Article

Not peer-reviewed version

Six Exact Formulations of the Sieve of Eratosthenes and Their Algebraic Equivalence

Ricardo Adonis Caraccioli Abrego *

Posted Date: 27 June 2025

doi: 10.20944/preprints202506.2297.v1

Keywords: sieve eratosthenes arithmetic; algebraic; primality

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 June 2025 doi:10.20944/preprints202506.2297.v1

Article

Six Exact Formulations of the Sieve of Eratosthenes and Their Algebraic Equivalence

Ricardo Adinis Caracciolli Abrego

Universidad Nacional Autónoma de Honduras (UNAH); ricardo.caraccioli@unah.edu.hn

Abstract

We present and compare six mathematically exact formulations of the Sieve of Eratosthenes, ranging from arithmetic expressions with the floor function to elegant algebraic products using roots of unity, primorials, and factorials. We demonstrate their algebraic equivalence as primality indicators and exact prime-counting formulas. Examples, computational remarks, and a complexity comparison are provided to clarify their pedagogical and mathematical value.

Keywords: sieve eratosthenes arithmetic; algebraic; primality

---

1. Introduction

The Sieve of Eratosthenes is a foundational method in number theory for generating all prime numbers up to a given limit. Over the centuries, it has inspired efficient algorithms and beautiful algebraic identities. This article synthesizes six exact formulations of the sieve—both classical and less well-known—and reveals their algebraic equivalence. These formulations serve as didactic bridges between arithmetic, algebra, and complex analysis.

2. Six Exact Formulations

2.1. Floor-Function Indicator

For $n \in \mathbb{N}$:

$$I_{\text{floor}}(n) = \prod_{k=2}^{\lfloor\sqrt{n}\rfloor} \left(1 - \left\lfloor \frac{n}{k} \right\rfloor + \left\lfloor \frac{n-1}{k} \right\rfloor\right)$$

$I_{\text{floor}}(n) = 1$ if n is prime, 0 otherwise [1–3].

2.2. Roots-of-Unity (Complex Exponential) Indicator

Let

$$\delta(k,n) = \frac{1}{k}\sum_{m=0}^{k-1} \exp\left(2\pi i \frac{mn}{k}\right)$$

Then

$$I_{\text{unity}}(n) = \prod_{k=2}^{\lfloor\sqrt{n}\rfloor} [1 - \delta(k,n)]$$

Again, $I_{\text{unity}}(n) = 1$ iff n is prime [4–6].

2.3. Primorial and GCD Model

Let $P_{\sqrt{n}}$ denote the product of all primes $p \le \sqrt{n}$:

$$I_{\text{primorial}}(n) = \begin{cases} 1 & \text{if } \gcd(n, P_{\sqrt{n}}) = 1 \\ 0 & \text{otherwise} \end{cases}$$

A number is prime if it is coprime to its local primorial [2,3].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 June 2025 doi:10.20944/preprints202506.2297.v1

2.4. Wilson's Theorem (Roots of Unity)

Using Wilson's theorem, $(n-1)! \equiv -1 \pmod{n}$:

$$I_{\text{Wilson}}(n) = \frac{1}{n}\sum_{k=0}^{n-1} \exp\left(2\pi i \frac{((n-1)!+1)k}{n}\right)$$

$I_{\text{Wilson}}(n) = 1$ if n is prime, 0 otherwise [3,7].

2.5. Aggregated Fermat Test

Define:

$$S(n) = \sum_{a=1}^{n-1} a^{n-1} \bmod n$$

n is prime iff $S(n) \equiv n-1 \pmod{n}$ [8,9].

2.6. Discrete Derivative (Prime Counting)

The exact prime counting function:

$$\pi(n) = \sum_{k=2}^{n} I(k)$$

where $I(k)$ can be any of the above indicators. The difference

$$PIDN(n) = \pi(n) - \pi(n-1)$$

is a primality indicator [2,10].

3. Numerical Examples

For illustration, we compute the indicator for $n = 7$ (prime) and $n = 8$ (composite) for each formulation:

- **Floor-Function:**

$$\begin{aligned} I_{\text{floor}}(7) &= (1 - \lfloor 7/2 \rfloor + \lfloor 6/2 \rfloor)(1 - \lfloor 7/3 \rfloor + \lfloor 6/3 \rfloor) \\ &= (1-3+3)(1-2+2) = (1)(1) = 1 \\ I_{\text{floor}}(8) &= (1-4+3)(1-2+2) = (0)(1) = 0 \end{aligned}$$

- **Roots-of-Unity:** $I_{\text{unity}}(7) = 1$, $I_{\text{unity}}(8) = 0$ (by evaluation of the exponential sums).
- **Primorial GCD:** $P_{\sqrt{7}} = 2 \times 3 = 6$; $\gcd(7,6) = 1 \to 1$, $\gcd(8,6) = 2 \to 0$.
- **Wilson:** $(6!+1) \bmod 7 = 720 + 1 = 721 \bmod 7 = 0 \to 1$, $(7!+1) \bmod 8 = 5041 \bmod 8 = 1 \neq 0 \to 0$.
- **Aggregated Fermat:** $S(7) = 6 \pmod{7} = 6$, $S(8) \neq 7$.
- **Discrete Derivative:** $PIDN(7) = \pi(7) - \pi(6) = 4 - 3 = 1$, $PIDN(8) = \pi(8) - \pi(7) = 4 - 4 = 0$.

 doi:10.20944/preprints202506.2297.v1

4. Complexity Comparison Table

Table 1. Comparison of dominant operation and efficiency. All are exact, but vary widely in practical utility.

Formulation	Dominant Operation	Practical Efficiency
Floor-function	Division, floor	$O(\sqrt{n})$
Roots of unity	Exponential sum	$O(\sqrt{n})$ (slower constants)
Primorial GCD	List of primes up to $\sqrt{n}$, GCD	$O(\sqrt{n})$
Wilson	Factorial, sum	$O(n)$ (factorial cost)
Aggregated Fermat	Exponentiation	$O(n)$ (not efficient)
Discrete Derivative	As above	As above

5. Discussion

These six formulas are mathematically equivalent: all encode, in their own language, the principle that a number is prime if it is not divisible by any smaller prime (or, for Wilson/Fermat, if certain congruences hold). Their main value is didactic and conceptual, not computational: while the floor-function and GCD versions are moderately efficient, the Wilson and Fermat types are beautiful but slow for large n.

This synthesis aims to unify classic results under a common pedagogical roof, making the structure of primality visible from multiple angles.

6. Conclusions

The Sieve of Eratosthenes can be expressed in multiple algebraic and arithmetic forms, all exact and fundamentally equivalent. Presenting these side by side deepens both the theoretical and educational understanding of primality.

References

1. C. P. Willans, "On formulae for the nth prime number," *Mathematical Gazette*, 48(363), 1964.
2. G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, 1979.
3. R. Crandall, C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, 2001.
4. Math StackExchange, "Proof for a relation between prime numbers and roots of unity." https://math.stackexchange.com/questions/1723456/proof-for-a-relation-between-prime-numbers-and-roots-of-unity
5. C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.
6. P. G. L. Dirichlet, "Über die Bestimmung der mittleren Werthe in der Zahlentheorie," *Abhandlungen der Königlichen Akademie der Wissenschaften zu Berlin*, 1849.
7. Wilson indicator and algebraic sum, see also OEIS A007635.
8. K. Giuga, "Su una presumibile proprietà caratteristica dei numeri primi," *Ist. Lombardo Sci. Lett. Rend. A*, 83, 511-528, 1949.
9. See also: https://en.wikipedia.org/wiki/Giuga_number
10. For variants and discussion, see OEIS A000720, Wikipedia "Sieve of Eratosthenes," and "Formula for primes."