symmetry

Article

Geometric Structures from Bézout Decompositions of Semiprimes

Nikolaos Verykios and Christos Gogos *

Department of Informatics and Telecommunications, University of Ioannina, 47150 Arta, Greece; n.verykios@uoi.gr
* Correspondence: cgogos@uoi.gr

Abstract

For a semiprime $N = sp$, the normalized CRT–Bézout map assigns each unit modulo N a unique pair (m, n) in the rectangle $\{1, \ldots, p-1\} \times \{1, \ldots, s-1\}$. The coordinates mn, $\Delta = ms + np$, and $\delta = ms - np$ satisfy $\Delta^2 - \delta^2 = 4Nmn$ and give the geometric diagrams studied here. We describe the bounded affine slices $Am + Bn = \lambda$, including their point counts, complement symmetry, vertices, and spacings. We also write modular squaring in these coordinates: the two components evolve independently, while the nonempty fibers are orbits of a four-element Klein group. The complement symmetry of the slices is compatible with these dynamics. Finally, we determine the two admissible points with $|\delta| = 1$ and prove an exact count for the points in a central strip $|\delta| < T$. These results describe the geometry attached to a known factorization; they do not give a new factorization algorithm.

Keywords: integer factorization; semiprimes; quadratic forms; Bézout decomposition; parabolic envelopes; difference of squares

1. Introduction

This article studies the geometric structure generated by the Bézout decomposition attached to a semiprime

$$N = sp, \qquad s < p,$$

with s and p being distinct odd primes. For each residue b with $\gcd(b, N) = 1$, the CRT–Bézout construction produces a unique admissible pair (m, n). This pair satisfies

$$ms + np = b + \kappa N, \qquad \kappa \in \{0, 1\},$$

and gives the quantities

$$mn, \qquad \Delta = ms + np, \qquad \delta = ms - np.$$

These quantities satisfy the fundamental relation

$$\Delta^2 - \delta^2 = 4Nmn.$$

The $\Delta(mn)$ and $\delta(mn)$ diagrams exhibit parabolic envelopes and linear families; the (ms, np) plane has a rectangular lattice structure; and the squaring orbit produces affine branch lines in the (Δ, mn) diagram, which become decreasing hyperbolas after the reciprocal transformation $Y = N/(mn)$.

Check for updates

Academic Editor: Calogero Vetro

Received: 2 July 2026
Revised: 25 July 2026
Accepted: 27 July 2026
Published: 29 July 2026

Related Work

Three lines of work are relevant here.

First, there is substantial literature on the squaring map $x \mapsto x^2 \pmod{n}$ and its functional graphs: cycles, trees, fixed points, and orbit structure in residue rings [1]. We also study squaring modulo a semiprime $N = sp$, but our focus is different. We use the Bézout decomposition of each residue to organize the orbit data into geometric diagrams in the coordinates mn, Δ, and δ.

Second, modular hyperbolas and their coordinate sum and difference sets have an established arithmetic and geometric theory [2–5]. The comparison with our diagrams is methodological, not an identification of point sets: our coordinates $(u, v) = (ms, np)$ satisfy the exact level relation $uv = Nmn$, whereas a standard modular hyperbola is defined by $xy \equiv a \pmod{q}$, usually with $\gcd(a, q) = 1$.

Third, the article builds on the algebraic structure of $\mathbb{Z}_{sp}$ and semiprime decompositions via the Chinese remainder theorem [6,7]. Here we emphasize the geometry of the Bézout coordinates—point clouds, envelopes, and curve families—rather than only the algebraic identities.

These comparisons also clarify the scope of the paper. The envelope, tangent, endpoint, rectangular-lattice, and branch formulas are direct consequences of the defining identities and standard inequalities. The contribution lies in using the CRT–Bézout correspondence as a common finite coordinate model, describing its bounded affine slices, and relating their complement symmetry to modular-squaring dynamics.

Sections 2 and 3 introduce the coordinates and their elementary geometry. Sections 4–8 develop the affine slices, the δ and (ms, np) projections, the squaring dynamics, and the special values of δ; Section 9 concludes the paper.

2. Notation and Preliminaries

Let s, p be distinct odd primes with $s < p$ and $N = sp$. Fix the normalized Bézout pair $(c, d) \in \mathbb{Z}^2$ satisfying [8]

$$-cs + dp = 1, \qquad 1 \le c \le p - 1, \qquad 1 \le d \le s - 1. \tag{1}$$

We shall use the following standard CRT decomposition, expressed through Bézout coefficients.

Proposition 1 (CRT decomposition via Bézout coefficients; cf. [8])**.** *For every $b \in \{1, 2, \ldots, N-1\}$, there exists a unique pair $(m, n) \in \mathbb{Z}^2$ with $0 \le m < p$, $0 \le n < s$ and a unique wrap index $\kappa \in \{0, 1\}$ such that*

$$ms + np \; = \; b + \kappa N. \tag{2}$$

The values are computed explicitly by

$$m \equiv -cb \pmod{p}, \qquad n \equiv db \pmod{s}. \tag{3}$$

Proof. Multiply (1) by b: $b = (-cb)s + (db)p$. Reduce $-cb \bmod p \to m \in [0, p)$ and $db \bmod s \to n \in [0, s)$. Then $ms + np \equiv b \pmod{N}$, and since $0 \le ms + np \le (p-1)s + (s-1)p = 2N - s - p < 2N$, the integer $\kappa = (ms + np - b)/N$ lies in $\{0, 1\}$. If another canonical pair gave the same residue, reduction modulo p and modulo s would give the same m and n, respectively; the equality then fixes κ. $\square$

Throughout this paper, we restrict ourselves to *non-degenerate* pairs, i.e., those with $m \geq 1$ and $n \geq 1$. The degenerate cases $m = 0$ (equivalently $p \mid b$) and $n = 0$ (equivalently $s \mid b$) are excluded.

Definition 1 (Key quantities)**.** *For a decomposition (m, n, κ) associated with b:*

$$\Delta := ms + np = b + \kappa N, \tag{4}$$
$$\delta := ms - np. \tag{5}$$

From Definition 1, we immediately obtain the fundamental identity

$$\Delta^2 - \delta^2 = (ms + np)^2 - (ms - np)^2 = 4msnp = 4Nmn. \tag{6}$$

We introduce the following quadratic, whose roots are ms and np:

Definition 2 (Associated quadratic)**.** *For (m, n) with $mn \neq 0$:*

$$f(x) = \frac{x^2}{mn} - \frac{\Delta}{mn}\,x + N = \frac{1}{mn}\left(x^2 - \Delta\,x + Nmn\right). \tag{7}$$

It follows directly from the definitions that

$$x^2 - \Delta x + Nmn = (x - ms)(x - np).$$

Thus the associated quadratic has roots ms and np.

Throughout this paper, m and n are taken in their canonical ranges $m \in [1, p-1]$ and $n \in [1, s-1]$. We use the pair (m, n) when studying the geometric structure of all admissible pairs (Sections 3–6), and the value b with wrap index κ when studying the squaring orbit (Section 7).

Proposition 2 (Normalized CRT–Bézout coordinate model)**.** *Let*

$$\mathcal{A}_{s,p} = \{1, \ldots, p-1\} \times \{1, \ldots, s-1\}.$$

The normalized coordinate map

$$\Phi_{s,p} : \mathbb{Z}_N^\times \longrightarrow \mathcal{A}_{s,p}, \qquad b \longmapsto (m(b), n(b)),$$

defined by Equation (3), is a bijection. Under the embedding

$$\Psi_{s,p}(m, n) = \big(mn,\ ms + np,\ ms - np,\ ms,\ np\big),$$

the $\Delta(mn)$, $\delta(mn)$, and (ms, np) diagrams are coordinate projections of the same finite set $\Psi_{s,p}(\mathcal{A}_{s,p})$. The orbit and reciprocal diagrams are obtained by selecting a squaring orbit in $\mathbb{Z}_N^\times$ and applying the corresponding projection, followed in the reciprocal case by $mn \mapsto N/(mn)$.

Proof. Proposition 1 gives a unique canonical pair for each residue. If b is a unit, neither coordinate is zero. Conversely, for $(m, n) \in \mathcal{A}_{s,p}$, the residue $b \equiv ms + np \pmod{N}$ is nonzero modulo both p and s, and hence is a unit, and Proposition 1 recovers the same pair. This proves bijectivity. The projection statements follow from the definitions of Δ, δ, and the two additional coordinates ms, np. □

3. Geometric Structure in the (mn, Δ) Plane

This diagram plots the $(p-1)(s-1)$ points (mn, Δ) for all admissible pairs (m, n) with $1 \le m \le p-1$ and $1 \le n \le s-1$ (Figure 1). For the associated quadratic $x^2 - \Delta x + Nmn = 0$, the discriminant condition is $\Delta^2 - 4Nmn \ge 0$, or equivalently

$$mn \le \frac{\Delta^2}{4N}. \tag{8}$$

In the present construction, this condition is automatically satisfied, since $\Delta^2 - 4Nmn = \delta^2$.

The formulas below are elementary consequences of AM–GM and substitution and are retained to interpret the figures.

3.1. Elementary Envelope and Coordinate Families

3.1.1. Parabolic Envelope

AM–GM applied to ms and np gives the lower envelope

$$\Delta \;\ge\; 2\sqrt{Nmn}, \tag{9}$$

with equality if and only if $ms = np$, i.e., $m/n = p/s$.

The curve $\Delta^2 = 4Nmn$ is a parabola in the (mn, Δ) plane with focal parameter $f = N$ and a focus at $(N, 0)$, depending only on the product $N = sp$ and not on the individual factors s and p. The equality condition $ms = np$ is formal in the admissible lattice: it would force $m/n = p/s$, and hence $(m, n) = (p, s)$ up to a common factor, which lies outside the ranges $1 \le m \le p-1$ and $1 \le n \le s-1$. Thus no data point touches the envelope.

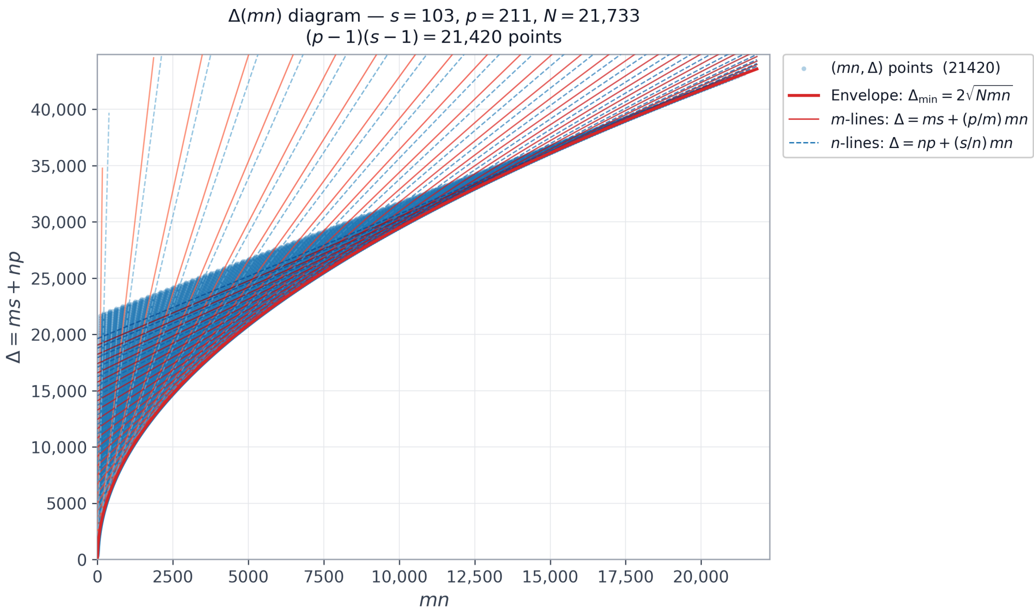

Figure 1. The $\Delta(mn)$ diagram for $s = 103$, $p = 211$. Blue dots: all (mn, Δ) points; red curve: parabolic envelope $\Delta_{\min} = 2\sqrt{Nmn}$. The families of straight lines (constant m or n) and parabolic arcs (constant ratio m/n) are visible in the structure. The admissible set lies above one N-dependent parabola, and a vertical cluster occurs when the same product mn has several admissible divisor pairs.

3.1.2. Constant-Coordinate Tangent Lines

In the (mn, Δ) diagram, fixing m and substituting $n = x/m$ gives

$$\Delta(x) = \frac{p}{m} \cdot x + ms. \tag{10}$$

https://doi.org/10.3390/sym18081291

This line is tangential to $\Delta = 2\sqrt{Nx}$ at

$$x^* = \frac{m^2 s}{p}, \qquad \Delta^* = 2ms. \tag{11}$$

For fixed n, the factor-exchange dual is

$$\Delta(x) = \frac{s}{n} \cdot x + np, \tag{12}$$

and is tangential to the same envelope at

$$x^* = \frac{n^2 p}{s}, \qquad \Delta^* = 2np. \tag{13}$$

Neither continuous tangency point is an admissible lattice point. Indeed, equating the slope p/m with $d(2\sqrt{Nx})/dx = \sqrt{N/x}$ gives (11); the corresponding value $n^* = ms/p$ is nonintegral. The fixed-n formulas follow by exchanging $(s, p; m, n)$ with $(p, s; n, m)$.

The two tangent-line families are exchanged by

$$(s, p; m, n) \longmapsto (p, s; n, m).$$

This relabeling preserves N, mn, and Δ, reverses the sign of δ, and identifies the second family as the factor-exchange dual of the first.

Every admissible pair (m_0, n_0) lies at the intersection of the line $m = m_0$ and the line $n = n_0$. Thus the scatter plot is formed by the superposition of the two tangent-line families. Within each line of constant m, the points have $x = m, 2m, \ldots, (s-1)m$, equally spaced with step m; lines with small m are thus more densely populated than lines with large m. Similarly, within each line of constant n, the points have $x = n, 2n, \ldots, (p-1)n$ with step n. When $x = mn$ has many divisors, several pairs (m, n) with $mn = x$ may exist, each lying on a different line and giving a different value of Δ; this creates vertical clusters above values of x with many divisors. Both families are visible in Figure 1.

3.1.3. Rational-Direction Families

For fixed coprime $h, \ell \geq 1$, the admissible pairs $(m, n) = (jh, j\ell)$ with

$$jh \leq p - 1, \qquad j\ell \leq s - 1,$$

trace the parabola

$$\Delta \;=\; \frac{hs + \ell p}{\sqrt{h\ell}} \cdot \sqrt{mn}. \tag{14}$$

It lies on or above (9), because AM–GM gives

$$\frac{hs + \ell p}{\sqrt{h\ell}} \;\geq\; 2\sqrt{N}, \tag{15}$$

with equality only for the formal ratio $h/\ell = p/s$, outside the admissible range.

For fixed coprime (h, ℓ), the δ-value of the j-th point in the family is

$$\delta_j = j(hs - \ell p) = j\delta_1, \qquad \delta_1 = hs - \ell p.$$

The classical theory of continued fractions [8] shows that convergents of p/s provide especially good rational approximations to p/s. In the present setting, this means that the corresponding pairs (h_i, ℓ_i) give small values of

$$|h_i s - \ell_i p|.$$

Consequently, the associated parabolic families lie close to the lower envelope

$$\Delta = 2\sqrt{Nmn}.$$

This structure is also visible as parabolic arcs in the (mn, Δ) diagram (Figure 2).

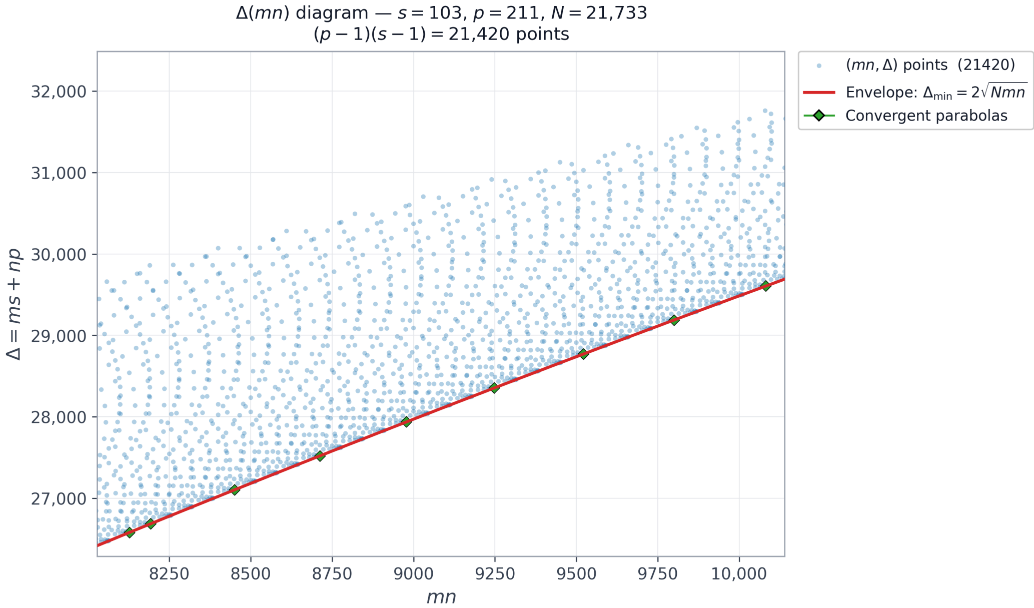

Figure 2. Parabolic families corresponding to convergents of p/s in the $\Delta(mn)$ diagram, shown as a detail (zoom) of Figure 1. Green diamonds mark the admissible integer multiples $(jh, j\ell)$ for the convergents h/ℓ of p/s; the corresponding parabolas are visually indistinguishable from the red envelope $\Delta_{\min} = 2\sqrt{Nmn}$ at this scale, because the exact excess coefficient $\left((hs + \ell p)/\sqrt{h\ell}\right)^2 - 4N = (hs - \ell p)^2/(h\ell)$ is at most 12.5 against $4N = 86{,}932$. This is why continued-fraction convergents give the rational-direction families nearest the envelope.

3.2. Envelope Bounds for Fixed mn

Fix $u = mn$ and consider the range of admissible values of $\Delta = ms + np$.

For fixed $u = mn$, each admissible divisor $m \mid u$ gives

$$\Delta_u(m) = sm + \frac{u}{m}p,$$

and the admissible values of Δ form the discrete set

$$\mathcal{D}(u) = \left\{\Delta_u(m) : m \mid u,\ 1 \le m \le p-1,\ 1 \le \frac{u}{m} \le s-1\right\}.$$

By (9), every element satisfies $\Delta \ge 2\sqrt{Nu}$, with the continuous minimum attained at $m^* = \sqrt{up/s}$, $n^* = \sqrt{us/p}$.

Elementary Endpoint Bound

For $1 \le u \le s-1$, the convexity of $\Delta_u(m) = sm + up/m$ on $1 \le m \le u$ places the maximum at an endpoint. Since $\Delta_u(1) = s + up$, $\Delta_u(u) = us + p$, and $(s + up) - (us + p) = (u-1)(p-s) \ge 0$, one has $\Delta_{\max}(u) = s + up$.

Thus the vertical fibers mentioned above are exactly the finite sets $\mathcal{D}(u)$, indexed by the admissible divisors of u.

4. Additional Curve Families in the (mn, Δ) Diagram

We now consider two additional families obtained from linear constraints on (m, n).

4.1. Family A: Constant $m + n$

Let $\lambda \geq 2$ be an integer and consider all admissible pairs (m, n) satisfying

$$m + n = \lambda.$$

Then, writing $n = \lambda - m$, one obtains

$$x = m(\lambda - m) = \lambda m - m^2$$

and

$$\Delta = ms + np = ms + (\lambda - m)p = m(s - p) + \lambda p.$$

Thus, for fixed λ, the quantity $x = mn$ depends quadratically on m, while Δ depends linearly on m. Solving the second relation for m, we get

$$m = \frac{\Delta - \lambda p}{s - p},$$

and substituting into $x = \lambda m - m^2$ yields

$$x = \lambda \frac{\Delta - \lambda p}{s - p} - \left(\frac{\Delta - \lambda p}{s - p}\right)^2.$$

Equivalently,

$$(s - p)^2 x = \lambda(\Delta - \lambda p)(s - p) - (\Delta - \lambda p)^2.$$

This is a quadratic relation between x and Δ, so for each fixed value of λ, the corresponding points in the (mn, Δ)-plane lie on a discrete arc of a conic section.

4.2. Family B: Constant $Am + Bn$

Fix coprime positive integers A, B with $A < p$ and $B < s$, and define

$$S_\lambda = \{(m, n) \in \mathcal{A}_{s,p} : Am + Bn = \lambda\}.$$

Theorem 1 (Structure of bounded affine slices)**.** *The nonempty slices S_λ have the following properties.*

(i) *In (Δ, δ) coordinates, S_λ lies on*

$$(Ap + Bs)\Delta + (Ap - Bs)\delta = 2N\lambda. \tag{16}$$

Thus the slices form a parallel line pencil, whose images under $mn = (\Delta^2 - \delta^2)/(4N)$ are conic arcs in the (mn, Δ) plane.

(ii) *For every integer λ, set*

$$n_{\min} = \max\left(1, \left\lceil \frac{\lambda - A(p-1)}{B} \right\rceil\right), \qquad n_{\max} = \min\left(s - 1, \left\lfloor \frac{\lambda - A}{B} \right\rfloor\right),$$

choose n_0 *with* $Bn_0 \equiv \lambda \pmod{A}$, *and define*

$$q_{A,B}(\lambda) = \max\left(0, \left\lfloor \frac{n_{\max} - n_0}{A} \right\rfloor - \left\lceil \frac{n_{\min} - n_0}{A} \right\rceil + 1\right). \tag{17}$$

Then

$$|S_\lambda| = q_{A,B}(\lambda), \qquad \Lambda_{A,B} = \{\lambda \in \mathbb{Z} : q_{A,B}(\lambda) > 0\}, \tag{18}$$

and

$$|\Lambda_{A,B}| \le A(p-2) + B(s-2) + 1. \tag{19}$$

(iii) *The complement map* $C(m,n) = (p-m, s-n)$ *satisfies*

$$C(S_\lambda) = S_{Ap+Bs-\lambda}, \qquad (\Delta, \delta) \mapsto (2N - \Delta, -\delta).$$

In particular, $|S_\lambda| = |S_{Ap+Bs-\lambda}|$.

(iv) *The underlying continuous conic has the vertex*

$$m^* = \frac{\lambda}{2A}, \qquad x^* = mn = \frac{\lambda^2}{4AB}, \qquad \delta^* = \frac{\lambda(Bs - Ap)}{2AB}.$$

Its segment inside the continuous rectangle $[1, p-1] \times [1, s-1]$ *contains this vertex if and only if*

$$1 \le \frac{\lambda}{2A} \le p - 1, \qquad 1 \le \frac{\lambda}{2B} \le s - 1.$$

The continuous extensions of consecutive slices satisfy

$$\delta(\lambda+1) - \delta(\lambda)\big|_m = -\frac{p}{B}, \tag{20}$$

and

$$x(\lambda+1, \delta) - x(\lambda, \delta) = \frac{\delta(Bs - Ap) + ps(2\lambda+1)}{(Bs + Ap)^2}. \tag{21}$$

Proof. The inverse formulas

$$m = \frac{\Delta + \delta}{2s}, \qquad n = \frac{\Delta - \delta}{2p}$$

transform $Am + Bn = \lambda$ into (16). The identity $\Delta^2 - \delta^2 = 4Nmn$ then gives the conic image.

The extreme values of $Am + Bn$ on the admissible rectangle are $A + B$ and $A(p-1) + B(s-1)$, which gives (19). For fixed λ, the box bounds applied to $n = (\lambda - Am)/B$ give $n_{\min}$ and $n_{\max}$, while the integrality of m is equivalent to $Bn \equiv \lambda \pmod{A}$. The coprimality of A and B leaves one residue class modulo A, whose elements in the bounded interval are counted by $q_{A,B}(\lambda)$. Consequently, the slice is nonempty exactly when this count is positive, proving (18).

Direct substitution proves the assertions for C. For the remaining formulas, parameterize a slice by

$$x = \frac{\lambda m - Am^2}{B}, \qquad \delta = \frac{m(Bs + Ap) - \lambda p}{B}.$$

The first expression has its continuous maximum at $m = \lambda/(2A)$, which gives x^* and δ^*. At that parameter value, $n = \lambda/(2B)$, so the two displayed box conditions are necessary and sufficient for the bounded continuous segment to contain the vertex. The second expression gives (20) for the continuous extensions. At fixed δ,

$$m = \frac{B\delta + \lambda p}{Bs + Ap}, \qquad n = \frac{\lambda s - A\delta}{Bs + Ap},$$

so

$$x(\lambda, \delta) = \frac{(B\delta + \lambda p)(\lambda s - A\delta)}{(Bs + Ap)^2}.$$

Taking the difference at $\lambda + 1$ proves (21). $\square$

Example: $A = 1$, $B = 2$

For $s = 103$ and $p = 211$, the integers $\lambda \in [3, 414]$ give 412 nonempty slices, with maximum cardinality 102. Consecutive solutions differ by $(m, n) \mapsto (m + 2, n - 1)$, so Δ changes by $2s - p = -5$; the same coefficient gives $\delta^* = -5\lambda/4$. Figures 3 and 4 show local and global views.

The equation $Am + Bn = \lambda$ is a bounded linear Diophantine problem. Its point count is a two-dimensional instance of lattice-point enumeration in rational polytopes [9].

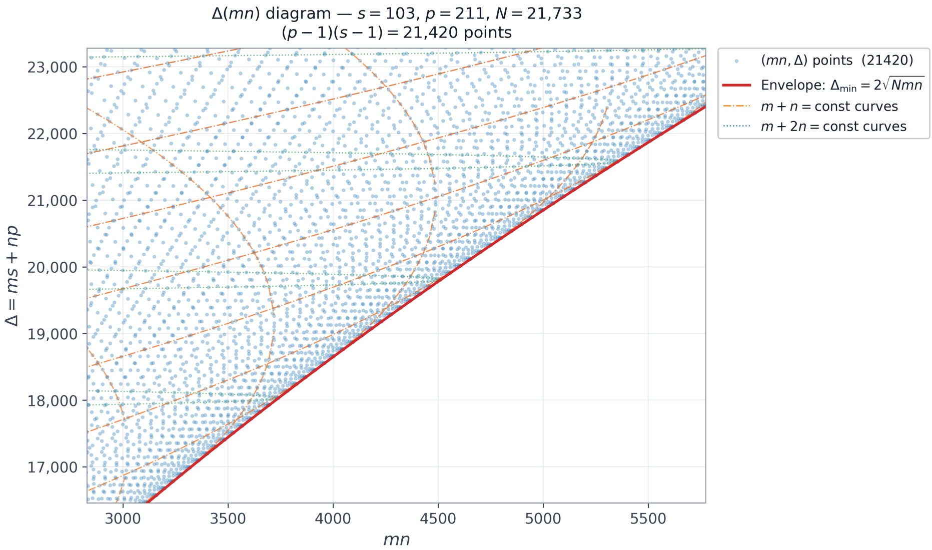

Figure 3. Local view of Families A and B in the (mn, Δ) plane. The continuous conics are the exact images of the displayed affine slices, and the red curve is $\Delta_{\min} = 2\sqrt{Nmn}$. This local view confirms that the bounded affine constraints produce discrete conic arcs rather than unrelated curve families, with all admissible points remaining above the common envelope.

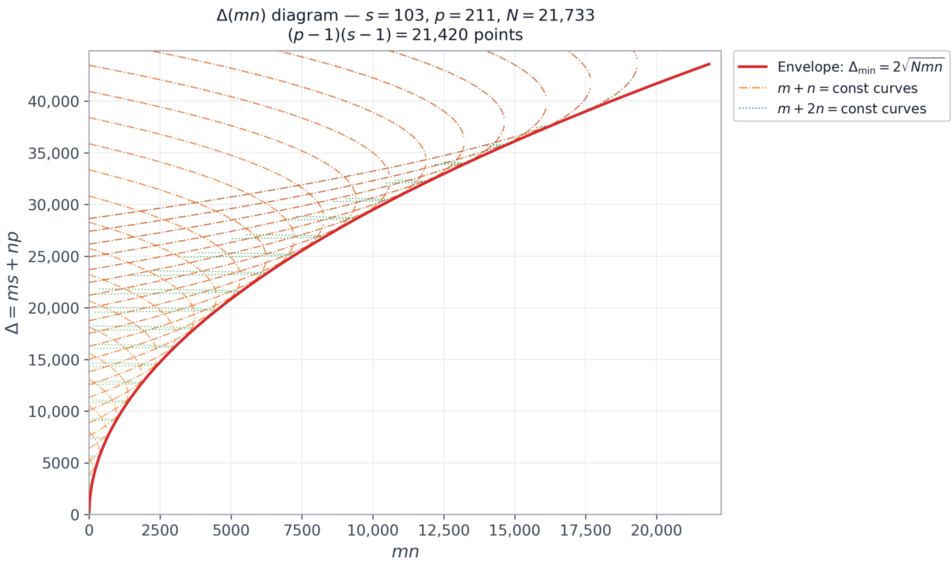

Figure 4. Global view of the affine-slice pencil over its full λ-range. The red parabola is $\Delta_{\min} = 2\sqrt{Nmn}$; the density of the conic arcs increases from the boundary toward the central slices.

https://doi.org/10.3390/sym18081291

5. Geometric Structure in the (mn, δ) Plane

The second product projection sends each admissible pair (m, n) to (mn, δ).

For fixed m, substituting $n = x/m$ into $\delta = ms - np$ gives $\delta = -(p/m) \cdot x + ms$, a line of slope $-p/m$ and intercept $+ms$. For fixed n, one obtains $\delta = (s/n) \cdot x - np$, a line of slope $+s/n$ and intercept $-np$. Compared with the dual families (10)–(12), the slopes are the same in magnitude but the signs are reversed: constant-m lines have negative slopes here (positive in the Δ diagram), and constant-n lines have positive slopes (also positive there). Points near $\delta = 0$ correspond to pairs satisfying $ms \approx np$, or equivalently $m/n \approx p/s$. Figure 5 shows these lines.

The rational-direction families $(jh, j\ell)$ of (14) also appear in this diagram. Substituting $(m, n) = (jh, j\ell)$ into $\delta = ms - np$ gives

$$\delta \;=\; \frac{hs - \ell p}{\sqrt{h\ell}} \cdot \sqrt{mn}, \tag{22}$$

a parabola with coefficient $(hs - \ell p)/\sqrt{h\ell}$. In contrast to the Δ diagram where the coefficient $(hs + \ell p)/\sqrt{h\ell}$ is always positive, here the coefficient is negative when $h/\ell < p/s$, positive when $h/\ell > p/s$, and zero when $h/\ell = p/s$. Families associated with convergents of p/s therefore lie close to the mn-axis.

Section 6 writes the Δ and δ projections in the common coordinates (ms, np).

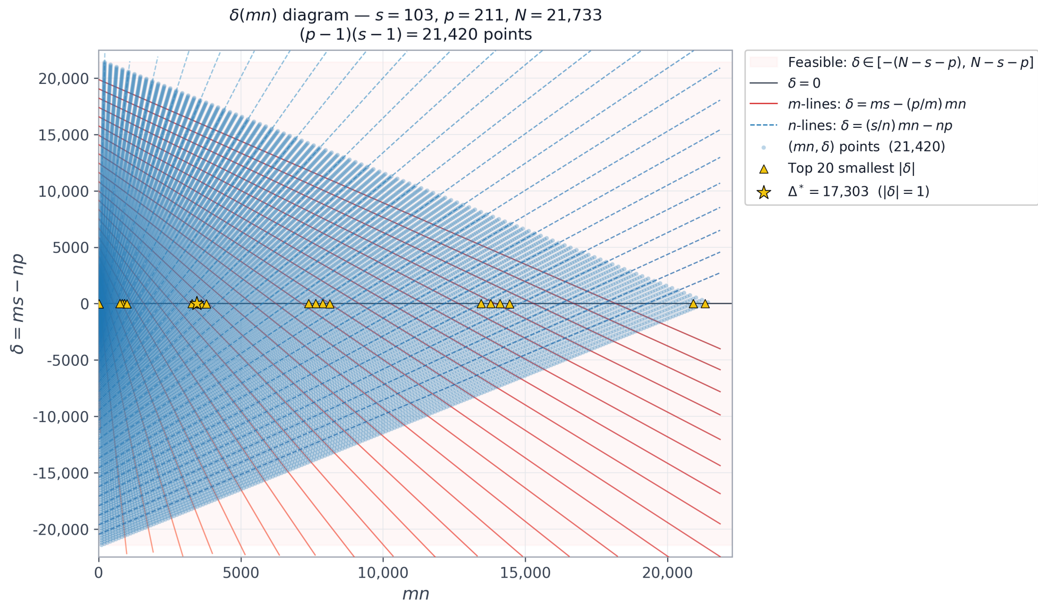

Figure 5. The $\delta(mn)$ diagram for $s = 103$, $p = 211$, with mn on the horizontal axis. Selected negative-slope lines correspond to constant m, and selected positive-slope lines correspond to constant n. Yellow triangles mark the 20 admissible points with the smallest $|\delta|$, corresponding to pairs (m, n) with $m/n \approx p/s$. The yellow star marks the special lifted value $\Delta^* = 17{,}303$, where $|\delta| = 1$ (Section 8.3). The shaded region is the exact range $\delta \in [-(N - s - p),\, N - s - p]$. The sign of δ records the side of $ms = np$, while $\Delta^2 - 4Nmn = \delta^2$ quantifies the departure from the envelope; the marked $|\delta| = 1$ point is the closest possible lattice approach.

6. The (ms, np) Plane

With $u = ms$ and $v = np$, the $\Delta(mn)$ and $\delta(mn)$ diagrams are projections $(u, v) \mapsto (uv/N, u + v)$ and $(u, v) \mapsto (uv/N, u - v)$ respectively.

Elementary Rectangular-Lattice Description

In coordinates $u = ms$ and $v = np$:

(a) Data points form a rectangular lattice with horizontal spacing s and vertical spacing p.
(b) Curves of constant mn are hyperbolas $uv = Nmn$.
(c) The vertex of the hyperbola $uv = Nmn$ lies on the diagonal $u = v$ at $u = v = \sqrt{Nmn}$, with $\Delta = 2\sqrt{Nmn}$ (the parabolic envelope value).

Indeed, u and v range through $\{s, 2s, \ldots, (p-1)s\}$ and $\{p, 2p, \ldots, (s-1)p\}$, while $uv = spmn = Nmn$; the vertex statement follows by setting $u = v$.

For fixed mn, the continuous hyperbola $uv = Nmn$ is invariant under $u \leftrightarrow v$ and has the diagonal $u = v$ as an axis of symmetry in the positive quadrant. The labeled rectangular lattice has spacings s and p, so for $s \neq p$, the reflected point need not belong to that same lattice.

Figure 6 illustrates this lattice, the diagonal $u = v$, and selected level hyperbolas $uv = Nmn$.

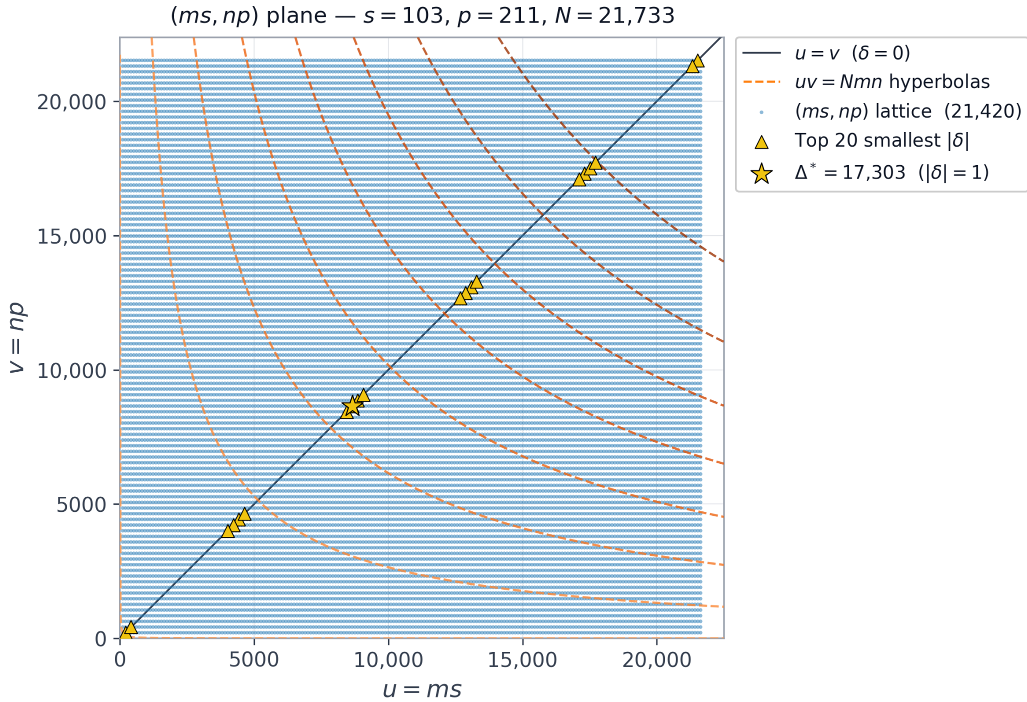

Figure 6. The (ms, np) plane for $s = 103$, $p = 211$, $N = 21{,}733$. The blue dots form a rectangular lattice with horizontal spacing s and vertical spacing p. The gray diagonal corresponds to $u = v$, which is the locus $\delta = 0$. The dashed orange curves are hyperbolas $uv = Nmn$ for selected values of mn. Points near the diagonal have small $|\delta|$, corresponding to pairs (m, n) with $m/n \approx p/s$. Yellow triangles mark the 20 admissible points with the smallest $|\delta|$, and the yellow star marks the special lifted value $\Delta^* = 17{,}303$, for which $|\delta| = 1$. Thus the continuous hyperbola has diagonal symmetry, although exchanging the coordinates also exchanges the unequal lattice spacings s and p.

7. Squaring Orbits: Branch Lines and Reciprocal Hyperbolas

Let

$$T(b) = b^2 \bmod N, \qquad b_0, b_1, b_2, \ldots$$

be the squaring orbit modulo $N = sp$. For each non-degenerate orbit point, write its Bézout decomposition as

$$\Delta_i = m_i s + n_i p = b_i + \kappa_i N, \qquad M_i = m_i n_i.$$

For every root of unity $r^2 \equiv 1 \pmod{N}$,

$$T(rb) = (rb)^2 \equiv b^2 = T(b) \pmod{N}.$$

A product of two distinct odd primes has four such roots [6,7]. The theorem below writes the standard CRT product decomposition of modular squaring [1] in Bézout coordinates and relates these fourfold fibers to the complement symmetry of Theorem 1.

We use two vertical coordinates for the same horizontal coordinate Δ:

$$(\Delta, M) = (\Delta, mn), \qquad (\Delta, Y) = \left(\Delta, \frac{N}{mn}\right), \qquad Y = \frac{N}{M}.$$

The two views are related by the reciprocal change of vertical coordinate $Y = N/M$.

7.1. Independent Recursions of the Bézout Coordinates

Theorem 2 (Coordinate conjugacy and fourfold symmetry for modular squaring)**.** *Let $T(b) = b^2 \bmod N$ on $\mathbb{Z}_N^\times$, and let $\langle x\rangle_q$ denote the canonical representative of a nonzero residue modulo q. Define*

$$F_{s,p}(m,n) = \left(\langle sm^2\rangle_p, \langle pn^2\rangle_s\right) \qquad ((m,n) \in \mathcal{A}_{s,p}).$$

Then the bijection of Proposition 2 conjugates the two finite dynamical systems:

$$\Phi_{s,p} \circ T = F_{s,p} \circ \Phi_{s,p}. \tag{23}$$

Equivalently, if $b_{i+1} \equiv b_i^2 \pmod N$ and $(m_i, n_i) = \Phi_{s,p}(b_i)$, then

$$m_{i+1} \equiv sm_i^2 \pmod p, \qquad n_{i+1} \equiv pn_i^2 \pmod s. \tag{24}$$

Thus, the two coordinates evolve under the independent maps

$$\mu(x) = sx^2 \bmod p, \qquad \nu(x) = px^2 \bmod s.$$

If the coordinate orbits have tail lengths τ_m, τ_n and eventual periods ℓ_m, ℓ_n, then the Bézout-coordinate orbit has

$$\tau = \max(\tau_m, \tau_n), \qquad \ell = \operatorname{lcm}(\ell_m, \ell_n).$$

Moreover, define the coordinate reflections

$$R_p(m,n) = (p-m, n), \qquad R_s(m,n) = (m, s-n), \qquad C = R_pR_s.$$

Together with the identity, they form a Klein four-group K, and

$$F_{s,p} \circ R = F_{s,p} \qquad (R \in K). \tag{25}$$

For every $y \in \operatorname{im}(F_{s,p})$, the fiber $F_{s,p}^{-1}(y)$ is one K-orbit and has four elements. In particular, if $L_{A,B}(m,n) = Am + Bn$, then

$$L_{A,B}(C(m,n)) = Ap + Bs - L_{A,B}(m,n), \qquad F_{s,p}(C(m,n)) = F_{s,p}(m,n). \tag{26}$$

Thus the central reflection exchanges the paired slices S_λ and $S_{Ap+Bs-\lambda}$, while paired points coalesce after one squaring step.

Proof. From $m_i \equiv -cb_i \pmod p$ and $b_{i+1} \equiv b_i^2 \pmod p$,

$$m_{i+1} \equiv -cb_i^2 \pmod p.$$

Since $b_i \equiv m_i s \pmod p$,

$$m_{i+1} \equiv -cm_i^2 s^2 \pmod p.$$

Using $-cs \equiv 1 \pmod{p}$, we obtain

$$m_{i+1} \equiv sm_i^2 \pmod{p}.$$

The proof for n_i is symmetric, using $n_i \equiv db_i \pmod{s}$, $b_i \equiv n_i p \pmod{s}$, and $dp \equiv 1 \pmod{s}$. Since $\Phi_{s,p}$ is bijective, the two recursions give the conjugacy (23). A product orbit enters its eventual cycle when both coordinate orbits have entered theirs, giving the maximum tail length; it returns precisely after a multiple of both coordinate periods, giving their least common multiple.

Each component of $F_{s,p}$ depends only on the square of its coordinate, so replacing m with $p-m$, replacing n with $s-n$, or making both replacements leaves the image unchanged. This proves (25). Conversely, over each odd prime, a nonzero value in the image of a scaled squaring map has exactly two preimages, related by sign. Hence every nonempty product fiber consists of the four displayed reflections and has cardinality four. Under $\Phi_{s,p}^{-1}$ these reflections are precisely multiplication by the four square roots of unity modulo N. Finally, the first identity in (26) follows by direct substitution, and the second is the case $R = C$ of (25); together they give the stated link between complementary slices and the dynamics. $\square$

7.2. Branch Lines in the (Δ, mn) Plane

Every non-degenerate point satisfies (8), so the curve $M = \Delta^2/(4N)$ is the upper parabolic envelope of the (Δ, M) diagram.

Fixing one Bézout coordinate gives a linear branch. From $\Delta = ms + np$, we get

$$M = \frac{m}{p}(\Delta - ms) \tag{27}$$

when m is fixed, and

$$M = \frac{n}{s}(\Delta - np) \tag{28}$$

when n is fixed. Thus the constant-coordinate branches in the (Δ, mn) view are affine lines, not hyperbolas; Figure 7 shows a squaring orbit together with several constant-n branch lines.

Relation with the Constant-Coordinate Lines

Equations (27) and (28) are obtained by solving (10) and (12) for the product coordinate; Theorem 2 determines which intersections of the two branch families are visited by a squaring orbit.

7.3. Reciprocal Hyperbolas in the $(\Delta, N/(mn))$ Plane

Setting $Y = N/M$, the two line families (27) and (28) become

$$Y_m(\Delta) = \frac{sp^2}{m(\Delta - ms)}, \tag{29}$$

$$Y_n(\Delta) = \frac{s^2 p}{n(\Delta - np)}. \tag{30}$$

These are genuine decreasing hyperbolas, with vertical asymptotes $\Delta = ms$ and $\Delta = np$. The asymptotes belong only to the reciprocal picture, not to the linear (Δ, mn) picture.

The upper envelope (8) transforms into

$$Y \geq \frac{4N^2}{\Delta^2}, \tag{31}$$

so the reciprocal diagram has a lower envelope. On logarithmic vertical scales, $\log Y = \log N - \log M$, so the two diagrams are vertical mirror images of each other around the horizontal level $\frac{1}{2}\log N$. Figure 8 shows the same orbit in this reciprocal view.

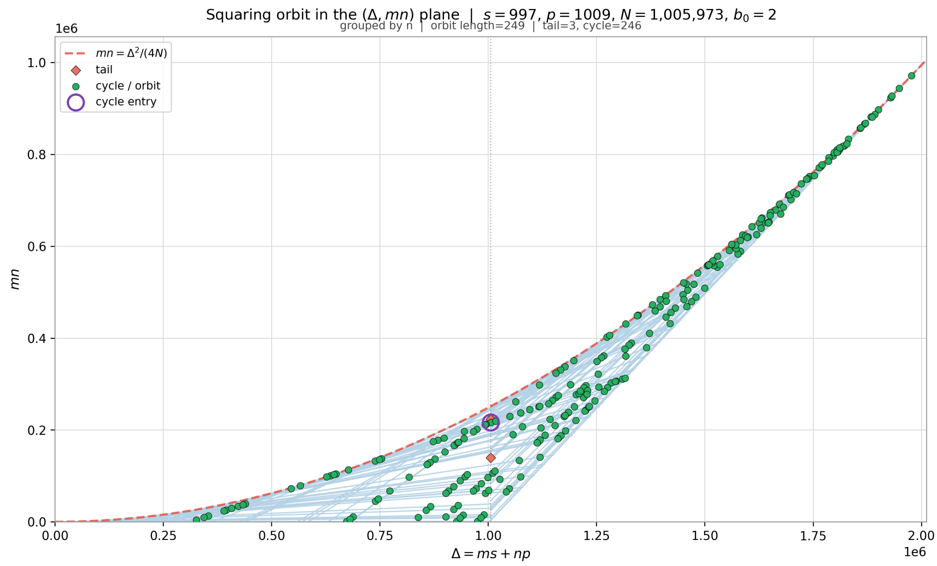

Figure 7. Squaring orbit in the (Δ, mn) plane for $s = 997$, $p = 1009$, $N = 1{,}005{,}973$, $b_0 = 2$ (orbit length 249, tail $\tau = 3$, cycle $\ell = 246$). The dashed red curve is $M = \Delta^2/(4N)$; the dotted vertical line marks $\Delta = N$. Blue lines show selected constant-n branch lines (28). No reciprocal curves $Y = N/M$ are shown in this figure. Red diamond: tail point; green circles: cycle points; purple circle: cycle entry. A single orbit selects a sparse dynamical subset of the admissible lattice, whose points remain on the constant-coordinate affine branches of the full diagram.

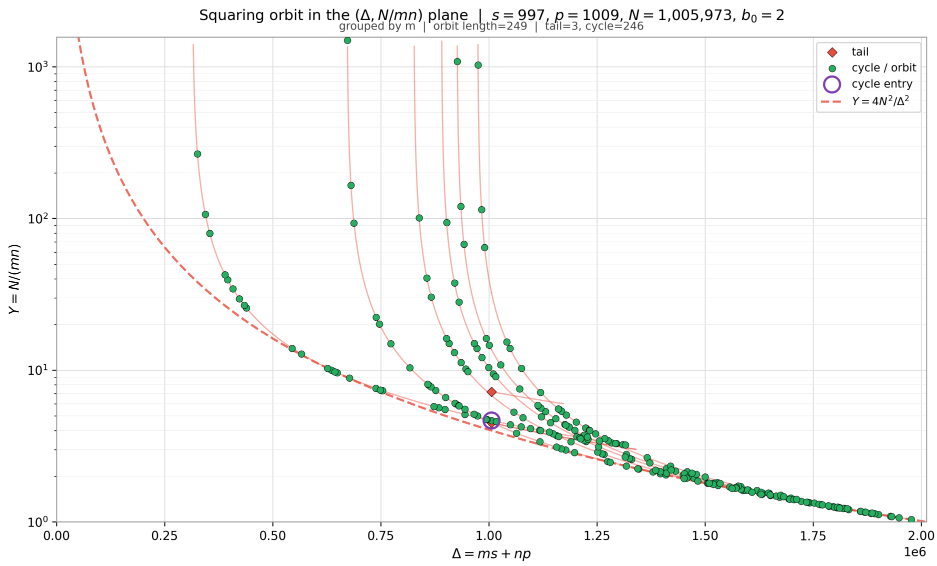

Figure 8. Reciprocal view of the same squaring orbit, $s = 997$, $p = 1009$, $N = 1{,}005{,}973$, $b_0 = 2$. The vertical coordinate is $Y = N/(mn)$ on a logarithmic scale. Red curves: constant-m hyperbolas (29); dashed red curve: lower envelope $Y = 4N^2/\Delta^2$. Red diamond: tail point; green circles: cycle points; purple circle: cycle entry. The transformation $Y = N/(mn)$ sends an affine branch to a decreasing hyperbola and changes the upper envelope in mn into the lower envelope $Y = 4N^2/\Delta^2$.

The figures in this section show only the points visited by one squaring orbit. The full (Δ, mn) diagram contains all admissible pairs (m, n), while the orbit selects only the pairs generated by (24). For large primes, the figures are clearer when only selected branch families are drawn and a logarithmic vertical scale is used.

8. Properties of δ

We collect here some basic properties of

$$\delta = ms - np$$

and of the special lifted value Δ^* with $|\delta| = 1$.

8.1. Range, Monotonicity, and Proximity to the Envelope

Proposition 3. *$\delta \in [-(N-s-p),\ N-s-p]$, a symmetric interval of width $2(N-s-p)$.*

Proof. From $\delta = ms - np$ with $1 \le m \le p-1$ and $1 \le n \le s-1$, the minimum is attained at $m = 1$, $n = s-1$, giving $\delta_{\min} = s - (s-1)p = -(N-s-p)$, and the maximum at $m = p-1$, $n = 1$, giving $\delta_{\max} = (p-1)s - p = N - s - p$. □

From $\Delta^2 - \delta^2 = 4Nmn$, for fixed Δ, the value of mn increases as $|\delta|$ decreases. At $|\delta| = 1$,

$$mn = \frac{\Delta^2 - 1}{4N}.$$

The distance to the envelope satisfies $\Delta - 2\sqrt{Nmn} \approx \delta^2/(4\sqrt{Nmn})$ for $|\delta| \ll \sqrt{Nmn}$.

8.2. Linear Variation Within a Branch

On any branch (interval of residues b without reduction modulo p or s), the Bézout coordinates satisfy

$$m(b+1) = m(b) - c, \qquad n(b+1) = n(b) + d,$$

giving $\Delta(b+1) - \Delta(b) = -cs + dp = 1$ by (1). Consequently,

$$\delta(b+1) - \delta(b) = -cs - dp = -(cs + dp),$$

so δ is affine in Δ along each branch:

$$\delta(\Delta) = \delta_0 - (cs + dp)(\Delta - \Delta_0). \tag{32}$$

8.3. The Special Value Δ^* with $|\delta| = 1$

The most important special case is obtained from admissible pairs (m, n) satisfying

$$|ms - np| = 1.$$

For such a pair, the lifted value

$$\Delta = ms + np$$

satisfies

$$\Delta^2 - 1 = \Delta^2 - (ms - np)^2 = 4Nmn.$$

Hence

$$\Delta^2 \equiv 1 \pmod{4N}.$$

Thus the residue class of such a lifted value is a square root of unity modulo $4N$.

The normalized Bézout pair (c, d) satisfies $-cs + dp = 1$, or equivalently $cs - dp = -1$. Thus the admissible pair (c, d) has $\delta = -1$. The complementary pair $(p - c, s - d)$ satisfies $(p - c)s - (s - d)p = -cs + dp = 1$, so it has $\delta = +1$. Both pairs are admissible, since $1 \le c \le p - 1$ and $1 \le d \le s - 1$ imply $1 \le p - c \le p - 1$ and $1 \le s - d \le s - 1$.

These are the only admissible pairs with $|\delta| = 1$. Indeed, if $ms - np = -1$, subtracting $cs - dp = -1$ gives $s(m - c) = p(n - d)$. Since $\gcd(s, p) = 1$, one has $m - c = tp$ and $n - d = ts$ for some $t \in \mathbb{Z}$; the canonical ranges force $t = 0$. The case $ms - np = 1$ is identical after comparison with $(p - c, s - d)$.

The two corresponding lifted values are

$$\Delta_- = cs + dp, \qquad \Delta_+ = (p - c)s + (s - d)p = 2N - (cs + dp).$$

We define

$$\Delta^* = \min(\Delta_-, \Delta_+), \qquad \Delta^{**} = \max(\Delta_-, \Delta_+) = 2N - \Delta^*.$$

Equivalently, (m^*, n^*) denotes the admissible pair among (c, d) and $(p - c, s - d)$ that gives the smaller lifted value $\Delta^* = m^*s + n^*p$.

The quantity Δ^* is the unique lifted value associated with the chosen admissible pair. Since $0 < \Delta^* < N$, reducing modulo N leaves it unchanged.

Both lifted values satisfy $\Delta^2 \equiv 1 \pmod{4N}$. Indeed,

$$(cs + dp)^2 - 1 = (cs + dp)^2 - (cs - dp)^2 = 4csdp = 4Ncd,$$

and

$$(2N - (cs + dp))^2 \equiv (cs + dp)^2 \equiv 1 \pmod{4N}.$$

The factorization is recovered directly. If $\delta = -1$, then

$$\gcd(\Delta - 1, N) = s, \qquad \gcd(\Delta + 1, N) = p,$$

whereas for $\delta = 1$ the two factors are interchanged. Thus each lifted value gives a non-trivial square root of unity and a factorization of N [10,11]; constructing it from the Bézout coefficients, however, already uses knowledge of s and p.

Example 1. *Table 1 lists the complementary lifted values determined above for several semiprimes.*

Table 1. Special lifted values Δ^* with $|m^*s - n^*p| = 1$ and their complements $\Delta^{**} = 2N - \Delta^*$, for several semiprimes $N = sp$.

s	p	m^*	n^*	Δ^*	Δ^{**}	N
11	13	6	5	131	155	143
17	19	9	8	305	341	323
101	103	51	50	10,301	10,505	10,403
997	1009	84	83	167,495	1,844,451	1,005,973
3803	7607	2	1	15,213	57,843,629	28,929,421

8.4. Distribution of $|\delta|$

Proposition 4 (Exact central count for δ)**.** *The map $(m, n) \mapsto \delta = ms - np$ is injective on $\mathcal{A}_{s,p}$. Moreover, for every integer T with $1 \le T \le p$,*

$$\#\{(m, n) \in \mathcal{A}_{s,p} : |ms - np| < T\} = 2\left(T - 1 - \left\lfloor \frac{T - 1}{s} \right\rfloor\right). \tag{33}$$

In particular, for $1 \le T \le s$ this number is exactly $2(T - 1)$.

Proof. If $ms - np = m's - n'p$, then $s(m - m') = p(n - n')$. Coprimality gives $m - m' = tp$ and $n - n' = ts$ for some $t \in \mathbb{Z}$, and the canonical ranges force $t = 0$. Hence the map is injective.

No admissible point has $\delta = 0$, because $ms = np$ would force $m = tp$ and $n = ts$ for some positive integer t. Now let $0 < k < p$. There is a unique $m \in \{1, \dots, p-1\}$ satisfying $ms \equiv k \pmod{p}$. Setting $n = (ms - k)/p$ gives an admissible integer $1 \le n \le s-1$ exactly when $s \nmid k$: if $s \mid k$, then $ms = k$ and $n = 0$; otherwise $ms - k$ is a nonzero multiple of p lying strictly between $-p$ and ps, and is therefore positive and at most $(s-1)p$. Thus the positive values $k < T$ that occur are precisely the integers $1 \le k \le T-1$ not divisible by s. The complement map changes the sign of δ, so the same number of negative values occurs. Counting these integers proves (33). $\square$

The formula proves the observed local density once the factorization is fixed. Locating the corresponding coordinates from N alone still requires the unknown split, so it does not give a factorization method.

9. Conclusions

The normalized CRT–Bézout map places the admissible pairs in a finite rectangle, and the diagrams considered in the paper are projections of this set. Theorem 1 describes the bounded slices $Am + Bn = \lambda$, while Theorem 2 gives the coordinate form of modular squaring and its fourfold fibers. The complement of a slice is compatible with the squaring map. The two points with $|ms - np| = 1$ give non-trivial square roots of unity, and Proposition 4 counts the points in the central strip $|\delta| < T$.

Let $L = \lceil \log_2 N \rceil$. If the factors are known, one coordinate pair is computable in time polynomial in L, but the full diagram contains $(p-1)(s-1) = \Theta(N)$ points. From N alone, constructing the special point is tied to finding a non-trivial modular square root and hence to factorization [12]. For comparison, Pollard's rho method has expected order $O(N^{1/4})$ for a balanced semiprime [13]; the number field sieve is the standard classical asymptotic benchmark [14], and Shor's algorithm is polynomial on a quantum computer [15]. Fermat's difference-of-squares construction corresponds here to $m = n = 1$. Thus the diagrams do not improve factorization complexity, although they give checks and examples for CRT coordinates, Diophantine equations, and modular-squaring orbits.

The identity $\Delta^2 - \delta^2 = 4Nmn$ also holds for a coprime split $N = uv$. If one part is composite, however, the unit coordinates run only through the corresponding reduced residue classes, so the full rectangular-lattice and affine-slice statements do not extend unchanged. For an odd squarefree product $N = p_1 \cdots p_r$, the 2^r CRT sign vectors describe the square roots of unity and complementary factor splits. A genuinely r-dimensional geometric model remains open.

Further questions include global distribution estimates for the Bézout point clouds and Ehrhart-type or higher-dimensional extensions of the affine-slice counts. The conics considered here are not modular curves in the algebro-geometric sense, and no such interpretation is claimed.

Author Contributions: Conceptualization, N.V.; Methodology, N.V. and C.G.; Software, N.V. and C.G.; Validation, N.V. and C.G.; Formal analysis, N.V.; Investigation, N.V.; Writing – original draft, N.V.; Writing – review and editing, C.G.; Visualization, N.V.; Supervision, C.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. DeVille, L. The Shape of x^2 mod n. *arXiv* **2022**, arXiv:2207.10512.
2. Eichhorn, D.; Khan, M.R.; Stein, A.H.; Yankov, C.L. Sums and Differences of the Coordinates of Points on Modular Hyperbolas. In *Combinatorial Number Theory: Proceedings of the "Integers Conference 2007"*; Landman, B., Nathanson, M.B., Nešetřil, J., Nowakowski, R.J., Pomerance, C., Robertson, A., Eds.; de Gruyter: Berlin, Germany, 2009; pp. 17–39.
3. Shparlinski, I.E. Modular Hyperbolas. *arXiv* **2011**, arXiv:1103.2879.
4. Shparlinski, I.E. Primitive Points on a Modular Hyperbola. *Bull. Pol. Acad. Sci. Math.* **2006**, *54*, 193–200. [CrossRef]
5. Bower, A.; Evans, R.; Luo, V.; Miller, S.J. Coordinate Sum and Difference Sets of d-Dimensional Modular Hyperbolas. *Integers* **2013**, *13*, #A31.
6. Verykios, N.; Gogos, C. Structures of Finite Fields of Primes and the Euclidean Square Roots of Unity in the Finite Rings. *Cryptogr. Commun.* **2025**, *17*, 41–55. [CrossRef]
7. Finch, S.; Martin, G.; Sebah, P. Roots of Unity and Nullity Modulo n. *Proc. Am. Math. Soc.* **2010**, *138*, 2729–2743. [CrossRef]
8. Hardy, G.H.; Wright, E.M. *An Introduction to the Theory of Numbers*, 6th ed.; Oxford University Press: Oxford, UK, 2008.
9. Beck, M.; Diaz, R.; Robins, S. The Frobenius Problem, Rational Polytopes, and Fourier–Dedekind Sums. *J. Number Theory* **2002**, *96*, 1–21. [CrossRef]
10. Miller, G.L. Riemann's Hypothesis and Tests for Primality. *J. Comput. Syst. Sci.* **1976**, *13*, 300–317. [CrossRef]
11. Rabin, M.O. Probabilistic Algorithm for Testing Primality. *J. Number Theory* **1980**, *12*, 128–138. [CrossRef]
12. Jeřábek, E. Integer Factoring and Modular Square Roots. *J. Comput. Syst. Sci.* **2016**, *82*, 380–394. [CrossRef]
13. Pollard, J.M. A Monte Carlo Method for Factorization. *BIT Numer. Math.* **1975**, *15*, 331–334. [CrossRef]
14. Buhler, J.P.; Lenstra, H.W., Jr.; Pomerance, C. Factoring Integers with the Number Field Sieve. In *The Development of the Number Field Sieve*; Lecture Notes in Mathematics; Springer: Berlin/Heidelberg, Germany, 1993; Volume 1554, pp. 50–94. [CrossRef]
15. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]