#A83 INTEGERS 25 (2025)

# A NOTE ON SOPHIE GERMAIN PRIMES

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

*Received: 2/3/25, Accepted: 8/21/25, Published: 9/17/25*

**Abstract**

It is the main purpose of this note to investigate the arithmetic and structural properties of Sophie Germain primes — those primes $p$ for which $2p + 1$ is also prime. Let $\mathbf{P}$, $\mathbf{S}$, and $\mathbf{T}$ be the sets of all primes, all Sophie Germain primes, and all the primes that are not Sophie Germain, respectively. At first, we establish an explicit relationship between these sets via another special set composed of arithmetic progressions. Subsequently, we prove that $\mathbf{T}$ is an infinite set in two different ways and discuss the primitive densities of $\mathbf{S}$ and $\mathbf{T}$. Lastly, we search for congruence relations characterizing each of the sets $\mathbf{S}$ and $\mathbf{T}$ by means of the value of a certain polynomial and Wilson's theorem.

## 1. Introduction

A prime number $p$ is called a *Sophie Germain prime* if $2p + 1$ is also a prime. These types of primes were first studied by Sophie Germain in connection with the first case of Fermat's Last Theorem. Indeed, she proved that if $p$ is a Sophie Germain prime, then there are no integers $x, y, z$ satisfying $x^p + y^p = z^p$ in the case when $p \nmid xyz$ (for the proof, see, e.g., [14, Chapter 4]). It can also be seen from Euler's divisor criterion that if $p$ is a Sophie Germain prime with $p \equiv 3 \pmod 4$ and $M_p = 2^p - 1$ is a Mersenne number, then $2p + 1$ divides $M_p$.

When $p$ is Sophie Germain, a corresponding 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 $(p, q)$ can be enumerated as follows:

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

and so on. More pairs can be found in the OEIS [11]: A005384 and A005385. As is easily seen, every Sophie Germain prime except 2 and 3 is of the form $6n - 1$. It is conjectured that there are infinitely many these prime pairs much like, for example,

DOI: 10.5281/zenodo.17144360

the twin prime conjecture and Dickson's conjecture on the infinity of primes of linear forms (cf., e.g., Ribenboim [15]).

In what follows, we use the following notation. Denoting by $\#M$ the cardinality of a given set $M$,

$\mathbb{Z}^+$ : the set of positive integers;

$\mathbf{P}$ : the set of all primes;

$\mathbf{S}$ : the set of Sophie Germain primes;

$\mathbf{T}$ : the set of primes that are not Sophie Germain;

$\pi(x) := \#\{p \in \mathbf{P} \mid p \leq x\}$ (the prime counting function);

$\pi_{\mathrm{S}}(x) := \#\{p \in \mathbf{S} \mid p \leq x\}$;

$\pi_{\mathrm{T}}(x) := \#\{p \in \mathbf{T} \mid p \leq x\}$.

Thus, $\mathbf{P} = \mathbf{S} \cup \mathbf{T}$, where $\mathbf{S} \cap \mathbf{T} = \emptyset$. Therefore, $\pi(x) = \pi_{\mathrm{S}}(x) + \pi_{\mathrm{T}}(x)$ for any $x > 0$.

The following heuristic estimate for $\pi_{\mathrm{S}}(x)$ is widely known as the most reliable result in the literature (see, e.g., [16, Chapter 5.5.5]). Asymptotically,

$$\pi_{\mathrm{S}}(x) \sim \frac{2Cx}{(\log x)^2}, \tag{1.1}$$

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

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

By the way, the explicit values of $\pi_{\mathrm{S}}(10^n)$ for $n \geq 1$ are listed in the OEIS [11]: A092816.

Apart from the above, we next pick out an elementary result characterizing Sophie Germain primes by means of certain congruences (cf. [2, Theorem 3.3]). We see that a prime $p$ is Sophie Germain if and only if each of the following congruences holds true for every $a \in \mathbb{Z}^+$ coprime to $p(2p+1)$:

$$\begin{aligned} &\text{(i)} \quad a^{2p} \equiv (2p+1)a^{p+1} - 2p \pmod{p(2p+1)}; \\ &\text{(ii)} \quad (2p+1)a^{p-1} \equiv pa^{2p} + p + 1 \pmod{p(2p+1)}. \end{aligned} \tag{1.2}$$

This result can be proved based on Fermat's little theorem and the fact that if $p$ is a prime satisfying (1.2) (i) or (ii), then $2p+1$ is never a Carmichael number identified by Korselt's criterion in [8], which states that a composite number $n$ is Carmichael if and only if $n$ is square-free and $p - 1 \mid n - 1$ for every prime factor $p$ of $n$ (for a detailed proof, see, e.g., [4, p. 134] and [3, p. 414]).

It is the main purpose of this note to investigate the arithmetic and structural properties of Sophie Germain primes. In Section 2, we establish an explicit relationship between the set $\mathbf{S}$ and its complement $\mathbf{T}$ among $\mathbf{P}$ via another special set composed of arithmetic progressions depending on odd primes. Section 3 is devoted to proving that **T** is an infinite set in two different ways. In Section 4, we discuss the primitive densities of **S** and **T**. We conclude this note, in Section 5, by giving some types of congruence relations characterizing each of the sets **S** and **T**.

## 2. A Relationship between S, T, and P via Another Special Set

Given an odd prime $p$, consider the set composed of an arithmetic progression with the common difference $p$ such that

$$\mathbf{A}(p) := \left\{ pr + \frac{p-1}{2} \;\middle|\; r = 1, 2, 3, \ldots \right\}. \tag{2.1}$$

We next define the set **A** by the union of $\mathbf{A}(p)$ for all odd primes $p$, namely

$$\mathbf{A} := \bigcup_{\substack{p \text{ prime} \\ p>2}} \mathbf{A}(p).$$

Since $2\,(pr + (p-1)/2) + 1 = p(2r+1) \equiv 0 \pmod{p}$ for every $r \in \mathbb{Z}^+$, we have $\mathbf{A}(p) \cap \mathbf{S} = \emptyset$ and hence $\mathbf{A} \cap \mathbf{S} = \emptyset$.

We will now establish an explicit relationship between the sets **S**, **T**, and **P** via **A** defined above in a convincing way. It should be noted that exactly the same relationship as that has been already stated in [1, Theorem 4.1], but there were some inaccuracies in its proof. The new proof given below was personally communicated by Andrew Granville to the present author (May, 2024).

**Theorem 2.1.** *With the above notation, it follows that*

$$\mathbf{T} = \mathbf{P} \cap \mathbf{A}, \;\; \textit{or equivalently}, \;\; \mathbf{S} = \mathbf{P} \setminus (\mathbf{P} \cap \mathbf{A})\,. \tag{2.2}$$

*Proof.* First note that the smallest odd integer in **A** is the prime 7, which is an element of $\mathbf{A}(3)$ for $r = 2$ and $\mathbf{A}(5)$ for $r = 1$. The only primes less than 7 that do not belong to **A** are 2, 3, and 5, all of which are Sophie Germain. So assuming that $n \geq 7$ is odd, write it as $n = pm$, where $p$ is the largest prime that divides $n$, and thus $m = n/p \geq 1$ is an odd integer. Now put $r' := (m-1)/2$ for an odd $m \geq 1$. As is obvious, $n = p$ is a prime only for $m = 1$. Therefore, letting $m \geq 3$ and so $r' \geq 1$, we get $n = p(2r'+1)$, which belongs to the set

$$2\mathbf{A}(p) + 1 := \{p(2r+1) \mid r = 1, 2, 3, \ldots\}.$$

All elements of this set are odd and composite, and this fact implies that the set **A** contains all primes $q$ except those of the form $q = (p-1)/2$ with $p$ a prime. The primes $q$ excluded here give $p = 2q + 1$ and this shows that such the primes $q$ are

Sophie Germain primes not belonging to the set $\mathbf{P} \cap \mathbf{A}$. Therefore, we can conclude that $\mathbf{P} \setminus (\mathbf{P} \cap \mathbf{A})$ is exactly the same as the set $\mathbf{S}$ of Sophie Germain primes and so the proof of (2.2) is now complete. □

Unfortunately, we cannot think of a simple good way to extract all the primes or all the composite numbers from the set $\mathbf{A}$ right now.

## 3. The Infinitude of T

The following statement seems almost self-evident at first glance, but in reality, proving this was not as easy as one might imagine. We will prove it below in two different ways, but both of them are a bit roundabout and not very direct.

**Theorem 3.1.** *The set* $\mathbf{T}$ *is infinite, i.e.,* $\#\mathbf{T} = \infty$.

*Proof (i).* Given any prime $p$, consider the infinite sequence $(q_j)_{j \geq 1}$ defined by

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

Let $l(p)$ be the length of a *Sophie Germain prime chain* (also known as a *Cunningham prime chain of the first kind*) with the initial term $q_1 = p$. That is to say, all $l(p)$ terms $q_1, q_2,, \ldots, q_{l(p)}$ belong to $\mathbf{S}$, but $q_{l(p)+1}$ does not. Given an odd prime $p$, let $\mathrm{ord}_p(2)$ denote the order of 2 modulo $p$, i.e., the least positive exponent satisfying $2^{\mathrm{ord}_p(2)} \equiv 1 \pmod{p}$. As is obvious, an upper bound for $l(p)$ can be given as $l(p) \leq \mathrm{ord}_p(2)$ for any $p \in \mathbf{S} \setminus \{2\}$. Further, since $\mathrm{ord}_p(2) \leq p - 1$, it is impossible to constitute an infinite Sophie Germain prime chain with the initial term $p$ (see also Löh [9] on this matter). By collecting all such primes $q_{l(p)}$ for infinitely many $p \in \mathbf{P} \setminus \{2\}$, we see that $\#\mathbf{T} = \infty$ and the proof is complete. □

Incidentally, letting $N := (p + 1)/2$ for a prime $p$, the above sequence $(q_j)_{j \geq 1}$ can be written as $2^j N - 1$, $j = 1, 2, 3, \ldots$ (including also the case for $p = 2$). For numbers of these forms, very efficient primality testing algorithms are available.

*Proof (ii).* For another way to make clear the assertion, we next observe the set $\mathbf{A}(p)$ defined in (2.1). Since $\gcd(p, (p - 1)/2) = 1$ for an odd prime $p$, Dirichlet's theorem on arithmetic progressions states that there are infinitely many primes in $\mathbf{A}(p)$, i.e., $\#\{q \in \mathbf{P} \mid q \in \mathbf{A}(p)\} = \infty$ for any fixed odd prime $p$. These primes are not Sophie Germain. In fact, if we take out from $\mathbf{A}(p)$ any one of primes such that $q = pr' + (p - 1)/2$ for some $r' \geq 1$, then $2q + 1 = p(2r' + 1) \equiv 0 \pmod{p}$, which implies $q \in \mathbf{T}$. Therefore, we have shown that $\#\mathbf{T} = \infty$, as desired. □

We cannot say for sure at this point, but there may be other simple proofs of Theorem 3.1 without the complicated procedures mentioned above.

## 4. The Primitive Densities of S and T

Based on either the Prime Number Theorem or Selberg's sieve method (for this sieve method, see, e.g., [5, Chapter 2] and [17]), one is able to show that the set **S** has the primitive density 0. In fact, since the relative error between $\pi(x)$ and $x/\log x$ approaches 0 as $x$ increases, formula (1.1) allows us to derive

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

where $C$ is the twin prime constant. In other words, most primes are not Sophie Germain. On the other hand, by applying the Prime Number Theorem and (1.1) again, we can get the asymptotic relation such that

$$\pi_{\mathrm{T}}(x)=\pi(x)-\pi_{\mathrm{S}}(x)\sim\frac{x}{\log x}\left(1-\frac{2C}{\log x}\right),$$

which implies that

$$\lim_{x\to\infty}\frac{\pi_{\mathrm{T}}(x)}{\pi(x)}=\lim_{x\to\infty}\left(1-\frac{2C}{\log x}\right)=1, \tag{4.1}$$

and thus **T** has the primitive density 1. In addition, it may be worth observing

$$\lim_{x\to\infty}\frac{\pi_{\mathrm{S}}(x)}{\pi_{\mathrm{T}}(x)}=\lim_{x\to\infty}\frac{2C}{\log x-2C}=0. \tag{4.2}$$

So, we can say that the number of Sophie Germain primes not exceeding (large) $x$ is much smaller than that of all the primes in **T** less than or equal to $x$.

Next, we would like to try to get a possible approximation of the positive-valued function $\delta(x)$ that satisfies

$$\pi_{\mathrm{T}}(x)=\left(\pi_{\mathrm{S}}(x)\right)^{\delta(x)}.$$

From the above discussion on $\pi_{\mathrm{T}}(x)$, it is necessary to observe the fact that

$$\frac{x}{\log x}\sim\left(\frac{2Cx}{(\log x)^2}\right)^{\delta(x)}$$

holds. Taking logarithms of both sides immediately leads to

$$\delta(x)\sim\frac{\log x-\log\log x}{\log(2Cx)-2\log\log x}=1+\frac{\log\log x-\log(2C)}{\log x-2\log\log x+\log(2C)}.$$

Therefore, it is possible to approximate $\delta(x)$ by $1+(\log\log x-\log(2C))/\log x$ with a small error. This conclusion is naturally consistent with (4.1) and (4.2).

All the results stated above are based on formula (1.1), and hence the above discussion serves just to reaffirm the authenticity of (1.1).

## 5. Congruences Characterizing S and T

In this section, we would like to search for possible congruences for identifying the sets $\mathbf{S}$ and $\mathbf{T}$. Hereafter, we always assume that $a \in \mathbb{Z}^+$.

### 5.1. Congruences Using the Value of a Polynomial

In what follows, let $p_n$ denote the $n$th prime, i.e., $p_1 = 2, p_2 = 3, p_3 = 5$, and so on. For any $a \in \mathbb{Z}^+$, let $p_{\ell(a)}$ be the largest prime satisfying $p_{\ell(a)} \leq \sqrt{2a+1}$ and define the set $\mathbf{P}_{\ell(a)}$ by

$$\mathbf{P}_{\ell(a)} := \left\{p \in \mathbf{P} \mid p \leq \sqrt{2a+1}\right\} = \{p_1, p_2, \ldots, p_{\ell(a)}\}.$$

The first prime $p_1 = 2$ always belongs to this set unless $a = 1$. It is obvious by the Eratosthenes sieve that if $a \not\equiv 0 \pmod{p}$ for all $p \in \mathbf{P}_{\ell(a)}$, then both $a$ and $2a+1$ are primes, and thus $a \in \mathbf{S}$.

For any $p \in \mathbf{P}$, consider the polynomial $f_p(X)$ in $X$ defined by

$$f_p(X) := \begin{cases} X & \text{for } \ p = p_1; \\ X\left(X - \dfrac{p-1}{2}\right) & \text{for all } \ p \in \mathbf{P}_{\ell(a)} \setminus \{p_1\}. \end{cases}$$

By evaluating the value of this polynomial at $X = a$ modulo $p$, it is possible to determine as to whether a given integer $a \geq 2$ is Sophie Germain or not.

**Theorem 5.1.** *The following are equivalent:*

(a) $a \in \mathbf{S}$;

(b) $f_{p_1}(a) \equiv 0 \pmod{p_1}$ *and* $f_p(a) \not\equiv 0 \pmod{p}$ *for all* $p \in \mathbf{P}_{\ell(a)} \setminus \{p_1\}$.

*Proof.* From what already has been said above, a proof may not be necessary, but we wish to repeat it briefly just to be sure. Since the case for $a = p_1$ is trivial, let $a \geq p_2$. Then, the condition in (b) such that

$$f_p(a) = \frac{1}{2}a(2a+1-p) \equiv \frac{1}{2}a(2a+1) \not\equiv 0 \pmod{p} \quad \text{for all } \ p \in \mathbf{P}_{\ell(a)} \setminus \{p_1\}$$

implies $a \in \mathbf{S}$ from the Eratosthenes sieve, and the reverse implication is also true. So (a) is equivalent to (b), as desired. □

Note that (b) is completely denied if $a$ is composite. In fact, if there exists a prime factor $q$ of $a$ with $2 \leq q < a$, then $q \in \mathbf{P}_{\ell(a)}$ and it satisfies $f_q(a) \equiv 0 \pmod{q}$. Therefore, every composite number does not apply to (b). In conclusion, an integer $a$ that satisfies (b) must be a prime.

Obviously, the negation of Theorem 5.1 can be stated as follows:

**Theorem 5.2.** *The following are equivalent:*

(c) $a \in \mathbf{T}$;

(d) *there exists at least one of* $p \in \mathbf{P}_{\ell(a)} \setminus \{p_1\}$ *such that* $f_p(a) \equiv 0 \pmod{p}$.

Summarizing Theorems 5.1 and 5.2, we get

$$\mathbf{S} = \{2\} \cup \left\{a \in \mathbb{Z}^+ \mid f_p(a) \not\equiv 0 \pmod{p} \text{ for all } p \in \mathbf{P}_{\ell(a)} \setminus \{p_1\}\right\};$$
$$\mathbf{T} = \left\{a \in \mathbb{Z}^+ \mid \text{there exists } p \in \mathbf{P}_{\ell(a)} \setminus \{p_1\} \text{ such that } f_p(a) \equiv 0 \pmod{p}\right\}.$$

For example, if $a = 131$, then $\mathbf{P}_{\ell(131)} = \{2, 3, 5, 7, 11, 13\}$, since $\lfloor\sqrt{2 \cdot 131 + 1}\rfloor = 16$. By direct verification, we see that $f_p(131) \not\equiv 0 \pmod{p}$ for all $p \in \mathbf{P}_{\ell(131)}$ and thereby $131 \in \mathbf{S}$. On the other hand, if $a = 157$, then $\mathbf{P}_{\ell(157)} = \{2, 3, 5, 7, 11, 13, 17\}$, since $\lfloor\sqrt{2 \cdot 157 + 1}\rfloor = 17$. In this case, we have $f_p(157) \equiv 0 \pmod{p}$ for $p = 3, 5, 7$, but $f_p(157) \not\equiv 0 \pmod{p}$ for $p = 11, 13, 17$. So we have verified that $157 \in \mathbf{T}$.

Here, we would like to briefly explain the main reason why we came up with the above polynomial $f_p(X)$. Let $a \in \mathbf{T}$, i.e., $a$ is not a Sophie Germain prime. From (d), there exists an odd prime $p$ in $\mathbf{P}_{\ell(a)}$ such that $f_p(a) \equiv 0 \pmod{p}$, so we have $a \equiv (p-1)/2 \pmod{p}$ since $p \nmid a$. Hence, $a$ can be expressed in the form

$$a = pr + \frac{p-1}{2} \quad \text{for some } r \in \mathbb{Z}^+,$$

which shows that $a \in \mathbf{A}(p)$ and so $a \in \mathbf{A}$. Since $\mathbf{T} = \mathbf{P} \cap \mathbf{A}$ from (2.2), it is quite reasonable to define the above $f_p(X)$ and evaluate its value at $X = a$ modulo $p$.

### 5.2. Congruences Derived from Wilson's Theorem

Next, we discuss possible congruence relations for Sophie Germain primes using Wilson's theorem, stating that $(n-1)! \equiv -1 \pmod{n}$ is valid only in the case when $n$ is a prime.

Here is the main result we want to mention in this subsection.

**Theorem 5.3.** *The following are equivalent:*

(a′) $a \in \mathbf{S} \setminus \{2\}$;

(b′) *one of the congruences given below holds true.*

$$\begin{aligned} &\text{(i)} \quad (a-1)! \equiv 2a - 1 \pmod{a(2a+1)}; \\ &\text{(ii)} \quad (a-1)! \equiv -(6a+1) \pmod{a(2a+1)}. \end{aligned} \tag{5.1}$$

*Proof.* If we observe the congruences in (5.1) for modulo $a$, then $a$ must be a prime from Wilson's theorem. Therefore, it is sufficient to prove the theorem only modulo $2a + 1$, that is to say,

$$\begin{aligned} &\text{(i)} \quad (a-1)! \equiv 2a - 1 \equiv (2a+1) - 2 \equiv -2 \pmod{2a+1}; \\ &\text{(ii)} \quad (a-1)! \equiv -(6a+1) \equiv -3(2a+1) + 2 \equiv 2 \pmod{2a+1}. \end{aligned} \tag{5.2}$$

(a$'$) $\Rightarrow$ (b$'$): Since $2a+1$ for $a \in \mathbf{S} \setminus \{2\}$ is a prime, Wilson's theorem provides

$$(2a)! \equiv -1 \pmod{2a+1}. \tag{5.3}$$

The left-hand side of this can be written as

$$\begin{aligned}(2a)! =&(a-1)! \prod_{j=1}^{a+1} ((2a+1)-j) \equiv (a-1)! \prod_{j=1}^{a+1} (-j) \\ \equiv&(a+1)a\{(a-1)!\}^2 \pmod{2a+1}.\end{aligned}$$

Multiplying the whole of this expression by 4,

$$4 \cdot (2a)! \equiv \{(2a+1)^2 - 1\}\{(a-1)!\}^2 \equiv -\{(a-1)!\}^2 \pmod{2a+1}.$$

Therefore, above (5.3) is equivalent to

$$\{(a-1)!\}^2 \equiv 4 \pmod{2a+1},$$

which implies that at least one of (5.2) (i) and (ii) holds true. These do not occur simultaneously because $2a+1 \nmid (a-1)!$, so only one of them is valid.

(b$'$) $\Rightarrow$ (a$'$): We prove that if either (5.2) (i) or (ii) holds, then $2a+1$ is a prime. Suppose that $2a+1$ is composite, i.e., $2a+1 = km$ with $k, m \in \mathbb{Z}^+$ such that $3 \le k \le m < 2a+1$. Since $k(m-2) \ge 3$, we can deduce the inequality

$$a - 1 = \frac{km-3}{2} = \frac{k(m-2) + 2k - 3}{2} \ge \frac{2k}{2} = k,$$

which gives $(a-1)! \equiv 0 \pmod{k}$ and hence $2 \equiv 0 \pmod{k}$ from (5.2), but this is contrary to $k \ge 3$. So $2a+1$ must be a prime and thus $a \in \mathbf{S} \setminus \{2\}$. □

Although we will not go into details here, the negation of Theorem 5.3 can also be easily derived. Summarizing all the discussion in this subsection, we get

$$\begin{aligned}&\mathbf{S} = \{2\} \cup \left\{a \in \mathbb{Z}^+ \mid a \text{ satisfies either (5.1) (i) or (ii)}\right\};\\ &\mathbf{T} = \{a \in \mathbf{P} \setminus \{2\} \mid a \text{ does not satisfy both (5.1) (i) and (ii)}\}.\end{aligned}$$

When $a \ge 3$ is fairly small, we can verify by hand calculations that $a = 11, 29$ (resp. $a = 3, 5, 23$) satisfy (5.1) (i) (resp. (ii)); but the prime $a = 7$ does not satisfy both of them, and so $7 \in \mathbf{T}$. When $a$ is large, it is technically impossible to directly clarify whether $a$ satisfies (5.1) (i) or (ii) without use of computer, because the amount of calculation is huge. For that reason, Theorem 5.3 itself may be interesting and meaningful in theory, but it has no practical application unlike Theorems 5.1 and 5.2. In any case, it is needed to find an efficient and reasonable algorithm for evaluating the rapidly growing factorial $(a-1)!$ modulo $a(2a+1)$ or modulo $2a+1$.

Lastly, we want to introduce some results involving primitive roots. Ramesh and Makeshwari [12] proved that if a prime $p$ is a primitive root of $2p+1$, then $p \in \mathbf{S}$ (see also [13] for a generalized version). Very recently, they also derived in [10] necessary and sufficient conditions for a prime $p$ to be a safe prime based on the number of primitive or semi-primitive roots of $p$. On the other hand, Ishii [7] showed that for a prime $p$ and an integer $n \geq 1$ with $n \equiv 1 \pmod 3$, if $np$ is a primitive root of $2p+1$, then $p \in \mathbf{S}$. In addition, Filipovski [6] revealed that the pairs $(p, k)$ ($p$ a prime; $k > 1$ an integer) for which $p$ is a primitive root of $2^k p + 1$ are only $(2, 2), (3, 3), (3, 4), (5, 4)$. Through these results, we can see that Sophie Germain primes and safe primes have many unexpected but very interesting connections to primitive or semi-primitive roots.

**Acknowledgments.** We would like to thank Andrew Granville and the anonymous referee for their various comments and suggestions, which were very helpful in improving the quality of this note. Furthermore, we would like to express our sincere gratitude to the editors who provided valuable comments and feedback at the early stages of the manuscript.

## References

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

[2] T. Agoh, A note on Fermat's congruence, *Integers* **25** (2025), #A31.

[3] L. N. Childs, *A Concrete Introduction to Higher Algebra*, 3rd ed., Springer-Verlag, New York, 2009.

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

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

[6] S. Filipovski, On prime primitive roots of $2^k p + 1$, *Math. Notes* **114** (5) (2023), 776–778.

[7] K. Ishii, A sufficient condition for a prime to be a Sophie Germain prime, *Amer. Math. Monthly* **131** (2) (2024), 169.

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

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

[10] M. Makeshwari and V. P. Ramesh, Characterizing safe primes via primitive roots, *Math. Mag.* **97** (4) (2024), 426–429.

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

[12] V. P. Ramesh and M. Makeshwari, A primitive root $p$ of $2p + 1$ is a Sophie Germain prime, *Amer. Math. Monthly* **129** (6) (2022), 538.

[13] V. P. Ramesh and M. Makeshwari, A note on generalized Sophie Germain primes: In the direction of Legendre's extended Sophie Germain primes, *Resonance* (Indian Academy of Sciences) **21** (6) (2023), 923–928.

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

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

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

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