $3Q_0Q_1Q_2$ *is a square. For* $d = 4123$*, one obtains*

$$Q_0 = 196m^2 - 364mn + n^2, \qquad Q_1 = 346921m^2 - 30628mn + 4n^2,$$

$$\begin{aligned} Q_2 = {} & 1122775471321m^4 - 2181600219344m^3n + 189596262198m^2n^2 \\ & - 529129328mn^3 + 66049n^4, \end{aligned}$$

and the condition is $Q_0Q_1Q_2 \in \mathbb{Q}^2$*.*

The pairwise resultants restrict common prime divisors to

$$\{2,3,7,11,17,29,61,2029\} \quad \textit{and} \quad \{3,7,11,17,19,29,31,61,2029\},$$

respectively. Hence the three individual squareclasses lie in finite explicit sets. A conservative local sieve, treating every residue cell not stabilized by the chosen precision as a wildcard and omitting the large prime 2029*, leaves at most the eight classes*

$$\kappa \in \{1,-5423,-3111,58377,-22319,1000297,69434409,-10767903\}.$$

For $d = 4123$ *the surviving triples are* $(\kappa,\kappa,1)$*; for* $d = 42$ *they are* $(\mathrm{sf}(3\kappa),\kappa,1)$*, where* sf *is the signed squarefree representative. In particular,* Q_2 *is a square in every surviving system.*

Both quartics $y^2 = Q_2(x,1)$ have the rational point $x = 0$. Exact PARI/GP two-descent proves that their elliptic Jacobians have rank one and torsion $(\mathbb{Z}/2\mathbb{Z})^2$; models are

$$[0,213130708,0,1269441618120816,158711955585544670400]$$

and

$$[0,189596262198,0,1154052025237722197916,57246404751217115284615747 5560].$$

Consequently the missing global step is reduced to one quadratic-squareclass condition on each of two explicit rank-one elliptic groups, with eight target classes in each case. Computation 10 is a finite reduction, not a determination of the rational points on those residual pullbacks.

8 Relation to known genus-three methods

The general decomposition of a Jacobian by commuting involutions is classical [6]; explicit elliptic quotients of genus-three hyperelliptic curves with extra involutions have also been studied systematically [7]. We therefore do not claim Theorem 2 as a new general splitting theorem. Its role here is to expose the complete arithmetic structure of the first-lift curve in this particular moving square-sum construction.

Hernandez recently determined rational points on members of a reciprocal genus-three family whose Jacobian has the form $E_a^2 \times E'$ up to isogeny [8]. Two independent maps to the same rank-one factor permit a Dem'yanenko–Manin height argument. The present two fibers instead have three pairwise non-isogenous factors: their ranks differ, except for the two rank-five factors of the second fiber, whose conductors differ. Thus that argument does not directly apply.

There is also a family-level obstruction to identifying the two most natural factors. Using

$$p+q = \frac{m^2-1277104}{4}, \qquad pq = 2164968m + 14569656624,$$

equality of the j-invariants of E_u and E_S factors into the four degenerate base roots, $m^2 - 6311344$, and a monic degree-twelve polynomial having no root modulo 7. The remaining values $m = \pm 2512$ do not give a rational point on the base quartic. Hence these two quotient curves are not geometrically isomorphic on any rational nondegenerate base fiber. This does not rule out higher-degree isogenies on other special fibers.

The same rational-function calculation gives a stronger low-degree obstruction.

Proposition 11. *At every rational parameter for which E_u, E_S, E_t are elliptic, no two of these curves are connected over $\overline{\mathbb{Q}}$ by a cyclic isogeny of degree N for any $2 \le N \le 10$.*

Proof. Let $\Phi_N(X, Y)$ be the classical modular polynomial, and let $F_{ij,N}(m)$ be the primitive integral numerator of $\Phi_N(j_i(m), j_j(m))$ for $ij = uS, ut, St$. Exact substitution gives the following pairs (deg $F_{ij,N}$, no-root prime):

N	uS	ut	St
2	$(51, 641)$	$(51, 37)$	$(49, 17)$
3	$(75, 17)$	$(74, 89)$	$(73, 17)$
4	$(113, 181)$	$(112, 823)$	$(110, 457)$
5	$(123, 269)$	$(122, 73)$	$(121, 17)$
6	$(225, 17)$	$(225, 37)$	$(220, 17)$
7	$(171, 17)$	$(170, 53)$	$(169, 17)$
8	$(246, 53)$	$(245, 1171)$	$(242, 2297)$
9	$(247, 17)$	$(246, 73)$	$(243, 17)$
10	$(369, 29)$	$(367, 73)$	$(363, 17)$

In each entry the leading coefficient is nonzero modulo the displayed prime, while exhaustive evaluation in that prime field gives no root. If a/b in lowest terms were a rational root, the rational-root theorem would give b dividing the leading coefficient. Thus b would be invertible modulo the witness prime and a/b would reduce to a root, a contradiction. The modular-polynomial criterion proves the claim. The coefficient tables are from Sutherland's archive [11]; their hashes and every residue check are recorded in independent exact verifiers. □

9 Reproducibility and limitations

The companion archive contains:

- `analyze_nondegenerate_quotients.gp`, which reproduces the minimal models, conductors, rank bounds, points, torsion, and saturation;
- `search_nondegenerate_quotients.py`, for direct exact group arithmetic and reconstruction;
- `sieve_nondegenerate_quotients.mjs`, for the good-prime sieve;
- an independent Python verifier for the symbolic map, models, points, and torsion;
- an independent Python checker for every modular survivor; and
- a PARI/GP certificate and an independent Python verifier for the complete split, six rank computations, and exact model checks;
- the two u-quotient sieves and their independent exact survivor checkers; and
- independent prime- and composite-level modular-polynomial verifiers for Proposition 11; and
- a unified PARI/GP certificate and independent symbolic/finite-field verifier for Proposition 6, together with the exact rank-two sieve for Computation 7; and

- the Magma two-cover, rational-rank, torsion, saturation, isogeny, and Siksek-bound certificates for Proposition 8, together with the PARI/GP and exact Python index certificates and the independent exact and modular verifiers for Computation 9; and
- the Magma inputs and records separating successful rank cross-checks, torsion-only checks, and public-service timeouts.

The conclusions are deliberately limited. The coefficient bounds in (16) do not impose a height bound on the resulting rational coordinates, but they cover only finite boxes in finite-index subgroups. The points are proved saturated only at primes below 1000. Points in larger coefficient boxes, possible large-index cosets, other base fibers, and other constructions remain untreated. Even a nondegenerate point of the present moving system would give only an intermediate rectangular square-sum packet; additional rows would still be required for Erdős Problem 885 at $k = 5$. The Jacobian ranks 12 and 16 exceed the genus, and the three factors on each displayed fiber are pairwise non-isogenous, so neither classical Chabauty nor the repeated-factor Dem'yanenko–Manin argument cited above gives an immediate global point determination. The exceptional full cover has rank 29 and genus 9, so its complete elliptic splitting likewise does not by itself supply a Chabauty inequality. Proposition 8 globally resolves only two of four covering square classes; the multiplier bound in Computation 9 is not a rational-point height bound. The full Mordell–Weil groups of the two remaining rank-one classes are known, but multipliers outside the finite sieve remain untreated.

Computer algebra and AI-assisted exploration were used in discovery and search design. The stated algebraic identities reduce to the displayed formulas, and the finite claims have independent exact verifiers. Novelty is provisional pending specialist review and a fuller bibliographic search.

References

[1] P. Erdős and M. Rosenfeld, *The factor-difference set of integers*, Acta Arith. 79 (1997), 353–359.

[2] J. Jiménez-Urroz, *A note on a conjecture of Erdős and Rosenfeld*, J. Number Theory 78 (1999), 140–143.

[3] A. Bremner, *On a problem of Erdős related to common factor differences*, Int. J. Number Theory 15 (2019), 1059–1068, https://doi.org/10.1142/S1793042119500581.

[4] T. F. Bloom, *Erdős Problem 885*, https://www.erdosproblems.com/885, accessed 14 July 2026.

[5] S. Mausberg, *Notes on Erdős Problem 885* and accompanying formalized findings, public repository snapshot of 19 April 2026, https://github.com/SamMausberg/lean-formalizations.

[6] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. 284 (1989), 307–328, https://eudml.org/doc/164555.

[7] P. Borowka and A. Shatsila, *Hyperelliptic genus 3 curves with involutions and a Prym map*, arXiv:2308.07038 (2023), https://arxiv.org/abs/2308.07038.

[8] R. Hernandez, *Rational points on a family of genus 3 hyperelliptic curves*, J. Number Theory 286 (2026), https://doi.org/10.1016/j.jnt.2026.02.008.

[9] The PARI Group, *PARI/GP version 2.17.4 and elliptic-curve function reference*, https://pari.math.u-bordeaux.fr/dochtml/html/Elliptic_curves.html.

[10] Computational Algebra Group, University of Sydney, *Magma V2.29-8 Calculator and Handbook*, https://magma.maths.usyd.edu.au/calc/.

[11] A. V. Sutherland, *Classical modular polynomials*, online coefficient archive, accessed 15 July 2026.