Scientific Research Publishing

Advances in Pure Mathematics, 2026, 16(7), 431-434
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

Erratum to "Analysis of Multiplication Tables by Sum, Difference and Product: A New Approach to Primality" [Advances in Pure Mathematics (2025) 505-517]

Gnouma Jérôme Kadouno

Independent Researcher, Conakry, Guinea
Email: gnoumajkadouno3219@gmail.com

How to cite this paper: Kadouno, G.J. (2026) Erratum to "Analysis of Multiplication Tables by Sum, Difference and Product: A New Approach to Primality" [Advances in Pure Mathematics (2025) 505-517]. *Advances in Pure Mathematics*, **16**, 431-434.
https://doi.org/10.4236/apm.2026.167024

Received: June 8, 2026
Accepted: July 11, 2026
Published: July 14, 2026

The original online version of this article (Kadouno, G.J. (2025) Analysis of Multiplication Tables by Sum, Difference and Product: A New Approach to Primality. Advances in Pure Mathematics, 15, 505-517. https://doi.org/10.4236/apm.2025.158025) unfortunately contains mistakes in the primality test (Sections 6-9). The author wishes to correct the scope of the primality claim, replace one numerical example, and restate the logarithmic version as a sieve with a proven performance guarantee. Statements introduced in this erratum are labelled with the prefix E (Proposition E1, Theorem E1, ...) to distinguish them from those of the original article, to which we refer by their original numbers.

1. The First Test Condition Is Trivial

For every $n \geq 2$ and every $k \geq 1$, the tabular product satisfies $\Pi_T(k,n) = n^k k!$, hence $n \mid \Pi_T(k,n)$. The condition

$$\Pi_T(k,n) \equiv 0 \pmod{n}$$

therefore holds for all n and carries no information. The decision rests entirely on the second condition, $\gcd(n,k!) = 1$, equivalently $\gcd(n,k\#) = 1$. Theorems 3 and 4 should be restated with the first condition removed.

2. The Logarithmic Depth Does Not Yield a Primality Test

Proposition E1 (Validity threshold) *Let* $n \geq 2$, *let* $K \geq 1$ *be an integer and* $K\# = \prod_{p \leq K} p$ *the primorial* (*the product of the primes* $\leq K$). *The implication*

$$\gcd(n,K\#) = 1 \Rightarrow n \text{ prime}$$

holds whenever $K \geq \sqrt{n}$.

Proof. Sufficiency. If $K \geq \sqrt{n}$ and n is composite, its least prime factor p satisfies $p \leq \sqrt{n} \leq K$; thus $p \mid K\#$ and $p \mid n$, so $\gcd(n, K\#) \geq p > 1$. Contrapositively, $\gcd = 1$ forces n prime.

Sharpness. The critical case is the square of a prime. For $n = p^2$ the least prime factor is $p = \sqrt{n}$. If $K < \sqrt{n}$, no prime $\leq K$ divides n, so $\gcd(n, K\#) = 1$ while n is composite: the implication fails.

The adaptive depth is $k(n) = \lfloor C(n) \log_2 n \rfloor$ with $C(n) = 3 + \left\lfloor \frac{1}{3} \log_{10} n \right\rfloor$.

Since $C(n)$ is itself unbounded, growing like $\frac{1}{3} \log_{10} n$, one has $k(n) = \Theta\left((\log n)^2\right)$, which is still far below $\sqrt{n}$ for large n; the logarithmic version is therefore necessarily a sieve, not a test. Two explicit instances, both within the range the article claimed reliable:

- $n = 101^2 = 10201$: $C(n) = 4$, $k(n) = \lfloor 4 \log_2 10201 \rfloor = 53$. As $101 > 53$, $\gcd(10201, 53\#) = 1$, so the procedure returns *prime* for a perfect square.
- $n = 1000003 \times 1000033 = 1000036000099$: $C(n) = 7$, $k(n) = 279$. Both prime factors exceed 279, so $\gcd(n, 279\#) = 1$ and the procedure returns *prime* for a composite.

3. Correction of Example 5 (Section 9.2.3)

Example 5 (Section 9.2.3 of the original article) presents $n = 999999000001$ as composite, equal to $\left(10^6 + 1\right)\left(10^6 - 1\right)$ with factor 101×9901001. However

$$\left(10^6 + 1\right)\left(10^6 - 1\right) = 10^{12} - 1 = 999999999999,$$

which factors as $3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901$, while $101 \times 9901001 = 1000001101$; neither equals 999999000001, which is in fact prime.[1] The example should be replaced by a composite with a small prime factor, for instance $n = 10^{12} - 1$ above, whose factor 3 is detected at once.

4. Corrected Statement of the Criterion

Theorem E1 (Primality criterion by coprimality; replaces Theorems 3-4) *For $n \geq 2$, let $k = \lfloor \sqrt{n} \rfloor$. Then*

$$n \text{ prime} \iff \gcd(n, k\#) = 1.$$

Proof. By the argument of Proposition E1, with $K = \lfloor \sqrt{n} \rfloor$: the least prime factor p of a composite n satisfies $p \leq \sqrt{n}$, hence $p \leq \lfloor \sqrt{n} \rfloor = k$ since p is an integer. (Here the depth is the fixed value $k = \lfloor \sqrt{n} \rfloor$, in contrast with the adaptive depth $k(n)$ of Section 5.)

[1]Indeed $999999000001 = 10^{12} - 10^6 + 1 = \Phi_6\left(10^6\right)$, the sixth cyclotomic polynomial evaluated at 10^6; this identifies the structural form of the number and the source of the original confusion (with $10^{12} - 1$), while its primality itself is confirmed by direct computation.

Remark E1 (Status of the criterion) *Under the bound* $k=\lfloor\sqrt{n}\rfloor$ *the criterion is decision-equivalent to trial division up to* $\sqrt{n}$ *: it decides the same thing on every input, namely the existence of a prime factor* $\le\sqrt{n}$ *. It differs as a procedure—a reformulation of primality as coprimality,* n *prime* $\Leftrightarrow$ n *coprime to the product of the primes* $\le\sqrt{n}$ *: by the prime number theorem* [1] [2], $\log(k\#)=\vartheta(k)\sim k$ *, so* $k\#$ *has on the order of* $\sqrt{n}$ *bits. The contribution of this work is the proposed tabular framework and its associated reformulation.*

5. Revised Section 8: From Test to Sieve

Definition E1 (Logarithmic primorial sieve) *For* $n\ge 10$ *, let* $C(n)=3+\left\lfloor\frac{1}{3}\log_{10} n\right\rfloor$*, depth* $k(n)=\lfloor C(n)\log_2 n\rfloor$ *and* $k(n)\#=\prod_{p\le k(n)}p$ *.*

The sieve returns composite (certain) when $\gcd(n,k(n)\#)>1$ *; otherwise, when* $\gcd(n,k(n)\#)=1$ *, it reports no prime factor* $\le k(n)$ *—inconclusive as to primality. In particular* $\gcd(n,k(n)\#)=1$ *does not imply that* n *is prime. The restriction* $n\ge 10$ *is necessary: for* $n\le 9$ *the adaptive depth satisfies* $k(n)\ge n$ *, so the candidate* n *itself lies among the primes* $\le k(n)$ *; a prime* n *then divides* $k(n)\#$ *and is wrongly reported composite (this affects precisely the primes* $2,3,5,7$ *). These small cases are settled directly by the exact bound* $k=\lfloor\sqrt{n}\rfloor$ *of Theorem* E1*, for which* $k<n$ *, so no prime can be its own factor.*

Theorem E2 (Performance, via Mertens) *By Mertens' third theorem* [3]*, the density of integers with no prime factor* $\le y$ *is*

$$\prod_{p\le y}\left(1-\frac{1}{p}\right)=\frac{\mathrm{e}^{-\gamma}}{\ln y}\left(1+o(1)\right),$$

with $\gamma\approx 0.5772$. Here $C=C(n)=3+\left\lfloor\frac{1}{3}\log_{10} n\right\rfloor\sim\ln n/(3\ln 10)$, so

$$y=k(n)\sim C(n)\frac{\ln n}{\ln 2}\sim\frac{(\ln n)^2}{3\ln 2\ln 10},\quad \ln k(n)\sim 2\ln\ln n.$$

The surviving fraction is therefore

$$S(n)\approx\frac{\mathrm{e}^{-\gamma}}{\ln k(n)}\sim\frac{\mathrm{e}^{-\gamma}}{2\ln\ln n}\to 0\ \text{ as } n\to\infty.$$

Hence the eliminated fraction of composites tends to 1, while the residual $S(n)$ stays strictly positive for every finite n and decays like $1/\ln\ln n$. These two facts are inseparable: they make the procedure an asymptotically near-perfect filter and, at the same time, forbid it the status of a complete test. Numerical validation (uniform sampling per band) confirms the analysis:

band	depth $k(n)$	composites eliminated	survival $\mathrm{e}^{-\gamma}/\ln k(n)$
10^3	39	100.0%	15.3%
10^6	99	94.6%	12.2%
10^9	179	93.9%	10.8%
10^{12}	279	93.7%	10.0%

At the smallest band the depth already exceeds $\sqrt{n}$ ($k\left(10^3\right)=39>31.6\approx\sqrt{10^3}$), so there the sieve is locally complete and eliminates every composite; the asymptotic estimate $\mathrm{e}^{-\gamma}/\ln k(n)$, valid for large n, correspondingly overestimates the survival rate in this regime.

Blind set. The composites missed at depth $k(n)$ form

$$B(n)=\{m \text{ composite}: \text{all prime factors of } m \text{ are} > k(n)\},$$

dominated by the semiprimes $m=pq$ with $k(n)<p\le q$ and containing the squares p^2 with $p>k(n)$. The sieve is blind precisely on $B(n)$, and its cryptographically relevant core—the balanced semiprimes pq with both factors large—is exactly where factoring itself is hard; the perfect squares and the strongly unbalanced semiprimes it also misses are, by contrast, easy to factor.

Complete two-stage test. Hence the correct, efficient architecture: the logarithmic primorial sieve as a first stage (eliminating ≈94% of composites at negligible cost), followed by a completion test on the survivors—deterministic Miller-Rabin [4] below known bounds, or BPSW [5]. The sieve plays the legitimate role of a front-end filter; completeness comes from the modular stage. The depth $k(n)$ is tunable: a larger constant lowers the survivor count as $\mathrm{e}^{-\gamma}/\ln k(n)$, at the cost of a primorial of size $\mathrm{e}^{\vartheta(k)}$.

6. Results That Remain Valid

1) **The tabular framework.** The identities $\Sigma_{\mathrm{T}}(k,n)=nk(k+1)/2$, $\Delta_{\mathrm{T}}(a,b,n)=(b-a)n$ and $\Pi_{\mathrm{T}}(k,n)=n^k k!$ are exact and retain their unifying and pedagogical value.

2) **Carmichael numbers.** The rejection result (Theorem 5 of the original article) uses the bound $k=\lfloor\sqrt{n}\rfloor+1$, *i.e.* the regime $k\ge\sqrt{n}$, and remains valid: a Carmichael number n is squarefree with at least three prime factors, so its least prime factor satisfies $p<n^{1/3}<\sqrt{n}$ and is detected. This property must be attached to the $\sqrt{n}$ bound, not to the logarithmic depth, which rejects only those Carmichael numbers having a prime factor $\le k(n)$.

References

[1] Hardy, G.H. and Wright, E.M. (2008) An Introduction to the Theory of Numbers. 6th Edition, Oxford University Press, Oxford.

[2] Tenenbaum, G. (1995) Introduction to Analytic and Probabilistic Number Theory. Cambridge University Press, Cambridge.

[3] Mertens, F. (1874) Ein Beitrag zur analytischen Zahlentheorie. *Journal fur die Reine und Angewandte Mathematik*, **78**, 46-62.

[4] Rabin, M.O. (1980) Probabilistic Algorithm for Testing Primality. *Journal of Number Theory*, **12**, 128-138. https://doi.org/10.1016/0022-314x(80)90084-0

[5] Baillie, R. and Wagstaff, S.S. (1980) Lucas Pseudoprimes. *Mathematics of Computation*, **35**, 1391-1417. https://doi.org/10.1090/s0025-5718-1980-0583518-6