A COUNTEREXAMPLE TO THE ERDŐS–SZEMERÉDI $n^{2-\varepsilon}$ SUM–PRODUCT BOUND OVER $\mathbb{R}$

Abstract. We show that the Erdős–Szemerédi sum–product conjecture over $\mathbb{R}$ — asserting that for every $\varepsilon > 0$ all sufficiently large finite sets $A \subset \mathbb{R}$ satisfy $\max(|A+A|, |A \cdot A|) \geq |A|^{2-\varepsilon}$ — is false for a fixed absolute ε. Concretely, taking $\varepsilon_0 = 10^{-5}$ we exhibit an infinite family of finite sets $A \subset \mathbb{R}$ with $\max(|A+A|, |A \cdot A|) < |A|^{2-\varepsilon_0}$. The sets are orbits of units acting on a fixed box of algebraic integers inside totally real number fields of growing degree and bounded root discriminant, drawn from an infinite unramified 2-class-field tower. All inputs are classical and unconditional: geometry of numbers, Dirichlet's unit theorem, the analytic class number formula, Louboutin's residue bound, genus theory, and the Golod–Shafarevich criterion. The examples are consistent with the known lower bounds $\max(|A+A|, |A \cdot A|) \gg |A|^{4/3+c}$; the degree of the number field must grow like $\log |A|$, so the mechanism is invisible in the bounded-degree regime.

1. Introduction

For a finite set $A \subset \mathbb{R}$ write $A + A = \{a + b : a, b \in A\}$ and $A \cdot A = \{ab : a, b \in A\}$. The sum–product phenomenon asserts that at least one of these two sets must be substantially larger than A itself. Erdős and Szemerédi conjectured that $\max(|A + A|, |A \cdot A|) \geq |A|^{2-o(1)}$; equivalently:

> *For every $\varepsilon > 0$ there exists n_0 such that every finite $A \subset \mathbb{R}$ with $|A| = n \geq n_0$ satisfies* $\max(|A + A|, |A \cdot A|) \geq n^{2-\varepsilon}$.

We disprove this conjecture: the statement fails already for a single fixed value of ε.

Theorem 1.1 (Main Theorem)**.** *There is an absolute constant $\varepsilon_0 > 0$ (one may take $\varepsilon_0 = 10^{-5}$) and an infinite set $\mathcal{N} \subset \mathbb{N}$ such that for every $n \in \mathcal{N}$ there is a finite set $A \subset \mathbb{R}$ with $|A| = n$ and*

$$\max\big(|A + A|,\, |A \cdot A|\big) \;<\; n^{2-\varepsilon_0}.$$

In particular, for $\varepsilon = \varepsilon_0$ there is no n_0 as in the displayed statement.

Strategy. Fix a totally real number field K of degree d with ring of integers $\mathcal{O}_K$ and real embeddings $\sigma_1, \ldots, \sigma_d$. We build a set $A = \sigma_1(U \cdot X)$, where U is a set of units all of whose conjugates lie in a fixed band $[e^{-\Theta}, e^{\Theta}]$, and X is a fixed box of algebraic integers. Three elementary mechanisms operate.

1. *Sums are controlled by a box.* All elements have conjugates bounded by a fixed $H = H(\Theta)$, independent of $|A|$. Distinct algebraic integers are 1-separated in the Minkowski sup-norm, so a box of radius M contains at most $(2M + 1)^d$ integers. Hence $|A + A| \leq (4H + 1)^d$, a bound *independent of how many points A packs into its box.*
2. *Products are controlled by the unit group.* Since $A = U \cdot X$, we have $A \cdot A \subseteq (U \cdot U) \cdot (X \cdot X)$, and $U \cdot U$ is again a band of units; a covering argument shows passing from U to $U \cdot U$ costs at most a factor 5^d. Thus $|A \cdot A| \leq 5^d |U||X|^2$, while $|A|^2 = |U|^2|X|^2$: the product set is smaller than $|A|^2$ by a factor $\asymp |U|5^{-d}$.
3. *Unique factorisation fixes the size.* Choosing $X \subset 1 + m\mathcal{O}_K$ with m larger than the house of any ratio of two units of U forces the representation $a = ux$ to be unique, so $|A| = |U||X|$ exactly.

To beat the exponent 2 we need $|U| \geq e^{cd}$ for units of *constant* height bound Θ, while all losses (5^d, box-count discrepancies, $\sqrt{|\Delta_K|}$) are $e^{O(d)}$. The decisive input is a regulator bound $\mathrm{Reg}_K \leq e^{Cd}$ with an absolute constant C; then the rank-$(d-1)$ unit lattice, of covolume $\asymp \mathrm{Reg}_K$, has at least $\Theta^{d-1}/(3d\,\mathrm{Reg}_K) \geq e^{(\log\Theta - C - o(1))d}$ points in the cube of side 2Θ. Choosing $\log\Theta > C + \log 5$ makes the product-set saving a genuine power of $n = |A|$. The regulator bound follows for *any* field of bounded root discriminant from the analytic class number formula, Louboutin's residue bound, and $h_K \geq 1$; infinitely many totally real fields of bounded root discriminant with $d \to \infty$ arise from the Golod–Shafarevich infinite class field tower.

Throughout, $A = \sigma_1(S)$ for a finite $S \subset K$, and since σ_1 is an injective field homomorphism we have $|A| = |S|$, $|A + A| = |S + S|$, $|A \cdot A| = |S \cdot S|$, with the latter computed inside K. We therefore do all counting inside K without further comment.

2. Number-theoretic preliminaries

2.1. **Boxes of algebraic integers.** Let K be a totally real number field of degree $d \geq 2$ with real embeddings $\sigma_1, \ldots, \sigma_d : K \to \mathbb{R}$, ring of integers $\mathcal{O}_K$ and discriminant Δ_K. Let

$$\iota : K \to \mathbb{R}^d, \qquad \iota(x) = (\sigma_1(x), \ldots, \sigma_d(x)),$$

be the Minkowski embedding, and for $M > 0$ put

$$B_M := \{x \in \mathcal{O}_K : \ |\sigma_i(x)| \leq M \text{ for } i = 1, \ldots, d\}.$$

Fact 2.1. $\iota(\mathcal{O}_K)$ is a full-rank lattice in $\mathbb{R}^d$ of covolume $\sqrt{|\Delta_K|}$.

See e.g. Neukirch, *Algebraic Number Theory*, Prop. I.5.2; for a totally real field all embeddings are real, so no factor 2^{-r_2} appears.

Lemma 2.2 (packing bound)**.** *For every $M \geq 0$, $|B_M| \leq (2M+1)^d$.*

Proof. If $x \neq y$ in $\mathcal{O}_K$, then $x - y$ is a nonzero algebraic integer, so its norm $N(x-y) = \prod_i \sigma_i(x-y)$ is a nonzero rational integer; hence $\prod_i |\sigma_i(x-y)| \geq 1$ and $\max_i |\sigma_i(x-y)| \geq 1$. Thus the points $\iota(x)$, $x \in B_M$, lie in $[-M, M]^d$ and are pairwise at sup-distance ≥ 1. The open axis-parallel unit cubes centred at these points are pairwise disjoint and lie in $[-M - \frac{1}{2}, M + \frac{1}{2}]^d$, of volume $(2M+1)^d$; each has volume 1, so there are at most $(2M+1)^d$ points. □

Theorem 2.3 (van der Corput)**.** *Let $\Lambda \subset \mathbb{R}^n$ be a full-rank lattice and $S \subset \mathbb{R}^n$ a bounded convex body symmetric about the origin. If $\mathrm{vol}(S) > m \cdot 2^n \det\Lambda$ for a positive integer m, then S contains at least $2m$ nonzero points of Λ.*

See van der Corput, Acta Arith. 2 (1936), 145–146, or Cassels, *An Introduction to the Geometry of Numbers*, Ch. III, Thm. II. For $m = 1$ this is Minkowski's first theorem.

Corollary 2.4. *In the setting of Theorem 2.3, if $\mathrm{vol}(S) \geq 2^{n+1} \det\Lambda$ then*

$$\#(S \cap \Lambda) \ \geq \ \frac{\mathrm{vol}(S)}{2^n \det\Lambda}.$$

Proof. Put $q := \mathrm{vol}(S)/(2^n \det\Lambda) \geq 2$ and $m := \lceil q \rceil - 1 \geq 1$. Then $m < q$, so Theorem 2.3 gives at least $2m$ nonzero lattice points in S; adding the origin, $\#(S \cap \Lambda) \geq 2m + 1 \geq 2(q-1) + 1 \geq q$. □

Lemma 2.5 (box lower bound)**.** *If $M^d \geq 2\sqrt{|\Delta_K|}$, then $|B_M| \geq M^d/\sqrt{|\Delta_K|}$.*

Proof. Apply Corollary 2.4 to $\Lambda = \iota(\mathcal{O}_K)$ (covolume $\sqrt{|\Delta_K|}$ by Fact 2.1) and $S = [-M, M]^d$, of volume $(2M)^d = 2^d M^d \geq 2^{d+1}\sqrt{|\Delta_K|}$. This gives $\#(S \cap \Lambda) \geq (2M)^d/(2^d\sqrt{|\Delta_K|}) = M^d/\sqrt{|\Delta_K|}$, and every lattice point of S is $\iota(x)$ for some $x \in B_M$. □

2.2. **Units: a counting lower bound and a doubling upper bound.** Let $\mathcal{O}_K^\times$ be the unit group and

$$\ell : \mathcal{O}_K^\times \to \mathbb{R}^d, \qquad \ell(u) = \big(\log|\sigma_1(u)|, \dots, \log|\sigma_d(u)|\big).$$

Since $|N(u)| = 1$, the image lies in the hyperplane $H := \{v \in \mathbb{R}^d : \ v_1 + \cdots + v_d = 0\}$.

Fact 2.6 (Dirichlet's unit theorem)**.** For a totally real field of degree d we have $\ker(\ell) = \{\pm 1\}$ and $\Lambda_U := \ell(\mathcal{O}_K^\times)$ is a full-rank lattice in the $(d-1)$-dimensional space H. For a fundamental system $u_1, \dots, u_{d-1}$ (so that $\ell(u_1), \dots, \ell(u_{d-1})$ is a $\mathbb{Z}$-basis of Λ_U), the regulator

$$\mathrm{Reg}_K := \big|\det\big(\log|\sigma_j(u_i)|\big)_{1\le i,j\le d-1}\big|$$

is independent of the choice of $d-1$ embeddings and of the fundamental system.

See Neukirch, *Algebraic Number Theory*, §I.7. For $\Theta > 0$ define the *unit box*

$$U_\Theta := \{u \in \mathcal{O}_K^\times : \ e^{-\Theta} \le |\sigma_i(u)| \le e^{\Theta} \ \forall i\} = \{u : \ \ell(u) \in [-\Theta, \Theta]^d\}.$$

Note $U_\Theta \cdot U_\Theta \subseteq U_{2\Theta}$ and $u/u' \in U_{2\Theta}$ for $u, u' \in U_\Theta$.

Lemma 2.7 (unit count)**.** *If $\Theta^d \ge 2(2\Theta+1)\, d\ \mathrm{Reg}_K$, then*

$$|U_\Theta| \ \ge \ \frac{\Theta^{d-1}}{3\, d\ \mathrm{Reg}_K}.$$

Proof. Let L be the $(d-1)\times d$ matrix with rows $\ell(u_1), \dots, \ell(u_{d-1})$, and let $\mathbf{1} = (1, \dots, 1) \in \mathbb{R}^d$. Set $v_0 := (2\Theta+1)\mathbf{1}$ and $\widetilde{\Lambda} := \Lambda_U + \mathbb{Z}v_0$. Since $v_0 \notin H$ and Λ_U spans H, the vectors $\ell(u_1), \dots, \ell(u_{d-1}), v_0$ are linearly independent and form a $\mathbb{Z}$-basis of $\widetilde{\Lambda}$, which is therefore a full-rank lattice in $\mathbb{R}^d$ with

$$\det\widetilde{\Lambda} = \left|\det\begin{pmatrix} L \\ v_0 \end{pmatrix}\right| = (2\Theta+1)\left|\det\begin{pmatrix} L \\ \mathbf{1} \end{pmatrix}\right|.$$

Expanding the last determinant along its final row, $\det\begin{pmatrix} L \\ \mathbf{1} \end{pmatrix} = \sum_{j=1}^{d}(-1)^{d+j}M_j$, where M_j is the minor of L obtained by deleting column j. The vector $c := \big((-1)^{d+1}M_1, \dots, (-1)^{d+d}M_d\big)$ satisfies $\langle c, \ell(u_i)\rangle = 0$ for each i (it is the expansion of a determinant with a repeated row), i.e. $c \perp H$; hence $c = \lambda\mathbf{1}$ for some $\lambda \in \mathbb{R}$, so all signed minors $(-1)^{d+j}M_j$ equal λ, and $|\lambda| = |M_d| = \mathrm{Reg}_K$. Therefore $\left|\det\begin{pmatrix} L \\ \mathbf{1} \end{pmatrix}\right| = d\ \mathrm{Reg}_K$ and

$$\det\widetilde{\Lambda} = (2\Theta+1)\, d\ \mathrm{Reg}_K\,.$$

Apply Corollary 2.4 to $\widetilde{\Lambda}$ and $S = [-\Theta, \Theta]^d$: the hypothesis $\mathrm{vol}(S) = 2^d\Theta^d \ge 2^{d+1}(2\Theta+1)d\ \mathrm{Reg}_K$ holds by assumption, so

$$\#\big(\widetilde{\Lambda} \cap [-\Theta, \Theta]^d\big) \ \ge \ \frac{\Theta^d}{(2\Theta+1)\, d\ \mathrm{Reg}_K} \ \ge \ \frac{\Theta^{d-1}}{3\, d\ \mathrm{Reg}_K}.$$

Finally, every point $\lambda + kv_0$ ($\lambda \in \Lambda_U$, $k \in \mathbb{Z}$) of $\widetilde{\Lambda} \cap [-\Theta, \Theta]^d$ has coordinate sum $kd(2\Theta+1)$, while any point of $[-\Theta, \Theta]^d$ has coordinate sum of absolute value at most $d\Theta < d(2\Theta+1)$; hence $k = 0$ and the point lies in Λ_U. Each such $v = \ell(u)$ gives a unit $u \in U_\Theta$, and distinct lattice points give distinct units, whence $|U_\Theta| \ge \Theta^{d-1}/(3d\ \mathrm{Reg}_K)$. □

Lemma 2.8 (doubling of the unit count)**.** *For every $\Theta > 0$, $|U_{2\Theta}| \le 5^d|U_\Theta|$.*

Proof. Write $B := [-\Theta,\Theta]^d$, so $2B = [-2\Theta,2\Theta]^d$, and $\Lambda := \Lambda_U$. Since $u \mapsto \ell(u)$ is 2-to-1 onto Λ (Fact 2.6) and, for any T, $u \in U_T$ iff $\ell(u) \in [-T,T]^d$, it suffices to show $\#(\Lambda\cap 2B) \le 5^d\,\#(\Lambda\cap B)$.

Choose a maximal $\{y_1,\dots,y_m\} \subseteq \Lambda \cap 2B$ with the sets $y_i + \frac12 B$ pairwise disjoint. These lie in $2B + \frac12 B = \frac52 B$, so comparing volumes, $m\,\mathrm{vol}(\frac12 B) \le \mathrm{vol}(\frac52 B)$, i.e. $m \le 5^d$. By maximality, every $y \in \Lambda \cap 2B$ satisfies $(y+\frac12 B)\cap(y_i+\frac12 B) \neq \emptyset$ for some i, i.e. $y \in y_i + B$. Hence

$$\#(\Lambda\cap 2B) \;\le\; \sum_{i=1}^{m} \#\big((\Lambda - y_i)\cap B\big) = m\,\#(\Lambda\cap B) \le 5^d\,\#(\Lambda\cap B),$$

using $\Lambda - y_i = \Lambda$. □

2.3. **An upper bound for the regulator.**

Theorem 2.9 (analytic class number formula)**.** *For a number field K of degree d with r_1 real and r_2 complex places, class number h_K, regulator Reg_K, w_K roots of unity, and discriminant Δ_K,*

$$\kappa_K := \operatorname*{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K\,\mathrm{Reg}_K}{w_K\sqrt{|\Delta_K|}}.$$

Theorem 2.10 (Louboutin)**.** *For every number field $K \neq \mathbb{Q}$ of degree d,*

$$\kappa_K \;\le\; \Big(\frac{e\,\log|\Delta_K|}{2(d-1)}\Big)^{d-1}.$$

See S. Louboutin, *Explicit upper bounds for residues of Dedekind zeta functions …*, Canad. J. Math. 53 (2001), 1194–1222, Thm. 1; also J. Number Theory 85 (2000), 263–282. Any bound of shape $\kappa_K \le (C_0 \log|\Delta_K|/d)^{d-1}$ would suffice below.

Lemma 2.11 (regulator bound)**.** *Let K be totally real of degree $d \ge 2$ with root discriminant $|\Delta_K|^{1/d} \le e^{\gamma}$, $\gamma \ge 4$. Then*

$$\mathrm{Reg}_K \;\le\; e^{C_R\,d}, \qquad C_R := \frac{\gamma}{2} + 1 + \log\frac{\gamma}{4}.$$

Proof. For totally real K we have $r_1 = d$, $r_2 = 0$, $w_K = 2$. By Theorem 2.9 and $h_K \ge 1$,

$$\mathrm{Reg}_K \le h_K\,\mathrm{Reg}_K = \frac{2\kappa_K\sqrt{|\Delta_K|}}{2^d}.$$

By Theorem 2.10 and $\log|\Delta_K| \le \gamma d$,

$$\kappa_K \le \Big(\frac{e\gamma d}{2(d-1)}\Big)^{d-1} = \Big(\frac{e\gamma}{2}\Big)^{d-1}\Big(\frac{d}{d-1}\Big)^{d-1} \le e\Big(\frac{e\gamma}{2}\Big)^{d-1}.$$

Hence

$$\mathrm{Reg}_K \le \frac{2e}{2^d}\Big(\frac{e\gamma}{2}\Big)^{d-1} e^{\gamma d/2} = \frac{4}{\gamma}\Big(\frac{e\gamma}{4}\Big)^{d} e^{\gamma d/2} = \frac{4}{\gamma}\,e^{d(1+\log(\gamma/4)+\gamma/2)} \le e^{C_R d},$$

using $\gamma \ge 4$ in the last step. □

2.4. **An infinite family of totally real fields of bounded root discriminant.**

Theorem 2.12 (Golod–Shafarevich criterion)**.** *Let F be a number field and p a prime. If*

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

where d_p is the $\mathbb{F}_p$-rank of the p-torsion, $\mathrm{Cl}(F)$ is the ideal class group, and $\delta_p(F) = 1$ if $\mu_p \subset F$ and 0 otherwise, then the Hilbert p-class field tower $F = F^{(0)} \subset F^{(1)} \subset \cdots$ (with $F^{(i+1)}$ the maximal unramified abelian p-extension of $F^{(i)}$, unramified at all places) is infinite.

See Golod–Shafarevich, Izv. Akad. Nauk SSSR 28 (1964), 261–272, with Shafarevich's relation-rank bound; or P. Roquette, *On class field towers*, in Cassels–Fröhlich (eds.), *Algebraic Number Theory*, Academic Press 1967, Ch. IX; or H. Koch, *Galois Theory of p-Extensions*, Springer 2002, Thm. 11.16 and §11.4. The Galois group G of the maximal unramified p-extension satisfies $d(G) = d_p(\mathrm{Cl}(F))$ and $r(G) \le d(G) + r_1 + r_2 - 1 + \delta_p$, and a finite p-group obeys $r(G) > d(G)^2/4$.

Lemma 2.13 (genus theory)**.** *Let $F = \mathbb{Q}(\sqrt{D})$ be real quadratic with discriminant having exactly t distinct prime divisors. Then the narrow class group $\mathrm{Cl}^+(F)$ has 2-rank $t-1$, and $\mathrm{Cl}(F)$ has 2-rank at least $t-2$.*

This is Gauss's genus theory; see e.g. D. A. Cox, *Primes of the Form $x^2 + ny^2$*. The second statement follows because the kernel of $\mathrm{Cl}^+(F) \twoheadrightarrow \mathrm{Cl}(F)$ has order at most 2, and quotienting by a group of order 2 drops the 2-rank by at most 1.

Proposition 2.14 (the tower)**.** *Let $D := 3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23 = 111\,546\,435$ and $F_0 := \mathbb{Q}(\sqrt{D})$. There is an infinite sequence of number fields $F_0 \subset F_1 \subset F_2 \subset \cdots$ such that for every $j \ge 1$:*

1. *F_j is totally real;*
2. *$[F_j : \mathbb{Q}] \to \infty$ as $j \to \infty$;*
3. *$|\Delta_{F_j}|^{1/[F_j:\mathbb{Q}]} = |\Delta_{F_0}|^{1/2} = 2\sqrt{D} < 21\,124$.*

Proof. Since $D \equiv 3 \pmod 4$ and D is squarefree, $\Delta_{F_0} = 4D$, whose distinct prime divisors are $2, 3, 5, 7, 11, 13, 17, 19, 23$; thus $t = 9$ and, by Lemma 2.13, $d_2(\mathrm{Cl}(F_0)) \ge 7$. For F_0 real quadratic, $r_1 = 2$, $r_2 = 0$, $\delta_2 = 1$ (as $-1 \in F_0$), so the Golod–Shafarevich threshold in Theorem 2.12 is $2 + 2\sqrt{3} < 5.47 < 7$. Hence the Hilbert 2-class field tower of F_0 is infinite; let $F_j := F_0^{(j)}$.

Each $F^{(i+1)}/F^{(i)}$ is unramified at all places, hence so is F_j/F_0. Unramifiedness at the infinite places means no real place becomes complex, so each F_j is totally real, giving (1). The tower being infinite means $F_j \subsetneq F_{j+1}$ for all j, so the degrees strictly increase, giving (2). Since F_j/F_0 is unramified at all finite places, the relative different is trivial, and the conductor–discriminant (transitivity) formula gives $\Delta_{F_j} = \pm\Delta_{F_0}^{[F_j:F_0]}$; taking $[F_j : \mathbb{Q}]$-th roots gives (3). □

We record the numerical consequence: every $K = F_j$ from Proposition 2.14 is totally real with

$$|\Delta_K|^{1/d} \le e^{\gamma}, \qquad \gamma := \log(2\sqrt{D}) < 9.96,$$

and hence, by Lemma 2.11 (note $\gamma > 4$),

$$\mathrm{Reg}_K \le e^{C_R d}, \qquad C_R = \frac{\gamma}{2} + 1 + \log\frac{\gamma}{4} < 6.90.$$

3. The construction

Throughout this section $K = F_j$ is one of the fields of Proposition 2.14, of degree d, and we use the absolute constants

$$\gamma < 9.96, \quad C_R < 6.90, \quad \Theta := e^9, \quad m := \lceil e^{2\Theta} \rceil + 2, \quad s := 3\Theta + 30, \quad S := e^s, \quad R := 1 + mS.$$

These are fixed (astronomically large but independent of d). Define

$$X := 1 + m\,B_S = \{1 + my : \ y \in \mathcal{O}_K,\ |\sigma_i(y)| \le S\ \forall i\}, \qquad A_K := U_\Theta \cdot X = \{ux : \ u \in U_\Theta,\ x \in X\},$$

and finally $A := \sigma_1(A_K) \subset \mathbb{R}$.

Basic size facts: every $x \in X$ has $|\sigma_i(x)| \le 1 + mS = R$ for all i, and every $a = ux \in A_K$ has $|\sigma_i(a)| \le e^{\Theta} R$ for all i. Also $0 \notin A_K$, and $|A| = |A_K|$, $|A + A| = |A_K + A_K|$, $|A \cdot A| = |A_K \cdot A_K|$ since σ_1 is an injective field homomorphism.

3.1. The size of A.

Lemma 3.1 (unique factorisation)**.** *The map $U_\Theta \times X \to K$, $(u,x) \mapsto ux$, is injective. Consequently*

$$|A| = |U_\Theta| \cdot |X| = |U_\Theta| \cdot |B_S|.$$

Proof. Suppose $ux = u'x'$ with $u, u' \in U_\Theta$, $x, x' \in X$. Set $w := u/u' = x'/x \in \mathcal{O}_K^\times$. For each i,

$$|\sigma_i(w)| = \frac{|\sigma_i(u)|}{|\sigma_i(u')|} \le \frac{e^\Theta}{e^{-\Theta}} = e^{2\Theta}.$$

Since $x \equiv 1 \equiv x' \pmod{m\mathcal{O}_K}$, in $\mathcal{O}_K/m\mathcal{O}_K$ both classes equal that of 1, and from $wx = x'$ we get $\bar{w} = \bar{1}$, i.e. $w \equiv 1 \pmod{m\mathcal{O}_K}$. If $w \neq 1$, then $w - 1 = m\beta$ with $\beta \in \mathcal{O}_K \setminus \{0\}$, so $|N(w-1)| = m^d |N(\beta)| \ge m^d$. But for each i,

$$|\sigma_i(w-1)| \le |\sigma_i(w)| + 1 \le e^{2\Theta} + 1 < m$$

because $m \ge e^{2\Theta} + 2$; multiplying over i gives $|N(w-1)| < m^d$, a contradiction. Hence $w = 1$, i.e. $u = u'$ and $x = x'$. Finally $|X| = |B_S|$ since $y \mapsto 1 + my$ is injective, and $|A| = |U_\Theta||X|$ by the injectivity proved. □

Lemma 3.2 (lower bound for $|A|$)**.** *Suppose d is large enough that $\Theta^d \ge 2(2\Theta+1)d\, e^{C_R d}$ and $S^d \ge 2e^{\gamma d/2}$ (both hold for all $d \ge 8$, since $\log\Theta = 9 > C_R + 2$ and $s > \gamma$). Then*

$$|A| \;\ge\; \frac{\Theta^{d-1}}{3d\, e^{C_R d}} \cdot \frac{S^d}{e^{\gamma d/2}}.$$

Proof. Combine Lemma 3.1 with Lemma 2.7 (using $\mathrm{Reg}_K \le e^{C_R d}$ from Lemma 2.11 and Proposition 2.14, so its hypothesis is met) and with Lemma 2.5 for $M = S$ (using $\sqrt{|\Delta_K|} \le e^{\gamma d/2}$). □

3.2. The sumset.

Lemma 3.3. $|A + A| \le (4e^\Theta R + 1)^d$.

Proof. Every $a \in A_K$ satisfies $|\sigma_i(a)| \le e^\Theta R$, so every element of $A_K + A_K$ lies in $B_{2e^\Theta R}$; Lemma 2.2 gives $|A_K + A_K| \le (4e^\Theta R + 1)^d$. □

3.3. The product set.

Lemma 3.4. $|A \cdot A| \le 5^d |U_\Theta| \cdot |X|^2$.

Proof. Every element of $A_K \cdot A_K$ has the form $(ux)(u'x') = (uu')(xx')$ with $uu' \in U_{2\Theta}$ and $xx' \in X \cdot X$, so $A_K \cdot A_K \subseteq U_{2\Theta} \cdot (X \cdot X)$ and $|A_K \cdot A_K| \le |U_{2\Theta}|\,|X \cdot X| \le |U_{2\Theta}|\,|X|^2$. By Lemma 2.8, $|U_{2\Theta}| \le 5^d |U_\Theta|$. □

4. Proof of the Main Theorem

Recall the absolute constants

$$\gamma < 9.96,\ C_R < 6.90,\ \Theta = e^9,\ m = \lceil e^{2\Theta} \rceil + 2 \le e^{2\Theta} + 3,\ s = 3\Theta + 30,\ S = e^s,\ R = 1 + mS,$$

and set $\varepsilon_0 := 10^{-5}$.

Proposition 4.1. *There is an absolute constant d_0 (one may take $d_0 = 100$) such that for every field $K = F_j$ of degree $d \ge d_0$ the set $A = A(K) \subset \mathbb{R}$ of Section 3 satisfies*

$$|A \cdot A| \;\le\; e^{-d/20}\,|A|^{2-\varepsilon_0} \qquad \text{and} \qquad |A + A| \;\le\; e^{-d/20}\,|A|^{2-\varepsilon_0}.$$

In particular both are strictly smaller than $|A|^{2-\varepsilon_0}$.

Proof. Write $n := |A| = |U_\Theta||X|$ (Lemma 3.1); all logarithms are natural.

(a) Product set. By Lemma 3.4, $|A \cdot A| \le 5^d |U_\Theta||X|^2$, and $n^{2-\varepsilon_0} = |U_\Theta|^{2-\varepsilon_0}|X|^{2-\varepsilon_0}$, so it suffices to prove

$$e^{d/20}\, 5^d\, |X|^{\varepsilon_0} \;\le\; |U_\Theta|^{1-\varepsilon_0}. \tag{1}$$

We use $|X| = |B_S| \le (2S+1)^d$ (Lemma 2.2) and $|U_\Theta| \ge \Theta^{d-1}/(3de^{C_R d})$ (Lemmas 2.7 and 2.11, whose hypothesis was checked in Lemma 3.2). Taking logarithms, (1) follows from

$$\frac{d}{20} + d\log 5 + \varepsilon_0 d \log(2S+1) \;\le\; (1-\varepsilon_0)\big[(d-1)\log\Theta - C_R d - \log(3d)\big]. \tag{2}$$

Now $\log(2S+1) \le s + \log 2 + e^{-s} \le s + 0.70$, $\log\Theta = 9$, and $s + 0.70 = 3e^9 + 30.70 < 24\,341$. The left-hand side of (2) is at most

$$d\big[0.05 + 1.61 + 10^{-5}\cdot 24\,341\big] \le 1.91\, d,$$

while the right-hand side is at least

$$(1-10^{-5})(9d - 6.90d) - (9 + \log(3d)) \;\ge\; 2.09\, d - 9 - \log(3d) \;\ge\; 1.91\, d$$

for all $d \ge 100$ (indeed $0.18d \ge 9 + \log(3d)$ there). This proves (1).

(b) Sumset. By Lemmas 3.3 and 3.2 it suffices to prove

$$e^{d/20}\,(4e^{\Theta}R + 1)^d \;\le\; \Big(\frac{\Theta^{d-1}}{3de^{C_R d}} \cdot \frac{S^d}{e^{\gamma d/2}}\Big)^{2-\varepsilon_0}. \tag{3}$$

Take logarithms. Since $R = 1 + mS \le (e^{2\Theta}+3)S + 1 \le e^{2\Theta}S(1 + 4e^{-2\Theta})$,

$$\log(4e^{\Theta}R + 1) \le \log 5 + \Theta + 2\Theta + s + 4e^{-2\Theta} \le 3\Theta + s + 1.62,$$

so $\log(\text{LHS}) \le d(3\Theta + s + 1.62) + d/20 \le d(3\Theta + s + 1.67)$. For the right-hand side,

$$\log(\text{RHS}) \;\ge\; (2-\varepsilon_0)\Big[d\big(\log\Theta + s - C_R - \tfrac{\gamma}{2}\big) - \log\Theta - \log(3d)\Big].$$

Numerically, with $\Theta = e^9 = 8103.08\ldots$ and $s = 3\Theta + 30$,

$$3\Theta + s + 1.67 = 6\Theta + 31.67 \le 48\,650.3,$$

$$\log\Theta + s - C_R - \tfrac{\gamma}{2} \;\ge\; 9 + 3\Theta + 30 - 6.90 - 4.98 \;\ge\; 3\Theta + 27.1 \;\ge\; 24\,336.3.$$

Hence

$$\log(\text{RHS}) \;\ge\; (2-10^{-5})\cdot 24\,336.3\, d - 2(9 + \log(3d)) \;\ge\; 48\,672.3\, d - 2(9+\log(3d)),$$

and since $48\,672.3\, d - 2(9+\log(3d)) \ge 48\,650.3\, d$ for all $d \ge 2$ (indeed $22d \ge 18 + 2\log(3d)$), inequality (3) holds. □

Proof of Theorem 1.1. Take the infinite sequence of totally real fields F_j from Proposition 2.14 and discard the finitely many of degree $< d_0$. For each remaining K of degree d, Section 3 produces a finite set $A(K) \subset \mathbb{R}$ with, by Proposition 4.1,

$$\max\big(|A(K)+A(K)|,\, |A(K)\cdot A(K)|\big) \;\le\; e^{-d/20}|A(K)|^{2-\varepsilon_0} \;<\; |A(K)|^{2-\varepsilon_0}, \qquad \varepsilon_0 = 10^{-5}.$$

By Lemma 3.2, $|A(K)| \ge S^d e^{-\gamma d/2}\,\Theta^{d-1}/(3de^{C_R d}) \to \infty$ as $d \to \infty$ (the exponential rate $\log\Theta + s - C_R - \gamma/2 > 0$ is positive), so $\mathcal{N} := \{|A(F_j)| : [F_j : \mathbb{Q}] \ge d_0\}$ is an infinite subset of $\mathbb{N}$; for every $n \in \mathcal{N}$ we have a set of size exactly n with $\max(|A+A|, |A\cdot A|) < n^{2-\varepsilon_0}$.

Thus the conjecture fails for $\varepsilon = \varepsilon_0$: no matter how large n_0 is, there are $n \in \mathcal{N}$ with $n \ge n_0$ and sets A of size n for which $\max(|A+A|, |A\cdot A|) \ge n^{2-\varepsilon_0}$ does not hold. □

5. Remarks

Remark 5.1 (Consistency with known lower bounds)**.** The best unconditional sum–product lower bounds over $\mathbb{R}$ have the form $\max(|A+A|, |A\cdot A|) \gg |A|^{4/3+c}$ (Elekes; Solymosi; Konyagin–Shkredov; Rudnev–Stevens). Our sets satisfy these comfortably: we prove only the upper bound $|A|^{2-\varepsilon_0}$ with $\varepsilon_0 = 10^{-5}$, far above $4/3$. Likewise, Elekes–Ruzsa-type results ("very small sumset forces nearly maximal product set") are not contradicted, as here both doubling constants are of size $|A|^{1-O(\varepsilon_0)}$, outside their regime.

Remark 5.2 (Where the approximate subring lives)**.** The construction exploits that $\mathbb{R}$ contains number fields of arbitrarily large degree d whose rings of integers look, inside a bounded Minkowski box, like d-dimensional arithmetic progressions, and whose unit groups have rank $d-1$ with covolume only $e^{O(d)}$ (bounded root discriminant). The degree is tied to the set size by $d \asymp \log n$ (here $n \approx e^{(3\Theta+O(1))d}$); for any fixed degree the same computation saves only a constant factor, which is why the mechanism is invisible in the classical bounded-degree regime.

Remark 5.3 (Effectivity)**.** Everything is explicit: $\gamma < 9.96$ comes from the specific real quadratic field $\mathbb{Q}(\sqrt{3\cdot 5\cdots 23})$, and $\Theta = e^9$, $m = \lceil e^{2\Theta} \rceil + 2$, $S = e^{3\Theta+30}$, $\varepsilon_0 = 10^{-5}$, $d_0 = 100$. The first admissible $n \in \mathcal{N}$ is of size roughly $e^{2.4\cdot 10^6}$ — astronomically large but finite, and the statement disproved is asymptotic. No attempt has been made to optimise; towers with smaller root discriminant (e.g. Martinet's) and tighter counting would improve ε_0 by several orders of magnitude.

Remark 5.4 (On the inputs)**.** The construction uses only elementary geometry of numbers (Minkowski/van der Corput counting and a covering argument), Dirichlet's unit theorem, the analytic class number formula, Louboutin's explicit residue bound for $\mathrm{Res}_{s=1}\zeta_K$, Gauss's genus theory, and the Golod–Shafarevich criterion for infinite class field towers — all classical and unconditional.