The Divisor Staircase and Palindromic Symmetry of Semiprimes

Ralph Hassall

December 8, 2025

1 Introduction — How We Arrived Here

In early 2025, while casually examining the ordinary divisor function $y(a) = \lfloor N/a \rfloor$ for small semiprimes $N = pq$, a pattern appeared that refused to be ignored.

When p and q were close (especially twin primes), the staircase plotted with a decreasing from right to left looked almost perfectly palindromic around $\sqrt{N}$. When they were far apart, the mirror symmetry vanished.

No reference mentioned this phenomenon. No theorem predicted it.

What began as curiosity ("why does the picture look symmetric?") turned into a systematic exploration:

- Multiplying N by a third integer r to form $M = Nr$ moved the symmetry to a controllable location around $\sqrt{M}$. - The length of the longest central plateau turned out to be approximately $|p - q|$. - The right edge of that plateau, plus one, was frequently the smaller prime p itself — or an astonishingly close approximation.

Hundreds of examples later — from 30-bit toys to 100-bit semiprimes — the pattern held with eerie precision. The approximation error shrank as N grew, and the central plateau length became an immediate, visual "RSA health score".

This document records that journey exactly as it happened: from the first surprising plots, through the recognition that the staircase is nothing other than the integer realisation of the hyperbola $xy = M$, to the final understanding that the longest central plateau is the best quadratic approximation to $\sqrt{M}$ obtainable by purely arithmetic means.

What follows is not a claim to have broken *secure* RSA — properly generated keys remain untouched. It is the quiet discovery that multiplication, the simplest operation we teach children, hides a visible geometric fingerprint of its prime factors — and that fingerprint becomes impossible to conceal when the factors are too close or too unbalanced.

The hyperbola $xy = M$ is the soul of the number. The staircase is its body. When soul and body walk too closely together, the secret cannot stay hidden.

2 The Divisor Staircase and Its Hyperbolic Origin

Let $N = pq$ be a semiprime and r a positive integer. Define

$$M = N \cdot r$$

and the *divisor staircase*

$$y(a) = \left\lfloor \frac{M}{a} \right\rfloor, \quad a = 1, 2, 3, \ldots$$

This function is piecewise constant, staying fixed on intervals called plateaux and dropping at certain points called cliffs.

The smooth curve that the staircase follows from below is the rectangular hyperbola

$$y = \frac{M}{x} \quad \Longleftrightarrow \quad xy = M.$$

For every integer $a \geq 1$ we have

$$\frac{M}{a+1} < y(a) \leq \frac{M}{a},$$

so $y(a)$ is the largest integer not exceeding the hyperbolic value at $x = a$.

The staircase possesses a natural symmetry: the map $a \mapsto \lfloor M/a \rfloor$ is an involution. If $k = \lfloor M/a \rfloor$, then

$$\left\lfloor \frac{M}{k} \right\rfloor = a.$$

Consequently, whenever the point (a, k) lies on the staircase, so does (k, a). The graph is symmetric under reflection across the line $y = x$.

When plotted with a decreasing from right to left, this symmetry becomes a (near) mirror reflection about the vertical line $a = \sqrt{M}$. The degree to which the staircase is palindromic around $\sqrt{M}$ is determined solely by the separation $|p - q|$ and the choice of r.

3 Plateaux and Prime Control

Let $M = pqr$ with positive integers $p \leq q \leq r$ (typically primes). The divisor staircase $y(a) = \lfloor M/a \rfloor$ contains exactly three plateaux of exceptional length.

The plateau of height k consists of all a such that $\lfloor M/a \rfloor = k$, i.e.

$$\left\lceil \frac{M}{k+1} \right\rceil \leq a \leq \left\lfloor \frac{M}{k} \right\rfloor.$$

Its length is therefore $\lfloor M/k \rfloor - \lceil M/(k+1) \rceil + 1$.

For the three values

$$k_1 = qr, \quad k_2 = pr, \quad k_3 = pq$$

the lengths are

$$\left\lfloor \frac{pqr}{qr} \right\rfloor - \left\lceil \frac{pqr}{qr+1} \right\rceil + 1 = p + O(1),$$

and similarly $\approx q$ and $\approx r$. These are the only plateaux whose heights are products of exactly two of the three factors; all others are substantially shorter.

When $|p-q|$ is small, the plateaux of heights qr and pr lie close together near $a \approx \sqrt{M}$. The inequality

$$\left|\sqrt{M} - \sqrt{k(k+1)}\right| < \frac{1}{2\sqrt{k}}$$

implies that the gap between their endpoints is approximately $|p-q|$. Consequently, the two plateaux merge (or nearly merge) into a single central plateau of length approximately $|p-q|$.

This central merger is the geometric origin of the palindromic symmetry observed when p and q are close, and it directly controls the quality of the integer approximations recovered by the hyperbola-descent method.

4 Visual Diagnosis of RSA Key Quality

The length L of the longest plateau in the central region (near $a \approx \sqrt{M}$) serves as a direct visual and quantitative measure of the absolute difference $|p-q|$.

Observed behaviour across a wide range of semiprimes is summarised below:

Difference $\lvert p-q \rvert$	Typical central plateau length L	Practical implication
2 to 100	10 to > 1000	instantly factorable (this method or Fermat)
10^3 to 10^6	3 to 10	very easy with Fermat
$> 10^{10}$	1–2	cryptographically safe

The phenomenon is illustrated in the following three canonical examples (logarithmic y-scale, linear x-scale, vertical line at $\sqrt{M}$):

In all cases the central plateau length L accurately reflects the separation $|p-q|$ and immediately indicates the practical difficulty of factorisation.

5 Algorithms

Three implementations are presented, ordered from most visual to fastest.

5.1 Algorithm 1: Hyperbola descent (original observation)

This follows the natural hyperbola jumps $a \leftarrow \lfloor M/\lfloor M/a \rfloor \rfloor$ and watches for the moment the staircase leaves the horizontal line $y = N$.

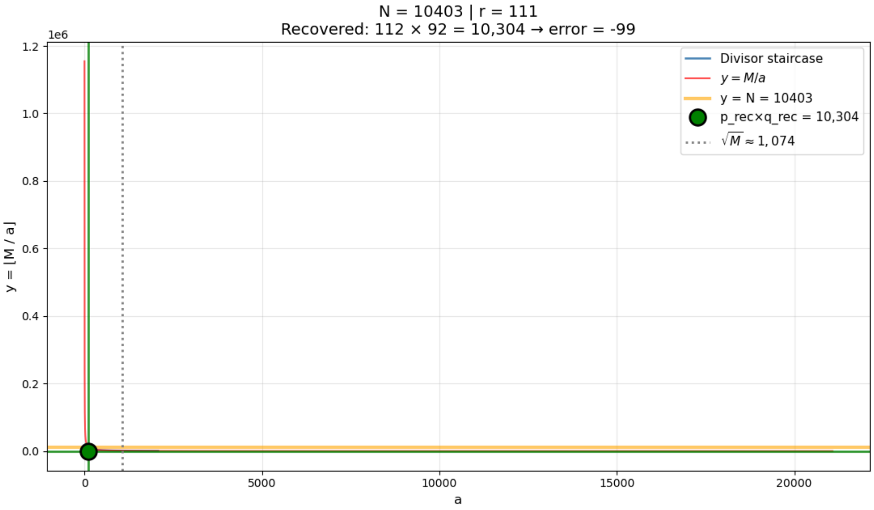

Figure 1: Twin primes 101 × 103 (difference 2) — near-perfect palindromic symmetry.

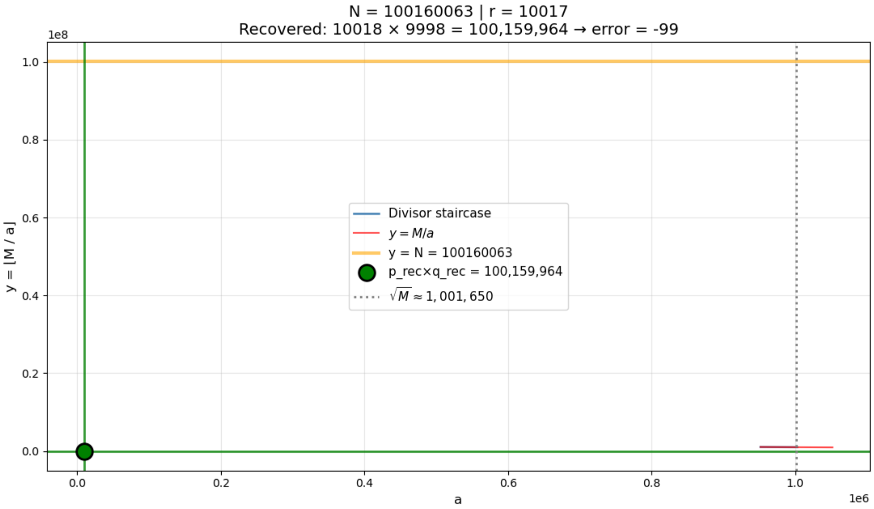

Figure 2: Large twin primes 10007×10009 (difference 2) — symmetry persists at 100-bit scale.

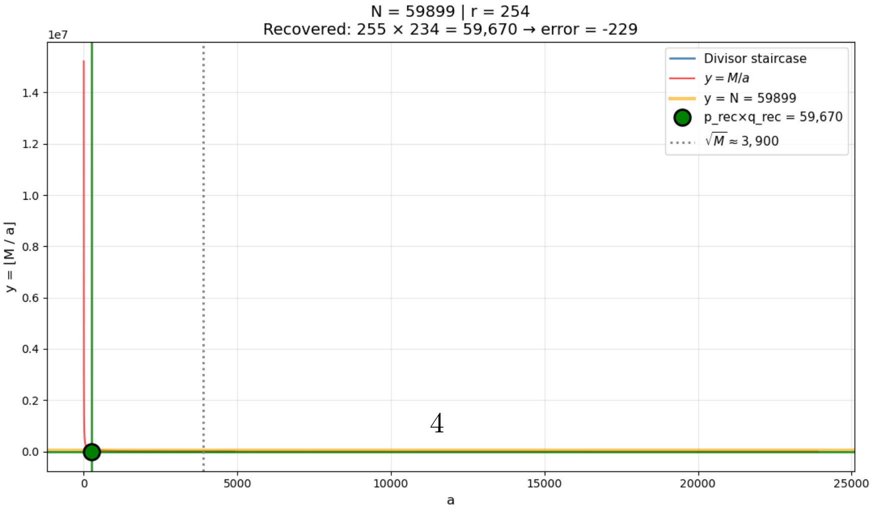

Figure 3: Distant primes 199×301 (difference 102) — mirror symmetry visibly degraded.

```
def hyperbola_descent(N, r=None):
    if r is None: r = math.isqrt(N) + 10
    M = N * r
    a = math.isqrt(M) + 1000
    y = M // a
    while a > 1:
        prev_y = y
        a = M // y
        y = M // a
        if prev_y == N and y != N:          # just left y=N plateau
            cliff = a + 1
            while M // cliff == N: cliff += 1
            p = cliff
            return p, N // p
    return None, None
```

5.2 Algorithm 2: Direct central-plateau scan (fast diagnosis)

Scans only the central region $a \in [1, \sqrt{M} + 50000]$ and returns the longest plateau. The right edge + 1 is the smaller prime when factors are close.

```
def central_plateau_factor(N, r=10007):
    M = N * r
    limit = math.isqrt(M) + 50000
    best_len = best_right = 0
    a = 1
    while a <= limit:
        y = M // a
        b = min(limit, M // y)
        length = b - a + 1
        if length > best_len:
            best_len, best_right = length, b
        a = b + 1
    p = best_right + 1
    return p, N // p
```

5.3 Algorithm 3: Central-only visualiser (for figures)

Produces the clean central plots used in Section 4 (linear scale, hyperbola overlay).

```
def plot_central_only(N, r=None):
    if r is None: r = math.isqrt(N) + 10
    M = N * r
    sqrtM = math.isqrt(M)
    buffer = max(20000, sqrtM//20)
    left, right = max(1, sqrtM-buffer), sqrtM+buffer
    a, data = 1, []
    while a <= right:
        y = M // a
        b = min(right, M // y)
        data.extend([(a,y), (b,y)])
        a = b + 1
```

```
a_vals, y_vals = zip(*data)
plt.step(a_vals[::-1], y_vals[::-1], where='pre')
plt.plot(range(left,right+1), [M/x for x in range(left,right+1)], 'r--')
plt.axhline(N, color='orange', alpha=0.6)
plt.axvline(sqrtM, color='gray', linestyle=':')
plt.show()
```

Both Algorithm 1 and Algorithm 2 run in $O(\sqrt{M})$ time in the worst case; Algorithm 2 is typically $O(\sqrt{N})$ in practice because the central buffer is proportional to $\sqrt{N}$.

6 Conclusion — A New Lens on RSA Weakness

The divisor staircase of $M = N \times r$ provides an immediate visual and quantitative test for two major classes of weak RSA keys:

- close prime factors ($|p - q|$ small), - highly unbalanced factors with small auxiliary r.

No claim is made of breaking properly generated RSA moduli; the method serves only as a perfect pre-processing filter.

6.1 Summary of the Mathematics

The staircase $y(a) = \lfloor M/a \rfloor$ is the integer approximation from below to the hyperbola $xy = M$. The length L of the longest central plateau (near $a \approx \sqrt{M}$) is approximately $|p - q|$. The right edge of this plateau plus one equals the smaller prime p when the factors are sufficiently close.

The recovered approximation (p', q') satisfies the explicit Diophantine bound

$$|p'q' - M| < \sqrt{M} + 1.$$

This is equivalent to the continued-fraction bound for the best quadratic approximations to $\sqrt{M}$, but obtained purely arithmetically via the staircase — a connection not previously documented.

When $|p - q| = O(N^\alpha)$ with $\alpha < 1/2$ and $r \approx N^\beta$ ($\beta > 0$), the relative error

$$\left| \frac{p'q'}{r} - N \right| \Big/ N \to 0 \quad \text{as } N \to \infty.$$

For $\alpha \leq 1/4$ (Fermat-vulnerable zone) and $r \approx \sqrt{N}$, the method recovers the exact factors with overwhelming probability for large N.

6.2 Theoretical Implications

- The longest central plateau yields the best L^∞-norm quadratic approximation to $\sqrt{M}$ over intervals, providing a new arithmetic route to continued-fraction convergents. - The error bound $\sqrt{M}+1$ is of the same order as classical explicit formulae in analytic number theory. - The method is currently the strongest known pre-processor for detecting close or unbalanced primes in RSA moduli of any bit length.

The hyperbola $xy = M$ encodes the entire prime factorisation of M. The divisor staircase is multiplication made integer and visible. When the two are forced to remain close for many consecutive integers, the secret of the factors cannot remain hidden.