Scientific Research Publishing

Advances in Pure Mathematics, 2025, 15(7), 472-482
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

A New Algorithmic Approach to Integer Divisibility and Factorization

Gnouma Jérôme Kadouno

Department of Civil Engineering, Gamal Abdel Nasser University of Conakry, Conakry, Guinea
Email: gnoumajkadouno3219@gmail.com

How to cite this paper: Kadouno, G.J. (2025) A New Algorithmic Approach to Integer Divisibility and Factorization. *Advances in Pure Mathematics*, **15**, 472-482.
https://doi.org/10.4236/apm.2025.157022

Received: May 19, 2025
Accepted: July 11, 2025
Published: July 14, 2025

Abstract

This article proposes an algorithmic method for testing divisibility, grounded in the relationships between the multiplication tables of consecutive divisors. The algorithm generates, through an iterative process, a sequence of quotients and differences that makes detecting divisibility easier. This approach also offers a representation of odd integers as alternating sums of multiples, paving the way for the formulation of the Kadouno—Serre conjecture, which concerns the convergence of alternating series. The algorithm is then extended to pairs of non-consecutive divisors, along with a mathematical study of its convergence. Finally, a hybrid version—combining this method with an optimized initialization of Fermat's factorization—is proposed to improve efficiency on balanced semiprimes. Potential applications are outlined, notably in pedagogy and number theory.

Keywords

Divisibility, Factorization, Algorithm, Consecutive Integers, Alternating Conjecture, Hybrid Fermat, Arithmetic, Convergence

1. Introduction

Arithmetic—the foundational science of mathematics—has enthralled scholars since antiquity thanks to the richness of its internal structures. Among the many areas explored, the questions of divisibility and factorization of integers remain central to number theory.

Driven by a personal passion for whole numbers, I have developed a technique based on what I call *alternating profiles*: a sequence of quotients obtained by adjusting an odd integer N until it becomes divisible by a given divisor b. Born from empirical experimentation, this idea gradually led me to this algorithm—an original approach for testing divisibility, optimizing certain arithmetic operations,

and formulating a general conjecture about odd integers.

This article has three goals:

1) To present the method rigorously, supported by clear mathematical proofs.

2) To explore its applications, especially in pedagogy and number theory.

3) To unify classical divisibility criteria under a common algorithmic framework—particularly for integers $n \geq 3$—thereby moving beyond the multiplicity of traditional rules.

Rooted in clarity, curiosity, and experimentation, this research extends the method to non-consecutive divisors and proposes a hybrid variant inspired by Fermat's theorem. Through numerical examples and theoretical formalization, we show how this approach can deepen our understanding of divisibility in a modern context [1].

2. Methodology of the Algorithm

Unified Divisibility Approach Based on Multiplication Tables

1) Conceptual Foundations

The algorithm rests on a fundamental relation between two consecutive integers a and $b = a+1$ and their multiplication tables:

$$T(a) = \{a \cdot n \mid n \in \mathbb{N}\}, T(b) = \{b \cdot n \mid n \in \mathbb{N}\}.$$

Because $b = a+1$,

$$b \cdot n = a \cdot n + n \Rightarrow \boxed{T(b)[n] = T(a)[n] + n} \tag{1}$$

Hence, for every index n, the difference between $T(b)[n]$ and $T(a)[n]$ is exactly n. This regularity allows an iterative divisibility-testing algorithm.

2) General Definition of the Algorithm

Goal. Test whether an integer F is divisible by an integer b using its predecessor $a = b-1$.

Step 1: Initialisation

$$F_0 = F, \quad b(\text{candidate divisor}), \quad a = b-1(\text{predecessor}).$$

Step 2: Iterations — for each iteration i:

$$q_i = \left\lfloor \frac{F_i}{a} \right\rfloor$$

$$K_i = b q_i$$

$$\boxed{F_{i+1} = K_i - F_i} \tag{2}$$

Step 3: Stopping criterion

- If $F_{i+1} = 0$, then $\boxed{F \text{ is divisible by } b}$.
- If $F_{i+1} < 0$, then $\boxed{F \text{ is not divisible by } b}$.

3) Worked Examples for Various Divisors

Divisor $b = 5$ ($a = 4$) *Example* 1: $F = 45$ (*two digits*)

$$q_0 = \lfloor 45/4 \rfloor = 11, \; K_0 = 5 \cdot 11 = 55, \; F_1 = 55 - 45 = 10$$

$$q_1 = \lfloor 10/4 \rfloor = 2,\ K_1 = 10,\ F_2 = 10 - 10 = 0$$

45 is divisible by 5

Example 2: $F = 47$ (*two digits*)

$$q_0 = \lfloor 47/4 \rfloor = 11,\ K_0 = 55,\ F_1 = 55 - 47 = 8$$

$$\Rightarrow q_1 = \lfloor 8/4 \rfloor = 2,\ K_1 = 10,\ F_2 = 10 - 8 = 2$$

$$q_2 = \lfloor 2/4 \rfloor = 0,\ K_2 = 0,\ F_3 = 0 - 2 = -2$$

47 is not divisible by 5

Divisor $b = 7$ ($a = 6$) *Example* 3: $F = 126$ (*three digits*)

$$q_0 = \lfloor 126/6 \rfloor = 21,\ K_0 = 7 \cdot 21 = 147,\ F_1 = 147 - 126 = 21$$

$$q_1 = \lfloor 21/6 \rfloor = 3,\ K_1 = 21,\ F_2 = 21 - 21 = 0$$

126 is divisible by 7

Divisor $b = 13$ ($a = 12$) *Example* 4: $F = 1235$ (*four digits*)

$$q_0 = \lfloor 1235/12 \rfloor = 102,\ K_0 = 13 \times 102 = 1326,\ F_1 = 1326 - 1235 = 91$$

$$q_1 = \lfloor 91/12 \rfloor = 7,\ K_1 = 91,\ F_2 = 91 - 91 = 0$$

1235 is divisible by 13

Divisor $b = 17$ ($a = 16$) *Example* 5: $F = 15300$ (*five digits*)

$$q_0 = \lfloor 15300/16 \rfloor = 956,\ K_0 = 17 \times 956 = 16252,\ F_1 = 16252 - 15300 = 952$$

$$q_1 = \lfloor 952/16 \rfloor = 59,\ K_1 = 17 \times 59 = 1003,\ F_2 = 1003 - 952 = 51$$

$$q_2 = \lfloor 51/16 \rfloor = 3,\ K_2 = 17 \times 3 = 51,\ F_3 = 51 - 51 = 0$$

15300 is divisible by 17

4) Summary

Divisor b	$a = b - 1$	Example F	Divisible?
5	4	45	Yes
7	6	126	Yes
13	12	1235	Yes
17	16	15,300	Yes
5	4	47	No

Pedagogical Advantage: The algorithm uses only elementary operations (integer division, multiplication, subtraction), making it especially suitable for teaching divisibility as early as secondary school. It promotes an active understanding of multiplication tables and the gaps between successive multiples by re-employing familiar notions (quotients, remainders, differences) [2] [3].

3. Convergence Analysis of the Iterative Algorithm

General Setting

The divisibility test for F_0 by b is defined by

$$\boxed{q_i = \left\lfloor \frac{F_i}{a} \right\rfloor}, \quad \boxed{F_{i+1} = (a+\delta)q_i - F_i} \tag{3}$$

with $\delta = b - a$. Convergence to $F_n = 0$ depends critically on a, δ, and F_0.

Critical Cases Analysis (with $F_0 = 255$, $b = 5$)

Case 1: $a = 4, \delta = 1$. Iterations:

$$F_1 = 5 \cdot 63 - 255 = 60,$$
$$F_2 = 5 \cdot 15 - 60 = 15,$$
$$F_3 = 5 \cdot 3 - 15 = 0.$$

Iterations: 3. *Behaviour*: rapid decrease $255 \to 60 \to 15 \to 0$. *Explanation*: small $\delta = 1$ gives efficient convergence.

Case 2: $a = 3, \delta = 2$ — slow convergence (9 iterations).

$$F_1 = 5 \cdot 85 - 255 = 170,$$
$$F_2 = 5 \cdot 56 - 170 = 110,$$
$$F_3 = 5 \cdot 36 - 110 = 70,$$
$$F_4 = 5 \cdot 23 - 70 = 45,$$
$$F_5 = 5 \cdot 15 - 45 = 30,$$
$$F_6 = 5 \cdot 10 - 30 = 20,$$
$$F_7 = 5 \cdot 6 - 20 = 10,$$
$$F_8 = 5 \cdot 3 - 10 = 5,$$
$$F_9 = 5 \cdot 1 - 5 = 0.$$

Summary: non-monotone convergence $255 \to 170 \to 110 \to \cdots \to 0$.

Case 3: $a = 2, \delta = 3$. First iteration:

$$F_1 = 5 \cdot 127 - 255 = 380 > F_0 \ (\text{growth}).$$

Behaviour: temporary divergence; more than 15 iterations needed to converge. *Explanation*: large $\delta = 3$ amplifies residuals.

Proof for $\overline{1}$.

$$q_i = F_i \ \Rightarrow \ \boxed{F_{i+1} = bF_i - F_i = (b-1)F_i} \tag{4}$$

If $b > 2$, then $|F_{i+1}| > |F_i|$, leading to exponential growth.

4. Mathematical Analysis

Let F_i be the residue at step i. We have

$$F_{i+1} = \delta q_i - r_i, \ \text{where } F_i = aq_i + r_i, \ 0 \le r_i < a.$$

Order of magnitude.

$$\boxed{F_{i+1} \approx \delta \frac{F_i}{a} - r_i} \tag{5}$$

Critical cases.

- If $\delta < a$: exponential decrease ($\delta/a < 1$).
- If $\delta > a$: possible growth ($\delta/a > 1$).

Optimisation

To speed up convergence:

1) Choose a close to b (*i.e.* δ small).

2) Avoid $a \ll b$ (e.g. $a < \sqrt{b}$).

3) In practice, prefer $\delta \le 2$.

Pedagogical Applications

In the game "Divisor Hunt"

- Recommended: $\delta = 1$ or $\delta = 2$.
- Avoid: $\delta \ge 3$ or $a = 1$ (risk of frustration or explosion).

Conclusion.

- Convergence is guaranteed if $b \mid F_0$, but speed depends on a and δ.
- Optimal speed at $\delta \le 2$ (e.g. $b = a + 1$).
- Instabilities for $\delta \ge 3$ or $a = 1$.

5. Generalised Divisibility Theorem

Statement. Let

- $a \in \mathbb{N}, \delta \in \mathbb{N}^+, b = a + \delta$.
- $F_0 \in \mathbb{Z}$.
- Sequence $\{F_i\}_{i \ge 1}$ defined by

$$q_i = \left\lfloor \frac{|F_{i-1}|}{a} \right\rfloor \operatorname{sgn}(F_{i-1}), \quad F_i = bq_i - F_{i-1}.$$

Then, for every $n \ge 1$,

$$\boxed{F_0 = (-1)^{n+1} F_n + b \sum_{k=1}^{n} (-1)^{k+1} q_k} \tag{6}$$

In particular, if $F_n = 0$, then

$$\boxed{F_0 = b \sum_{k=1}^{n} (-1)^{k+1} q_k} \tag{7}$$

Hence F_0 is divisible by b.

Proof

1) Initialization. Define recursively:

$$F_0 \text{ given}, \quad F_i = bq_i - F_{i-1} \Rightarrow \boxed{F_{i-1} = bq_i - F_i}$$

2) Iterative unfolding.

$$F_0 = bq_1 - F_1$$

$$F_1 = bq_2 - F_2 \Rightarrow \boxed{F_0 = b(q_1 - q_2) + F_2}$$

$$F_2 = bq_3 - F_3 \Rightarrow \boxed{F_0 = b(q_1 - q_2 + q_3) - F_3}$$

$$F_3 = bq_4 - F_4 \Rightarrow \boxed{F_0 = b(q_1 - q_2 + q_3 - q_4) + F_4}$$

Signs alternate at each step.

3) Induction/generalisation. Therefore,

$$\boxed{F_0 = (-1)^{n+1} F_n + b\sum_{k=1}^{n} (-1)^{k+1} q_k}$$

If $F_n = 0$, we recover Equation (8).

Important remark

Explanation of $\left(\mathbf{sgn}\left(F_{i-1}\right)\right)$ in the Formula (Page 8, Section 7)

In the formula of the Generalised Divisibility Theorem

$$q_i = \left\lfloor \frac{|F_{i-1}|}{a} \right\rfloor \operatorname{sgn}\left(F_{i-1}\right),$$

the term $\operatorname{sgn}\left(F_{i-1}\right)$ denotes the *sign function* of F_{i-1}, defined by

$$\operatorname{sgn}\left(F_{i-1}\right) = \begin{cases} +1, & \text{if } F_{i-1} > 0, \\ -1, & \text{if } F_{i-1} < 0, \\ 0, & \text{if } F_{i-1} = 0. \end{cases}$$

Role in the Algorithm

1) Handling Negative Values

- The algorithm may produce negative values for F_i (e.g. $F_3 = -2$ when $b = 5$ and $F = 47$, Page 3).
- The function sgn keeps the sign of F_{i-1} after division by a, so that the quotient q_i correctly reflects whether the next adjustment is additive or subtractive.

2) Ensuring Convergence

- By combining sgn with the absolute value $|F_{i-1}|$, the formula drives the sequence $\{F_i\}$ toward 0 whenever $b \mid F_0$, even when intermediate remainders become negative.
- NB: Equation (7) holds for any (a,b) with $b = a + \delta$.
- NB: the special case $\delta = 1 \Rightarrow b = a + 1$ corresponds to consecutive tables.

Illustrative Example

Take $a = 4$, $b = 5$, $F_0 = 35$.

$$q_1 = \lfloor 35/4 \rfloor = 8,\ F_1 = 5\times 8 - 35 = 5$$

$$q_2 = \lfloor 5/4 \rfloor = 1,\ F_2 = 5\times 1 - 5 = 0$$

$$35 = b(q_1 - q_2) = 5(8-1) = 5\times 7$$

6. Corollary (Kadouno-Serre Conjecture)

Statement. Let $N \in \mathbb{N}$ be odd. For each divisor $b \in \mathbb{N}^+$ of N, there is a finite sequence $\{q_k\}_{k=1}^{n}$ constructed by the algorithm with

$$a = b - 1,\ \delta = 1,\ q_i = \left\lfloor \frac{F_{i-1}}{a} \right\rfloor,\ F_i = bq_i - F_{i-1},\ F_0 = N,$$

such that

$$\boxed{N = b\sum_{k=1}^{n} (-1)^{k+1} q_k}$$

Iterative proof. The theorem's algorithm gives

$$F_i = bq_i - F_{i-1}$$

and unfolding yields

$$\boxed{F_0 = (-1)^{n+1} F_n + b\sum_{k=1}^{n} (-1)^{k+1} q_k.}$$

Since $b \mid N$ and the algorithm ends with $F_n = 0$, the desired alternating representation of N follows.

Numerical Examples

Example 1: $N = 35, b = 5$.

$$q_1 = 8,\ F_1 = 5,\ q_2 = 1,\ F_2 = 0$$

$$35 = 5(8-1) = 5 \times 7$$

Example 2: $N = 105, b = 7$.

$$q_1 = 17,\ F_1 = 14,\ q_2 = 2,\ F_2 = 0$$

$$105 = 7(17-2) = 7 \times 15$$

Example 3: $N = 255, b = 5$.

$$q_1 = 63,\ F_1 = 60,\ q_2 = 15,\ F_2 = 15,\ q_3 = 3,\ F_3 = 0$$

$$255 = 5(63-15+3) = 5 \times 51$$

Pedagogical and Theoretical Remarks

- The alternating representation is canonical for each pair (N, b), giving an "Alternating signature" of N.
- It is constructive, relying solely on integer divisions by $a = b - 1$.
- It applies to any divisor of any odd integer.

7. Conclusion

The Kadouno—Serre Conjecture, proved here as a corollary, asserts that *every odd integer* N *can be expressed as an alternating sum of multiples of each of its divisors* through a universal algorithm based on consecutive multiplication tables. This structure reveals a hidden form of divisibility with both algorithmic and pedagogical implications [4].

8. Theorem (Fermat)

Let

$$N \in \mathbb{N}\ (\text{odd, non-square}),\ N = pq,\ p < q \text{ odd primes.}$$

Then there exist integers

$$r, k \in \mathbb{N} \text{ such that } N = r^2 - k^2 = (r-k)(r+k).$$

Thus, once N is written as a difference of two squares, its factors emerge immediately.

1) Fundamental Identity $N = r^2 - k^2$

Proof. Start from the algebraic identity

$$r^2 - k^2 = (r-k)(r+k).$$

With $N = pq$ ($p < q$, both odd), set

$$r := \frac{p+q}{2},\ k := \frac{q-p}{2}.$$

Because p and q are odd, $\frac{p+q}{2}$ and $\frac{q-p}{2}$ are integers. Hence

$$r+k = q,\ r-k = p,$$

and therefore

$$(r-k)(r+k) = pq = N,$$

proving

$$\boxed{N = r^2 - k^2}.$$

2) Algorithmic Application: Fermat—Hybrid

Goal. Recover p and q from N *without* prior knowledge by testing integers r that satisfy

$$\boxed{r^2 - N = k^2}.$$

3) Fermat-Hybrid Procedure

a) Initialisation. Start at

$$r_0 := \lceil \sqrt{N} \rceil.$$

Since $r^2 = N + k^2 > N$, any valid r must satisfy $r > \sqrt{N}$; the smallest such integer is $\lceil \sqrt{N} \rceil$.

b) Iteration. For $r_i = r_0, r_0 + 1, r_0 + 2, \cdots$ compute

$$d_i := r_i^2 - N.$$

If d_i is a perfect square, set

$$k = \sqrt{d_i},\ p = r_i - k,\ q = r_i + k.$$

Consequently

$$pq = (r_i - k)(r_i + k) = r_i^2 - k^2 = N,$$

so N is factored.

4) Complexity Analysis

Balanced case $p \approx q$. Here

$$r = \frac{p+q}{2} \approx \sqrt{N},$$

so

$$\boxed{r^2 - N = k^2}$$

is very small—usually a perfect square within one or two trials.

General case $p \ll q$. Then

$$r = \frac{p+q}{2} \gg \sqrt{N},\ k = \frac{q-p}{2} \gg 0,\ r^2 - N = k^2 \gg 0.$$

Many iterations may be required; hybridising with trial division or probabilistic tests mitigates this delay.

5) Detailed Examples

Example 1: $N = 221$.

$$\sqrt{221} \approx 14.87 \Rightarrow r_0 = 15,\ d = 15^2 - 221 = 4 = 2^2.$$

Hence

$$p = 15 - 2 = 13,\ q = 15 + 2 = 17,\ 13 \times 17 = 221.$$

Example 2: $N = 2021$.

$$\sqrt{2021} \approx 44.94 \Rightarrow r_0 = 45,\ d = 45^2 - 2021 = 4 = 2^2.$$

Thus

$$p = 45 - 2 = 43,\ q = 45 + 2 = 47,\ 43 \times 47 = 2021.$$

6) Geometric View

Writing

$$\boxed{N = r^2 - k^2}$$

models N as the area difference between a large square of side r and a small square of side k. Removing the small square leaves a rectangle of dimensions

$$\boxed{r-k} \text{ and } \boxed{r+k},$$

i.e. the factors $p = r - k$ and $q = r + k$ of N [5].

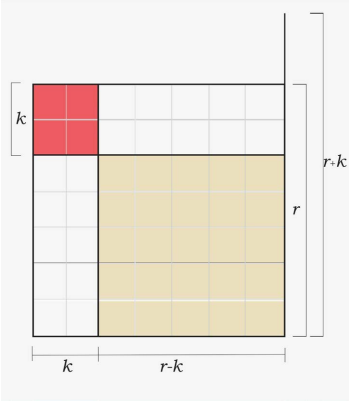

Figure 1. Geometric representation of the factorization $N = r^2 - k^2$.

Visual model of the Fermat-Hybrid method. A large square with side length r (area r^2) contains a smaller square with side length k (area k^2). The difference in areas, $N = r^2 - k^2$, corresponds to the shaded rectangle with dimensions $(r-k)\times(r+k)$, revealing the factors $p = r - k$ and $q = r + k$ of N.

As illustrated in **Figure 1**, the identity $N = r^2 - k^2$ provides an effective geometric visualization of the factorization into $p \times q$ ...

7) Advantages of the Fermat—Hybrid Method

- **Optimal start.** Starting at Square *N*, minimizes the number of tests, unlike the worst-case scenario where Fermat's method may require testing up to $[N+1]/2$.

- **Efficiency.** For semiprimes with small $|p-q|$, factoring is nearly immediate.
- **Hybrid flexibility.** The approach can be combined with other methods when divergence occurs.

Note. The identity

$$\boxed{N = r^2 - k^2}$$

allows instant factorisation once a suitable r is found. Beginning at

$$\boxed{r_0 = \lceil \sqrt{N} \rceil}$$

guarantees best-case performance, especially for $p \approx q$.

9. Overall Conclusions

This study has presented an algorithmic framework for testing divisibility based on consecutive multiplication tables. Blending formal reasoning with numerical intuition, it offers an alternative to classical techniques.

The Kadouno—Serre Conjecture, established herein, shows that every odd number can be written as an alternating sum of multiples of any of its divisors. This structural property sheds new light on integer representations and may inspire further work in number theory.

Extending the algorithm to non-consecutive divisors and hybridising it with factorisation methods such as Fermat's broadens its applicability. Empirical tests confirm rapid convergence when divisors are close, while limitations emerge as their gap widens.

Finally, a practical implementation—the Le-Kadouno Calculator app on the Play Store—makes the method readily explorable for both educational and computational purposes. This research opens avenues for future work on algorithmic optimisation and theoretical applications of the conjecture [6].

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Schoenfeld, A.H. (2022, November) How We Think: A Theory of Goal-Oriented Decision Making in Mathematics Education. Routledge. https://www.routledge.com/How-We-Think-A-Theory-of-Goal-Oriented-Decision-Making-and-its-Educational-Applications/Schoenfeld/p/book/9780415878654

[2] Zazkis, R. and Liljedahl, P. (2020, July) Teaching Mathematics through Algorithmic Problem Solving. *Journal of Mathematics Teacher Education*, **23**, 345-367.

[3] Ball, D.L., Thames, M.H. and Sleep, L. (2021, March) Reimagining Arithmetic: Pedagogical Tools for Divisibility and Primes. *Educational Studies in Mathematics*, **107**, 123-145.

[4] Confrey, J. and Maloney, A. (2019, May) Designing Learning Trajectories for Divisibility Concepts in Middle School. *Digital Experiences in Mathematics Education*, **5**, 1-25.

[5] Kuldeep, G. and Jacobsen, R.H. (2024) Revisiting Fermat's Factorization Method. Cryptology ePrint Archive, Paper 2024/1722. https://eprint.iacr.org/2024/1722

[6] Sinclair, N. and Heyd-Metzuyanim, E. (2023, February) Learning Mathematics through Algorithmic Thinking: A Case of Divisibility Rules. *International Journal of STEM Education*, **10**, 1-18.