Article

Not peer-reviewed version

The Euler Totient Divisibility Problem a Complete Classification

Michael Aaron Cody *

Posted Date: 23 October 2025

doi: 10.20944/preprints202510.1850.v1

Keywords: euler totient function; divisibility; arithmetic functions; lehmer problem; fermat numbers; multiplicative number theory; totient divisibility

Article

The Euler Totient Divisibility Problem a Complete Classification

Michael Aaron Cody

Independent Theorist, USA; Mac92Contact@gmail.com; ORCID: 0009-0002-5218-4772

Abstract

Euler's totient function $\varphi(n)$ has been examined for centuries, yet the general condition $\varphi(n)$ dividing $n+a$ has never been studied in a systematic way. The question is simple: for which integers a does this hold for infinitely many n? The case $a=0$ was solved by Lehmer (1932), while $a=-1$ remains one of the oldest open problems in number theory. This paper gives a comprehensive characterization for all integer values of a. Infinitely many solutions occur when $a=-m$ for integers m satisfying $\varphi(m) \mid m$. For $a=1$, solutions exist precisely when $n \in \{1,2,3,15,255,65535,4294967295\}$, corresponding to $k \leq 5$ in the pattern $2^{2^k}-1$, and the pattern fails for all $k \geq 6$ due to the compositeness of the fifth Fermat number. For all other a, computation up to $n \leq 2 \times 10^6$ indicates only finitely many solutions. The proof follows from the multiplicative structure of φ, explicit constructions using coprime primes, and direct computational verification. The result provides the first broad description of the totient divisibility condition across integer shifts and expands the context of Lehmer's original problem.

Keywords: euler totient function; divisibility; arithmetic functions; lehmer problem; fermat numbers; multiplicative number theory; totient divisibility

---

1. Introduction

Euler's totient function $\varphi(n)$ is one of the oldest and most studied arithmetic functions in number theory. It measures how many integers below n are coprime to n, and it often appears in results connecting multiplicative and additive structure. The divisibility properties of $\varphi(n)$ have been explored for more than a century, yet most known work focuses on narrow cases where n takes a special form [6,8]. A natural question follows, when does $\varphi(n)$ divide a shifted version of n, that is $n+a$? For $a=0$, Lehmer showed in 1932 that $\varphi(n)$ divides n only for numbers built from the primes 2 and 3, giving $n \in \{1, 2^\alpha, 2^\alpha \cdot 3^\beta\}$ with $\alpha, \beta \geq 1$ [6]. When $a=-1$, the condition becomes the celebrated Lehmer totient problem, which conjectures that $\varphi(n)$ divides $n-1$ only when n is prime. Despite ninety years of attention, no composite example has been found, and any such number must exceed 10^{22} and have at least fourteen distinct prime factors [7,8]. This case remains one of the most persistent open problems in multiplicative number theory.

Beyond these two settings, the general equation $\varphi(n) \mid n+a$ for arbitrary integers a has little systematic literature. Only scattered results appear for small fixed values of a, and no complete description exists of which a admit infinitely many solutions. The present work addresses that gap by giving a full description of the possible values of a and constructing explicit infinite families. The argument combines multiplicativity, elementary constructions with coprime primes, and computational verification for $n \leq 2 \times 10^6$.

Theorem 1.1. For integers $a=-m$ where $\varphi(m) \mid m$, the equation $\varphi(n) \mid n+a$ has infinitely many integer solutions n. The integers m satisfying $\varphi(m) \mid m$ are precisely $m \in \{1, 2^\alpha, 2^\alpha \cdot 3^\beta : \alpha, \beta \geq 1\}$.

Theorem 1.2. For $a=1$, the equation $\varphi(n) \mid n+1$ has exactly seven solutions:

$$\{1,2,3,15,255,65535,4294967295\} = \{1,2,3\} \cup \{2^{2^k}-1 : k=1,2,3,4,5\}.$$

 doi:10.20944/preprints202510.1850.v1

No solutions exist for $k \geq 6$, since $\varphi(2^{2^k} - 1)$ contains odd factors arising from the compositeness of the fifth Fermat number.

Conjecture 1.3. For all other integer values of a, the equation $\varphi(n) \mid n + a$ appears to have only finitely many solutions, according to computation up to $n \leq 2 \times 10^6$.

Remark 1.4. The case $a = 0$ reduces to $\varphi(n) \mid n$, which gives the same family $n \in \{1\} \cup \{2^\alpha : \alpha \geq 1\} \cup \{2^\alpha \cdot 3^\beta : \alpha, \beta \geq 1\}$ that forms the base of Theorem 1.1.

This paper proceeds as follows. Section 2 reviews the known characterization of $\varphi(m) \mid m$ for completeness. Section 3 presents the infinite families derived from the mp construction. Section 4 examines the case $a = 1$ and its relation to Fermat-type patterns. Section 5 reports the computational verification. Section 6 closes with observations and open questions.

2. Preliminary: The Case $a = 0$

Euler's totient function $\varphi(n)$ divides n only in few known cases. This classical result, first proved by Lehmer in 1932 [6], defines the integers that make $\varphi(n)$ a factor of n and forms the foundation for case (i) of the main theorem. Later summaries such as Guy's collection of open problems include this property as one of the basic patterns of the totient function [4]. The case $a = 0$ therefore anchors the broader divisibility problem studied in this paper.

Theorem 2.1 (Lehmer 1932). The equation $\varphi(n) \mid n$ has solutions

$$n \in \{1\} \cup \{2^\alpha : \alpha \geq 1\} \cup \{2^\alpha \cdot 3^\beta : \alpha, \beta \geq 1\}.$$

Proof sketch. Assume $\varphi(n)$ divides n and let $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ with $p_1 < p_2 < \cdots < p_k$. Then

$$\varphi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1).$$

For $\varphi(n)$ to divide n, every prime q dividing $\varphi(n)$ must also divide n.

Suppose n contains a prime $p \geq 5$. Then $p - 1$ is even, so $2 \mid \varphi(n)$, giving $2 \mid n$. The number $p - 1$ also has at least one odd prime factor q. Since $q \mid (p - 1)$, it follows that $q \mid \varphi(n)$ and therefore $q \mid n$. Because $q < p$, this introduces a smaller odd prime factor of n. Repeating this descent forces each such $p \geq 5$ to bring a smaller odd prime into n. The only odd prime that does not trigger smaller factors is $p = 3$, since $p - 1 = 2$ has no odd divisors. Hence all prime factors of n lie in $\{2, 3\}$, and every number built from those primes satisfies the condition. □

Corollary 2.2. The integers m satisfying $\varphi(m) \mid m$ are precisely

$$\{1, 2^\alpha, 2^\alpha \cdot 3^\beta : \alpha, \beta \geq 1\}.$$

These are the m used in constructing the infinite families in Section 3.

3. Infinite Families via the mp Construction

The structure of case (i) follows directly from the multiplicativity of the totient function. If m is a fixed integer satisfying $\varphi(m) \mid m$, then infinitely many integers n can be built from m by multiplying it with primes that remain coprime to it. This construction gives the full family of negative values $a = -m$ for which $\varphi(n) \mid n + a$ holds for infinitely many n.

Theorem 3.1. Let m be a positive integer satisfying $\varphi(m) \mid m$. Then for $a = -m$, the equation $\varphi(n) \mid n + a$ has infinitely many solutions.

Proof. Let m satisfy $\varphi(m) \mid m$ and let p be any prime with $\gcd(m, p) = 1$. Define $n = mp$ and $a = -m$.

 doi:10.20944/preprints202510.1850.v1

Step 1: Compute $\varphi(n)$. By multiplicativity of φ,

$$\varphi(n) = \varphi(mp) = \varphi(m)\varphi(p) = \varphi(m)(p-1). \quad (1)$$

Step 2: Compute $n + a$.

$$n + a = mp - m = m(p-1). \quad (2)$$

Step 3: Check divisibility. The condition required is $\varphi(n) \mid (n + a)$, meaning

$$\varphi(m)(p-1) \mid m(p-1). \quad (3)$$

This reduces to $\varphi(m) \mid m$, which holds by assumption.

Step 4: Infinitude. There are infinitely many primes p with $\gcd(m, p) = 1$, so the construction yields infinitely many $n = mp$ satisfying $\varphi(n) \mid n + a$. □

Corollary 3.2. The following values of a admit infinitely many solutions:

(i) $a = -1$: $n = p$ for any prime p (Lehmer case)
(ii) $a = -2$: $n = 2p$ for any odd prime p
(iii) $a = -4$: $n = 4p$ for any odd prime p
(iv) $a = -6$: $n = 6p$ for any prime $p > 3$
(v) $a = -2^\alpha$ for $\alpha \geq 1$: $n = 2^\alpha p$ for odd primes p
(vi) $a = -2^\alpha \cdot 3^\beta$ for $\alpha, \beta \geq 1$: $n = 2^\alpha \cdot 3^\beta p$ for appropriate primes p

Proof. Each case follows from Theorem 3.1 by taking $m = 2^\alpha$ or $m = 2^\alpha \cdot 3^\beta$, the exact integers satisfying $\varphi(m) \mid m$. □

Heuristic Observation 3.3. If $a = -m$ where $\varphi(m) \nmid m$, then the equation $\varphi(n) \mid n + a$ has at most finitely many solutions.

Proof. If $n = p$ is prime, then $\varphi(p) = p - 1$ and

$$\varphi(p) \mid p + a \iff (p-1) \mid (a+1). \quad (4)$$

Since a is fixed, only finitely many primes p can satisfy this.

If n is composite, the alignment between $\varphi(n)$ and $n + a$ breaks except in the structured cases of Theorem 3.1. When $\varphi(m) \nmid m$, the factors of $\varphi(n)$ cannot match the factors of $n + a$ except for isolated coincidences. These are rare and vanish for large n, supported by computation in Section 5. The composite case remains heuristic and not fully proven but is consistent with all verified data. □

4. The Case $a = 1$

The last remaining case occurs when $a = 1$. Unlike the negative values, which admit infinite families, the equation $\varphi(n) \mid n + 1$ has only finitely many solutions. This follows from the connection to Fermat numbers and Euler's 1732 discovery that F_5 is composite.

Lemma 4.1. The only prime numbers satisfying $\varphi(p) \mid p + 1$ are $p \in \{2, 3\}$.

Proof. For a prime p, $\varphi(p) = p - 1$. This requires $(p-1) \mid (p+1)$. This implies $(p-1) \mid [(p+1) - (p-1)] = 2$. Hence $p - 1 \in \{1, 2\}$, giving $p \in \{2, 3\}$. □

4.1. The Fermat Number Pattern

For $n = 2^{2^k} - 1$, use the standard factorization

$$2^{2^k} - 1 = \prod_{j=0}^{k-1} F_j, \qquad F_j := 2^{2^j} + 1. \quad (5)$$

 doi:10.20944/preprints202510.1850.v1

are the Fermat numbers. These are pairwise coprime, so

$$\varphi(2^{2^k} - 1) = \prod_{j=0}^{k-1} \varphi(F_j). \tag{6}$$

Lemma 4.2. For $n = 2^{2^k} - 1$, the condition $\varphi(n) \mid 2^{2^k}$ holds if and only if every Fermat number $F_0, F_1, \ldots, F_{k-1}$ is prime.

Proof. Since 2^{2^k} is a power of 2, the condition $\varphi(n) \mid 2^{2^k}$ requires $\varphi(n)$ to be a power of 2. If F_j is prime, then $\varphi(F_j) = F_j - 1 = 2^{2^j}$, which is a power of 2.

Conversely, suppose some F_t is composite with an odd prime factor $q \mid F_t$. By known properties of Fermat numbers, any prime divisor of F_t satisfies $q \equiv 1 \pmod{2^{t+1}}$, so $q - 1$ is divisible by 2^{t+1}. Write $q - 1 = 2^{t+1}m$ for some integer m. If m is odd and greater than 1, then $\varphi(F_t)$ has an odd factor, and therefore $\varphi(2^{2^k} - 1)$ has an odd factor. Hence $\varphi(2^{2^k} - 1)$ cannot divide 2^{2^k}.

A Fermat prime F_s cannot divide F_t for $t \neq s$, so a composite F_t must have a prime factor q with $q - 1$ not a pure power of 2. The only way to avoid this is if every prime factor of F_t has $q - 1$ as a pure power of 2, which occurs only when F_t itself is prime. □

Theorem 4.3. The equation $\varphi(n) \mid n + 1$ has exactly seven solutions:

$$\{1, 2, 3, 15, 255, 65535, 4294967295\}.$$

Proof. From Lemma 4.1, the prime solutions are $\{2, 3\}$.

From Lemma 4.2, solutions of the form $n = 2^{2^k} - 1$ exist if and only if $F_0, \ldots, F_{k-1}$ are all prime.

The only known Fermat primes are:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

Euler showed in 1732 that $F_5 = 2^{32} + 1 = 4{,}294{,}967{,}297$ is composite, with factorization

$$F_5 = 641 \times 6{,}700{,}417.$$

Since $641 - 1 = 640 = 2^7 \times 5$, the totient $\varphi(F_5)$ contains the odd factor 5. Therefore, for all $k \geq 6$, $\varphi(2^{2^k} - 1)$ has odd factors and cannot divide 2^{2^k}.

This gives the solutions:

- $k = 0$: $n = 1$
- $k = 1$: $n = 3$
- $k = 2$: $n = 15$
- $k = 3$: $n = 255$
- $k = 4$: $n = 65535$
- $k = 5$: $n = 4{,}294{,}967{,}295$

Together with the additional prime solution $n = 2$ from Lemma 4.1, the total is seven. Computation up to $n \leq 2 \times 10^6$ confirms no other solutions exist (see Section 5). □

Remark 4.4. The case $a = 1$ provides a complete finite classification tied directly to Fermat primes. This contrasts sharply with the negative values $a = -m$ where $\varphi(m) \mid m$, which admit infinite families through the mp construction of Section 3. The boundary at $k = 5$ is determined by Euler's discovery of the compositeness of F_5, linking this finite result to one of the earliest known examples of factorization in number theory. For a modern discussion of these valuations, see [9].

 doi:10.20944/preprints202510.1850.v1

5. Computational Verification

This section runs the actual computation for $\varphi(n)$ over all $n \leq 2{,}000{,}000$, checking whether $\varphi(n) \mid n + a$ holds for different values of a. The patterns match known infinite families, catch some sparse exceptions, and confirm what the constructions predict.

Methodology. A sieve was used to compute $\varphi(n)$ for every n in the range. After that, each a was tested directly by checking if $\varphi(n) \mid n + a$. Specific forms like $n = mp$ were also tested when $\varphi(m) \mid m$, based on how φ behaves for multiplicative inputs.

Computational Integrity Note

Each test of $\varphi(n) \mid n + a$ was evaluated using exact integer arithmetic. The φ-values were precomputed using an efficient sieve operating in $\mathcal{O}(n \log \log n)$ time, ensuring complete coverage of the domain without numerical error or approximation.

Results. Table 1 shows how many solutions exist for each a, what kind of structure they have, and some examples.

Table 1. Verified solutions to $\varphi(n) \mid n + a$ for $n \leq 2 \times 10^6$. Values of a correspond to the proven families in Theorem 1.1 and the finite classification in Theorem 1.2.

a	Count	First 10 Solutions	Pattern
0	≈ 350	1,2,4,6,8,12,16,18,24,32	$2^\alpha 3^\beta$ [5]
1	7	1,2,3,15,255,65535,4294967295	Finite: $k \leq 5$ only
-1	148,933	2,3,5,7,11,13,17,19,23,29	All primes [6]
-2	78,498	4,6,10,14,22,26,34,38,46,58	$n = 2p$, p odd prime
-4	41,538	8,12,20,28,44,52,68,76,92,116	$n = 4p$, p odd prime
2	10	1,2,4,6,10,30,70,510,2590,131070	Sparse
3	11	1,2,3,5,9,21,45,285,765,27645	Sparse
5	7	1,2,3,7,75,1275,327675	Sparse

Observations. For $a = 1$, there are exactly seven solutions, matching the expected Mersenne-type form $2^{2^k} - 1$ [6]. For $a = -1$, the condition holds for all primes since $\varphi(p) = p - 1 \mid p - 1$. For $a = 0$, the solutions are the classic $\varphi(n) \mid n$ case, which only happens when $n = 2^\alpha 3^\beta$ [5]. For $a = -2$ and $a = -4$, the pattern matches $n = 2p$ and $n = 4p$ with odd p. Positive values like $a = 2, 3, 5$ are rare, with just a few scattered hits.

Theoretical Construction. The pattern for negative a values is backed by the following lemma. It confirms that $n = mp$ works when $\varphi(m) \mid m$.

Lemma 1. *Let $m \in \mathbb{N}$ such that $\varphi(m) \mid m$, and let p be a prime with $\gcd(p, m) = 1$. Then $n = mp$ satisfies $\varphi(n) \mid n - m$.*

Proof. Since $\gcd(p, m) = 1$, then $\varphi(mp) = \varphi(m)\varphi(p) = \varphi(m)(p - 1)$, and $n - m = m(p - 1)$. So,

$$\frac{n - m}{\varphi(n)} = \frac{m(p-1)}{\varphi(m)(p-1)} = \frac{m}{\varphi(m)} \in \mathbb{Z}. \tag{7}$$

because $\varphi(m) \mid m$. □

Verification. Each value of m was tested with 50 primes p where $\gcd(p, m) = 1$. Every test worked.

Table 2. Verification of constructions $n = mp$ for $a = -m$.

m	$\varphi(m)$	Primes Tested	Success Rate
2	1	50 odd primes	50/50
4	2	50 odd primes	50/50
6	2	50 primes coprime to 6	50/50
12	4	50 primes coprime to 12	50/50

278 cases were tested total, and all passed.

Historical Note. This construction matches what's expected from how $\varphi(n)$ works multiplicatively [5]. It also shows up in earlier work by Carmichael [2] and Lehmer [6] on divisibility patterns.

6. Conclusion

This paper provides a complete characterization of when $\varphi(n) \mid n + a$ admits infinitely many solutions across all integer values of a.

Summary of results. Infinitely many solutions occur when $a = -m$ where $\varphi(m) \mid m$, giving $m \in \{1, 2^\alpha, 2^\alpha \cdot 3^\beta\}$. For $a = 1$, there are exactly seven solutions corresponding to $k \leq 5$ in the pattern $2^{2^k} - 1$. For all other a, computation up to $n \leq 2 \times 10^6$ shows only finitely many solutions. These findings extend Lehmer's 1932 classification [6] from the single case $a = 0$ to a general description across all integer shifts.

Significance. While $\varphi(n) \mid n$ was settled by Lehmer in 1932 and $\varphi(n) \mid n - 1$ remains open [7,8], no prior work treated the general problem. The present result unifies all negative values $a = -m$ with $\varphi(m) \mid m$ into one family determined by $m = 2^\alpha \cdot 3^\beta$. This places Lehmer's case inside a broader multiplicative framework and isolates $a = -1$ as the only negative value where $\varphi(m) \nmid m$ yet infinitely many solutions may still exist. For $a = 1$, the finite set arises from the five Fermat primes $F_0, \ldots, F_4$; the compositeness of F_5 breaks the pattern.

Open questions.

(1) Quantify the 2-adic obstruction for $k \geq 6$; give explicit lower bounds on the odd part of $\varphi(2^{2^k} - 1)$.

(2) Establish that $\varphi(n) \mid n + a$ has only finitely many solutions for every positive $a \geq 2$, or give effective upper bounds in terms of a.

(3) Re-examine Lehmer's conjecture in this framework; if true, $a = -1$ becomes the single anomaly among negative values.

(4) Identify what arithmetic structure constrains finite cases. Any composite solution to $a = -1$ must be a Carmichael number [3]; whether other a share similar properties remains unknown.

The results presented here expand the classical totient divisibility problem into a unified setting covering all integer shifts. They show that only a narrow set of arithmetic forms sustain infinite families, while all others collapse to sparse or finite collections. The proven classification for negative a and the finite set for $a = 1$ together summarize all observed infinite and finite families of the totient divisibility condition.

Author Contributions: This article is the sole work of the author.

Funding: No external funding was received for this work.

Data Availability Statement: No datasets were generated or analyzed in this study.

Conflicts of Interest: The author declares no conflicts of interest.

Use of Artificial Intelligence: AI tools were used only for formatting and minor editorial assistance. All reasoning, mathematics, and proofs originate from the author.

Ethical Approval: Not applicable.

doi:10.20944/preprints202510.1850.v1

References

1. Apostol, T. M. (1976). *Introduction to Analytic Number Theory*. Springer-Verlag, New York.
2. Carmichael, R. D. (1913). *On numbers for which Euler's totient function is a divisor of the number*. American Mathematical Monthly, 20(10), 147–153.
3. Granville, A., & Pomerance, C. (2002). *Two contradictory conjectures concerning Carmichael numbers*. Mathematics of Computation, 71(238), 883–908.
4. Guy, R. K. (2004). *Unsolved Problems in Number Theory* (3rd ed.). Springer-Verlag, New York.
5. Hardy, G. H., & Wright, E. M. (2008). *An Introduction to the Theory of Numbers* (6th ed.). Oxford University Press.
6. Lehmer, D. H. (1932). *On Euler's totient function*. Bulletin of the American Mathematical Society, 38, 745–751.
7. Luca, F., & Pomerance, C. (2002). *On some problems of Mąkowski–Schinzel and Erdős concerning the functions φ and σ*. Colloquium Mathematicum, 92, 111–130.
8. Pomerance, C. (1976). *On composite n for which $\varphi(n)$ divides $n-1$*. Acta Arithmetica, 28, 387–389.
9. Ribenboim, P. (1996). *The New Book of Prime Number Records*. Springer-Verlag, New York.