Sieve methods and a problem of Erdős

Przemyslaw Chojecki

January 26, 2026

Abstract

We study a problem of Erdős concerning representations

$$n = x^2 + y^2 - z^2 \qquad \text{with} \qquad \max(x^2, y^2, z^2) \leq n.$$

Using an elementary large-sieve/second-moment method, we prove that this representation exists for a density-one set of integers n. More precisely, we show that the number of exceptions up to N is $O(N^{3/4})$. We also briefly outline how one might attempt to upgrade such a density-one statement to "all sufficiently large n" via a δ–method/Kuznetsov approach: the expected main term is governed by local densities (Task A), while the remaining obstacle is a pointwise bound for the off-diagonal (Task B), which reduces to cancellation in Selberg/transition-range sums of half-integral weight Kloosterman–Salié sums.

1 Introduction

Let

$$Q(x, y, z) = x^2 + y^2 - z^2.$$

Erdős asked whether there exists N_0 such that every integer $n \geq N_0$ admits a representation

$$n = Q(x, y, z) = x^2 + y^2 - z^2 \qquad \text{with} \qquad \max(x^2, y^2, z^2) \leq n. \tag{1}$$

Equivalently, writing $m = \lfloor \sqrt{n} \rfloor$, one asks for integers $0 \leq x, y, z \leq m$ with $n = x^2 + y^2 - z^2$. The constraint (1) is sharp in the sense that each variable is forced to lie on the natural scale $\sqrt{n}$.

The goal of this paper is more modest: we establish (1) for a density-one set of integers using an elementary sieve/large-sieve argument, and we record the analytic framework (Tasks A/B) that one would pursue to attempt a full resolution.

Main result

Let

$$E(N) := \#\{1 \leq n \leq N : \ n \text{ does not admit a representation (1)}\}.$$

Our main theorem is the following power-saving bound.

Theorem 1 (Density one)**.** *For every $\varepsilon > 0$ one has*

$$E(N) \ \ll_\varepsilon \ N^{3/4+\varepsilon}.$$

In particular, (1) *holds for a density-one set of integers n.*

Idea of the proof

The argument is a second-moment method on short intervals. For each shell $\mathcal{I}_M = (M^2, (M+1)^2]$ we build a nonnegative weight $S(n)$ which counts divisibility relations $d \mid (n - y^2)$ with y in a short interval $(M-H, M]$ and d in a short interval $(\sqrt{M}, 2\sqrt{M}]$, together with a parity restriction. Any such divisor relation produces a factorization $n - y^2 = (x-z)(x+z)$ with $x, z \le M$, hence yields (1). We then show that $\mathbb{E}[S(n)] \asymp \sqrt{M}$ on $\mathcal{I}_M$ while $\mathrm{Var}(S(n)) \ll \sqrt{M}$, using a dual large sieve inequality and a simple orthogonality bound for short quadratic exponential sums. Chebyshev's inequality implies that at most $O(\sqrt{M})$ integers in each shell satisfy $S(n) = 0$, and summing over shells gives $E(N) \ll N^{3/4}$.

A roadmap toward pointwise results (Tasks A/B)

Although Theorem 1 proves (1) for almost all n, it does not rule out a sparse infinite exceptional set. A standard analytic approach to pointwise existence is to consider a nonnegative weighted count

$$\Gamma_W(n) = \sum_{x \in \mathbb{Z}^3} W\left(\frac{x}{\sqrt{n}}\right) \mathbf{1}_{Q(x)=n},$$

where W is supported in a fixed open patch of $\{Q = 1\}$ inside $(0,1)^3$. Positivity $\Gamma_W(n) > 0$ implies (1). Applying the δ–method and Poisson summation leads to a decomposition $\Gamma_W(n) = M(n) + E(n)$. The main term $M(n)$ is governed by local densities and a singular series (Task A), while bounding the off-diagonal $E(n)$ pointwise (Task B) leads naturally to the Kuznetsov–Proskurin formula and cancellation in Selberg/transition-range sums of half-integral weight Kloosterman–Salié sums. In this paper we do not attempt those analytic estimates; we only outline the framework in the concluding notes.

2 A large-sieve method and a density-one theorem

In this section we prove that Erdős' inequality (1) holds for a density-one set of integers. Our argument is elementary: we construct a nonnegative weight $S(n)$ which counts "good" divisibility relations $d \mid (n - y^2)$ with y near $\sqrt{n}$ and d in a short interval of length $\asymp \sqrt{n}$; we then bound the first and second moments of $S(n)$ on each short shell $(M^2, (M+1)^2]$ using a dual large sieve inequality.

2.1 A divisor criterion

Let $n \ge 1$ and let $m = \lfloor \sqrt{n} \rfloor$. If $n = x^2 + y^2 - z^2$ with $0 \le x, y, z \le m$, then

$$n - y^2 = x^2 - z^2 = (x-z)(x+z).$$

Conversely, if for some $0 \le y \le m$ the integer $t := n - y^2$ admits a factorization

$$t = ab, \qquad a \equiv b \pmod{2},$$

with

$$0 \le a \le b, \qquad b \le 2m, \qquad a + b \le 2m,$$

then setting $x = (a+b)/2$ and $z = (b-a)/2$ gives integers $0 \le x, z \le m$ and $n = x^2 + y^2 - z^2$.

In this section we force such a factorization by producing, for many n, a divisor d of $t = n - y^2$ with $d \asymp \sqrt{m}$ and y chosen very close to m.

2.2 A weight on each square shell

Fix an integer $M \geq 2$ and consider the shell

$$\mathcal{I}_M := \{n \in \mathbb{Z} : \ M^2 < n \leq (M+1)^2\}, \qquad L := |\mathcal{I}_M| = 2M+1.$$

Let

$$H := \left\lfloor \frac{\sqrt{M}}{100} \right\rfloor, \qquad R := \lfloor \sqrt{M} \rfloor, \qquad \mathcal{Y} := \{y \in \mathbb{Z} : \ M - H < y \leq M\}, \qquad \mathcal{D} := \{d \in \mathbb{Z} : \ R < d \leq 2R\}.$$

Thus $|\mathcal{Y}| = H$ and $|\mathcal{D}| \asymp R \asymp \sqrt{M}$.

For $n \in \mathcal{I}_M$ define the nonnegative weight

$$S(n) := \sum_{\substack{y \in \mathcal{Y} \\ y \not\equiv n \pmod 2}} \ \sum_{\substack{d \in \mathcal{D} \\ d \mid (n - y^2)}} 1. \tag{2}$$

The parity restriction ensures $n - y^2$ is odd; hence if $d \mid (n - y^2)$ then d and $(n - y^2)/d$ have the same parity, so $n - y^2$ factors as $(x - z)(x + z)$ with $x, z \in \mathbb{Z}$.

Lemma 1 (Positivity of $S(n)$ implies a bounded representation)**.** *There exists M_0 such that for all $M \geq M_0$ and all $n \in \mathcal{I}_M$, if $S(n) > 0$ then n admits a representation* (1)*.*

Proof. Assume $S(n) > 0$. Then there exist $y \in \mathcal{Y}$ and $d \in \mathcal{D}$ with $d \mid t := n - y^2$ and t odd. Put $a = d$ and $b = t/d$. Then $t = ab$ and $a \equiv b \pmod 2$. Set

$$x := \frac{a+b}{2}, \qquad z := \frac{b-a}{2},$$

so $t = x^2 - z^2$ and hence $n = x^2 + y^2 - z^2$.

It remains to check $x, y, z \leq \lfloor \sqrt{n} \rfloor$. Since $y \in (M - H, M]$ and $n \leq (M+1)^2$,

$$0 < t = n - y^2 \leq (M+1)^2 - (M-H)^2 = 2MH - H^2 + 2M + 1 \ll M^{3/2}.$$

As $d > R \asymp \sqrt{M}$, we have $b = t/d \ll M$, while $a = d \ll \sqrt{M}$. With the fixed choice $H = \lfloor \sqrt{M}/100 \rfloor$, a direct computation shows that for all M sufficiently large,

$$b \leq 2M - a \qquad \text{and} \qquad b \leq 2M,$$

hence $a + b \leq 2M$ and therefore

$$x = \frac{a+b}{2} \leq M, \qquad z = \frac{b-a}{2} \leq M.$$

Also $y \leq M$. Since $n > M^2$, we have $M \leq \lfloor \sqrt{n} \rfloor$, hence $x, y, z \leq \lfloor \sqrt{n} \rfloor$, proving (1). ☐

2.3 First moment

Summing (2) over $n \in \mathcal{I}_M$ and switching the order of summation gives

$$\sum_{n \in \mathcal{I}_M} S(n) = \sum_{y \in \mathcal{Y}} \ \sum_{d \in \mathcal{D}} \#\{n \in \mathcal{I}_M : \ n \equiv y^2 \pmod d\} \ + \ O(HR),$$

where the $O(HR)$ term accounts for the parity restriction and boundary effects.

For each fixed (y,d), the congruence class $n \equiv y^2 \pmod{d}$ hits the interval $\mathcal{I}_M$ with frequency $1/d$, hence

$$\#\{n \in \mathcal{I}_M :\ n \equiv y^2 \pmod{d}\} = \frac{L}{d} + O(1).$$

Therefore

$$\sum_{n \in \mathcal{I}_M} S(n) = L \cdot H \sum_{d \in \mathcal{D}} \frac{1}{d} \ +\ O(H|\mathcal{D}| + HR). \tag{3}$$

Since $\sum_{R<d\le 2R} \frac{1}{d} = \log 2 + O(1/R)$ and $|\mathcal{D}| \asymp R$,

$$\mathbb{E}_{\mathcal{I}_M}[S] := \frac{1}{L} \sum_{n \in \mathcal{I}_M} S(n) = H(\log 2 + o(1)) \asymp \sqrt{M}. \tag{4}$$

2.4 Second moment via a dual large sieve

Write the divisibility indicator using additive characters:

$$\mathbf{1}_{d|(n-y^2)} = \frac{1}{d} \sum_{a \bmod d} e\!\left(\frac{a(n-y^2)}{d}\right).$$

Define the centered fluctuation

$$E(n) := S(n) - \mu_M, \qquad \mu_M := H \sum_{d \in \mathcal{D}} \frac{1}{d},$$

so that $E(n)$ involves only the nonzero frequencies $a \neq 0$.

A standard dual large sieve inequality for additive characters (see, e.g., [9, Ch. 7]) yields

$$\sum_{n \in \mathcal{I}_M} |E(n)|^2 \ \ll\ (L + R^2) \sum_{d \in \mathcal{D}} \sum_{a \bmod d} \frac{|G(a;d)|^2}{d^2}, \tag{5}$$

where

$$G(a;d) := \sum_{y \in \mathcal{Y}} e\!\left(-\frac{ay^2}{d}\right).$$

We bound $\sum_{a \bmod d} |G(a;d)|^2$ by orthogonality:

$$\sum_{a \bmod d} |G(a;d)|^2 = \sum_{y_1,y_2 \in \mathcal{Y}} \sum_{a \bmod d} e\!\left(\frac{a(y_2^2 - y_1^2)}{d}\right) = d \cdot \#\{(y_1,y_2) \in \mathcal{Y}^2 :\ y_1^2 \equiv y_2^2 \pmod{d}\}.$$

Since $d \in \mathcal{D}$ implies $d > R \geq \sqrt{M} - 1$ while $H \leq \sqrt{M}/100$, we have $H < d$. Thus, for fixed $y_1 \in \mathcal{Y}$, the congruences $y_2 \equiv \pm y_1 \pmod{d}$ can have at most one solution $y_2 \in \mathcal{Y}$ each, and hence

$$\#\{(y_1,y_2) \in \mathcal{Y}^2 :\ y_1^2 \equiv y_2^2 \pmod{d}\} \leq 2H.$$

Consequently,

$$\sum_{a \bmod d} |G(a;d)|^2 \leq 2Hd.$$

Inserting this into (5) gives

$$\sum_{n\in\mathcal{I}_M} |E(n)|^2 \;\ll\; (L+R^2)\sum_{d\in\mathcal{D}} \frac{H}{d} \;\ll\; (L+R^2)\,H,$$

since $\sum_{d\in\mathcal{D}} 1/d \ll 1$. As $L \asymp M$ and $R^2 \asymp M$, this yields

$$\sum_{n\in\mathcal{I}_M} |E(n)|^2 \;\ll\; M\,H \;\asymp\; M^{3/2}. \tag{6}$$

Dividing by $L \asymp M$ we obtain the variance bound

$$\mathrm{Var}_{\mathcal{I}_M}(S) := \frac{1}{L}\sum_{n\in\mathcal{I}_M} |S(n)-\mathbb{E}_{\mathcal{I}_M}[S]|^2 \;\ll\; H \;\asymp\; \sqrt{M}. \tag{7}$$

2.5 Chebyshev and the exceptional set

From (4) and (7), the mean satisfies $\mathbb{E}_{\mathcal{I}_M}[S] \asymp \sqrt{M}$ while the variance is $O(\sqrt{M})$. By Chebyshev's inequality,

$$\#\{n\in\mathcal{I}_M:\ S(n)=0\} \le \#\Big\{n\in\mathcal{I}_M:\ |S(n)-\mathbb{E}_{\mathcal{I}_M}[S]| \ge \tfrac{1}{2}\mathbb{E}_{\mathcal{I}_M}[S]\Big\} \ll \frac{L\cdot\mathrm{Var}_{\mathcal{I}_M}(S)}{(\mathbb{E}_{\mathcal{I}_M}[S])^2} \ll \frac{M\cdot\sqrt{M}}{M} \ll \sqrt{M}.$$

Hence all but $O(\sqrt{M})$ integers in the shell $\mathcal{I}_M$ have $S(n)>0$ and therefore satisfy (1) by Lemma 1.

Summing over $M \le \sqrt{N}$ gives

$$E(N) := \#\{1\le n\le N:\ n \text{ fails to satisfy (1)}\} \ll \sum_{M\le\sqrt{N}} \sqrt{M} \ll N^{3/4}.$$

This proves Theorem 1.

3 Concluding notes: what is known here and what remains

The proof in §2 is entirely elementary and yields a quantitative density-one statement, Theorem 1. It is natural to ask whether one can upgrade the exceptional-set bound $E(N) \ll N^{3/4+\varepsilon}$ to the stronger assertion that only finitely many integers fail (1). Our method does not appear flexible enough to achieve this: it controls only the first two moments of an auxiliary weight and hence cannot preclude a thin infinite exceptional sequence.

A conceptually different route is to work with a nonnegative weighted count $\Gamma_W(n)$ supported on a fixed real patch of $\{Q=1\}$ and to seek pointwise positivity $\Gamma_W(n)>0$ for all large n. In the δ–method (or circle method) framework this leads to two complementary tasks.

Task A (main term/local densities). One identifies the arithmetic main term with an Euler product of p-adic local densities (a singular series). For $Q = x^2+y^2-z^2$ there are no local obstructions, so these local factors are positive. Making this effective requires uniform control of the product as n varies, and a careful treatment of finitely many bad primes.

Task B (off-diagonal/spectral cancellation). After Poisson summation, the off-diagonal is governed by dyadic sums of Kloosterman–Salié sums with a half-integral weight (theta-multiplier) structure. Bounding these sums uniformly in the relevant transition regime leads to the Kuznetsov–Proskurin trace formula and delicate spectral estimates. Obtaining a pointwise bound strong enough to ensure $E(n) = o(M(n))$ for every large n remains the central analytic obstacle.

We expect that any proof of the full Erdős statement will require genuinely new uniform input beyond what is needed for density-one results, either on the analytic side (transition-range cancellation) or via an alternative geometric/dynamical principle that forces integral points into a fixed real patch for every large n.

References

[1] Y. Benoist and H. Oh, *Effective equidistribution of S-integral points on symmetric varieties*, Ann. Inst. Fourier (Grenoble) **62** (2012), no. 5, 1889–1942.

[2] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. **92** (1988), no. 1, 73–90.

[3] W. Duke, Z. Rudnick, and P. Sarnak, *Density of integer points on affine homogeneous varieties*, Duke Math. J. **71** (1993), no. 1, 143–179.

[4] E. Lindenstrauss, P. Michel, and A. Venkatesh, *Duke's theorem and branching laws for representations of* $\mathrm{SL}_2(\mathbb{R})$, Ann. of Math. (2) **176** (2012), no. 2, 863–921.

[5] A. Gorodnik and A. Nevo, *The ergodic theory of lattice subgroups*, Annals of Mathematics Studies, vol. 172, Princeton Univ. Press, 2010.

[6] D. R. Heath-Brown, *A new form of the circle method, and its application to quadratic forms*, J. Reine Angew. Math. **481** (1996), 149–206.

[7] Z. Huang, *Quantitative strong approximation for ternary quadratic forms II*, preprint, arXiv:2412.05903.

[8] Z. Huang, *Quantitative strong approximation for ternary quadratic forms III*, preprint, arXiv:2512.13091.

[9] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc. Colloq. Publ., vol. 53, AMS, 2004.

[10] H. Oh and N. Shah, *Equidistribution and counting for orbits of geometrically finite hyperbolic groups*, J. Amer. Math. Soc. **26** (2013), no. 2, 511–562.

[11] P. Sarnak and J. Tsimerman, *On Linnik and Selberg's conjecture about sums of Kloosterman sums*, in *Algebra, Arithmetic, and Geometry: in honor of Yu. I. Manin*, Vol. I, Progress in Math. 269, Birkhäuser, 2009, 619–635 (see also earlier notes/versions by the authors).

[12] Y. Sun, *Sums of Kloosterman sums with half-integral weight multipliers*, preprint, arXiv:2305.19651.

[13] T. Bloom Erdős Problems, *Problem #1148*, `https://www.erdosproblems.com/1148`.