

Polynomial Unit-Distance Lower Bounds over Prime Fields

Alper Ferudun*

October 5, 2026

Abstract

For each $a \in \{1, 3\}$, we prove that infinitely many primes $p \equiv a \pmod{4}$ admit a set of exactly p points in $\mathbb{F}_p^2$ with at least $p^{1.0058}$ unordered pairs at quadratic distance one. We transfer Sawin's number-field unit-distance construction to prime fields using a field-uniform quantitative Chebotarev estimate of Zaman. A relative ideal-norm bound prevents collisions without requiring a bounded global denominator. Reduction at split or inert primes gives the required quadratic form, and disjoint translates supply exactly p points. The exponent is certified by rational interval arithmetic. This is a lower-bound result for the prime-field question in an AIM additive-combinatorics problem list; it does not determine the optimal exponent or cover every sufficiently large prime.

1 The statement and its scope

For an odd prime p and $S \subseteq \mathbb{F}_p^2$, write

$$U(S) = \#\{(u, v) \in S^2 : (u_1 - v_1)^2 + (u_2 - v_2)^2 = 1\}.$$

This counts ordered pairs; the unordered count is $U(S)/2$. The quadratic form is algebraic, not a real-valued metric. In particular, distinct points can have zero quadratic distance when $p \equiv 1 \pmod{4}$. Problem 4.1, attributed to T. Tao in the AIM workshop list [1], asks how large $U(S)$ can be when $|S| = p$. The corresponding frozen dataset record is AIM-COMBINATORICS-0257 [5].

Theorem 1.1. *For each $a \in \{1, 3\}$ there are infinitely many primes $p \equiv a \pmod{4}$ and sets $S \subseteq \mathbb{F}_p^2$, $|S| = p$, having at least $p^{1.0058}$ unordered unit-distance pairs.*

The theorem keeps both the prime-field and exact-cardinality requirements. It does not determine the extremal order in the AIM question, whose elementary $O(p^{3/2})$ upper bound is not improved here. The proof imports the fields, norm fibers and lattice-window method from Sawin [2]. Zaman's discriminant-only counting theorem [3, Theorem 1.3.1] supplies appropriately sized reduction primes. Norm-controlled reduction already appears in the sum-product work of Bloom, Sawin, Schildkraut and Zhelezov [4, Section 7.2]; we do not claim that general principle as new. The point here is to retain the quadratic norm relation in both splitting cases and obtain exactly p vertices with a quantitative exponent. A bounded primary-source review has not certified novelty or absolute priority.

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: <https://github.com/AlperTheKing>.
Unrefereed preprint. CC BY 4.0.

2 The arithmetic window

Fix the parameters from the proof of [2, Theorem 1]:

$$T = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43\}, \quad \lambda = \sqrt{4 \prod_{q \in T} q}, \quad R = 72.$$

The auxiliary primes ℓ and weights k_ℓ are

ℓ	2	3	5	7	11	13	17	19	23	29	47
k_ℓ	50	31	21	17	14	13	12	11	10	10	8
ℓ	71	79	97	101	107	109	139	151	163	167	179
k_ℓ	7	7	7	7	7	7	6	6	6	6	6

Call the auxiliary prime set P . Put $e_\ell = 2$ if $\ell = 2$ or $\ell \in T$, and $e_\ell = 1$ otherwise. Define

$$A = \prod_{\ell \in P} \ell^{k_\ell/e_\ell}, \quad B = (2R\sqrt{A} + 1)^2, \quad (1)$$

$$\eta = 2 \log(1 - 1/R) + \log(2\pi/e) + \sum_{\ell \in P} \frac{\log(k_\ell + 1)}{2e_\ell} - \frac{1}{2} \log \lambda - \log \log \lambda. \quad (2)$$

All logarithms are natural.

Proposition 2.1 (Arithmetic input). *There are arbitrarily large d with a Galois totally real field $F/\mathbb{Q}$ of degree d and $K = F(i)$ such that*

$$D_F = \lambda^d, \quad D_K = \lambda^{2d}, \quad h^-(K) \leq 8\lambda^2 \left(\sqrt{\lambda} \log \lambda \frac{e}{4\pi} \right)^d.$$

For each such field there are a nonzero fractional ideal I of K and a totally positive $\alpha \in N_{K/F}(I)$ such that

$$H := \#(N_{K/F}(I)/(\alpha)) = A^d, \quad (3)$$

$$M := \#\{\beta \in I : \beta c(\beta) = \alpha\} \geq \frac{\prod_{\ell \in P} (k_\ell + 1)^{d/(2e_\ell)}}{2^d h^-(K)}. \quad (4)$$

Here c denotes complex conjugation and $N_{K/F}$ the ideal norm.

Source justification. These are [2, Lemmas 8, 9 and 12], with the parameters on page 12 of that paper. The residue degrees of the auxiliary primes in F are at most two. The field F is unramified over $\mathbb{Q}(\sqrt{\prod T})$, whose discriminant is λ^2 , and K/F is unramified at finite places; this gives the two discriminant identities. The norm fiber is nonempty, so α is totally positive. $\square$

We record the part of the lattice argument that is needed under reduction. It counts differences with a prescribed norm in F , not just differences whose image in one complex embedding has a prescribed length.

Lemma 2.2. *For the fields and ideal above, there is a nonempty finite set $V \subset I$, with $N = |V|$, such that*

$$N \leq B^d, \quad (5)$$

$$E_\alpha(V) := \#\{(u, v) \in V^2 : (u - v)c(u - v) = \alpha\} \geq \frac{Ne^{\eta d}}{8\lambda^2}, \quad (6)$$

$$\#(I/(z)) < B^d \quad (0 \neq z \in V - V). \quad (7)$$

Proof. Use the Minkowski embedding $I \subset \mathbb{C}^d$ and the norm $\|z\|_\alpha = \max_v |z_v|/\sqrt{\alpha_v}$, with one place from each complex-conjugate pair. The product formula, equivalently [2, Lemma 3], gives

$$\#(I/(z)) = H \prod_v \frac{|z_v|^2}{\alpha_v} \quad (0 \neq z \in I). \quad (8)$$

The left side is the norm of the integral ideal $(z)I^{-1}$, hence a positive integer even for fractional I . The minimum norm of a nonzero lattice vector is therefore at least $\rho = H^{-1/(2d)} = A^{-1/2}$.

For $w \in \mathbb{C}^d$ put $V_w = I \cap B_\alpha(R, w)$ and $N_w = |V_w|$. Packing disjoint open balls of radius $\rho/2$ gives $N_w \leq (2R/\rho + 1)^{2d} = B^d$. Every $v \in I \cap B_\alpha(R - 1, w)$ and every β in the norm fiber give a distinct designated pair $(v, v + \beta) \in V_w^2$. Integration over a fundamental domain gives

$$\int |I \cap B_\alpha(R - 1, w)| dw = (1 - 1/R)^{2d} \int N_w dw.$$

The latter integral is positive. With the probability measure proportional to $N_w dw$, the ratio of these counts has mean $(1 - 1/R)^{2d}$ and only finitely many values. Thus some nonempty window has ratio at least this mean. For that window, $E_\alpha(V) \geq N(1 - 1/R)^{2d}M$. Substituting Proposition 2.1 yields (6). Finally, every difference in this window has norm at most $2R$, so (8) gives

$$\#(I/(z)) \leq A^d (2R)^{2d} < B^d.$$

No global denominator estimate is involved. □

3 Choosing reduction primes

For a finite Galois extension $L/\mathbb{Q}$ with group G , let $\pi_C(x, L/\mathbb{Q})$ count unramified rational primes below x with Frobenius conjugacy class C . Zaman proves the field-uniform estimate

$$\pi_C(x, L/\mathbb{Q}) \gg D_L^{-19} \frac{|C|}{|G|} \text{Li}(x), \quad x \geq D_L^{35}, \quad (9)$$

for sufficiently large D_L , with absolute implied constants [3, Theorem 1.3.1]. This is a counting result, not just a bound for the least prime. It permits excluding a growing initial interval.

Lemma 3.1. *For all sufficiently large degrees supplied by Proposition 2.1, there is a prime in each of the Frobenius classes $\{1\}$ and $\{c\}$ of $K/\mathbb{Q}$ with*

$$B^d < p \leq \lambda^{70d}. \quad (10)$$

The first prime is 1 modulo four; the second is 3 modulo four.

Proof. Since F is totally real, $\text{Gal}(K/\mathbb{Q}) = \text{Gal}(F/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. Both classes are singletons. At $x = D_K^{35} = \lambda^{70d}$, (9), $|G| = 2d$ and $\text{Li}(x) \gg x/\log x$ give

$$\pi_C(x, K/\mathbb{Q}) \gg \lambda^{32d}/d^2.$$

Section 5.1 verifies $\log B < 32 \log \lambda$, so this count exceeds B^d for large d . At most B^d primes are at most B^d ; a prime in (10) remains in each class. Restriction to $\mathbb{Q}(i)$ gives its residue class modulo four. □

4 Local normalization and injectivity

Fix a prime from Lemma 3.1. In particular $H = A^d < p$, so $p \nmid H$. At every prime $\mathfrak{q}$ of F over p , the inclusion $(\alpha) \subset N_{K/F}(I)$ is therefore a local equality. All valuations in the argument below are normalized discrete valuations.

Lemma 4.1. *For either chosen Frobenius class there is an additive map $\phi : I \rightarrow \mathbb{F}_p^2$, injective on V , such that every designated norm- α difference in $V - V$ maps to a vector of quadratic norm one.*

Proof. First suppose Frobenius is c . The prime p splits completely in F , and a prime $\mathfrak{P}$ of K over $\mathfrak{q}$ has residue field $\mathbb{F}_{p^2}$. It is fixed by c , which acts on the residue field as $t \mapsto t^p$. Choose $a \in K^\times$ generating I locally at $\mathfrak{P}$. If $m = v_{\mathfrak{P}}(I)$, then

$$v_{\mathfrak{q}}(\alpha) = v_{\mathfrak{q}}(N(I)) = 2m = v_{\mathfrak{q}}(ac(a)).$$

Consequently $h = \overline{\alpha/(ac(a))}$ is in $\mathbb{F}_p^\times$. Surjectivity of the finite-field norm supplies $\kappa \in \mathbb{F}_{p^2}^\times$ with $\kappa\kappa^p = h$. Define

$$\phi(v) = \overline{v/a}/\kappa \in \mathbb{F}_{p^2}.$$

Write $\bar{i} = j$, so $j^2 = -1$ and $\mathbb{F}_{p^2} = \mathbb{F}_p \oplus \mathbb{F}_p j$. The coordinates $x + yj$ identify the field norm with $x^2 + y^2$. If $zc(z) = \alpha$, then

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\phi(z)) = \overline{zc(z)/(ac(a))}/h = 1.$$

A collision between distinct window points would give $0 \neq z \in V - V$ with $(z)I^{-1}$ divisible by $\mathfrak{P}$. This integral ideal would have norm at least p^2 , contradicting (7) and (10). Thus the map is injective on V .

Now suppose Frobenius is 1. The two primes $\mathfrak{P}, c\mathfrak{P}$ over $\mathfrak{q}$ are distinct and both have residue field $\mathbb{F}_p$. By weak approximation choose $a \in K^\times$ generating I locally at both primes. The valuations of I there may differ; their sum is $v_{\mathfrak{q}}(N(I))$. Hence again

$$h = \overline{\alpha/(ac(a))} \in \mathbb{F}_p^\times.$$

Taking all reductions in the following expressions at $\mathfrak{P}$, put

$$r(v) = \overline{v/a}, \quad s(v) = h^{-1}\overline{c(v/a)}.$$

The second expression is defined because v/a is also integral at $c\mathfrak{P}$. For a designated difference z , we have $r(z)s(z) = 1$. Let $j = \bar{i} \in \mathbb{F}_p$, and set

$$\phi(v) = \left(\frac{r(v) + s(v)}{2}, \frac{r(v) - s(v)}{2j} \right).$$

The sum of squares of these coordinates is $r(v)s(v)$. If two distinct window points collided, the associated $(z)I^{-1}$ would be divisible by both $\mathfrak{P}$ and $c\mathfrak{P}$, again forcing its norm to be at least p^2 , a contradiction. $\square$

The argument neither assumes that I is principal nor that $I = c(I)$. In the split case it is essential to retain both residue coordinates; reduction at just one of the primes need not be injective. In either case $E = \phi(V)$ has $N < p$ points and

$$U(E) \geq \frac{Ne^{\eta d}}{8\lambda^2}. \quad (11)$$

Additional unit pairs created by reduction only help this inequality.

5 Exact cardinality and the exponent

Lemma 5.1. *If $E \subseteq \mathbb{F}_p^2$ has $1 \leq N \leq p$ points, there is a set $S \subseteq \mathbb{F}_p^2$ of exactly p points with $U(S) \geq pU(E)/(2N)$.*

Proof. Place $k = \lfloor p/N \rfloor$ disjoint translates of E greedily. After $j < k$ copies, at most jN^2 translations are forbidden: an intersection specifies an old point and a point of E . Since $jN^2 < pN \leq p^2$, an allowed translate exists. The union has $kN \geq p/2$ points and at least $kU(E)$ ordered unit pairs. Add unused points until its size is p ; no existing pair is lost. $\square$

Proof of Theorem 1.1. Lemmas 2.2–5.1 give, in each residue class,

$$U(S) \geq \frac{pe^{\eta d}}{16\lambda^2} \geq \frac{p^{1+\theta}}{16\lambda^2}, \quad \theta = \frac{\eta}{70 \log \lambda},$$

where the second inequality uses $p \leq \lambda^{70d}$ and $\eta > 0$. As verified below, $\theta > 0.0058$. Dividing by two and absorbing the fixed constant $32\lambda^2$ gives the stated unordered bound for large d . Since $p > B^d$, these primes tend to infinity. $\square$

5.1 A rational certificate

The accompanying standard-library Python checker certifies the enclosures

$$\begin{aligned} 18.9016 &< \log \lambda < 18.9017, \\ 540.1710 &< \log A < 540.1711, \\ \log B &< 550.111, \\ 7.7644 &< \eta < 7.7646. \end{aligned}$$

They imply the two required inequalities by rational comparisons:

$$550.111 < 32(18.9016), \quad 0.0058 \cdot 70 \cdot 18.9017 < 7.7644.$$

For completeness, the certificate uses no floating-point inequality. Range reduction writes a positive rational as $2^m x$, $1 \leq x \leq 2$. For $t = (x - 1)/(x + 1)$ and $n = 70$,

$$2 \sum_{j=0}^{n-1} \frac{t^{2j+1}}{2j+1} \leq \log x \leq 2 \sum_{j=0}^{n-1} \frac{t^{2j+1}}{2j+1} + \frac{2t^{2n+1}}{(2n+1)(1-t^2)}.$$

Machin's identity $\pi = 16 \arctan(1/5) - 4 \arctan(1/239)$ and the alternating-series remainder bound enclose π . Nested intervals are rounded outward to rational endpoints before taking logarithms. Finally

$$\log B < \log A + 2 \log 144 + 10^{-6},$$

because $A \geq 2^{25} 3^{15} 5^{10} > 2^{50}$ and $\log(1+t) < t$ for $t > 0$. A finer output gives $0.005868357018 < \theta < 0.005868357019$.

6 Limitations and reproducibility

The result is existential and asymptotic: no practical first prime, explicit large-degree coordinate list or efficient construction algorithm is supplied. The elementary upper bound and the question for every sufficiently large prime remain unresolved here. The fixed parameters were selected to give a short reproducible transfer, not an optimized exponent.

The accompanying checker passes 440 tests: the arithmetic parameter hypotheses, rational intervals, finite-field norm identities, exact-size packing and failure witnesses for omitted hypotheses. These finite tests do not constitute a formal proof of the general argument or verify the cited number-theoretic theorems. The source package includes the detailed self-audit and does not redistribute third-party source PDFs.

This unrefereed manuscript was developed with AI assistance for the proof transfer, literature searches, exact checking and exposition. Its claims have undergone the originating workflow’s self-audit, not independent refereeing or proof-assistant verification. Alper Ferudun is responsible for the submitted text and its mathematical claims.

References

- [1] American Institute of Mathematics, *Recent trends in additive combinatorics: problem list*, Problem 4.1 (T. Tao), p. 10. <https://aimath.org/WWN/additivecomb/additivecomb.pdf>.
- [2] W. Sawin, *An explicit lower bound for the unit distance problem*, arXiv:2605.20579v1, 2026. <https://arxiv.org/abs/2605.20579>.
- [3] A. A. Zaman, *Analytic estimates for the Chebotarev Density Theorem and their applications*, Ph.D. thesis, University of Toronto, 2017, Theorem 1.3.1 and Section 7.2. <https://www.math.toronto.edu/zaman/files/thesis.pdf>.
- [4] T. F. Bloom, W. Sawin, C. Schildkraut and D. Zhelezov, *The sum-product conjecture is false for real numbers*, arXiv:2605.28781v1, 2026, Section 7.2. <https://arxiv.org/abs/2605.28781>.
- [5] ulamai, *UnsolvedMath*, version 1.6.0, record AIM-COMBINATORICS-0257, frozen dataset commit `c6e7f41b4eb6ce876feb83e7eb626be1b243fd7e`. <https://huggingface.co/datasets/ulamai/UnsolvedMath>.