THE DIAMETER OF $\mathrm{U}(3, \mathbb{Z}/m\mathbb{Z})$ WITH RESPECT TO THE FUNDAMENTAL ROOTS IS $2\lfloor m/2 \rfloor$ FOR EVERY $m \geq 8$

KOREA SUPERINTELLIGENCE LABS

Abstract. Let $\mathrm{U}(3, \mathbb{Z}/m\mathbb{Z})$ be the group of upper unitriangular 3×3 matrices over $\mathbb{Z}/m\mathbb{Z}$, and let its Cayley graph be taken with respect to the four fundamental-root generators $I \pm E_{12}$, $I \pm E_{23}$. The CayleyPy collaboration (arXiv:2509.19162) computed the diameter of this graph for $m = 8, \ldots, 50$, found it to be $2\lfloor m/2 \rfloor$ throughout that range, and conjectured (their Conjecture 8) that, for the undirected Cayley graph on the fundamental roots, the diameter of $\mathrm{U}(n, \mathbb{Z}/m\mathbb{Z})$ equals $(n-1)\lfloor m/2 \rfloor$ for all large enough m, without naming a threshold. We prove the case $n = 3$ of that conjecture for every $m \geq 8$: every element of $\mathrm{U}(3, \mathbb{Z}/m\mathbb{Z})$ is a product of at most $2\lfloor m/2 \rfloor$ generators, and the element $(\lfloor m/2 \rfloor, \lfloor m/2 \rfloor, 0)$ needs that many. The upper bound is an explicit lattice-path construction — one horizontal excursion carrying a prescribed number of up- and down-steps — together with a three-case arithmetic inequality; it involves no computation over m. The threshold 8 is sharp: at $m = 7$ the element $(0, 0, 3)$ is not a product of six generators, which is checked by enumerating all 5461 words of length at most six. Every statement is machine-checked in Lean 4 over Mathlib, with the standard axioms only.

1. Introduction

The objects. Fix an integer $m \geq 1$ and write $H_m = \mathrm{U}(3, \mathbb{Z}/m\mathbb{Z})$ for the group of upper unitriangular 3×3 matrices over $\mathbb{Z}/m\mathbb{Z}$ — the Heisenberg group modulo m. Writing the matrix $I + aE_{12} + bE_{23} + cE_{13}$ as the triple (a, b, c), where E_{ij} is the matrix unit, the product is

$$(a, b, c)\,(a', b', c') \;=\; (a + a',\ b + b',\ c + c' + ab'). \tag{1}$$

The *fundamental-root generators* are the four elements $I \pm E_{12}$, $I \pm E_{23}$, that is

$$x = (1, 0, 0), \quad x^{-1} = (-1, 0, 0), \quad y = (0, 1, 0), \quad y^{-1} = (0, -1, 0),$$

a symmetric set $\mathcal{S} = \{x^{\pm 1}, y^{\pm 1}\}$, so the Cayley graph Γ_m of H_m with respect to $\mathcal{S}$ (vertices H_m, an edge between g and gs for $s \in \mathcal{S}$) is an undirected graph. A Cayley graph is vertex-transitive, so its diameter is the eccentricity of the identity: writing $B_m(n)$ for the set of products of at most n elements of $\mathcal{S}$,

$$\operatorname{diam} \Gamma_m \;=\; \min\{\, n \geq 0 : B_m(n) = H_m \,\}.$$

The question is the value of $\operatorname{diam} \Gamma_m$ as a function of m.

The source. This question is raised in Section 3.9 (*Bounds on the diameters of unitriangular groups*, p. 27) of the CayleyPy collaboration's paper [1], which reports large-scale computations of growth functions and diameters of Cayley graphs. Concerning the groups $\mathrm{U}(n, \mathbb{Z}/m\mathbb{Z})$ it says, verbatim:

> Here the group is considered with respect to the generators $E \pm E_{i,i+1}$ (fundamental roots). Experimentally, we see that starting from large enough m, the diameters of $U(n, \mathbb{Z}/m\mathbb{Z})$ are in fact linear in m, see Fig. 12. In particular, for $n = 3$ and $m = 8, \ldots, 50$ the diameter equals $2\lfloor \frac{m}{2} \rfloor$, while for $n = 4$ and $m = 12, \ldots, 31$ it is $3\lfloor \frac{m}{2} \rfloor$.

and then, after introducing the alternative generating set of all positive roots $E \pm E_{ij}$, $i < j$, and the directed graphs on the monoid generators $E + E_{i,i+1}$ or $E + E_{ij}$, states

> **Conjecture 8.** For large enough m (depending on n) the diameter of $U(n, \mathbb{Z}/m\mathbb{Z})$ is a follows [sic]:

- Fundamental, undirected: $(n-1)\lfloor \frac{m}{2} \rfloor$;
- Fundamental, oriented: $(n-1)m + O(1)$;
- Positive, undirected: $(n-1)\lfloor \frac{m}{2} \rfloor$;
- Positive, oriented: $(n-1)m - 2$.

Note that the conjectural diameters in both undirected cases are equal to each other and to the diameter of $(\mathbb{Z}/m\mathbb{Z})^{n-1}$ under natural generators. Since the latter is the abelianization of $U(n, \mathbb{Z}/m\mathbb{Z})$, one immediately gets that these values serve as a lower bound (for all m).

(The statement number and the page are those of the arXiv PDF of v2. The raw LaTeX of the e-print carries neither a label nor a number for this conjecture, and a local compilation of the e-print places the passage on p. 28; the quotations above were checked against both.) So what the source proves is the lower bound, by the abelianization; what it verifies, by computation, is $n = 3$, $m = 8, \dots, 50$; and what it conjectures is the exact value for all large m, with no threshold named.

What is settled here. We prove the $n = 3$, fundamental, undirected case of Conjecture 8 for every $m \geq 8$, and we show that 8 is exactly the right threshold.

Theorem 1.1 (= Theorem 5.1)**.** *For every $m \geq 8$,* $\operatorname{diam} \Gamma_m = 2\lfloor m/2 \rfloor$.

Theorem 1.2 (= Theorem 4.6 and Proposition 5.2)**.** *For every $m \geq 8$, every element of* $\mathrm{U}(3, \mathbb{Z}/m\mathbb{Z})$ *is a product of at most* $2\lfloor m/2 \rfloor$ *of the generators* $x^{\pm 1}, y^{\pm 1}$*. For* $m = 7$ *the element* $(0, 0, 3)$ *is not a product of* $6 = 2\lfloor 7/2 \rfloor$ *of them, so the formula of Theorem 1.1 fails at* $m = 7$*.*

The lower bound $\operatorname{diam} \Gamma_m \geq 2\lfloor m/2 \rfloor$ is, as the source says, immediate from the abelianization; we include its short proof (Proposition 3.1) because the exact value rests on it, but we claim nothing new for it. The content of the paper is the upper bound. Its proof reads a word in $x^{\pm 1}, y^{\pm 1}$ as a lattice path in the plane and the third coordinate of its value as the discrete line integral $\sum x\,dy$ along the path; a single horizontal excursion — D steps to the left, then one sweep to the right of width $W = D + E$ carrying g up-steps and g' down-steps at freely chosen horizontal positions — realises *every* integer of an interval of $W(g + g') + 1$ consecutive values of $\sum x\,dy$ at word length $2D + E + g + g'$ (Lemma 4.3). Choosing the five parameters as an explicit function of the target and of m makes the interval at least m long and the word at most $2\lfloor m/2 \rfloor$ long, and the whole proof is then the verification of one arithmetic inequality in three regimes (Section 4). The proof is uniform in m: no case of the theorem is established by enumeration.

The threshold is where the arithmetic is tight. For $2 \leq m \leq 7$ the diameter is larger than $2\lfloor m/2 \rfloor$ (Section 7), and the one instance of this that the sharpness claim needs, $m = 7$, is proved by exhausting the 5461 words of length at most 6 (Proposition 5.2). Two further checks, a lower and an upper control at $m = 8$ and an upper control at $m = 100$, are recorded in Section 6 so that the main statement is pinned from both sides at concrete moduli.

Prior work. The only published diameter bounds for these groups that we know of are of a different kind. Ellenberg's thesis [2] treats the unipotent subgroup of $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$, that is, $\mathrm{U}(n, \mathbb{Z}/p\mathbb{Z})$ itself, and Ellenberg and Tymoczko [3] extend this to the unipotent subgroup of any finite group of Lie type of rank n over a *prime* field $\mathbb{Z}/p\mathbb{Z}$: with respect to its natural generators, the diameter of the Cayley graph is bounded above and below by constant multiples of $np + n^2 \log p$. That is an estimate up to unspecified constants, and it concerns prime moduli only; the present paper gives an exact value, for every modulus $m \geq 8$. (We cite [2] through [1] and the abstract of [3]; we have not seen it.)

The word metric of the *integer* Heisenberg group with respect to x, y has been computed exactly by Blachère [4], whose abstract announces "an exact formula for the word distance on the discrete Heisenberg group $\mathbb{H}_3$ with its standard set of generators". His Theorem 2.2 concerns the same group law (1) over $\mathbb{Z}$ and the generators $A = I + E_{12}$, $B = I + E_{23}$ and their inverses; it first reduces, by the same three symmetries as in Section 2, to $z \geq 0$, $x \geq 0$, $x \geq y \geq -x$, and then gives the word length of (x, y, z) by one of five closed forms, the cases being cut out by the sign of y and by the comparisons of x with $\sqrt{z}$, of xy with z and of x with $\sqrt{z - xy}$. For instance the length is $x + y$ when $y \geq 0$ and

$xy \geq z$, which is the monotone-staircase case of Lemma 4.1 below combined with the abelianization bound. See also Duchin and Mooney [5] for the asymptotic geometry of that metric and Alekseev and Magdiev [6] for its geodesics. One could imagine reducing such a formula modulo m. We do not: the two facts about the integer group that the proof uses — the lattice-path dictionary (Lemma 2.1) and the interval property of the excursion (Lemma 4.3) — are elementary and are proved here from the group law, and nothing in the paper depends on a citation.

The question here is also distinct from a random-generator question. Hermon and Olesker-Taylor [7], among the open questions closing their paper, conjecture that when the number k of generators diverges suitably, the law of the diameter of the Cayley graph of $\mathrm{U}(d, \mathbb{Z}/p\mathbb{Z})$, p prime, with respect to k generators chosen independently and uniformly at random concentrates. That concerns random generating sets; the graph here has one fixed generating set of four elements.

Verification. Every theorem, proposition and lemma stated below as a result is machine-checked in Lean 4 [8] over Mathlib [9]; Section 9 lists the checked statements verbatim and the axioms they depend on. The material in Section 7 (a breadth-first search over $m \leq 400$ and two scripts that exercise the construction) is computation outside the formal development, labelled as such, and nothing else in the paper depends on it.

2. Preliminaries

Throughout, $m \geq 1$, $H_m = \mathrm{U}(3, \mathbb{Z}/m\mathbb{Z})$ with the product (1), and the identity is $(0,0,0)$; the inverse is $(a,b,c)^{-1} = (-a,-b,ab-c)$. We write

$$h = \lfloor m/2 \rfloor, \qquad w = \lfloor h/2 \rfloor.$$

A *word* is a finite sequence $s_1 s_2 \cdots s_n$ of elements of $\mathcal{S} = \{x^{\pm 1}, y^{\pm 1}\}$; its *value* is the product $s_1 s_2 \cdots s_n \in H_m$ and its *length* is n. The *ball* $B_m(n) \subseteq H_m$ is the set of values of words of length at most n, so $B_m(0) = \{1\}$, $B_m(n) \subseteq B_m(n+1)$ and $B_m(n)B_m(n') \subseteq B_m(n+n')$. Since $\mathcal{S}$ generates H_m and H_m is finite, $B_m(n) = H_m$ for all large n, and $\operatorname{diam} \Gamma_m = \min\{n : B_m(n) = H_m\}$ is the diameter of the (undirected) Cayley graph.

The lattice-path dictionary. Read a word as a path in $\mathbb{Z}^2$ starting at the origin: the letter $x^{\pm 1}$ is a horizontal unit step in the direction ± 1 and $y^{\pm 1}$ a vertical unit step. For a word $s_1 \cdots s_n$ let $(p_i, q_i) \in \mathbb{Z}^2$ be the position after i steps, so $(p_0, q_0) = (0,0)$.

Lemma 2.1 (dictionary)**.** *The value of the word $s_1 \cdots s_n$ is*

$$\Big(p_n, \ \ q_n, \sum_{i \,:\, s_i = y^{\varepsilon_i}} \varepsilon_i \, p_{i-1} \Big) \pmod{m},$$

the sum running over the vertical steps, $\varepsilon_i \in \{\pm 1\}$ being the direction of the i-th step and p_{i-1} the horizontal coordinate at which it is taken. In words: the first two coordinates are the net displacements and the third is the discrete line integral $\sum x\,dy$ along the path.

Proof. By (1), $(a,b,c)\,(\pm 1,0,0) = (a \pm 1, b, c)$ and $(a,b,c)\,(0,\pm 1,0) = (a, b \pm 1, c \pm a)$: a horizontal step does not change the third coordinate, and a vertical step in direction ε adds ε times the current first coordinate. Induct on n. □

Three symmetries. The maps

$$\sigma_1(a,b,c) = (-a,b,-c), \qquad \sigma_2(a,b,c) = (a,-b,-c), \qquad \tau(a,b,c) = (b,a,c)$$

are, respectively, two automorphisms and one anti-automorphism ($\tau(gg') = \tau(g')\tau(g)$; in matrix terms τ is $M \mapsto JM^{\mathsf{T}}J$ for the antidiagonal permutation matrix J) of H_m, as one checks from (1). Each permutes $\mathcal{S}$: σ_1 exchanges $x \leftrightarrow x^{-1}$, σ_2 exchanges $y \leftrightarrow y^{-1}$, and τ exchanges $x \leftrightarrow y$. Hence each preserves word length: the image of the value of a word is the value of the letterwise image of the word, reversed in the case of τ. In particular $B_m(n)$ is stable under σ_1, σ_2, τ. In the formal development the two sign symmetries are not separate lemmas: every path lemma below is stated with two global signs $u, v \in \{\pm 1\}$ multiplying the horizontal and the vertical directions, and the reversal τ is the one symmetry proved as a lemma.

The ball of radius n in the formal development. For the reader comparing with Section 9: there H_m is the structure `H m` with fields `x`, `y`, `z` in `ZMod m`, the four generators are the predicate `IsGen`, "$g \in B_m(n)$" is `Reach m n g` (there is a list of at most n generators whose product is g), and $\operatorname{diam} \Gamma_m$ is `diam m`, the infimum of $\{n : \forall g,$ `Reach m n g`$\}$.

3. The lower bound

This is the source's own remark, in its most elementary form. Nothing in it needs $m \geq 8$.

Proposition 3.1 (abelianization bound; the source's remark after Conjecture 8)**.** *Let $m \geq 1$ and $h = \lfloor m/2 \rfloor$. If the element $(h, h, 0) \in \mathrm{U}(3, \mathbb{Z}/m\mathbb{Z})$ is a product of n generators, then $n \geq 2h$. Consequently* $\operatorname{diam} \Gamma_m \geq 2\lfloor m/2 \rfloor$ *for every m.*

Proof. Let $s_1 \cdots s_n$ be a word with value $(h, h, 0)$ and let $(p, q) = (p_n, q_n) \in \mathbb{Z}^2$ be the endpoint of its path. Each letter moves exactly one coordinate by one, so $|p| + |q| \leq n$, and by Lemma 2.1 $p \equiv h$ and $q \equiv h \pmod m$. If $|p| < h$ then $p - h$ is a nonzero integer with $|p - h| \leq |p| + h < 2h \leq m$, so it is not divisible by m, a contradiction. Thus $|p| \geq h$, likewise $|q| \geq h$, and $n \geq |p| + |q| \geq 2h$. The last sentence follows since $(h, h, 0) \notin B_m(2h - 1)$. $\square$

4. The upper bound

4.1. **Three path lemmas.** All three are statements about the set of values of $\sum x\,dy$ over paths of a given shape, and each is proved by writing down the path. Signs $u, v \in \{\pm 1\}$ are carried throughout: replacing x by x^u and y by y^v in a word multiplies the first coordinate of its value by u, the second by v and the third by uv (Lemma 2.1).

Lemma 4.1 (monotone staircase)**.** *Let $e, g, n \in \mathbb{N}$ with $n \leq eg$ and $u, v \in \{\pm 1\}$. Then $(ue,\ vg,\ uvn) \in B_m(e + g)$.*

Proof. By the sign remark it suffices to treat $u = v = 1$. If $g = 0$ then $n = 0$ and the word x^e does it. Otherwise write $n = kg + s$ with $0 \leq s < g$; then $k \leq e$, and $k + 1 \leq e$ if $s \geq 1$. The word

$$x^k\, y^g\, x^{e-k} \quad (s = 0), \qquad\qquad x^k\, y^{g-s}\, x\, y^s\, x^{e-k-1} \quad (s \geq 1)$$

has length $e + g$, endpoint (e, g), and $\sum x\,dy = kg$, respectively $k(g - s) + (k + 1)s = kg + s$, which is n in both cases. $\square$

Only two distinct horizontal coordinates carry vertical steps, so a word of five blocks $x^p y^q x^r y^s x^t$ — with value $(p + r + t,\ q + s,\ pq + (p + r)s)$ — suffices; this is the only reachability primitive the formal development derives directly from the generators.

Lemma 4.2 (one sweep, both vertical directions)**.** *Let $W, g, g' \in \mathbb{N}$, $u, v \in \{\pm 1\}$, and let $n \in \mathbb{Z}$ with $-Wg' \leq n \leq Wg$. Then $(uW,\ v(g - g'),\ uvn) \in B_m(W + g + g')$.*

Proof. Take $u = v = 1$. If $n \geq 0$, prefix the staircase word of Lemma 4.1 for (W, g, n) by $y^{-g'}$: the g' down-steps are taken at horizontal coordinate 0 and contribute nothing to $\sum x\,dy$, so the value is $(W, g - g', n)$ and the length is $W + g + g'$. If $n < 0$, prefix y^g to the staircase word for $(W, g', -n)$ with its vertical direction reversed (Lemma 4.1 with $v = -1$), whose value is $(W, -g', n)$. $\square$

Lemma 4.3 (one excursion)**.** *Let $D, E, g, g' \in \mathbb{N}$, $u, v \in \{\pm 1\}$, and let $c_0 \in \mathbb{Z}$ with*

$$-(Dg + Eg') \;\leq\; c_0 \;\leq\; Eg + Dg'.$$

Then $(uE,\ v(g - g'),\ uvc_0) \in B_m(2D + E + g + g')$. In particular, with $W = D + E$, the values of the third coordinate attained at the endpoint $(uE, v(g - g'))$ within this length fill an interval of $W(g + g') + 1$ consecutive integers.

Proof. Take $u=v=1$. Go left D steps, then perform the sweep of Lemma 4.2 with width $W=D+E$ and $n=c_0+D(g-g')$. Every vertical step of the sweep is taken at a horizontal coordinate that is D less than in Lemma 4.2, so the endpoint is $(E,g-g')$ and $\sum x\,dy=n-D(g-g')=c_0$. The hypotheses on c_0 are exactly $-Wg'\le n\le Wg$, and the length is $D+(W+g+g')=2D+E+g+g'$. □

4.2. **The parameter rule.** Let $m\ge 1$. Every residue $t\in\mathbb{Z}/m\mathbb{Z}$ is uA for a sign u and an integer $0\le A\le h$ (take $A=\min(t,m-t)$ for the representative $0\le t<m$). So a target (a,b,c) can be written (uA,vB,c) with $0\le A,B\le h$, and, applying τ if necessary, with $B\le A$. Given such A,B, set

$$\begin{aligned} &W=\max(A,w), && T=2h+A-2W, && G=\text{the largest integer}\le T\text{ with }G\equiv B \pmod 2,\\ &g=\tfrac{G+B}{2}, && g'=\tfrac{G-B}{2}, && D=W-A, \qquad E=A. \end{aligned} \tag{2}$$

One checks $T\ge B$ in every case ($T=2h-A\ge h\ge B$ when $W=A$, and $T\ge h+A\ge B$ when $W=w$), so $B\le G\le T$ and $G\ge T-1$; and $g,g'\in\mathbb{N}$ with $g+g'=G$, $g-g'=B$.

Lemma 4.4 (the excursion, packaged)**.** *Let $m\ge 1$, $u,v\in\{\pm1\}$, $c\in\mathbb{Z}/m\mathbb{Z}$ and $A,B,W,G\in\mathbb{N}$ with $A\le W$, $B\le G$, $G\equiv B \pmod 2$,*

$$2W+G\le 2h+A \qquad \text{and} \qquad m-1\le WG.$$

Then $(uA,vB,c)\in B_m(2h)$.

Proof. With g,g',D,E as in (2), Lemma 4.3 realises (uA,vB,uvc_0) at length $2D+E+g+g'=2W-A+G\le 2h$ for every integer c_0 in an interval of $(D+A)(g+g')+1=WG+1\ge m$ consecutive integers. Such an interval meets every residue class modulo m, in particular the class of $uv\,c$ (as $u^2=v^2=1$). □

4.3. **The three regimes.** By Lemma 4.4, and since $m-1\le 2h$, the upper bound reduces to the inequality $WG\ge 2h$ for the parameters (2). Here is where $m\ge 8$, i.e. $h\ge 4$ and $w\ge 2$, enters.

Lemma 4.5. *Let $m\ge 8$, $0\le B\le A\le h$, and let W,G be given by* (2)*. Then $2W+G\le 2h+A$ and $WG\ge 2h\ge m-1$.*

Proof. The length bound is $G\le T$. For the coverage bound there are three regimes.

Regime 1: $A\ge 2$ and $A\ge w$. Then $W=A$, $T=2h-A$ and $G\ge 2h-A-1$, so it suffices that $A(2h-A-1)\ge 2h$. Put $A=A'+2$ with $0\le A'\le h-2$ and $Q=2h-A'-6\ge h-4\ge 0$; then $2h-A-1=Q+3$ and $A(2h-A-1)=(A'+2)(Q+3)=A'Q+3A'+2Q+6\ge A'+Q+6=2h$.

Regime 2: $2\le A<w$. Then $W=w\ge 3$ and $T=2h+A-2w\ge h+2$ (as $2w\le h$), so $G\ge h+1$ and $WG\ge 3(h+1)>2h$.

Regime 3: $A\le 1$, hence $B\le 1$. Then $W=w\ge 2$ and $T=2h+A-2w$. We claim $G\ge 2h-2w$. If $A=1$ this is $G\ge T-1$. If $A=0$ then $B=0$ and $T=2h-2w$ is even, so the parity condition is satisfied by T itself and $G=T$. Hence $WG\ge 2(2h-2w)\ge 2h$, using $2w\le h$ once more. □

Regime 3 is the delicate one, and it explains both the reduction to $B\le A$ and the threshold. At $m=8$ ($h=4$, $w=2$) the target $(0,1,c)$ taken with $A=0$, $B=1$ would give $T=4$, $G=3$ and $WG=6<7=m-1$: the family of words (2) does not cover it. Its mirror image $(1,0,c)$, $A=1$, $B=0$, gives $T=5$, $G=4$, $WG=8\ge 7$ at length $2W-A+G=7$, and τ transports the word. At $m=7$ ($h=3$, $w=1$) the target $(0,0,c)$ gives $W=1$, $G=4$, $WG=4<6$, and there the theorem itself is false (Proposition 5.2).

Theorem 4.6 (upper bound)**.** *Let $m\ge 8$. Every element of $\mathrm{U}(3,\mathbb{Z}/m\mathbb{Z})$ is a product of at most $2\lfloor m/2\rfloor$ of the generators $x^{\pm1},y^{\pm1}$; that is, $B_m(2\lfloor m/2\rfloor)=H_m$.*

Proof. Write the target as (uA,vB,c) with $0\le A,B\le h$ as above. If $B\le A$, Lemmas 4.5 and 4.4 give $(uA,vB,c)\in B_m(2h)$. If $A<B$, the same applied to (vB,uA,c) gives a word of length at most $2h$ with that value, and its image under the anti-automorphism τ — the reversed word with $x\leftrightarrow y$ exchanged — has value $\tau(vB,uA,c)=(uA,vB,c)$ and the same length. □

The proof is constructive and uniform in m: the word for a given target is determined by (2), and no step of the argument is a case analysis over m or over the elements of the group.

5. The exact value, and the threshold

Theorem 5.1 ($n = 3$, fundamental, undirected case of Conjecture 8 of [1]). *For every* $m \geq 8$ *the diameter of the Cayley graph of* $\mathrm{U}(3, \mathbb{Z}/m\mathbb{Z})$ *with respect to* $\{I \pm E_{12},\, I \pm E_{23}\}$ *is exactly* $2\lfloor m/2 \rfloor$.

Proof. $B_m(2h) = H_m$ by Theorem 4.6, so $\operatorname{diam}\Gamma_m \leq 2h$; and $B_m(2h-1) \neq H_m$ by Proposition 3.1, so $\operatorname{diam}\Gamma_m \geq 2h$. □

The theorem is what the source verified for $8 \leq m \leq 50$, now for every $m \geq 8$, and "large enough m" in Conjecture 8 is, for $n = 3$, precisely $m \geq 8$:

Proposition 5.2 (the threshold is sharp). *In* $\mathrm{U}(3, \mathbb{Z}/7\mathbb{Z})$ *the element* $(0, 0, 3)$ *is not a product of at most* $6 = 2\lfloor 7/2 \rfloor$ *generators. Consequently* $\operatorname{diam}\Gamma_7 \neq 2\lfloor 7/2 \rfloor$.

Proof. This is a finite check, and it is carried out inside the proof assistant: the list of all values of words of length exactly k is built by appending one generator to each value of length $k-1$, for $k = 0, 1, \ldots, 6$ — $1 + 4 + \cdots + 4^6 = 5461$ products in all — and it is proved (by induction on the word) that the value of every word of length k occurs in the k-th list. The element $(0, 0, 3)$ occurs in none of the seven lists, which the kernel verifies by evaluation. The second sentence follows: if $\operatorname{diam}\Gamma_7$ were 6 then $B_m(6)$ would be all of $\mathrm{U}(3, \mathbb{Z}/7\mathbb{Z})$. □

Remark 5.3. Since balls are nested, the proposition says that $\operatorname{diam}\Gamma_7 \geq 7$; together with Proposition 3.1 this is all that is proved about $m = 7$. The value $\operatorname{diam}\Gamma_7 = 8$, and the values for $2 \leq m \leq 6$, are computed in Section 7 and are not part of the formal development. Note also that the hypothesis $m \geq 8$ of Theorem 5.1 is used, not merely convenient: the proof of Lemma 4.5 needs $h \geq 4$, and the conclusion is false at $h = 3$.

6. Controls

A statement of the form "$\operatorname{diam}\Gamma_m = f(m)$" can be wrong in two directions, and a misplaced quantifier in a formal definition of the diameter could make it vacuously provable. The following instances pin Theorem 5.1 from below and from above at concrete moduli, and were checked independently of it as far as their content allows.

Proposition 6.1 (not too small). *In* $\mathrm{U}(3, \mathbb{Z}/8\mathbb{Z})$ *the element* $(4, 4, 0)$ *is not a product of* 7 *generators. Hence* $\operatorname{diam}\Gamma_8 \leq 7$ *is false.*

Proof. The instance $m = 8$, $n = 7$ of Proposition 3.1. (The value 7 was taken from the breadth-first search of Section 7, which gives $\operatorname{diam}\Gamma_8 = 8$, not from memory.) □

Proposition 6.2 (not too large, and attained). $\operatorname{diam}\Gamma_8 = 8$ *and* $\operatorname{diam}\Gamma_{100} = 100$*; moreover* $(4, 4, 0) \in \mathrm{U}(3, \mathbb{Z}/8\mathbb{Z})$ *is a product of* 8 *generators.*

Proof. Instances of Theorem 5.1 at $m = 8$ and $m = 100$, and of Theorem 4.6 at $m = 8$. The two moduli straddle the source's verified range: 8 is its first verified modulus and 100 twice its last. For $(4, 4, 0)$ the rule (2) gives $A = B = 4$, $W = 4$, $T = 4$, $G = 4$, $g = 4$, $g' = 0$, $D = 0$: the word is a staircase from $(0, 0)$ to $(4, 4)$ whose $\sum x\,dy$ is $\equiv 0 \pmod 8$, e.g. $x^2y^4x^2$ with $\sum x\,dy = 8$. □

7. Outside the formal development: the small moduli

Everything in this section is computation that was run while the theorems were being found; it is reported for completeness and is *not* machine-checked, and no statement above depends on it.

Breadth-first search. A breadth-first search from the identity over the m^3 elements of $\mathrm{U}(3,\mathbb{Z}/m\mathbb{Z})$, with the four generators as neighbours (a short C program with 16-bit distance labels), was run for every $1 \le m \le 400$, and the whole range was re-run for this paper with an independently written program, which returned the same 400 diameters. It gives

range	$\operatorname{diam}\Gamma_m$	
$m = 1$	$0 = 2\lfloor m/2 \rfloor$	
$2 \le m \le 7$	$2\lfloor m/2 \rfloor + 2$	i.e. $4, 4, 6, 6, 8, 8$
$8 \le m \le 400$	$2\lfloor m/2 \rfloor$	all 393 values

The source's range $m = 8, \dots, 50$ is reproduced value for value, and the range $8 \le m \le 400$ is, after Theorem 5.1, a corollary. The information that is not a corollary is the exceptional list $2 \le m \le 7$, where the diameter exceeds the abelianization bound by exactly 2. The elements at maximal distance were also recorded, by the re-run, for every $m \le 400$: for $2 \le m \le 7$ they are central elements $(0, 0, c)$ only, with c near $m/2$ (at $m = 7$: $(0, 0, 3)$ and $(0, 0, 4)$, which is where the witness of Proposition 5.2 comes from); for $8 \le m \le 11$ both such central elements and the abelianization-extremal elements $(h, h, *)$ occur (for odd m also $(h, h+1, *)$, $(h+1, h, *)$, $(h+1, h+1, *)$), and at $m = 9$ in addition the four elements $(1, 1, 5)$, $(1, 8, 4)$, $(8, 1, 4)$, $(8, 8, 5)$, the orbit of $(1, 1, 5)$ under the sign symmetries; and for $12 \le m \le 400$ only the abelianization-extremal elements. This is what shaped the proof: for $12 \le m \le 400$ the only elements at maximal distance are the ones the abelianization already explains, so a construction may be lossy elsewhere, while at $8 \le m \le 11$ the central elements are also extremal, which is why the parity of G in (2) has to be tracked and why the threshold is 8 rather than 12. Each run of the whole table cost under fifteen CPU-minutes.

Two checks of the rule. Before the formal proof was written, the rule (2) was exercised numerically. First, for every $8 \le m \le 600$ and every $0 \le B \le A \le h$ the inequalities $2W - A + G \le 2h$ and $WG \ge m - 1$ were evaluated directly: no failure. For $4 \le m \le 7$ the same evaluation fails, at $(A, B) \in \{(0, 0), (0, 1), (1, 0)\}$, matching the failure of the theorem there. Second, for every $8 \le m \le 40$ and every one of the m^3 elements — 671 616 targets in all — the actual word (the excursion of Lemma 4.3 with the sign and τ reductions applied) was built from (2), evaluated in $\mathrm{U}(3,\mathbb{Z}/m\mathbb{Z})$ by (1), and compared with the target and with the length bound $2h$: no failure. Neither check is used in any proof; the second is what would have caught a wrong parameter rule before the formal proof was attempted.

8. What remains open

Conjecture 8 of [1] has four cases for every $n \ge 3$, and this paper settles one case for $n = 3$. We record what the source reports about the rest, and what the present method does and does not offer.

- *$n = 4$, fundamental, undirected.* The source reports the value $3\lfloor m/2 \rfloor$ for $m = 12, \dots, 31$. The abelianization lower bound is again immediate. The construction here is one-dimensional in the "area" coordinate; $\mathrm{U}(4,\mathbb{Z}/m\mathbb{Z})$ has three superdiagonal coordinates and two independent commutator coordinates, so the analogue of Lemma 4.3 would have to cover a two-dimensional set of values, and we have no such lemma.
- *The oriented cases.* These concern the directed Cayley graph on the monoid generators $E + E_{i,i+1}$ (or $E + E_{ij}$). The lattice-path picture applies with monotone paths, but nothing is proved here; the $O(1)$ in the fundamental oriented case is not pinned by the source.
- *Positive roots, $n = 3$.* The additional generator $I \pm E_{13}$ is central; the undirected diameter is conjectured to be $2\lfloor m/2 \rfloor$ again, presumably with a different exceptional list. Nothing is proved here.
- *The exceptional list.* That $\operatorname{diam}\Gamma_m = 2\lfloor m/2 \rfloor + 2$ for $2 \le m \le 7$ is computed (Section 7), and only the half of the $m = 7$ case needed for sharpness is proved. The "not reachable" halves can be proved as in Proposition 5.2; the "reachable" halves need one word per element.
- The source adds that "a similar phenomenon occurs for other unipotent groups, in particular, the maximal unipotent subgroups of symplectic groups", without printing values.

9. Verification

All results of Sections 3–6 are formalised and checked in Lean 4 (v4.32.0) over Mathlib [9], in five modules — `Core` (the group, the generators, the ball, the five-block word), `Paths` (Lemmas 4.1–4.3 and the reversal τ), `Upper` (Lemma 4.4, Lemma 4.5, Theorem 4.6), `Lower` (Proposition 3.1, the diameter, Theorem 5.1) and `Controls` (Propositions 5.2–6.2). Repository reference to be added at submission. The definitions are

```
structure H (m : ℕ) where
  x : ZMod m
  y : ZMod m
  z : ZMod m

instance : Mul (H m) := ⟨fun g h => ⟨g.x + h.x, g.y + h.y, g.z + h.z + g.x * h.y⟩⟩

def IsGen (g : H m) : Prop :=
  g = ⟨1, 0, 0⟩ ∨ g = ⟨-1, 0, 0⟩ ∨ g = ⟨0, 1, 0⟩ ∨ g = ⟨0, -1, 0⟩

def Reach (m : ℕ) (n : ℕ) (g : H m) : Prop :=
  ∃ w : List (H m), w.length ≤ n ∧ (∀ s ∈ w, IsGen s) ∧ w.prod = g

noncomputable def diam (m : ℕ) : ℕ := sInf {n | ∀ g : H m, Reach m n g}
```

(with `m : ℕ` a variable, and a `Group (H m)` instance proved from the product), and the checked statements, verbatim, are:

```
theorem reach_all (hm : 8 ≤ m) (g : H m) : Reach m (2 * (m / 2)) g

theorem le_of_reach_extremal {n : ℕ}
    (h : Reach m n (⟨((m / 2 : ℕ) : ZMod m), ((m / 2 : ℕ) : ZMod m), 0⟩ : H m)) :
    2 * (m / 2) ≤ n

theorem diam_eq (hm : 8 ≤ m) : diam m = 2 * (m / 2)

theorem not_reach_extremal : ¬ Reach 8 7 (⟨(4 : ZMod 8), (4 : ZMod 8), 0⟩ : H 8)

theorem not_reach_seven : ¬ Reach 7 6 (⟨(0 : ZMod 7), (0 : ZMod 7), 3⟩ : H 7)

theorem diam_seven_ne : diam 7 ≠ 2 * (7 / 2)

theorem diam_eight : diam 8 = 8

theorem diam_hundred : diam 100 = 100

theorem reach_extremal_eight : Reach 8 8 (⟨(4 : ZMod 8), (4 : ZMod 8), 0⟩ : H 8)
```

Here `reach_all` is Theorem 4.6, `le_of_reach_extremal` is Proposition 3.1, `diam_eq` is Theorem 5.1, `not_reach_seven` and `diam_seven_ne` are Proposition 5.2, `not_reach_extremal` is Proposition 6.1, and the last three are Proposition 6.2. Two remarks on the formal statements. In Lean, `m / 2` on natural numbers is $\lfloor m/2 \rfloor$, and `sInf` of a set of natural numbers is its least element when the set is nonempty (which it is for every $m \geq 1$, the group being finite), so `diam m` is $\operatorname{diam} \Gamma_m$; the proof of `diam_seven_ne` treats the empty case separately and does not rely on this. The only computation performed by the kernel anywhere in the development is the enumeration of Proposition 5.2: the seven lists are built by a recursive definition, completeness of the enumeration is a proved lemma, and non-membership of $(0, 0, 3)$ is decided by evaluation (`decide`); no compiled evaluator (`native_decide`) is used. Consequently, by `#print axioms`, every listed statement depends only on `propext`, `Classical.choice` and `Quot.sound`, and `not_reach_seven` only on `propext` and `Quot.sound`; there is no `sorry`. Lemmas 2.1 and the three symmetries are, in the formal text, the group law itself, the lemma `Reach.swp` for τ, and the sign parameters of the path lemmas.

References

[1] CayleyPy collaboration (A. Chervov, D. Fedoriaka, E. Konstantinova, A. Naumov, I. Kiselev, A. Sheveleva, I. Koltsov, S. Lytkin, A. Smolensky, A. Soibelman, F. Levkovich-Maslyuk, R. Grimov, D. Volovich, A. Isakov, A. Kostin, M. Litvinov, N. Vilkin-Krom, A. Bidzhiev, A. Krasnyi, M. Evseev, E. Geraseva, L. Grunwald, S. Galkin, E. Koldunov, S. Diner, A. Chevychelov, E. Kudasheva, A. Sychev, A. Kravchenko, Z. Kogan, A. Natyrova, L. Shishina, L. Cheldieva, V. Zamkovoy, D. Kovalenko, O. Papulov, S. Kudashev, D. Shiltsov, R. Turtayev, O. Nikitina, D. Mamayeva, S. Nikolenko, M. Obozov, A. Titarenko, A. Dolgorukova, A. Aparnev, O. Debeaupuis, S. Alami C., H. Isambert), *CayleyPy Growth: Efficient growth computations and hundreds of new conjectures on Cayley graphs (Brief version)*, arXiv:2509.19162v2 (v1 23 Sep 2025; v2 1 Apr 2026). Section 3.9 and Conjecture 8 are on p. 27 of the arXiv PDF of v2.

[2] J. Ellenberg, *A sharp diameter bound for an upper triangular matrix group*, senior honors thesis, Harvard University, 1993. Cited after [1]; not seen by the authors.

[3] J. S. Ellenberg and J. Tymoczko, *A sharp diameter bound for unipotent groups of classical type over $\mathbb{Z}/p\mathbb{Z}$*, Forum Mathematicum **22** (2010), no. 2, 327–347; `doi:10.1515/forum.2010.018`; arXiv:math/0510506.

[4] S. Blachère, *Word distance on the discrete Heisenberg group*, Colloquium Mathematicum **95** (2003), no. 1, 21–36; `doi:10.4064/cm95-1-2`.

[5] M. Duchin and C. Mooney, *Fine asymptotic geometry in the Heisenberg group*, Indiana University Mathematics Journal **63** (2014), no. 3, 885–916; `doi:10.1512/iumj.2014.63.5308`; arXiv:1106.5276.

[6] I. Alekseev and R. Magdiev, *The language of geodesics for the discrete Heisenberg group*, arXiv:1905.03226 (2019).

[7] J. Hermon and S. Olesker-Taylor, *Cutoff for random walks on upper triangular matrices*, arXiv:1911.02974v2 (2021); the conjecture quoted is in the section *Open Questions and Conjectures* of v2.

[8] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: A. Platzer and G. Sutcliffe (eds.), Automated Deduction — CADE 28, Lecture Notes in Computer Science **12699**, Springer, Cham, 2021, pp. 625–635; `doi:10.1007/978-3-030-79876-5_37`.

[9] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381; `doi:10.1145/3372885.3373824`.