hexagon:2611.00095v1

A composite modulus and Frobenius digits in the Heilbronn triangle construction

David Niedbala Giraudin
ORCID 0009-0009-1526-1178
Technical assistance: Claude (Anthropic)

November 2026

Abstract

OpenAI proved that for every sufficiently large n there are n points in the unit square all of whose triangles have area at least $c\,n^{-2+\eta}$, with an explicit but extremely small η (of order 10^{-235}). Subsequent public work lowered the cost of the construction, the latest claimed exponent being $\eta = 2/100866719 \approx 1.98 \cdot 10^{-8}$. We introduce two changes. First, the digit base is taken to be a multiple of the label prime r and the main modulus is $h = rB^{k-1}$ instead of B^k; this reduces the ratio h/τ between the modulus and the excluded determinant window from about B to about r, which allows the extension degree $d = 3$. Second, the norm polynomial is placed in the digits by a digit-wise convolution along the Frobenius expansion of the exponents, with a trace digit in a polynomial basis, giving $k = 1440$ positions. The result is

$$\Delta(n) \;\geq\; c\,n^{-2+\eta}, \qquad \eta = \frac{1}{177\,022} > 5.64 \cdot 10^{-6},$$

for every sufficiently large n. The finite identities are checked by exact computation in the ancillary files.

1 Introduction

For a finite set $P \subset [0,1]^2$ with $|P| \geq 3$ let $\Delta(P)$ be the least area of a triangle with vertices in P, and let $\Delta(n)$ be the maximum of $\Delta(P)$ over n-point sets. Komlós, Pintz and Szemerédi proved $\Delta(n) \gg (\log n)/n^2$ [4]. OpenAI [1] proved a power improvement $\Delta(n) \geq c_1 n^{-2+\eta}$ with $\eta = 2/(45435k + 16)$, $k = T^2 + 1$, $T = \binom{M}{3}$, $M = \binom{163}{41}$, so that $\eta \approx 10^{-235.5}$. Their construction samples integral columns whose residues modulo a main modulus h carry a determinant obstruction coming from a field norm, together with an auxiliary cap modulo a second prime q, and deletes the few bad triples.

Public follow-up work reduced the parameters inside the same framework: Blinov [2] lowered the extension degree to $d = 5$ using row-dependent digit lengths, label tags, a fresh-digit collision bound and a slab version of the auxiliary cap, and the Euler team [3] obtained the claimed exponent $\eta = 2/100866719$ with $k = 408781$ and a smaller lift box.

Theorem 1.1. *There are $c > 0$ and n_0 such that for every integer $n \geq n_0$,*

$$\Delta(n) \geq c\,n^{-2+\eta}, \qquad \eta = \frac{1}{177022}.$$

The two new ingredients are the following.

Composite modulus. Let r be the label prime and choose the digit base $B = rB_2$ with B_2 prime. The main modulus is $h = rB^{k-1}$. Since $B \equiv 0$ modulo r, the part of the determinant above the digit position $k-1$ reduces modulo r to the single designated coefficient, whose residue is the field norm. Distinct labels then exclude every representative of absolute value at most $\tau \approx B^{k-1}/2$, while $h/\tau \approx 2r$ instead of $\approx 2B$. The price of a label collision becomes $r^{2\gamma} \cdot r \cdot r^{-d}$ and $d = 3$ suffices (Section 6).

Frobenius digits. The norm of the Vandermonde product, $\mathrm{N}(V) = \prod_t V^{r^t}$, has monomials whose exponents have r-adic digits in $\{0, 1, 2\}$, with a coefficient that factors over the digits. We place the monomials in the digit positions by a mixed-radix convolution in which each lower Frobenius digit is handled by a fixed three-row design of radix 6 (Table 1), the most significant digit by a design whose rows 1 and 3 never reach the target together (Table 2), and the descent to $\mathbb{F}_r$ by a trace digit of radix $2d-1$ in a polynomial basis. With $d = 3$ this uses $k = 1440$ positions.

Everything else follows the framework of [1] with the row-dependent digit lengths and the slab cap of [2] and the smaller lift box of [3]. We give proofs of every statement that changes, citing [1] for the lattice-point counts and the weight bounds of the auxiliary cap, whose proofs apply with the changes indicated.

Conventions. $A \ll B$ means $|A| \le CB$ with C depending only on the fixed parameters $d = 3$ and $k = 1440$, never on the growing prime r. Lengths are Euclidean. All logarithms are natural.

2 Frobenius digits

2.1 The digit design

For $(x, y, z) \in \{0, 1, 2\}^3$ let $w(x, y, z)$ be the sign of the permutation $0 \mapsto x$, $1 \mapsto y$, $2 \mapsto z$ when $\{x, y, z\} = \{0, 1, 2\}$, and $w(x, y, z) = 0$ otherwise. Then, for commuting indeterminates,

$$\sum_{x,y,z} w(x, y, z) X^x Y^y Z^z = \det \begin{pmatrix} 1 & 1 & 1 \\ X & Y & Z \\ X^2 & Y^2 & Z^2 \end{pmatrix} = (Y - X)(Z - X)(Z - Y). \tag{2.1}$$

A *design* is a triple of finite lists $\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3$ of options; each option o carries a value $x(o) \in \{0, 1, 2\}$, a height $u(o) \in \mathbb{Z}_{\ge 0}$ and a sign $\epsilon(o) \in \{\pm 1\}$. We use the design $\mathcal{D}_6$ of Table 1, with target $\kappa = 5$.

row	options (x, u, ϵ)
1	$(0, 1, +)$, $(0, 3, +)$, $(1, 4, -)$, $(2, 0, +)$
2	$(0, 1, +)$, $(1, 2, +)$, $(2, 0, -)$
3	$(0, 3, -)$, $(0, 1, +)$, $(1, 4, +)$, $(2, 0, +)$

Table 1: The digit design $\mathcal{D}_6$ (target $\kappa = 5$).

Lemma 2.1. *The design $\mathcal{D}_6$ has the following properties.*

(D1) For every $(x, y, z) \in \{0, 1, 2\}^3$,

$$\sum_{\substack{o_i \in \mathcal{O}_i,\ (x(o_1), x(o_2), x(o_3)) = (x, y, z) \\ u(o_1) + u(o_2) + u(o_3) = 5}} \epsilon(o_1)\epsilon(o_2)\epsilon(o_3) = w(x, y, z).$$

(D2) For all options, $|u(o_1) + u(o_2) + u(o_3) - 5| \le 5$.

(D3) All heights are at most 4.

Proof. A finite check of the $4 \cdot 3 \cdot 4 = 48$ option triples; see `anc/check_design.py`. For example, for $(x, y, z) = (0, 1, 2)$ the option triples have heights $(1, 2, 0)$ and $(3, 2, 0)$; only the second sums to 5, with sign $+$. For $(0, 0, 0)$ the triples summing to 5 are $(1, 1, 3)$ with sign $-$ and $(3, 1, 1)$ with sign $+$, which cancel. □

For the most significant digit we use the design $\mathcal{T}_7$ of Table 2, with target 7.

row	options (x, u, ϵ)
1	$(0, 4, +)$, $(1, 1, -)$, $(2, 0, +)$
2	$(0, 5, -)$, $(0, 6, -)$, $(1, 3, -)$, $(2, 1, +)$
3	$(0, 5, -)$, $(0, 4, +)$, $(1, 2, -)$, $(2, 0, -)$

Table 2: The top design $\mathcal{T}_7$ (target 7).

Lemma 2.2. *The design* $\mathcal{T}_7$ *satisfies (D1) with* 5 *replaced by* 7*, and moreover:*

(T1) no option of row 1 *and option of row* 3 *have heights summing to* 7*;*

(T2) the options of height 0 *in rows* 1 *and* 3 *have value* $x = 2$*, and row* 2 *has no option of height* 0*.*

The rows of $\mathcal{D}_6$ *have options of height* 0 *only with value* $x = 2$*.*

Proof. A finite check; see `anc/check_design.py`. For (T1), the heights in rows 1 and 3 are $\{0, 1, 4\}$ and $\{0, 2, 4, 5\}$, whose sums avoid 7. □

2.2 Field, labels and the norm

Fix $d = 3$. Let $r > 6d$ be a prime, $\mathbb{F} = \mathbb{F}_r$, and $K = \mathbb{F}_{r^d} = \mathbb{F}[\theta]$ with θ a root of an irreducible cubic. Write $c_\mu(\xi)$, $\mu = 0, 1, 2$, for the coordinates of $\xi \in K$ in the basis $1, \theta, \theta^2$, and Tr for the trace $K \to \mathbb{F}$. For $e = (e_0, e_1, e_2) \in \{0, 1, 2\}^3$ put $\xi^{[e]} = \xi^{e_0 + e_1 r + e_2 r^2} = \prod_t (\xi^{r^t})^{e_t}$. For labels $\xi_1, \xi_2, \xi_3 \in K^\times$ let $V = (\xi_2 - \xi_1)(\xi_3 - \xi_1)(\xi_3 - \xi_2)$ and $\mathrm{N}(V) = \prod_{t<d} V^{r^t} \in \mathbb{F}$. Since d is odd, $\mathrm{N}(-v) = -\mathrm{N}(v)$, so $\mathrm{N}(V)$ is alternating in the labels; it is nonzero when the labels are distinct.

2.3 Positions and residues

Use the mixed radix with digit weights

$$W_{\mathrm{tr}} = 1, \qquad W_0 = 5, \qquad W_1 = 30, \qquad W_2 = 180,$$

that is, a trace digit of radix $2d - 1 = 5$, two Frobenius digits of radix 6 (digits $t = 0, 1$, design $\mathcal{D}_6$) and a most significant Frobenius digit ($t = 2$, design $\mathcal{T}_7$). Write $\mathcal{O}_i^{(t)}$ for the options of row i in the design of digit t. For a row i and an option word $o = (o_0, o_1, o_2)$ with $o_t \in \mathcal{O}_i^{(t)}$ put

$$x(o) = (x(o_0), x(o_1), x(o_2)), \quad \epsilon(o) = \prod_t \epsilon(o_t), \quad H(o) = \sum_{t=0}^{2} u(o_t) W_t.$$

The *terms* of the three rows, their *positions* and their *functions* $K \to \mathbb{F}$ are:

row	term	position	function
1	(o,μ), $0\le\mu\le 2$	$\mu+H(o)$	$\epsilon(o)\,c_\mu(\xi^{[x(o)]})$
2	(o,ν), $0\le\nu\le 2$	$\nu+H(o)$	$\epsilon(o)\,c_\nu(\xi^{[x(o)]})$
3	(o,s), $0\le s\le 4$	$4-s+H(o)$	$\epsilon(o)\ \mathrm{Tr}(\theta^s\xi^{[x(o)]})$

Put

$$X^*=4\cdot W_{\mathrm{tr}}+5W_0+5W_1+7W_2=1439,\qquad k=X^*+1=1440.$$

The largest position is $2+4\cdot 5+4\cdot 30+4\cdot 180=862$ in row 1, $2+2\cdot 5+2\cdot 30+6\cdot 180=1152$ in row 2 and $4+4\cdot 5+4\cdot 30+5\cdot 180=1044$ in row 3, all below $k-1=1439$. For a label $\xi\in K^\times$, a row i and a position $0\le v<k$, let $\rho_{i,v}(\xi)\in\mathbb{F}$ be the sum of the functions of all row-i terms at position v (zero if there are none), except that we add the *control*

$$\rho_{2,0}(\xi)=\varphi(\xi)\,\mathrm{N}(\xi)^2,\qquad \varphi(\xi)=c_0(\xi);\tag{2.2}$$

by (T2) row 2 has no term at position 0. By (T2) and Lemma 2.2, the only terms at position 0 are, in row 1, the word of value $(2,2,2)$ with $\mu=0$, of function $c_0(\xi^{[2,2,2]})=c_0(\mathrm{N}(\xi)^2)=\mathrm{N}(\xi)^2$, and, in row 3, the word of value $(2,2,2)$ with $s=4$, of function $-\mathrm{Tr}(\theta^4\,\mathrm{N}(\xi)^2)$. Hence

$$(\rho_{1,0},\rho_{2,0},\rho_{3,0})(\xi)=\mathrm{N}(\xi)^2\,\big(1,\ \varphi(\xi),\ -\mathrm{Tr}(\theta^4)\big).\tag{2.3}$$

Lemma 2.3 (Encoding)**.** *For all labels $\xi_1,\xi_2,\xi_3\in K^\times$,*

$$\sum_{p_1+p_2+p_3=k-1}\det\big(\rho_{i,p_i}(\xi_j)\big)_{i,j=1}^{3}=6d\ \mathrm{N}(V)=18\ \mathrm{N}(V)\tag{2.4}$$

in $\mathbb{F}$, the sum running over $0\le p_i<k$. In particular the left side is nonzero when the labels are distinct.

Proof. Selection. Consider three terms (o^1,μ), (o^2,ν), (o^3,s) of rows $1,2,3$ with positions summing to X^*. Put $\delta_{\mathrm{tr}}=\mu+\nu-s\in[-4,4]$ and $\delta_t=u(o^1_t)+u(o^2_t)+u(o^3_t)-\kappa_t$ with $\kappa_0=\kappa_1=5$, $\kappa_2=7$; by (D2), $\delta_0,\delta_1\in[-5,5]$. Then $0=\delta_{\mathrm{tr}}+5\delta_0+30\delta_1+180\delta_2$. Reduction modulo 5 gives $\delta_{\mathrm{tr}}=0$, then reduction modulo 6 gives $\delta_0=0$, then $\delta_1=0$, and finally $\delta_2=0$. Conversely these equalities give the target. So the contributing triples of terms are exactly those with $\mu+\nu=s$ and, in each digit t, heights summing to κ_t.

The control. The control (2.2) contributes only through triples with $p_2=0$ and $p_1+p_3=X^*$, where p_1,p_3 carry terms of rows 1 and 3 (otherwise a residue is 0). For such terms put $\delta'_{\mathrm{tr}}=\mu+(4-s)-4\in[-4,2]$ and $\delta'_t=u(o^1_t)+u(o^3_t)-\kappa_t$, with $\delta'_0,\delta'_1\in[-5,3]$ because the heights of $\mathcal{D}_6$ in rows 1 and 3 lie in $[0,4]$ (D3). As above $\delta'_{\mathrm{tr}}=\delta'_0=\delta'_1=\delta'_2=0$, so the top heights of rows 1 and 3 would sum to 7, contradicting (T1). Hence the control does not contribute.

Expansion. By multilinearity of the determinant in its rows, the left side of (2.4) equals

$$\sum\epsilon(o^1)\epsilon(o^2)\epsilon(o^3)\det\begin{pmatrix}c_\mu(\xi_j^{[a]})\\ c_\nu(\xi_j^{[b]})\\ \mathrm{Tr}(\theta^s\xi_j^{[c]})\end{pmatrix}_{j=1,2,3},$$

over the contributing triples, where $a=x(o^1)$, $b=x(o^2)$, $c=x(o^3)$. Fix (a,b,c). By (D1) for $\mathcal{D}_6$ and $\mathcal{T}_7$ applied digit by digit, the total sign of the option words with these values and digit sums

κ_t is $\prod_t w(a_t, b_t, c_t)$. For fixed (a, b, c) the sum over $\mu + \nu = s$ is, expanding the determinant over permutations σ,

$$\sum_{\sigma} \operatorname{sgn}(\sigma) \sum_{s} \sum_{\mu+\nu=s} c_\mu(\alpha) c_\nu(\beta) \operatorname{Tr}(\theta^s \gamma) = \sum_{\sigma} \operatorname{sgn}(\sigma) \operatorname{Tr}(\alpha\beta\gamma),$$

with $\alpha = \xi^{[a]}_{\sigma(1)}$, $\beta = \xi^{[b]}_{\sigma(2)}$, $\gamma = \xi^{[c]}_{\sigma(3)}$, because $\alpha\beta = \sum_{\mu,\nu} c_\mu(\alpha) c_\nu(\beta) \theta^{\mu+\nu}$ and the trace is $\mathbb{F}$-linear. Summing over (a, b, c) and using that Frobenius is a ring endomorphism together with (2.1),

$$\begin{aligned} \sum_{a,b,c} \prod_t w(a_t, b_t, c_t)\, X^{[a]} Y^{[b]} Z^{[c]} &= \prod_{t<d} \sum_{x,y,z} w(x, y, z) (X^{r^t})^x (Y^{r^t})^y (Z^{r^t})^z \\ &= \prod_{t<d} V(X, Y, Z)^{r^t} = \mathrm{N}\, V(X, Y, Z). \end{aligned}$$

Hence the left side is

$$\sum_{\sigma} \operatorname{sgn}(\sigma) \operatorname{Tr}\big(\mathrm{N}\, V(\xi_{\sigma(1)}, \xi_{\sigma(2)}, \xi_{\sigma(3)})\big) = \sum_{\sigma} \operatorname{sgn}(\sigma)^2 \operatorname{Tr}(\mathrm{N}\, V) = 6\ \operatorname{Tr}(\mathrm{N}\, V) = 6d\ \mathrm{N}\, V,$$

since $\mathrm{N}\, V$ is alternating and lies in $\mathbb{F}$. Finally $6d = 18$ is invertible because $r > 18$. □

The identity is checked by exact computation for random labels in `anc/check_encoding.py`.

3 Digit columns and the composite modulus

3.1 Parameters

Let $r > 18$ be a prime and put

$$M = 4800k^2r^3, \qquad L_1 = L_2 = r, \qquad L_3 = rM, \qquad A_0 = 6k^2 L_1 L_2 L_3 = 6k^2 r^3 M. \tag{3.1}$$

Let B_2 be a prime with $Q < B_2 \le 2Q$, where $Q = 600k^2r^2M$ (it exists for large r by Bertrand's postulate), and set

$$B = rB_2, \qquad h = rB^{k-1} = r^k B_2^{k-1}, \qquad \tau = \lfloor B^{k-1}/2 \rfloor. \tag{3.2}$$

Then $B = rB_2 > 600k^2r^3M = 100A_0$, so $B - 1 \ge 100A_0$; also $L_3 < B_2$, $B_2 \ne r$, and

$$\theta_0 := \frac{B_2 r}{M^2} \le \frac{2(600k^2r^2M + 1)r}{M^2} \le \frac{1}{2}. \tag{3.3}$$

Moreover $B \asymp r^6$, with constants depending only on k.

3.2 Random columns

A column is drawn as follows. Choose a label ξ uniformly in $K^\times$. For rows $i = 1, 2$ and every position $0 \le v < k$, let $d_{i,v}$ be the unique integer in $[1, r]$ congruent to $\rho_{i,v}(\xi)$ modulo r. For row 3 and every v, choose $d_{3,v}$ uniformly from the M integers in $[1, rM]$ congruent to $\rho_{3,v}(\xi)$, independently. Put $c_i = \sum_{v<k} d_{i,v} B^v \bmod h$. Different columns use independent labels and digits. Since $B \equiv 0$ modulo both primes, $c_i \equiv d_{i,0}$ modulo r and modulo B_2. In particular $c_1 \equiv \mathrm{N}(\xi)^2 \not\equiv 0 \pmod r$ by (2.3), and $c_1 \equiv d_{1,0} \in [1, r]$ is a unit modulo B_2. By (2.3) the third row of C mod r is a multiple of the first, so C mod r always has rank at most two and $r \mid \det C$; this is harmless, since the obstruction below only uses $\mathrm{Hi} \not\equiv 0 \pmod r$ and the divisor E cancels in (6.2).

Lemma 3.1 (Obstruction)**.** *Let C be the residue matrix of three such columns. If the three labels are distinct, then no integer in $[-\tau,\tau]$ is congruent to $\det C$ modulo h.*

Proof. Let $\widehat{C}$ be the integer matrix with entries $\sum_v d_{i,v}^{(j)} B^v$ and put $F(Y) = \det\bigl(\sum_v d_{i,v}^{(j)} Y^v\bigr) = \sum_e \gamma_e Y^e$. For each exponent e and permutation, the positions in two rows determine the third, so $|\gamma_e| \le A_0$. Write $F(B) = L_0 + B^{k-1}\,\mathrm{Hi}$ with $L_0 = \sum_{e<k-1} \gamma_e B^e$ and $\mathrm{Hi} = \sum_{e\ge k-1} \gamma_e B^{e-k+1}$. Since $B - 1 \ge 100A_0$, $|L_0| \le A_0(B^{k-1}-1)/(B-1) \le \frac{1}{100}(B^{k-1}-1)$. Since $B \equiv 0 \pmod r$, $\mathrm{Hi} \equiv \gamma_{k-1} \pmod r$, and since every digit is congruent to its residue, Lemma 2.3 gives $\gamma_{k-1} \equiv 18\,\mathrm{N}(V) \not\equiv 0 \pmod r$. Every integer $t \equiv \det C \equiv F(B) \pmod h$ has the form $t = L_0 + B^{k-1}(\mathrm{Hi} + rm)$ with $m \in \mathbb{Z}$, and $\mathrm{Hi} + rm \neq 0$. Hence $|t| \ge B^{k-1} - |L_0| > \frac{99}{100} B^{k-1} > \tau$. □

3.3 Smith forms modulo h

For a prime $p \mid h$ let $h_p = p^{k_p}$ be the p-part of h ($k_r = k$, $k_{B_2} = k-1$). By the Chinese remainder theorem $\mathbb{Z}/h\mathbb{Z} = \mathbb{Z}/h_r\mathbb{Z} \times \mathbb{Z}/h_{B_2}\mathbb{Z}$ and $\mathrm{SL}_3(\mathbb{Z}/h\mathbb{Z}) = \prod_p \mathrm{SL}_3(\mathbb{Z}/h_p\mathbb{Z})$. Since C_{11} is a unit modulo both primes, [1, Lemma 4.1] applies to C mod h_p and gives $C \equiv P_p \,\mathrm{diag}(1, p^{b_p}, p^{e_p}) Q_p$ with $0 \le b_p \le e_p \le k_p$, where $b_p \ge j$ if and only if all 2×2 minors of C vanish modulo p^j. Put $D = \prod_p p^{b_p}$, $E = \prod_p p^{e_p}$ and $I = DE$. Let $\Lambda = \Lambda_C$ be the set of $v \in \mathbb{Z}^3$ whose reduction modulo h lies in the row span of C.

Lemma 3.2. *$[\mathbb{Z}^3 : \Lambda] = I$, $E\mathbb{Z}^3 \subseteq \Lambda$, and the orbit $\mathcal{O}_C = \{GC : G \in \mathrm{SL}_3(\mathbb{Z}/h\mathbb{Z})\}$ satisfies $|\mathcal{O}_C| \ge (21/64)^2 h^8/(D^3E^2)$. For uniform G, GC is uniform on $\mathcal{O}_C$, and all elements of $\mathcal{O}_C$ have the row span and the determinant of C. Moreover, for $x \in \mathbb{Z}^3$ write $x \cdot \Lambda = g\mathbb{Z}$; for every $m \mid h$, $m \mid g$ if and only if $Cx \equiv 0 \pmod m$; and for $m = \prod_p p^{j_p}$ with $j_p \le e_p$ the proportion of residues x modulo m with $Cx \equiv 0 \pmod m$ is $\prod_p p^{-j_p - \max(j_p - b_p, 0)}$.*

Proof. For $p \in \{r, B_2\}$ put

$$\Lambda_p = \{v \in \mathbb{Z}^3 :\ v \bmod h_p \in \text{row span of } C \bmod h_p\}.$$

By the Chinese remainder theorem, $\Lambda = \Lambda_r \cap \Lambda_{B_2}$, and $\mathcal{O}_C$ is the product of the orbits of C mod h_r and C mod h_{B_2}. For each prime p, [1, Lemma 4.1 and Lemma 4.2], which are stated for a prime power modulus and need one unit entry, give: the row span modulo h_p has $h_p^3/p^{b_p+e_p}$ elements, so $[\mathbb{Z}^3 : \Lambda_p] = p^{b_p+e_p}$; $p^{e_p}\mathbb{Z}^3 \subseteq \Lambda_p$; and $|\mathcal{O}_{C \bmod h_p}| \ge (21/64)\, h_p^8/p^{3b_p+2e_p}$. In the diagonal form, the proportion of x modulo p^j, $j \le e_p$, with $Cx \equiv 0 \pmod{p^j}$ is $p^{-j-\max(j-b_p,0)}$, as in the proof of [1, Lemma 7.3]. Since the two indices are coprime,

$$[\mathbb{Z}^3 : \Lambda] = \prod_p [\mathbb{Z}^3 : \Lambda_p] = I, \qquad E\mathbb{Z}^3 \subseteq \bigcap_p p^{e_p}\mathbb{Z}^3 \subseteq \Lambda, \qquad |\mathcal{O}_C| = \prod_p |\mathcal{O}_{C \bmod h_p}|,$$

and the proportions multiply. A uniform $G \in \mathrm{SL}_3(\mathbb{Z}/h\mathbb{Z})$ has uniform components, so GC is uniform on $\mathcal{O}_C$, and left multiplication by G preserves the row span and the determinant. Finally, for $m \mid h$ the reduction of Λ modulo m is the row span of C mod m, because $\Lambda \supseteq h\mathbb{Z}^3$; hence $m \mid g$, that is $x \cdot v \equiv 0 \pmod m$ for all $v \in \Lambda$, holds if and only if x is orthogonal modulo m to the rows of C, that is $Cx \equiv 0 \pmod m$. □

3.4 The divisor moment

Lemma 3.3. *Fix the three labels. Then*

$$\mathbb{E}[D \mid \textit{labels}] \le 2 + 6r\,\mathbf{1}\{\mathrm{rank}(C \bmod r) \le 1\}.$$

Proof. Write $b = b_{B_2}$ and $b' = b_r$. Since $p^\beta \le \sum_{i=0}^{\beta} p^i$,

$$D \le \sum_{j\ge 0}\sum_{j'\ge 0} B_2^j\, r^{j'}\, \mathbf{1}\{b \ge j,\ b' \ge j'\}.$$

Condition on the first column and on the first entries of the second and third columns. As C_{11} is a unit modulo p, $b_p \ge j$ implies the two congruences $C_{3v} \equiv C_{31}C_{11}^{-1}C_{1v} \pmod{p^j}$, $v = 2, 3$, whose right sides are now fixed. We use only these two bottom entries, which have fresh independent digits.

The prime B_2. Modulo B_2^j only the digits at positions $< j$ of an entry matter. The congruence modulo B_2 fixes $d_{3,0}$ modulo B_2, hence fixes $d_{3,0}$ since $1 \le d_{3,0} \le rM < B_2$. Inductively, given the lower digits, the congruence modulo B_2^{u+1} fixes $d_{3,u}B^u = r^u B_2^u d_{3,u}$ modulo B_2^{u+1}, hence $d_{3,u}$ modulo B_2 (as r is invertible modulo B_2), hence $d_{3,u}$. Each digit has M equally likely values, so the event $b \ge j$ fixes the bottom digits at positions $< j$ of both entries and has probability at most M^{-2j}.

The prime r. The event $b' \ge 1$ is the deterministic event that $C \bmod r$ has rank at most one. Write $d_{3,u} = \rho_{3,u} + rm_u$; the integers m_u range over M consecutive values, and $r \mid M$, so $m_u \bmod r$ is uniform. Since $B^u = r^u B_2^u$, an entry is $\sum_u d_{3,u} r^u B_2^u = \sum_u \rho_{3,u} r^u B_2^u + \sum_u m_u r^{u+1} B_2^u$. Its residue modulo r^{t+1} $(1 \le t \le k-1)$ is therefore the residue modulo r^{t+1} of a quantity determined by the residues $\rho_{3,u}$ and the m_u with $u \le t-2$, plus $m_{t-1}B_2^{t-1}r^t$. As B_2 is invertible modulo r, given the congruence of the entry modulo r^t and all m_u with $u \le t-2$, the congruence modulo r^{t+1} (whose right side is fixed) holds for exactly one value of $m_{t-1} \bmod r$, hence with conditional probability $1/r$. The same holds for the second entry, with its own independent m_{t-1}.

Joint bound. Here $0 \le j \le k-1$ and $0 \le j' \le k$. The event $b \ge j$ depends only on the bottom digits at positions $< j$ and fixes them; it costs at most M^{-2j}, and the congruences modulo r^t with $t \le j$ then cost nothing more. Next condition, in the order $t = j+1, \dots, j'-1$, on the congruence modulo r^{t+1}: it involves m_{t-1} with $t-1 \ge j$, which is uniform modulo r and independent of the event $b \ge j$ and of all digits at positions $\le t-2$, so by the previous paragraph each step costs a factor $1/r$ in each of the two entries. Therefore

$$\Pr(b \ge j,\ b' \ge j') \le \mathbf{1}\{j' = 0 \text{ or } \operatorname{rank}(C \bmod r) \le 1\}\, M^{-2j}\, r^{-2\max(j'-1-j,0)}.$$

The terms with $j' = 0$ contribute at most $\sum_j (B_2/M^2)^j \le 2$. If $\operatorname{rank}(C \bmod r) \le 1$, the terms with $j' \ge 1$ contribute at most

$$\sum_j (B_2/M^2)^j \Big(\sum_{j'=1}^{j+1} r^{j'} + \sum_{s\ge 1} r^{j+1+s} r^{-2s} \Big) \le \sum_j (B_2/M^2)^j\, 3r^{j+1} = 3r \sum_j \theta_0^j \le 6r,$$

using (3.3). □

Let $\mathcal{J}$ be the event that some integer in $[-\tau, \tau]$ is congruent to $\det C$ modulo h.

Corollary 3.4. *For three independent columns, $\mathbb{E}[D\mathbf{1}_{\mathcal{J}}] \le 33r^{-3}$.*

Proof. By Lemma 3.1, $\mathcal{J}$ requires two equal labels. Exactly two labels coincide with probability at most $3/(r^3-1) \le 4r^{-3}$. By (2.3) the columns of $C \bmod r$ are $\mathrm{N}(\xi_j)^2(1, \varphi(\xi_j), -\operatorname{Tr}\theta^4)^{\mathsf{T}}$, two of them equal; the rank is at most one only if the third label has the same value of φ, which has conditional probability at most $(r^2-1)/(r^3-2) \le 1/r$ (the number of $\xi \ne \xi_1$ with $\varphi(\xi) = \varphi(\xi_1)$ is r^2-1 or r^2-2). By Lemma 3.3 this case contributes at most $4r^{-3}(2 + 6r \cdot r^{-1}) = 32r^{-3}$. Three equal labels have probability at most $2r^{-6}$ and contribute at most $2r^{-6}(2+6r)$. □

4 The auxiliary modulus

Put $H = 2h$ and choose a prime q with $h^6 < q \le 2h^6$. Let $w = \lfloor q/(1000H^2) \rfloor$. Choose a nonsquare $\nu \in \mathbb{F}_q$ and put

$$S = \{(x, y, x^2 - \nu y^2) : 0 \le x < w,\ y \in \mathbb{F}_q\}, \qquad s = |S| = wq.$$

This is the slab cap of [2]. A line meets the graph of $x^2 - \nu y^2$ in at most two points (the restriction is a quadratic with nonzero leading coefficient $x_0^2 - \nu y_0^2$ for a direction with $(x_0, y_0) \neq 0$, and vertical lines meet once), so S has no three collinear points. Since $q \ge 2000H^2$,

$$s \ge \frac{q^2}{2000H^2}, \qquad \frac{q^3}{s} \le 2000H^2 q = 8000h^2 q. \tag{4.1}$$

The allowed shifts $\mathcal{A} = \{a \in \mathbb{F}_q^3 : \|ma_1\|_q > 3Hw \text{ for } 1 \le m \le 3H\}$, the random set $\mathcal{V} = G_q(a + S)$ with a uniform in $\mathcal{A}$ and G_q uniform in $\mathrm{GL}_3(\mathbb{F}_q)$, and the weight

$$W(A) = (q^3/s)^3 \Pr(\text{all columns of } A \bmod q \text{ lie in } \mathcal{V})$$

are as in [1, Section 5]; the same analysis for the slab is written out in [3, Section 3.4]. Lemma 5.2 of [1] is stated for $S \subset \{0, \dots, w-1\}^3$, but its proof uses the box only through the first coordinate. Indeed: (a) a uniform shift violates the condition for a given m with probability $(6Hw+1)/q$, so $\Pr(a \notin \mathcal{A}) \le 3H(6Hw+1)/q < 1/2$, which does not involve S; (b) if $a + v = 0$ with $v \in S$, then $\|a_1\|_q = \|v_1\|_q \le w - 1$, contrary to $m = 1$; (c) a relation $\sum_i x_i u^{(i)} = 0$ with $u^{(i)} = G_q(a + v^{(i)})$, $0 < |x| \le H$ and $m = \sum x_i \neq 0$ gives $ma_1 = -\sum_i x_i v_1^{(i)}$, of absolute value at most $3H(w-1)$ because $0 \le v_1^{(i)} < w$, again a contradiction; (d) if $m = 0$ the relation contradicts the affine independence of distinct points of $\mathcal{V}$, which follows from the line property. The proof of [1, Proposition 5.3] uses only the affine invariance of the line property, the transitivity of the affine group on affinely independent triples, and $|S| = s$. We obtain: $|\mathcal{A}| \ge q^3/2$; $0 \notin \mathcal{V}$; a relation $\sum x_i u^{(i)} = 0$ in $\mathbb{F}_q^3$ with $0 < |x| \le H$ is impossible for three distinct points of $\mathcal{V}$; and

$$W(A) \ll \begin{cases} 1 & \text{if the columns of } A \bmod q \text{ are affinely independent,} \\ q^3/s & \text{if } \operatorname{rank}(A \bmod q) \ge 2, \\ (q^3/s)^2 & \text{always.} \end{cases} \tag{4.2}$$

If $W(A) > 0$ then no column of $A \bmod q$ is zero, and the columns are either affinely independent or two of them are equal.

5 Weighted lattice counts

Fix C with the data D, E, I, Λ of Lemma 3.2, and an integer $N \ge h$ with $hq \mid N$. Let $\mathcal{B} = ([0, N)^2 \times [N, 2N)) \cap \mathbb{Z}^3$ and $\pi(u) = (u_1/u_3, u_2/u_3)$.

Proposition 5.1. *For every integer t with $|t| \le \tau$, the sum of $W(A)$ over integer matrices A with columns in $\mathcal{B}$, rows in Λ, pairwise distinct projected columns and $\det A = t$ is $\ll (\log 2N)^2 N^6/I^2$.*

Proof. If $t \neq 0$, then $0 < |t| \le \tau < q$, so $A \bmod q$ has rank three and $W(A) \ll 1$; every row has length $< 4N$ and $\lambda_3(\Lambda) \le E \le h < 4N$, so [1, Proposition 2.5] with $X = 4N$ gives the bound.

Let $t = 0$. We follow the proof of [1, Proposition 7.1]. The matrix has rational rank two, and its primitive null vector x has all coordinates nonzero and $|x| \ll N^2$. Put $\Lambda_x = \Lambda \cap x^\perp$, $x \cdot \Lambda = g(x)\mathbb{Z}$

and $J_x = I|x|/g(x)$. Then $g(x) \mid E$, so $g(x)^3/I \le E^2/D \le h^2$, and Λ_x reduces onto the plane $\Pi_x \subset \mathbb{F}_q^3$ orthogonal to x because $q \nmid E$ [1, Lemma 7.2]. For a sublattice of index m in Λ_x, the number of rank-two row triples of length $\le 4N$ is $\ll N^6/(mJ_x)^3$.

Moment. For $Y \ge h$, $\sum_{Y \le |x| < 2Y} g(x)^3 \ll Y^3 I$. Indeed $g^3 \le \sum_{m|g} m^3$ over $m = \prod_p p^{j_p}$ with $j_p \le e_p$, and by Lemma 3.2 the vectors with $m \mid g(x)$ form a union of residue classes modulo m of proportion $\prod_p p^{-j_p - \max(j_p - b_p, 0)}$; since $m \le E \le h \le Y$ each class has $\ll (Y/m)^3$ vectors of length $< 2Y$. Hence the sum is $\ll Y^3 \prod_p \sum_{j \le e_p} p^{2j - \max(j-b_p,0)} \ll Y^3 \prod_p p^{b_p + e_p} = Y^3 I$, each inner sum being dominated by its last term.

Split the null vectors into $O(\log 2N)$ dyadic shells $Y \le |x| < 2Y$; for fixed x and index m the count is $\ll N^6 g(x)^3/(m^3 I^3 Y^3)$. The cases are those of [1, Proposition 7.1], with (4.1) in place of $q^3/s \ll qh^{12}$:

- affinely independent residues: $|x| > H$, so $Y > H/2 = h$; with $m = 1$, $W \ll 1$ and the moment bound, the shell contributes $\ll N^6/I^2$;
- an equal pair i, j with $x \bmod q \notin \mathbb{F}_q(\mathbf{e}_i - \mathbf{e}_j)$: rows lie in an index-$q$ sublattice, there are $\ll Y^3$ normals, and with $g^3 \le Ih^2$ and $W \ll (q^3/s)^2$ the shell contributes $\ll (N^6/I^2)\, h^2 q^{-3} (q^3/s)^2 \ll (N^6/I^2) h^6/q \le N^6/I^2$;
- an equal pair with $x \bmod q \in \mathbb{F}_q(\mathbf{e}_i - \mathbf{e}_j)$: then $Y > q/2$ and there are $\ll Y^3/q^2$ normals; rank ≥ 2 modulo q gives $\ll (N^6/I^2) h^2 q^{-2} (q^3/s) \ll (N^6/I^2) h^4/q$, and rank ≤ 1 (rows in one of $q+1$ lines, each of index q) gives $\ll (N^6/I^2) h^2 q^{-4} (q^3/s)^2 \ll (N^6/I^2) h^6/q^2$.

Since $q > h^6$ all contributions are $\ll N^6/I^2$ per shell. □

6 Sampling, deletion and the exponent

6.1 Sampling

Let $s_0 = 479$ and

$$N = \frac{(hq)^4}{B^{s_0}} = r^{4k - s_0} B_2^{4(k-1) - s_0} q^4. \tag{6.1}$$

This is an integer divisible by hq, and $N \ge h$. Choose G_h uniformly in $\mathrm{SL}_3(\mathbb{Z}/h\mathbb{Z})$ and $\mathcal{V}$ as in Section 4, independently. Given these shared choices, each sample draws a fresh column c as in Section 3, a fresh uniform element of $\mathcal{V}$, and a uniform $u \in \mathcal{B}$ with $u \equiv G_h c \pmod h$ and $u \bmod q$ equal to that element. Each prescribed residue pair has exactly $(N/(hq))^3$ lifts. The exact lifting identity [1, Lemma 6.2] holds verbatim: conditional on C and the labels,

$$\Pr(A \in \mathcal{E} \mid C) = \frac{h^9}{N^9 |\mathcal{O}_C|} \sum_{A \in \mathcal{E},\ A \bmod h \in \mathcal{O}_C} W(A).$$

A triple is *bad* if its projections are pairwise distinct and $|\det A| \le \tau$. Since $2\tau < h$, at most one determinant value in $[-\tau, \tau]$ is possible, and none unless $\mathcal{J}$ occurs. By Lemma 3.2, Proposition 5.1 and Corollary 3.4,

$$\Pr(\text{bad}) \ll (\log 2N)^2 \frac{h}{N^3} \mathbb{E}[D \mathbf{1}_{\mathcal{J}}] \ll (\log 2N)^2 \frac{h}{N^3 r^3}. \tag{6.2}$$

For two samples, $\Pr(\pi(u) = \pi(v)) \ll (hq)^6 N^{-3}$ [1, Lemma 6.1].

6.2 Deletion

Fix $\gamma = 354042/354043 < 1$, put $a_r = r^\gamma\sqrt{N^3/\tau}$, $n_r = \lfloor a_r \rfloor$, and take $2n_r$ samples. Let Z count the pairs with equal projections and the bad triples. Then

$$\frac{\mathbb{E}Z}{n_r} \ll n_r\frac{(hq)^6}{N^3} + n_r^2(\log 2N)^2\frac{h}{N^3r^3}.$$

For the first term, $N^{3/2} = (hq)^6B^{-3s_0/2}$ and $\tau \geq B^{k-1}/3$, so

$$n_r\frac{(hq)^6}{N^3} \leq \frac{r^\gamma B^{3s_0/2}}{\sqrt{\tau}} \leq \sqrt{3}\,r^\gamma B^{(3s_0-(k-1))/2} = \sqrt{3}\,r^\gamma B^{-1} \to 0,$$

because $3s_0 - (k-1) = 1437 - 1439 = -2$ and $B \gg r^6$. For the second term, $n_r^2 \leq r^{2\gamma}N^3/\tau$ and $h/\tau \leq 3r$, so it is $\ll (\log 2N)^2 r^{2\gamma-2} \to 0$, since $\log 2N \ll \log r$ and $\gamma < 1$. Hence $\mathbb{E}Z < n_r$ for all large r. Deleting one index from each counted pair or triple leaves at least n_r samples whose projections are distinct and whose triples satisfy $|\det A| > \tau$. Every coordinate u_3 lies in $[N, 2N)$, so the projective area identity gives

$$\Delta(P_r) \geq \frac{\tau}{16N^3}, \qquad n_r^2\Delta(P_r) \geq \frac{a_r^2}{4}\cdot\frac{\tau}{16N^3} = \frac{r^{2\gamma}}{64}$$

for a set P_r of n_r points.

6.3 The exponent

We have $h = rB^{k-1}$, $h^6 < q \leq 2h^6$, $B \asymp r^6$ and $\tau \asymp B^{k-1}$. Hence

$$a_r = r^\gamma\frac{(hq)^6}{B^{3s_0/2}\sqrt{\tau}} \asymp r^\gamma\, h^{42}B^{-3s_0/2-(k-1)/2} \asymp r^{\gamma+42}B^{\frac{83}{2}(k-1)-\frac{3}{2}s_0} \asymp r^\alpha,$$

$$\alpha = \gamma + 42 + 249(k-1) - 9s_0 = \gamma + 42 + 249\cdot 1439 - 4311 = \gamma + 354042.$$

So $a_0r^\alpha \leq n_r \leq b_0r^\alpha$ for constants $a_0, b_0 > 0$ and all large primes r, and $n_r^2\Delta(P_r) \geq r^{2\gamma}/64 \geq c\,n_r^{2\gamma/\alpha}$. With $\gamma = 354042/354043$,

$$\frac{2\gamma}{\alpha} = \frac{2\cdot 354042/354043}{354042\cdot 354044/354043} = \frac{2}{354044} = \frac{1}{177022} = \eta.$$

6.4 Every cardinality

Given a large n, let $y = (n/a_0)^{1/\alpha}$ and choose a prime $r \in (y, 2y]$. Then $n \leq n_r \leq C_0n$ with $C_0 = 2^\alpha b_0/a_0$. Keeping n points of P_r does not decrease the minimum area, so $\Delta(n) \geq \Delta(P_r) \geq c\,n_r^{-2+\eta} \geq c\,C_0^{-2}n^{-2+\eta}$. This proves Theorem 1.1. □

7 Remarks

Where the gain comes from. In [1, 2, 3] the modulus is $h = B^k$ and the obstruction excludes $[-\tau, \tau]$ with $h/\tau \asymp B$; the collision probability must beat $B\,r^{2\gamma}$, which forces $d = 5$ even with the fresh-digit refinement. With $B \equiv 0 \pmod r$ the information "$\gamma_{k-1} \not\equiv 0 \pmod r$" already excludes the window for the smaller modulus rB^{k-1}, so only $r\,r^{2\gamma}$ must be beaten. The digit lengths, the cap and the lift box are unchanged from [2, 3].

The value of γ. Any $\gamma < 1$ works in the deletion step; the choice $\gamma = 354042/354043$ gives the clean value $1/177022$, and the exponents obtained approach $2/354043$. With γ this close to 1 the second term in the deletion step is small only once $(\log r)^2 r^{-2/354043}$ is, so n_0 is astronomically large; this does not affect the theorem.

Checks. The ancillary files contain: the design check (`check_design.py`); the exact identity (2.4) and the column (2.3) for random labels with $d = 3$, $r = 23$ (`check_encoding.py`); an end-to-end test that builds the actual integer digit columns with the parameters (3.1)–(3.2) for $r = 23$ and verifies Lemma 3.1 (`check_obstruction.py`); and the exponent arithmetic (`exponent.py`).

Status. This note has not been refereed.

References

[1] OpenAI, *A power improvement in the Heilbronn triangle lower bound*, OpenAI Math Release preprint, September 25, 2026; source commit 1581d4cb.

[2] I. Blinov, *Heilbronn triangle bounds: finite packings and improved scales*, GitHub research draft (littleBro/heilbronn-triangle-bounds), October 2026.

[3] Euler team (canghaimeng), *A smaller lift box in the degree-five Heilbronn construction*, GitHub (canghaimeng/openai-math-improvement, bound-191), October 18, 2026.

[4] J. Komlós, J. Pintz and E. Szemerédi, A lower bound for Heilbronn's problem, *J. London Math. Soc.* (2) 25 (1982), 13–24.