Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2025, Volume 31, Number 3, 504–534
DOI: 10.7546/nntdm.2025.31.3.504-534

On the special cases of Carmichael's totient conjecture

Anthony G. Shannon [1], Peter J.-S. Shiue [2], Tian-Xiao He [3], and Christopher Saito [4]

[1] Warrane College, The University of New South Wales
Kensington, NSW 2033, Australia
e-mail: t.shannon@warrane.unsw.edu.au

[2] Department of Mathematical Sciences, University of Nevada, Las Vegas
Las Vegas, Nevada, 89154-4020, USA
e-mail: peter.shiue@unlv.edu

[3] Department of Mathematics, Illinois Wesleyan University
Bloomington, Illinois 61702, USA
e-mail: the@iwu.edu

[4] Department of Mathematical Sciences, University of Nevada, Las Vegas
Las Vegas, Nevada, 89154-4020, USA
e-mail: saitoc1@unlv.nevada.edu

Received: 19 May 2025 **Revised:** 28 July 2025
Accepted: 4 August 2025 **Online First:** 15 August 2025

Abstract: Euler's totient function, $\varphi(n)$, is the arithmetic function defined as the number of positive integers less than or equal to n that are relatively prime to n. In his 1922 paper [3], Professor R. D. Carmichael conjectured that for each positive integer n, there exists at least one positive integer $m \neq n$ such that $\varphi(m) = \varphi(n)$.

In this paper, we consider some relevant literature and explore Carmichael's totient conjecture for particular values of $\varphi(n) = k$. Our main consideration will be the set $X_k = \{n \in \mathbb{N} : \varphi(n) = k\}$. In identifying X_k for $k = 2^t,\ 2p^s,\ 2^2p,$ and $2pq$, where p and q are distinct prime numbers, we

find that Carmichael's conjecture holds for those select cases, provide an algorithm, and some related results. The conjecture remains an open problem in number theory [9].
Keywords: Carmichael Conjecture, Euler totient function, Fermat chain, Fermat primes, Fibonacci numbers, Germain primes, Integer components, Primitive prime divisors.
2020 Mathematics Subject Classification: 11A07, 11Y11.

1 Introduction

1.1 Preliminaries

Euler's totient function, $\varphi(n)$, is the arithmetic function defined as the number of positive integers less than or equal to n that are relatively prime to n. We write

$$\varphi(n) = |\{x \in \mathbb{N} : 1 \leq x \leq n,\ x \text{ relatively prime to } n\}|,$$

where $\mathbb{N} = \{1, 2, 3, \ldots\}$. For example, $\varphi(15) = 8$ because $|\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$.

We state the following properties of φ for reference as they are used throughout the paper. The reader is directed to Chapter 7 of [23] for further properties and proofs.

Proposition 1.1.1. *If p is a prime number and a is a positive integer, then*

$$\varphi(p^a) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right) = p^{a-1}(p-1).$$

Proposition 1.1.2. *If m and n are relatively prime positive integers, then*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Proposition 1.1.3. *Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime-power factorization of the positive integer n. Then*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Corollary 1.1.4. *Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime-power factorization of the positive integer n. Then*

$$n = \frac{\varphi(n)}{(p_1 - 1)(p_2 - 1)\cdots(p_r - 1)} \cdot p_1 p_2 \cdots p_r.$$

Corollary 1.1.4 is the main tool we will use to study Carmichael's totient conjecture.

Proposition 1.1.5. *Let a and b be positive integers, and $d = \gcd(a, b)$. Then*

$$\varphi(ab) = d \cdot \frac{\varphi(a)\varphi(b)}{\varphi(d)}.$$

Proof. Let a and b be positive integers, and $d = \gcd(a, b)$. Then

$$\begin{aligned}
\varphi(ab) &= ab \cdot \prod_{p|ab} \left(1 - \frac{1}{p}\right) \\
&= ab \cdot \frac{\prod_{p|a}\left(1 - \frac{1}{p}\right) \cdot \prod_{p|b}\left(1 - \frac{1}{p}\right)}{\prod_{p|d}\left(1 - \frac{1}{p}\right)} \\
&= d \cdot \frac{a\prod_{p|a}\left(1 - \frac{1}{p}\right) \cdot b\prod_{p|b}\left(1 - \frac{1}{p}\right)}{d\prod_{p|d}\left(1 - \frac{1}{p}\right)} \\
&= d \cdot \frac{\varphi(a)\varphi(b)}{\varphi(d)},
\end{aligned}$$

as desired. □

Proposition 1.1.5 takes Proposition 1.1.2 as a special case. To see this, let the $\gcd(a, b) = 1$.

Proposition 1.1.6. *If m and n are positive integers with $m \mid n$, then*

$$\varphi(m) \mid \varphi(n).$$

We saw previously that $\varphi(15) = 8$, and in addition, $\varphi(20) = 8$ because

$$|\{1, 3, 7, 9, 11, 13, 17, 19\}| = 8.$$

Hence, the equation $\varphi(n) = 8$ has at least two solutions.

Fix a positive integer k. We denote the set of solutions of the equation $\varphi(n) = k$ by

$$X_k = \{n \in \mathbb{N} : \varphi(n) = k\}.$$

Moving forward, we refer to the number of solutions of the equation $\varphi(n) = k$ as $|X_k|$. Table 1 lists X_k for all $k \leq 50$, and we see that $|X_8| = 5$. Alois Pichler gave a similar table for all $k \leq 200$ in [19].

The general observation that $|X_k| = 0$ or $|X_k| \geq 2$ [10,17,21,22,28] is the basis of this paper and Carmichael's totient conjecture [3]. The statement of Carmichael's totient conjecture is as follows.

Carmichael's totient conjecture. *For each positive integer n, there exists at least one positive integer $m \neq n$ such that $\varphi(m) = \varphi(n)$.*

In what follows, we provide a brief history of the investigation of Carmichael's totient conjecture. Beginning in 1908, Carmichael tabulated all the solutions of $\varphi(n) = k$ for $k \leq 1000$ in the *American Journal of Mathematics* [1]. Wegner and Savitzky [32] later corrected this table of Carmichael and extended it to $k = 1978$ by computer. In 1947, Klee [12] showed that

Carmichael's conjecture is valid below $k = 10^{400}$, which extended the result of 10^{37} given in [3]. The lower bound for a counterexample was further extended to $10^{10{,}000}$ by Masai and Valette [15] in 1982. In 1994, Schlafly and Wagon [25] showed that Carmichael's conjecture is valid below $10^{10{,}000{,}000}$. In 1998, Ford [6] sharpened earlier work to show that any exception to this conjecture must exceed $10^{10^{10}}$. Grosswald [7] has proved that if there is a unique solution for $\varphi(n) = k$, then $32 \mid k$. Donnelly [5] and Pomerance [21] have extended the study of this particular problem. For a comprehensive review of earlier known results the reader is referred to Sivaramakrishnan [26]. Some authors have tended to focus on particular cases of X_k [16, 18, 29]. Schinzel [24], in effect, deduced that for every $k > 1$, there exist infinitely many numbers m_k such that $\varphi(x) = m_k$ has exactly k solutions. Other authors have considered critical reviews of open problems in the literature [4, 9, 13, 30, 31].

The conjecture is proven for all odd positive integers; see Proposition 1.1.7.

Proposition 1.1.7. *If n is an odd positive integer, then $\varphi(n) = \varphi(2n)$.*

Proof. Since φ is multiplicative,

$$\varphi(2n) = \varphi(2)\varphi(n) = 1 \cdot \varphi(n) = \varphi(n). \qquad \square$$

Additionally, we note that the unique odd positive integer k for which $X_k \neq \{\}$ is $k = 1$, and $X_1 = \{1, 2\}$. All other integers k for which $X_k \neq \{\}$ are even by Proposition 1.1.8.

Proposition 1.1.8. *If n is a positive integer, then $\varphi(n) = 1$ or $\varphi(n)$ is even.*

Proof. If $n = 1$ or 2, then $\varphi(n) = 1$. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime-power factorization of the positive integer $n > 2$. That is, $p_1 < p_2 < \cdots < p_r$ are prime numbers, and a_i are positive integers for all $i = 1, 2, \ldots, r$.

If n is even, then $\varphi(n)$ is even by Proposition 1.1.3. If n is odd, then for each $i = 1, 2, \ldots, r$, p_i is odd. Since p_i is odd, $p_i - 1$ is even, and so

$$\varphi(n) = \prod_{i=1}^{r} \varphi\left(p_i^{a_i}\right) = \prod_{i=1}^{r} p_i^{a_i - 1}\left(p_i - 1\right)$$

is even. Thus, $\varphi(n) = 1$ or $\varphi(n)$ is even. $\square$

We conclude that X_k is empty for all odd $k \geq 3$ and only need to consider

$$k = 2^{\mu} \prod_{i=1}^{r} p_i^{a_i},$$

where μ is a positive integer, $p_1 < p_2 < \cdots < p_r$ are odd prime numbers, and a_i are positive integers for all $i = 1, 2, \ldots, r$. Note that this does not imply that $X_k \neq \{\}$ if k is an even positive integer. It can be seen directly in Table 1 that there are even integers for which $X_k = \{\}$; the smallest of these is $k = 14$.

Table 1. $X_k = \{n \in \mathbb{N} : \varphi(n) = k\}$ for all $k \leq 50$

$\boldsymbol{k}$	$\lvert \boldsymbol{X_k} \rvert$	$\boldsymbol{X_k}$
1	2	$\{1, 2\}$
2	3	$\{3, 4, 6\}$
4	4	$\{5, 8, 10, 12\}$
6	4	$\{7, 9, 14, 18\}$
8	5	$\{15, 16, 20, 24, 30\}$
10	2	$\{11, 22\}$
12	6	$\{13, 21, 26, 28, 36, 42\}$
14	0	$\varnothing \equiv \{\}$
16	6	$\{17, 32, 34, 40, 48, 60\}$
18	4	$\{19, 27, 38, 54\}$
20	5	$\{25, 33, 44, 50, 66\}$
22	2	$\{23, 46\}$
24	10	$\{35, 39, 45, 52, 56, 70, 72, 78, 84, 90\}$
26	0	$\varnothing$
28	2	$\{29, 58\}$
30	2	$\{31, 62\}$
32	7	$\{51, 64, 68, 80, 96, 102, 120\}$
34	0	$\varnothing$
36	8	$\{37, 57, 63, 74, 76, 108, 114, 126\}$
38	0	$\varnothing$
40	9	$\{41, 55, 75, 82, 88, 100, 110, 132, 150\}$
42	4	$\{43, 49, 86, 98\}$
44	3	$\{69, 92, 138\}$
46	2	$\{47, 94\}$
48	11	$\{65, 104, 105, 112, 130, 140, 144, 156, 168, 180, 210\}$
50	0	$\varnothing$

Furthermore, the question of which positive integers k for which X_k is empty has been answered by Vassilev-Missana in [31]. The result is the following:

“ **Theorem 2.** *When the number A is given by*

$$A = 2^g \cdot \prod_{i=1}^{r} q_i^{B_i},$$

$g = 1$ and $r \geq 2$, then the equation $\varphi(x) = A$ does not have solutions iff the following two conditions are valid simultaneously:

1. $q_r \neq A/q_r^{B_r} + 1$
2. *The number $A + 1$ is a composite one.* ”

From Proposition 1.1.3 and Table 1, we have the following observations.

Proposition 1.1.9. *For any prime number x or $x = 1$ and for any prime number $p \neq x$, we have the following chain for the pairs $(x, (p-1)p^i k)$, where $k = \varphi(x)$ and $i = 0, 1, 2, \dots$:*

$$\begin{array}{r|llllll} x & px & p^2x & p^3x & p^4x & \cdots \\ k = \varphi(x) & (p-1)k & (p-1)pk & (p-1)p^2k & (p-1)p^3k & \cdots \end{array}. \tag{1}$$

Proof. Let p be a prime number, and let $x \neq p$ be a prime number or $x = 1$. Since φ is multiplicative, we have $\varphi(p^\alpha x) = \varphi(p^\alpha)\varphi(x) = (p-1)p^{\alpha-1}\varphi(x)$, which implies chart (1). □

Example 1.1. If $x = 1$ and $p = 2$, then $\varphi(1) = 1$ and

$$\begin{array}{r|llllllll} \alpha & 0 & 1 & 2 & 3 & 4 & 5 & 6 & \cdots \\ 2^\alpha \cdot 1 & 1 & 2 & 4 & 8 & 16 & 32 & 64 & \cdots \\ \varphi(2^\alpha) & 1 & 1 & 2 & 4 & 8 & 16 & 32 & \cdots \end{array}. \tag{2}$$

If $x = 1$ and $p = 3$, then $\varphi(1) = 1$ and

$$\begin{array}{r|lllllll} \alpha & 0 & 1 & 2 & 3 & 4 & 5 & \cdots \\ 3^\alpha \cdot 1 & 1 & 3 & 9 & 27 & 81 & 243 & \cdots \\ \varphi(3^\alpha) & 1 & 2 & 6 & 18 & 54 & 162 & \cdots \end{array}. \tag{3}$$

If $x = 2$ and $p = 3$, then $\varphi(2) = 1$ and

$$\begin{array}{r|llllll} \alpha & 0 & 1 & 2 & 3 & 4 & \cdots \\ 3^\alpha \cdot 2 & 2 & 6 & 18 & 54 & 162 & \cdots \\ \varphi(3^\alpha \cdot 2) & 1 & 2 & 6 & 18 & 54 & \cdots \end{array}. \tag{4}$$

Proposition 1.1.10. *For any positive integers $x = \Pi_{i=1}^r p_i^{\alpha_i}$ and $y = \Pi_{i=1}^r p_i^{\beta_i}$, where $\alpha_i \geq 1$ and $\beta_i \geq 0$, we have*

$$\varphi(xy) = y\varphi(x). \tag{5}$$

Proof. It is sufficient to prove (5) for $y = p_j$, where $1 \leq j \leq r$. From Proposition 1.1.3, we have

$$\varphi(xp_j) = p_j x \Pi_{i=1}^r \left(1 - \frac{1}{p_i}\right) = p_j \varphi(x).$$ □

In Proposition 1.1.10, we do not need $y \mid x$; instead, we only need that each prime factor of y is also a prime factor of x. In particular, if $y \mid x$, we immediately have the following corollary.

Corollary 1.1.11. *For any positive integers x and t with $t \mid x$, we have $\varphi(tx) = t\varphi(x)$.*

Example 1.2. Let $\varphi(x) = k$, and let $t \mid x$. Then

$$\begin{array}{r|llllll} \alpha & 0 & 1 & 2 & 3 & 4 & \cdots \\ t^\alpha \cdot x & x & tx & t^2x & t^3x & t^4x & \cdots \\ \varphi(t^\alpha \cdot x) & k & tk & t^2k & t^3k & t^4k & \cdots \end{array}. \tag{6}$$

In particular, if $t = x$, then

$$\begin{array}{r|llllll} \alpha & 1 & 2 & 3 & 4 & 5 & \cdots \\ x^\alpha & x & x^2 & x^3 & x^4 & x^5 & \cdots \\ \varphi(x^\alpha) & k & xk & x^2k & x^3k & x^4k & \cdots . \end{array} \tag{7}$$

Theorem 1.1.12. *Fix an arbitrary $k \in \mathbb{N}$. Let $n \in X_k$ and $c \in \mathbb{N}$ such that $c|n$ and $c|k$. Then:*

(i) $\varphi(cn) = ck,$ *and*

(ii) $\varphi\left(\frac{n}{c}\right) = \frac{k}{c}$ *whenever* $c|\frac{n}{c}$ *and* $2|\frac{k}{c}$.

Proof. Part (i) follows directly from Corollary 1.1.11. To see this, identify t in the corollary with c of the theorem.

To show part (ii), we use Proposition 1.1.5. We write

$$\varphi(n) = \varphi\left(\frac{c}{c} \cdot n\right) = \varphi\left(c \cdot \frac{n}{c}\right).$$

Since $c|n$, we have $\frac{n}{c}$ is a positive integer. Since $c|\frac{n}{c}$, we have $\gcd\left(c, \frac{n}{c}\right) = c$. Then by Proposition 1.1.5,

$$\varphi\left(c \cdot \frac{n}{c}\right) = c \cdot \frac{\varphi(c)\varphi\left(\frac{n}{c}\right)}{\varphi(c)} = c \cdot \varphi\left(\frac{n}{c}\right).$$

Thus,

$$\varphi(n) = c \cdot \varphi\left(\frac{n}{c}\right) = k,$$

or equivalently,

$$\varphi\left(\frac{n}{c}\right) = \frac{k}{c}$$

as desired. □

Example 1.3 Consider $X_{24} = \{35, 39, 45, 52, 56, 70, 72, 78, 84, 90\}$. Here $k = 24$.

a. Let $n = 84$ and $c = 4$. We have $c|n$ and $c|k$. Since $\varphi(n) = 24$, we conclude $\varphi(cn) = \varphi(336) = 96 = ck$ by part (i) of the theorem.

b. Let $n = 72$ and $c = 2$. We have $c|n$, $c|k$, $\frac{n}{c} = 36$, and $\frac{k}{c} = 12$. Since $c|\frac{n}{c}$ and $2|\frac{k}{c}$, we conclude that $\varphi(36) = 12$ by part (ii) of the theorem.

c. Let $n = 90$ and $c = 3$. We have $c|n$, $c|k$, $\frac{n}{c} = 30$, and $\frac{k}{c} = 8$. Since $c|\frac{n}{c}$ and $2|\frac{k}{c}$, we conclude that $\varphi(30) = 8$ by part (ii) of the theorem.

2 Main results

Fix a positive integer k. Given the equation $\varphi(n) = k$, we aim to determine the set

$$X_k = \{n \in \mathbb{N} : \varphi(n) = k\}$$

and provide conditions for which it is empty.

In [8], Hansraj Gupta shows that any nonempty set X_k is bounded both above and below. We state these results as Propositions 2.0.1 and 2.0.2.

Proposition 2.0.1. *Let k be a positive integer and p a prime number. Define*

$$U(k) = k \cdot \prod_{(p-1)|k} \frac{p}{p-1}.$$

If $x \in X_k$, then $k \leqq x \leqq U(k)$.

Proof. Let $x \in X_k$. We have $k \leqq x$ by the definition of X_k. From Corollary 1.1.4, it follows that

$$\frac{x}{\varphi(x)} = \prod_{p|x} \frac{p}{p-1}.$$

If $p \mid x$, then $\varphi(p) \mid \varphi(x)$; that is, $p-1 \mid k$. However, if $p-1 \mid k$, then p may or may not divide x. Hence,

$$\prod_{p|x} \frac{p}{p-1} \leqq \prod_{p-1|k} \frac{p}{p-1},$$

and so

$$\frac{x}{\varphi(x)} \leqq \prod_{p-1|k} \frac{p}{p-1}.$$

Multiplying both sides of the inequality by k, we obtain $x \leqq U(k)$ as desired. □

Proposition 2.0.2. *Let P_j denote the product of the first j prime numbers. If $x \in X_k$ and $P_j \leqq x < P_{j+1}$, then $x \leqq k \cdot \frac{P_j}{(p_1-1)(p_2-1)(p_3-1)\cdots(p_j-1)}$.*

Proof. Let $x \in X_k$ such that $P_j \leqq x < P_{j+1}$. From Corollary 1.1.4, it follows that

$$\frac{x}{\varphi(x)} = \prod_{p|x} \frac{p}{p-1}.$$

Since

$$\prod_{p|x} \frac{p}{p-1} \leqq \frac{P_j}{(p_1-1)(p_2-1)(p_3-1)\cdots(p_j-1)},$$

we have the desired inequality after multiplying both sides by k. □

In this way, X_k can be determined by calculating $\varphi(x)$ for each x in the range of $k \leqq x \leqq U(k)$. Another method proposed by Gupta utilizes the sets $X_{k/\varphi(p^d)}$; see Section 4 in [8]. However, this requires that X_i are available for all $i < k$.

In what follows, we offer another approach by considering the arbitrary prime-power factorization of k and checking the prime combinations for a solution n.

2.1 Case 1: The set X_{2^t} and Fermat primes

Suppose that we are tasked to find all positive integers n such that $\varphi(n) = 2^t$ for some positive integer t. Then, as in Corollary 1.1.4 with the identification $\varphi(n) = 2^t$, n satisfies

$$n = \frac{2^t}{(p_1-1)(p_2-1)\cdots(p_r-1)} \cdot p_1 p_2 \cdots p_r.$$

From here, we can find candidates for $d_i = p_i - 1$ and hence for p_i. For each p_i, it follows that $p_i - 1 \mid 2^t$ by Proposition 1.1.5. Then, the aforementioned candidates are $d_1 = 1$, $d_2 = 2$, and, in general, $d_i = 2^{\alpha_i}$, where $\alpha_i = 0, 1, \dots, t$. The same $p_i = d_i + 1$ must be prime. Hence, $p_1 = 2$, $p_2 = 3$, and, in general, $p_i = 2^{\alpha_i} + 1$. In summary, we have

$$n = 2^s \prod_{i=1}^{r} \left(2^{\alpha_i} + 1\right),$$

where $s \geqq 0$ and $2^{\alpha_i} + 1$ is a prime number.

Furthermore, it is known that if $2^{\alpha_i} + 1$ is a prime number and $\alpha_i > 0$, then α_i must be a power of two, and so $2^{\alpha_i} + 1$ are Fermat primes [2]. The only known Fermat primes are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$. Therefore, n may be written as

$$n = 2^a \cdot F_0^b \cdot F_1^c \cdot F_2^d \cdot F_3^e \cdot F_4^f = 2^a \cdot 3^b \cdot 5^c \cdot 17^d \cdot 257^e \cdot 65537^f, \tag{1}$$

where $0 \leqq a \leqq t + 1$, and $b, c, d, e, f \in \{0, 1\}$.

Let us assume that n is of the form (1). Then, for each integer a in the range of $0 \leqq a \leqq t+1$, we can obtain a Diophantine equation corresponding to exactly one value of n as follows:

If $a = 0$, then

$$\begin{aligned} 2^t = \varphi(n) &= \varphi\left(2^a \cdot 3^b \cdot 5^c \cdot 17^d \cdot 257^e \cdot 65537^f\right) \\ &= \varphi\left(3^b\right) \cdot \varphi\left(5^c\right) \cdot \varphi\left(17^d\right) \cdot \varphi\left(257^e\right) \cdot \varphi\left(65537^f\right) \\ &= 2^{2^0 b} \cdot 2^{2^1 c} \cdot 2^{2^2 d} \cdot 2^{2^3 e} \cdot 2^{2^4 f} \\ &= 2^b \cdot 2^{2c} \cdot 2^{4d} \cdot 2^{8e} \cdot 2^{16f} \\ &= 2^{b+2c+4d+8e+16f}, \end{aligned}$$

yielding the Diophantine equation

$$t = b + 2c + 4d + 8e + 16f. \tag{2}$$

The solution to this equation provides the odd element of X_{2^t} whereas the next provides the even elements.

If $0 < a \leqq t + 1$, then

$$\begin{aligned} 2^t = \varphi(n) &= \varphi\left(2^a \cdot 3^b \cdot 5^c \cdot 17^d \cdot 257^e \cdot 65537^f\right) \\ &= \varphi\left(2^a\right) \cdot \varphi\left(3^b\right) \cdot \varphi\left(5^c\right) \cdot \varphi\left(17^d\right) \cdot \varphi\left(257^e\right) \cdot \varphi\left(65537^f\right) \\ &= 2^{a-1} \cdot 2^{2^0 b} \cdot 2^{2^1 c} \cdot 2^{2^2 d} \cdot 2^{2^3 e} \cdot 2^{2^4 f} \\ &= 2^{a-1} \cdot 2^b \cdot 2^{2c} \cdot 2^{4d} \cdot 2^{8e} \cdot 2^{16f} \\ &= 2^{(a-1)+b+2c+4d+8e+16f}, \end{aligned}$$

yielding the Diophantine equation

$$t = (a - 1) + b + 2c + 4d + 8e + 16f. \tag{3}$$

Therefore, we have a method to determine $t + 2$ distinct values for n, one of which is odd and the remaining $t + 1$ are even. This verifies with the result of [7] that $|X_{2^t}| = \min\{t + 2, 32\}$.

The following example demonstrates how we identify X_{2^t} using (1), (2), and (3).

Example 2.1. Let us identify X_{512}. Noting that $512 = 2^9$, by (1), $n \in X_{512}$ is of the form

$$n = 2^a \cdot 3^b \cdot 5^c \cdot 17^d \cdot 257^e,$$

where $0 \leqq a \leqq 10$ and $b, c, d, e \in \{0, 1\}$. If $a = 0$, then by (2),

$$b + 2c + 4d + 8e = 9,$$

which has the solution $b = e = 1$, $c = d = 0$. This implies that $n = 3^1 \cdot 257^1 = 771$. If $a = 1$, then by (3)

$$b + 2c + 4d + 8e = 9,$$

which has the solution $b = e = 1$, $c = d = 0$. This implies that $n = 2^1 \cdot 3^1 \cdot 257^1 = 1542$. If $a = 2$, then by (3)

$$b + 2c + 4d + 8e = 8,$$

which has the solution $b = c = d = 0$, $e = 1$. This implies that $n = 2^2 \cdot 257^1 = 1028$. If $a = 3$, then by (3)

$$b + 2c + 4d + 8e = 7,$$

which has the solution $b = c = d = 1$, $e = 0$. This implies that $n = 2^3 \cdot 3^1 \cdot 5^1 \cdot 16^1 = 2040$. If $a = 4$, then by (3),

$$b + 2c + 4d + 8e = 6,$$

which has the solution $b = e = 0$, $c = d = 1$. This implies that $n = 2^4 \cdot 5^1 \cdot 17^1 = 1360$. If $a = 5$, then by (3),

$$b + 2c + 4d + 8e = 5,$$

which has the solution $b = c = 1$, $d = e = 0$. This implies that $n = 2^5 \cdot 3^1 \cdot 17^1 = 1632$. If $a = 6$, then by (3),

$$b + 2c + 4d + 8e = 4,$$

which has the solution $b = c = e = 0$, $d = 1$. This implies that $n = 2^6 \cdot 17^1 = 1088$. If $a = 7$, then by (3)

$$b + 2c + 4d + 8e = 3,$$

which has the solution $b = c = 1$, $d = e = 0$. This implies that $n = 2^7 \cdot 3^1 \cdot 5^1 = 1920$. If $a = 8$, then by (3),

$$b + 2c + 4d + 8e = 2,$$

which has the solution $b = d = e = 0$, $c = 1$. This implies that $n = 2^8 \cdot 5^1 = 1280$. If $a = 9$, then by (3)

$$b + 2c + 4d + 8e = 1,$$

which has the solution $b = 1$, $c = d = e = 0$. This implies that $n = 2^9 \cdot 3^1 = 1536$. If $a = 10$, then by (3)

$$b + 2c + 4d + 8e = 0,$$

which has the solution $b = c = d = e = 0$. This implies that $n = 2^{10} = 1024$.

Algorithms

Given a positive integer t, we can now identify the set X_{2^t} by solving (2) and (3) for all a in the range of $0 \leqq a \leqq t+1$. The following Algorithm 1 is our initial attempt to find all such solutions.

Input: An empty list N and a positive integer t.

Algorithm 1 preimageEulerPhi $(N,\ t)$

```
1:  for a ← 0 to t + 1 do
2:      // Assumes a solution to (2) or (3) exists and finds by brute force
3:      for f ← 0, 1 do
4:          for e ← 0, 1 do
5:              for d ← 0, 1 do
6:                  for c ← 0, 1 do
7:                      for b ← 0, 1 do
8:                          if a, b, c, d, e, f satisfies (2) or (3) then
9:                              n ← 2^a · 3^b · 5^c · 17^d · 257^e · 65537^f
10:                             Append n to N
11:                             goto label
12:                         end if
13:                     end for
14:                 end for
15:             end for
16:         end for
17:     end for
18:     label
19: end for
```

We observe that $t = b+2c+4d+8e+16f \leqq 31$ and $t-(a-1) = b+2c+4d+8e+16f \leqq 31$ because $b, c, d, e, f \in \{0,1\}$. Hence, (2) and (3) have solutions whenever

(i) $a = 0$ and $t \leqq 31$ **and** (ii) $0 < a \leqq t+1$ and $t-(a-1) \leqq 31$, respectively.

This means that we are performing excess checks if $t > 31$. We modify Algorithm 1 in the following way to reduce this number.

Algorithm 2 preimageEulerPhi $(N,\ t)$

```
for a ← 0 to t + 1 do
    if [a == 0 and t ≦ 31] or [a ≦ t + 1 and t − (a − 1) ≦ 31] then    ▷ Modification
        Algorithm 1                                                    ▷ Lines 2 through 18
    end if
end for
```

We next visit a familiar problem. Recall the 0/1 knapsack problem, that is, given a set of positive integers $a_1, a_2, \ldots, a_n$ and an integer s, we want to find $x_1, x_2, \ldots, x_n \in \{0, 1\}$ such that

$$s = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

With this in mind, we see that the problems posed in (2) and (3) are, in fact, $0/1$ knapsack problems. In Algorithms 1 and 2, we solved these by implementing a brute-force method. Alternatively, we observe that the sequence $(a_n) = (1,\ 2,\ 4,\ 8,\ 16)$ satisfies the inequality

$$\sum_{i=1}^{j-1} a_i < a_j \quad \text{for all } j = 2, 3, \ldots, n.$$

This means that (a_n) is a super-increasing sequence. Rosen [23] provides an algorithm to easily solve knapsack problems for such sequences. We implement it as follows in Algorithm 3.

Input: A list A whose elements are the terms of a super-increasing sequence (in increasing order), positive integers s and n, which are the sum and number of terms in the sequence, respectively, and an empty list X that will contain the solution $x_1, x_2, \ldots, x_n$.

Algorithm 3 knapsackSuperInc $(A,\ s,\ n,\ X)$

```
if A[n] ≤ s then
    X[n] ← 1
else
    X[n] ← 0
end if
for j ← n − 1 to 1 do
    if A[j] ≤ s − ∑_{i=j+1}^{n} X[i] A[i] then
        X[j] ← 1
    else
        X[j] ← 0
    end if
end for
```

Then, we further modify our Algorithm 2 by replacing the brute-force method of Algorithm 1 with Algorithm 3. See Algorithm 4.

Algorithm 4 preimageEulerPhi $(N,\ t)$

```
A = (1, 2, 4, 8, 16)
Declare an array X of 5 integers
for a ← 0 to t + 1 do
    if [a == 0 and t ≤ 31] or [a ≤ t + 1 and t − (a − 1) ≤ 31] then
        if a == 0 then
            knapsackSuperInc(A, t, 5, X)
        else
            knapsackSuperInc(A, t − a + 1, 5, X)
        end if
        n ← 2^a · 3^X[1] · 5^X[2] · 17^X[3] · 257^X[4] · 65537^X[5]
        Append n to N
    end if
end for
```

Lastly, we note that solving equations (2) and (3) is akin to finding the base-2 representations of t and $t - a + 1$, respectively. That is to say, this representation returns b, c, d, e, and f, the same array of integers X from Algorithm 4. Consequently, we may interchange the knapsack super-increasing sequence method with another base-10 to base-2 conversion method.

We conclude this section with some further results about the set X_{2^t}.

Theorem 2.1.2. *If $n \in X_{2^t}$ and n is an even number, then $2n \in X_{2^{t+1}}$, and conversely.*

Proof. Since $\gcd(2, n) = 2$, we have $\varphi(2n) = 2\varphi(n) = 2^{t+1}$. □

Remark 1. *This can alternatively be seen as a corollary of the previous result. See Corollary 1.1.11.*

Assume that we have the set X_{2^t} available. Then, using Theorem 2.1.2, we can find *most* even elements of $X_{2^{t+1}}$. To find the odd element, set $a = 0$ in (2). Then, the remaining even element is found using Proposition 1.1.7. We demonstrate this in the next example.

Example 2.2. We begin by considering $X_1 = \{1, 2\}$. $2 \in X_2$, so $4 \in X_2$. Solving (2) with $t = 1$, we find $3 \in X_2$. Then $6 \in X_2$. Thus, $X_2 = \{3, 4, 6\}$.

$4, 6 \in X_2$, so $8, 12 \in X_4$. Solving (2) with $t = 2$, we find $5 \in X_4$. Then $10 \in X_4$. Thus, $X_4 = \{5, 8, 10, 12\}$.

$8, 10, 12 \in X_4$, so $16, 20, 24 \in X_8$. Solving (2) with $t = 3$, we find $15 \in X_8$. Then $30 \in X_8$. Thus, $X_8 = \{15, 16, 20, 24, 30\}$.

$16, 20, 24, 30 \in X_8$, so $32, 40, 48, 60 \in X_{16}$. Solving (2) with $t = 4$, we find $17 \in X_{16}$. Then $34 \in X_{16}$. Thus, $X_{16} = \{17, 32, 34, 40, 48, 60\}$.

More generally, we have

Theorem 2.1.4. *If $n \in X_{2^t}$ and n is an even number, then $2^a \cdot n \in X_{2^{a+t}}$ for all $1 \leqq a \leqq t$.*

Proof. Let $d = \gcd(2^a, m)$. Since m is an even number, we can write $m = 2^k b$, where $k \in \mathbb{N}$ and $\gcd(2, b) = 1$. Notice that $d = \min\{2^a, 2^k\}$. If $d = 2^a$, then

$$\varphi(2^a \cdot m) = d \cdot \frac{\varphi(2^a)\varphi(m)}{\varphi(d)} = 2^a \cdot \frac{2^{a-1} \cdot 2^t}{2^{a-1}} = 2^{a+t}.$$

If $d = 2^k$, then

$$\varphi(2^a \cdot m) = d \cdot \frac{\varphi(2^a)\varphi(m)}{\varphi(d)} = 2^k \cdot \frac{2^{a-1} \cdot 2^t}{2^{k-1}} = 2^{a+t}.$$

□

2.2 Case 2: The set X_{2p^s}

In this section, we investigate the set X_{2p^s} for some odd prime number p and positive integer s. Alois Pichler mentions [4] that $X_{2p^s} = \{\}$ for all positive integers s whenever $p > 3$ and $2p^s + 1$ is not prime. We verify this for X_{2p^s} for $s = 1,\ 2,\ 3,$ and 4 in the following theorems.

Theorem 2.2.1. *Let p be an odd prime number such that $p \neq 3$. If $2p + 1$ is prime, then $X_{2p} = \{2p + 1, 4p + 2\}$. If $2p + 1$ is not prime, then $X_{2p} = \{\}$.*

For the sake of completeness, in the case that $p = 3$, we have $X_6 = \{7, 9, 14, 18\}$.

Proof. Let p be an odd prime number such that $p \neq 3$. Suppose that $2p + 1$ is prime. If $X_{2p} \neq \{\}$, then there exists an $n \in X_{2p}$ such that $\varphi(n) = 2p$. Then, as in Corollary 1.1.4 with the identification $\varphi(n) = 2p$, n satisfies

$$n = \frac{2p}{(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)} \cdot p_1 p_2 \cdots p_r.$$

From here, we can find candidates for $d_i = p_i - 1$ and hence for p_i. For each p_i, it follows that $p_i - 1 \mid 2p$ by Proposition 1.1.5. We look to the positive divisors of $2p$ (that is, $1, 2, p,$ and $2p$). Then, the aforementioned candidates are $d_1 = 1$, $d_2 = 2$, $d_3 = p$, and $d_4 = 2p$. The same $p_i = d_i + 1$ must be prime. Hence, $p_1 = 2$, $p_2 = 3$, and $p_3 = 2p + 1$ are the candidate prime factors of n. This leads to the following cases:

i. If $p_1 = 2$ is the only prime factor of n, then

$$n = \frac{2p}{1} \cdot 2 = 2^2 \cdot p$$

so that

$$\begin{aligned} \varphi(n) &= \varphi(2^2 \cdot p) \\ &= \varphi(2^2) \cdot \varphi(p) \\ &= \left(2^2 - 2^1\right)(p - 1) \\ &= 2p - 2. \end{aligned}$$

Since $\varphi(n) = 2p$, we have $\varphi(n) = 2p = 2p - 2$, which implies that $0 = 2$. Hence, there is no such n.

ii. If $p_2 = 3$ is the only prime factor of n, then

$$n = \frac{2p}{2} \cdot 3 = 3 \cdot p$$

so that

$$\begin{aligned} \varphi(n) &= \varphi(3 \cdot p) \\ &= \varphi(3) \cdot \varphi(p) \qquad (p \neq 3) \\ &= (3-1)\,(p-1) \\ &= 2p - 2. \end{aligned}$$

Since $\varphi(n) = 2p$, we have $\varphi(n) = 2p = 2p - 2$, which implies that $0 = 2$. Hence, there is no such n.

iii. If $p_3 = 2p + 1$ is the only prime factor of n, then

$$n = \frac{2p}{2p} \cdot (2p+1) = \boxed{2p+1}$$

so that

$$\begin{aligned} \varphi(n) &= \varphi(2p+1) \\ &= 2p. \end{aligned}$$

iv. If $p_1 = 2$ and $p_2 = 3$ are the only prime factors of n, then

$$n = \frac{2p}{1 \cdot 2} \cdot (2 \cdot 3) = 2 \cdot 3 \cdot p$$

so that

$$\begin{aligned} \varphi(n) &= \varphi(2 \cdot 3 \cdot p) \\ &= \varphi(2) \cdot \varphi(3) \cdot \varphi(p) \qquad (p \neq 3) \\ &= (2-1)\,(3-1)(p-1) \\ &= 2p - 2. \end{aligned}$$

Since $\varphi(n) = 2p$, we have $\varphi(n) = 2p = 2p - 2$, which implies that $0 = 2$. Hence, there is no such n.

v. If $p_1 = 2$ and $p_2 = 2p + 1$ are the only prime factors of n, then

$$x = \frac{2p}{1 \cdot 2p} \cdot [2 \cdot (2p+1)] = 2 \cdot (2p+1) = \boxed{4p+2}$$

so that

$$\begin{aligned} \varphi(n) &= \varphi\left(2 \cdot (2p+1)\right) \\ &= \varphi(2) \cdot \varphi(2p+1) \\ &= (2-1)\,(2p+1-1) \\ &= 2p. \end{aligned}$$

vi. If $p_1 = 3$ and $p_2 = 2p + 1$ are the only prime factors of n, then

$$n = \frac{2p}{2 \cdot 2p} \cdot [3 \cdot (2p+1)] = \frac{1}{2} \cdot [3 \cdot (2q+1)],$$

which is a contradiction as $n \notin \mathbb{N}$. Hence, there is no such n.

vii. If $p_1 = 2$, $p_2 = 3$, and $p_3 = 2p + 1$ are the only prime factors of n, then

$$n = \frac{2p}{1 \cdot 2 \cdot 2p} \cdot [2 \cdot 3 \cdot (2p+1)] = 3 \cdot (2p+1)$$

so that

$$\begin{aligned} \varphi(n) &= \varphi(3 \cdot (2p+1)) \\ &= \varphi(3) \cdot \varphi(2p+1) \\ &= (3-1)(2p+1-1) \\ &= 4p. \end{aligned}$$

Since $\varphi(n) = 2p$, we have $\varphi(n) = 2p = 4p$, which implies that $p = 0$. This is a contradiction. Hence, there is no such n.

Thus, if $2p + 1$ is prime, then $n = 2p + 1$ or $n = 4p + 2$, that is, $X_{2p} = \{2p + 1, 4p + 2\}$. Otherwise, if $2p + 1$ is not prime, we may discard the cases assuming so, and observe that there are then no such n, that is, $X_{2p} = \{\}$. □

Next, we consider X_{2p^2}. Using the same method as in the proof of Theorem 2.2.1, we have

Theorem 2.2.2. *Let p be an odd prime number such that $p \neq 3$. If $2p^2 + 1$ is not prime, then $X_{2p^2} = \{\}$.*

Proof. Let p be an odd prime number such that $p \neq 3$. Suppose that $2p^2 + 1$ is not prime. For the sake of contradiction, suppose that $X_{2p^2} \neq \{\}$. Then, there exists an $n \in X_{2p^2}$ such that $\varphi(n) = 2p^2$. As in Corollary 1.1.4 with the identification $\varphi(n) = 2p^2$, n satisfies

$$n = \frac{2p^2}{(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)} \cdot p_1 p_2 \cdots p_r.$$

From here, we can find candidates for $d_i = p_i - 1$ and hence for p_i. For each p_i, it follows that $p_i - 1 \mid 2p^2$ by Proposition 1.1.5. We look to the positive divisors of $2p^2$ (that is, 1, 2, p, $2p$, p^2 and $2p^2$). Then, the aforementioned candidates are $d_1 = 1$, $d_2 = 2$, $d_3 = p$, $d_4 = 2p$, $d_5 = p^2$, and $d_6 = 2p^2$. The same $p_i = d_i + 1$ must be prime. Hence, $p_1 = 2$, $p_2 = 3$, and $p_3 = 2p + 1$ (provided that $2p + 1$ is prime) are the candidate prime factors of n. This leads to the following cases:

i. If $p_1 = 2$ is the only prime factor of n, then

$$n = \frac{2p^2}{1} \cdot 2 = 2^2 \cdot p^2$$

so that

$$\begin{aligned}\varphi(n) &= \varphi(2^2 \cdot p^2)\\ &= \varphi(2^2)\cdot\varphi(p^2)\\ &= \left(2^2-2^1\right)\left(p^2-p^1\right)\\ &= 2p^2-2p.\end{aligned}$$

Since $\varphi(n) = 2p^2$, we have $\varphi(n) = 2p^2 = 2p^2 - 2p$, which implies that $2p = 0$. This is a contradiction. Hence, there is no such n.

ii. If $p_1 = 3$ is the only prime factor of n, then

$$n = \frac{2p^2}{2}\cdot 3 = 3\cdot p^2$$

so that

$$\begin{aligned}\varphi(n) &= \varphi(3 \cdot p^2)\\ &= \varphi(3)\cdot\varphi(p^2)\\ &= (3-1)\left(p^2-p^1\right)\\ &= 2p^2-2p.\end{aligned}$$

Since $\varphi(n) = 2p^2$, we have $\varphi(n) = 2p^2 = 2p^2 - 2p$, which implies that $2p = 0$. This is a contradiction. Hence, there is no such n.

iii. If $p_1 = 2p+1$ is the only prime factor of n, then

$$n = \frac{2p^2}{2p}\cdot(2p+1) = p\cdot(2p+1)$$

so that

$$\begin{aligned}\varphi(n) &= \varphi\left(p\cdot(2p+1)\right)\\ &= \varphi(p)\cdot\varphi(2p+1)\\ &= (p-1)\left(2p+1-1\right)\\ &= (p-1)\cdot 2p\\ &= 2p^2-2p.\end{aligned}$$

Since $\varphi(n) = 2p^2$, we have $\varphi(n) = 2p^2 = 2p^2 - 2p$, which implies that $2p = 0$. This is a contradiction. Hence, there is no such n.

iv. If $p_1 = 2$ and $p_2 = 3$ are the only prime factors of n, then

$$n = \frac{2p^2}{1\cdot 2}\cdot(2\cdot 3) = 2\cdot 3\cdot p^2$$

so that

$$\begin{aligned}\varphi(n) &= \varphi\left(2\cdot 3\cdot p^2\right)\\ &= \varphi(2)\cdot\varphi(3)\cdot\varphi(p^2)\\ &= (2-1)\,(3-1)(p^2-p)\\ &= 2p^2-2p.\end{aligned}$$

Since $\varphi(n) = 2p^2$, we have $\varphi(n) = 2p^2 = 2p^2 - 2p$, which implies that $2p = 0$. This is a contradiction. Hence, there is no such n.

v. If $p_1 = 2$ and $p_2 = 2p+1$ are the only prime factors of n, then

$$n = \frac{2p^2}{1 \cdot 2p} \cdot [2 \cdot (2p+1)] = 2 \cdot p \cdot (2p+1)$$

so that

$$\begin{aligned}\varphi(n) &= \varphi\left(2 \cdot p \cdot (2p+1)\right) \\ &= \varphi(2) \cdot \phi(p) \cdot \varphi(2p+1) \\ &= (2-1)\,(p-1)(2p+1-1) \\ &= 2p^2 - 2p.\end{aligned}$$

Since $\varphi(n) = 2p^2$, we have $\varphi(n) = 2p^2 = 2p^2 - 2p$, which implies that $2p = 0$. This is a contradiction. Hence, there is no such n.

vi. If $p_1 = 3$ and $p_2 = 2p+1$ are the only prime factors of n, then

$$n = \frac{2p^2}{2 \cdot 2p} \cdot [3 \cdot (2p+1)] = \frac{p}{2} \cdot 3 \cdot (2p+1),$$

which is a contradiction as $n \notin \mathbb{N}$. Hence, there is no such n.

vii. If $p_1 = 2$, $p_2 = 3$, and $p_3 = 2p+1$ are the only prime factors of n, then

$$n = \frac{2p^2}{1 \cdot 2 \cdot 2p} \cdot [2 \cdot 3 \cdot (2p+1)] = 3 \cdot p \cdot (2p+1)$$

so that

$$\begin{aligned}\varphi(n) &= \varphi\left(3 \cdot p \cdot (2p+1)\right) \\ &= \varphi(3) \cdot \phi(p) \cdot \varphi(2p+1) \\ &= (3-1)\,(p-1)(2p+1-1) \\ &= 2\left(2p^2 - 2p\right) \\ &= 4p^2 - 4p.\end{aligned}$$

Since $\varphi(n) = 2p^2$, we have $\varphi(n) = 2p^2 = 4p^2 - 4p$, which implies that $2p^2 - 4p = 2p(p-2) = 0$. If $2p = 0$, we have a contradiction, and if $p = 2$, we have a contradiction. Hence, there is no such n.

Thus, $X_{2p^2} = \{\}$, which is a contradiction. We conclude that $X_{2p^2} = \{\}$. □

Proven similarly, we were able to show Theorems 2.2.3 and 2.2.4.

Theorem 2.2.3. *Let p be an odd prime number such that $p \neq 3$. If $2p^3 + 1$ is not prime, then $X_{2p^3} = \{\}$.*

Theorem 2.2.4. *Let p be an odd prime number such that $p \neq 3$. If $2p^4 + 1$ is not prime, then $X_{2p^4} = \{\}$.*

We conjecture that the result holds for all positive integers s. Related work can be seen in [19].

2.3 Case 3: The set X_{2^2p}

Theorem 2.3.1. *Let p be an odd prime number such that $p \equiv 1 \pmod 6$. If 2^2p+1 is prime, then $X_{2^2p} = \{2^2p+1, 2^3p+2\}$. If 2^2p+1 is not prime, then $X_{2^2p} = \{\}$.*

Proof. Let p be an odd prime number such that $p \equiv 1 \pmod 6$. Suppose that 2^2p+1 is prime. If $X_{2^2p} \neq \{\}$, then there exists an $n \in X_{2^2p}$ such that $\varphi(n) = 2^2p$. Then, as in Corollary 1.1.4 with the identification $\varphi(n) = 2^2p$, n satisfies

$$n = \frac{2^2p}{(p_1-1)(p_2-1)\cdots(p_r-1)} \cdot p_1p_2\cdots p_r.$$

From here, we can find candidates for $d_i = p_i - 1$ and hence for p_i. For each p_i, it follows that $p_i - 1 \mid 2^2p$ by Proposition 1.1.5. We look to the positive divisors of 2^2p (that is, 1, 2, p, 2^2, $2p$, and 2^2p). Then, the aforementioned candidates, are $d_1 = 1$, $d_2 = 2$, $d_3 = p$, $d_4 = 2^2$, $d_5 = 2p$, and $d_6 = 2^2p$. The same $p_i = d_i + 1$ must be prime. Hence, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and $p_4 = 2^2p + 1$ are the candidate prime factors of n.

As before, we next check every possible prime factor combination of n using the above candidates. There are $2^4 - 1 = 15$ such combinations. Let us see if we can lighten that a bit.

We observe that $2^2p + 1$ is the largest prime number whose totient is 2^2p. Hence, any n consisting of 2^2p+1 as a prime factor must either be identically 2^2p+1, or any additional prime factors must have a totient of one. Otherwise, $\varphi(n) > 2^2p$. Only the numbers one and two have this property, so we may safely disregard all combinations that include a prime factor of 2^2p+1 except for $n = 2^2p+1$ and $n = 2(2^2p+1)$. This leads to the following $2^3 - 1 + 2 = 9$ cases:

1. If $p_1 = 2$ is the only prime factor of n, then

$$n = \frac{2^2p}{1} \cdot 2 = 2^3p$$

so that

$$\begin{aligned}\varphi(n) &= \varphi\left(2^3p\right) \\ &= \varphi\left(2^3\right)\varphi\left(p\right) \\ &= 2^2\left(p-1\right).\end{aligned}$$

Since $\varphi(n) = 2^2p$, we have $\varphi(n) = 2^2p = 2^2(p-1)$, which implies that $0 = 1$. This is a contradiction. Hence, there is no such n.

2. If $p_1 = 3$ is the only prime factor of n, then

$$n = \frac{2^2p}{2} \cdot 3 = 2 \cdot 3 \cdot p,$$

so that

$$\begin{aligned}\varphi(n) &= \varphi\left(2 \cdot 3 \cdot p\right) \\ &= \varphi(2)\varphi\left(3\right)\varphi\left(p\right) \\ &= 2\left(p-1\right).\end{aligned}$$

Since $\varphi(n) = 2^2p$, we have $\varphi(n) = 2^2p = 2(p-1)$, which implies that $p = -1$. This is a contradiction. Hence, there is no such n.

3. If $p_1 = 5$ is the only prime factor of n, then

$$n = \frac{2^2 p}{4} \cdot 5 = 5p,$$

so that

$$\begin{aligned} \varphi(n) &= \varphi(5p) \\ &= \varphi(5)\varphi(p) \\ &= 2^2(p-1). \end{aligned}$$

Since $\varphi(n) = 2^2 p$, we have $\varphi(n) = 2^2 p = 2^2(p-1)$, which implies that $0 = 1$. This is a contradiction. Hence, there is no such n.

4. If $p_1 = 2^2 p + 1$ is the only prime factor of n, then

$$n = \frac{2^2 p}{2^2 p} \cdot \left(2^2 p + 1\right) = 2^2 p + 1,$$

so that

$$\begin{aligned} \varphi(n) &= \varphi\left(2^2 p + 1\right) \\ &= 2^2 p. \end{aligned}$$

Hence, $2^2 p + 1 \in X_{2^2 p}$.

5. If $p_1 = 2$ and $p_2 = 3$ are the only prime factors of n, then

$$n = \frac{2^2 p}{1 \cdot 2} \cdot 2 \cdot 3 = 2^2 \cdot 3 \cdot p$$

so that

$$\begin{aligned} \varphi(n) &= \varphi\left(2^2 \cdot 3 \cdot p\right) \\ &= \varphi\left(2^2\right)\varphi(3)\varphi(p) \\ &= 2^2(p-1). \end{aligned}$$

Since $\varphi(n) = 2^2 p$, we have $\varphi(n) = 2^2 p = 2^2(p-1)$, which implies that $0 = 1$. This is a contradiction. Hence, there is no such n.

6. If $p_1 = 2$ and $p_2 = 5$ are the only prime factors of n, then

$$n = \frac{2^2 p}{1 \cdot 4} \cdot 2 \cdot 5 = 2 \cdot 5 \cdot p$$

so that

$$\begin{aligned} \varphi(n) &= \varphi(2 \cdot 5 \cdot p) \\ &= \varphi(2)\varphi(5)\varphi(p) \\ &= 2^2(p-1). \end{aligned}$$

Since $\varphi(n) = 2^2 p$, we have $\varphi(n) = 2^2 p = 2^2(p-1)$, which implies that $0 = 1$. This is a contradiction. Hence, there is no such n.

7. If $p_1 = 2$ and $p_2 = 2^2p + 1$ are the only prime factors of n, then

$$n = \frac{2^2p}{1 \cdot 2^2p} \cdot 2\left(2^2p + 1\right) = 2\left(2^2p + 1\right)$$

so that

$$\begin{aligned}\varphi(n) &= \varphi\left(2\left(2^2p + 1\right)\right) \\ &= \varphi(2)\,\varphi\left(2^2p + 1\right) \\ &= 2^2p.\end{aligned}$$

Hence, $2\left(2^2p + 1\right) \in X_{2^2p}$.

8. If $p_1 = 3$ and $p_2 = 5$ are the only prime factors of n, then

$$n = \frac{2^2p}{2 \cdot 4} \cdot 3 \cdot 5 = \frac{p}{2} \cdot 3 \cdot 5,$$

which is a contradiction because $n \notin \mathbb{N}$. Hence, there is no such n.

9. If $p_1 = 2$, $p_2 = 3$, and $p_3 = 5$ are the only prime factors of n, then

$$n = \frac{2^2p}{1 \cdot 2 \cdot 4} \cdot 2 \cdot 3 \cdot 5 = 3 \cdot 5 \cdot p,$$

so that

$$\begin{aligned}\varphi(n) &= \varphi(3 \cdot 5 \cdot p) \\ &= \varphi(3)\,\varphi(5)\varphi(p) \\ &= 2^3(p - 1).\end{aligned}$$

Since $\varphi(n) = 2^2p$, we have $\varphi(n) = 2^2p = 2^3(p-1)$, which implies that $p = 2$. This is a contradiction. Hence, there is no such n.

We conclude that if $2^2p + 1$ is prime, then $X_{2^2p} = \{2^2p + 1, 2^3p + 2\}$, and if X_{2^2p} is not prime, then $X_{2^2p} = \{\}$. □

Example 2.3.

a. Take $p = 7$, then $2^2p = 28$. Note that $2^2p + 1 = 29$ is a prime number. Then $X_{2^2p} = \{29, 58\}$.
b. Take $p = 13$, then $2^2p = 52$. Note that $2^2p + 1 = 53$ is a prime number. Then $X_{2^2p} = \{53, 106\}$.
c. Take $p = 19$, then $2^2p = 76$. Note that $2^2p + 1 = 77$ is a composite number. Then $X_{2^2p} = \{\}$.
d. Take $p = 31$, then $2^2p = 124$. Note that $2^2p + 1 = 125$ is a composite number. Then $X_{2^2p} = \{\}$.

e. Take $p = 37$, then $2^2 p = 148$. Note that $2^2 p + 1 = 149$ is a prime number. Then $X_{2^2 p} = \{149, 298\}$.

f. Take $p = 43$, then $2^2 p = 172$. Note that $2^2 p + 1 = 173$ is a prime number. Then $X_{2^2 p} = \{173, 346\}$.

Criteria for which $X_{2^l q}$ is empty are given by Vassilev-Missana in [30]. See Theorem 2 on page 508.

2.4 Case 4: The set X_{2pq} and Germain primes

The following result verifies Carmichael's totient conjecture for $k = 2pq$, where p and q are odd prime numbers such that $p < q$. In proving so, we encounter the Germain primes, which further leads to some related results.

Theorem 2.4.1. *Let $k = 2pq$, where p and q are odd prime numbers such that $p < q$.*

a. If $q = 2p + 1$ is prime, then $q^2, 2q^2 \in X_k$.

b. If $2pq + 1$ is prime, then $2pq + 1, 2(2pq + 1) \in X_k$.

c. Otherwise, $X_k = \{\}$.

Proof. Let p and q be odd prime numbers such that $p < q$, and let $k = 2pq$. If $X_k \neq \{\}$, then there exists an $x \in X_k$ such that $\varphi(x) = 2pq$. Then, as in Corollary 1.1.4 with the identification $\varphi(x) = 2pq$, x satisfies

$$x = \frac{2pq}{(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)} \cdot p_1 p_2 \cdots p_r.$$

From here, we can find candidates for $d_i = p_i - 1$ and hence for p_i. For each p_i, it follows that $p_i - 1 \mid 2pq$ by Proposition 1.1.5. We look to the positive divisors of $2pq$ (that is, 1, 2, p, q, $2p$, $2q$, pq and $2pq$). Then, the aforementioned candidates, are $d_1 = 1$, $d_2 = 2$, $d_3 = p$, $d_4 = q$, $d_5 = 2p$, $d_6 = 2q$, $d_7 = pq$, and $d_8 = 2pq$. The same $p_i = d_i + 1$ must be prime. Hence, $p_1 = 2$, $p_2 = 3$, $p_3 = 2p + 1$, $p_4 = 2q + 1$, and $p_5 = 2pq + 1$ are the candidate prime factors of x.

As before, we next check every possible prime factor combination of x using the above candidates. There are $2^5 - 1 = 31$ such combinations. Let's see if we can lighten that a bit.

We observe that $2pq + 1$ is the largest prime number whose totient is $2pq$. Hence, any x consisting of $2pq + 1$ as a prime factor must either be identically $2pq + 1$, or any additional prime factors must have a totient of one. Otherwise, $\varphi(x) > 2pq$. Only the numbers one and two have this property, so we may safely disregard all combinations that include a prime factor of $2pq + 1$ except for $x = 2pq + 1$ and $x = 2(2pq + 1)$. Moving forward, we will further suppose that $2p + 1$, $2q + 1$, and $2pq + 1$ are prime. This leads to the following $2^4 - 1 + 2 = 17$ cases:

i. If $p_1 = 2$ is the only prime factor of x, then

$$x = \frac{2pq}{1} \cdot 2 = 2^2 pq,$$

so that

$$\begin{aligned}\varphi(x) &= \varphi\left(2^2pq\right)\\ &= \varphi\left(2^2\right)\varphi\left(p\right)\varphi(q)\\ &= 2\left(p-1\right)\left(q-1\right)\\ &= 2(pq-p-q+1).\end{aligned}$$

Since $\varphi(x) = 2pq$, we have $\varphi(x) = 2pq = 2(pq - p - q + 1)$, which implies that $p + q = 1$. This is a contradiction. Hence, there is no such x.

ii. If $p_1 = 3$ is the only prime factor of x, then

$$x = \frac{2pq}{2} \cdot 3 = 3pq,$$

so that

$$\begin{aligned}\varphi(x) &= \varphi\left(3pq\right)\\ &= \varphi\left(3\right)\varphi\left(p\right)\varphi(q)\\ &= 2\left(p-1\right)\left(q-1\right)\\ &= 2(pq-p-q+1).\end{aligned}$$

Since $\varphi(x) = 2pq$, we have $\varphi(x) = 2pq = 2(pq - p - q + 1)$, which implies that $p + q = 1$. This is a contradiction. Hence, there is no such x.

iii. If $p_1 = 2p + 1$ is the only prime factor of x, then

$$x = \frac{2pq}{2p} \cdot (2p+1) = q(2p+1).$$

It must be that $q = 2p + 1$. Then $x = (2p + 1)^2$, so

$$\begin{aligned}\varphi(x) &= \varphi\left((2p+1)^2\right)\\ &= (2p+1)^2 - (2p+1)\\ &= 4p^2 + 4p + 1 - 2p - 1\\ &= 2p(2p+1)\\ &= 2pq.\end{aligned}$$

Hence, $x = (2p + 1)^2 \in X_k$ if $q = 2p + 1$.

iv. If $p_1 = 2q + 1$ is the only prime factor of x, then

$$x = \frac{2pq}{2q} \cdot (2q+1) = p(2q+1).$$

This is the same case as before with p and q interchanged. Here, there will be a contradiction because we specified $p < q$.

v. If $p_1 = 2pq + 1$ is the only prime factor of x, then

$$x = \frac{2pq}{2pq} \cdot (2pq+1) = 2pq+1$$

so that

$$\begin{aligned}\varphi(x) &= \varphi\left(2pq+1\right)\\ &= 2pq.\end{aligned}$$

Hence, $x = 2pq+1 \in X_k$ if $2pq+1$ is prime.

vi. If $p_1 = 2$ and $p_2 = 3$ are the only prime factors of x, then

$$x = \frac{2pq}{1\cdot 2}\cdot 2(3) = 6pq.$$

It must be that $p = q = 3$, which is a contradiction. Hence, there are no such x.

vii. If $p_1 = 2$ and $p_2 = 2p+1$ are the only prime factors of x, then

$$x = \frac{2pq}{1\cdot 2p}\cdot 2(2p+1) = 2q(2p+1).$$

It must be that $q = 2p+1$. Then $x = 2(2p+1)^2$, so

$$\begin{aligned}\varphi(x) &= \varphi\left(2(2p+1)^2\right)\\ &= \varphi(2)\varphi\left((2p+1)^2\right)\\ &= (2p+1)^2 - (2p+1)\\ &= 4p^2+4p+1-2p-1\\ &= 2p(2p+1)\\ &= 2pq.\end{aligned}$$

Hence, $x = 2(2p+1)^2 \in X_k$ if $q = 2p+1$.

viii. If $p_1 = 2$ and $p_2 = 2q+1$ are the only prime factors of x, then

$$x = \frac{2pq}{1\cdot 2q}\cdot 2(2q+1) = 2p(2q+1).$$

This is the same case as before with p and q interchanged. Here, there will be a contradiction because we specified $p < q$.

ix. If $p_1 = 2$ and $p_2 = 2pq+1$ are the only prime factors of x, then

$$x = \frac{2pq}{1\cdot 2pq}\cdot 2(2pq+1) = 2(2pq+1),$$

so that

$$\begin{aligned}\varphi(x) &= \varphi\left(2(2pq+1)\right)\\ &= \varphi(2)\varphi\left(2pq+1\right)\\ &= 2pq.\end{aligned}$$

Hence, $x = 2(2pq+1) \in X_k$ if $2pq+1$ is prime.

x. If $p_1 = 3$ and $p_2 = 2p+1$ are the only prime factors of x, then

$$x = \frac{2pq}{2\cdot 2p}\cdot 3(2p+1) = \frac{q}{2}\cdot 3(2p+1),$$

which is a contradiction because $\frac{q}{2} \notin \mathbb{N}$. Hence, there is no such x.

xi. If $p_1 = 3$ and $p_2 = 2q+1$ are the only prime factors of x, then

$$x = \frac{2pq}{2 \cdot 2q} \cdot 3(2q+1) = \frac{p}{2} \cdot 3(2q+1),$$

which is a contradiction because $\frac{p}{2} \notin \mathbb{N}$. Hence, there is no such x.

xii. If $p_1 = 2p+1$ and $p_2 = 2q+1$ are the only prime factors of x, then

$$x = \frac{2pq}{2p \cdot 2q} \cdot (2p+1)(2q+1) = \frac{1}{2} \cdot (2p+1)(2q+1)$$

which is a contradiction because $\frac{1}{2} \notin \mathbb{N}$. Hence, there is no such x.

xiii. If $p_1 = 2$, $p_2 = 3$, and $p_3 = 2p+1$ are the only prime factors of x, then

$$x = \frac{2pq}{1 \cdot 2 \cdot 2p} \cdot 2(3)(2p+1) = \frac{q}{2} \cdot 2(3)(2p+1),$$

which is a contradiction because $\frac{q}{2} \notin \mathbb{N}$. Hence, there is no such x.

xiv. If $p_1 = 2$, $p_2 = 3$, and $p_3 = 2q+1$ are the only prime factors of x, then

$$x = \frac{2pq}{1 \cdot 2 \cdot 2q} \cdot 2(3)(2q+1) = \frac{p}{2} \cdot 2(3)(2q+1),$$

which is a contradiction because $\frac{p}{2} \notin \mathbb{N}$. Hence, there is no such x.

xv. If $p_1 = 2$, $p_2 = 2p+1$, and $p_3 = 2q+1$ are the only prime factors of x, then

$$x = \frac{2pq}{1 \cdot 2p \cdot 2q} \cdot 2(2p+1)(2q+1) = \frac{1}{2} \cdot 2(2p+1)(2q+1),$$

which is a contradiction because $\frac{1}{2} \notin \mathbb{N}$. Hence, there is no such x.

xvi. If $p_1 = 3$, $p_2 = 2p+1$, and $p_3 = 2q+1$ are the only prime factors of x, then

$$x = \frac{2pq}{2 \cdot 2p \cdot 2q} \cdot 3(2p+1)(2q+1) = \frac{1}{4} \cdot 3(2p+1)(2q+1),$$

which is a contradiction because $\frac{1}{4} \notin \mathbb{N}$. Hence, there is no such x.

xvii. If $p_1 = 2$, $p_2 = 3$, $p_3 = 2p+1$, and $p_4 = 2q+1$ are the only prime factors of x, then

$$x = \frac{2pq}{1 \cdot 2 \cdot 2p \cdot 2q} \cdot 2(3)(2p+1)(2q+1) = \frac{1}{4} \cdot 2(3)(2p+1)(2q+1),$$

which is a contradiction because $\frac{1}{4} \notin \mathbb{N}$. Hence, there is no such x.

We conclude that

a. $q^2, 2q^2 \in X_k$ if $q = 2p+1$ is prime,

b. $2pq+1, 2(2pq+1) \in X_k$ if $2pq+1$ is prime, and

c. $X_k = \{\}$, otherwise. □

Theorem 2.4.2. *Let p be a Germain prime such that $p \geq 5$, and $k = 2p(2p+1)$. Then $k+1$ is composite.*

Proof. Let p be a Germain prime such that $p \geq 5$, and $k = 2p(2p+1)$. It is known from Forgues [27] that p is 2, 3, or $p \equiv 5 \pmod 6$. Then

$$\begin{aligned} k+1 &= 2p(2p+1)+1 \\ &= 4p^2+2p+1 \\ &\equiv 4+4+1 \pmod 6 \\ &\equiv 3 \pmod 6. \end{aligned}$$

Thus, $k+1 = 6m+3 = 3(2m+1)$, where $m \in \mathbb{N}$; that is, 3 divides $k+1$. □

An immediate consequence of Theorem 2.4.2 is that the only instance of $\left|X_{2p(2p+1)}\right| = 4$ comes from the Germain prime $p = 3$. See example (d), where $k = 42$.

Example 2.4.

a. Let $p = 23$ and $q = 47$. Then $k = 2pq = 2162$. We have $2p+1 = 47 = q$ is prime, and $2pq+1 = 2163$ is composite. Thus,

$$X_k = \left\{q^2, 2q^2\right\} = \{2209, 4418\}.$$

b. Let $p = 19$ and $q = 29$. Then $k = 2pq = 1102$. We have $2p+1 = 39 \neq q$ is composite, and $2pq+1 = 1103$ is prime. Thus,

$$X_k = \{2pq+1, 2(2pq+1)\} = \{1103, 2206\}.$$

c. Let $p = 7$ and $q = 13$. Then $k = 2pq = 182$. We have $2p+1 = 15 \neq q$ is composite, and $2pq+1 = 183$ is composite. Thus,

$$X_k = \{\}.$$

d. Let $p = 3$ and $q = 7$. Then $k = 2pq = 42$. We have $2p+1 = 7 = q$ is prime, and $2pq+1 = 43$ is prime. Thus,

$$X_k = \left\{q^2, 2q^2, (2pq+1), 2(2pq+1)\right\} = \{49, 98, 43, 86\}.$$

Next, we attempt to generalize the result of Theorem 2.4.1. Let p be an odd prime number. Additionally, let p and $2p+1$ be Germain primes. Then, $2p+1$ and $4p+3$ are prime numbers. Consider

$$k = 2^2 \cdot p \cdot (2p+1) \cdot (4p+3) = 4 \cdot p \cdot (2p+1) \cdot (4p+3),$$

and let $x = (4p+3)^2 \cdot (2p+1)$. Then

$$\begin{aligned}\varphi(x) &= \left[(4p+3)^2-(4p+3)\right]\cdot 2p\\ &= (4p+3)\cdot(4p+2)\cdot 2p\\ &= 2^2\cdot p\cdot(2p+1)\cdot(4p+3)\\ &= k.\end{aligned}$$

Hence, $(4p+3)^2\cdot(2p+1), 2(4p+3)^2\cdot(2p+1)\in X_k$.

Similarly, consider $k=2p(2p+1)$, where p is a Germain prime, and let $x=(2p+1)^2$. Then

$$\begin{aligned}\varphi(x) &= (2p+1)^2-(2p+1)\\ &= 2p(2p+1)\\ &= k.\end{aligned}$$

Hence, $(2p+1)^2, 2(2p+1)^2\in X_k$. This is part (a) in Theorem 2.4.1.

Furthermore, consider $k=2^3p(2p+1)(4p+3)(8p+7)$, where $p,\ 2p+1$, and $4p+3$ are Germain primes, and let $x=(8p+7)^2(4p+3)(2p+1)$. Then

$$\begin{aligned}\varphi(x) &= \left[(8p+7)^2-(8p+7)\right](4p+2)2p\\ &= (8p+7)(8p+6)(4p+2)2p\\ &= 2^3p(2p+1)(4p+3)(8p+7)\\ &= k.\end{aligned}$$

Hence, $(8p+7)^2(4p+3)(2p+1), 2(8p+7)^2(4p+3)(2p+1)\in X_k$.

The above discussions are specific cases of the following result.

Theorem 2.4.3. *Let p be an odd prime number. Define $g_1=p$ and $g_i=2g_{i-1}+1$ for all $i\geq 2$. Suppose that g_i is prime for all $i=2,3,\ldots,m$. Let $k=2^m\prod_{i=1}^{m+1}g_i$. Then*

$$g_{m+1}^2\prod_{i=2}^{m}g_i,\ 2g_{m+1}^2\prod_{i=2}^{m}g_i\in X_k.$$

Proof. Let $x=g_{m+1}^2\prod_{i=2}^{m}g_i$. Then

$$\begin{aligned}\varphi(x) &= \left(g_{m+1}^2-g_{m+1}\right)\cdot\varphi\left(\prod_{i=2}^{m}g_i\right)\\ &= g_{m+1}\left(g_{m+1}-1\right)\cdot\varphi\left(\prod_{i=2}^{m}g_i\right)\\ &= g_{m+1}\left(2g_m+1-1\right)\cdot\varphi\left(\prod_{i=2}^{m}g_i\right)\\ &= 2g_{m+1}g_m\cdot\varphi\left(\prod_{i=2}^{m}g_i\right)\end{aligned}$$

$$= 2g_{m+1}g_m\,(g_2-1)\,(g_3-1)\ldots(g_m-1)$$
$$= 2g_{m+1}g_m\,(2g_1+1-1)\,(2g_2+1-1)\cdots(2g_{m-1}+1-1)$$
$$= 2^m g_1 g_2\cdots g_{m-1}g_m g_{m+1}$$
$$= 2^m\prod_{i=1}^{m+1} g_i$$
$$= k.$$

Thus, $x \in X_k$, and so $2x \in X_k$ by Proposition 1.1.7. □

Example 2.5.

a. Let $p = 3$. We have $g_1 = 3$ and $g_2 = 7$. Note that g_1 is a Germain prime. For $k = 2\prod_{i=1}^{2} g_i = 42$, we have $g_2^2 = 49 \in X_k$, and $2g_2^2 = 98 \in X_k$.

b. Let $p = 5$. We have $g_1 = 5$, $g_2 = 11$, $g_3 = 23$, and $g_4 = 47$. Note that g_1, g_2, and g_3 are Germain primes. For $k = 2^3\prod_{i=1}^{4} g_i = 475640$, we have $g_4^2\prod_{i=2}^{3} g_i = 558877 \in X_k$, and $2g_4^2 = 1117754 \in X_k$.

c. Let $p = 89$. We have $g_1 = 89$, $g_2 = 179$, $g_3 = 359$, $g_4 = 719$, $g_5 = 1439$, and $g_6 = 2879$. Note that g_1, g_2, g_3, g_4, and g_5 are Germain primes. For $k = 2^5\prod_{i=1}^{6} g_i = 545153511332496992$, we have $g_6^2\prod_{i=2}^{5} g_i = 551087415423545941 \in X_k$, and $2g_6^2 = 1102174830847091882 \in X_k$.

It is conjectured that there are infinitely many Germain prime numbers. The largest known is

$$2618163402417 \times 2^{12618163402417} - 1,$$

which is 388,342 digits. The second largest known is

$$18543637900515 \times 2^{666667} - 1,$$

which is 200,701 digits.

3 Conclusion

We have shown that Carmichael's totient conjecture holds in the following cases:

1. X_{2^t}, where t is a nonnegative integer.
2. X_{2p^s}, where $p \neq 3$ is an odd prime number, $s = 1,\ 2,\ 3,$ or 4, and $2p^s + 1$ is not prime.
3. X_{2^2p}, where p is an odd prime number such that $p \equiv 1 \pmod 6$.
4. X_k, where $k = 2^m\prod_{i=1}^{m+1} g_i$ is the product of a power of 2 and a sequence of $m+1$ Germain primes.

This was done primarily using Corollary 1.1.4. The most general case of X_k, where $k = 2^\mu\prod p^\alpha$, is Carmichael's totient conjecture and remains open.

As a general aside, the propositions, examples and particularly the conjectures in this paper are a number theoretic exemplification of Iverson's view of the importance of notation [11], especially with 'suggestivity' leading to shrewd guessing, a necessary ingredient in undergraduate development of the ability to think mathematically in capstone subjects and to recognize conjectures in general [14, 20].

Acknowledgements

The authors would like to thank Dr. Vassia Atanassova, the managing editor of NNTDM for her comments, corrections, and suggestions. The authors would also like to thank the referee for their corrections of the paper and providing references [30, 31].

References

[1] Carmichael, R. D. (1908). A table of the values of m corresponding to given values of $\phi(m)$. *American Journal of Mathematics*, 30(4), 394–400.

[2] Carmichael, R. D. (1919). Fermat numbers $F_n = 2^{2^n} + 1$. *The American Mathematical Monthly*, 26(4), 137–146.

[3] Carmichael, R. D. (1922). Note on Euler's φ-function. *Bulletin of the American Mathematical Society*, 28(3), 109–110.

[4] Dickson, L. E. (1919). *History of the Theory of Numbers, Vol. 1*. Chelsea, New York.

[5] Donnelly, H. (1973). On a problem concerning Euler's phi-function. *The American Mathematical Monthly*, 80(9), 1029–1031.

[6] Ford, K. (1998). The distribution of totients. *The Ramanujan Journal*, 2, 67–151.

[7] Grosswald, P. (1973). Contribution to the theory of Euler's function $\varphi(x)$. *Bulletin of the American Mathematical Society*, 79(2), 337–341.

[8] Gupta, H. (1981). Euler's totient function and its inverse. *Indian Journal of Pure and Applied Mathematics*, 12(1), 22–30.

[9] Guy, R. (2004). *Unsolved Problems in Number Theory, Vol. 3*. Springer, New York.

[10] Holt, J. J. (2003). The minimal number of solutions to $\phi(n) = \phi(n + k)$. *Mathematics of Computation*, 72(244), 2059–2061.

[11] Iverson, K. E. (1980). Notation as a tool of thought. *Communications of the ACM*, 23(8), 444–465.

[12] Klee, V. L., Jr. (1947). On a conjecture of Carmichael. *Bulletin of the American Mathematical Society*, 53(12), 1183–1186.

[13] Leveque, W. J. (1974). *Reviews in Number Theory 1940–1972: As printed in Mathematical Reviews 1940-1972*. American Mathematical Society, Providence.

[14] Mahatmya, D., Morrison, J., Jones, R. M., Garner, P. W., Davis, S. N., Manske, J., Berner, N., Johnson, A., & Ditty, J. (2017). Pathways to undergraduate research experiences: A multi-institutional study. *Innovative Higher Education*, 42(5–6), 591–504.

[15] Masai, P., & Valette, A. (1982). A lower bound for a counterexample to Carmichael's conjecture. *Bollettino della Unione Matemàtica Italiana. Serie VI. A*, 1(2), 313–316.

[16] Mendelsohn, N. S. (1976). The equation $\phi(x) = k$. *Mathematics Magazine*, 49(1), 37–39.

[17] Merow, S. D. (2019). Has Carmichael's conjecture been proven? No, no, it has not. *Notices of the American Mathematical Society*, 66(5), 759–761.

[18] Olunloyo, V. O. S. (1975). On the numerical solution of a Diophantine equation connected with near-primality. *Abacus*, 10, 123–144.

[19] Pichler, A. (1900–1901). Über die Auflösung der Gleichung: $\varphi(x) = n$, wenn $\varphi(m)$ die Anzahl derjenigen Zahlen bezeichnet, welche relativ prim zu m und kleiner als m sind. *Jahresbericht des K. K. Maximilian-Gymnasiums in Wien*, 3–17.

[20] Polya, G. (1957). *How to Solve It: A New Aspect of Mathematical Method* (2nd edition). Princeton University Press, Princeton.

[21] Pomerance, C. (1974). On Carmichael's conjecture. *Proceedings of the American Mathematical Society*, 43(2), 297–298.

[22] Ramadan-Jradi, W. (1999). Carmichael's conjecture and a minimal unique solution. *Notes on Number Theory and Discrete Mathematics*, 5(2), 55–70.

[23] Rosen, K. H. (2011). *Elementary Number Theory and Its Applications* (6th edition). Pearson Addison-Wesley.

[24] Schinzel, A. (1961). Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers". *Acta Arithmetica*, 7(1), 1–8.

[25] Schlafly, A., & Wagon, S. (1994). Carmichael's conjecture on the Euler function is valid below $10^{10,000,000}$. *Mathematics of Computation*, 63(207), 415–419.

[26] Sivaramakrishnan, R. (1986). The many facets of Euler's totient I: A general perspective. *Nieuw Archief voor Wiskunde*, 4, 175–190.

[27] Sloane, N. J. A. (2023). A005384 Sophie Germain primes: Sophie Germain primes p: $2p+1$ is also prime. *The On-Line Encyclopedia of Integer Sequences*. Available online at: `https://oeis.org/A005384`.

[28] Spyropoulos, K. (1989). Euler's equation $\phi(x) = k$ with no solution. *Journal of Number Theory*, 32(2), 254–256.

[29] Stepanova, L. L., & Flikop, E. L. (1972). On the question of the number of solutions of the equation $\varphi(x) = m$. *Studies in Number Theory Izdat Saratov University*, 4, 89–93.

[30] Vassilev-Missana, M. (1996). Note on the equation $\varphi(x) = 2^l.q$. *Notes on Number Theory and Discrete Mathematics*, 2(3), 45–46.

[31] Vassilev-Missana, M. (1996). The numbers which cannot be values of Euler's function φ. *Notes on Number Theory and Discrete Mathematics*, 2(4), 41–48.

[32] Wegner, K. W., & Savitsky, S. R. (1970). Solutions of $\phi(x) = n$, where ϕ is Euler's ϕ-function. *The American Mathematical Monthly*, 77(3), 287.