Erdős Problem 943 on sums of two squarefull numbers

Przemyslaw Chojecki

March 18, 2026

Abstract

Let $\mathcal{A}$ be the set of squarefull positive integers and write

$$r(n) := \#\{(a,b) \in \mathcal{A}^2 : \ a+b=n\},$$

where ordered pairs are counted. Erdős asked whether $r(n) = n^{o(1)}$ for every n.

First, we give a rigorous pointwise bound for the full representation function:

$$r(n) \ll_\varepsilon n^{2/5+\varepsilon}.$$

Second, we study the coprime subcount

$$c(n) := \#\{(a,b) \in \mathcal{A}^2 : \ a+b=n, \ (a,b)=1\}$$

and develop two parallel exact reformulations. The first is kernel/class-group flavoured: it interprets the relevant squarefree kernels through principal forms and records a twisted Rédei system for odd kernels. The second is a dyadic lifted-root programme: it rewrites the coprime problem through the family $n-u^3x^2$, proves a fixed-u bound

$$N_u(n) \ll_\varepsilon n^{\theta+\varepsilon}u^\gamma$$

with $\theta \approx 0.2865$ and $\gamma \approx 0.1442$ coming from Mordell-curve point counts, and obtains dyadic congruence bounds from Chan's theorem on box counts for congruences $a^2b^3 \equiv \ell \pmod q$.

Third, we isolate the exact obstruction in the square-sieve approach. The weighted square sieve, combined with the currently available quadratic large sieve, controls the square-detection problem by a square-pair norm

$$\mathcal{Q}(w) := \sum_{m_1m_2=\square} w(m_1)w(m_2),$$

not merely by $\|w\|_2^2$. In optimistic generic situations this still yields only a square-root saving in the candidate set size, so a purely second-moment strategy cannot settle the coprime model through this route. We therefore formulate a precise *sufficient* first-moment theorem for twisted lifted cube-modulus roots.

Finally, we summarise the most relevant 2025–2026 literature around the problem: Heath-Brown's 2026 improvement for global squarefull solutions of $x+y=z$, Zhao's 2025 published bound, Wongcharoenbhorn–Meemark on squarefull values of quadratic polynomials, Liu's explicit quadratic large sieve, Baier's 2025–2026 work on bilinear sums with modular square roots, the prime-power congruence results of Baier–Bhandari–Haldar, and related work of Grimmelt–Merikoski, Meemark–Wongcharoenbhorn, Destagnol–Sofos, Destagnol–Lyczak–Sofos, and Chan–Koymans–Rome.

A final caution is essential: the coprime model does *not* yet recover the full function $r(n)$, because dividing a squarefull representation by $\gcd(a,b)$ need not preserve squarefullness. Thus the note cleanly separates what is now unconditional for the full Erdős problem, what is currently understood only for a coprime model, and what additional theorem would still be needed to pass from that model to the full statement.

Contents

1 Introduction

A positive integer is *squarefull* if every prime dividing it does so to exponent at least 2. Write $\mathcal{A}$ for the set of squarefull integers. The pointwise problem we have in mind is the one currently listed online as Erdős Problem 943 on Bloom's *Erdős Problems* website [5]; the page states the problem in terms of the additive convolution $1_{\mathcal{A}} * 1_{\mathcal{A}}$.

Problem 1.1 (Erdős). Is it true that

$$r(n) = \#\{(a,b) \in \mathcal{A}^2 : \ a+b=n\} = n^{o(1)}$$

for every $n \geq 1$?

There are three distinct goals for this note:

(i) Record a rigorous unconditional pointwise bound for the *full* representation function $r(n)$.

(ii) Develop the strongest exact reformulations we currently have for a coprime model, and isolate where the square-sieve approach really breaks.

(iii) Summarise the 2025–2026 literature surrounding squarefull values, modular square roots, quadratic large sieves, and related averaging problems, and explain precisely which theorem is still missing.

The first task is completed by the following theorem.

Theorem 1.2. *For every $\varepsilon > 0$ and every $n \geq 1$,*

$$r(n) \ll_{\varepsilon} n^{2/5+\varepsilon}.$$

The later sections then turn to the coprime subcount

$$c(n) := \#\{(a,b) \in \mathcal{A}^2 : \ a+b=n, \ (a,b)=1\}$$

and isolate several exact structures:

- an exact decomposition of $c(n)$ into the family $n - u^3x^2$;
- a principal-form interpretation of the relevant squarefree kernels;
- a twisted Rédei linear system for odd kernels;
- a fixed-u bound from Mordell-curve point counts;
- dyadic congruence-box bounds coming from Chan's theorem;
- a rigorous second-moment barrier expressed in terms of a square-pair norm; and
- a first-moment theorem whose proof would settle the coprime model.

Two warnings are important. First, the coprime model is *not* yet the full Erdős problem: if (a,b) is a squarefull representation and $g = (a,b)$, then g is squarefull, but a/g and b/g need not be. So there is currently no correct reduction of the full function $r(n)$ to the coprime subproblem alone. Second, the square-sieve barrier in this note is genuinely a barrier about *second moments*: the current quadratic large sieve controls square detection through a square-pair norm, and even an optimistic improvement to an ℓ^2-norm would still leave only square-root savings in the critical boxes.

The paper is therefore organised in three stages. Sections 2 and 3 concern the full representation function $r(n)$ and prove Theorem 1.2. The later sections then split into two complementary coprime routes. The kernel route, developed in Sections 5 and 6, packages the arithmetic into squarefree kernels, principal forms, and twisted Rédei data; it makes local structure explicit but does not yet control the number of admissible kernels or their global lifts. The lifted-root route, developed in Sections 7–10, packages the same problem into dyadic square detection for the family $n - u^3x^2$; it ends with a sufficient first-moment theorem for the coprime model and explains why currently available second-moment tools stop short of that target. The note ends with a literature survey explaining how the 2025–2026 advances fit around these remaining gaps.

2 Basic lemmas

We begin with two standard normal forms for squarefull integers.

Lemma 2.1. *For $m \in \mathbb{N}$ the following are equivalent.*

(i) *m is squarefull.*

(ii) *There are unique integers $x \in \mathbb{N}$ and squarefree $y \in \mathbb{N}$ such that*

$$m = x^2y^3.$$

(iii) *There are unique integers $r \in \mathbb{N}$ and squarefree $u \in \mathbb{N}$ such that*

$$m = ur^2, \qquad u \mid r.$$

Proof. Write

$$m = \prod_p p^{e_p}.$$

Then m is squarefull exactly when every $e_p \geq 2$.

For (ii), write uniquely

$$e_p = 2\alpha_p + 3\beta_p, \qquad \beta_p \in \{0, 1\}.$$

Set

$$x := \prod_p p^{\alpha_p}, \qquad y := \prod_{\beta_p = 1} p.$$

Then y is squarefree and $m = x^2 y^3$. Uniqueness is prime-by-prime.

For (iii), define

$$u := \prod_{e_p \text{ odd}} p, \qquad r := \prod_p p^{(e_p - 1_{e_p \text{ odd}})/2}.$$

Then u is squarefree, $u \mid r$, and $m = ur^2$. Conversely, if $m = ur^2$ with u squarefree and $u \mid r$, then each prime exponent in m is either $2a$ or $2a + 1$ with $a \geq 1$, hence at least 2. Again uniqueness is prime-by-prime. □

The next lemma is a uniform divisor-type bound for binary quadratic forms $x^2 + dy^2$.

Lemma 2.2. *Let $d \geq 1$ be squarefree and $M \geq 1$. Then*

$$\#\{(x, y) \in \mathbb{Z}^2 : \ x^2 + dy^2 = M\} \leq 6\tau(M).$$

In particular, for every $\varepsilon > 0$,

$$\#\{(x, y) \in \mathbb{Z}^2 : \ x^2 + dy^2 = M\} \ll_\varepsilon M^\varepsilon$$

uniformly in d and M.

Proof. Let $K = \mathbb{Q}(\sqrt{-d})$ with ring of integers $\mathcal{O}_K$. Every solution to

$$x^2 + dy^2 = M$$

gives

$$\alpha = x + y\sqrt{-d} \in \mathcal{O}_K$$

with norm $N_{K/\mathbb{Q}}(\alpha) = M$. Hence $\alpha\mathcal{O}_K$ is a principal integral ideal of norm M.

Conversely, any principal ideal of norm M has at most $w_K \leq 6$ generators, since an imaginary quadratic field has at most six roots of unity. Thus it is enough to show that the number of integral ideals of norm M is at most $\tau(M)$.

Write $M = \prod_p p^{e_p}$. By unique factorisation of ideals it is enough to count ideals of norm p^{e_p}. If p is inert or ramified in K, there is at most one such ideal. If p splits as

$$p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}, \qquad N\mathfrak{p} = N\bar{\mathfrak{p}} = p,$$

then the ideals of norm p^{e_p} are exactly

$$\mathfrak{p}^j \bar{\mathfrak{p}}^{\,e_p - j} \qquad (0 \leq j \leq e_p),$$

so there are $e_p + 1$ of them. Thus the total number of integral ideals of norm M is at most

$$\prod_{p^{e_p} \| M} (e_p + 1) = \tau(M).$$

Multiplying by the factor $w_K \leq 6$ proves the claim. □

Our second external input is Heath-Brown's uniform point count for primitive solutions of a diagonal cubic.

Lemma 2.3 (Heath-Brown)**.** *For every $\varepsilon > 0$ one has*

$$\#\{(X,Y,Z) \in \mathbb{Z}^3_{\text{prim}} : \ aX^3 + bY^3 + cZ^3 = 0, \ \max(|X|,|Y|,|Z|) \le B\} \ll_\varepsilon B^\varepsilon$$

uniformly for all non-zero integers a, b, c.

Proof. This is Theorem 1.3 of Heath-Brown [11]. □

3 A pointwise bound for the full function $r(n)$

We first fix the squarefree parts.

Proposition 3.1. *Fix squarefree integers $y_1, y_2 \ge 1$. Then for every $\varepsilon > 0$ the number of pairs $(x_1, x_2) \in \mathbb{N}^2$ satisfying*

$$x_1^2 y_1^3 + x_2^2 y_2^3 = n$$

is $O_\varepsilon(n^\varepsilon)$, uniformly in y_1, y_2 and n.

Proof. Write $g = (y_1, y_2)$ and $y_1 = gu$, $y_2 = gv$, where u and v are squarefree and coprime. If $g^3 \nmid n$ there are no solutions, so write $n = g^3 m$. Then

$$u^3 x_1^2 + v^3 x_2^2 = m.$$

Multiplying by u gives

$$um = (u^2 x_1)^2 + uv\,(vx_2)^2.$$

Since u and v are squarefree and coprime, uv is squarefree. Hence the map

$$(x_1, x_2) \mapsto (X, Y) := (u^2 x_1, v x_2)$$

injects the solution set into

$$\{(X,Y) \in \mathbb{Z}^2 : \ X^2 + uvY^2 = um\}.$$

Lemma 2.2 therefore gives at most $6\tau(um)$ possibilities.

Now $u \le y_1 \le n^{1/3}$ and $m \le n$, so $um \le n^{4/3}$. Given $\varepsilon > 0$, choose $\delta = 3\varepsilon/4$ in the divisor bound $\tau(t) \ll_\delta t^\delta$. Then

$$\tau(um) \ll_\delta (um)^\delta \le n^{(4/3)\delta} = n^\varepsilon,$$

proving the proposition. □

Now fix the square parts.

Proposition 3.2. *Fix integers $x_1, x_2 \ge 1$. Then for every $\varepsilon > 0$ the number of squarefree pairs $(y_1, y_2) \in \mathbb{N}^2$ satisfying*

$$x_1^2 y_1^3 + x_2^2 y_2^3 = n$$

is $O_\varepsilon(n^\varepsilon)$, uniformly in x_1, x_2 and n.

Proof. Every such solution gives a primitive integer point $(y_1, y_2, 1)$ on the diagonal cubic

$$x_1^2 Y_1^3 + x_2^2 Y_2^3 - nZ^3 = 0.$$

Moreover $y_1, y_2 \le n^{1/3}$. Apply Lemma 2.3 with its parameter ε replaced by 3ε, and with

$$(a, b, c) = (x_1^2, x_2^2, -n), \qquad B = n^{1/3}.$$

Then

$$\#\{(y_1, y_2)\} \ll_{3\varepsilon} (n^{1/3})^{3\varepsilon} = n^{\varepsilon},$$

which is exactly the required bound after relabelling the implied constant. □

We may now prove Theorem 1.2.

Proof of Theorem 1.2. By Lemma 2.1, every squarefull number can be written uniquely as $x^2 y^3$ with y squarefree. Thus

$$r(n) = \#\{(x_1, x_2, y_1, y_2) \in \mathbb{N}^4 : \ y_1, y_2 \text{ sqfree}, \ x_1^2 y_1^3 + x_2^2 y_2^3 = n\}.$$

For dyadic parameters (X_1, X_2, Y_1, Y_2), let

$$\mathscr{N}(X_1, X_2, Y_1, Y_2; n)$$

count the solutions with

$$X_i < x_i \le 2X_i, \qquad Y_i < y_i \le 2Y_i \qquad (i = 1, 2).$$

Since $x_i^2 y_i^3 \le n$, every contributing box satisfies

$$X_i^2 Y_i^3 \le n \qquad (i = 1, 2). \tag{3.1}$$

Proposition 3.1 gives

$$\mathscr{N}(X_1, X_2, Y_1, Y_2; n) \ll_{\varepsilon} n^{\varepsilon} Y_1 Y_2,$$

while Proposition 3.2 gives

$$\mathscr{N}(X_1, X_2, Y_1, Y_2; n) \ll_{\varepsilon} n^{\varepsilon} X_1 X_2.$$

Hence

$$\mathscr{N}(X_1, X_2, Y_1, Y_2; n) \ll_{\varepsilon} n^{\varepsilon} \min(X_1 X_2, Y_1 Y_2).$$

Set

$$A := X_1 X_2, \qquad B := Y_1 Y_2.$$

Multiplying the two inequalities in (3.1) yields

$$A^2 B^3 \le n^2.$$

If $A \le B$, then $A^5 \le A^2 B^3 \le n^2$, so $A \le n^{2/5}$. If $B \le A$, then similarly $B \le n^{2/5}$. Therefore

$$\min(A, B) \le n^{2/5},$$

and every dyadic box contributes

$$O_{\varepsilon}(n^{2/5+\varepsilon})$$

solutions. Since there are $O((\log n)^4)$ relevant boxes, the logarithmic factor is absorbed into n^{ε}, and the theorem follows. □

4 The coprime subproblem

From this point onward we study

$$c(n) := \#\{(a,b) \in \mathcal{A}^2 : \ a+b=n, \ (a,b)=1\}.$$

Remark 4.1 (A warning). The naive identity

$$r(n) \stackrel{?}{=} \sum_{\substack{g \mid n \\ g \in \mathcal{A}}} c(n/g)$$

is false: the representation

$$12 = 8 + 4$$

has $\gcd(8,4) = 4 \in \mathcal{A}$, but after dividing by 4 one obtains $3 = 2+1$, and $2 \notin \mathcal{A}$. Thus factoring out the gcd does not preserve squarefullness in general. The rest of the paper therefore concerns the coprime subcount $c(n)$ rather than the full function $r(n)$.

For squarefree $u \geq 1$ define

$$N_u(n) := \#\{(v,x,y) \in \mathbb{N}^3 : \ v \text{ sqfree}, \ n = u^3x^2 + v^3y^2, \ (ux, vy) = 1\}.$$

Then every coprime representation counted by $c(n)$ has a unique first squarefree kernel u, so

$$c(n) = \sum_{\substack{u \leq n^{1/3} \\ u \text{ sqfree}}} N_u(n). \tag{4.1}$$

It is often more convenient to absorb the second squarefull summand into a one-variable squarefull condition. Set

$$M_u(n) := \#\{x \in \mathbb{N} : \ n - u^3x^2 \in \mathcal{A}, \ (ux, \ n-u^3x^2) = 1\}.$$

Proposition 4.2. *For every squarefree u and every $n \geq 1$ one has*

$$N_u(n) = M_u(n).$$

Consequently

$$c(n) = \sum_{\substack{u \leq n^{1/3} \\ u \text{ sqfree}}} M_u(n).$$

Proof. If

$$n = u^3x^2 + v^3y^2, \qquad (ux, vy) = 1,$$

then $n - u^3x^2 = v^3y^2$ is squarefull, and the coprimality condition gives

$$(ux, \ n - u^3x^2) = 1.$$

Hence every solution counted by $N_u(n)$ contributes to $M_u(n)$.

Conversely, let x be counted by $M_u(n)$, and write

$$n - u^3x^2 = v^3y^2$$

using the unique normal form from Lemma 2.1. Then v is squarefree. If a prime p divided both ux and vy, then p would divide ux and $v^3y^2 = n - u^3x^2$, contradicting $(ux, \ n-u^3x^2) = 1$. Thus $(ux, vy) = 1$, and we get a solution counted by $N_u(n)$. □

The next proposition shows that pointwise estimates for the individual quadratic families $n - u^3x^2$ cannot finish the coprime problem by themselves.

Proposition 4.3 (A fixed-polynomial barrier)**.** *Suppose there is a real number $\eta < 2/3$ such that for every $\varepsilon > 0$ one has*

$$M_u(n) \ll_\varepsilon X_u^{\eta+\varepsilon}, \qquad X_u := \sqrt{\frac{n}{u^3}},$$

uniformly for all squarefree $u \le n^{1/3}$ and all $n \ge 1$. Then

$$c(n) \ll_\varepsilon n^{1/3+\varepsilon}.$$

Proof. Fix $\varepsilon > 0$ and choose

$$\delta := \min\left(\frac{\varepsilon}{2}, \frac{2/3 - \eta}{2}\right).$$

Then $\eta + \delta < 2/3$, and Proposition 4.2 gives

$$c(n) \ll_\delta \sum_{u \le n^{1/3}} X_u^{\eta+\delta} = n^{(\eta+\delta)/2} \sum_{u \le n^{1/3}} u^{-3(\eta+\delta)/2}.$$

Since $3(\eta + \delta)/2 < 1$, the sum is

$$\ll n^{(1-3(\eta+\delta)/2)/3}.$$

Multiplying the two powers of n gives

$$c(n) \ll_\delta n^{1/3} \ll_\varepsilon n^{1/3+\varepsilon}.$$

□

Remark 4.4. In particular, even a hypothetical pointwise bound

$$M_u(n) \ll_\varepsilon X_u^{\varepsilon}$$

for each individual quadratic polynomial $x \mapsto n - u^3x^2$ would still only yield

$$c(n) \ll_\varepsilon n^{1/3+\varepsilon}$$

after summing over u.

5 Squarefree kernels and principal forms

Define the squarefree kernel set for the coprime problem by

$$\mathcal{K}(n) := \left\{ d \text{ sqfree} : \ \exists\, u, v, x, y \ge 1,\ uv = d,\ n = u^3x^2 + v^3y^2,\ (ux, vy) = 1 \right\}.$$

The first principalisation is quadratic in n.

Proposition 5.1. *For squarefree d, the following are equivalent.*

(i) $d \in \mathcal{K}(n)$.

(ii) *There exist integers X, Y such that*

$$n^2 = X^2 + dY^2,$$

and

$$A := \frac{n+X}{2}, \qquad B := \frac{n-X}{2}$$

are coprime squarefull integers.

Proof. Assume $d \in \mathcal{K}(n)$, so

$$n = u^3x^2 + v^3y^2, \qquad uv = d, \qquad (ux, vy) = 1.$$

Set

$$X := u^3x^2 - v^3y^2, \qquad Y := 2uvxy.$$

Then

$$n^2 - X^2 = 4u^3v^3x^2y^2 = uv(2uvxy)^2 = dY^2,$$

so $n^2 = X^2 + dY^2$. Also

$$\frac{n+X}{2} = u^3x^2, \qquad \frac{n-X}{2} = v^3y^2,$$

which are squarefull and coprime.

Conversely, assume $n^2 = X^2 + dY^2$ with

$$A = \frac{n+X}{2}, \qquad B = \frac{n-X}{2}$$

coprime and squarefull. By Lemma 2.1 write uniquely

$$A = u^3x^2, \qquad B = v^3y^2$$

with u, v squarefree. Since $(A, B) = 1$, we have $(u, v) = 1$ and $(ux, vy) = 1$. Now

$$dY^2 = n^2 - X^2 = 4AB = 4u^3v^3x^2y^2 = uv(2uvxy)^2.$$

Both d and uv are squarefree, so uniqueness of the squarefree kernel gives $d = uv$. Hence

$$n = u^3x^2 + v^3y^2, \qquad uv = d, \qquad (ux, vy) = 1,$$

so $d \in \mathcal{K}(n)$. □

The next reformulation places the problem on the principal form $X^2 + dY^2$ of discriminant $-4d$.

Proposition 5.2. *For squarefree d, the following are equivalent.*

(i) $d \in \mathcal{K}(n)$.

(ii) *There is a divisor $u \mid d$, with $v := d/u$, and coprime positive integers a, b such that*

$$un = b^2 + da^2, \qquad v \mid a, \qquad u^2 \mid b.$$

Proof. Assume $d \in \mathcal{K}(n)$, so

$$n = u^3x^2 + v^3y^2, \qquad uv = d, \qquad (ux, vy) = 1.$$

Set

$$a := vy, \qquad b := u^2x.$$

Then $a, b \in \mathbb{N}$, $(a, b) = 1$, and

$$b^2 + da^2 = u^4x^2 + uv \cdot v^2y^2 = u(u^3x^2 + v^3y^2) = un.$$

Moreover $v \mid a$ and $u^2 \mid b$.

Conversely, suppose

$$un = b^2 + da^2, \qquad v = d/u, \qquad v \mid a, \qquad u^2 \mid b, \qquad (a, b) = 1,$$

with $a, b \in \mathbb{N}$. Write

$$a = vy, \qquad b = u^2x,$$

so $x, y \in \mathbb{N}$. Then

$$un = u^4x^2 + dv^2y^2 = u^4x^2 + uv^3y^2 = u(u^3x^2 + v^3y^2),$$

hence

$$n = u^3x^2 + v^3y^2.$$

If a prime p divided both ux and vy, then it would divide both $u^2x = b$ and $vy = a$, contradicting $(a, b) = 1$. Therefore $(ux, vy) = 1$, and $d \in \mathcal{K}(n)$. □

Corollary 5.3. *For every $\varepsilon > 0$,*

$$c(n) \ll_\varepsilon n^\varepsilon \, \#\mathcal{K}(n).$$

Proof. Given a coprime representation

$$n = u^3x^2 + v^3y^2, \qquad (ux, vy) = 1,$$

let $d = uv$ and define

$$X = u^3x^2 - v^3y^2, \qquad Y = 2uvxy.$$

Then Proposition 5.1 gives

$$n^2 = X^2 + dY^2.$$

For fixed d, Lemma 2.2 with $M = n^2$ shows that the number of possibilities for (X, Y) is $O_\varepsilon(n^\varepsilon)$. But (X, Y) determines

$$A = \frac{n + X}{2}, \qquad B = \frac{n - X}{2},$$

and hence determines the original ordered pair $(A, B) = (u^3x^2, v^3y^2)$. Summing over $d \in \mathcal{K}(n)$ proves the claim. □

Remark 5.4. The same kernel can arise from more than one split $d = uv$. For example

$$40825 = 39^2 + 34^3 = 17^3 + 2^3 \cdot 67^2,$$

so the same kernel $d = 34$ occurs with the two splits $(u, v) = (1, 34)$ and $(2, 17)$. The point of Corollary 5.3 is that fixed-d multiplicity is still only n^ε.

6 A twisted Rédei system for odd kernels

In this section we restrict to *odd* kernels $d \in \mathcal{K}(n)$. Write

$$d = p_1 \cdots p_t$$

with distinct odd primes p_i. Suppose

$$n = u^3x^2 + v^3y^2, \qquad uv = d, \qquad (ux, vy) = 1.$$

Then $(n, d) = 1$: if $p_i \mid d$ and $p_i \mid n$, reducing the defining equation modulo p_i forces $p_i \mid ux$ or $p_i \mid vy$, and hence contradicts $(ux, vy) = 1$. In particular each Legendre symbol $\left(\frac{n}{p_i}\right)$ is defined. Define $\varepsilon_i \in \mathbb{F}_2$ by

$$\varepsilon_i = \begin{cases} 0, & p_i \mid u, \\ 1, & p_i \mid v. \end{cases}$$

We also encode signs of Legendre symbols additively by

$$[\lambda] := \begin{cases} 0, & \lambda = 1, \\ 1, & \lambda = -1. \end{cases}$$

Now define the twisted Rédei matrix $R_d = (r_{ij}) \in M_t(\mathbb{F}_2)$ by

$$r_{ij} := \begin{cases} \left[\left(\dfrac{p_j}{p_i}\right)\right], & i \neq j, \\ \displaystyle\sum_{k \neq i} r_{ik}, & i = j, \end{cases}$$

so that every row sum is 0. Finally set

$$h_n(d) := \left(\left[\left(\frac{n}{p_1}\right)\right], \ldots, \left[\left(\frac{n}{p_t}\right)\right]\right)^T \in \mathbb{F}_2^t.$$

Proposition 6.1. *If $d \in \mathcal{K}(n)$ is odd, then the split vector ε satisfies*

$$R_d\varepsilon = h_n(d).$$

Conversely, a vector $\varepsilon \in \mathbb{F}_2^t$ solves this system if and only if the corresponding split $d = uv$ satisfies all odd-prime residue conditions forced by

$$n = u^3x^2 + v^3y^2, \qquad (ux, vy) = 1.$$

Proof. Fix i.

If $p_i \mid u$, then $p_i \nmid vy$ and

$$n \equiv v^3y^2 \pmod{p_i}.$$

Hence

$$\left(\frac{n}{p_i}\right) = \left(\frac{v}{p_i}\right) = \prod_{j:\, \varepsilon_j = 1} \left(\frac{p_j}{p_i}\right).$$

Passing to $\mathbb{F}_2$ gives

$$\left[\left(\frac{n}{p_i}\right)\right] = \sum_{j \neq i} r_{ij}\varepsilon_j = (R_d\varepsilon)_i,$$

since now $\varepsilon_i = 0$.

If $p_i \mid v$, then similarly

$$n \equiv u^3 x^2 \pmod{p_i}, \qquad \left(\frac{n}{p_i}\right) = \left(\frac{u}{p_i}\right) = \prod_{j:\,\varepsilon_j=0} \left(\frac{p_j}{p_i}\right).$$

Therefore

$$\left[\left(\frac{n}{p_i}\right)\right] = \sum_{j\neq i} r_{ij}(1-\varepsilon_j).$$

Because the ith row sum of R_d is zero,

$$\sum_{j\neq i} r_{ij}(1-\varepsilon_j) = r_{ii} + \sum_{j\neq i} r_{ij}\varepsilon_j = (R_d\varepsilon)_i,$$

and now $\varepsilon_i = 1$. This proves $R_d\varepsilon = h_n(d)$.

The converse is simply the same calculation backwards: a solution vector ε is equivalent to the collection of local residue conditions at the primes dividing d. □

Since $R_d\mathbf{1} = 0$, swapping u and v corresponds to adding the all-ones vector.

Corollary 6.2. *Assume $d \in \mathcal{K}(n)$ is odd and*

$$\operatorname{rank} R_d = t - 1.$$

Then the split $d = uv$ is unique up to swapping u and v.

Proof. The kernel of R_d has dimension 1, and it contains $\mathbf{1}$, so

$$\ker R_d = \{0, \mathbf{1}\}.$$

Hence the affine solution set of $R_d\varepsilon = h_n(d)$ has at most two elements, namely ε and $\varepsilon + \mathbf{1}$, corresponding exactly to (u, v) and (v, u). □

Remark 6.3 (How the two coprime routes differ). Sections 5 and 6 form a kernel/class-group route. They package a coprime representation through the squarefree kernel $d = uv$, principal representations by $X^2 + dY^2$, and, for odd d, a twisted Rédei linear system controlling the split $d = uv$. This route makes the local and genus-theoretic structure transparent, but it currently stalls at the point where one would need to count admissible kernels or prove global lifting statements from the local data.

The later sections follow a different route. They keep the squarefree parameter u explicit, rewrite the problem through the one-variable family $n - u^3x^2$, and then study dyadic boxes for the lifted quotient $(n - u^3x^2)/v^3$. That route is the one which leads to the square-sieve barrier and to the sufficient first-moment theorem formulated in Section 10.

7 A fixed-u bound from Mordell curves

We now quote the current Mordell-curve point-counting input.

Proposition 7.1 (Wongcharoenbhorn–Meemark)**.** *There is an absolute exponent*

$$\varpi_0 \approx 0.1688$$

such that for every $\varepsilon > 0$ and every non-zero integer D,

$$\#\{(X, Y) \in \mathbb{Z}^2 :\ Y^2 = X^3 + D\} \ll_\varepsilon |D|^{\varpi_0+\varepsilon}.$$

Proof. This is Proposition 3.2 of Wongcharoenbhorn and Meemark [14]. □

Theorem 7.2. *Let*

$$\theta := \frac{1+6\varpi_0}{5+12\varpi_0}, \qquad \gamma := \frac{6\varpi_0}{5+12\varpi_0}.$$

Then for every $\varepsilon > 0$ and every squarefree $u \le n^{1/3}$,

$$N_u(n) \ll_\varepsilon n^{\theta+\varepsilon} u^\gamma.$$

In particular,

$$N_1(n) \ll_\varepsilon n^{\theta+\varepsilon}, \qquad \theta \approx 0.2865.$$

Proof. For dyadic parameters E and V, let

$$\mathscr{M}_u(E, V; n)$$

count the solutions to

$$n = u^3x^2 + v^3y^2, \qquad (ux, vy) = 1,$$

with

$$E < y \le 2E, \qquad V < v \le 2V, \qquad v \text{ sqfree}.$$

First bound: fix v. For such a solution one has $(u, v) = 1$, since any common prime would divide both ux and vy. Multiplying the defining equation by u yields

$$un = (u^2x)^2 + uv\,(vy)^2.$$

Since uv is squarefree, Lemma 2.2 shows that for each fixed v the number of possible pairs (x, y) is $O_\delta((un)^\delta)$ for every $\delta > 0$. Since $u \le n^{1/3}$,

$$(un)^\delta \le n^{4\delta/3}.$$

Taking $\delta = 3\varepsilon/4$ and renaming ε therefore gives $O_\varepsilon(n^\varepsilon)$ possibilities for (x, y) when v is fixed. Summing over $v \sim V$ gives

$$\mathscr{M}_u(E, V; n) \ll_\varepsilon n^\varepsilon V. \tag{7.1}$$

Second bound: fix $y = e$. For a fixed integer e with $E < e \le 2E$, define

$$X := ue^2v, \qquad Y := u^3e^2x.$$

Then

$$Y^2 = u^6e^4x^2 = u^3e^4(n - v^3e^2) = u^3ne^4 - X^3.$$

Replacing X by $X' := -X$, each choice of e therefore leads to an integral point on the Mordell curve

$$Y^2 = (X')^3 + u^3ne^4.$$

By Proposition 7.1, for fixed e there are at most

$$O_\varepsilon\big((u^3ne^4)^{\varpi_0+\varepsilon}\big)$$

such points, and hence

$$\mathscr{M}_u(E, V; n) \ll_\varepsilon u^{3\varpi_0} n^{\varpi_0+\varepsilon} E^{1+4\varpi_0+\varepsilon}. \tag{7.2}$$

Optimisation. Since $v^3y^2 \le n$, every solution satisfies

$$V^3E^2 \le n, \qquad \text{hence} \qquad V \le n^{1/3}E^{-2/3}.$$

Combining (7.1) and (7.2),

$$\mathscr{M}_u(E,V;n) \ll_\varepsilon n^\varepsilon \min\Big(n^{1/3}E^{-2/3},\ u^{3\varpi_0}n^{\varpi_0}E^{1+4\varpi_0}\Big).$$

Balancing the two quantities gives

$$E^{5/3+4\varpi_0} = n^{1/3-\varpi_0}u^{-3\varpi_0},$$

and the corresponding common value is

$$n^\theta u^\gamma, \qquad \theta = \frac{1+6\varpi_0}{5+12\varpi_0}, \qquad \gamma = \frac{6\varpi_0}{5+12\varpi_0}.$$

Thus

$$\mathscr{M}_u(E,V;n) \ll_\varepsilon n^{\theta+\varepsilon}u^\gamma.$$

Finally, summing over the $O((\log n)^2)$ dyadic boxes (E,V) gives

$$N_u(n) \ll_\varepsilon n^{\theta+\varepsilon}u^\gamma.$$

□

8 Dyadic congruence boxes

For dyadic parameters (U,V,X,Y), let

$$\mathscr{B}(U,V,X,Y;n)$$

denote the number of coprime solutions to

$$n = u^3x^2 + v^3y^2, \qquad u,v \text{ sqfree}, \qquad (ux,vy) = 1,$$

with

$$U < u \le 2U, \qquad V < v \le 2V, \qquad X < x \le 2X, \qquad Y < y \le 2Y.$$

The underlying congruence is

$$x^2u^3 \equiv n \pmod{v^3}.$$

To count such pairs in a box we use Chan's theorem for the congruence $a^2b^3 \equiv \ell \pmod q$.

Lemma 8.1 (Chan)**.** *Let $(\ell,q)=1$. For real numbers A,B,K,L with $K,L \ge 1$,*

$$N_{A,B}(K,L) := \#\{(a,b):\ a^2b^3 \equiv \ell \pmod q,\ A < a \le A+K,\ B < b \le B+L\}$$

satisfies

$$N_{A,B}(K,L) = \frac{\phi(q)KL}{q^2} + O\Big(K + \frac{L}{q^{1/2-\varepsilon}} + q^{1/2+\varepsilon}\Big)$$

for every $\varepsilon > 0$.

Proof. This is Theorem 4 of Chan [6]. □

Theorem 8.2. *For every $\varepsilon > 0$ one has*

$$\mathscr{B}(U,V,X,Y;n) \ll_\varepsilon \frac{UX}{V^2} + VX + UV^{-1/2+\varepsilon} + V^{5/2+\varepsilon},$$

and symmetrically

$$\mathscr{B}(U,V,X,Y;n) \ll_\varepsilon \frac{VY}{U^2} + UY + VU^{-1/2+\varepsilon} + U^{5/2+\varepsilon}.$$

Proof. For fixed u, v, x, the variable y is uniquely determined if it exists, since it must satisfy

$$v^3y^2 = n - u^3x^2.$$

Thus, for an upper bound, one may discard the Y-condition and simply count triples (u, v, x) obeying the box conditions and the congruence.

Fix $v \sim V$. Since $(ux, vy) = 1$, we have $(u, v) = 1$. Also $(n, v) = 1$: if a prime p divided both n and v, then reducing

$$n = u^3x^2 + v^3y^2$$

modulo p would give $p \mid u^3x^2$, hence $p \mid ux$, contradicting $(ux, vy) = 1$ because $p \mid v$.

Thus Chan's lemma applies with

$$q = v^3, \qquad \ell = n, \qquad a = x, \qquad b = u, \qquad K \asymp X, \qquad L \asymp U.$$

For this fixed v, the number of pairs (u, x) is therefore

$$\ll_\varepsilon \frac{\phi(v^3)UX}{v^6} + X + \frac{U}{v^{3/2-\varepsilon}} + v^{3/2+\varepsilon}.$$

Since $\phi(v^3) \le v^3$, this is

$$\ll_\varepsilon \frac{UX}{v^3} + X + \frac{U}{v^{3/2-\varepsilon}} + v^{3/2+\varepsilon}.$$

Summing over $v \sim V$ gives

$$\mathscr{B}(U,V,X,Y;n) \ll_\varepsilon \frac{UX}{V^2} + VX + UV^{-1/2+\varepsilon} + V^{5/2+\varepsilon}.$$

The second estimate follows by symmetry after exchanging (u, x) and (v, y). □

Remark 8.3. In the balanced box

$$U \asymp V \asymp X \asymp Y \asymp n^{1/5},$$

the main terms

$$\frac{UX}{V^2}, \qquad \frac{VY}{U^2}$$

are of order 1. Thus the congruence structure is at the right scale there, but the current error terms are still far too large.

Remark 8.4 (Why congruence control alone is not enough). Even an ideal short-box congruence estimate of the shape

$$\mathscr{B}(U,V,X,Y;n) \ll_\varepsilon \frac{UX}{V^2} + n^\varepsilon$$

and its symmetric twin would still leave large boxes. Indeed, taking

$$U = V = n^{1/9}, \qquad X = Y = n^{1/3}$$

gives

$$\frac{UX}{V^2} = \frac{VY}{U^2} = n^{2/9}.$$

So one must use not only the congruence

$$x^2u^3 \equiv n \pmod{v^3},$$

but also the exact square condition

$$\frac{n - u^3x^2}{v^3} \in \square.$$

Remark 8.5 (Why the exponents $1/5$ and $1/9, 1/3$ both occur). The balanced scale

$$U \asymp V \asymp X \asymp Y \asymp n^{1/5}$$

from Theorem 1.2 belongs to the raw four-variable dyadic decomposition of

$$n = u^3x^2 + v^3y^2.$$

By contrast, the later scale

$$U \asymp V \asymp n^{1/9}, \qquad X \asymp Y \asymp n^{1/3}$$

appears only after one projects away one variable and keeps the congruence-plus-square condition on

$$\frac{n - u^3x^2}{v^3}.$$

These are two different projections of the same representation problem, not conflicting critical regimes.

9 Dyadic square detection and a second-moment barrier

For dyadic U, V, X define

$$\mathscr{S}(U,V,X;n) := \#\left\{ \begin{array}{l} u,v,x \in \mathbb{N} :\ u \sim U,\ v \sim V,\ x \sim X,\ u,v \text{ sqfree}, \\ u^3x^2 < n,\ u^3x^2 \equiv n \pmod{v^3},\ (ux,\ n - u^3x^2) = 1, \\ \dfrac{n - u^3x^2}{v^3} \in \square \end{array} \right\}.$$

Thus $\mathscr{S}(U,V,X;n)$ is the dyadic square-detection problem naturally attached to the coprime model. It is convenient to remove the square condition and work with the larger candidate set

$$\mathscr{T}(U,V,X;n) := \left\{ \begin{array}{l} u,v,x \in \mathbb{N} :\ u \sim U,\ v \sim V,\ x \sim X,\ u,v \text{ sqfree}, \\ u^3x^2 < n,\ u^3x^2 \equiv n \pmod{v^3},\ (ux,\ n - u^3x^2) = 1 \end{array} \right\}.$$

Write

$$N(U,V,X;n) := \#\mathscr{T}(U,V,X;n).$$

For $t = (u, v, x) \in \mathscr{T}(U, V, X; n)$, set

$$m_t := \frac{n - u^3 x^2}{v^3} \in \mathbb{N}.$$

Then t contributes to $\mathscr{S}(U, V, X; n)$ if and only if m_t is a square. Define the weight function

$$w(m) := \#\{t \in \mathscr{T}(U, V, X; n) : \ m_t = m\}.$$

If $B := n/V^3$, then $w(m) = 0$ unless $1 \le m \le B$, and

$$N(U, V, X; n) = \sum_{m \le B} w(m), \qquad \mathscr{S}(U, V, X; n) = \sum_{r^2 \le B} w(r^2). \tag{9.1}$$

The next lemma is the weighted square sieve in a form adapted to (9.1).

Lemma 9.1 (Weighted square sieve)**.** *Let $\mathcal{P}$ be a set of P odd primes, each exceeding B. Then*

$$\mathscr{S}(U, V, X; n) \le P^{-1} N(U, V, X; n) + P^{-2} \sum_{\substack{p, q \in \mathcal{P} \\ p \ne q}} \left| \sum_{m \le B} w(m) \left(\frac{m}{pq}\right) \right|.$$

Proof. If $m = r^2 \le B$ and $p \in \mathcal{P}$, then $p > m$, so $p \nmid m$ and

$$\left(\frac{m}{p}\right) = 1.$$

Hence

$$\sum_{r^2 \le B} w(r^2) = P^{-2} \sum_{r^2 \le B} w(r^2) \left(\sum_{p \in \mathcal{P}} \left(\frac{r^2}{p}\right) \right)^2 \le P^{-2} \sum_{m \le B} w(m) \left| \sum_{p \in \mathcal{P}} \left(\frac{m}{p}\right) \right|^2.$$

Expanding the square gives

$$P^{-2} \sum_{p, q \in \mathcal{P}} \sum_{m \le B} w(m) \left(\frac{m}{pq}\right).$$

For the diagonal terms $p = q$ we have $p \nmid m$ for all $m \le B$, so

$$\left(\frac{m}{p^2}\right) = \left(\frac{m}{p}\right)^2 = 1,$$

and the diagonal contribution is

$$P^{-2} \cdot P \sum_{m \le B} w(m) = P^{-1} N(U, V, X; n).$$

Taking absolute values in the off-diagonal terms yields the claim. □

We next import the standard quadratic large sieve in the form relevant to our application.

Lemma 9.2 (Quadratic large sieve)**.** *For every $\varepsilon > 0$, every $D, B \ge 1$, and every complex sequence (a_m) supported on $1 \le m \le B$,*

$$\sum_{\substack{d \le D \\ d \text{ odd},\ d \text{ sqfree}}} \left| \sum_{m \le B} a_m \left(\frac{m}{d}\right) \right|^2 \ll_\varepsilon (DB)^\varepsilon (D + B) \sum_{\substack{m_1, m_2 \le B \\ m_1 m_2 = \square}} |a_{m_1} a_{m_2}|.$$

Proof. This is Heath-Brown's quadratic large sieve, in the explicit form recorded by Liu [12]. □

Define the associated square-pair norm

$$\mathcal{Q}(w) := \sum_{\substack{m_1,m_2\le B\\ m_1m_2=\square}} w(m_1)w(m_2).$$

Since the weights are nonnegative, one always has $\mathcal{Q}(w) \ge \sum_m w(m)^2$.

Theorem 9.3 (Rigorous second-moment barrier)**.** *For every $\varepsilon > 0$ one has*

$$\mathscr{S}(U,V,X;n) \ll_\varepsilon n^\varepsilon \mathcal{Q}(w)^{1/2}.$$

Consequently, even under the optimistic hypothesis

$$\mathcal{Q}(w) \ll_\varepsilon n^\varepsilon N(U,V,X;n),$$

one still obtains only

$$\mathscr{S}(U,V,X;n) \ll_\varepsilon n^\varepsilon N(U,V,X;n)^{1/2}.$$

Proof. For n large, choose $\mathcal{P}$ to be the set of primes in the interval $(2n, 4n]$. By the prime number theorem,

$$P := \#\mathcal{P} \asymp \frac{n}{\log n}.$$

Since $B \le n$, every prime in $\mathcal{P}$ exceeds B, so Lemma 9.1 applies to give

$$\mathscr{S}(U,V,X;n) \ll P^{-1}N(U,V,X;n) + P^{-2}\sum_{\substack{p,q\in\mathcal{P}\\ p\ne q}}\left|\sum_{m\le B} w(m)\left(\frac{m}{pq}\right)\right|.$$

For the finitely many small values of n, the stated estimate may be absorbed into the implied constant.

Set

$$S(d) := \sum_{m\le B} w(m)\left(\frac{m}{d}\right).$$

By Cauchy,

$$\sum_{\substack{p,q\in\mathcal{P}\\ p\ne q}} |S(pq)| \le P\left(\sum_{\substack{p,q\in\mathcal{P}\\ p\ne q}} |S(pq)|^2\right)^{1/2}.$$

Since each pq is an odd squarefree integer at most $16n^2$, and each such product occurs at most twice among the ordered pairs (p,q) and (q,p), Lemma 9.2 with $D = 16n^2$ and $a_m = w(m)$ yields

$$\sum_{\substack{p,q\in\mathcal{P}\\ p\ne q}} |S(pq)|^2 \le 2 \sum_{\substack{d\le 16n^2\\ d \text{ odd},\ d \text{ sqfree}}} |S(d)|^2 \ll_\delta n^\delta(n^2+B)\mathcal{Q}(w) \ll_\delta n^{2+\delta}\mathcal{Q}(w)$$

for any $\delta > 0$, because $B \le n$. Hence

$$P^{-2}\sum_{\substack{p,q\in\mathcal{P}\\ p\ne q}} |S(pq)| \ll_\delta P^{-1}n^{1+\delta/2}\mathcal{Q}(w)^{1/2} \ll_\delta (\log n)n^{\delta/2}\mathcal{Q}(w)^{1/2}.$$

For the diagonal term, the box constraints imply

$$N(U,V,X;n) \le UVX \le n^{5/6}.$$

Therefore

$$P^{-1}N(U,V,X;n) \ll \frac{\log n}{n} N(U,V,X;n) \ll n^{-1/6}\log n.$$

If $\mathcal{Q}(w)=0$, then $\mathscr{S}(U,V,X;n)=0$ and there is nothing to prove. Otherwise $\mathcal{Q}(w)\ge 1$, so

$$n^{-1/6}\log n \ll_\varepsilon n^{\varepsilon}\mathcal{Q}(w)^{1/2}.$$

Combining the two estimates and choosing $\delta<\varepsilon$ proves the theorem. □

Remark 9.4 (Interpretation of the barrier). Theorem 9.3 already shows that a square-sieve argument powered only by quadratic-character second moments cannot settle the coprime model through this route. In the most optimistic scenario one would hope that the square-pair norm is of the same order as the candidate set size,

$$\mathcal{Q}(w) \asymp N(U,V,X;n),$$

which would force only

$$\mathscr{S}(U,V,X;n) \ll_\varepsilon n^{\varepsilon} N(U,V,X;n)^{1/2}.$$

For example, if one also had the ideal congruence-box bound

$$N(U,V,X;n) \ll_\varepsilon n^{2/9+\varepsilon}$$

in the short projected range

$$U \asymp V \asymp n^{1/9}, \qquad X \asymp Y \asymp n^{1/3},$$

then Theorem 9.3 would still give only

$$\mathscr{S}(U,V,X;n) \ll_\varepsilon n^{1/9+\varepsilon}.$$

So the missing ingredient on this route must be a *first-moment* statement for the twisted lifted-root sums, not merely another second-moment large-sieve inequality.

10 A sufficient first-moment theorem for the coprime model

For an odd squarefree integer d define the twisted lifted-root sum

$$T_d(U,V,X;n) := \sum_{m\le B} w(m)\left(\frac{m}{d}\right) = \sum_{t\in\mathscr{T}(U,V,X;n)} \left(\frac{m_t}{d}\right).$$

For $Z \ge \max(2B,3)$ let

$$\mathcal{P}_Z := \{p\in[Z,2Z] : p \text{ odd prime}\}, \qquad P_Z := \#\mathcal{P}_Z.$$

The next problem is not claimed to be equivalent to the dyadic square-detection problem, but it is a clean *sufficient* theorem for the coprime model.

Problem 10.1 (A sufficient first-moment theorem for the coprime model). Prove that for every $\varepsilon > 0$ there is a constant C_ε such that, for every $n \geq 1$, every dyadic box with $\mathscr{T}(U, V, X; n) \neq \varnothing$, and every real $Z \geq \max(2B, 3)$,

$$\sum_{\substack{p,q \in \mathcal{P}_Z \\ p \neq q}} |T_{pq}(U, V, X; n)| \leq C_\varepsilon P_Z^2 n^\varepsilon.$$

Proposition 10.2. *A proof of Problem 10.1 would imply*

$$\mathscr{S}(U, V, X; n) \ll_\varepsilon n^\varepsilon$$

for every dyadic box, and hence

$$c(n) = n^{o(1)}.$$

In other words, Problem 10.1 is sufficient to settle the coprime model (but not by itself the full function $r(n)$).

Proof. Fix a dyadic box and choose

$$Z := \max(2B, n^2, 3).$$

Then $Z \geq 2B$, and by the prime number theorem

$$P_Z \asymp \frac{Z}{\log Z}.$$

Applying Lemma 9.1 with $\mathcal{P} = \mathcal{P}_Z$ and then using Problem 10.1 gives

$$\mathscr{S}(U, V, X; n) \ll P_Z^{-1} N(U, V, X; n) + n^\varepsilon.$$

Now

$$N(U, V, X; n) \leq UVX,$$

and the box constraints imply $U^3 X^2 < n$ and $V^3 < n$. Hence

$$UVX \leq V n^{1/2} U^{-1/2} \leq n^{1/3} n^{1/2} = n^{5/6}.$$

Therefore

$$P_Z^{-1} N(U, V, X; n) \ll \frac{n^{5/6} \log Z}{Z} \ll n^{-7/6} \log n \ll n^\varepsilon.$$

So indeed $\mathscr{S}(U, V, X; n) \ll_\varepsilon n^\varepsilon$.

Finally, every coprime representation

$$n = u^3 x^2 + v^3 y^2, \qquad (ux, vy) = 1,$$

has a unique triple (u, v, x) with u, v squarefree and

$$\frac{n - u^3 x^2}{v^3} = y^2.$$

Hence each such representation contributes to exactly one dyadic box in (u, v, x), and

$$c(n) \leq \sum_{U,V,X} \mathscr{S}(U, V, X; n),$$

where the sum runs over the $O((\log n)^3)$ dyadic boxes with

$$U \le n^{1/3}, \qquad V \le n^{1/3}, \qquad X \le (n/U^3)^{1/2}.$$

Using the bound $\mathscr{S}(U,V,X;n) \ll_\varepsilon n^\varepsilon$ for each box and absorbing the logarithmic factor into n^ε yields

$$c(n) \ll_\varepsilon n^\varepsilon,$$

which is the same as $c(n) = n^{o(1)}$. □

Sections 4–9 show why this is a genuinely bilinear problem. Pointwise estimates for the individual quadratic families $n - u^3x^2$ are too weak after summation over u (Proposition 4.3), congruence equidistribution for

$$x^2u^3 \equiv n \pmod{v^3}$$

is still too weak unless one also exploits the lifted square condition from Remark 8.4, and a pure second-moment square-sieve argument stops at the barrier of Theorem 9.3. The exact remaining task on the lifted-root route is therefore a first-moment square-sieve theorem over cube-modulus congruences.

What this does and does not resolve. A proof of Problem 10.1 would settle the coprime model $c(n) = n^{o(1)}$. It would not by itself settle the full Erdős problem for $r(n)$, because there is currently no correct reduction from all squarefull representations to coprime ones. So the full problem would be resolved either by

(i) a proof of Problem 10.1 together with a valid passage from the full function $r(n)$ to the coprime model, or by

(ii) a direct noncoprime analogue of the same first-moment theorem in the natural dyadic model for all representations.

Summary of the unconditional state of play. The rigorous conclusions of this note are:

- the full representation function satisfies $r(n) \ll_\varepsilon n^{2/5+\varepsilon}$;
- the coprime subproblem admits the exact decomposition

$$c(n) = \sum_{u \text{ sqfree}} M_u(n);$$

- the associated squarefree kernels admit the principal-form reformulations in Propositions 5.1 and 5.2;
- odd kernels satisfy the twisted Rédei system of Proposition 6.1;
- fixed-u counts satisfy Theorem 7.2;
- dyadic congruence boxes satisfy Theorem 8.2;
- second-moment square-sieve technology stops at Theorem 9.3; and
- a proof of Problem 10.1 would settle the coprime model, but an additional valid reduction (or a direct noncoprime analogue) would still be needed to recover the full function $r(n)$.

11 Current status of the literature (2025–2026)

The preceding sections isolate the mathematical gap rather sharply, and it is useful to compare it with what the current literature actually provides.

Squarefull counting and squarefull values

On the global squarefull-counting side, Zhao's 2025 paper improved the earlier Browning–Van Valckenborgh upper bound for squarefull solutions of $x + y = z$ [15]. Heath-Brown's January 2026 preprint then gave the first improvement over the "easy" exponent $3/5$, proving

$$N_{\mathrm{glob}}(B) \ll_\varepsilon B^{3/5-3/1555+\varepsilon}$$

for global squarefull triples $x + y = z$ and simultaneously establishing the uniform primitive diagonal-cubic estimate used in Lemma 2.3 [11]. At the pointwise level for polynomial values, Wongcharoenbhorn and Meemark prove that if f is an admissible quadratic polynomial then the number of $n \le N$ for which $f(n)$ is squarefull is

$$O_{\varepsilon,f}(N^{\varpi+\varepsilon}), \qquad \varpi \approx 0.4769,$$

while for the special family $x^2+\alpha^2$ they obtain the sharper exponent $29/100$ in a uniform range for α [14]. The same paper proves a Mordell-curve point bound with exponent $\varpi_0 \approx 0.1688$ and notes that the conjectural target N^ε would follow from a much stronger Mordell-curve estimate; under the *abc* conjecture they do prove $O_{\varepsilon,f}(N^\varepsilon)$ for fixed admissible quadratic f [14]. On a different front, Meemark and Wongcharoenbhorn show in 2025 that the variance of squarefull integers in short intervals has the expected order under a quasi-Riemann-hypothesis-type assumption, and that the variance in arithmetic progressions admits an asymptotic formula after averaging a quadratic residue and a nonresidue by a half for all primes $q \gg x^{51/114+\varepsilon}$ [13].

Quadratic characters, modular roots, and sparse moduli

For the quadratic-character input, Liu's 2025 paper gives an explicit form of Heath-Brown's quadratic large sieve [12]. Importantly, this still has the square-pair norm

$$\sum_{n_1 n_2 = \square} |a_{n_1} a_{n_2}|$$

on the right-hand side rather than an honest ℓ^2 norm for arbitrary coefficients, so the second-moment barrier isolated in Section 9 is already optimistic.

On the modular-root side, Grimmelt and Merikoski obtain in 2025 a uniform equidistribution theorem for roots of quadratic congruences modulo primes, with uniformity in shifts $h \le n^{1+o(1)}$ under a natural hypothesis on real characters; the same paper also proves a divisor-problem variant for forms $ax^2 + by^3$ [10]. Baier's March 2025 preprint *The large sieve for square moduli, revisited* emphasizes that the classical large sieve with square moduli still has an unconditional barrier at the critical point $N = Q^3$, and that the factor $Q^{1/2}$ in the known bound has not yet been improved unconditionally there [2]. Baier's January 2026 paper then proves nontrivial bilinear bounds for modular square roots when the relevant lengths are above the $r^{1/3}$ scale; in particular it explicitly notes that its method does not yield a nontrivial result when both summation lengths are $\le r^{1/3}$ [3]. The March 2026 sequel improves the complementary large-range regime, focusing on summation lengths larger than the square-root scale and on moduli with a large squarefree part [4]. For quadratic congruences modulo odd prime powers, the asymptotic theory of Baier, Bhandari and Haldar still requires side lengths at least about the square-root scale of the modulus [1].

Averaging results, geometric viewpoints, and the remaining gap

A separate modern direction is the many-variable circle method for averaging arithmetic functions at polynomial values. Destagnol and Sofos develop this for smooth polynomials in many variables, and Destagnol, Lyczak and Sofos apply it in 2025 to multivariate local-solubility problems for families of high-dimensional Châtelet varieties [9, 8]. This is powerful, but it is structurally orthogonal to the present note: our obstacle sits in a genuinely two-variable lifted family and in a critical dyadic range where a first-moment square-sieve theorem is required. On a more class-group-theoretic side, Chan, Koymans and Rome use related averaging technology to obtain an asymptotic for triples (a, b, c) with prescribed Rédei symbol [7], which is closely related to the odd-kernel linear algebra appearing in Section 6, but still does not address the lifted-square first moment needed here.

The online forum page for Erdős Problem 943 also records a recent geometric suggestion: a comment of 3 February 2026 points out a Campana-point interpretation of squarefull representations along the pencil of lines $x + y = nz$ in $\mathbb{P}^2$ [5]. This is a useful heuristic reformulation, but the same comment also stresses that any such global Campana-Manin viewpoint would still need uniform fibrewise control of exceptional thin sets. That warning is very much in line with the analysis of the present note.

In short, the 2025–2026 literature substantially strengthens every surrounding ingredient—global squarefull counts, squarefull values of quadratic polynomials, prime-modulus root equidistribution, quadratic large sieves, and bilinear sums with modular square roots—but it still does not supply the first-moment estimate for the twisted lifted-root sums $T_d(U, V, X; n)$ that would finish the coprime model studied here, let alone the additional reduction needed to pass from that model to the full function $r(n)$.

References

[1] S. Baier, A. Bhandari and A. Haldar, *Small solutions to inhomogeneous and homogeneous quadratic congruences modulo prime powers*, arXiv:2406.12758, 2024.

[2] S. Baier, *The large sieve for square moduli, revisited*, arXiv:2503.18009, 2025.

[3] S. Baier, *On certain bilinear sums with modular square roots and applications*, arXiv:2601.15448, 2026.

[4] S. Baier, *On bilinear sums with modular square roots and applications II*, arXiv:2603.00768, 2026.

[5] T. F. Bloom, *Erdős Problem #943*, https://www.erdosproblems.com/forum/thread/943, accessed 2026-03-18.

[6] T. H. Chan, *Squarefull numbers in arithmetic progression II*, arXiv:1407.0054, 2014.

[7] S. Chan, P. Koymans and N. Rome, *Serre's problem for multiple conics*, arXiv:2504.21792, 2025.

[8] K. Destagnol, J. Lyczak and E. Sofos, *Local solubility in generalised Châtelet varieties*, arXiv:2504.11388, 2025.

[9] K. Destagnol and E. Sofos, *Averages of arithmetic functions over polynomials in many variables*, arXiv:2409.18116, 2024.

[10] L. Grimmelt and J. Merikoski, *On the greatest prime factor and uniform equidistribution of quadratic polynomials*, arXiv:2505.00493, 2025.

[11] D. R. Heath-Brown, *Counting Square-full Solutions to $x + y = z$*, arXiv:2601.07817, 2026.

[12] Z. Liu, *Explicit quadratic large sieve inequality*, arXiv:2505.09637, 2025.

[13] Y. Meemark and W. Wongcharoenbhorn, *Variance of square-full integers in short intervals and in arithmetic progressions*, arXiv:2504.14511, 2025.

[14] W. Wongcharoenbhorn and Y. Meemark, *Square-full values of quadratic polynomials*, Bull. Aust. Math. Soc. **113** (2026), 40–54; arXiv:2405.06968.

[15] X. Zhao, *The upper bound on sums of three squareful numbers*, Ramanujan J. **68** (2025), no. 1, Paper No. 7.