A NOTE ON FERMAT'S CONGRUENCE

Takashi Agoh
Department of Mathematics, Tokyo University of Science, Noda, Chiba, Japan
agoh_takashi@ma.noda.tus.ac.jp

Received: 4/21/23, Revised: 10/29/24, Accepted: 3/19/25, Published: 3/26/25

Abstract

By combining a couple of Fermat's congruences, we consider a special type of congruence that is satisfied by either primes or Carmichael numbers. After examining some characteristic properties of this congruence, we apply it to study possible conditions for twin primes and Sophie Germain primes.

1. Introduction

As is very familiar to everyone, Fermat's little theorem states that if n is a prime and a is an integer coprime to n, then it follows that

$$a^{n-1} \equiv 1 \pmod{n}. \tag{1.1}$$

However, the reverse implication is not always true. In fact, a Carmichael number n, which is composite and square-free, also satisfies (1.1) to every base a coprime to n. Congruence (1.1) is usually called *Fermat's congruence*. As is well-known, the integers $n \geq 2$ satisfying (1.1) to every base a coprime to n are either prime numbers or Carmichael numbers. Hereafter, by quoting his words mentioned in Ore [19], we will say that these numbers preserve the '*Fermat property*'. Especially, a composite number n that satisfies (1.1) for a specific integer $a \geq 2$ is called a *Fermat pseudoprime to base a*. Therefore, a Carmichael number n is a Fermat pseudoprime to every base a coprime to n.

The following criterion is widely known and very useful to identify Carmichael numbers, established by Korselt [13] in 1899.

Korselt's Criterion. *A composite $n > 0$ is a Carmichael number if and only if n is square-free and $p - 1 \mid n - 1$ for every prime factor p of n.*

A proof of this criterion is not so difficult (see, e.g., [10, p.134] and [8, p.414]).

DOI: 10.5281/zenodo.15091101

It would be worth mentioning here that Borwein and Wong [7] discussed some variations and generalizations of Giuga's conjecture suggesting that n is a prime if and only if the congruence

$$\sum_{0<a<n} a^{n-1} \equiv -1 \pmod{n}$$

holds. As one of results, they showed that $n \geq 2$ satisfies the congruence

$$\sum_{\substack{0<a<n \\ \gcd(a,n)=1}} a^{n-1} \equiv \varphi(n) \pmod{n} \tag{1.2}$$

if and only if it follows that $p-1 \mid n-1$ for every prime factor p of n, where φ is Euler's totient function. So a square-free integer $n \geq 2$ that satisfies (1.2) is either a prime or a Carmichael number. We will not go into details, but the left-hand side of (1.2) is closely related to Bernoulli numbers (see, e.g., [1]).

In their celebrated paper [5], Alford, Granville, and Pomerance proved that there are infinitely many Carmichael numbers (see also Pomerance's beautiful survey [20] on this result). Subsequently, it was verified in Harman's work [12] that there are more than $x^{1/3}$ Carmichael numbers for sufficiently large x. This result was recently improved by Lichtman [15, Corollary 1.2] and it was shown that there are at least $x^{0.3389}$ Carmichael numbers for sufficiently large x. A small table of these numbers up to 512461 can be found in the OEIS [18]: A002997.

Combining a couple of Fermat's congruences for distinct integers $n, m > 0$ with common base a, we now consider a special type of congruence such that

$$a^{m-1} \equiv \frac{a^{m-n}-1}{m-n} \cdot n + a^{m-n} \equiv \frac{a^{m-n}-1}{m-n} \cdot m + 1 \pmod{nm}. \tag{1.3}$$

The next theorem describes how (1.3) is concerned with the Fermat property.

Theorem 1.1. *The conditions for* (1.3) *to hold for every integer a coprime to nm can be stated as follows:*

(a) *Under the assumption* $\gcd(n, m) = 1$, (1.3) *holds if and only if both n and m preserve the Fermat property.*

(b) *If* (1.3) *holds, then it follows that* $\gcd(n, m) = 1$.

(c) *If* (1.3) *holds, then both n and m preserve the Fermat property.*

In view of the above theorem, we can assert that (1.3) is a natural generalization of Fermat's congruence (1.1) to a composite modulus nm.

In Section 2, we first discuss some kinds of variations of (1.3) and subsequently give a proof of Theorem 1.1 in an elementary way. In Section 3, by applying the characteristic properties of (1.3) stated in the above theorem, we study possible congruence conditions for twin primes and Sophie Germain primes.

2. Proof of Theorem 1.1

Before giving a proof of Theorem 1.1, we would like to introduce some variations of (1.3). At first, we see that multiplying the whole of (1.3) by a^n leads to

$$ya^{n+m-1} \equiv \frac{a^m - a^n}{m-n} \cdot n + a^m \equiv \frac{a^m - a^n}{m-n} \cdot m + a^n \pmod{nm}.$$

Next, we multiply the whole of (1.3) by a^{n-1} and then use the obvious identity

$$a^{(m-1)+(n-1)} = (a^{m-1} - 1)(a^{n-1} - 1) + (a^{m-1} + a^{n-1}) - 1$$

in order to transform (1.3) into

$$\begin{aligned}(a^{m-1} - 1)(a^{n-1} - 1) &\equiv \frac{a^{m-1} - a^{n-1}}{m-n} \cdot n - (a^{n-1} - 1) \\ &\equiv \frac{a^{m-1} - a^{n-1}}{m-n} \cdot m - (a^{m-1} - 1) \pmod{nm},\end{aligned}$$

where the most left-hand side vanishes modulo nm if $\gcd(n, m) = 1$. Further, adding $a^{n-1} - 1$ to each side gives

$$a^{m-1}(a^{n-1} - 1) \equiv \frac{a^{m-1} - a^{n-1}}{m-n} \cdot n \pmod{nm}, \tag{2.1}$$

which is much simpler than the above. Of course, there are several other variations of (1.3) besides the above.

In addition, let us consider the congruence such that

$$a^{n-1} - 1 \equiv \frac{a^{m-1} - a^{n-1}}{m-n} \cdot n \pmod{nm}, \tag{2.2}$$

which is similar to, but slightly different from (2.1). It is clear that if $\gcd(n, m) = 1$, then (2.2) is actually equivalent to (2.1), and hence to (1.3). In the next section, we will use (2.2) independently of (1.3) to derive certain congruence conditions for twin primes and Sophie Germain primes.

Proof of Theorem 1.1. Since condition (c) is just an immediate consequence of (a) and (b), we will give below only the proofs of (a) and (b).
(a): In the case when $\gcd(n, m) = 1$, we may observe (1.3) for modulo m and for modulo n independently, thereby (1.3) yields

$$a^{m-1} \equiv \frac{a^{m-n} - 1}{-n} \cdot n + a^{m-n} \equiv 1 \pmod{m}$$

and

$$a^{m-1} \equiv a^{m-n} \pmod{n}, \text{ i.e., } a^{n-1} \equiv 1 \pmod{n},$$

which verify that both n and m preserve the Fermat property. By following the opposite process, we can see that the reverse implication is also true.
(b): Next, assume that (1.3) holds for distinct integers n, m with $m > n$. We will show that the assumption $\gcd(n, m) > 1$ leads to a contradiction. Letting p be a prime factor of $\gcd(n, m)$, now take an integer a such that $a \equiv 1 + p \pmod{p^2}$, which is clearly coprime to p. Since $p \mid m$, we obtain from (1.3),

$$\begin{aligned} a^{m-1} &\equiv (1+p)^{m-1} \equiv \sum_{i=0}^{m-1} \binom{m-1}{i} p^i \equiv 1 + (m-1)p \\ &\equiv 1 - p \equiv \frac{(1+p)^d - 1}{d} \cdot m + 1 \pmod{p^2}, \end{aligned} \tag{2.3}$$

where $d := m - n > 0$. Noting that $d \geq p \geq 2$ and $\binom{d}{j} = \frac{d}{j}\binom{d-1}{j-1}$ for $j \geq 1$, we get

$$\frac{(1+p)^d - 1}{d} = \frac{1}{d} \sum_{j=1}^{d} \binom{d}{j} p^j = \sum_{j=1}^{d} \binom{d-1}{j-1} \frac{p^j}{j} \equiv 0 \pmod{p},$$

which indicates that the fraction term on the last side of (2.3) vanishes modulo p^2 because $p \mid m$. So (2.3) leads to $1 - p \equiv 1 \pmod{p^2}$, but this is a contradiction. Consequently, if (1.3) holds, then we have $\gcd(n, m) = 1$, as desired. □

It should be added that if (2.2) holds for every integer a coprime to nm, then we can show that $\gcd(n, m) = 1$ in much the same way as above. In fact, assuming $\gcd(n, m) > 1$, let p be any prime factor of $\gcd(n, m)$. As above, take $a \equiv 1 + p \pmod{p^2}$ in (2.2). Since $p \mid n$ and so $(1 + p)^{n-1} \equiv 1 + (n - 1)p \equiv 1 - p \pmod{p^2}$, we see that (2.2) provides

$$1 - p \equiv \frac{(1 + p(m-1)) - (1 + p(n-1))}{m - n} \cdot n \equiv pn \equiv 0 \pmod{p^2},$$

which is, however, impossible. So we have $\gcd(n, m) = 1$, which indicates that n and m satisfying (2.2) preserve the Fermat property as is (1.3).

3. Application

In this section, by applying the characteristics of (1.3) stated in Theorem 1.1, we derive possible congruence conditions for twin primes and Sophie Germain primes. In what follows, let us denote by $\mathbf{P}$ and $\mathbf{C}$ the sets of primes and Carmichael numbers, respectively. Thus, any element in $\mathbf{P} \cup \mathbf{C}$ preserves the Fermat property, as already noted in Section 1.

3.1. Twin Primes

When both p and $p+2$ are prime, they are called *twin primes*. It is not known whether there are infinitely many twin primes (the so-called *twin prime conjecture*). Although the sum of the reciprocals of all primes diverges to infinity, Viggo Brun surprisingly proved in 1919 by the Eratosthenes-Legendre sieve method that the series obtained by adding the reciprocals of twin primes converges to a finite value known now as *Brun's constant* B. That is to say,

$$B \equiv \sum_{p,\, p+2 \in \mathbf{P}} \left(\frac{1}{p} + \frac{1}{p+2} \right).$$

It is known that B equals approximately 1.90216058 (cf. the OEIS [18]: A042165), but whether the above sum actually consists of infinitely many terms depends on the irrationality of B. Needless to say, Brun's result greatly contributed to the subsequent development of sieve theory.

Apart from the above, we next pick up some elementary results on twin primes. As is easily seen, all twin prime pairs except $(3,5)$ are of the form $(6k-1, 6k+1)$ with $k \geq 1$. Further, a twin prime pair $(n, n+2)$ can be characterized by

$$4((n-1)!+1) \equiv -n \pmod{n(n+2)} \quad \text{(see Clement [9])}.$$

This is a nice generalization of Wilson's theorem stating that $(n-1)! \equiv -1 \pmod{n}$ is valid only for a prime n. In addition, if a pair $(n, n+2)$ consists of twin primes, then it follows that ([3, Corollary 3.2])

$$\begin{aligned} &\text{(i)} && 2^{n+1} \equiv \frac{3n}{2} + 4 \pmod{n(n+2)}; \\ &\text{(ii)} && 3^{n+1} \equiv 4n + 9 \pmod{n(n+2)}; \\ &\text{(iii)} && 3^{n+2} + 2^{n+4} \equiv -5 \pmod{n(n+2)}. \end{aligned} \tag{3.1}$$

Congruence (3.1) (iii) is an easy consequence of (i) and (ii).

The main purpose of this subsection is to generalize (3.1) using the properties of (1.3) stated in Theorem 1.1 and to prove the following theorem.

Theorem 3.1. *Let $n \geq 3$ be any given odd integer. Under the assumption that both n and $n+2$ are not Carmichael numbers, a pair $(n, n+2)$ consists of twin primes if and only if each one of the congruences*

$$\begin{aligned} &\text{(i)} \quad 2a^{n+1} \equiv (n+2)a^2 - n \pmod{n(n+2)}; \\ &\text{(ii)} \quad na^{n+1} \equiv (n+2)a^{n-1} - 2 \pmod{n(n+2)} \end{aligned} \tag{3.2}$$

holds for every integer a coprime to $n(n+2)$.

Proof. If $(n, n+2)$ is a twin prime pair, then (1.3) gives, by setting $m = n+2$,

$$a^{n+1} \equiv \frac{a^2-1}{2} \cdot n + a^2 \equiv \frac{a^2-1}{2} \cdot (n+2) + 1 \pmod{n(n+2)},$$

which leads to (i) after doubling the whole expression and rearranging the terms included. Conversely, if (i) holds, then we can deduce Fermat's congruences modulo n and modulo $n+2$, because $\gcd(n.n+2) = 1$. Thus, $n, n+2 \in \mathbf{P} \cup \mathbf{C}$. However, the given assumption forces both n and $n+2$ to be prime, so $(n, n+2)$ must be a pair of twin primes. Next, recall (2.2) for distinct $n, m > 0$. By removing the denominator and rearranging the terms, we get

$$n(a^{m-1} - 1) \equiv m(a^{n-1} - 1) \pmod{nm} \tag{3.3}$$

for every integer a coprime to nm. If $\gcd(n, m) = 1$, then (3.3) provides (1.1) for n and the same one replaced n with m, so $n, m \in \mathbf{P} \cup \mathbf{C}$. Since $\gcd(n, n+2) = 1$ for an odd n, setting $m = n+2$ in (3.3) yields (ii). As a result, two congruences in (3.2) are actually equivalent via (1.1). Further, as is obvious, (3.1) (i) and (ii) are just the special cases of (3.2) (i) where $a = 2$ and 3. □

Incidentally, the above discussion raises the following question asking about the existence of "twin" Carmichael numbers.

Question. *Is there a case where both n and $n+2$ are Carmichael numbers?*

It seems extremely difficult to uncover the truth of this question at this time for the reason that nothing is known about bounded gaps between consecutive Carmichael numbers, as far as we know. Recently, Larsen [14] conducted research on Bertrand's postulate for Carmichael numbers and proved that for all $\delta > 0$ and x sufficient large in terms of δ, there are at least $e^{(\log x)/(\log\log x)^{2+\delta}}$ Carmichael numbers between x and $x + x/(\log x)^{1/(2+\delta)}$. This result is very interesting and valuable, but it does not guarantee the existence of twin Carmichael numbers.

3.2. Sophie Germain Primes

A prime number p is called a *Sophie Germain prime* if $2p+1$ is again a prime. These types of primes were first discussed by Sophie Germain in connection with Fermat's Last Theorem. Indeed, she proved that if p is a Sophie Germain prime, then there are no integers x, y, z, different from 0 and not multiples of p, such that $x^p + y^p = z^p$. For a sketch of its proof, see, e.g., [21, Chapter 4]. It is also known as Euler's divisor criterion for Mersenne numbers that if p is an odd prime with $p \equiv 3 \pmod 4$ and $M_p := 2^p - 1$ is a Mersenne number, then $2p+1$ divides M_p if and only if p is Sophie Germain. When p is Sophie Germain, a prime $q = 2p+1$

is called a *safe prime* for the reason that $q-1$ does not have many small factors. The first few of these pairs (p,q) are given as follows:

$$(2,5),\ (3,7),\ (5,11),\ (11,23),\ (23,47),\ (29,59),\ (41,83),\ (53,107),\ (83,167),$$

and so on. For more pairs, see the OEIS [18]: A005384 and A005385. It is easy to see that every Sophie Germain prime except 2 and 3 can be expressed in the form $6n-1$. It is still open whether there are infinitely many of these prime pairs, much like the twin prime conjecture.

Denote by $\mathbf{S}$ the set of Sophie Germain primes and by $\pi_{\mathrm{SG}}(x)$ the number of Sophie Germain primes not exceeding x. The next heuristic estimate for $\pi_{\mathrm{SG}}(x)$ is widely known as a reliable result in the literature (see, e.g., [23, Chapter 5.5.5]):

$$\pi_{\mathrm{SG}}(x) \sim \frac{2Cx}{(\log x)^2} \quad (x \to \infty), \tag{3.4}$$

where C is Hardy-Littlewood's twin prime constant, namely

$$C = \prod_{\substack{p \in \mathbf{P} \\ p>2}} \frac{p(p-2)}{(p-1)^2} \approx 0.660161\cdots.$$

Based on the prime number theorem, we can see that the set $\mathbf{S}$ has the primitive density 0. In fact, the relative error between the prime counting function $\pi(x)$ and $x/\log x$ approaches 0 as x increases, so (3.4) allows us to derive

$$\lim_{x\to\infty} \frac{\pi_{\mathrm{SG}}(x)}{\pi(x)} = \lim_{x\to\infty} \frac{2C}{\log x} = 0.$$

By the way, the explicit values of $\pi_{\mathrm{SG}}(10^n)$ for $n = 1, 2, \ldots, 14$ are listed in the OEIS [18]: A092816.

Remark. We directly applied the prime number theorem to find the primitive density of the set $\mathbf{S}$, but the referee of this note kindly pointed out that it is also possible to get the same conclusion as above based on Selberg's sieve method (for reference on this sieve method; see, e.g., [6, 11, 24]).

The following excellent result, recently proved, completely denies the existence of a certain special type of Carmichael number.

Theorem 3.2 (Alahmadi and Luca [4]). *For every integer $n \geq 0$, there is no Carmichael number of the form $2^n p + 1$ with p an odd prime.*

By building upon this result, it was further proved in [17] that there is no Carmichael number of the form $2^n p^2 + 1$ with some integer $n \geq 0$ and prime p.

With the help of Theorem 3.2, we wish to prove the following theorem.

Theorem 3.3. *A given prime p is Sophie Germain if and only if each one of the congruences*

$$\begin{aligned} &\text{(i)} \quad a^{2p} \equiv (2p+1)a^{p+1} - 2p \pmod{p(2p+1)}; \\ &\text{(ii)} \quad (2p+1)a^{p-1} \equiv pa^{2p} + p + 1 \pmod{p(2p+1)} \end{aligned} \tag{3.5}$$

holds for every integer a coprime to $p(2p+1)$.

Proof. When $p = 2$, we can confirm by direct calculation that both (i) and (ii) are valid for all $a = 1, 3, 7, 9$. Next, assuming that $p \geq 3$ is Sophie Germain and taking $n = p$ and $m = 2p + 1$ in (1.3), we get for every integer a as indicated,

$$a^{2p} \equiv \frac{a^{p+1} - 1}{p+1} \cdot p + a^{p+1} \equiv \frac{a^{p+1} - 1}{p+1} \cdot (2p+1) + 1 \pmod{p(2p+1)}. \tag{3.6}$$

To deduce (i), we have only to multiply the whole of (3.6) by $p + 1$ and then use the trivial $pa^{2p} \equiv p \pmod{p(2p+1)}$. Conversely, if (i) holds, then, since $\gcd(p, 2p+1) = 1$, we get $a^{2p} \equiv -2p \equiv 1 \pmod{2p+1}$, hence $2p + 1 \in \mathbf{P} \cup \mathbf{C}$. Since Theorem 3.2 asserts that $2p + 1 \notin \mathbf{C}$, we see that $2p + 1$ must be a prime, thus $p \in \mathbf{S}$. Next, by taking $n = p$ and $m = 2p + 1$ in (2.2) (or by directly taking these n, m in (3.3)), we have

$$p(a^{2p} - 1) \equiv (2p+1)(a^{p-1} - 1) \pmod{p(2p+1)}, \tag{3.7}$$

which is just the same as (ii). Conversely, if (ii) holds, then we obtain (1.1) for $n = p$ and $2p + 1$. For the same reason as mentioned above, p must be Sophie Germain. Note that (i) is actually equivalent to (ii) via (1.1), since both p and $2p+1$ preserve the Fermat property. Such the equivalence relation can be also shown directly using (3.7), because both sides of this vanish modulo $p(2p + 1)$. □

Given a prime p, let us consider the sequence $q_1, q_2, \ldots, q_j, \ldots$, defined by

$$q_1 := p, \quad q_{j+1} := 2q_j + 1 \ \ (j \geq 1).$$

Let $l = l(p)$ be length of a Sophie Germain prime chain (i.e., a Cunningham prime chain of the first kind) with the initial term $q_1 = p$. Needless to say, all l integers $q_1, q_{2,}, \ldots, q_l$ are prime, but q_{l+1} is not. For example, if $p = 2$, then we have the prime chain $2, 5, 11, 23, 47$, where $2 \cdot 47 + 1 = 95$ is composite, thus $l(2) = 5$. Similarly, we have $l(3) = 2$, $l(5) = 4$, $l(7) = 1$, $l(11) = 3$, $l(13) = l(17) = l(19) = 1$, $l(23) = 2$, and so on. As is self-evident, if the last digit of p is 7, then $l(p) = 1$ because of $2p + 1 \equiv 0 \pmod 5$.

As is easily seen, letting $N := (p + 1)/2$, the sequence as stated above can be written as $2^j N - 1$ (including also the case when $p = 2$) for $j \geq 1$. For numbers of these forms, very efficient primality testing algorithms are available.

The following corollary reveals the explicit relationships between adjacent terms of a Sophie Germain prime chain.

Corollary 3.4. *With the above notation, if $p = q_1$ is a Sophie Germain prime having $l = l(p) \geq 2$, then for each $j = 1, 2, \ldots, l-1$, the congruences*

$$\begin{aligned} &\text{(i)} \quad a^{q_{j+1}-1} \equiv q_{j+1}a^{q_j+1} - 2q_j \pmod{q_jq_{j+1}}; \\ &\text{(ii)} \quad q_{j+1}a^{q_j-1} \equiv q_ja^{q_{j+1}-1} + q_j + 1 \pmod{q_jq_{j+1}} \end{aligned} \tag{3.8}$$

hold for every integer a coprime to $q_1q_2\cdots q_l$.

Proof. To deduce (3.8), replace p in (3.5) with q_j for each $j = 1, 2, \ldots, l-1$, noting that q_{l+1} is not a prime. □

For an odd prime p, let $\mathrm{ord}_p(2)$ denote the order of 2 modulo p, i.e., the least positive exponent such that $2^{\mathrm{ord}_p(2)} \equiv 1 \pmod{p}$. An upper bound for $l(p)$ can be given as follows.

Theorem 3.5 ([2, Proposition 3.1])**.** *We have $l(p) \leq \mathrm{ord}_p(2)$ for $p \in \mathbf{S}\backslash\{2\}$.*

Proof. The proof is quite easy. For brevity, putting $k := \mathrm{ord}_p(2)$, we get

$$q_{k+1} = 2q_k + 1 = 2^2q_{k-1} + (2^2 - 1) = \cdots = 2^kq_1 + (2^k - 1) \equiv 0 \pmod{q_1},$$

thus, q_{k+1} is not a prime and this verifies $l(p) \leq k$, as desired. □

Since $\mathrm{ord}_p(2) \leq p - 1$ for any $p \in \mathbf{S}\backslash\{2\}$, the above theorem shows that it is impossible to create an infinite Sophie Germain prime chain starting from p (see also Löh [16] on this matter). Although not yet resolved, it is expected that there exists a prime chain of the above type having arbitrarily long length. Various kinds of conjectures (directly or indirectly) intertwined with this problem, for example, Dickson's conjecture on the infinity of primes of linear forms, are introduced in Ribenboim's classic book [22].

Acknowledgments. The author would like to thank Andrew Granville for his helpful comments and suggestions on the proof of Theorems 1.1. Furthermore, the author would be grateful to the anonymous referee and Bruce Landman for helpful remarks and corrections, which improved the quality of this note.

References

[1] T. Agoh, On Bernoulli and Euler numbers, *Manuscripta Math.* **61** (1988), 1–10.

[2] T. Agoh, On Sophie Germain primes, *Tatra Mt. Math. Publ.* **20** (2000), 65–73.

[3] T. Agoh, A characterization of primes based on Eulerian numbers, *Integers* **23** (2023), #A 28.

[4] A. Alahmadi and F. Luca, There are no Carmichael numbers of the form $2^n p+1$ with p prime, *C. R. Math. Acad. Sci. Paris* **360** (2022), 1177–1181.

[5] W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math.* (2) **139** (1994), 703–722.

[6] M. Bordignon and E. S. Lee, Explicit upper bounds for the number of primes simultaneously representable by any set of irreducible polynomials, preprint, arXiv:2211.11012.

[7] J. M. Borwein and E. Wong, A survey of results relating to Giuga's conjecture on primality, in *Adv. Math. Sci.: CRM's 25 years* (Montreal, PQ, 1994), Amer. Math. Soc., Providence, RI, **11** (1997), 13–27.

[8] L. N. Childs, *A Concrete Introduction to Higher Algebra (Undergraduate Texts in Mathematics)*, 3rd ed. Springer-Verlag, New York, 2009.

[9] P. A. Clement, Congruences for sets of primes, *Amer. Math. Monthly* **56** (1949), 23–25.

[10] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, 2nd ed., Springer-Verlag, New York, 2005.

[11] G. Creaves, *Sieves in Number Theory*, Ergebnisee der Mathematik und ihrer Grenzgebiete. 3. Folge. Vol. 43, Springer-Verlag, Berlin, 2001.

[12] G. Harman, Watt's mean value theorem and Carmichael numbers, *Int. J. Number Theory* **4** (2008), 241–248.

[13] A. Korselt, Problème chinois, *L'Intermédiaire des Math.* **6** (1899), 142–143.

[14] D. Larsen, Bertrand's postulate for Carmichael numbers, *Int. Math. Res. Not. IMRN* (2023), No, **15**, 13072–13098. Available online at: https://arxiv.org/pdf/2111.06963.pdf.

[15] J. D. Lichtman, Primes in arithmetic progressions to large moduli and shifted primes without large prime factors, preprint, arXiv:2211.09641.

[16] G. Löh, Long chains of nearly doubled primes, *Math. Compt.* **53** (1989), 751–759.

[17] F. Luca and J. L. Randrianantenaina, There is no Carmichael number of the form $2^n p^2 + 1$ with p prime, *Integers* **23** (2023), #A 51.

[18] OEIS Foundation Inc. (2024), The On-Line Encyclopedia of Integer Sequences. Available online at: http://oeis.org.

[19] Ø. Ore, *Number Theory and Its History*, McGraw-Hill Book Co., Inc., New York, 1948. Reprint, Dover Publications, Inc., New York, 1988.

[20] C. Pomerance, Carmichael numbers, *Nieuw Arch. Wiskd. IV,* (4), **11** (1993), 199–209.

[21] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

[22] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, Berlin, Heidelberg, 3rd ed. 1996.

[23] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge Univ. Press, 2009.

[24] J. Teräväinen, *Join's Math Notes*: Selberg's upper bound sieve, 2014. Available online at his website: joinsmathnotes.blogspot.com/2014/10/selbergs-upper-bound-sieve.html.