Bounded Representations by $x^2 + y^2 - z^2$

Przemyslaw Chojecki

March 16, 2026

Abstract

We prove that every sufficiently large integer n can be written in the form

$$n = x^2 + y^2 - z^2, \qquad \max(x^2, y^2, z^2) \le n.$$

The proof converts the problem into finding a primitive binary quadratic form of positive discriminant $4n$ inside a fixed relatively compact open patch of the real hyperboloid $b^2 - 4ac = 4n$. This is then supplied by Duke's theorem in the precise point-counting form deduced from the measure-theoretic duality of Einsiedler–Lindenstrauss–Michel–Venkatesh. A finite parity correction returns to the original ternary variables. This settles Erdős Problem 1148.

1 Introduction

Let

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

We shall prove the following which is Erdős Problem 1148 ([1]):

Theorem 1.1. *There exists N such that every integer $n \ge N$ admits integers x, y, z with*

$$n = x^2 + y^2 - z^2, \qquad \max(x^2, y^2, z^2) \le n.$$

The key point is that the bounded representation problem for Q is equivalent, after a linear change of variables, to a point-picking problem for primitive binary quadratic forms of discriminant $4n$. Duke's theorem gives equidistribution of such forms on the one-sheeted hyperboloid attached to the discriminant form. A short parity argument then recovers the integral triple (x, y, z).

For a positive integer d we write

$$R^*_{\mathrm{disc}}(d) := \{(a, b, c) \in \mathbb{Z}^3 : b^2 - 4ac = d,\ \gcd(a, b, c) = 1\}.$$

This is exactly the set denoted $R_{\mathrm{disc}}(d)$ in [2]; the superscript $*$ is only to emphasize primitivity. We also set

$$V_{\mathrm{disc},+1}(\mathbb{R}) := \{(A, B, C) \in \mathbb{R}^3 : B^2 - 4AC = 1\}.$$

2 From ternary representations to discriminant points

Write $[a, b, c]$ for the binary quadratic form

$$q_{a,b,c}(u, v) = au^2 + buv + cv^2.$$

The following linear dictionary is immediate.

Lemma 2.1. *Let $n \geq 1$ and let $(a, b, c) \in \mathbb{Z}^3$ satisfy*

$$b^2 - 4ac = 4n, \qquad b \equiv 0 \pmod 2, \qquad a \equiv c \pmod 2.$$

Then

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

are integers and satisfy

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

Conversely, every integer solution of $x^2 + y^2 - z^2 = n$ arises in this way from

$$a = x + z, \qquad b = 2y, \qquad c = z - x.$$

Proof. A direct computation gives

$$x^2 + y^2 - z^2 = \frac{(a-c)^2 + b^2 - (a+c)^2}{4} = \frac{b^2 - 4ac}{4} = n.$$

The converse is the same identity in reverse. □

Thus the problem is to find a discriminant point with the stated parity and lying in a suitable box. Define

$$\mathcal{K} := \Big\{(A, B, C) \in V_{\mathrm{disc},+1}(\mathbb{R}) : |A - C| < 1,\ |B| < 1,\ |A + C| < 1\Big\}. \tag{2.1}$$

This set is open and relatively compact in $V_{\mathrm{disc},+1}(\mathbb{R})$: indeed the inequalities on $A - C$, B and $A + C$ bound A, B and C individually.

If (a, b, c) satisfies the congruences in Lemma 2.1 and

$$\left(\frac{a}{2\sqrt{n}}, \frac{b}{2\sqrt{n}}, \frac{c}{2\sqrt{n}}\right) \in \mathcal{K},$$

then the corresponding (x, y, z) obeys

$$\left|\frac{x}{\sqrt{n}}\right| = \left|\frac{a-c}{2\sqrt{n}}\right| < 1, \qquad \left|\frac{y}{\sqrt{n}}\right| = \left|\frac{b}{2\sqrt{n}}\right| < 1, \qquad \left|\frac{z}{\sqrt{n}}\right| = \left|\frac{a+c}{2\sqrt{n}}\right| < 1.$$

Hence $|x|, |y|, |z| < \sqrt{n}$, so

$$\max(x^2, y^2, z^2) < n.$$

For non-square n this is stronger than the desired bound $\leq n$.

3 Three elementary coefficient moves

Define operators on binary quadratic forms by

$$(Tq)(u, v) := q(u + v, v), \qquad (Sq)(u, v) := q(-v, u).$$

Then

$$T[a, b, c] = [a, b + 2a, a + b + c], \qquad S[a, b, c] = [c, -b, a]. \tag{3.1}$$

We also write

$$U := T \circ S,$$

so that

$$U[a, b, c] = [c, -b + 2c, a - b + c]. \tag{3.2}$$

Each of T, S, U preserves integrality and discriminant.

The only congruence obstruction needed for Lemma 2.1 is disposed of by a finite case split.

Lemma 3.1. *Suppose* $(a,b,c) \in \mathbb{Z}^3$ *satisfies*

$$b^2 - 4ac \equiv 0 \pmod 4.$$

Then b *is even, and at least one of the three forms*

$$[a,b,c], \qquad T[a,b,c], \qquad U[a,b,c]$$

has first and third coefficients of the same parity.

Proof. From $b^2 \equiv 4ac \pmod 4$ we get $b^2 \equiv 0 \pmod 4$, hence b is even. If $a \equiv c \pmod 2$, then the original form already has first and third coefficients of the same parity.

Assume now that $a \not\equiv c \pmod 2$, so a and c have opposite parity. If c is even, then a is odd and the third coefficient of $T[a,b,c]$ satisfies

$$a+b+c \equiv a+c \equiv 1 \pmod 2,$$

so $T[a,b,c]$ has first and third coefficients of the same parity. If instead a is even, then c is odd and the third coefficient of $U[a,b,c]$ satisfies

$$a-b+c \equiv a+c \equiv 1 \pmod 2,$$

so $U[a,b,c]$ has first and third coefficients of the same parity. □

We now choose a small patch of $V_{\mathrm{disc},+1}(\mathbb{R})$ that stays inside $\mathcal{K}$ under the relevant moves. Set

$$P_0 := \left(\frac{2}{5}, -\frac{2}{5}, -\frac{21}{40}\right) \in V_{\mathrm{disc},+1}(\mathbb{R}).$$

Indeed,

$$\left(-\frac{2}{5}\right)^2 - 4 \cdot \frac{2}{5} \cdot \left(-\frac{21}{40}\right) = 1.$$

Using (3.1) and (3.2),

$$T(P_0) = \left(\frac{2}{5}, \frac{2}{5}, -\frac{21}{40}\right), \qquad U(P_0) = \left(-\frac{21}{40}, -\frac{13}{20}, \frac{11}{40}\right).$$

A direct check shows that all three points belong to $\mathcal{K}$: for P_0 and $T(P_0)$ one has

$$|A-C| = \frac{37}{40}, \qquad |B| = \frac{2}{5}, \qquad |A+C| = \frac{1}{8},$$

while for $U(P_0)$ one has

$$|A-C| = \frac{4}{5}, \qquad |B| = \frac{13}{20}, \qquad |A+C| = \frac{1}{4}.$$

Since $\mathcal{K}$ is open and the maps $T, U : V_{\mathrm{disc},+1}(\mathbb{R}) \to V_{\mathrm{disc},+1}(\mathbb{R})$ are continuous, there exists a nonempty open relatively compact neighborhood

$$P_0 \in \Omega \Subset V_{\mathrm{disc},+1}(\mathbb{R}) \tag{3.3}$$

such that

$$\overline{\Omega} \subset \mathcal{K}, \qquad T(\overline{\Omega}) \subset \mathcal{K}, \qquad U(\overline{\Omega}) \subset \mathcal{K}. \tag{3.4}$$

4 Duke's theorem in the needed point-counting form

Let

$$G = \mathrm{PGL}_2(\mathbb{R}), \qquad \Gamma = \mathrm{PGL}_2(\mathbb{Z}),$$

and let $A \subset G$ be the diagonal torus. Following [2, §2.4], the homogeneous space G/A is identified with $V_{\mathrm{disc},+1}(\mathbb{R})$; under this identification the base point is $q_0 = (0,1,0) \in V_{\mathrm{disc},+1}(\mathbb{R})$, corresponding to the form uv. The G-invariant Radon measure on G/A transports to a positive G-invariant Radon measure on $V_{\mathrm{disc},+1}(\mathbb{R})$, which we denote by $\mu_{\mathrm{disc},+1}$. The measure $\mu_{\mathrm{disc},+1}$ is the pushforward of the G-invariant quotient measure on G/A under the identification described in [2, §2.4]. This agrees with the cone measure $\mu_{\mathrm{disc},+1}$ used in [2] up to a positive scalar normalization, which is irrelevant for the equidistribution statements used below.

For each $x = (a,b,c) \in R^*_{\mathrm{disc}}(d)$ choose $g_x \in G$ with

$$g_x \cdot q_0 = d^{-1/2} x.$$

ELMV define a discrete measure on G/A by

$$\lambda_d := \sum_{x \in R^*_{\mathrm{disc}}(d)} \delta_{g_x A/A}$$

(see [2, Eq. (2.8) and the paragraph following it]). Via the measure-theoretic duality of [2, Eq. (2.8)], this corresponds to a measure ν_d on $\Gamma\backslash G$ supported on the union G_d of closed A-orbits attached to discriminant-d forms. ELMV prove that

$$\mu_d := \frac{1}{\mathrm{vol}(G_d)} \nu_d$$

converges weak-* to Haar measure on $\Gamma\backslash G$ as $d \to \infty$ through positive non-square discriminants; this is their Theorem 2.3.

For positive discriminant $d > 0$ the set $R^*_{\mathrm{disc}}(d)$ of primitive binary quadratic forms of discriminant d is infinite. However, if ϕ is compactly supported on $V_{\mathrm{disc},+1}(\mathbb{R})$, then only finitely many points of the scaled set

$$\frac{1}{\sqrt{d}} R^*_{\mathrm{disc}}(d)$$

lie in $\mathrm{supp}(\phi)$. Indeed, $\mathrm{supp}(\phi)$ is contained in a compact region of the one-sheeted hyperboloid $V_{\mathrm{disc},+1}(\mathbb{R})$, and the lattice $V_{\mathrm{disc}}(\mathbb{Z})$ intersects any compact subset of $V_{\mathrm{disc}}(\mathbb{R})$ in finitely many points. Consequently the sum defining $\Lambda_d(\phi)$ below is finite.

The precise consequence we need is the following.

Proposition 4.1 (Point-counting consequence of Duke–ELMV). *Let $\phi \in C_c(V_{\mathrm{disc},+1}(\mathbb{R}))$. For every positive discriminant d define*

$$\Lambda_d(\phi) := \sum_{(a,b,c) \in R^*_{\mathrm{disc}}(d)} \phi\left(\frac{a}{\sqrt{d}}, \frac{b}{\sqrt{d}}, \frac{c}{\sqrt{d}}\right).$$

Then, as $d \to \infty$ through positive non-square discriminants,

$$\Lambda_d(\phi) = \mathrm{vol}(G_d)\big(\mu_{\mathrm{disc},+1}(\phi) + o_\phi(1)\big).$$

In particular, if $\phi \geq 0$ and $\phi \not\equiv 0$, then $\Lambda_d(\phi) > 0$ for all sufficiently large positive non-square discriminants d.

Proof. Let $\widetilde{\phi} \in C_c(G/A)$ correspond to ϕ under the identification $G/A \simeq V_{\mathrm{disc},+1}(\mathbb{R})$. ELMV note just after Theorem 2.3 that every function in $C_c(G/A)$ is of the form F_A for some $F \in C_c(G)$, where

$$F_A(gA) := \int_A F(gh)\, d\mu_A(h).$$

Choose such an F with $F_A = \widetilde{\phi}$.

By construction of λ_d and the choice of g_x,

$$\Lambda_d(\phi) = \lambda_d(\widetilde{\phi}).$$

Now let

$$F_\Gamma(\Gamma g) := \sum_{\gamma \in \Gamma} F(\gamma g),$$

which is compactly supported on $\Gamma\backslash G$. The measure correspondence in [2, Eq. (2.8)] gives

$$\lambda_d(\widetilde{\phi}) = \nu_d(F_\Gamma).$$

Since $\mu_d = \nu_d / \operatorname{vol}(G_d)$ and $\mu_d \to \mu_{\Gamma\backslash G}$ weak-*, ELMV Theorem 2.3 yields

$$\nu_d(F_\Gamma) = \operatorname{vol}(G_d)\big(\mu_{\Gamma\backslash G}(F_\Gamma) + o_\phi(1)\big).$$

Transporting $\mu_{\Gamma\backslash G}$ back through the same measure correspondence and then through $G/A \simeq V_{\mathrm{disc},+1}(\mathbb{R})$ gives

$$\mu_{\Gamma\backslash G}(F_\Gamma) = \mu_{\mathrm{disc},+1}(\phi).$$

Combining the last three displays proves the asymptotic formula.

For the final claim, note that $\mu_{\mathrm{disc},+1}$ is a positive Radon measure with full support on $V_{\mathrm{disc},+1}(\mathbb{R})$, because it is induced from Haar measure on the homogeneous space G/A. Hence $\mu_{\mathrm{disc},+1}(\phi) > 0$ whenever $\phi \geq 0$ and $\phi \not\equiv 0$. The asymptotic formula then forces $\Lambda_d(\phi) > 0$ for all sufficiently large positive non-square d. □

Corollary 4.2. *Let $\mathcal{U} \subset V_{\mathrm{disc},+1}(\mathbb{R})$ be a nonempty open relatively compact set. Then, for all sufficiently large positive non-square discriminants d,*

$$d^{-1/2} R^*_{\mathrm{disc}}(d) \cap \mathcal{U} \neq \varnothing.$$

Proof. Choose $\phi \in C_c(V_{\mathrm{disc},+1}(\mathbb{R}))$ with $\phi \geq 0$, $\phi \not\equiv 0$, and $\operatorname{supp}(\phi) \subset \mathcal{U}$. Then Proposition 4.1 gives $\Lambda_d(\phi) > 0$ for all large positive non-square d, which means exactly that the scaled set $d^{-1/2} R^*_{\mathrm{disc}}(d)$ meets $\mathcal{U}$. □

5 Proof of the main theorem

Proof of Theorem 1.1. If $n = m^2$ is a square, then

$$n = m^2 + 0^2 - 0^2,$$

so the desired bound is immediate. It remains to treat non-square n.

Let n be sufficiently large and non-square, and set $d = 4n$. Then d is a positive non-square discriminant. By Corollary 4.2 applied to the open set Ω from (3.3)–(3.4), there exists a primitive triple $(a, b, c) \in R^*_{\mathrm{disc}}(4n)$ such that

$$\left(\frac{a}{2\sqrt{n}}, \frac{b}{2\sqrt{n}}, \frac{c}{2\sqrt{n}} \right) \in \Omega.$$

Because $4n \equiv 0 \pmod 4$, Lemma 3.1 shows that at least one of the three forms

$$[a, b, c], \qquad T[a, b, c], \qquad U[a, b, c]$$

has first and third coefficients of the same parity; in each case the middle coefficient is even. Let $[a', b', c']$ denote such a form. Since T and U preserve discriminant, we still have

$$b'^2 - 4a'c' = 4n, \qquad b' \equiv 0 \pmod 2, \qquad a' \equiv c' \pmod 2.$$

Moreover, by (3.4) the scaled point

$$\left(\frac{a'}{2\sqrt{n}}, \frac{b'}{2\sqrt{n}}, \frac{c'}{2\sqrt{n}}\right)$$

lies in $\mathcal{K}$.

Lemma 2.1 therefore gives integers

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

with

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

Since the scaled point lies in $\mathcal{K}$, Section 2 shows that

$$|x|, |y|, |z| < \sqrt{n},$$

whence

$$\max(x^2, y^2, z^2) < n.$$

This proves the theorem for all sufficiently large non-square n, and hence for all sufficiently large integers n. □

Remark 5.1. *The proof is qualitative: it supplies a threshold N but does not make it explicit.*

References

[1] T. F. Bloom, *Erdos Problem 1148*, https://www.erdosproblems.com/1148

[2] M. Einsiedler, E. Lindenstrauss, P. Michel, and A. Venkatesh, *The distribution of closed geodesics on the modular surface, and Duke's theorem*, Enseign. Math. (2) **58** (2012), no. 3–4, 249–313. doi:10.4171/LEM/58-3-2.