An explicit 5×4 square-sum specialization and a genus-13 reduction

Yicheng Pan
independent researcher

Draft of 15 July 2026

Abstract

We give an explicit pair of integer sets of cardinalities five and four whose twenty pairwise sums are squares. The example arises from a one-parameter subfamily of Choudhry's rational 5×3 construction. An elliptic-curve addition produces a candidate fourth shift as a rational function of the parameter; the two remaining conditions reduce to the simultaneous rational-square values of two explicit degree-eight polynomials. Their fiber product has genus 13, and their difference admits a useful factorization. The specialization $m = -8/19$ satisfies both conditions. We also give an exact finite certificate that the resulting five-column set has no further integer shift. For rational extensions of the fixed grid, a complete two-square parametrization gives natural genus-three necessary covers. Bounded rational-point searches find only the displayed rows and columns, while all thirty-six natural covers have Jacobian rank above their genus. This is an auxiliary square-sum result and does not solve Erdős Problem 885 for $k = 5$.

1 Introduction

For finite sets $A, B \subset \mathbb{Z}$, call (A, B) a square-sum pair if $a + b$ is a square for every $a \in A$ and $b \in B$. Choudhry [1] constructed multiparameter examples of sizes 3×3, 5×3, and 4×4, and asked for examples of sizes 5×4 and 5×5. Mausberg subsequently posted a 5×4 square packet in connection with Erdős Problem 885 [5]. The present note records a distinct 5×4 specialization and, more importantly, an explicit algebraic reduction that explains how it arises inside Choudhry's family.

The relation with the factor-difference problem is

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

Thus five positive integers with five common factor differences would give a 5×5 square-sum grid; after adjoining the zero row, this is an anchored 6×5 grid. The construction below has only four anchored rows, so it does not settle the $k = 5$ case.

2 A one-parameter subfamily

In Choudhry's 5×3 family, set

$$(f, g, u_1, u_2, v_1, v_2) = (4, 1, 2, 1, 3, 1)$$

and retain $m \in \mathbb{Q}$ as a parameter. The five columns are

$$\begin{aligned} a_1 &= 4(24m^2 + 145m - 4)^2, \\ a_2 &= 100(24m^2 + 49m + 4)^2, \\ a_3 &= 25(97m^2 + 8)^2, \\ a_4 &= 4(24m^2 - 145m - 4)^2, \\ a_5 &= 100(24m^2 - 49m + 4)^2, \end{aligned}$$

and three shifts are

$$\begin{aligned} b_1 &= 0, \\ b_2 &= 96(3m - 4)(3m + 4)(8m - 1)(8m + 1), \\ b_3 &= 3300(m - 1)(m + 1)(6m - 1)(6m + 1). \end{aligned}$$

All fifteen sums $a_i + b_j$ are rational squares.

Put

$$D = 97m^2 - 8m - 8$$

and, for $D \neq 0$, define

$$b_4 = \frac{12(2m-1)(2m+1)(3m-1)(3m+1)}{D^2} \times (35m + 4)(85m - 28)(89m - 20)(109m + 20). \quad (1)$$

The expression (1) was found by elliptic-curve addition on the curve determined by the columns (a_1, a_3, a_5). No sign convention for that group law is needed below: the following proposition is proved by direct identities.

Proposition 1. *For b_4 as in (1), the sums $a_1 + b_4$, $a_3 + b_4$, and $a_5 + b_4$ are rational squares. The remaining two sums are rational squares if and only if $F_2(m)$ and $F_4(m)$ below are rational squares:*

$$\begin{aligned} F_2(m) = {} & 3252420900m^8 - 268152720m^7 - 846520196m^6 \\ & + 226981960m^5 + 70762193m^4 - 37069520m^3 \\ & - 3000736m^2 + 1580800m + 160000, \\ F_4(m) = {} & 3122350884m^8 - 865433712m^7 - 1137811292m^6 \\ & + 310045192m^5 + 136716497m^4 - 33456848m^3 \\ & - 6350752m^2 + 978688m + 135424. \end{aligned}$$

Proof. Direct expansion gives

$$\begin{aligned} a_1 + b_4 &= \left(\frac{2(55878m^4 - 6572m^3 - 10761m^2 + 1128m + 368)}{D}\right)^2, \\ a_3 + b_4 &= \left(\frac{121165m^4 - 14696m^3 - 23010m^2 + 2384m + 800}{D}\right)^2, \\ a_5 + b_4 &= \left(\frac{2(57030m^4 - 12052m^3 - 7095m^2 + 408m + 400)}{D}\right)^2, \end{aligned}$$

and

$$a_2 + b_4 = \frac{4F_2(m)}{D^2}, \qquad a_4 + b_4 = \frac{4F_4(m)}{D^2}.$$

The assertion follows. □

Proposition 1 replaces a five-column search by the simultaneous rational points on the two hyperelliptic curves $y^2 = F_2(m)$ and $z^2 = F_4(m)$.

Proposition 2. *The polynomials F_2 and F_4 are squarefree and coprime, and*

$$F_2 - F_4 = 24(m+4)(4m+1)(9m+4)(16m+1)D^2. \tag{2}$$

The smooth projective normalization of the fiber product

$$y^2 = F_2(m), \qquad z^2 = F_4(m)$$

has genus 13.

Proof. Polynomial gcd calculations give $\gcd(F_i, F_i') = 1$ and $\gcd(F_2, F_4) = 1$; direct expansion gives (2). Each double cover of the m-line is branched at the eight distinct finite roots of its octic, and the two branch loci are disjoint. For the resulting degree-four cover, each of the sixteen branch values has two points of ramification index two. Riemann–Hurwitz therefore gives

$$2g - 2 = 4(-2) + 16 \cdot 2 = 24,$$

so $g = 13$. □

3 The specialization $m = -8/19$

At $m = -8/19$ one has

$$F_2(m) = \left(\frac{35668080}{130321}\right)^2, \qquad F_4(m) = \left(\frac{32892048}{130321}\right)^2,$$

and

$$b_4 = -\frac{15740769200}{1172889}.$$

Clearing denominators and translating the least shift to zero produces

$$A = \{202720644, 827712900, 1476864900, 494706564, 80729856900\},$$
$$B = \{0, 358400700, 1398239500, 17139008700\}.$$

Theorem 1. *Every element of $A + B$ is a square.*

Proof. The square roots, with rows indexed by the displayed order of A and columns by the displayed order of B, are

14238	23688	40012	131688
28770	34440	47180	134040
38430	42840	53620	136440
22242	29208	43508	132792
284130	284760	286580	312840.

Squaring the entries gives the twenty sums exactly. □

4 An exhaustive integer-shift certificate

The displayed grid cannot be extended by a fifth *integer* shift while keeping the same five columns.

Lemma 1. *Let $a < c$ be integers. Every integer b for which both $a + b$ and $c + b$ are squares arises from a factorization*

$$(x - y)(x + y) = c - a,$$

with $x, y \geq 0$, by $b = y^2 - a$.

Proof. Write $a + b = y^2$ and $c + b = x^2$ and subtract. □

For $a = 202720644$ and $c = 494706564$ the difference is

$$291985920 = 2^9\, 3^2\, 5\, 19\, 23\, 29.$$

There are 192 parity-compatible factor pairs with $x - y \leq x + y$. Testing the remaining three columns leaves exactly

$$0, \quad 358400700, \quad 1398239500, \quad 17139008700.$$

This is a finite proof, implemented independently of the parameter search. It does not exclude rational shifts with new denominators or different five-column sets.

The example is not affinely equivalent to the Mausberg packet. Indeed, for ordered shifts $b_0 < b_1 < b_2 < b_3$ put

$$\lambda(B) = \frac{(b_0 - b_2)(b_1 - b_3)}{(b_0 - b_3)(b_1 - b_2)}.$$

Positive scaling and translation preserve this invariant. For the present shift set and the Mausberg shift set, respectively, its values are

$$\frac{541359200}{411195147} \qquad \text{and} \qquad \frac{951142}{921557},$$

which are unequal.

5 Rational extensions of the fixed grid

There is a direct way to search for rational extensions without returning to the parameter m. Let $C_0, C_1 \in \mathbb{Q}$ be distinct, put $d = C_1 - C_0$, and suppose

$$C_0 + t = X^2, \qquad C_1 + t = Y^2.$$

Writing $s = X + Y$ gives the complete parametrization

$$X = \frac{s - d/s}{2}, \qquad Y = \frac{s + d/s}{2}, \qquad t = \left(\frac{s - d/s}{2}\right)^2 - C_0. \tag{3}$$

Choose a known solution $s_0 \neq 0$, write $s = s_0 r$, and put

$$\rho = \frac{d}{s_0^2}, \qquad Q_j(r) = r^4 + \left(\frac{4(C_j - C_0)}{s_0^2} - 2\rho\right) r^2 + \rho^2.$$

Then direct substitution in (3) gives

$$C_j + t = \frac{s_0^2 Q_j(r)}{4r^2}. \tag{4}$$

Consequently, if two further entries $C_a + t$ and $C_b + t$ are squares, then

$$w^2 = Q_a(r)Q_b(r). \tag{5}$$

Because the C_j are distinct, each quartic is squarefree and two different quartics are coprime. Thus (5) is a genus-three hyperelliptic curve. Searching the product may introduce points at which the two factors have the same nonsquare class; testing the individual factors in (4) removes these false positives and cannot remove a genuine extension.

For row extensions take $(C_j) = B$, the known value $t = 202720644$, and $s_0 = 14238 + 23688 = 37926$. For column extensions take $(C_j) = A$, the known value $t = 0$, and $s_0 = 14238 + 28770 = 43008$. Exact rational-point enumeration on the resulting degree-eight models through naive parameter height 10^6 returns respectively 42 and 34 affine points. Exact tests of every individual Q_j leave precisely the five displayed elements of A on the row side and the four displayed elements of B on the column side. These are bounded statements, not complete determinations of the rational points.

The polynomials in (5) are even and reciprocal under $r \mapsto \rho/r$. The two involutions split their Jacobians, up to isogeny, into three elliptic factors by the standard Kani–Rosen mechanism [6]. We exhausted all choices of the two entries used in (3) and the two remaining quartics used in (5): six models for row extension and thirty for column extension. Exact two-descent rank intervals give minimum total Jacobian ranks 13 and 11, respectively. Both exceed the genus, so none of these thirty-six natural models satisfies the classical Chabauty inequality. This explains why the most immediate completeness argument fails; it does not prove that the fixed grid has no rational extension. Independently of the rank program, a second implementation verifies all thirty-six squarefree models, the quotient maps and differential determinant, and the corresponding trace decomposition at three good primes per model.

As an independent bounded check, rank-three elliptic projections were searched in the coefficient cube $[-200, 200]^3$ for row extension and $[-250, 250]^3$ for column extension. The chosen bases were unchanged by saturation at primes below 1000. The cubes contain 64,481,201 and 125,751,501 representations, respectively; a twenty-prime sieve followed by exact rational-square tests found no new compatible value. These coefficient boxes are unrelated to the parameter-height bound above, and none is a global height bound.

6 Computational checks and bounded search

All symbolic identities in Proposition 1 were checked by exact polynomial cancellation. The twenty identities in Theorem 1 were checked by two independent integer programs. Reduced fractions $m = p/q$ with $0 < |p| \le 20000$ and $1 \le q \le 20000$ were enumerated exactly. Homogeneous evaluations of F_2 and F_4 were first sieved modulo eight primes; every survivor was then tested by arbitrary-precision integer square root. Among 486,361,582 values there were nine simultaneous-square hits. Eight of these,

$$\pm\tfrac{1}{2}, \quad \pm\tfrac{1}{3}, \quad -\tfrac{4}{35}, \quad \tfrac{28}{85}, \quad \tfrac{20}{89}, \quad -\tfrac{20}{109},$$

make $b_4 = 0$. The only hit giving a new shift was $m = -8/19$. An independent Python enumeration agrees through height 2000. These are bounded computations, not a global uniqueness theorem.

Search code, identity certificates, and raw parameters are supplied with the companion verification archive. Computer algebra and AI-assisted exploration were used to locate and simplify the identities; every stated theorem reduces to the exact displayed formulas and integer checks.

7 Concluding remarks

The example answers the existence question for another 5×4 square-sum pair but does not address the more difficult 5×5 question, nor the anchored 6×5 configuration needed for Erdős Problem 885 at $k = 5$. The genus-13 curve in Proposition 2, together with the factorization (2), provides a compact starting point for determining whether this subfamily contains further 5×4 examples. For the fixed specialization, Section 5 shows that every natural genus-three extension projection has rank well above its genus. A global determination would therefore require a covering or combined Mordell–Weil sieve, quadratic-Chabauty input, or a different specialization with lower-rank quotients.

References

[1] A. Choudhry, *Two sets of integers such that all elements of the sumset of the two sets are perfect squares*, arXiv:2508.07806 (2025).

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

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

[4] A. Bremner, *On a problem of Erdős related to common factor differences*, Int. J. Number Theory 15 (2019), 1059–1068.

[5] S. Mausberg, comment and verification packet on Erdős Problem 885, 19 April 2026, `https://www.erdosproblems.com/forum/thread/885`.

[6] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. 284 (1989), 307–328.