Planar Point Sets with Many Unit Distances

OpenAI

Abstract

For a finite planar set P, let $\nu(P)$ be the number of unordered unit-distance pairs in P, and let $\nu(n)$ be the maximum of $\nu(P)$ over all n-point planar sets. We prove that, for some fixed $\delta > 0$, one has $\nu(n) \geq n^{1+\delta}$ for infinitely many n. This disproves the well-known unit distance conjecture from [Erd46].

The construction passes through an infinite unramified tower of totally real number fields with 3-power Galois groups of growing degree, in which a fixed set of rational primes splits completely. After adjoining i, these fields produce high-dimensional lattices with many elements whose images under every complex embedding have absolute value 1. Golod–Shafarevich theory ensures existence of an infinite such tower, even after a quotient step making the prescribed Frobenius classes trivial. A crucial property of the construction is that all resulting discriminants and class numbers are at most exponential in the extension degree.

1 Main Result

For a finite set $P \subset \mathbb{R}^2$, let $\nu(P) = \#\{\{x, y\} \subset P : |x - y| = 1\}$ and $\nu(n) = \max_{|P|=n} \nu(P)$. The planar unit-distance problem goes back to Erdős [Erd46], who conjectured that there should be an absolute constant C such that, for all sufficiently large n,

$$\nu(n) \leq n^{1+C/\log\log n}. \tag{1}$$

The same 1946 paper also introduced the distinct-distances problem, later resolved up to logarithmic factors by Guth–Katz [GK15]. An elementary upper bound is $\nu(n) = O(n^{3/2})$: the Euclidean unit-distance graph is $K_{2,3}$-free, since two unit circles meet in at most two points, and the Kővári–Sós–Turán theorem applies [KST54]. The best known upper bound $\nu(n) = O(n^{4/3})$ is due to Spencer–Szemerédi–Trotter [SST84]; Székely later gave a short crossing-number proof of this incidence bound [Sze97].

It is useful to compare this with the same question for other norms on $\mathbb{R}^2$, a direction studied systematically by Brass [Bra96]. If the unit ball has a flat segment, one can arrange quadratically many unit distances, so the interesting normed-plane analogues usually impose strict convexity or genericity. Székely's crossing-number argument extends to strictly convex norms, again giving $O(n^{4/3})$, and Valtr constructed a strictly convex norm for which this exponent is attained [Sze97, Val05]. Related work of Eisenbrand–Pach–Rothvoß–Sopher on convexly independent subsets of Minkowski sums gave the corresponding $O(m^{2/3}n^{2/3} + m + n)$ upper bound, with later matching lower bounds by Bílka–Buchin–Fulek–Kiyomi–Okamoto–Tanigawa–Tóth [EPRS08, BBF+10]; Brass–Moser–Pach give a broader survey [BMP05]. For Baire-generic norms the behavior is now known much more sharply. Matoušek proved $O(n \log n \log\log n)$ for

most planar norms [Mat11]. For each fixed $d \geq 2$, Alon–Bucić–Sauermann proved that a comeagre set of norms on $\mathbb{R}^d$ has at most $\frac{d}{2} n \log_2 n$ unit distances on every n-point set [ABS25]. A matching lower bound $(\frac{d}{2} - o(1))n \log_2 n$ was then shown by Greilhuber–Schildkraut–Tidor to hold for *all* norms on $\mathbb{R}^d$ [GST25]. These results provided evidence in favor of Erdős's conjecture, which was widely believed to be true prior to our work. However we disprove the unit distance conjecture; our main theorem is as follows.

Theorem 1.1. *There exists an absolute constant $\delta > 0$ and infinitely many positive integers n for which $\nu(n) \geq n^{1+\delta}$.*

We note that a similar, stronger conjecture posed in [EF97] concerns point sets $P \subset \mathbb{R}^2$ such that every point $x \in P$ has at least k equidistant neighbors in P, at a distance d_x that may depend on x. Theorem 1.1 also refutes the predicted bound $k \leq n^{o(1)}$: along our sequence the unit-distance graph has average degree $n^{\Omega(1)}$, and a graph of average degree at least $2k$ contains a subgraph of minimum degree at least k.

The construction can be viewed as a high-dimensional analogue of the arithmetic behind Erdős's classical square-grid lower bound. In the Gaussian integers $\mathbb{Z}[i]$, a product of many rational primes $q \equiv 1 \pmod 4$ has many representations of the form $z\bar{z}$. Geometrically, these representations give many lattice vectors of the same length. Our construction replaces $\mathbb{Q}(i)$ by $K = L(i)$, where L is a totally real field whose degree tends to infinity. The nontrivial automorphism c of K/L plays the role of complex conjugation: under every complex embedding of K, c becomes ordinary complex conjugation.

The proof separates into an arithmetic part and a geometric part. The arithmetic part builds fields L in which a fixed set of rational primes splits completely. These split primes give many ideal factorizations in $K = L(i)$; after a class-group pigeonhole, they produce many elements $u \in K^\times$ with $u\,c(u) = 1$. Under every complex embedding these elements have absolute value 1, so they become candidate unit translations. The class-group loss is harmless because the fields have bounded root discriminant $\mathrm{rd}(F) = |D_F|^{1/[F:\mathbb{Q}]}$. Minkowski's theorem then gives class numbers at most exponential in the field degree.

The bounded root discriminants are obtained at the same time as the prescribed splitting. We use an unramified pro-3 tower over a cyclic cubic field. Chebotarev supplies rational primes whose Frobenius classes can be made trivial in every later layer. Shafarevich's relation-rank estimate and Golod–Shafarevich theory keep the resulting quotient tower infinite. This is the Hajir–Maire class-field-tower method, in an unramified pro-3 setting; see Remark 3.1.

Section 2 proves the geometric criterion: given suitable number fields and split primes, it constructs the planar point sets by embedding norm-one elements into a high-dimensional Minkowski lattice, cutting by a product of discs, and projecting to one complex coordinate. Section 3 then constructs the required fields using the unramified pro-3 tower. Appendix A collects the number-field conventions and citations used below.

Statement on AI Use

This problem was solved in a completely automated fashion. Our internal model was given an AI-written statement of the problem, and its output was sent to an AI grading pipeline, which indicated high confidence that the solution was correct. It was only after this point that in-

ternal human researchers and mathematicians began to examine the solution carefully. After preliminary AI-assisted verification and rewriting, a draft was sent to external mathematicians, including several number theory experts, who confirmed the proof's correctness (and have already simplified and strengthened the argument). The present manuscript is a human-edited exposition of the autonomously produced solution, with references, reorganized proofs, and additional explanatory material added afterward.

The original AI-written prompt given to the internal model was:

> **Prompt.**
>
> Let $P \subset \mathbb{R}^2$ be a finite set of distinct points. Define
>
> $$\nu(P) = \left| \left\{ \{p, q\} \in \binom{P}{2} : \|p - q\|_2 = 1 \right\} \right|$$
>
> and, for each integer $n \geq 1$, $\nu(n) = \max_{\substack{P \subset \mathbb{R}^2 \\ |P|=n}} \nu(P)$.
>
> Resolve Erdős's planar unit-distance problem completely: $\nu(n) \leq n^{1+O(1/\log\log n)}$ as $n \to \infty$? Equivalently, determine whether there exist absolute constants $C > 0$ and $N \in \mathbb{N}$ such that $\nu(n) \leq n^{1+C/\log\log n}$ for every integer $n \geq N$. Here log denotes the natural logarithm, and N may be taken large enough that $\log\log n > 0$. The hidden constant in $O(1/\log\log n)$ is absolute and independent of P and n.
>
> A complete solution must prove exactly one of the following.
>
> *Affirmative resolution.* Prove that there exist absolute constants $C > 0$ and $N \in \mathbb{N}$ such that every set $P \subset \mathbb{R}^2$ of $n \geq N$ distinct points satisfies $\nu(P) \leq n^{1+C/\log\log n}$.
>
> *Negative resolution.* Prove that no such constants exist. Equivalently, prove that for every $C > 0$ and every $N \in \mathbb{N}$, there are an integer $n \geq N$ and a set $P \subset \mathbb{R}^2$ of n distinct points such that $\nu(P) > n^{1+C/\log\log n}$.
>
> Pairs are unordered, the distance is the usual Euclidean distance in $\mathbb{R}^2$, and the asymptotic assertion is for all sufficiently large integers n, not merely infinitely many n.
>
> Partial progress does not count unless it implies one of the two resolutions above. In particular, improved bounds such as $O(n^{4/3-\varepsilon})$, better constants in the $n^{4/3}$ bound, finite verification, special cases, structural reductions, or heuristic evidence are insufficient unless they prove the full Erdős bound or disprove it.

We emphasize that the final paragraph of the prompt does not reflect the mathematical value of partial progress. Certainly any bound $O(n^{4/3-\varepsilon})$ would be a major advance over the estimate from Spencer–Szemerédi–Trotter [SST84], which has stood since 1984 with only constant-factor improvements [ÁP22].

Below we also reproduce verbatim the original solution output by the internal model, before any automated grading or rewriting was performed.

> **Final Response from Internal Model.**
>
> *I will use a standard form of the Golod-Shafarevich argument with prescribed splitting. I write* $\mathrm{rd}(L) = |D_L|^{1/[L:\mathbb{Q}]}$. *For a finitely generated pro-p group G, let $d(G)$ and $r(G)$ denote the minimal numbers of generators and relations and let $\Phi(G)$ be its Frattini subgroup. I shall use the following two standard facts. First, if $(g_1, \dots, g_k \in \Phi(G))$, then the quotient of G by the closed normal subgroup generated by the g_i has the same generator rank and*

relation rank at most $r(G)+k$. Second, a finite pro-p group with d generators and r relations satisfies $r > d^2/4$. I use $p = 3$ in the tower construction (this avoids all dyadic infinite-prime issues). Let ℓ be large. Choose distinct primes $r_1, \dots, r_\ell \equiv 1 \pmod 3$ among the first such primes, and let L_i be the cyclic cubic subfield of $\mathbb{Q}(\zeta_{r_i})$. Put $D = \prod_i r_i$ and $M = L_1 \cdots L_\ell$. Thus $\mathrm{Gal}(M/\mathbb{Q}) \simeq (\mathbb{Z}/3\mathbb{Z})^\ell$. If χ_i is a cubic character of conductor r_i, let F be the cyclic cubic subfield corresponding to the character $\chi_1 \cdots \chi_\ell$. By the conductor-discriminant formula, $|D_F| = D^2$. Indeed the two non-trivial characters of F both have conductor D. Similarly, every character of M is of the form $\prod_i \chi_i^{a_i}$, $a_i \in 0, 1, 2$, and its conductor is the product of those r_i with $a_i \neq 0$. Hence each r_i occurs in $2 \cdot 3^{\ell-1}$ of the non-trivial characters, so

$$|D_M| = D^{2\cdot 3^{\ell-1}} = |D_F|^{[M:F]}.$$

Thus M/F is everywhere unramified. All these fields are totally real. Consequently, if G is the Galois group of the maximal unramified pro-3 extension of F, then

$$d(G) \geq \ell - 1. \tag{1}$$

(We have the elementary abelian unramified extension M/F.) Since F is a totally real cubic field and does not contain ζ_3, Shafarevich's relation-rank estimate for the unramified pro-3 group gives

$$r(G) \leq d(G) + C_0 \tag{2}$$

with an absolute constant C_0 (any linear bound with an absolute constant would suffice here). Also

$$\log \mathrm{rd}(F) = \frac{2}{3} \log D = O(\ell \log \ell). \tag{3}$$

Let E/F be the finite elementary abelian extension corresponding to $G/\Phi(G)$. Put $d = d(G)$ and

$$t = \left\lfloor \frac{d^2}{100} \right\rfloor.$$

By Chebotarev, choose distinct rational primes $q_1, \dots, q_t$, avoiding $3D$, which split completely in the normal closure over $\mathbb{Q}$ of $E(i)$. Then each $q_b \equiv 1 \pmod 4$, each q_b splits completely in F, and for every prime v of F above q_b the Frobenius element in G lies in $\Phi(G)$. There are $3t$ such primes v. Quotient G by the closed normal subgroups generated by these Frobenius elements. By the group-theoretic observation above, the quotient has generator rank d and at most $r(G) + 3t$ relations; for ℓ large, (2) gives $r(G) + 3t < d^2/4$. Hence this quotient is infinite. In it the decomposition groups at all primes above the q_b's are trivial (the extensions are unramified), so the q_b's split completely. Taking a descending chain of open normal subgroups gives an infinite tower

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots$$

of finite unramified extensions in which every q_b splits completely. Since the extensions have 3-power Galois groups, all fields in the tower are totally real. Write $f_j = [F_j : \mathbb{Q}]$; then $f_j \to \infty$ and $\mathrm{rd}(F_j) = \mathrm{rd}(F)$. Now set $K_j = F_j(i)$, with complex conjugation c. The relative discriminant of adjoining i divides (4), so

$$\mathrm{rd}(K_j) \leq 2, \qquad \mathrm{rd}(F) =: A_\ell. \tag{4}$$

We shall use the elementary bound: if $[L : \mathbb{Q}] = n$ and $\mathrm{rd}(L) \leq A$, then

$$h(L) \leq C(A)^n, \qquad \log C(A) = O(\log A + \log\log(3A)). \tag{5}$$

Indeed, Minkowski gives an integral ideal of norm $X \leq (C\sqrt{A})^n$ in every ideal class. The number of ideals of norm m is at most the n-fold divisor function $d_n(m)$, and

$$\sum_{m \leq X} d_n(m) \leq C^n X (1 + \log X)^{n-1}/(n-1)!,$$

which is exponential in n when $\log X = O_A(n)$. From (4),(5) we get

$$h(K_j) \le H_\ell^{f_j}, \qquad \log H_\ell = O(\ell \log \ell). \tag{6}$$

Let $Q = \prod_{b=1}^{t} q_b$. For fixed j, each q_b has f_j degree-one primes in F_j, and each of these splits in K_j into a conjugate pair $\mathfrak{P}_s, c\mathfrak{P}_s$. Thus there are $m = tf_j$ such pairs. For $\epsilon = (\epsilon_s) \in 0, 1^m$ put

$$\mathfrak{A}_\epsilon = \prod_{\epsilon_s=1} \mathfrak{P}_s \prod_{\epsilon_s=0} c\mathfrak{P}_s.$$

At least $2^m/h(K_j)$ of these ideals lie in the same ideal class. Fix one element η in such a fibre. For every ϵ in the fibre choose $\alpha_\epsilon \in K_j^*$ with

$$(\alpha_\epsilon) = \mathfrak{A}_\epsilon \mathfrak{A}_\eta^{-1},$$

and define

$$u_\epsilon = \alpha_\epsilon / c(\alpha_\epsilon).$$

For every complex embedding σ of K_j, $\sigma(c\alpha) = \overline{\sigma(\alpha)}$, hence $|\sigma(u_\epsilon)| = 1$. The finite valuations of u_ϵ are supported above Q and are in $-2, 0, 2$, so $Q^2 u_\epsilon \in \mathcal{O}K_j$. At the prime $\mathfrak{P}_s$ the valuation is $2(\epsilon_s - \eta_s)$, so the $u\epsilon$'s are distinct. By (6), for ℓ large,

$$|U_j| \ge \frac{2^{tf_j}}{h(K_j)} \ge \exp(\gamma f_j), \qquad \gamma := t \log 2 - \log H_\ell > 0, \tag{7}$$

where U_j denotes this set of elements. Embed K_j in $V_j = \mathbb{C}^{f_j}$ by choosing one embedding from each conjugate pair, and let $\Lambda_j = Q^{-2}\mathcal{O}_{K_j}$ in this Minkowski embedding. Then $U_j \subset \Lambda_j$, and every coordinate of every $u \in U_j$ has modulus 1. Fix $R > 1/2$. Let $W \subset V_j$ be the product of the discs $|z| \le R$. Write $b = \pi R^2$, and let $a = a(R)$ be the area of overlap of two radius-R discs whose centres are distance 1; put $\rho_R = a/b$, so $\rho_R \to 1$ as $R \to \infty$. For a coset $y + \Lambda_j$, set $X_y = (y+\Lambda_j) \cap W$, and let D_y be the number of directed pairs $(x, x+u)$ with $x, x+u \in X_y$ and $u \in U_j$. Averaging over the torus V_j/Λ_j gives

$$\mathbb{E}|X_y| = \frac{b^{f_j}}{\mathrm{covol}(\Lambda_j)}, \qquad \mathbb{E}D_y = \frac{|U_j| a^{f_j}}{\mathrm{covol}(\Lambda_j)}.$$

Hence some coset satisfies $D_y \ge |U_j| \rho_R^{f_j} |X_y|$. Choose R so large that $\log \rho_R > -\gamma/2$. For this coset, writing $X = X_y$, (7) yields

$$D_y \ge e^{\gamma f_j/2} |X|. \tag{8}$$

Project X to the first complex coordinate. This projection is injective on a coset of Λ_j: if two points have the same first coordinate, their difference is an element of K_j with one conjugate equal to zero, hence is zero. Let $P_j \subset \mathbb{C} \simeq \mathbb{R}^2$ be the projected set and $n_j = |P_j| = |X|$. Each directed pair counted in (8) projects to a unit segment, since the first coordinate of u has modulus 1. For fixed ordered endpoints the difference (hence u) is unique, so an unordered segment is counted at most twice. Therefore

$$\nu(P_j) \ge \frac{1}{2} e^{\gamma f_j/2}, n_j. \tag{9}$$

Finally, if $0 \ne \lambda \in \Lambda_j$, then $\beta = Q^2\lambda$ is a nonzero algebraic integer, and for the chosen embeddings

$$\prod_{r=1}^{f_j} |\sigma_r(\lambda)| = |N_{K_j/\mathbb{Q}}(\beta)|^{1/2} Q^{-2f_j} \ge Q^{-2f_j}.$$

Thus some coordinate of λ has modulus at least Q^{-2}. A packing argument in the polydisc W gives

$$n_j \le (CRQ^2)^{2f_j} = e^{Bf_j} \tag{10}$$

with B independent of j. Also (8) and $D_y \le n_j^2$ imply $n_j \ge e^{\gamma f_j/2}$, so $n_j \to \infty$. Combining (9) and (10), and absorbing the factor $1/2$ for large j, we obtain

$$\nu(P_j) \ge n_j^{1+\delta}, \qquad \delta = \frac{\gamma}{4B} > 0. \tag{11}$$

Given arbitrary $C_0 > 0$ and N, choose j so large that $n_j \ge N$ and $C_0/\log\log n_j < \delta$. Then

$$\nu(n_j) \ge \nu(P_j) > n_j^{1+C_0/\log\log n_j}.$$

Thus no universal constants C, N can satisfy the proposed upper bound.

The remainder of the paper explains the above proof in more detail.

2 Planar Point Sets from Number Fields

Assuming the existence of the admissible fields defined below, we construct planar point sets with many unit distances. Section 3 supplies the fields.

Definition 2.1. An admissible datum consists of:

- a totally real number field L of degree $f = [L : \mathbb{Q}]$;
- the CM field $K = L(i)$, with nontrivial automorphism c over L (see Definition A.4);
- a positive integer t, the number of selected rational primes;
- distinct rational primes $q_1, \dots, q_t$, each congruent to $1 \pmod 4$ and splitting completely in L (see Definition A.2 for the definition of splitting).

Put $Q = \prod_{b=1}^{t} q_b$. In the geometric part we also write $\mathcal{D} = Q^2$ for the corresponding fixed denominator.

Each q_b gives many conjugate prime-ideal pairs in $K = L(i)$. Since q_b splits completely in L, it gives f prime ideals $\mathfrak{q}$ of L, each with residue field $\mathcal{O}_L/\mathfrak{q} \cong \mathbb{F}_{q_b}$. Since $q_b \equiv 1 \pmod 4$, the polynomial $x^2 + 1$ splits over this residue field, so each $\mathfrak{q}$ splits in K. Hence the fixed rational primes give $m = tf$ conjugate pairs of prime ideals of K:

$$\{\mathfrak{P}_s, c\mathfrak{P}_s\}, \qquad s = 1, \dots, m. \tag{2}$$

Proposition 2.2. *Let $L, K, t, q_1, \dots, q_t, Q$ be an admissible datum in the sense of Definition 2.1. Suppose $h(K) \le H^f$ for some real $H > 0$. Then there is a set $U \subset Q^{-2}\mathcal{O}_K$ such that every $u \in U$ satisfies $\mathrm{N}_{K/L}(u) = 1$, where, for $K = L(i)$, the relative norm is $\mathrm{N}_{K/L}(u) = u\,c(u)$. Every $u \in U$ also satisfies $|\sigma(u)| = 1$ for every complex embedding $\sigma : K \hookrightarrow \mathbb{C}$. Moreover, $|U| \ge \exp\{(t\log 2 - \log H)f\}$.*

Proof. For each binary vector $\varepsilon = (\varepsilon_s) \in \{0,1\}^m$, choose one prime from each conjugate pair in (2) and set

$$\mathfrak{A}_\varepsilon = \prod_{\varepsilon_s=1} \mathfrak{P}_s \prod_{\varepsilon_s=0} c\mathfrak{P}_s.$$

These 2^m ideals need not be principal, but they occupy only $h(K)$ ideal classes. Thus some fiber of $\varepsilon \mapsto [\mathfrak{A}_\varepsilon] \in \mathrm{Cl}(K)$ has size at least $2^m/h(K)$. Fix one vector η in such a fiber; for every ε in the same fiber, $\mathfrak{A}_\varepsilon\mathfrak{A}_\eta^{-1}$ is principal, so choose $\alpha_\varepsilon \in K^\times$ with $(\alpha_\varepsilon) = \mathfrak{A}_\varepsilon\mathfrak{A}_\eta^{-1}$, and set $u_\varepsilon = \alpha_\varepsilon/c(\alpha_\varepsilon)$. Then $u_\varepsilon c(u_\varepsilon) = 1$, so $\mathrm{N}_{K/L}(u_\varepsilon) = 1$. Since L is totally real, c becomes ordinary complex conjugation under every complex embedding of K. Therefore

$$|\sigma(u_\varepsilon)| = \left|\frac{\sigma(\alpha_\varepsilon)}{\overline{\sigma(\alpha_\varepsilon)}}\right| = 1. \tag{3}$$

Let U be the set of all u_ε's obtained from this fiber. The principal ideal of u_ε is

$$(u_\varepsilon) = \frac{\mathfrak{A}_\varepsilon\mathfrak{A}_\eta^{-1}}{c(\mathfrak{A}_\varepsilon\mathfrak{A}_\eta^{-1})}.$$

Therefore, at the chosen primes,

$$v_{\mathfrak{P}_s}(u_\varepsilon) = 2(\varepsilon_s - \eta_s), \qquad v_{c\mathfrak{P}_s}(u_\varepsilon) = -2(\varepsilon_s - \eta_s). \tag{4}$$

The displayed ideal identity and (4) show that all poles of u_ε have order at most 2 and lie above the q_b's. Since $Q\mathcal{O}_K$ has valuation 1 at each such prime, $Q^2u_\varepsilon \in \mathcal{O}_K$. So $u_\varepsilon \in Q^{-2}\mathcal{O}_K$.

By (4), distinct ε's give distinct valuation vectors, hence distinct elements u_ε. Therefore

$$|U| \geq \frac{2^{tf}}{h(K)} \geq \exp\{(t\log 2 - \log H)f\}. \qquad \square$$

Set $\gamma := t\log 2 - \log H$. The following result is the geometric part of the proof: a sequence of admissible fields with the same split rational primes and $\gamma > 0$ already gives the desired planar point sets.

Theorem 2.3. *Suppose there is a sequence of admissible data $(L_j, K_j = L_j(i), q_1, \ldots, q_t)$, with the same rational primes $q_1, \ldots, q_t$, degrees $f_j = [L_j : \mathbb{Q}] \to \infty$, and a constant $H > 0$, independent of j, such that $h(K_j) \leq H^{f_j}$ and $\gamma := t\log 2 - \log H > 0$. Then there is a constant $\delta > 0$ and infinitely many n such that $\nu(n) \geq n^{1+\delta}$.*

For the proof of Theorem 2.3, fix one admissible datum in the sequence and suppress the index j. Thus $f = [L : \mathbb{Q}]$, $K = L(i)$, and the primes q_b and their product Q are fixed. Proposition 2.2 gives $|U| \geq e^{\gamma f}$, where $\gamma = t\log 2 - \log H$. Put $\mathcal{D} = Q^2$, so that $U \subset \mathcal{D}^{-1}\mathcal{O}_K$. The next two subsections construct the corresponding finite planar set.

2.1 Choosing a Window and Projecting

After an admissible datum is fixed, the set U supplied by Proposition 2.2 gives many norm-one elements that will serve as translations in a Minkowski lattice. We choose a random translate of this lattice, keep the points inside a product of discs, and count pairs whose difference lies in U.

For each real embedding of L, choose one extension $\sigma_r : K \hookrightarrow \mathbb{C}$, $r = 1, \ldots, f$, and use the Minkowski map

$$\Phi : K \longrightarrow V = \mathbb{C}^f, \qquad \Phi(x) = (\sigma_1(x), \ldots, \sigma_f(x)).$$

We identify the fractional ideal $\mathcal{D}^{-1}\mathcal{O}_K$ with the lattice $\Lambda = \Phi(\mathcal{D}^{-1}\mathcal{O}_K) \subset V$, and also write U for its image $\Phi(U) \subset \Lambda$.

The boundedness condition below is an Archimedean one. For $z = (z_1, \ldots, z_f) \in V$, put $\|z\|_\infty = \max_{1 \le r \le f} |z_r|$, and let $B_R = \{z \in V : \ \|z\|_\infty \le R\}$. Thus B_R is a product of f radius-R discs.

For a coset $a + \Lambda$, define $X_a = (a + \Lambda) \cap B_R$, $N_a = |X_a|$, and

$$E_a = \#\{(x, x') \in X_a^2 : \ x' - x \in U\}.$$

Thus N_a counts the bounded-norm lattice points in the lattice coset, while E_a counts the ordered pairs among them whose difference is one of our norm-one translations.

Let $b(R) = \pi R^2$ be the area of one radius-R disc, let $a(R)$ be the overlap area of two radius-R discs whose centers are distance 1 apart – the coordinatewise size of each translation in U by (3) – and set $\rho_R = a(R)/b(R)$. Then $\rho_R \to 1$ as $R \to \infty$.

Lemma 2.4. *Choose $R > 1/2$ so large that $\log \rho_R > -\gamma/2$. Then some nonempty coset $a + \Lambda$ satisfies $E_a \ge e^{\gamma f/2} N_a$.*

Proof. Averaging over $a \in V/\Lambda$ with respect to Haar probability measure, the standard unfolding identity gives

$$\mathbb{E}_a[N_a] = \frac{\mathrm{vol}(B_R)}{\mathrm{covol}(\Lambda)} = \frac{b(R)^f}{\mathrm{covol}(\Lambda)}.$$

For a fixed $u \in U$, the pairs with $x' - x = u$ correspond to points in $(a+\Lambda) \cap B_R \cap (B_R - u)$. By (3), every coordinate of this Minkowski-space translation has absolute value 1. Hence $\mathrm{vol}(B_R \cap (B_R - u)) = a(R)^f$. Summing over $u \in U$ and averaging over the torus gives

$$\mathbb{E}_a[E_a] = \frac{|U| a(R)^f}{\mathrm{covol}(\Lambda)} = |U| \rho_R^f \, \mathbb{E}_a[N_a].$$

If every nonempty coset had $E_a < |U| \rho_R^f N_a$, then integrating over all cosets would contradict the preceding identity; empty cosets contribute zero to both sides. Thus some nonempty coset has $E_a \ge |U| \rho_R^f N_a$. Using $|U| \ge e^{\gamma f}$ and the choice of R gives $E_a \ge e^{\gamma f/2} N_a$. □

Fix a coset supplied by Lemma 2.4, and write $X = X_a$ and $N = |X|$. Any one of the chosen complex coordinates may now be used to obtain a planar set. For concreteness, let $\pi_1 : V \to \mathbb{C}$ be the first-coordinate projection, corresponding to the embedding σ_1, and put $P = \pi_1(X) \subset \mathbb{C} \simeq \mathbb{R}^2$.

Lemma 2.5. *The map $\pi_1 : X \to \mathbb{C}$ is injective. Moreover, $\nu(P) \ge \frac{1}{2} e^{\gamma f/2} |P|$.*

Proof. If $x, x' \in X$ and $\pi_1(x) = \pi_1(x')$, then $x - x' = \Phi(\mathcal{D}^{-1}\beta)$ for some $\beta \in \mathcal{O}_K$, with $\sigma_1(\beta) = 0$. Because σ_1 is a field embedding, $\beta = 0$, so $x = x'$. Thus $|P| = |X| = N$.

Each ordered pair counted by E_a has the form $(x, x + u)$, with $u \in U$, and it projects to an ordered unit-distance pair because $|\pi_1(x + u) - \pi_1(x)| = |\pi_1(u)| = 1$. Injectivity of π_1 on X

shows that distinct ordered pairs in X^2 give distinct ordered planar pairs. Since each unordered unit segment has at most two orientations,

$$2\nu(P) \geq E_a \geq e^{\gamma f/2}|P|. \qquad \square$$

2.2 The Size Bound

Lemma 2.5 gives many unit distances relative to the field degree. To turn this into a statement about $n = |P|$, we need a uniform exponential upper bound for the number of points that can fit in the finite window. This is a packing estimate in the Archimedean sup norm.

Lemma 2.6. *Let $n = |P|$. Then $n \leq e^{\mathcal{B}f}$, where $\mathcal{B} = 2\log(4R\mathcal{D})$.*

Proof. Since π_1 is injective on X, it is enough to bound $|X|$. If $x \neq x'$ in X, write $x - x' = \Phi(\mathcal{D}^{-1}\beta)$, with $\beta \in \mathcal{O}_K \setminus \{0\}$. Then

$$\prod_{r=1}^{f} |\sigma_r(\mathcal{D}^{-1}\beta)| = \mathcal{D}^{-f}|\,\mathrm{N}_{K/\mathbb{Q}}(\beta)|^{1/2} \geq \mathcal{D}^{-f},$$

because the algebraic norm of a nonzero algebraic integer is a nonzero integer. Hence some coordinate differs by at least $\mathcal{D}^{-1}$, so X is $\mathcal{D}^{-1}$-separated in the sup norm.

The open polydiscs of sup-norm radius $\mathcal{D}^{-1}/2$ centered at the points of X are pairwise disjoint and all lie in $B_{R+\mathcal{D}^{-1}/2}$. Comparing volumes,

$$|X|\big(\pi(\mathcal{D}^{-1}/2)^2\big)^f \leq \big(\pi(R + \mathcal{D}^{-1}/2)^2\big)^f.$$

Therefore

$$|P| = |X| \leq (1 + 2R\mathcal{D})^{2f} \leq (4R\mathcal{D})^{2f} = e^{\mathcal{B}f}. \qquad \square$$

Proof of Theorem 2.3. For each j, Lemmas 2.4, 2.5, and 2.6 give a planar set P_j, with $n_j = |P_j|$, such that

$$\nu(P_j) \geq \frac{1}{2} n_j e^{\gamma f_j/2}, \qquad n_j \leq e^{\mathcal{B}f_j}.$$

Also $n_j \to \infty$. Indeed, every ordered pair counted by E_a is determined by its two endpoints, so $E_a \leq n_j^2$, while Lemma 2.4 gives $E_a \geq e^{\gamma f_j/2} n_j$. Thus $n_j \geq e^{\gamma f_j/2}$.

From $n_j \leq e^{\mathcal{B}f_j}$, we obtain $f_j \geq \log n_j/\mathcal{B}$. Hence

$$\nu(P_j) \geq \frac{1}{2} n_j e^{\gamma f_j/2} \geq \frac{1}{2} n_j^{1+\gamma/(2\mathcal{B})}.$$

Set $\delta = \gamma/(4\mathcal{B}) > 0$. Since $n_j \to \infty$, the factor $1/2$ is absorbed for all sufficiently large j, and

$$\nu(P_j) \geq n_j^{1+\delta}. \qquad \square$$

3 Producing the Fields

It remains to produce fields satisfying the hypotheses of Theorem 2.3. The construction starts from a cyclic cubic field F, builds an infinite unramified pro-3 quotient tower over it, and uses Chebotarev to choose fixed rational primes q_b that split completely in every finite layer. Because the tower is unramified, root discriminants stay bounded; after adjoining i, the class-number estimate below gives the uniform exponential bound needed in the geometric criterion.

Remark 3.1. The class-field-theoretic construction is a specialization of the Hajir–Maire method for building T-split S-ramified p-towers [HM01, Section 2]. In the present proof S is empty, so the tower is unramified, and T is the set of primes of F above the selected rational primes q_b. The Frobenius-killing step below is the same tower-cutting mechanism developed further by Hajir, Maire, and Ramakrishna [HMR21]: choose primes whose Frobenius classes lie in the Frattini subgroup, impose those Frobenius elements as new relations, and retain enough Golod–Shafarevich deficiency for the quotient tower to remain infinite.

3.1 Auxiliary Results for the Field Construction

We first state the number-theoretic results used directly in the construction. A *rational prime* means a prime number in $\mathbb{Z}$. A *prime of a number field* means a nonzero prime ideal in its ring of integers, so one rational prime can have several primes of F above it. Appendix A records the conventions and references behind these results.

The first proposition is the cyclotomic calculation that creates the base field. The conductor language is recalled in Definition A.5. The general tool is the conductor–discriminant formula: if a finite abelian field $L/\mathbb{Q}$ has character group X, then $|D_L| = \prod_{\psi \in X} f(\psi)$, where $f(\psi)$ is the conductor of the character ψ. The exact calculation is needed not only to bound a discriminant. It lets us compare the discriminants of M and F; equality $|D_M| = |D_F|^{[M:F]}$ forces the relative discriminant of M/F to be trivial, hence shows that M/F is unramified. This is what later gives a large elementary abelian quotient of the unramified pro-3 Galois group.

Proposition 3.2. *Let $r_1, \dots, r_\ell$ be distinct rational primes congruent to $1 \bmod 3$. For each i, let L_i be the cyclic cubic subfield of $\mathbb{Q}(\zeta_{r_i})$, and put $M = L_1 \cdots L_\ell$. Let χ_i be a cubic Dirichlet character of conductor r_i, and let $F \subset M$ be the cyclic cubic field cut out by $\chi = \chi_1 \cdots \chi_\ell$ in the sense of Definition A.5. Then the fields L_i are totally real and linearly disjoint,*

$$\mathrm{Gal}(M/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^\ell, \qquad \mathrm{Gal}(M/F) \cong (\mathbb{Z}/3\mathbb{Z})^{\ell-1},$$

and, writing $D = \prod_i r_i$, $|D_F| = D^2$. Moreover, M/F is everywhere unramified.

Proof. The standard cyclotomic facts are that L_i is totally real, has conductor r_i, and is ramified only at r_i. Since the ramified rational primes are disjoint, the L_i's are linearly disjoint, giving the displayed Galois group for $M/\mathbb{Q}$. The product character χ cuts out a cyclic cubic subfield $F \subset M$, and the quotient $\mathrm{Gal}(M/F)$ has rank $\ell - 1$.

Set $D = \prod_i r_i$. The conductor–discriminant formula gives

$$|D_F| = D^2, \qquad |D_M| = D^{2 \cdot 3^{\ell-1}} = |D_F|^{[M:F]}.$$

The tower discriminant formula for the relative discriminant (Definition A.6) says

$$|D_M| = |D_F|^{[M:F]} \, \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{d}_{M/F}).$$

The equality above therefore forces $\mathfrak{d}_{M/F} = \mathcal{O}_F$, so there is no finite ramification in M/F. Both fields are totally real, so there is no infinite ramification either. Hence M/F is everywhere unramified. For background and references, see Proposition A.11, [Was97, Chapter 3, especially Theorem 3.11], and [Neu99, Chapter VI]. □

The next proposition is the group-theoretic step that lets us impose splitting conditions without destroying the tower. If G is a finitely generated pro-p group, its Frattini subgroup is $\Phi(G) = \bigcap_M M$, where M runs over maximal proper open subgroups of G; equivalently $\Phi(G) = \overline{G^p[G,G]}$. It consists of the "non-generators" of G: quotienting by elements in $\Phi(G)$ does not lower the minimal number of generators, though it does add relations. Write $d(G)$ for the minimal number of topological generators, and $r(G)$ for the minimal number of relations in a pro-p presentation.

Proposition 3.3. *Let G be a finitely generated pro-p group. Then $d(G) = \dim_{\mathbb{F}_p} G/\Phi(G)$. If $g_1, \dots, g_k \in \Phi(G)$ and N is their closed normal closure, then $d(G/N) = d(G)$ and $r(G/N) \le r(G) + k$. For definitions and references, see Proposition A.8; in particular [RZ10, Section 2.8], [Koc02, Theorem 4.10], [DdSMS99, Proposition 1.9(ii)].*

We will apply the preceding proposition after choosing Frobenius elements that lie in $\Phi(G)$. The next result is the relation-counting criterion that proves infinitude once the relation rank is small compared with the generator rank.

Proposition 3.4 (Golod–Shafarevich inequality)**.** *If a finite nontrivial pro-p group has generator rank d and relation rank r, then $r > d^2/4$. Equivalently, a nontrivial finitely generated pro-p group with $r \le d^2/4$ is infinite. See Proposition A.9, [GS64, GS65], and [Koc02, Chapter 11].*

Proposition 3.5 (Shafarevich relation-rank estimate)**.** *Let F be a totally real cubic field, so $\zeta_3 \notin F$, and let $G = \mathrm{Gal}(F^{\mathrm{ur},3}/F)$ be the Galois group of its maximal everywhere-unramified pro-3 extension, in the sense of Definition A.3. Then $r(G) \le d(G) + C_0$ for an absolute constant C_0. See Proposition A.10, [Sha63, Sha66], and [NSW08, Chapter X, Section 10].*

We use Chebotarev to find rational primes that are already split at the finite level $E(i)$. Complete splitting in the normal closure of $E(i)$ over $\mathbb{Q}$ simultaneously gives the three properties needed below: the congruence $q_b \equiv 1 \pmod 4$, complete splitting in F, and trivial Frobenius in the Frattini quotient $G/\Phi(G)$. The last property is what lets us kill the corresponding Frobenius elements without decreasing the generator rank of the pro-3 tower.

Proposition 3.6 (Chebotarev density theorem)**.** *Let $G = \mathrm{Gal}(F^{\mathrm{ur},3}/F)$, and let E/F be the finite extension corresponding to the Frattini quotient $G/\Phi(G)$. For any positive integer t, and after excluding any prescribed finite set of rational primes, there exist distinct rational primes $q_1, \dots, q_t$ which split completely in the normal closure over $\mathbb{Q}$ of $E(i)$. For each such prime q_b, $q_b \equiv 1 \pmod 4$ and q_b splits completely in F, and every prime $v \mid q_b$ of F has Frobenius class trivial in $G/\Phi(G)$. Hence a Frobenius representative at v lies in $\Phi(G)$. For references, see Proposition A.12, [Neu99, Chapter VII, Section 13], and [Tsc26].*

Proposition 3.7. *There is an absolute constant $C_{\mathrm{class}} > 0$ such that every number field K satisfies $h(K) \le \max\{2, \mathrm{rd}(K)\}^{C_{\mathrm{class}}[K:\mathbb{Q}]}$. The constant C_{class} is absolute: it is independent of the field K, its degree, and its signature. For fields with $\mathrm{rd}(K) \ge 2$, this is simply $h(K) \le \mathrm{rd}(K)^{O([K:\mathbb{Q}])} = |D_K|^{O(1)}$. This is the class-number consequence of Minkowski's ideal-class bound used in Proposition A.13; see also [Neu99, Chapter I, Section 5] and [Lan94, Chapter V].*

3.2 The Field Construction

We now assemble the results from Subsection 3.1. The parameter ℓ counts the auxiliary cyclic cubic fields in the initial compositum. It will give $t \asymp \ell^2$ split rational primes, while the constant H_ℓ in the class-number bound below has $\log H_\ell = O(\ell \log \ell)$.

Proposition 3.8. *For all sufficiently large integers ℓ, set $t = \lfloor (\ell-1)^2/100 \rfloor$. Then one can find a number field F, distinct rational primes $q_1, \dots, q_t$ fixed independently of j, and fields F_j with $F_0 = F$, satisfying the following properties. Write $f_j = [F_j : \mathbb{Q}]$ and $K_j = F_j(i)$.*

(P1) *The base field F is totally real, cyclic cubic over $\mathbb{Q}$, does not contain ζ_3, and has controlled root discriminant $\log \mathrm{rd}(F) = O(\ell \log \ell)$.*

(P2) *The fields form an infinite tower*

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots$$

such that each F_j/F is finite Galois, everywhere unramified, and has 3-group Galois group. Moreover $f_j \to \infty$.

(P3) *Every F_j is totally real, and the root discriminant is constant: $\mathrm{rd}(F_j) = \mathrm{rd}(F)$.*

(P4) *Each q_b, $1 \le b \le t$, satisfies $q_b \equiv 1 \pmod 4$ and splits completely in every F_j.*

(P5) *There is a constant H_ℓ, independent of j, such that*

$$\mathrm{rd}(K_j) \le 2\,\mathrm{rd}(F), \qquad h(K_j) \le H_\ell^{f_j}, \qquad \log H_\ell = O(\ell \log \ell).$$

(P6) *The contribution from the split primes dominates the class-number loss: $t \log 2 - \log H_\ell > 0$.*

Proof. We build the tower in four steps. We first construct F and a large elementary abelian unramified 3-extension above it. We then impose the splitting conditions by passing to an infinite quotient $\overline{G}$ of the maximal unramified pro-3 group. The finite layers of that quotient give the fields F_j, and the last step checks the class-number and numerical bounds.

Step 1: construct F and the initial generator lower bound. Choose $r_1, \dots, r_\ell$ to be the first ℓ rational primes with $r_i \equiv 1 \pmod 3$. Let L_i be the cyclic cubic subfield of $\mathbb{Q}(\zeta_{r_i})$, and put $M = L_1 \cdots L_\ell$. Let χ_i be a cubic Dirichlet character of conductor r_i. Let F be the cyclic cubic field cut out by the character $\chi = \chi_1 \cdots \chi_\ell$. The conductor language and the phrase "cut out" are explained in Definition A.5; the cyclotomic calculation itself is Proposition 3.2. Applying that proposition, F is a totally real cyclic cubic field, M/F is everywhere unramified, and

$$\mathrm{Gal}(M/F) \cong (\mathbb{Z}/3\mathbb{Z})^{\ell-1}.$$

Since F is totally real, it does not contain the non-real root of unity ζ_3.

Because M/F is an everywhere-unramified 3-extension, the Galois group of the maximal everywhere-unramified pro-3 extension, $G = \mathrm{Gal}(F^{\mathrm{ur},3}/F)$, has a quotient $(\mathbb{Z}/3\mathbb{Z})^{\ell-1}$, and so

$$d(G) \geq \ell - 1. \tag{5}$$

This lower bound is what makes the later choice $t = \lfloor(\ell-1)^2/100\rfloor$ compatible with the Golod–Shafarevich relation count.

Writing $D = \prod_i r_i$, Proposition 3.2 also gives $|D_F| = D^2$. Since the r_i are the first ℓ primes congruent to 1 mod 3, the prime number theorem in arithmetic progressions [Dav00] gives

$$\log \mathrm{rd}(F) = \frac{1}{3}\log|D_F| = \frac{2}{3}\sum_i \log r_i = O(\ell \log \ell). \tag{6}$$

This is the required root-discriminant bound for the base field. Together with the previous paragraph, this proves property P1. The same bound will be used to prove property P5 after the finite layers are constructed.

Step 2: construct an infinite quotient with trivial selected Frobenius classes. Shafarevich's relation-rank estimate (Proposition 3.5) gives

$$r(G) \leq d(G) + C_0 \tag{7}$$

for an absolute constant C_0, because F is totally real cubic and $\zeta_3 \notin F$.

Let E/F be the Frattini quotient extension corresponding to $G/\Phi(G)$, and put $d = d(G)$ and $t = \lfloor(\ell-1)^2/100\rfloor$. By Proposition 3.6, choose distinct rational primes $q_1, \ldots, q_t$, avoiding $3D$, with the stated splitting and Frattini-trivial Frobenius properties. We now pass to a quotient in which the selected Frobenius elements are trivial, so that the selected primes split in all later layers.

There are exactly

$$k = \#\{\, v \subset \mathcal{O}_F : \ v \mid q_b \text{ for some } b \,\} = 3t$$

such primes v of F, because each q_b splits completely in the cubic field F. Choose one Frobenius representative $\sigma_v \in G$ for each of these primes, and let

$$N = \overline{\langle\langle \sigma_v : \ v \mid q_b \text{ for some } b \rangle\rangle} \triangleleft G$$

be their closed normal closure. Set $\overline{G} = G/N$. This adds at most $k = 3t$ relations. Since these representatives lie in $\Phi(G)$, the Frattini quotient identity from Proposition 3.3 gives $d(\overline{G}) = d$, while the relation count is bounded by

$$r(\overline{G}) \leq r(G) + k = r(G) + 3t \leq d + C_0 + \frac{3d^2}{100}.$$

For ℓ, hence d, sufficiently large, the right side is $< d^2/4$. By Golod-Shafarevich, again as stated in Proposition 3.4, $\overline{G}$ is infinite. Thus $\overline{G}$ is infinite, and the selected Frobenius classes are trivial in it. These two facts produce the infinite tower in property P2 and the complete splitting in property P4.

Step 3: extract the tower and prove prescribed splitting. Choose a descending chain

$$\overline{G} = H_0 \supset H_1 \supset H_2 \supset \cdots$$

of open normal subgroups with indices tending to infinity, and let F_j be the corresponding fixed fields. Then F_j/F is finite Galois, everywhere unramified, and has 3-group Galois group; since the indices tend to infinity, $f_j \to \infty$. This proves property P2.

Since trivial Frobenius is equivalent to complete splitting (Definition A.7), the quotient makes the selected Frobenius classes trivial, so each q_b splits completely in every F_j: the Frobenius is already trivial in $\overline{G}$, hence also in each finite quotient corresponding to F_j/F. The congruence $q_b \equiv 1 \pmod 4$ was built into the Chebotarev choice. This proves property P4.

The layers remain totally real: if a real place became complex in F_j/F, the decomposition group at that infinite place would have order 2, impossible inside a 3-group. Finite unramified extensions preserve root discriminant, so $\mathrm{rd}(F_j) = \mathrm{rd}(F)$. This proves property P3.

Step 4: prove the class-number and numerical bounds. Finally put $K_j = F_j(i)$. The relative discriminant $\mathfrak{d}_{K_j/F_j}$ divides $4\mathcal{O}_{F_j}$, so

$$|D_{K_j}| = |D_{F_j}|^2 \,\mathrm{N}_{F_j/\mathbb{Q}}(\mathfrak{d}_{K_j/F_j}) \le |D_{F_j}|^2 4^{f_j}.$$

Taking $2f_j$-th roots, since $[K_j : \mathbb{Q}] = 2f_j$, gives $\mathrm{rd}(K_j) \le 2\,\mathrm{rd}(F)$. Also, because $q_b \equiv 1 \pmod 4$ and q_b splits completely in F_j, each prime $v \mid q_b$ of F_j splits in $K_j = F_j(i)$, as required for the construction of Section 2. The class-number estimate in Proposition 3.7 therefore gives

$$h(K_j) \le (2\,\mathrm{rd}(F))^{C_{\mathrm{class}}[K_j:\mathbb{Q}]} = H_\ell^{f_j}, \quad H_\ell = (2\,\mathrm{rd}(F))^{2C_{\mathrm{class}}}.$$

Thus $\log H_\ell = O(\log \mathrm{rd}(F)) = O(\ell \log \ell)$. This proves property P5.

Finally, the explicit choice of t gives

$$t = \left\lfloor \frac{(\ell-1)^2}{100} \right\rfloor \ge \frac{(\ell-1)^2}{200}$$

for all sufficiently large ℓ. Combining this quadratic lower bound for t with $\log H_\ell = O(\ell \log \ell)$ gives $t \log 2 - \log H_\ell > 0$ for all sufficiently large ℓ, which proves property P6. □

Proof of Theorem 1.1. Choose ℓ large enough that Proposition 3.8 applies and $\gamma := t \log 2 - \log H_\ell > 0$. Then the fields $L_j = F_j$ and fixed rational primes q_b satisfy the hypotheses of Theorem 2.3. Hence there is $\delta > 0$ and a sequence of planar sets P_j, $n_j = |P_j| \to \infty$, with $\nu(P_j) \ge n_j^{1+\delta}$ for all sufficiently large j. Since $\nu(n_j)$ is the maximum over all n_j-point planar sets, $\nu(n_j) \ge \nu(P_j) \ge n_j^{1+\delta}$. The integers n_j tend to infinity, so this gives infinitely many n. □

Remark 3.9. The constants are fixed before the tower level j varies. First choose ℓ large enough that the estimates above give $\gamma = t \log 2 - \log H_\ell > 0$. Chebotarev then gives fixed rational primes $q_1, \ldots, q_t$, and hence the fixed product $Q = \prod_b q_b$. After R is chosen in the averaging argument, these choices determine the fixed constants $\mathcal{D} = Q^2$ and $\mathcal{B} = 2\log(4R\mathcal{D})$. Finally set $\delta = \gamma/(4\mathcal{B}) > 0$. This δ is fixed throughout the infinite tower. Since the degrees $[F_j : \mathbb{Q}]$ tend to infinity, the point-set sizes n_j produced by Theorem 2.3 also tend to infinity.

A Background Facts and Citations

This appendix records conventions and references used above. The main theorems are stated in Section 3.1; the entries below supply the surrounding standard language and sources.

Field and Ramification Conventions

Definition A.1 (Basic field conventions)**.** A number field is a finite extension of $\mathbb{Q}$. A rational prime is a prime number $q \in \mathbb{Z}$, while a finite prime of a number field L is a nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}_L$. A field L is totally real if every embedding $L \hookrightarrow \mathbb{C}$ has image in $\mathbb{R}$. See, for example, [Neu99, Chapter I, Sections 1–5].

Definition A.2 (Splitting, ramification, and unramified extensions)**.** Let M/F be a finite extension and let $\mathfrak{p}$ be a finite prime of F. In the factorization

$$\mathfrak{p}\mathcal{O}_M = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})},$$

the exponent $e(\mathfrak{P}/\mathfrak{p})$ is the ramification index. The prime $\mathfrak{p}$ is unramified if all these indices are 1, and it splits completely if there are $[M : F]$ primes above it, all unramified and with residue degree 1. For a rational prime q, complete splitting in L means $q\mathcal{O}_L = \mathfrak{p}_1 \cdots \mathfrak{p}_{[L:\mathbb{Q}]}$ and $\mathcal{O}_L/\mathfrak{p}_i \cong \mathbb{F}_q$.

Infinite ramification concerns Archimedean places: a real place ramifies if it becomes complex. Thus a totally real extension of a totally real field has no infinite ramification. "Everywhere unramified" means unramified at all finite and infinite places.

Definition A.3 (Maximal unramified pro-p extension)**.** For a number field F, $F^{\mathrm{ur},p}$ denotes the compositum of all finite everywhere-unramified Galois extensions of F whose Galois groups are finite p-groups. Its Galois group $\mathrm{Gal}(F^{\mathrm{ur},p}/F)$ is a pro-p group, and its finite quotients correspond to finite everywhere-unramified Galois p-group extensions of F.

Definition A.4 (CM fields)**.** A CM field is a totally imaginary quadratic extension K/K^+ of a totally real field. The nontrivial automorphism of K/K^+ is denoted c. In this paper $K = L(i)$ with L totally real, and for every complex embedding $\sigma : K \hookrightarrow \mathbb{C}$, $\sigma(c(\alpha)) = \overline{\sigma(\alpha)}$. Consequently, elements u with $u\,c(u) = 1$ have $|\sigma(u)| = 1$ in every complex embedding.

Definition A.5 (Conductors and fields cut out by characters)**.** For a finite abelian extension $L/\mathbb{Q}$, the Kronecker–Weber theorem embeds L in a cyclotomic field $\mathbb{Q}(\zeta_m)$. The field conductor is the least such m. A Dirichlet character χ has conductor $f(\chi)$, the least modulus of a primitive Dirichlet character inducing χ.

Choose a common modulus m for a finite subgroup X of Dirichlet characters, for instance a common multiple of their conductors. Via $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$, the group X determines the fixed field of the common kernel $\bigcap_{\chi\in X} \ker\chi$. If $X = \langle\chi\rangle$, we say that this field is cut out by χ. Thus an order-3 character cuts out a cyclic cubic field.

Definition A.6 (Discriminants)**.** The absolute discriminant of L is denoted D_L. For an extension M/F, the relative discriminant $\mathfrak{d}_{M/F}$ is an ideal of $\mathcal{O}_F$, and the tower formula is

$$|D_M| = |D_F|^{[M:F]}\,\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{d}_{M/F}).$$

Thus $\mathfrak{d}_{M/F} = \mathcal{O}_F$ is equivalent to no finite ramification in M/F. The root discriminant is $\mathrm{rd}(L) = |D_L|^{1/[L:\mathbb{Q}]}$. Finite unramified extensions preserve root discriminant.

Definition A.7 (Frobenius elements)**.** Let N/K be a finite Galois extension and let $\mathfrak{p}$ be a finite prime of K unramified in N. For a prime $\mathfrak{P} \mid \mathfrak{p}$ of N, the Frobenius element $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}} \in \mathrm{Gal}(N/K)$ acts on the residue field by $x \mapsto x^{|\mathcal{O}_K/\mathfrak{p}|}$. In a nonabelian extension only its conjugacy class is independent of $\mathfrak{P}$. The prime $\mathfrak{p}$ splits completely in N exactly when this Frobenius class is the identity. See [Neu99, Chapter VII, Section 13].

Group-Theoretic and Class-Field References

Proposition A.8. For a finitely generated pro-p group G, the Frattini subgroup satisfies $\Phi(G) = \bigcap_M M = \overline{G^p[G,G]}$, where M runs over maximal proper open subgroups. Burnside's basis theorem gives $d(G) = \dim_{\mathbb{F}_p} G/\Phi(G)$. If $g_1, \dots, g_k \in \Phi(G)$ and N is their closed normal closure, then $d(G/N) = d(G)$ and $r(G/N) \le r(G) + k$. See [RZ10, Section 2.8], [Koc02, Theorem 4.10], and [DdSMS99, Proposition 1.9(ii)].

Proposition A.9 (Golod–Shafarevich inequality)**.** If a finite nontrivial pro-p group has generator rank d and relation rank r, then $r > d^2/4$. Equivalently, a nontrivial finitely generated pro-p group with $r \le d^2/4$ is infinite. See [GS64, GS65] and [Koc02, Chapter 11].

Proposition A.10 (Shafarevich relation-rank estimate)**.** Shafarevich's estimate bounds the relation rank of Galois groups of maximal pro-p extensions with prescribed ramification. In the only form used here, if F is totally real cubic, $\zeta_3 \notin F$, and $G = \mathrm{Gal}(F^{\mathrm{ur},3}/F)$, then $r(G) \le d(G) + C_0$ for an absolute constant C_0. See [Sha63, Sha66] and [NSW08, Chapter X, Section 10].

Proposition A.11. If r is a rational prime with $r \equiv 1 \pmod 3$, the unique cyclic cubic subfield of $\mathbb{Q}(\zeta_r)$ is totally real, has conductor r, and is ramified only at r. For a finite abelian extension $L/\mathbb{Q}$ with character group X, the conductor–discriminant formula is $|D_L| = \prod_{\chi \in X} f(\chi)$. For characters with pairwise coprime conductors, $f(\chi_1 \cdots \chi_m) = \prod_i f(\chi_i)$, ignoring conductor-1 trivial factors. These are standard facts from cyclotomic class field theory; see [Was97, Chapter 3, especially Theorem 3.11] and [Neu99, Chapter VI].

Proposition A.12 (Chebotarev density theorem)**.** Chebotarev's density theorem implies that, after excluding finitely many bad primes, infinitely many rational primes split completely in any prescribed finite Galois extension of $\mathbb{Q}$. Applied to the normal closure over $\mathbb{Q}$ of $E(i)$, where E/F is the Frattini quotient extension corresponding to $G/\Phi(G)$, it gives the primes used in Proposition 3.6. See [Neu99, Chapter VII, Section 13] and [Tsc26].

Proposition A.13. Minkowski's ideal-class bound, combined with the elementary divisor-function bound for the number of ideals of a given norm, gives $h(K) \le \max\{2, \mathrm{rd}(K)\}^{O([K:\mathbb{Q}])}$, with an absolute implicit constant. Equivalently, when $\mathrm{rd}(K) \ge 2$, $h(K) \le |D_K|^{O(1)}$. See [Neu99, Chapter I, Section 5] and [Lan94, Chapter V].

References

[ABS25] Noga Alon, Matija Bucić, and Lisa Sauermann. Unit and distinct distances in typical norms. *Geometric and Functional Analysis*, 35:1–42, 2025.

[ÁP22] Péter Ágoston and Dömötör Pálvölgyi. An improved constant factor for the unit distance problem. *Studia Scientiarum Mathematicarum Hungarica*, 2022.

[BBF+10] Ondřej Bílka, Kevin Buchin, Radoslav Fulek, Masashi Kiyomi, Yoshio Okamoto, Shin-ichi Tanigawa, and Csaba D. Tóth. A tight lower bound for convexly independent subsets of the Minkowski sums of planar point sets. *Electronic Journal of Combinatorics*, 17(1):Note 35, 2010.

[BMP05] Peter Brass, William O. J. Moser, and János Pach. *Research Problems in Discrete Geometry*. Springer, New York, 2005.

[Bra96] Peter Brass. Erdős distance problems in normed spaces. *Computational Geometry*, 6(4):195–214, 1996.

[Dav00] Harold Davenport. *Multiplicative Number Theory*, volume 74 of *Graduate Texts in Mathematics*. Springer, New York, third edition, 2000. Revised by Hugh L. Montgomery.

[DdSMS99] John D. Dixon, Marcus P. F. du Sautoy, Avinoam Mann, and Dan Segal. *Analytic Pro-p Groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.

[EF97] Paul Erdős and Peter C. Fishburn. Minimum planar sets with maximum equidistance counts. *Computational Geometry*, 7(4):207–218, 1997.

[EPRS08] Friedrich Eisenbrand, János Pach, Thomas Rothvoß, and Nir B. Sopher. Convexly independent subsets of the Minkowski sum of planar point sets. *Electronic Journal of Combinatorics*, 15(1):Note 8, 2008.

[Erd46] Paul Erdős. On sets of distances of n points. *American Mathematical Monthly*, 53(5):248–250, 1946.

[GK15] Larry Guth and Nets Hawk Katz. On the Erdős distinct distances problem in the plane. *Annals of Mathematics*, 181(1):155–190, 2015.

[GS64] E. S. Golod and I. R. Shafarevich. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28(2):261–272, 1964. English translation: Amer. Math. Soc. Transl. (2) 48 (1965), 91–102.

[GS65] E. S. Golod and I. R. Shafarevich. On class field towers. In *Fourteen Papers on Logic, Algebra, Complex Variables and Topology*, volume 48 of *American Mathematical Society Translations, Series 2*, pages 91–102. American Mathematical Society, Providence, RI, 1965. English translation of the 1964 Russian paper.

[GST25] Josef Greilhuber, Carl Schildkraut, and Jonathan Tidor. More unit distances in arbitrary norms. *Bulletin of the London Mathematical Society*, 57(9):2885–2901, 2025.

[HM01] Farshid Hajir and Christian Maire. Asymptotically good towers of global fields. In Carles Casacuberta, Rosa Maria Miró-Roig, Joan Verdera, and Sebastià Xambó-Descamps, editors, *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, volume 202 of *Progress in Mathematics*, pages 207–218. Birkhäuser, Basel, 2001.

[HMR21] Farshid Hajir, Christian Maire, and Ravi Ramakrishna. Cutting towers of number fields. *Annales Mathématiques du Québec*, 45(2):321–345, 2021.

[Koc02] Helmut Koch. *Galois Theory of p-Extensions*. Springer Monographs in Mathematics. Springer, Berlin, Heidelberg, 2002.

[KST54] Tamás Kővári, Vera T. Sós, and Pál Turán. On a problem of K. Zarankiewicz. *Colloquium Mathematicum*, 3:50–57, 1954.

[Lan94] Serge Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 1994.

[Mat11] Jiří Matoušek. The number of unit distances is almost linear for most norms. *Advances in Mathematics*, 226(3):2618–2628, 2011.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer, Berlin, Heidelberg, 1999. Translated from the German by Norbert Schappacher; with a foreword by G. Harder.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften*. Springer, Berlin, Heidelberg, second edition, 2008.

[RZ10] Luis Ribes and Pavel Zalesskii. *Profinite Groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge*. Springer, Berlin, Heidelberg, second edition, 2010.

[Sha63] Igor R. Shafarevich. Extensions à points de ramification donnés (en russe). *Publications Mathématiques de l'IHÉS*, 18:71–92, 1963.

[Sha66] Igor R. Shafarevich. Extensions with given points of ramification. *American Mathematical Society Translations, Series 2*, 59:128–149, 1966. English translation by J. W. S. Cassels; title also cited as "Extensions with prescribed ramification points".

[SST84] Joel H. Spencer, Endre Szemerédi, and William T. Trotter. Unit distances in the Euclidean plane. In Béla Bollobás, editor, *Graph Theory and Combinatorics*, pages 293–303. Academic Press, London, 1984. Proceedings of the Cambridge Conference, 1983.

[Sze97] László A. Székely. Crossing numbers and hard Erdős problems in discrete geometry. *Combinatorics, Probability and Computing*, 6(3):353–358, 1997.

[Tsc26] N. Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Mathematische Annalen*, 95(1):191–228, 1926.

[Val05] Pavel Valtr. Strictly convex norms allowing many unit distances and related touching questions. Manuscript, 2005.

[Was97] Lawrence C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 1997.