Zero-Class Geometry and Boundary Growth in the Multiplication Table Modulo N

Ofer Barasofsky

March 2026

Abstract

For $A_{N,a} = \{(x, y) \in \{1, \ldots, N-1\}^2 : xy \equiv a \pmod{N}\}$, let $S(N, a)$ be the area of the convex hull of $A_{N,a}$ and let $S(N) = \sum_{a=0}^{N-1} S(N, a)$. We study these areas as geometric invariants of the full multiplication table modulo N. The central exact package concerns the zero residue class: one obtains a sharp degeneracy criterion, an exact divisor-rectangle description of the hull, a lower-envelope formulation, and an exact hyperbola-gap decomposition of $S(N, 0)$. As a complementary global result, the first boundary model yields an exact residue-wise lower model and implies the cubic-order theorem $S(N) = \Theta(N^3)$. The point of view differs from the usual single-class modular-hyperbola treatment by keeping the full residue family in view and by making the zero-divisor side of the geometry structurally explicit.

Keywords. multiplication table modulo N; modular hyperbolas; convex hulls; zero divisors; boundary models

1 Introduction and positioning

For a fixed integer $N \geq 2$, the multiplication table modulo N is the array whose (x, y) entry is the residue of xy modulo N, with

$$1 \leq x, y \leq N - 1.$$

For each residue $a \in \{0, 1, \ldots, N-1\}$ we write

$$A_{N,a} := \{(x, y) \in \{1, \ldots, N-1\}^2 : xy \equiv a \pmod{N}\},$$

and we measure its Euclidean size by

$$S(N, a) := \text{Area}(\text{conv}(A_{N,a})).$$

The associated total area is

$$S(N) := \sum_{a=0}^{N-1} S(N,a).$$

Proposition 1.1 (Integrality of residue-class areas)**.** *For every $N \geq 2$ and every residue $a \in \{0,\dots,N-1\}$, the area $S(N,a)$ is an integer.*

Proof. If $A_{N,a}$ is empty or collinear, then $S(N,a)=0$. Otherwise conv$(A_{N,a})$ is a lattice polygon, because its vertices are points of $A_{N,a} \subset \mathbb{Z}^2$.

The map

$$(x,y) \mapsto (N-x, N-y)$$

preserves the congruence $xy \equiv a \pmod{N}$, so $A_{N,a}$ and its convex hull are centrally symmetric about $(N/2, N/2)$. For a nondegenerate centrally symmetric lattice polygon, the center lies in the interior, so every boundary lattice point is paired with a distinct boundary lattice point under this half-turn. Hence the number B of lattice points on the boundary is even.

Pick's theorem [1] now gives

$$S(N,a) = I + \frac{B}{2} - 1,$$

where I is the number of interior lattice points. Since I is an integer and B is even, $S(N,a)$ is an integer. ■

Each fixed set $A_{N,a}$ is already a modular hyperbola in the usual sense [2]. Convex-hull questions for such sets also appear in the existing literature; see for example Konyagin and Shparlinski's work on vertex counts [3]. The point of view taken here is different. Rather than studying a single congruence class in isolation, we keep the whole residue family

$$\{A_{N,0}, A_{N,1}, \dots, A_{N,N-1}\}$$

inside one multiplication table and ask how the residue-wise convex hulls fit together.

There is also a nearby multiplication-table lineage. The classical Erdős problem asks how many distinct ordinary products occur in an $N \times N$ multiplication table, a quantity known to grow more slowly than the naive quadratic scale; Koukoulopoulos studies a generalized asymptotic version of that question [4]. The present note studies a different global invariant: the summed residue-wise convex-hull area $S(N)$, whose first theorem already shows genuine cubic order of growth.

This shift changes the geometry in two ways.

1. The zero residue class becomes central rather than exceptional. For non-prime moduli it

records the zero-divisor side of the multiplication table, and that side has a rigid divisor-controlled geometry that does not appear in the unit classes.

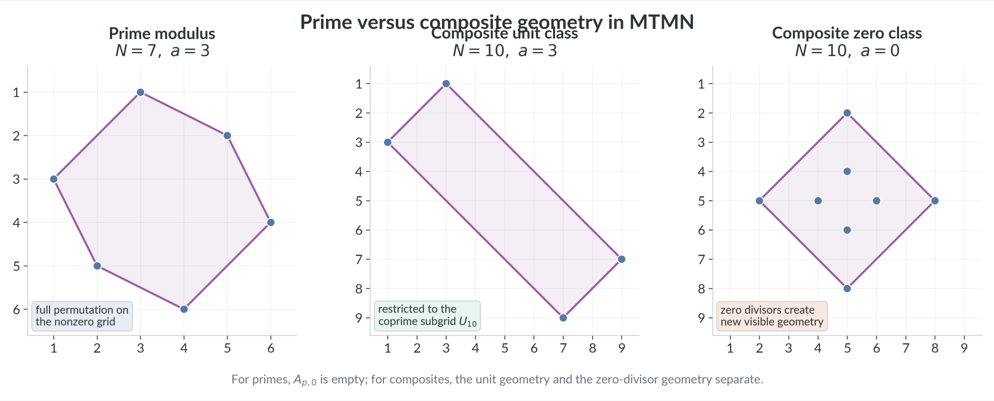
2. The table can be built border by border, so the first geometric approximations are forced by the table itself. This leads to exact boundary-layer models and, already from the first layer, to a nontrivial global theorem on the growth of $S(N)$.

The present note isolates the strongest theorem-bearing package now available. Its main results are:

1. the integrality of every residue-class area $S(N, a)$;
2. a sharp degeneracy criterion for the zero class;
3. an exact divisor-rectangle description of conv$(A_{N,0})$;
4. a lower-envelope description of the same hull;
5. an exact hyperbola-gap decomposition of $S(N, 0)$;
6. exact first-boundary formulas;
7. the cubic-order theorem $S(N) = \Theta(N^3)$.

The paper is intentionally compact. It does not try to reproduce the broader framework of support functions, residue-area polynomials, or higher boundary layers. Those belong to the longer monograph. The goal here is narrower: to put the zero-class geometry and the first exact global growth theorem into a form that can be read quickly and judged on its own.

Figure 1 is the opening picture to keep in mind. Prime moduli present only the unit-side geometry, whereas composite moduli already contain a visible zero-divisor class.



Prime versus composite geometry in MTMN

Prime modulus
$N = 7,\ a = 3$

Composite unit class
$N = 10,\ a = 3$

Composite zero class
$N = 10,\ a = 0$

For primes, $A_{p,0}$ is empty; for composites, the unit geometry and the zero-divisor geometry separate.

Figure 1: Prime and composite moduli separate immediately into different geometric regimes. Prime nonzero classes occupy the full nonzero grid, while composite moduli exhibit both a restricted coprime subgrid and a visible zero-divisor class.

2 Zero-class geometry

The residue class $A_{N,0}$ is where the multiplication table first distinguishes prime from composite moduli geometrically. For primes there are no zero divisors, so no interior zero class appears. For composite moduli the same arithmetic obstruction creates a visible planar object.

Theorem 2.1 (Zero-class degeneracy criterion). *For every integer $N \geq 2$,*

$$S(N,0) = 0 \iff \big(N \text{ is prime}\big) \text{ or } N = 4.$$

Proof. If $N = p$ is prime, then no $x, y \in \{1, \dots, p-1\}$ is divisible by p, so $xy \not\equiv 0 \pmod{p}$ and $A_{p,0} = \varnothing$. Hence $S(p,0) = 0$. For $N = 4$ one has

$$A_{4,0} = \{(2,2)\},$$

so again the hull is degenerate.

Now assume that N is composite and $N > 4$. If N is even, then

$$(2, N/2), \quad (N/2, 2), \quad (N-2, N/2), \quad (N/2, N-2)$$

all belong to $A_{N,0}$ and form a rhombus of positive area. If N is odd composite, choose a proper divisor d of N and write $e = N/d$. Then

$$(d, e), \quad (N-d, e), \quad (d, N-e), \quad (N-d, N-e)$$

all belong to $A_{N,0}$ and form a rectangle of positive area. Thus every composite $N > 4$ gives $S(N,0) > 0$. ■

To describe the full hull, one must use the divisor structure of N more systematically.

Definition 2.1 (Divisor rectangles). For each proper divisor d of a composite integer N, define

$$R_d := [d, N-d] \times \left[\frac{N}{d}, N - \frac{N}{d}\right].$$

The point is that a proper divisor produces not only one zero-class point such as $(d, N/d)$, but an entire divisor-controlled rectangle or, in degenerate cases, a segment.

Theorem 2.2 (Exact divisor-rectangle description). *If N is composite, then*

$$\mathrm{conv}(A_{N,0}) = \mathrm{conv}\left(\bigcup_{\substack{d \mid N \\ 1<d<N}} R_d \right).$$

Proof. Let $(x, y) \in A_{N,0}$ and set $d = \gcd(x, N)$. Write $x = dx'$ and $N = dN'$ with $\gcd(x', N') = 1$. Since $N \mid xy$, one has $N' \mid x'y$, hence $N' \mid y$. The divisor d is proper because $d = 1$ would force $N \mid y$ and $d = N$ would force $x = N$, both impossible. Therefore

$$d \le x \le N - d, \qquad \frac{N}{d} \le y \le N - \frac{N}{d},$$

so $(x, y) \in R_d$. This proves

$$A_{N,0} \subseteq \bigcup_{\substack{d \mid N \\ 1<d<N}} R_d.$$

Conversely, for each proper divisor d the four corners

$$\left(d, \frac{N}{d}\right), \quad \left(N - d, \frac{N}{d}\right), \quad \left(d, N - \frac{N}{d}\right), \quad \left(N - d, N - \frac{N}{d}\right)$$

all lie in $A_{N,0}$. Since R_d is the convex hull of those corners, one has $R_d \subseteq \mathrm{conv}(A_{N,0})$. Taking unions and convex hulls gives the reverse inclusion. ■

Figure 2 shows why the smallest divisor pair is not enough in general. For $N = 12$, the rectangles coming from the intermediate divisors 3 and 4 enlarge the hull beyond the seed rhombus suggested by $(2, 6)$ and $(6, 2)$ alone.

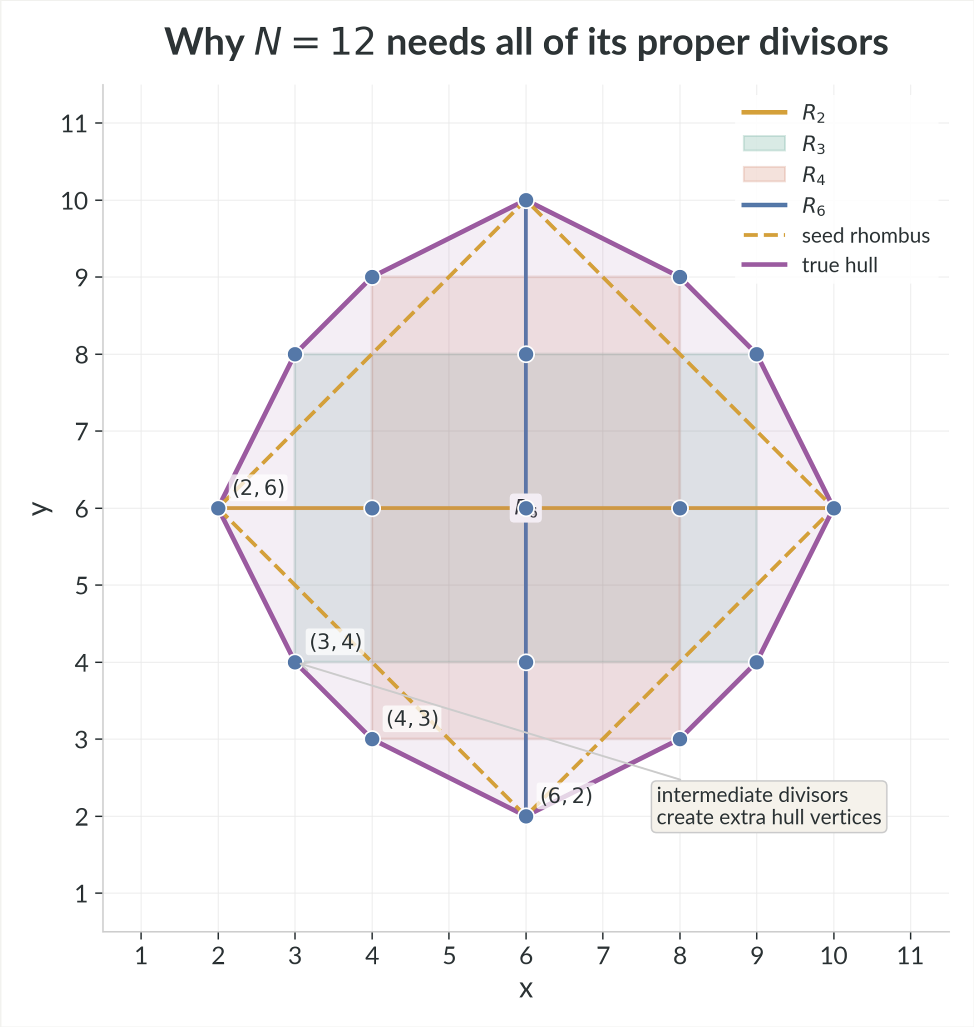


Figure 2: The zero class for $N = 12$ is built from all proper divisors, not only the extreme pair. The intermediate divisor rectangles enlarge the true hull beyond the dashed seed rhombus.

The rectangle description can be compressed further by keeping only the lower corners of the divisor rectangles.

Definition 2.2 (Divisor points and lower envelope). Assume that N is composite, and let

$$p := \min\{d > 1 : d \mid N\}$$

be the smallest proper divisor of N. Define

$$E_N := \left\{ \left(d, \frac{N}{d}\right), \left(N-d, \frac{N}{d}\right) : 1 < d < N,\ d \mid N \right\}.$$

For $p \le x \le N-p$, let $\ell_N(x)$ be the y-coordinate of the lower edge of conv(E_N) at horizontal position x.

Proposition 2.3 (Lower-envelope description of the zero-class hull). *If N is composite, then*

$$\text{conv}(A_{N,0}) = \{(x,y) : p \le x \le N-p,\ \ell_N(x) \le y \le N - \ell_N(x)\}.$$

Proof. By the divisor-rectangle theorem it is enough to describe the hull of the union of the rectangles R_d. For a fixed x-coordinate, the lowest point in any contributing rectangle occurs on its lower edge at height N/d for some proper divisor d. These lower-edge points are exactly the points that generate conv(E_N). Thus the lowest possible height in the hull at coordinate x is $\ell_N(x)$.

The zero class is centrally symmetric under $(x,y) \mapsto (N-x, N-y)$, so the upper boundary is the reflected graph $y = N - \ell_N(x)$. The horizontal range is exactly $[p, N-p]$ because every divisor rectangle lives in that strip. ■

Corollary 2.4 (Integral formula). *If N is composite, then*

$$S(N,0) = \int_p^{N-p} \big(N - 2\ell_N(x)\big)\, dx.$$

Proof. The previous proposition identifies the vertical thickness of the hull at coordinate x as

$$\big(N - \ell_N(x)\big) - \ell_N(x) = N - 2\ell_N(x).$$

Integrating this thickness over $[p, N-p]$ gives the area. ■

3 Hyperbola-gap decomposition

The divisor points

$$\left(d, \frac{N}{d}\right)$$

lie on the continuous hyperbola

$$y = \frac{N}{x},$$

but the lower edge of the zero-class hull is not the hyperbola itself. It is the polygonal lower convex envelope through the sampled divisor points. The first task is therefore to compare the exact envelope with the continuous curve.

Figure 3 shows the basic picture. The support vertices lie on the hyperbola, but the line segments joining them lie above it.

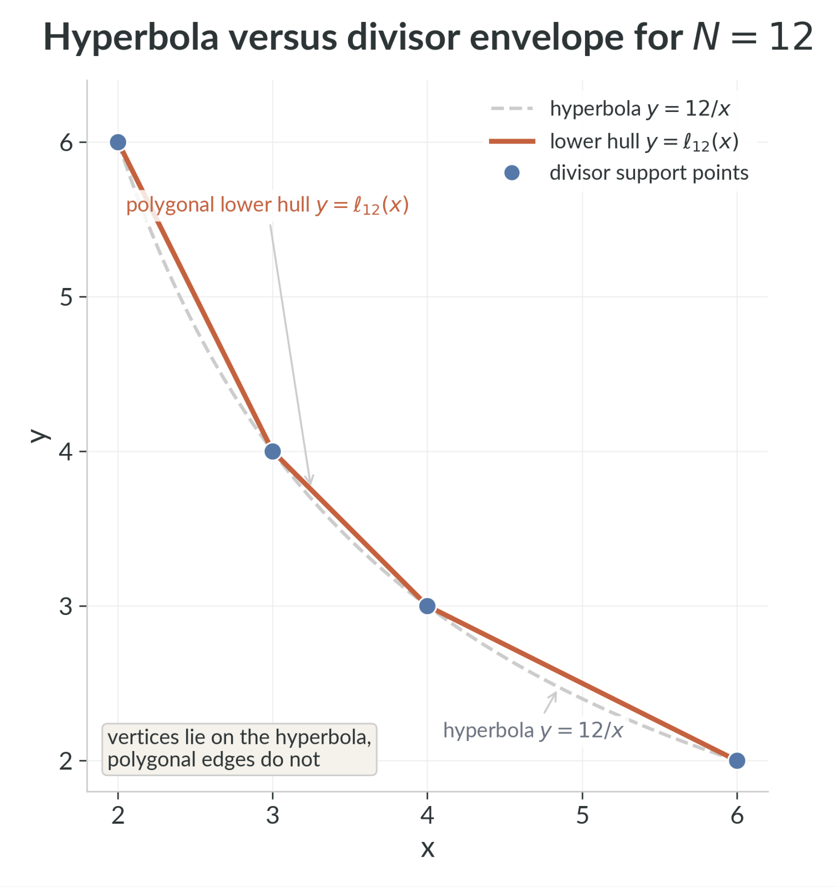


Figure 3: For $N = 12$, the lower hull is a polygonal envelope through divisor points on the hyperbola $y = 12/x$. The vertices lie on the curve, but the edges are straight chords and therefore sit above the hyperbola.

Proposition 3.1 (The divisor envelope lies above the hyperbola). *If N is composite, then*

$$\ell_N(x) \geq \frac{N}{x} \qquad \text{for } p \leq x \leq \frac{N}{2}.$$

Proof. The function $x \mapsto N/x$ is convex on $(0, \infty)$ because

$$\frac{d^2}{dx^2}\left(\frac{N}{x}\right) = \frac{2N}{x^3} > 0.$$

Hence every secant line between two divisor points on the left lower hull lies above the hyperbola on the interval between them. Those secants are precisely the linear pieces of ℓ_N before the symmetry point $x = N/2$. If N is odd, the final interval from the last divisor point to $N/2$ is horizontal, and the decreasing hyperbola still lies below it. Thus $\ell_N(x) \geq N/x$ throughout the informative half. ■

Definition 3.1 (Left-half hyperbola gap). For composite N, define

$$\Delta_N := \int_p^{N/2} \left(\ell_N(x) - \frac{N}{x}\right) dx.$$

By the preceding proposition, $\Delta_N \geq 0$. Geometrically it is exactly the area between the polygonal lower envelope and the continuous hyperbola on the informative left half of the picture.

Theorem 3.2 (Exact hyperbolic decomposition of the zero-class area). *If N is composite, then*

$$S(N, 0) = N(N - 2p) - 4N \ln\left(\frac{N}{2p}\right) - 4\Delta_N.$$

Proof. From the integral formula of the previous section,

$$S(N, 0) = \int_p^{N-p} \big(N - 2\ell_N(x)\big)\, dx.$$

Because $\ell_N(N - x) = \ell_N(x)$, the integrand is symmetric about $x = N/2$, so

$$S(N, 0) = 2\int_p^{N/2} \big(N - 2\ell_N(x)\big)\, dx.$$

Now write

$$\ell_N(x) = \frac{N}{x} + \left(\ell_N(x) - \frac{N}{x}\right).$$

Then

$$N - 2\ell_N(x) = \left(N - \frac{2N}{x}\right) - 2\left(\ell_N(x) - \frac{N}{x}\right),$$

and substitution yields

$$S(N,0) = 2\int_p^{N/2} \left(N - \frac{2N}{x}\right)\,dx - 4\int_p^{N/2} \left(\ell_N(x) - \frac{N}{x}\right)\,dx.$$

The second integral is exactly Δ_N. The first is elementary:

$$2\int_p^{N/2} \left(N - \frac{2N}{x}\right)\,dx = 2\left[Nx - 2N \ln x\right]_p^{N/2} = N(N-2p) - 4N \ln\left(\frac{N}{2p}\right).$$

Combining the two terms gives the identity. ■

The significance of the formula is conceptual as well as exact. The term

$$N(N-2p) - 4N \ln\left(\frac{N}{2p}\right)$$

is the area obtained by replacing the polygonal divisor envelope with the smooth hyperbola on the informative half and then reflecting by symmetry. The exact zero-class area is that continuous baseline minus the arithmetic correction $4\Delta_N$.

This places the formula beside the same classical hyperbolic backdrop that underlies the Dirichlet divisor problem [5]. The object measured here is different, however: Δ_N is not a lattice-point counting error term below the hyperbola, but the exact convex-envelope discrepancy between the smooth curve and the polygonal divisor hull.

4 First boundary and cubic growth

The zero class controls one sharp piece of the composite geometry. A complementary global theorem comes from the outer frame of the multiplication table.

Definition 4.1 (First boundary). For $N \geq 2$ and $a \in \{0, 1, \dots, N-1\}$, define

$$B^{(1)}_{N,a} := A_{N,a} \cap \big((\{1, N-1\} \times \{1, \dots, N-1\}) \cup (\{1, \dots, N-1\} \times \{1, N-1\})\big),$$

and set

$$S^{(1)}(N,a) := \text{Area}(\text{conv}(B^{(1)}_{N,a})), \qquad S^{(1)}(N) := \sum_{a=0}^{N-1} S^{(1)}(N,a).$$

By construction,

$$B_{N,a}^{(1)} \subseteq A_{N,a}, \qquad S^{(1)}(N,a) \leq S(N,a), \qquad S^{(1)}(N) \leq S(N).$$

So the first boundary is an exact lower model, not a heuristic truncation.

> **Theorem 4.1** (Exact first-boundary formula)**.** *For every* $N \geq 2$,
>
> $$S^{(1)}(N,0) = 0,$$
>
> *and for* $1 \leq a \leq N-1$,
>
> $$S^{(1)}(N,a) = 2(a-1)(N-a-1).$$

Proof. On the row $x = 1$, the congruence $xy \equiv a \pmod{N}$ gives the point $(1,a)$. On the column $y = 1$ it gives $(a,1)$. On the opposite row and column one gets

$$(N-1, N-a), \qquad (N-a, N-1).$$

These four points form a parallelogram, degenerate when $a = 1$ or $a = N-1$. Its area is the determinant

$$\left|\det\begin{pmatrix} a-1 & N-2 \\ 1-a & N-2a \end{pmatrix}\right| = 2(a-1)(N-a-1).$$

This proves the formula. ■

Figure 4 shows the four-point geometry in one glance.

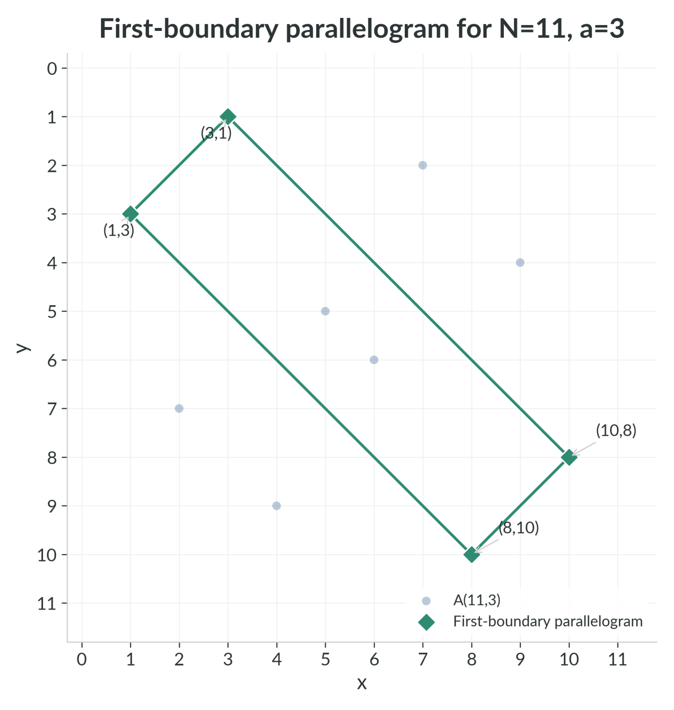


Figure 4: For $N = 11$ and $a = 3$, the four first-boundary points form a parallelogram whose area is the exact first-boundary contribution $S^{(1)}(11, 3)$.

Corollary 4.2 (Exact total first-boundary sum). *For every* $N \geq 2$,

$$S^{(1)}(N) = \frac{(N-3)(N-2)(N-1)}{3}.$$

Proof. Summing the residue-wise formula gives

$$S^{(1)}(N) = \sum_{a=1}^{N-1} 2(a-1)(N-a-1).$$

With the change of variables $b = a - 1$, this becomes

$$2\sum_{b=0}^{N-2} b\big((N-2) - b\big),$$

and the standard identities for $\sum b$ and $\sum b^2$ simplify it to the stated cubic polynomial. ■

The first boundary already forces the correct scale for the total area.

Theorem 4.3 (Cubic-order theorem). *For every* $N \geq 2$,

$$\frac{(N-3)(N-2)(N-1)}{3} \leq S(N) \leq N(N-2)^2.$$

In particular,

$$S(N) = \Theta(N^3).$$

Proof. The lower bound is exactly

$$S^{(1)}(N) \leq S(N)$$

together with the previous corollary. For the upper bound, every hull $\operatorname{conv}(A_{N,a})$ lies inside the square $[1, N-1]^2$, whose area is $(N-2)^2$. Hence

$$S(N,a) \leq (N-2)^2$$

for every residue a, and summing over the N residue classes gives

$$S(N) \leq N(N-2)^2.$$

The two explicit cubic bounds imply $S(N) = \Theta(N^3)$. ■

This theorem does not identify the sharp leading constant, but it already shows that the accumulated area of all residue classes has genuine cubic size. In particular, the outer frame alone contributes a full cubic-order amount:

$$S^{(1)}(N) \sim \frac{N^3}{3}.$$

5 Closing remarks

Two natural continuations lie immediately beyond the scope of this note.

The first is the second boundary. When N is odd, the same border-by-border viewpoint yields a second exact lower model: if

$$B^{(2)}_{N,a} := A_{N,a} \cap \big((\{2, N-2\} \times \{1, \dots, N-1\}) \cup (\{1, \dots, N-1\} \times \{2, N-2\})\big),$$

$$S^{(2)}(N,a) := \text{Area}(\operatorname{conv}(B^{(2)}_{N,a})),$$

and $b \equiv 2^{-1}a \pmod{N}$, then

$$S^{(2)}(N,a) = 2\,|b-2|\,|N-b-2|$$

for $1 \leq a \leq N-1$, together with an explicit cubic formula for the total $S^{(2)}(N)$. That result fits naturally behind the first-boundary theory developed here, but it is not needed for the main theorem package of the present paper.

The second continuation is structural rather than quantitative: characterize the points of $A_{N,a}$ that actually become vertices of conv$(A_{N,a})$. The zero class is now understood exactly, and the first boundary already forces cubic growth of $S(N)$, but the general vertex mechanism remains open. That problem seems to be the right next step if one wants to move from explicit lower models toward a sharper description of the full hull geometry.

The broader monograph develops these extensions, examples, and related conjectures. The purpose of the present note is more concentrated: to record a compact exact theory in which the zero-divisor geometry of the multiplication table modulo N becomes visible and the first global growth theorem for the total area follows from an equally explicit boundary model.

References

[1] G. Pick, “Geometrisches zur zahlenlehre,” *Sitzungsberichte des deutschen naturwissenschaftlich-medicinischen Vereines fur Bohmen “Lotos” in Prag*, vol. 19, pp. 311–319, 1899, Available: `https://hdl.handle.net/10622/02638381-D295-4F97-95C3-57EF49FE3D89`

[2] I. E. Shparlinski, “Modular hyperbolas,” *Japanese Journal of Mathematics*, vol. 7, 2012.

[3] S. V. Konyagin and I. E. Shparlinski, “On the convex hull of the points on modular hyperbolas.” 2010. Available: `https://arxiv.org/abs/1012.1444`

[4] D. Koukoulopoulos, “On the number of integers in a generalized multiplication table,” *Journal für die reine und angewandte Mathematik*, vol. 689, pp. 33–99, 2014, doi: 10.1515/crelle-2012-0064.

[5] A. Ivić, E. Krätzel, M. Kühleitner, and W. G. Nowak, “Lattice points in large regions and related arithmetic functions: Recent developments in a very classic topic.” 2004. Available: `https://arxiv.org/abs/math/0410522`