Integral points on norm–one tori and the Erdős unit–distance exponent

Abstract

For a finite planar set $P \subset \mathbb{R}^2$ let $u(P)$ denote the number of unordered pairs of points of P at Euclidean distance exactly 1, and write $u(n) = \max\{u(P) : |P| = n\}$. Erdős, in 1946, conjectured the upper bound $u(n) \leq n^{1+O(1/\log\log n)}$. We refute this conjecture: along an infinite sequence of integers n,

$$u(n) \;\geq\; n^{\,1+c_0\,\dfrac{\log\log\log n}{\log\log n}}$$

with $c_0 > 0$ an absolute constant. Our point sets are produced by projecting $\mathcal{O}_K^2$ to $\mathbb{R}^2$ via a single real embedding of a number field K drawn from an infinite unramified tower of mixed signature and bounded root discriminant. The unit–distance pairs come from $\mathcal{O}_K$–points of the affine conic $u^2+v^2 = 1$, which form a group of rank $r_2(K)$ — a fixed positive fraction of $d = [K : \mathbb{Q}]$. Applying van der Corput's theorem turns this rank into $e^{\Omega(d\log\log d)}$ unit–distance directions, which dominates the remaining $e^{O(d)}$ losses.

Contents

1. Introduction

For a finite set $P \subset \mathbb{R}^2$ define the unit–distance count

$$u(P) = \#\big\{\{p,q\} \subset P : \|p-q\| = 1\big\}, \qquad u(n) = \max_{|P|=n} u(P).$$

Erdős observed in 1946 that the $\sqrt{n} \times \sqrt{n}$ integer grid, after a suitable rescaling, satisfies $u(n) \geq n^{1+c/\log\log n}$ for some absolute $c > 0$, and conjectured that this was essentially the truth:

$$u(n) \;\leq\; n^{1+O(1/\log\log n)}. \tag{1}$$

On the upper–bound side, the best result to date is the Spencer–Szemerédi–Trotter bound $u(n) = O(n^{4/3})$.

Theorem 1.1. *The inequality (1) fails. More precisely, there are absolute constants $c_0 > 0$ and n_0 and an infinite set $\mathcal{N} \subset \mathbb{Z}_{\geq n_0}$ for which*

$$u(n) \;\geq\; n^{\,1+c_0 \frac{\log\log\log n}{\log\log n}} \qquad (n \in \mathcal{N}).$$

In particular, given any $C > 0$, there are infinitely many n with $u(n) > n^{1+C/\log\log n}$.

The second statement follows from the first since $\log\log\log n$ tends to infinity. Our construction does not threaten the Spencer–Szemerédi–Trotter ceiling: the exponent we produce is $1 + o(1)$.

Idea of the proof. What drives Erdős's grid is the fact that the Gaussian integers $\mathbb{Z}[i]$ contain many elements of a fixed norm; the supply, however, is controlled by the divisor function, and so is at most $\exp\big(O(\log n/\log\log n)\big)$ for any norm value. We exchange $\mathbb{Z}[i]$ for the ring of integers $\mathcal{O}_K$ of a number field K of large degree d with at least one real embedding and $r_2 \asymp d$ complex places. In this regime the norm–one torus $\{u^2 + v^2 = 1\}$ acquires *infinitely many* $\mathcal{O}_K$–rational points, organized into a group of rank r_2. Choosing a real embedding $\sigma : K \hookrightarrow \mathbb{R}$ projects each such point to an honest unit vector in $\mathbb{R}^2$, and van der Corput's theorem furnishes at least $T^{r_2}/R^{(1)}$ points with every archimedean valuation in $[e^{-T}, e^{T}]$, where $R^{(1)}$ is the covolume of the relevant logarithm lattice. Picking K along an infinite class–field tower keeps the root discriminant bounded; Louboutin's bound on $\mathrm{Res}_{s=1}\,\zeta_{K(i)}$ together with Zimmert's regulator estimate then limit $R^{(1)} \leq e^{O(d)}$. With $T \asymp \log d$ this yields $e^{\Omega(d\log\log d)}$ unit directions, dwarfing the other losses, which are only $e^{O(d)}$.

2. Number–theoretic preliminaries

2.1. Number fields, places, and the Minkowski embedding

Let K be a number field of degree $d = [K : \mathbb{Q}]$ with ring of integers $\mathcal{O}_K$. Denote its real embeddings by $\sigma_1, \dots, \sigma_{r_1}$ and its pairs of complex embeddings by $\tau_1, \bar{\tau}_1, \dots, \tau_{r_2}, \bar{\tau}_{r_2}$, so that $d = r_1 + 2r_2$. We write w for a generic archimedean place of K, setting $n_w = 1$ if w is real and $n_w = 2$ if w is complex, and $|x|_w$ for the corresponding normalized absolute value ($|x|_{\sigma_k} = |\sigma_k(x)|$ and $|x|_{\tau_j} = |\tau_j(x)|$). The product formula then reads $\prod_w |x|_w^{n_w} = |\,\mathrm{N}_{K/\mathbb{Q}}(x)|$ for $x \in K^\times$.

The *Minkowski embedding*

$$\iota : K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^d, \qquad x \longmapsto \big(\sigma_1(x), \dots, \sigma_{r_1}(x), \tau_1(x), \dots, \tau_{r_2}(x)\big),$$

identifies $\mathcal{O}_K$ with a full–rank lattice of covolume $2^{-r_2}|\Delta_K|^{1/2}$, where $\Delta_K = \mathrm{disc}(K/\mathbb{Q})$; see, for example, Neukirch, *Algebraic Number Theory*, Springer 1999, Prop. I.5.2.

For $R > 0$ define

$$B_R \;:=\; \big\{\, x \in \mathcal{O}_K : \; |x|_w \le R \text{ for every archimedean } w \,\big\}.$$

The defining region of B_R under ι is the convex, origin–symmetric body $[-R, R]^{r_1} \times \{|z| \le R\}^{r_2} \subset \mathbb{R}^d$, whose volume is

$$\mathrm{vol}\big([-R,R]^{r_1} \times \{|z| \le R\}^{r_2}\big) \;=\; (2R)^{r_1}(\pi R^2)^{r_2} \;=\; 2^{r_1}\pi^{r_2} R^d. \tag{2}$$

2.2. The norm–one torus and its logarithm lattice

Henceforth assume $r_1 \ge 1$, which in particular forces $i \notin K$ (any totally real embedding would send i into $\mathbb{R}$). Set $L := K(i)$, a quadratic extension of degree $2d$, with non–trivial Galois element $\eta \mapsto \bar{\eta}$; on the level of generators $\overline{a + bi} = a - bi$ for $a, b \in K$. Because i is imaginary, all archimedean places of L are complex, and we label them as follows.

Lemma 2.1. *The archimedean places of L split as:*

- *For each real embedding σ_k of K, a single complex place $\tilde{\sigma}_k$ of L, represented by $\sigma_k^+ : a + bi \mapsto \sigma_k(a) + i\sigma_k(b)$.*
- *For each complex embedding τ_j of K, two complex places $\tilde{\tau}_j^{(1)}, \tilde{\tau}_j^{(2)}$ of L, represented by $\tau_j^\pm : a + bi \mapsto \tau_j(a) \pm i\tau_j(b)$ respectively.*

In total L has $r_1 + 2r_2 = d$ complex places, so $r_1(L) = 0$ and $r_2(L) = d$. Furthermore, for every $\eta \in L$,

$$|\bar{\eta}|_{\tilde{\sigma}_k} = |\eta|_{\tilde{\sigma}_k}, \qquad |\bar{\eta}|_{\tilde{\tau}_j^{(1)}} = |\eta|_{\tilde{\tau}_j^{(2)}}. \tag{3}$$

Proof. Any embedding $\psi : K \hookrightarrow \mathbb{C}$ has two extensions $\psi^\pm : L \to \mathbb{C}$ specified by $\psi^\pm(i) = \pm i$, and complex conjugation on $\mathbb{C}$ takes ψ^+ to $\overline{\psi}^-$. When $\psi = \sigma_k$ is real, $\overline{\sigma_k} = \sigma_k$, so $\sigma_k^\pm$ are complex conjugates and define a single place. When $\psi = \tau_j$ is complex, $\overline{\tau_j} = \bar{\tau}_j$, so the two conjugate pairs $\{\tau_j^+, \bar{\tau}_j^-\}$ and $\{\tau_j^-, \bar{\tau}_j^+\}$ yield two distinct places. Finally, the identity $\psi^+(\bar{\eta}) = \psi^+(a - bi) = \psi(a) - i\psi(b) = \psi^-(\eta)$ gives (3). $\square$

Definition 2.2. Set $U^{(1)} := \{\zeta \in \mathcal{O}_L^\times : \ \mathrm{N}_{L/K}(\zeta) = \zeta\bar{\zeta} = 1\}$.

Lemma 2.3. *$U^{(1)}$ is a finitely generated abelian group of rank r_2. Moreover, every $\zeta \in U^{(1)}$ satisfies $|\zeta|_{\tilde{\sigma}_k} = 1$ for all k and $|\zeta|_{\tilde{\tau}_j^{(1)}} \cdot |\zeta|_{\tilde{\tau}_j^{(2)}} = 1$ for all j.*

Proof. By definition, $U^{(1)}$ is the kernel of $\mathrm{N} : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$. Its image contains $(\mathcal{O}_K^\times)^2$ — because $\mathrm{N}(\epsilon) = \epsilon^2$ whenever $\epsilon \in \mathcal{O}_K^\times \subset \mathcal{O}_L^\times$ — and so has finite index in $\mathcal{O}_K^\times$. Dirichlet's unit theorem gives $\operatorname{rank} \mathcal{O}_L^\times = r_2(L) - 1 = d - 1$ and $\operatorname{rank} \mathcal{O}_K^\times = r_1 + r_2 - 1$; subtracting, $\operatorname{rank} U^{(1)} = (d-1) - (r_1 + r_2 - 1) = r_2$. For the valuation identities, $\zeta\bar{\zeta} = 1$ combined with (3) gives $|\zeta|_{\tilde{\sigma}_k}^2 = |\zeta|_{\tilde{\sigma}_k}|\bar{\zeta}|_{\tilde{\sigma}_k} = |\zeta\bar{\zeta}|_{\tilde{\sigma}_k} = 1$ and $|\zeta|_{\tilde{\tau}_j^{(1)}}|\zeta|_{\tilde{\tau}_j^{(2)}} = |\zeta|_{\tilde{\tau}_j^{(1)}}|\bar{\zeta}|_{\tilde{\tau}_j^{(1)}} = 1$. □

Definition 2.4. Introduce the *logarithm map*

$$\mathcal{L} : U^{(1)} \longrightarrow \mathbb{R}^{r_2}, \qquad \zeta \longmapsto \big(\log |\zeta|_{\tilde{\tau}_j^{(1)}}\big)_{j=1}^{r_2},$$

and write $R^{(1)} := \det\big(\mathcal{L}(U^{(1)})\big)$ for the covolume of the image lattice inside $\mathbb{R}^{r_2}$.

Lemma 2.5. *$\mathcal{L}$ is a homomorphism with finite kernel (precisely the roots of unity inside $U^{(1)}$), and its image $\mathcal{L}(U^{(1)})$ is a full–rank lattice in $\mathbb{R}^{r_2}$.*

Proof. That $\mathcal{L}$ is a homomorphism is immediate. If $\mathcal{L}(\zeta) = 0$ then combining this with Lemma 2.3 forces $|\zeta|_w = 1$ at every archimedean place of L, and Kronecker's theorem then identifies ζ as a root of unity. Thus $\ker \mathcal{L}$ is finite, and $\operatorname{rank} \mathcal{L}(U^{(1)}) = \operatorname{rank} U^{(1)} = r_2$. □

2.3. From $U^{(1)}$ to integral vectors on a circle

For any $\zeta \in L$, write $\zeta = u + iv$ with $u = \frac{1}{2}(\zeta + \bar{\zeta})$ and $v = \frac{1}{2i}(\zeta - \bar{\zeta})$ both in K.

Lemma 2.6. *The rule $\zeta \mapsto (2u, 2v)$ defines a bijection*

$$U^{(1)} \ \xrightarrow{\sim}\ \mathcal{T} := \{(a,b) \in \mathcal{O}_K^2 : \ a^2 + b^2 = 4\}.$$

Proof. Given $\zeta \in U^{(1)}$, the quantity $2u = \zeta + \bar{\zeta}$ is $\mathrm{Tr}_{L/K}(\zeta)$ and lies in $\mathcal{O}_K$, while $2vi = \zeta - \bar{\zeta} \in \mathcal{O}_L$ and, since $i \in \mathcal{O}_L^\times$, the element $2v$ lies in $\mathcal{O}_L \cap K = \mathcal{O}_K$. A direct calculation gives $(2u)^2 + (2v)^2 = 4(u^2 + v^2) = 4\zeta\bar{\zeta} = 4$, so $(2u, 2v) \in \mathcal{T}$; injectivity is plain.

For the reverse direction, take any $(a, b) \in \mathcal{T}$ and put $\zeta := \frac{1}{2}(a + bi)$. Then ζ satisfies the integral equation $X^2 - aX + \frac{1}{4}(a^2 + b^2) = X^2 - aX + 1 \in \mathcal{O}_K[X]$, hence $\zeta \in \mathcal{O}_L$. Furthermore $\zeta\bar{\zeta} = \frac{1}{4}(a^2 + b^2) = 1$, so $\zeta^{-1} = \bar{\zeta} \in \mathcal{O}_L$ and $\zeta \in U^{(1)}$. Since $(2u, 2v) = (a, b)$, the map is surjective. □

Lemma 2.7. *Let $\zeta \in U^{(1)}$ satisfy $\|\mathcal{L}(\zeta)\|_\infty \le T$, and form $(a, b) = (2u, 2v) \in \mathcal{O}_K^2$ as above. Then*

$$|a|_{\sigma_k},\ |b|_{\sigma_k} \ \le\ 2 \quad (1 \le k \le r_1), \qquad |a|_{\tau_j},\ |b|_{\tau_j} \ \le\ 2e^T \quad (1 \le j \le r_2).$$

Proof. At a real place we have $\sigma_k(u)^2 + \sigma_k(v)^2 = \sigma_k(u^2 + v^2) = 1$, so $|u|_{\sigma_k}, |v|_{\sigma_k} \le 1$. At a complex place, $\tau_j^{\pm}(\zeta) = \tau_j(u) \pm i\tau_j(v)$ gives $\tau_j(u) = \frac{1}{2}(\tau_j^+(\zeta) + \tau_j^-(\zeta))$, hence with $y_j = \log |\zeta|_{\tilde{\tau}_j^{(1)}}$,

$$|u|_{\tau_j} \ \le\ \tfrac{1}{2}\big(|\zeta|_{\tilde{\tau}_j^{(1)}} + |\zeta|_{\tilde{\tau}_j^{(2)}}\big) = \tfrac{1}{2}(e^{y_j} + e^{-y_j}) = \cosh y_j \le e^{|y_j|} \le e^T,$$

and similarly for v. □

3. Four lemmas

Throughout this section K denotes a number field of degree d with $r_1 \geq 1$ real and r_2 complex places, and we write $\gamma := \frac{1}{d}\log|\Delta_K|$ for the *logarithmic root discriminant*. Every constant below depends only on γ and on $c := r_2/d \in (0, \tfrac{1}{2}]$, never on d itself.

3.1. A packing upper bound

Lemma 3.1. *For every real $M \geq 1$, $|B_M| \;\leq\; (2M+1)^d$.*

Proof. Endow $\mathbb{R}^d \cong \mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ with the norm $\|x\|_*^2 := \sum_k |x|_{\sigma_k}^2 + 2\sum_j |x|_{\tau_j}^2 = \sum_w n_w |x|_w^2$. For any $0 \neq x \in \mathcal{O}_K$ the weighted AM–GM inequality yields

$$\frac{\|x\|_*^2}{d} = \frac{\sum_w n_w |x|_w^2}{\sum_w n_w} \;\geq\; \Big(\prod_w (|x|_w^2)^{n_w}\Big)^{1/d} = |\,\mathrm{N}_{K/\mathbb{Q}}(x)|^{2/d} \;\geq\; 1,$$

so $\|x\|_* \geq \sqrt{d}$. If in addition $x \in B_M$ then $\|x\|_*^2 \leq M^2 \sum_w n_w = dM^2$, i.e. $\|x\|_* \leq M\sqrt{d}$. Consequently the images $\iota(B_M)$ sit inside the $\|\cdot\|_*$–ball of radius $M\sqrt{d}$ and are pairwise separated by at least $\sqrt{d}$ in this norm; open $\|\cdot\|_*$–balls of radius $\sqrt{d}/2$ around them are then disjoint and contained in the ball of radius $M\sqrt{d} + \sqrt{d}/2$, so

$$|B_M| \;\leq\; \frac{\mathrm{vol}_{\|\cdot\|_*}\big(M\sqrt{d} + \frac{\sqrt{d}}{2}\big)}{\mathrm{vol}_{\|\cdot\|_*}\big(\frac{\sqrt{d}}{2}\big)} \;=\; \Big(\frac{M\sqrt{d}+\sqrt{d}/2}{\sqrt{d}/2}\Big)^d \;=\; (2M+1)^d. \qquad \square$$

3.2. A van der Corput lower bound

The following is the classical refinement of Minkowski's first theorem that we will need.

Theorem 3.2 (van der Corput)**.** *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and let $S \subset \mathbb{R}^n$ be a bounded, convex, origin–symmetric body. If $\mathrm{vol}(S) > m \cdot 2^n \det\Lambda$ for some positive integer m, then S contains at least $2m$ non–zero points of Λ; in particular $|S \cap \Lambda| \geq 2m+1$.*

Proof. See J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer 1971, Ch. III, Theorem II (p. 71); or P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, 2nd ed., North–Holland 1987, §6, Theorem 1. The original reference is J. G. van der Corput, *Acta Arith.* **2** (1936), 145–146. $\square$

Corollary 3.3. *Under the hypotheses of Theorem 3.2, if $\mathrm{vol}(S) \geq 2\cdot 2^n \det\Lambda$ then $|S\cap\Lambda| \geq \mathrm{vol}(S)/(2^n\det\Lambda)$.*

Proof. Set $m = \lfloor \mathrm{vol}(S)/(2^n\det\Lambda)\rfloor - 1 \geq 1$ when $\mathrm{vol}(S)/(2^n\det\Lambda)$ is an integer, and $m = \lfloor \mathrm{vol}(S)/(2^n\det\Lambda)\rfloor$ otherwise. In both cases $m \geq \mathrm{vol}(S)/(2^n\det\Lambda) - 1$, and so $|S\cap\Lambda| \geq 2m+1 \geq 2\,\mathrm{vol}(S)/(2^n\det\Lambda) - 1 \geq \mathrm{vol}(S)/(2^n\det\Lambda)$. $\square$

Lemma 3.4. *There exists a constant $R_0 = R_0(\gamma, c)$ such that for all $R \geq R_0$,*

$$|B_R| \;\geq\; \Big(\tfrac{\pi}{2}\Big)^{r_2} \frac{R^d}{|\Delta_K|^{1/2}}.$$

Proof. We apply Corollary 3.3 with $\Lambda = \iota(\mathcal{O}_K) \subset \mathbb{R}^d$ and $S = \iota(B_R)$. Using (2) and the identity $\det \Lambda = 2^{-r_2}|\Delta_K|^{1/2}$,

$$\frac{\mathrm{vol}(S)}{2^d \det \Lambda} = \frac{2^{r_1}\pi^{r_2}R^d}{2^d \cdot 2^{-r_2}|\Delta_K|^{1/2}} = \frac{2^{r_1+r_2}\pi^{r_2}R^d}{2^d|\Delta_K|^{1/2}} = \left(\tfrac{\pi}{2}\right)^{r_2} \frac{R^d}{|\Delta_K|^{1/2}}.$$

The requisite hypothesis $\mathrm{vol}(S) \geq 2 \cdot 2^d \det \Lambda$ is equivalent to $(\pi/2)^{r_2}R^d \geq 2|\Delta_K|^{1/2}$, that is $R \geq \left(2|\Delta_K|^{1/2}(2/\pi)^{r_2}\right)^{1/d} \leq 2^{1/d}e^{\gamma/2}(2/\pi)^c =: R_0$. □

3.3. Upper bound for $R^{(1)}$

We recall two classical inputs.

Theorem 3.5 (Louboutin)**.** *For any number field E of degree $n \geq 2$,*

$$\kappa_E := \mathrm{Res}_{s=1}\, \zeta_E(s) \;\leq\; \left(\frac{e \log |\Delta_E|}{2(n-1)}\right)^{n-1}.$$

Proof. S. Louboutin, *Explicit upper bounds for residues of Dedekind zeta functions and values of L–functions at $s = 1$, and explicit lower bounds for relative class numbers of CM–fields*, Canad. J. Math. **53** (2001), 1194–1222, Theorem 1. □

Theorem 3.6 (Zimmert)**.** *There exists an absolute constant $c_Z > 0$ for which $R_E \geq c_Z$ holds at every number field $E \neq \mathbb{Q}$ satisfying $r_1(E) + r_2(E) \geq 2$.*

Proof. R. Zimmert, *Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung*, Invent. Math. **62** (1981), 367–380, Satz 3, gives $R_E/w_E \geq 0.02\, e^{0.1\, r_2(E)}$ (in fact more); combined with $w_E \geq 2$ this yields $R_E \geq 2 \cdot 0.02 = 0.04$. One may take $c_Z = 0.04$. □

Lemma 3.7. *With $L = K(i)$ and $R^{(1)}$ as in Definition 2.4,*

$$R^{(1)} \;\leq\; \frac{w_K}{2^{r_2}} \cdot \frac{R_L}{R_K} \;\leq\; \frac{w_K}{c_Z} R_L.$$

In particular there is a constant $C_1 = C_1(\gamma)$ such that $R^{(1)} \leq e^{C_1 d}$ holds for all sufficiently large d.

Proof. Write $\ell_L^* : \mathcal{O}_L^\times \to \mathbb{R}^d$, $\eta \mapsto (2\log|\eta|_w)_w$, and $\ell_K^* : \mathcal{O}_K^\times \to \mathbb{R}^{r_1+r_2}$, $\epsilon \mapsto (n_v \log|\epsilon|_v)_v$, for the standard logarithm embeddings. Their images lie in the hyperplanes $H_L := \{x : \sum_w x_w = 0\}$ and $H_K := \{y : \sum_v y_v = 0\}$ respectively, and (cf. Neukirch, *op. cit.*, Ch. I, §7)

$$\mathrm{covol}_{H_L}\big(\ell_L^*(\mathcal{O}_L^\times)\big) = \sqrt{d}\, R_L, \qquad \mathrm{covol}_{H_K}\big(\ell_K^*(\mathcal{O}_K^\times)\big) = \sqrt{r_1+r_2}\, R_K. \tag{4}$$

(For a rank–$(m-1)$ lattice inside $\{\sum x_i = 0\} \subset \mathbb{R}^m$ whose rows sum to zero, all $(m-1)\times(m-1)$ minors share a common absolute value R, and the hyperplane covolume equals $\sqrt{m}\,R$; for ℓ_L^* that common value is R_L by the definition of the regulator.)

Set $H' := \{x \in \mathbb{R}^d : \; x_{\tilde\sigma_k} = 0,\; x_{\tilde\tau_j^{(1)}} + x_{\tilde\tau_j^{(2)}} = 0 \;\forall k, j\}$, an r_2–dimensional subspace contained in H_L. By Lemma 2.3, $\ell_L^*(U^{(1)}) \subset H'$. Let

$$A := H' \cap \ell_L^*(\mathcal{O}_L^\times), \qquad B := \ell_L^*(\mathcal{O}_L^\times).$$

Then $A \subset B$ is a sublattice of rank r_2, the short exact sequence $0 \to A \to B \to B/A \to 0$ produces a full–rank lattice B/A inside H_L/H', and

$$\operatorname{covol}_{H_L}(B) = \operatorname{covol}_{H'}(A) \cdot \operatorname{covol}_{H_L/H'}(B/A). \tag{5}$$

Index $[A : \ell_L^*(U^{(1)})]$. For $\eta \in \mathcal{O}_L^\times$, the condition $\ell_L^*(\eta) \in H'$ holds exactly when $|\operatorname{N}_{L/K}(\eta)|_v = 1$ at every archimedean v of K, equivalently when $\operatorname{N}_{L/K}(\eta) \in \mu_K$ (the roots of unity of K). Hence $A = \ell_L^*(\{\eta : \operatorname{N}\eta \in \mu_K\})$, and since $U^{(1)}$ is the full kernel of $\operatorname{N}|_{\mathcal{O}_L^\times}$,

$$\big[A : \ell_L^*(U^{(1)})\big] \;\le\; \big[\{\eta : \operatorname{N}\eta \in \mu_K\} : U^{(1)}\big] \;\le\; |\mu_K| = w_K,$$

the last step because N embeds the quotient into μ_K.

Covolume of B/A. Define $N_* : \mathbb{R}^d \to \mathbb{R}^{r_1+r_2}$ by $(N_*x)_{\sigma_k} = x_{\tilde\sigma_k}$ and $(N_*x)_{\tau_j} = x_{\tilde\tau_j^{(1)}} + x_{\tilde\tau_j^{(2)}}$; a place–by–place check with Lemma 2.1 confirms that $N_* \circ \ell_L^* = \ell_K^* \circ \operatorname{N}_{L/K}$ on $\mathcal{O}_L^\times$. Its kernel is H', so N_* induces a linear isomorphism $H_L/H' \xrightarrow{\sim} H_K$. In the orthonormal basis $\{e_{\tilde\sigma_k}\} \cup \{f_j := (e_{\tilde\tau_j^{(1)}} + e_{\tilde\tau_j^{(2)}})/\sqrt{2}\}$ of $(H')^\perp \subset \mathbb{R}^d$, $N_* e_{\tilde\sigma_k} = e_{\sigma_k}$ and $N_* f_j = \sqrt{2}\, e_{\tau_j}$, so $N_*|_{(H')^\perp}$ is diagonal with determinant $2^{r_2/2}$. Decomposing $(H')^\perp = \big((H')^\perp \cap H_L\big) \oplus \mathbb{R}\mathbf{1}_L$ and $\mathbb{R}^{r_1+r_2} = H_K \oplus \mathbb{R}\mathbf{1}_K$ (where $\mathbf{1}_\bullet$ is the all–ones vector), one verifies $N_*^T \mathbf{1}_K = \mathbf{1}_L|_{(H')^\perp}$, hence $N_*\big((H')^\perp \cap H_L\big) = H_K$; a block–triangular calculation then yields

$$J := \big|\det\big(N_* :\, H_L/H' \to H_K\big)\big| \;=\; 2^{r_2/2}\sqrt{\tfrac{r_1+r_2}{d}}.$$

The map N_* sends B/A isomorphically onto $\ell_K^*(\operatorname{N}(\mathcal{O}_L^\times))$, which sits inside $\ell_K^*(\mathcal{O}_K^\times)$ at index $Q' := [\ell_K^*(\mathcal{O}_K^\times) : \ell_K^*(\operatorname{N}(\mathcal{O}_L^\times))] \ge 1$. Therefore

$$\operatorname{covol}_{H_L/H'}(B/A) \;=\; \frac{\operatorname{covol}_{H_K}\big(\ell_K^*(\operatorname{N}(\mathcal{O}_L^\times))\big)}{J} \;=\; \frac{Q'\sqrt{r_1+r_2}\, R_K}{J} \;=\; \frac{Q'\sqrt{d}\, R_K}{2^{r_2/2}}.$$

Assembling. Substituting (4) and the last two paragraphs into (5),

$$\operatorname{covol}_{H'}\big(\ell_L^*(U^{(1)})\big) \;\le\; w_K \operatorname{covol}_{H'}(A) \;=\; w_K \cdot \frac{\sqrt{d}\, R_L}{Q'\sqrt{d}\, R_K/2^{r_2/2}} \;=\; \frac{2^{r_2/2}\, w_K\, R_L}{Q' R_K}.$$

On $U^{(1)}$ one has $\mathcal{L} = \frac{1}{2} \cdot \pi \circ \ell_L^*$, with $\pi : H' \to \mathbb{R}^{r_2}$, $x \mapsto (x_{\tilde\tau_j^{(1)}})_j$; in the orthonormal basis $e'_j := (e_{\tilde\tau_j^{(1)}} - e_{\tilde\tau_j^{(2)}})/\sqrt{2}$ of H', $\pi e'_j = \frac{1}{\sqrt{2}} e_j$, so $|\det \pi| = 2^{-r_2/2}$ and

$$R^{(1)} = \det \mathcal{L}(U^{(1)}) = 2^{-r_2} \cdot 2^{-r_2/2} \cdot \operatorname{covol}_{H'}\big(\ell_L^*(U^{(1)})\big) \;\le\; \frac{w_K}{2^{r_2} Q'} \cdot \frac{R_L}{R_K} \;\le\; \frac{w_K}{2^{r_2}} \cdot \frac{R_L}{R_K}.$$

This is the first claimed inequality; the second follows from Theorem 3.6 (applicable because $r_1 + r_2 \ge 2$).

For the asymptotic estimate, the analytic class number formula $h_L R_L = w_L |\Delta_L|^{1/2} \kappa_L / (2\pi)^d$ (recall every place of L is complex) gives

$$R_L \le h_L R_L \;=\; \frac{w_L |\Delta_L|^{1/2}}{(2\pi)^d}\, \kappa_L. \tag{6}$$

The conductor–discriminant formula yields $|\Delta_L| = |\Delta_K|^2 \,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})$, and $\mathfrak{d}_{L/K} \mid (4)\mathcal{O}_K$ (the discriminant of X^2+1), so $|\Delta_L| \le 4^d|\Delta_K|^2 = 4^d e^{2\gamma d}$ and $\log|\Delta_L| \le (2\gamma + 2\log 2)d$. Theorem 3.5 applied with $n = 2d$ now gives

$$\kappa_L \le \left(\tfrac{e(2\gamma+2\log 2)d}{2(2d-1)}\right)^{2d-1} \le \big(e(\gamma+\log 2)\big)^{2d}$$

for $d \ge 1$. Finally $w_E \le 2[E:\mathbb{Q}]^2$ for any number field E — since $\mu_m \subset E$ forces $\varphi(m) \mid [E:\mathbb{Q}]$, hence $m \le 2[E:\mathbb{Q}]^2$ — so $w_L \le 8d^2$ and $w_K \le 2d^2$. Putting all of this together,

$$R^{(1)} \le \frac{2d^2}{c_Z} \cdot \frac{8d^2 \cdot 2^d e^{\gamma d} \cdot (e(\gamma+\log 2))^{2d}}{(2\pi)^d} = e^{C_1 d + O(\log d)}$$

with $C_1 := \log 2 + \gamma - \log(2\pi) + 2 + 2\log(\gamma+\log 2)$, a constant that depends only on γ. □

3.4. Counting bounded–height points of $U^{(1)}$

Lemma 3.8. *For $T > 0$ put $D(T) := \#\{\zeta \in U^{(1)} : \|\mathcal{L}(\zeta)\|_\infty \le T\}$. If $T \ge (2R^{(1)})^{1/r_2}$, then $D(T) \ge T^{r_2}/R^{(1)}$.*

Proof. Because $\ker\mathcal{L}$ is finite, $D(T) \ge \#\big(\mathcal{L}(U^{(1)}) \cap [-T,T]^{r_2}\big)$. Applying Corollary 3.3 with $\Lambda = \mathcal{L}(U^{(1)}) \subset \mathbb{R}^{r_2}$ — full–rank by Lemma 2.5, of determinant $R^{(1)}$ — and $S = [-T,T]^{r_2}$, the ratio $\mathrm{vol}(S)/(2^{r_2}\det\Lambda) = T^{r_2}/R^{(1)} \ge 2$ by hypothesis, and the lemma follows. □

4. The point set and the key inequality

Fix a real embedding $\sigma = \sigma_1 : K \hookrightarrow \mathbb{R}$, and for $M \ge 4$ define

$$P = P_{K,M} \;:=\; \Big\{\big(\tfrac12\sigma(x), \tfrac12\sigma(y)\big) : \; (x,y) \in B_M \times B_M\Big\} \;\subset\; \mathbb{R}^2.$$

Injectivity of σ gives $|P| = |B_M|^2 =: n$.

Proposition 4.1. *With $T := \log(M/4)$,*

$$u(P) \;\ge\; \tfrac12\, D(T) \cdot |B_{M/2}|^2.$$

Proof. Pick $\zeta \in U^{(1)}$ with $\|\mathcal{L}(\zeta)\|_\infty \le T$ and let $(a,b) \in \mathcal{O}_K^2$ be the corresponding pair from Lemma 2.6. Lemma 2.7 then bounds $|a|_w, |b|_w \le \max(2, 2e^T) = M/2$ at every archimedean w (since $M \ge 4$).

Given any $(x,y) \in B_{M/2} \times B_{M/2}$, set $p := (\frac12\sigma(x), \frac12\sigma(y))$ and $q := (\frac12\sigma(x+a), \frac12\sigma(y+b))$. Then $p \in P$ because $B_{M/2} \subset B_M$, and $|x+a|_w \le |x|_w + |a|_w \le M/2 + M/2 = M$ at every w, so $(x+a, y+b) \in B_M \times B_M$ and $q \in P$ as well. A direct computation gives

$$\|p-q\|^2 = \tfrac14\big(\sigma(a)^2 + \sigma(b)^2\big) = \tfrac14\,\sigma(a^2+b^2) = \tfrac14 \cdot 4 = 1.$$

Hence the map

$$\Phi : \; \{\zeta : \|\mathcal{L}(\zeta)\|_\infty \le T\} \times (B_{M/2} \times B_{M/2}) \longrightarrow \{(p,q) \in P \times P : \|p-q\| = 1\}$$

sending $(\zeta,(x,y))$ to the pair (p,q) above is well–defined. It is also injective: from (p,q) one recovers (x,y) via injectivity of σ, then $(a,b)=(x'-x,y'-y)$ where (x',y') corresponds to q, and finally ζ by inverting Lemma 2.6. Hence the number of ordered unit–distance pairs in P is at least $D(T)\cdot|B_{M/2}|^2$, and $u(P)$ is half this count. □

Proposition 4.2. *There is a constant $C_2=C_2(\gamma,c)>0$ such that for every $M\geq\max(4,2R_0)$ (with R_0 from Lemma 3.4),*

$$\frac{u(P)}{n}\;\geq\;\tfrac{1}{2}\,D(T)\cdot e^{-C_2 d},\qquad T=\log(M/4).$$

Proof. Combining Proposition 4.1 with Lemmas 3.1 and 3.4 (the latter applied with $R=M/2\geq R_0$),

$$\frac{u(P)}{n}\geq\frac{D(T)}{2}\cdot\frac{|B_{M/2}|^2}{|B_M|^2}\geq\frac{D(T)}{2}\cdot\frac{(\pi/2)^{2r_2}(M/2)^{2d}}{|\Delta_K|\,(2M+1)^{2d}}.$$

The trivial bound $(M/2)/(2M+1)\geq 1/6$ for $M\geq 1$ gives $\big((M/2)/(2M+1)\big)^{2d}\geq 6^{-2d}$, and so

$$\frac{u(P)}{n}\;\geq\;\frac{D(T)}{2}\cdot\frac{(\pi/2)^{2r_2}}{|\Delta_K|\cdot 36^d}=\frac{D(T)}{2}\,\exp\Big(2r_2\log\tfrac{\pi}{2}-\gamma d-d\log 36\Big);$$

we may take $C_2=\gamma+\log 36-2c\log(\pi/2)$. □

5. An infinite family of number fields

Proposition 5.1. *There exist a real number $\gamma_\star>0$, a rational $c_\star\in(0,\frac12)$, and an infinite sequence of number fields $(K_m)_{m\geq 0}$ with $d_m:=[K_m:\mathbb{Q}]\to\infty$, such that for each m:*

(i) $r_1(K_m)\geq 1$ *and* $r_2(K_m)=c_\star\,d_m$;

(ii) $\frac{1}{d_m}\log|\Delta_{K_m}|\leq\gamma_\star$.

The proof spans the rest of the section.

5.1. An infinite totally real 2–class–field tower

Theorem 5.2 (Golod–Shafarevich criterion)**.** *Let F be a number field and p a prime. If*

$$d_p\big(\mathrm{Cl}(F)\big)\;>\;2+2\sqrt{r_1(F)+r_2(F)+\delta_p(F)}\,,$$

where $\delta_p(F)=1$ when $\mu_p\subset F$ and 0 otherwise, then the Hilbert p–class–field tower $F=F_0\subset F_1\subset F_2\subset\cdots$ is infinite.

Proof. E. S. Golod and I. R. Shafarevich, *On the class field tower* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), 261–272, show that a pro–p group G with $d(G)$ generators and $r(G)$ relations is infinite whenever $r(G)<d(G)^2/4$. Taking G to be the Galois group of the maximal unramified p–extension of F gives $d(G)=d_p(\mathrm{Cl}(F))$, and Shafarevich's relation–rank bound,

$$r(G)\leq d(G)+\dim_{\mathbb{F}_p}\big(\mathcal{O}_F^\times\otimes\mathbb{F}_p\big)=d(G)+(r_1+r_2-1)+\delta_p,$$

controls $r(G)$ (see P. Roquette, *On class field towers*, in Cassels–Fröhlich, *Algebraic Number Theory*, Academic Press 1967, Ch. IX, Theorems 1–3, or H. Koch, *Galois Theory of p–Extensions*, Springer 2002, Theorem 11.16). Solving $d(G)+(r_1+r_2-1+\delta_p) < d(G)^2/4$ recovers the stated criterion. $\square$

Lemma 5.3. *There exists a real quadratic field $F_0 = \mathbb{Q}(\sqrt{D})$ whose Hilbert 2–class–field tower is infinite.*

Proof. Let $D > 0$ be squarefree with exactly t distinct prime divisors. Gauss's genus theory (see e.g. D. A. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley 1989, Prop. 3.11) gives $d_2(\mathrm{Cl}^+(F_0)) = t-1$ for the narrow class group. The natural surjection $\mathrm{Cl}^+(F_0) \twoheadrightarrow \mathrm{Cl}(F_0)$ has kernel of order at most 2 (generated by the narrow class of a totally positive non–square unit, when one exists), so $d_2(\mathrm{Cl}(F_0)) \geq t-2$. In the real quadratic case $r_1 = 2$, $r_2 = 0$, $\delta_2 = 1$, and Theorem 5.2 demands $d_2(\mathrm{Cl}(F_0)) > 2 + 2\sqrt{3}$, equivalently $d_2(\mathrm{Cl}(F_0)) \geq 6$. Taking $t = 8$ — for instance with $D = 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23$ — yields $d_2(\mathrm{Cl}(F_0)) \geq 6$, and the tower is therefore infinite. $\square$

Fix such an F_0 and its tower $F_0 \subset F_1 \subset \cdots$. Each step is unramified at every place, including at infinity, so every F_m remains totally real, and $|\Delta_{F_m}|^{1/[F_m:\mathbb{Q}]} = |\Delta_{F_0}|^{1/2}$ for all m.

5.2. The quadratic twist

Put $\alpha := \sqrt{D} \in F_0$. Its two real embeddings carry α to $\pm\sqrt{D}$, so it has one positive and one negative real conjugate.

Lemma 5.4. *α is not a square in F_m for any $m \geq 0$.*

Proof. The extension $F_0(\sqrt{\alpha})/F_0$ is ramified at the real place at which $\alpha < 0$ (where the place becomes complex), and so cannot be contained in any everywhere–unramified extension of F_0. Since F_m/F_0 is everywhere unramified, we conclude $\sqrt{\alpha} \notin F_m$. $\square$

Definition 5.5. For each $m \geq 0$, set $K_m := F_m(\sqrt{\alpha})$.

Lemma 5.6. *For every $m \geq 0$:*

(a) $[K_m : \mathbb{Q}] = 2[F_m : \mathbb{Q}]$*; in particular* $d_m = [K_m : \mathbb{Q}] \to \infty$.

(b) K_m/K_0 *is everywhere unramified; consequently* $|\Delta_{K_m}|^{1/d_m} = |\Delta_{K_0}|^{1/d_0} =: e^{\gamma_\star}$.

(c) $r_1(K_m) = \tfrac{1}{2}d_m$ *and* $r_2(K_m) = \tfrac{1}{4}d_m$.

(d) $i \notin K_m$.

Proof. (a) Lemma 5.4 gives $[K_m : F_m] = 2$.

(b) The fields F_m and $K_0 = F_0(\sqrt{\alpha})$ are linearly disjoint over F_0 (again by Lemma 5.4), so $K_m = F_m \cdot K_0$ and $\mathrm{Gal}(K_m/K_0) \cong \mathrm{Gal}(F_m/F_0)$. Unramifiedness behaves well under base change: for any place w of K_0 lying over a place v of F_0, the completion $(K_m)_W/(K_0)_w$ is contained in $(F_m)_{W'} \cdot (K_0)_w/(K_0)_w$ for suitable W, W', and the compositum of the unramified extension $(F_m)_{W'}/(F_0)_v$ with $(K_0)_w$ is unramified over $(K_0)_w$ (unramifiedness of local extensions is preserved by base change; see Neukirch, *op. cit.*,

Prop. II.7.2). This applies at all places, infinite included, so K_m/K_0 is everywhere unramified and $|\Delta_{K_m}| = |\Delta_{K_0}|^{[K_m:K_0]}$.

(c) Each real place $\tilde{\sigma}$ of F_m lies above a unique real place σ_0 of F_0, with $\tilde{\sigma}(\alpha) = \sigma_0(\alpha)$. Over the $[F_m : F_0]$ places of F_m above the real place of F_0 where $\sigma_0(\alpha) > 0$, K_m has $2[F_m : F_0]$ real places; over the $[F_m : F_0]$ places above the place where $\sigma_0(\alpha) < 0$, K_m has $[F_m : F_0]$ complex places. Summing these contributions with the one–positive–one–negative sign data gives $r_1(K_m) = 2[F_m : F_0]$, $r_2(K_m) = [F_m : F_0]$, and $d_m = 2[F_m : \mathbb{Q}] = 4[F_m : F_0]$, proving (c).

(d) Suppose, for contradiction, $i = a + b\sqrt{\alpha}$ with $a, b \in F_m$. Squaring gives $-1 = a^2 + b^2\alpha + 2ab\sqrt{\alpha}$, so (by Lemma 5.4) $2ab = 0$. If $b = 0$, then $a^2 = -1$ is impossible in the totally real F_m. If $a = 0$, then $\alpha = -1/b^2$ is totally negative in F_m, contradicting $\sigma_0(\alpha) = \sqrt{D} > 0$ at one real place of F_0. □

Proof of Proposition 5.1. Take $c_\star = \frac{1}{4}$ and $\gamma_\star = \frac{1}{d_0}\log|\Delta_{K_0}|$, where $K_0 = \mathbb{Q}(D^{1/4})$ with D as in Lemma 5.3. Then Lemma 5.6 verifies (i)–(ii). □

Remark 5.7. Concretely, $|\Delta_{K_0}|$ divides $256\,D^3$ (the discriminant of $X^4 - D$), so $e^{\gamma_\star} \le 4D^{3/4}$. For $D = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ this is a finite, if large, number. We make no attempt to optimise $\gamma_\star$.

6. Proof of the main theorem

Let (K_m), $c_\star = \frac{1}{4}$, $\gamma_\star$ be as supplied by Proposition 5.1. Write $d = d_m$, $K = K_m$, $r_2 = c_\star d$, and let $C_1 = C_1(\gamma_\star)$, $C_2 = C_2(\gamma_\star, c_\star)$ be the constants appearing in Lemma 3.7 and Proposition 4.2. Fix once and for all $A := 2$.

Lemma 6.1. *There exists $d_\star = d_\star(\gamma_\star)$ such that for every m with $d_m \ge d_\star$, setting $M := d^A$ and $T := \log(M/4)$:*

(i) $M \ge \max(4, 2R_0)$ *and* $T \ge (2R^{(1)})^{1/r_2}$;

(ii) $\log D(T) \ge c_\star d \log\log d - C_1 d - d$;

(iii) $\log n \le 2Ad\log d + 3d$, *and* $\log n \ge 2Ad\log d - (\gamma_\star + 1)d$;

(iv) $\log(u(P)/n) \ge c_\star d\log\log d - (C_1 + C_2 + 2)d$.

Proof. (i) $R_0 = R_0(\gamma_\star, c_\star)$ is a constant, and $M = d^2 \ge \max(4, 2R_0)$ for d large. Lemma 3.7 gives $(2R^{(1)})^{1/r_2} \le (2e^{C_1 d})^{1/(c_\star d)} = 2^{1/(c_\star d)} e^{C_1/c_\star}$, which is bounded, while $T = A\log d - \log 4 \to \infty$, so (i) holds once $d \ge d_\star$.

(ii) By Lemma 3.8 and part (i), $D(T) \ge T^{r_2}/R^{(1)}$. Hence

$$\log D(T) \ge r_2 \log T - \log R^{(1)} \ge c_\star d \log(A\log d - \log 4) - C_1 d \ge c_\star d \log\log d - C_1 d - d$$

for d large, using $\log(A\log d - \log 4) \ge \log\log d - 1/c_\star$ eventually.

(iii) Lemma 3.1 gives $n = |B_M|^2 \le (2M+1)^{2d} \le (3M)^{2d}$, so $\log n \le 2d\log(3d^A) = 2Ad\log d + 2d\log 3 \le 2Ad\log d + 3d$. In the opposite direction, Lemma 3.4 (applicable by (i)) gives $n \ge (\pi/2)^{2r_2} M^{2d}/|\Delta_K|$, so $\log n \ge 2Ad\log d + 2r_2\log(\pi/2) - \gamma_\star d \ge 2Ad\log d - (\gamma_\star + 1)d$.

(iv) From Proposition 4.2 together with (ii), $\log(u(P)/n) \geq \log D(T) - C_2 d - \log 2 \geq c_\star d \log\log d - (C_1 + C_2 + 2)d$. □

Proof of Theorem 1.1. Set $C_3 := C_1 + C_2 + 2$ and $c_0 := c_\star/(12A) = 1/96$. Take m large enough that $d = d_m \geq d_\star$ and $c_\star \log\log d \geq 2C_3$, and put $n = n_m = |B_{d^A}|^2$ and $P = P_{K_m, d^A}$ as above. Lemma 6.1(iv) then gives

$$\log \frac{u(P)}{n} \;\geq\; \tfrac{1}{2} c_\star d \log\log d.$$

By Lemma 6.1(iii), for large d we have $\tfrac{1}{2} \cdot 2Ad\log d \leq \log n \leq 3Ad\log d$ and $\tfrac{1}{2}\log d \leq \log\log n \leq 2\log d$. Therefore

$$\frac{\log(u(P)/n)}{\log n} \cdot \log\log n \;\geq\; \frac{\tfrac{1}{2} c_\star d \log\log d}{3Ad\log d} \cdot \tfrac{1}{2}\log d \;=\; \frac{c_\star}{12A}\log\log d \;=\; c_0 \log\log d.$$

Since $\log\log n \leq 2\log d$, $\log\log d \geq \tfrac{1}{2}\log\log n - \log 2 \geq \tfrac{1}{2}\log\log\log n$ for n large (using $\log\log n \geq \log\log\log n$). More directly, the inequality $\log d \geq \tfrac{1}{2}\log\log n$ yields $\log\log d \geq \log\log\log n - \log 2$. Combining,

$$u(n) \;\geq\; u(P) \;\geq\; n^{1 + c_0(\log\log d)/\log\log n} \;\geq\; n^{1 + \frac{c_0}{2}\cdot\frac{\log\log\log n}{\log\log n}}$$

for all sufficiently large m. As $m \to \infty$, $n_m \to \infty$ by Lemma 6.1(iii), so the set $\mathcal{N} := \{n_m : m \text{ large}\}$ is infinite. Replacing c_0 by $c_0/2$ delivers the first statement of the theorem.

For the second statement: given $C > 0$, choose m large enough that also $c_0 \log\log d_m > C$. Then with $n = n_m$,

$$\frac{\log(u(n)/n)}{\log n} \cdot \log\log n \;>\; C,$$

which is to say $u(n) > n^{1 + C/\log\log n}$. □

7. Consistency with known bounds

Proposition 7.1. *For the point sets $P = P_{K_m, d_m^A}$ constructed above, $u(P) = n^{1+o(1)}$ as $m \to \infty$; in particular $u(P) \leq n^{4/3}$ for all m large enough.*

Proof. By Lemma 6.1(iii)–(iv), $\log(u(P)/n) \leq \log D(T) \leq r_2 \log(2T) + O(d)$ (trivially $D(T) \leq |\{\zeta\}|$ is finite and any crude bound suffices); even more simply, $u(P) \leq \binom{n}{2}$ implies $\log(u(P)/n) \leq \log n$, while our lower bound $\log(u(P)/n) \geq \Omega(d\log\log d)$ combined with $\log n = \Theta(d\log d)$ gives $\log(u(P)/n)/\log n = O(\log\log d/\log d) = o(1)$. Thus $u(P) = n^{1+o(1)} \ll n^{4/3}$. □

8. Concluding remarks

Remark 8.1. The threshold $d_\star$ in Lemma 6.1 depends doubly–exponentially on $\gamma_\star$ and hence on the chosen base field F_0; in absolute terms it is astronomically large. No optimisation of constants has been attempted. Our construction shows that $u(n) \geq n^{1+\Omega(\log\log\log n/\log\log n)}$ along a sparse sequence; we leave open whether $u(n) = n^{1+\Theta(\log\log\log n/\log\log n)}$, or whether a further iterated logarithm can be extracted.

Remark 8.2. The mechanism differs in spirit from Erdős's. In the $\mathbb{Z}[i]$ grid, the unit–distance directions are the set $\{\alpha \in \mathbb{Z}[i] : |\alpha|^2 = r\}$ for a highly composite r; this is a single *orbit* of divisors of r under the finite unit group $\{\pm 1, \pm i\}$, and its size is dictated by the divisor function. Over K, the unit group of the relevant order acquires *positive rank* $r_2 = c_\star d$, and van der Corput's theorem translates that rank into a count of bounded–height directions growing as $(\log M)^{c_\star d}$ rather than $\exp(O(\log M/\log\log M))$. The cost is an $e^{O(d)}$ loss in the overlap ratio, which is dominated as soon as $\log\log d$ exceeds a constant depending only on $\gamma_\star$.

Remark 8.3 (On the cited inputs). All four external inputs are unconditional and classical: van der Corput's theorem (1936), Louboutin's residue bound (2001), Zimmert's regulator bound (1981), and the Golod–Shafarevich criterion (1964) applied via Gauss's genus theory at the base field. Precise page/theorem references have been supplied throughout. The proof of Lemma 3.7 contains a detailed covolume computation; a reader content with the cruder estimate $R^{(1)} \le e^{O_\gamma(d)}$ may replace that computation by the observation that each normalisation factor present is bounded by $d^{O(1)} \cdot 2^{O(d)}$, which is absorbed.