The Semiprime Equivalent Proof of the Goldbach Conjecture

Stephen Marshall

14 June 2023

Abstract

In number theory, for very difficult Number theory problems that have been open and unsolved for long periods of time it can often be wise to take alternative approaches to the problem. There more old unsolved Number Theory problems than most would think. The Goldbach's conjecture is one of the oldest and best-known unsolved problems in number theory and all of mathematics, it has been unsolved for over 281 years. On 7 June 1742, the German mathematician Christian Goldbach wrote a letter to Leonhard Euler (letter XLIII) in which he proposed the following conjecture:

Every even integer which is ≥ 4 can be written as the sum of two primes. It also states that every even natural number greater than 2 is the sum of two prime numbers. Or more specifically, that the "strong" Goldbach Conjecture asserts that all positive even integers ≥ 4 can be expressed as the sum of two primes. Two primes (p,q) such that p + q = 2n for n a positive integer ≥ 2.

The conjecture has been shown via computer to hold for all integers less than 4×10^{18}, but remains unproven despite enormous effort by many mathematicians over hundreds of years. Even the author has spent much effort attempting to solve this conjecture using several different direct methods and have come very close but was not able to prove the Goldbach Conjecture using any of these direct approaches. All of this effort made the author realize how difficult the Goldbach Conjecture is to solve using direct approaches, so this made him consider looking for a back door approach, or a work around the direct approaches. Any such approach could be different than the Goldbach Conjecture, but if it is a different Conjecture must be the equivalent of the Goldbach Conjecture, conjecture otherwise it would not solve the Goldbach Conjecture. This is exactly what the author has done, an equivalent conjecture has been developed and proven, thus solving the Goldbach Conjecture. Therefore, we call this a “back door” proof of the Goldbach Conjecture.

Proof:

Recall that a semiprime is a natural number that is the product of exactly two prime numbers.

An example first few semiprimes are 4, 6, 9, 10, 14, 15, …

The following proposed Semiprime Equivalent Conjecture is equivalent to the Goldbach conjecture. We shall prove so below:

Semiprime Equivalent Conjecture:

For all $n \geq 2$, there exists a whole number m such that $0 \leq m \leq n-2$ and $n^2 - m^2$ is a semiprime.

To help demonstrate that the Semiprime Equivalent Conjecture is equivalent to the Goldbach Conjecture we need to prove that $n^2 - m^2$ is a semiprime if and only if $n – m$ and $n + m$ are both prime.

Proof: Since $n^2 - m^2 = (n - m)(n + m)$, then it follows that $n – m$ and $n + m$ must also both be prime for $n^2 - m^2$ to be semiprime, since $n^2 - m^2$ must be the product of two prime numbers to be semiprime.

Now we will prove the **Semiprime Equivalent Conjecture:**

Specifically, we will prove that the Semiprime Equivalent Conjecture is Equivalent to the Goldbach Conjecture:

First, assume the Goldbach conjecture and suppose we are given a whole number $n \geq 2$. We Then by assumption $2n = p + q$ for some prime numbers p and q.

Assume without loss of generality we assume that $p \leq q$, then by the Semiprime Equivalent Conjecture, there exists a whole number m such that $0 \leq m \leq n-2$ and since $2n = p + q$ we can state the following two equations are equivalent using simple algebra:

- $p = n - m$
- $q = n + m$

Multiplying both sides of the above two equations yields the following:

$pq = (n - m)(n + m)$

Since $(n - m)(n + m) = n^2 - m^2$

Therefore, this implies that $n^2 - m^2 = (n - m)(n + m) = p\cdot q$.

So, we can conclude that $n^2 - m^2$ is a semiprime since both p and q are prime.

Conversely, assume the Semiprime Equivalent Conjecture and suppose we are given a number 2n with $n \geq 2$. We need to show that 2n can be written as a sum of two primes.

By assumption, we can find a number m with $0 \leq m \leq n-2$ and $n^2 - m^2$ a semiprime. And since $n^2 - m^2 = (n - m)(n + m)$ then both $(n – m)$ and $(n + m)$ must be prime numbers but then we have

$2n = (n - m) + (n + m)$, thus 2n must be the sum of two primes. Thus, we have proven that the Semiprime Equivalent Conjecture is the equivalent of the Goldbach Conjecture. And we have proven that the Goldbach Conjecture is the equivalent of the Semiprime Equivalent Conjecture. Thus, this completes the proof of the equivalence of both conjectures. We will proceed with a proof of the Semiprime Equivalent Conjecture to provide a proof of the Goldbach Conjecture. We have chosen this method because it is much simpler to prove the Semiprime Equivalent Conjecture than to attempt a direct proof of the Goldbach Conjecture. However, the result is the same since the Goldbach Conjecture will be proven, even though in an indirect method.

Now we shall proceed to prove the Semiprime Equivalent Conjecture in order to prove the Goldbach Conjecture. We will use Fermat's Factorization Method to prove the Semiprime Equivalent Conjecture. Fermat, in a letter to Mersenne around 1643, exposed an algorithm to factor odd integers by writing them as a difference of two squares. Fermat was responding to a challenge proposed by Mersenne. Fermat and Euler contributed much towards developing factorization methods. Our proof using Fermat's Factorization Method is provided below:

Fermat's Factorization Method

Fermat knew that every odd number, x, could be written as the difference of two squares ($x = n^2 – m^2$). A proof of this theorem is provided by the author below:

Proof: Let x be an odd number and re-write x as $x = y_1y_2$ with $y_1 \leq y_2$ (y_1 can equal 1). Since x is odd, y_1 and y_2 are both odd. Let $n = ½(y_1 + y_2)$ and $m = ½(y_2 – y_1)$. Notice that n and m are both integers, since y_1 and y_2 are both odd. Then y_1 = n-m and y_2 = n+m, so $x = y_1y_2 = (n-m)(n+m) = n^2 – m^2$. Thus, we have proven that every odd number, x, can be written as the difference of two squares.

A similar proof is provided, in Lemma 3.9, below from a textbook by the University of Sargodha (Reference 2).

Lemma 3.9: If *n* is an odd positive integer, then there is a one-to-one correspondence between factorizations of *n* into two positive integers and differences of two squares that equal *n*.

Proof: Let *n* be an odd positive integer and let *n* = *ab* be a factorization of *n* into two positive integers. Then *n* can be written as the difference of two squares, because

$$n = ab = s^2 - t^2,$$

where $s = (a+ b)/2$ and $t = (a - b)/2$ are both integers because *a* and *b* are both odd.

Conversely, if *n* is the difference of two squares, say, $n = s^2 - t^2$, then we can factor

n by noting that $n = (s - t)(s + t)$.

Recall that our Semiprime Equivalent Conjecture states:

For all n ≥ 2, there exists a whole number m such that 0 ≤ m ≤ n-2 and $n^2 - m^2$ is a semiprime.

However, our proof of Fermat's Factorization Method proves that:

Every odd number, x, can be written as the difference of two squares ($x = n^2 – m^2$).

Therefore, $n^2 - m^2$ in our Semiprime Equivalent Conjecture must be odd. However, since every prime number other than 2 is odd, then every semiprime number must be odd other than 2p, for any prime number p. However, recall that the Semiprime Equivalent Conjecture states:

For all $n \geq 2$, there exists a whole number m such that $0 \leq m \leq n-2$ and $n^2 - m^2$ is a semiprime.

Also recall, that we have proven that $n^2 - m^2$ is a semiprime if and only if $n - m$ and $n + m$ are both prime.

Therefore, we must also show that $n^2 - m^2 = 2p$, for any prime number p. But we know that $(n - m)$ and $(n + m)$ must both prime.

Therefore, $n^2 - m^2 = (n - m)(n + m) = 2p$.

Reducing $p = (n - m)(n + m)/2$, therefore either $(n - m)$ or $(n + m)$ must be divisible by 2, since both are prime the only way that either can be divisible by 2 is if one is for one to be equal to 2.

Thus $(n - m) = 2$ or $(n + m) = 2$. $(n + m)$

If $(n - m) = 2$

Thus, $n^2 - m^2 = (n - m)(n + m) = 2(n + m)$. However, we know that $(n + m)$ is prime and 2 is prime, so $2(n + m)$ is semiprime. Thus, $n^2 - m^2$ is semiprime.

If $(n + m) = 2$

Thus, $n^2 - m^2 = (n - m)(n + m) = 2(n - m)$. However, we know that $(n - m)$ is prime and 2 is prime, so $2(n - m)$ is semiprime. Thus, $n^2 - m^2$ is semiprime.

Therefore, we have proven that all semiprime numbers are of form $n^2 - m^2$, thus we have proven that the Semiprime Equivalent Conjecture is true for all semiprime numbers. Also, since the Semiprime Equivalent Conjecture is equivalent to the Goldbach Conjecture, thus we have also proven that the Goldbach Conjecture is true for all even numbers (2n). Specifically, we have proven that for every even integer N, and $N > 2$, then $N = p + q$, where p, and q, are prime numbers.

Although a direct proof of the Goldbach Conjecture remains unsolved, the Goldbach Conjecture now has been unequivocally proven through this “back door” novel approach using an equivalent conjecture for a remarkably simple proof.

We would be remiss not to mention that this proof of the “strong” Goldbach Conjecture also implies a proof of the “weak” Goldbach Conjecture. The “weak” Goldbach Conjecture, also known as the ternary Goldbach problem, states that every odd number greater than 5 can be expressed as the sum of three primes. (A prime may be used more than once in the same sum). The Goldbach Conjecture provides that every even number greater than 4 is the sum of two odd primes. Adding 3 to each even number greater than 4 will produce the odd numbers greater than 7 (and 7 itself is equal to 2+2+3). Since 3 is prime we have proven the “weak” Goldbach Conjecture with the proof of the “strong” Goldbach Conjecture.

This is not the first proof of the “weak” Goldbach Conjecture, Harald Helfgott proved the weak conjecture before the “strong” Goldbach Conjecture was ever proven. The author was not taking credit for its proof, he was merely stating that it has been known since Goldbach’s time that a proof of the “strong” Goldbach Conjecture implies a proof of the “weak” Goldbach Conjecture.

References

1. A Reformulation of the Goldbach Conjecture, LARRY J. GERSTEIN, University of California, Santa Barbara, CA 93106.

2. Factorization Methods and the Fermat Numbers, Textbook University of Sargodha.

3. A Fast Factorization of Semi-Primes Using Sum of Squares, Anthony Overmars and Sitalakshmi Venkatraman, Department of Information Technology, Melbourne Polytechnic, 11 June 2019.

4. The Fermat Factorization Method Revisited, Robert Erra and Christophe Grenier, 30 June 2009.

5. A Study of Goldbach's Conjecture and Polignac's Conjecture Equivalence Issues, Jian Ye and Chenglian Liu, Long Yan University

6. Additively and Multiplicatively Structured Sets, Dmitrii Zhelezov, Department of Mathematical Sciences Chalmers University of Technology and University of Gothenburg, 2015.

7. Guy, Richard K., Unsolved problems in number theory, (3rd edition). Springer-Verlag (2004).

8. From Euclid to Present: A Collection of Proofs regarding the Infinitude of Primes, Lindsey Harrison, December 14, 2013.

9. (Dun) W. Dunham, “Journey Through Genius: The Great Theorems of Mathematics," Penguin Books, John Wiley and Sons, 1990.