Proof That an Infinite Number of Sophie Germain Primes Exist

Stephen Marshall

29 Aug 2014

Abstract: In number theory, a prime number p is a Sophie Germain prime if 2p + 1 is also prime. For example, 29 is a Sophie Germain prime because it is a prime and 2 × 29 + 1 = 59, and 59 is also a prime number. These numbers are named after French mathematician Marie-Sophie Germain. We shall prove that there are an infinite number of Sophie Germain primes.
Keywords: Sophie Germain primes, Prime Numbers
AMS Classification:11A41.

1. Introduction

Marie-Sophie Germain; April 1, 1776 – June 27, 1831) was a French mathematician, physicist, and philosopher. When Germain was 13, turned to her father's library for entertainment, and quickly became fascinated in mathematics. She studied every book on mathematics in her father's library (see reference 3), even teaching herself Latin and Greek so she could read works like those of Sir Isaac Newton and Leonhard Euler.

One of Germain's areas of expertise was number theory, and she introduced Sophie Germain Primes. A Sophie Germain Prime states that a prime number p is a Sophie Germain prime if 2p + 1 is also prime.

We shall prove that there are only a finite number of Sophie Germain primes. The first few Sophie Germain primes are:

2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, …...

It has been conjectured that there are an infinite number of Sophie Germain primes, however, this has never been proven or disproven, and we shall disprove this conjecture, proving there are an infinite number of Sophie Germain primes. This paper presents a complete and exhaustive proof that there exists an infinite number of Sophie Germain Primes. The approach to this proof begins by using same logic that Euclid used to prove there are an infinite number of prime numbers. Finally we prove that if p > 1 and d > 0 are integers, that p and p + d are both primes if

and only if for integer n (see reference 1 and 2):

$$n = (p-1)!\left(\frac{1}{p} + \frac{(-1)^q d!}{p + d}\right) + \frac{1}{p} + \frac{1}{p+d}$$

We use this proof for d = 2p +1 to prove that only a finite number of Sophie Germain Primes exist.

2. Proof of Finite Number of Sophie Germain Primes

We shall begin by using Euclid's logic that he used to prove there are an infinite number of prime numbers to attempt to prove there are a finite number Sophie Germain Primes.

First we shall assume there are only a finite number of n Sophie Germain Primes for all positive integers, specifically;

1) The finite set is: $p_1, (2p_1 + 1), p_2, (2p_2 + 1) \ldots, p_{n-1}, (2p_{n-1} + 1), p_n, (2p_n + 1)$

2) Let $N = p_1(2p_1 + 1)p_2(2p_2 + 1) \ldots, p_{n-1}(2p_{n-1} + 1)p_n(2p_n + 1) + 1$

By the fundamental theorem of arithmetic, N is divisible by some prime q. Since N is the product of all existing Sophie Germain Primes plus 1, then this prime q cannot be among the p_i, $2p_i + 1$ that make up the n Sophie Germain Primes since by assumption these are all the Sophie Germain Primes that exist and N is not divisible by any of the p_i, $2p_i + 1$ Sophie Germain Primes. N is clearly seen not to be divisible by any of the p_i, $2p_i + 1$ Sophie Germain Primes. First we know that 2 is a prime number that is not in the set of finite twins since 2 + 2 = 4 and 4 is not prime. We also know that 2 is the only even prime number, therefore, for the finite set of Sophie Germain Primes all of the p_i, $2p_i + 1$are odd numbers. Since the product of odd numbers is always odd, then the product of all the p_i, $2p_i + 1$ in our finite set of Sophie Germain Primes is an odd number. Since N is product of all the p_i, $2p_i + 1$, + 1, then N is an even number, and since all the p_i, $2p_i + 1$ are odd numbers and N is even, then N is not divisible by any of the p_i, $2p_i + 1$ Sophie Germain Primes. Therefore, q must be another prime number that does not exist in the finite set of Sophie Germain Prime numbers. Therefore, since this proof could be repeated an infinite number of times we have proven that an infinite number of prime numbers q exist outside of our finite set of Sophie Germain Primes.

Now we must prove that two of these infinite prime numbers, q, are Sophie Germain Primes. We will pick a prime number p from the infinite set of primes outside our finite set of Sophie Germain Primes and we will need to prove that there does exist a prime 2p + 1 that is also

prime. Both p and 2p + 1 do not exist in the finite set of Sophie Germain Primes. Note we are not proving this for all q primes outside the finite set of Sophie Germain Primes, we are only picking one prime, p, from the infinite set of primes and then we will attempt to prove that p+2 is also prime, this will show that a Sophie Germain Prime exists outside our finite set of Sophie Germain Primes.

First we shall show that if 2p + 1 is prime it cannot be in the set of finite p_i, $2p_i + 1$ Sophie Germain primes above. Since p is a prime number that does not exist in the set of finite Sophie Germain Primes, then if there exists a prime number equal to p +2 that is prime, it would be a Sophie Germain Prime to p; therefore a prime p+2 cannot be in the set of finite n Sophie Germain Primes otherwise p would be in the set of n finite Sophie Germain Primes and we selected a prime, p, that is not in the set of fine Sophie Germain Primes, therefore if p +2 is prime it cannot be in the finite set of Sophie Germain Primes since it would be Sophie Germain to p and p is not in the finite set.

Now we shall proceed to prove 2p + 1 is prime as follows:

We will prove that if p > 1 and d > 0 are integers, that p and p + d are both primes if and only if for positive integer n (see reference 1 and 2):

$$n = (p-1)!\left(\frac{1}{p} + \frac{(-1)^{q} d!}{p + d}\right) + \frac{1}{p} + \frac{1}{p+d}$$

Proof:

The equation above can be reduced and re-written as:

$$3) \quad \frac{(p-1)! + 1}{p} + \frac{(-1)^{q} d!\,(p-1)! + 1}{p+d}$$

Since $(p + d - 1)! = (p + d - 1)(p + d - 2)\cdots(p + d - d)(p - 1)!$, we have $(p + d - 1)! \equiv (-1)^{d} d!(p - 1)! \pmod{p + d}$, and it follows that equation 3 above is an integer if and only if:

$$4) \quad \frac{(p-1)! + 1}{p} + \frac{(p+d-1)! + 1}{p+d}$$

is an integer. From Wilson's Theorem, if p and $p + d$ are two prime numbers, then each of the terms of, equation 4 above, is an integer, which proves the necessary condition. Wilson's Theorem states:

That a natural number $n > 1$ is a prime number if and only if

$$(n-1)! \equiv -1 \pmod{n}.$$

That is, it asserts that the factorial $(n-1)! = 1 \times 2 \times 3 \times \cdots \times (n-1)$ is one less than a multiple of n exactly when n is a prime number. Another way of stating it is for a natural number $n > 1$ is a prime number if and only if:

When (n − 1)! is divided by n, the remainder minus 1 is divides evenly into (n-1)!

Conversely, assume equation 4 above, is an integer. If p or $p + d$ is not a prime, then by Wilson's Theorem, at least one of the terms of (4) is not an integer. This implies that none of the terms of equation 4 is an integer or equivalently neither of p and $p + d$ is prime. It follows that both fractions of (4) are in reduced form.

It is easy to see that if a/b and a'/b' are reduced fractions such that $a/b + a'/b' = (ab' + a'b)/(bb')$ is an integer, then $b|b'$ and $b'|b$.

Applying this result to equation 4, we obtain that $(p+d)|p$, which is impossible. We may therefore conclude that if equation 4 is an integer, then both p and $p + d$ must be prime numbers. Therefore, the equation below is proven since it can be reduced to equation 3 above.

Therefore, since the below equation can be reduced to equation 3 above, we have proven that if p > 1 and d > 0 are integers, then p and p + d are both primes if and only if for integer n:

$$n = (p-1)!\left(\frac{1}{p} + \frac{(-1)^d d!}{p+d}\right) + \frac{1}{p} + \frac{1}{p+d}$$

For our case p is known to be prime and d = p + 1 for Sophie Germain Primes.

Therefore, $n = (p-1)!((1/p) + ((-1)^{(p+1)} + (p+1)!)/(2p+1)) + 1/p + 1/(2p+1)$

Since p + 1 is an odd number, then $(-1)^{(p+1)} = 1$

Reducing, $np = p!((1/p) - (p+1)!/(2p+1)) + 1 + p/(2p+1)$

Reducing again, $(2p+1)np = (2p+1)p!((1/p) - (2p+1)!/(2p+1)) + (2p+1) + p$

Reducing again, $(2p+1)np = p!((2p+1)/p - (2p+1)!)) + 3p + 1$

Reducing again, $(2p+1)np = p(p-1)!((2p+1)/p - (2p+1)!)) + 3p + 1$

And reducing one final time, $(2p+1)np = (p-1)!((2p+1) - p(2p+1)!)) + 4p + 1$

We already know p is prime, therefore, p = integer. To prove there are an infinite number of Sophie Germain Primes, we must show that n is a positive integer. Since p is an integer the right hand side of the above equation is an integer. Since the right hand side of the above equation is an integer and p is an integer on the left hand side of the equation, then n must be an integer for the left side of equation to be an integer, or n would need to be a rational fraction that is divisible by p. This implies that $n = \frac{x}{p}$ where, p is prime and x is an integer. Then $p = \frac{x}{n}$, since p is

prime, then p is only divisible by p and 1, therefore, n can only be equal to p or 1 in this case, which are both integers, thus n must be an integer. It suffices to show that n is an integer since we have proven that p and p + d, where d = p +1, are both primes if and only if for integer n:

$$n = (p-1)!\left(\frac{1}{p} + \frac{(-1)^d d!}{p+d}\right) + \frac{1}{p} + \frac{1}{p+d}$$

Since n = integer, we have proven that p and 2p + 1 are both prime. Since we proved earlier that if 2p + 1 is prime then it also is not in the finite set of p_i, $p_i + 1$ Sophie Germain primes, therefore, since we have proven that 2p + 1 is prime, then we have proven that there is a Sophie Germain prime outside the our assumed finite set of Sophie Germain primes. This is a contradiction from our assumption that the set of Sophie Germain primes is finite, therefore, by contradiction the set of Sophie Germain primes is infinite. Also this same proof can be repeated infinitely for each finite set of Sophie Germain primes, in other words a new Sophie Germain

prime can added to each set of finite Sophie Germain primes. This thoroughly proves that an infinite number of Sophie Germain primes exist.

References:

[1] TYCM, Vol. 19, 1988, p. 191

[2] 1001 Problems in Classical Number Theory, Jean-Marie De Koninck and Armel Mercier, 2004

[4] Cipra, Barry. “A Woman Who Counted.” Science 319.5865 (2008): 899. Web. Sept. 2009

[5] Mackinnon, Nick, “Sophie Germain, or, was Gauss a feminist?” p. 348.

[6] Moncrief, J. William. "Germain, Sophie." Mathematics. Ed. Barry Max Brandenberger, Jr.. Vol. 2. New York: Macmillan Reference USA, 2002. 103. Web. 15 Sept. 2009 4 vols.