A proof of Sophie Germain primes conjecture

Marko V Jankovic

A proof of Sophie Germain primes conjecture

Marko V. Jankovic

ARTORG Centre for Biomedical Engineering Research,
University of Bern, Switzerland

Abstract In this paper a proof of the existence of an infinite number of Sophie Germain primes, is going to be presented. In order to do that, we analyze the basic formula for prime numbers and decide when this formula would produce a Sophie Germain prime, and when not. Originally very difficult problem (in observational space) has been transformed into a simpler one (in generative space) that can be solved.

1 Introduction

A prime p is a Sophie Germain prime if $2p + 1$ is prime, too [1]. In that case the prime number $2p + 1$ is called safe prime. These special primes have applications in public key cryptography, pseudorandom number generation, and primality testing; see, for example, [2, 4, 6]. Originally, they have been used also in the investigation of cases of Fermat's last theorem [3]. It has been conjectured that there exist infinitely many Sophie Germain primes, but this was unproven (see for instance, [5]).

In this paper it is going to be proved that exists an infinite number of Sophie Germain primes. The problem is addressed in generative space, which means that prime numbers are not going to be analyzed directly, but rather their representatives, in the other space, that can be used to produce them.

Remark: *Prime numbers 2 and 3 are in a sense special primes, since they do not share some of the common features of all other prime numbers. For instance, every prime number, part from 2 and 3, can be expressed in the form $6l + 1$ or $6l - 1$, where $l \in N$. So, in this paper most of the time we analyze prime numbers bigger than 3. It has to be said that both 2 and 3 are Sophie Germain primes, but that has no impact on the conclusion of this paper.*

2 Proof

Outline of the proof: *First, the numbers that cannot be used for generation of Sophie Germain primes, are going to be analyzed. It is going to be shown that that number is smaller than the number of numbers that are used for generation of composite odd numbers. It is well known that exist infinite number of numbers that are used for generation of the prime numbers (odd prime numbers), and they represent the numbers that are not composite odd numbers. From that fact, it is easy to conclude that the number of numbers that can be used for generating Sophie Germain primes is infinite, too.*

It is easy to check that any prime number (apart form 2 and 3) can be expressed in the form $6l+1$ or $6s-1$ ($l, s \in N$). Having that in mind, it is easy to check that numbers in the form $6l + 1$, could never be Sophie Germain primes since the safe prime is in the form

$$2(6l + 1) + 1 = 12l + 3 = 3(4l + 1),$$

and that is composite number divisible by 3. So, the prime number that can potentially be Sophie Germain prime must be in the form $6s - 1$ and then the safe prime is going to be in the form $6(2s) - 1$.

We denote any composite number (that is represented as a product of prime numbers bigger than 3) with *CPN*5. Also, we mark with *mpl* a number in the form $6l + 1$, and with *mps* a number in the form $6s - 1$ ($l, s \in N$). In that case, it is easy to check that any composite number *CPN*5 can be expressed in the form *mpl x mpl*, *mps x mps* or *mpl x mps*.

So, if we have a number in the form $6k - 1$ that is composite number it must hold

$$k = \frac{CPN5 + 1}{6}$$

Since *CPN*5 should be in the *mps* form, *CPN*5 can be generally expressed as a product *mpl* x *mps*, or

$$mpl = 6x + 1 \text{ and } mps = 6y - 1 (x, y \in N),$$

which leads to

$$CPN5 = mpl \text{ x } mps = 6(6xy - x + y) - 1, \tag{2.2}$$

or, due to symmetry

$$mpl = 6y + 1 \text{ and } mps = 6x - 1,$$

which leads to

$$CPN5 = mpl \text{ x } mps = 6(6xy + x - y) - 1, \tag{2.3}$$

So, if we replace (2.2) or (2.3) in (2.1) we obtain forms of k that potentially cannot produce a Sophie Germain prime number. Those forms are expressed by the following equation

$$k = (6x - 1)y + x \tag{2.4a}$$

$$k = (6x + 1)y - x \tag{2.4b}$$

where $x, y \in N$, and they are equivalent (they will produce the same numbers). Having that in mind, it is possible to use one or the other form interchangeably.

Also, we know that safe prime which is generated by $2k$ cannot be composite if we would like to have Sophie Germain pair. If the safe number is composite the following equation must hold

$$k = \frac{CPN5+1}{6*2} \tag{2.5}$$

where *CPN*5 is composite number in the *mps* form. Using the same analysis as in the previous case, and replacing for instance (2.2) in (2.5), we obtain additional cases in which k cannot be used to produce Sophie Germain prime pairs, and they are defined by the following equation

$$k = \begin{cases} (6x-1)y + \frac{x}{2}, & x\ is\ even \\ (6x-1)y + 3x + \frac{x-1}{2}, & x\ is\ odd \end{cases} \tag{2.6}$$

where $x, y \in N$. Alternatively, it is possible to use the equation (2.3) and replace it in (2.5). In that case we can obtain different equations that produce the same numbers as the equation (2.6).

Equations (2.4b) and (2.6) (alternatively (2.4a) and (2.6) give a sufficient and necessary condition for k, so that it cannot be used for generation of the prime pairs in the form (p; $2p + 1$). In order to prove that there are infinitely many prime pairs in the form (p, $2p + 1$) we need to prove that exists infinitely many k that cannot be expressed in the form (2.4b) or (2.6). First, we will check the form of (2.4b, 2.6) for some values of x.

Case x=1: $k = 7y - 1, k = 5y + 3$

Case x=2: $k = 13y - 2, k = 11y + 2$

Case x=3: $k = 19y - 3, k = 17y + 10$

Case x=4: $k = 5(5y-1) + 1$, $k = 23y + 2$ *(equivalence of the equations (2.4a) and (2.4b) is used)*

Case x=5: $k = 31y - 5$, $k = 29y + 17$

Case x=6: $k = 37y - 6$, $k = 5(7y) + 3$

Case x=7: $k = 43y - 7$, $k = 41y + 24$

Case x=8: $k = 7(7y - 1) - 1$, $k = 47y + 4$

So, we can see that k is represented by the threads (series of numbers) that are defined by prime numbers bigger than 3. From examples, we can see that if $(6x - 1)$ or $(6x + 1)$ represent a composite number, k that is represented by that number has also representation by one of the prime factors of that composite number. This can be easily proved in the general case, by direct calculation, using representations similar to (2.2, 2.3). Here only one case is going to be analyzed. All other cases can be analyzed analogously. In this case we assume

$$(6x - 1) = (6l + 1)(6s - 1)$$

where ($l, s \in N$), we have

$$x = 6ls - l + s.$$

Having that in mind, and selecting one representation of k that includes form $(6x - 1)$, we have

$$k = (6x - 1)y + x = (6l + 1)(6s - 1)y + 6ls - l + s$$

or

$$k = (6x - 1)y + x = (6l + 1)(6s - 1)y + s(6l + 1) - l = (6l + 1)\big((6s - 1)y + s\big) - l$$

which means

$$k = (6l + 1)f - l$$

and that represents already existing form of the representation of k for factor $(6l+1)$, where

$$f = (6s - 1)y + s.$$

Here we used the equivalency of the equations (2.4a) and (2.4b). It can be seen that all patterns for k that potentially result in composite number, include prime numbers. Now, it is going to be proved that the number of k that cannot be represented by the models (2.4b, 2.6) is infinite.

In order to do that, we are going to analyze the formula for the odd numbers and formula for the odd composite numbers. It is well known that odd numbers a can be represented by the following formula

$$a = 2n + 1,$$

where $n \in N$. It is not difficult to prove that all composite odd numbers a_c could be presented by the following formula

$$a_c = 2(2ij + i + j) + 1 = 2\big((2j + 1)i + j\big) + 1, \qquad (2.7)$$

where $i, j \in N$. (Hint: It is simple to conclude that all composite numbers could be represented by the product (i+1) * (j+1), where $i, j \in N$. If we check how that formula looks like for the odd numbers, after simple calculation, equation (2.7) is obtained.)

It is clear that prime numbers are odd numbers that cannot be represented by the previous formula and we know that the number of the primes is infinite. Now, we are going to check what numbers can be presented by the formula $m = 2ij + i + j$ for some j.

Case j=1: $m = 3i + 1$

Case j=2: $m = 5i + 2$

Case j=3: $m = 7i + 3$

Case j=4: $m = 3(3i + 1) + 1$

Case j=5: $m = 11i + 5$

Case j=6: $m = 13i + 6$

Case j=7: $m = 5(3i + 1) + 2$

Case j=8: $m = 17i + 8$

Again we can see that we have m that is represented by threads that are represented by odd prime numbers. Here, again, we can see that the threads that are generated by composite numbers can be generated by some of the threads defined by one of the factors of that composite number. That can be easily checked. Comparing to the threads that define k, that represent numbers that cannot generate Sophie Germain primes, we can see that in both cases we have threads defined by the same numbers, with the only difference that in the case of composite primes we have an additional thread that is defined by number 3. Having in mind that threads that define m will leave infinite number of numbers that cannot be represented by (2.7), we can conclude that the number of k that cannot be represented by the models (2.4b, 2.6) is also infinite. And that completes the proof that number of Sophie Germain primes is infinite.

Although, it is not going to be analyzed here, it can be said that using very similar method it can be proved that the number of twin primes is infinite.

References

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

[2] M. Agrawal, N. Kayal, N. Saxena. PRIMES is in P, Ann. of Math. 160(2) (2004), 781-793.

[3] H. M. Edwards. Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory, Springer, 2000.

[4] R.A.J. Matthews. Maximally periodic reciprocals, Bull. Inst. Math. Appl. 28 (1992), 147-148.

[5] V. Shoup. A Computational Introduction to Number Theory and Algebra, Cambridge University Press, 2009.

[6] W.-S. Yap, S.L. Yeo, S.-H. Heng, M. Henricksen. Security analysis of GCM for communication, Security and Communication Networks 7(5) (2014), 854-864.