Proceedings of International Conference on Mathematics
and Mathematics Education (ICMME 2018)
Turk. J. Math. Comput. Sci.
10(2018) 18–21

http://dergipark.gov.tr/tjmcs

MATDER

Notes on Sophie Germain Primes

Recep BAŞTAN[a], Canan AKIN*,[b]

[a] *Institute of Science, Giresun University, 28100, Giresun, Turkey.*
[b] *Department of Mathematics, Faculty of Arts and Science, Giresun University, 28200, Giresun, Turkey.*

Received: 24-07-2018 • Accepted: 12-10-2018

Abstract. In this paper, a pair of Sophie Germain prime and connected safe prime is referred to as SG-S-prime pair in short. We focus on a characterization to obtain SG-S-prime pairs owing to an eliminating method. We form some certain instructions for a sieve as an elementary method to find the SG-S-prime pairs and we also give an example in which we use our instructions to obtain the SG-S-prime pairs up to 250.
Wilson's fundamental theorem in number theory gives a characterization of prime numbers via a congruence. Moreover, in this paper, we give a characterization of Sophie Germain primes via a congruence.

2010 AMS Classification: 11A41

Keywords: Prime number, Sophie Germain primes, safe primes.

1. Introduction

If p is a prime and $2p + 1$ is also prime, then p is called a Sophie Germain prime. If p is a Sophie Germain prime, then $2p+1$ is called safe prime. These primes are considered in the Sophie Germain's paper, in connection with the first case of Fermat's last theorem. She proves that if p is a Sophie Germain prime, then $x^p + y^p = z^p$ has no solution in the case $p \nmid xyz$. It can be found details related to Fermat's last theorem and these primes in Ribenboim's books [10–12]. It is unknown whether there exist infinitely many such primes. The largest known proven Sophie Germain prime pair as of Feb. 29, 2016 is given by $(p, 2p + 1)$, where $p = 2618163402417.2^{1290000} - 1$, each of which has 388342 decimal digits [4]. It can be seen more details on Sophie Germain primes in some present references [1–3, 6, 8, 9]. This paper consists in two observation on Sophie Germain primes.

$2m$-prime pairs are related the twin prime pairs since a $2m$-prime pair is a twin prime pair if $m = 1$, where m is an arbitrary positive integer. In [7], Lampret gives sieves as an elementary method for eliminating $2m$-prime pairs. He divide all $2m$-prime pairs into the four groups. One of them is $6n$-prime pairs, whose both members are congruent to -1 modulo 6. These are of the form: $(6k - 1, 6k + 6n - 1)$ for some positive integers n and k. He give a characterization for $6n$-prime pairs of the form $(6k - 1, 6k + 6n - 1)$ in Theorem 2.7 in his study. In this paper, a Sophie Germain prime and the related safe prime is called SG-S-prime pair. One of the our observation is that we can use Lampret's results to find SG-S-prime pairs. In section 2, we give a method to find SG-S-prime pairs by using Lampret's results.

A theorem based on Wilson's theorem is formulated by Clement in [5]. Clement has a characterization of twin prime

*Corresponding Author
Email addresses: canan.ekiz@giresun.edu.tr, cananekiz28@gmail.com (C. Akın), recepbastan61@gmail.com(R. Baştan)

pairs. The other observation is related in a characterization of Sophie Germain primes. In section 3, we characterize the Sophie Germain primes with a congruence according to the mod $p(2p+1)$ in the light of the inspiration of Clement's theorem, where p is an integer.

2. SG-S-prime pairs by Lampret's results

In [7], Lampret give the following theorem:

Theorem 2.1 ([7]). *Let k and n be positive integers. $(6k-1, 6k+6n-1)$ is not a $(6n-2)$-prime pair if and only if there exist positive integers i and j such that one of the following holds true:*

(i) *$p := 6j-1$ is a prime and $k = pi + j$ or $k = pi + j - n$,*
(ii) *$p := 6j+1$ is a prime and $k = pi - j$ or $k = pi - j - n$.*

In both cases $p \leq \sqrt{6k+6n-1}$.

Except 2 and 3 each prime number is of the form $6k-1$ or $6k+1$ for some positive integer k. If the prime p is the form of $6k+1$, then it is not a Sophie Germain prime since $2p+1$ is not a prime. Hence, $(6k+1, 12k+3)$ is not SG-S-prime pair. Thus, SG-S-prime pairs are the form $(6k-1, 12k-1)$ for some positive integer k. So, SG-S-prime pairs become an $2m$-prime pair in Lampret's paper since $(12k-1)-(6k-1) = 6k$, where $2m = 6k$ for some positive integer k. By writing $n = k$ in Theorem 2.1, we obtain the following result.

Result 2.2. *Let k be a positive integer. $(6k-1, 12k-1)$ is not a SG-S-prime pair if and only if there exist positive integers i and j such that one of the following holds true:*

(i) *$p := 6j-1$ is a prime and $k = pi + j$ or $k = (pi + j)/2$.*
(ii) *$p := 6j+1$ is a prime and $k = pi - j$ or $k = (pi - j)/2$.*

In both cases $p \leq \sqrt{12k-1}$.

Let us describe this method for sieving SG-S-prime pairs up to a given positive integer z.
1. Write down a list of all integers $k = 1, 2, ..., \lceil z/6 \rceil$.
2. Find all primes $3 < p \leq \sqrt{z}$.
3. For each prime $3 < p \leq \sqrt{z}$, we do the following:
-if $6 \mid p+1$ then $j = (p+1)/6$ and so, cross out integers $k = pi + j$ and $k = (pi + j)/2$, and
-if $6 \mid p-1$ then $j = (p-1)/6$ and so, cross out integers $k = pi - j$ and $k = (pi - j)/2$ for all $i = 1, 2, \ldots$, from the list.
4. Each remaining integer k in the list gives us a SG-S-prime pair $(6k-1, 12k-1)$.

Example 2.3. *Let us find all SG-S-prime pairs up to 250. We list all integers $k = 1, 2, ..., 41$. Next, we find all primes $3 < p \leq \sqrt{250}$, these are $5, 7, 11, 13$.*

(i) *For $p = 5 = 6.1 - 1$, we have $j = 1$ and hence, we cross out all integers k of the form $5i + 1$ and $(5i + 1)/2$ from the list.*
(ii) *For $p = 7 = 6.1 + 1$, we have $j = 1$ and hence, we cross out all integers k of the form $7i - 1$ and $(7i - 1)/2$ from the list.*
(iii) *For $p = 11 = 6.2 - 1$, we have $j = 2$ and hence, we cross out all integers k of the form $11i + 2$ and $(11i + 2)/2$ from the list.*
(iv) *For $p = 13 = 6.2 + 1$, we have $j = 2$ and hence, we cross out all integers k of the form $13i - 2$ and $(13i - 2)/2$ from the list.*

Thus, it must be crossed out the bold integers from the following list:

1	2	***3***	4	5	***6***	7	***8***	9	***10***
11	***12***	***13***	14	15	***16***	***17***	***18***	19	***20***
21	22	***23***	***24***	***25***	***26***	***27***	***28***	29	30
31	32	***33***	***34***	***35***	***36***	***37***	***38***	39	40
41									

For each remaining integer k in the list, we get a SG-S-prime pair $(6k-1, 12k-1)$. Thus, by adding $(2, 5), (3, 7)$, we obtain all SG-S-prime pairs up to 250:
$(2, 5), (3, 7), (5, 11), (11, 23), (23, 47), (29, 59), (41, 83), (53, 107), (83, 167), (89, 179),$
$(113, 227), (131, 263), (173, 347), (179, 359), (191, 383), (233, 467), (239, 479)$

3. A Characterization of Sophie Germain Primes

We give two lemmas which are required for the proof of main theorem.

Lemma 3.1. *Let $p > 1$ be an integer. p is a prime number $\Leftrightarrow (p+1)^2[(p-1)!]^2 \equiv 1 \pmod{p}$.*
Proof. Using Wilson's Theorem

$$\begin{aligned} p \quad is \quad prime \quad number \quad &\Rightarrow (p-1)! \equiv -1 \pmod{p} \\ &\Rightarrow [(p-1)!]^2 \equiv 1 \pmod{p} \\ &\Rightarrow (p+1)^2[(p-1)!]^2 \equiv 1 \pmod{p} \end{aligned}$$

On the contrary, let $(p+1)^2[(p-1)!]^2 \equiv 1 \pmod{p}$ and let p be not a prime number. Thus, there exists a divisor t for p such that $1 < t < p$. On the other hand, if $(p+1)^2[(p-1)!]^2 \equiv 1 \pmod{p}$, then $[(p-1)!]^2 \equiv 1 \pmod{p}$. Hence, $[(p-1)!]^2 \equiv 1 \pmod{t}$. It is a contradiction since t is also a divisor for $[(p-1)!]^2$. So, p is a prime number.

Lemma 3.2. *$p > 2$ is a Sophie Germain prime if and only if $(p+1)^2[(p-1)!]^2 \equiv 1 \pmod{2p+1}$.*
Proof. Using Wilson's Theorem

$$\begin{aligned} 2p+1 \quad is \quad prime \quad number \quad &\Leftrightarrow (2p)! \equiv -1 \pmod{2p+1} \\ &\Leftrightarrow 2p.(2p-1).(2p-2)...(2p-p)(2p-p-1)! \equiv -1 \pmod{2p+1} \\ &\Leftrightarrow (-1).(-2).(-3)....(-p-1)(p-1)! \equiv -1 \pmod{2p+1} \\ &\Leftrightarrow (-1)^{p+1}.(p+1)!(p-1)! \equiv -1 \pmod{2p+1} \\ &\Rightarrow (p+1)!(p-1)! \equiv -1 \pmod{2p+1} \\ &\Leftrightarrow (p+1).p.(p-1)!(p-1)! \equiv -1 \pmod{2p+1} \\ &\Leftrightarrow (p+1).p.[(p-1)!]^2 \equiv -1 \pmod{2p+1} \\ &\Leftrightarrow (p+1).(p+p+1-p-1).[(p-1)!]^2 \equiv -1 \pmod{2p+1} \\ &\Leftrightarrow (p+1).(-p-1).[(p-1)!]^2 \equiv -1 \pmod{2p+1} \\ &\Leftrightarrow (p+1).(p+1).[(p-1)!]^2 \equiv 1 \pmod{2p+1} \\ &\Leftrightarrow (p+1)^2.[(p-1)!]^2 \equiv 1 \pmod{2p+1}. \end{aligned}$$

On the contrary, let $(p+1)^2.[(p-1)!]^2 \equiv 1 \pmod{2p+1}$ and let $2p+1$ be not a prime number. Thus, there exists a divisor t for $2p+1$ such that $1 < t < 2p+1$. On the other hand, since

$$\begin{aligned} (p+1)^2.[(p-1)!]^2 \equiv 1 \pmod{2p+1} \quad &\Leftrightarrow (p+1)!(p-1)! \equiv -1 \pmod{2p+1} \\ &\Rightarrow (1).(2).(3)....(p+1)(p-1)! \equiv -1 \pmod{2p+1} \\ &\Rightarrow (-2p).-(2p-1).-(2p-2)...-(2p-p)(p-1)! \equiv -1 \pmod{2p+1} \\ &\Rightarrow (-1)^{p+1}.2p.(2p-1).(2p-2)...(2p-p)(p-1)! \equiv -1 \pmod{2p+1} \\ &\Rightarrow (-1)^{p+1}.(2p)! \equiv -1 \pmod{2p+1} \end{aligned}$$

then $(-1)^{p+1}.(2p)! \equiv -1 \pmod{t}$. It is a contradiction since t is also a divisor for $(2p)!$. So, $2p+1$ is a prime number.

Theorem 3.3. *Let $p > 2$ be an integer. Then p is a Sophie Germain prime number if and only if $(p+1)^2.[(p-1)!]^2 \equiv 1 \pmod{p(2p+1)}$.*
Proof. It is straightforward from Lemma 3.1 and Lemma 3.2. Let $p > 2$ be a Sophie Germain prime number. By Lemma 3.2, $(p+1)^2.[(p-1)!]^2 \equiv 1 \pmod{2p+1}$ and p is prime. Thus, by Lemma 3.1, $(p+1)^2.[(p-1)!]^2 \equiv 1 \pmod{p}$. Hence, $(p+1)^2.[(p-1)!]^2 \equiv 1 \pmod{p(2p+1)}$ since $\gcd(p, 2p+1) = 1$. Conversely, let $(p+1)^2.[(p-1)!]^2 \equiv 1 \pmod{p(2p+1)}$. Thus, $(p+1)^2.[(p-1)!]^2 \equiv 1 \pmod{2p+1}$ and $(p+1)^2.[(p-1)!]^2 \equiv 1 \pmod{p}$. Hence, p is prime by Lemma 3.1. Therefore, p is a Sophie Germain prime number by Lemma 3.2.

References

[1] Alkalay-Houlihan C., Sophie Germain and Special Cases of Fermat's Last Theorem. http://www.math.mcgill.ca/darmon/courses/12-13/nt/projects/Colleen-Alkalay-Houlihan.pdf. Accessed: 2017-03-20. 1

[2] Bishop, S. A., Okagbue, H. I., Adamu, M. O., Olajide, F. A., Sequences of numbers obtained by digit and iterative digit sums of Sophie Germain primes and its variants, Global Journal of Pure and Applied Mathematics 12, 2 (2016), 1473-1480. 1

[3] Bucciarelli, L.L., Dworsky N., Sophie Germain: An essay in the history of the theory of elasticity, Vol. 6., Springer Science and Business Media, Netherland, 2012. 1

[4] Caldwell, C.K., Prime Pages. The Top Twenty: Sophie Germain. http://primes.utm.edu/top20/page.php?id=2. 1

[5] Clement, P. A., Congruences to sets of primes, Am. Math. Mon. 56 (1949), 23-25. 1

[6] Daniloff, L.L., The Work of Sophie Germain and Niels Henrik Abel on Fermat's Last Theorem. MS thesis. 2017. 1

[7] Lampret, S., Sieving 2m-prime pairs, Notes on Number Theory and Discrete Mathematics 20 (2014), 54-46. 1, 2, 2.1

[8] Liu, F., On the Sophie Germain prime conjecture, WSEAS Transactions in Math 10, 2 (2011), 421-430. 1

[9] Meireles, M., On Sophie Germain primes. Proc. 13th WSEAS Int. Conf. App. Math. (2008), 370-373. 1

[10] Ribenboim, P., 13 Lectures on Fermat's Last Theorem, Springer-Verlag, New York, 1979. 1

[11] Ribenboim, P., Fermat's Last Theorem for Amateurs, Springer-Verlag, New York, 1999. 1

[12] Ribenboim, P., The Little Book of Bigger Primes, 2nd ed., Springer-Verlag, New York, 2004. 1