

Prime Faux Pas

Amanda Seitz

May 6, 2008

Abstract

There have been many conjectures made about prime numbers. We will look at a few of the major conjectures, discuss why they were thought to be true, and prove that they are false.

1 Introduction

The theory of numbers, more than any other branch of pure mathematics, has begun by being an empirical science. Its most famous theorems have all been conjectured, sometimes a hundred years or more before they have been proved; and they have been suggested by the evidence of a mass of computation.

G. H. Hardy (1877 – 1947) [1]

Most conjectures made about prime numbers take years to solve. In this paper, we will discuss why prime number conjectures are usually false, why proving these conjectures takes so many years, a couple of prime conjectures that were proposed centuries ago and have been proven false, and some unsolved prime conjectures.

1.1 Why are Prime Conjectures Usually False?

Over the years, there have been many conjectures made about the prime numbers. A *prime number* is a number that cannot be written as a product of any two numbers, except for itself and 1; this means that a prime number only has two factors, itself and 1. The number 1 is not considered a prime number since the only factor of one is itself. Some prime conjectures have been proven true, some have been proven false, and others still have yet to be solved. Although some prime conjectures have been proven true, prime conjectures usually turn out to be false due to the fact that most prime conjectures are based on smaller primes, which have a higher frequency than larger prime numbers. Since there is not a known pattern of the prime numbers, most mathematicians do not test their conjectures on large prime numbers due to technological constraints and time.



Figure 1: Pierre de Fermat [5]

Unfortunately, prime conjectures based solely on small prime numbers almost always fail for large prime numbers.

2 Fermat's Conjecture

French mathematician Pierre de Fermat (1601 – 1665) began his career as a French lawyer and pursued mathematics for enjoyment. Fermat had a habit of scribbling notes in the margins of books and in letters to friends. He is well known for his conjecture that the equation $x^n + y^n = z^n$ has no solutions in the integers with $xyz \neq 0$ and $n > 2$. Although Fermat came up with the conjecture, he did not prove it. He simply wrote the conjecture in the margin of a book and said there was not enough space to prove it, [5]. Today, it is known as Fermat's Last Theorem. This theorem was proven by Andrew Wiles in 1995; almost three hundred years after it had been conjectured. Even though mathematics was not Fermat's first career choice, he is considered one of the greatest mathematicians of all times, [5].

2.1 Fermat's Conjecture

In 1650, Fermat made a conjecture based on the first five terms of the sequence $F_n = 2^{2^n} + 1$. His conjecture stated that numbers of the form $F_n = 2^{2^n} + 1$ for nonnegative integers n are prime, [1]. Numbers of this form would later become known as *Fermat numbers*. Below is a table of the first five terms which Fermat found to be prime:

n	0	1	2	3	4
F_n	3	5	17	257	65537

2.2 Fermat's Faux Pas

Although, the first five terms of the sequence are prime, not all of the numbers in the sequence are prime. In 1732, over 80 years later, Euler disproved Fermat's conjecture using the fact that any prime factor of $2^{2^n} + 1$ is of the form $k \cdot 2^{n+1} + 1$, where k is a natural number, which he had already proven true. Eduoard Lucas later showed that k must be even, changing the previous equation, $k \cdot 2^{n+1} + 1$ to $k \cdot 2^{n+2} + 1$, where k is a natural number, [1].

2.3 Disproof of Fermat's Conjecture

Let $n = 5$. Using the fact that any prime factor of $2^{2^n} + 1$ is of the form $k \cdot 2^{n+2} + 1$, we know that the prime factors of F_5 are of the form $128k + 1$, where k is a natural number. Observe that the first two prime numbers of the form $128k + 1$ are 257 and 641. Two observations that Euler made were that $16 = 641 - 5^4$ and that $641 - 1 = 5 \cdot 2^7$. Using these two observations, Euler proved that 641 divides F_5 in the following way:

$$\begin{aligned}
F_5 &= 2^{2^5} + 1 \\
&= 2^{32} + 1 \\
&= (16)2^{28} + 1 \\
&= (641 - 5^4)2^{28} + 1 \\
&= (641)2^{28} - (5 \cdot 2^7)^4 + 1 \\
&= (641)2^{28} - (641 - 1)^4 + 1 \\
&= (641)2^{28} - 641^4 + 4(641)^3 - 6(641)^2 + 4(641) - 1 + 1 \\
&= 641[2^{28} - (641)^3 + 4(641)^2 - 6(641) + 4] - 1 + 1 \\
&= 641 \cdot 6,700,417
\end{aligned}$$

Thus, 641 divides F_5 , so F_5 is composite and the conjecture fails.

3 Mersenne's Conjecture

Marin Mersenne (1588 – 1648) was a French monk who was also a philosopher, mathematician, and scientist. Even though his father wanted him to have a career in the Church, Mersenne traveled to Paris to continue studying. While in Paris, Mersenne stayed with the Order of the Minims, who were devoted to prayer and study, and later became a member. Mersenne is best known for his discovery of the cycloid, which is a geometric curve.



Figure 2: Marin Mersenne [6]

Throughout his career, Mersenne was linked to several important scholars, such as Fermat, Descartes, Galileo, and several others. Mersenne's main goal was to make advancements in science, so he encouraged scholars to work together to achieve this goal, [6].

3.1 Mersenne's Conjecture

Mersenne studied numbers of the form $M_n = 2^n - 1$, where n is an integer. Although he was not the first to study these numbers, he is credited with them and today they are known as *Mersenne numbers*. Mersenne later based a conjecture on these numbers stating that the numbers $2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$, and 257 and are composite for all other positive integers $n < 257$, [1].

3.2 Mersenne's Faux Pas

Mersenne's peers knew Mersenne could not possibly have tested all of these numbers because they could not. The technology was not available to test such large numbers, and Mersenne later admitted to not testing all of these numbers. It took three centuries before all of the exponents in Mersenne's conjecture were completely checked, which yielded a total of five errors, [3]. It is still unknown how Mersenne came up with his list of numbers, but many mathematicians have speculating theories.

As stated before, other mathematicians had studied the Mersenne numbers. Since 2, 3, 5, 7, 13, 17, and 19 are smaller primes, calculations had been completed to prove that the number produced was in fact prime. Years later, in 1750, Euler found that $2^{31} - 1$ was prime. In 1876, Edouard Lucas found that $2^{127} - 1$ was prime. In 1883, Ivan Mikheevich Pervouchine found $2^{61} - 1$ to be prime, adding 61 to Mersenne's list of exponents, and proving the list incomplete. In the early 1900's, R. E. Powers found that $2^{89} - 1$ and $2^{107} - 1$ were prime, adding 89 and 107 to Mersenne's list of exponents, and proving the

list still incomplete. In 1903, F. N. Cole proved $2^{67} - 1$ to be composite, removing 67 from the list, [1]. It would later be found that $2^{257} - 1$ was also composite, removing 257 from the list. The new list of exponents now reads $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$, and 127. These numbers were found with an upper-bound of 257. Other Mersenne primes have been found that satisfy $n > 257$.

3.3 New Mersenne Conjecture

Mathematicians Paul T. Bateman, J. L. Selfridge, and Samuel S. Wagstaff later revised Mersenne's conjecture to say: Let p be any odd natural number. If two of the following conditions hold, then so does the third:

1. $p = 2^k + or - 1$ or $p = 4^k + or - 3$
2. M_p is prime
3. $\frac{2^p+1}{3}$ is prime.

This conjecture has been verified for all primes less than 100,000 via computers, [1].

4 Unsolved Conjectures

As stated before, many prime conjectures have yet to be proven. Many of them have been verified to a certain bound, but not completely proven for all prime numbers. Below, we will discuss a couple of these conjectures.

4.1 Unproven Prime Conjectures

Christian Goldbach (1690 – 1764) was raised in Königsberg, Prussia and later attended a university there. While there, Goldbach studied some mathematics, but studied mostly law and medicine. He later traveled around Europe, where he began correspondences with scientists and mathematicians. After moving to Moscow, Goldbach began correspondence with Euler, which yielded advancing work in number theory, [7]. In a letter to Euler, on June 7, 1742, he claimed that he believed numbers might be represented as the sum of primes, or even that every number is the sum of three primes. Today, we consider this to mean that any even number is the sum of two primes, excluding 2. This conjecture has never been proven. In 1998, Goldbach's conjecture had been verified up to $4 \cdot 10^4$ by Joerg Richstein, [1].

Georg Friedrich Bernhard Riemann (1826 – 1866) began courses at the University of Göttingen in the spring of 1846. At first, he studied theology after much encouragement from his father. But after attending mathematics lectures and receiving permission from his father, Riemann began taking mathematics courses. He later began study at Berlin University in 1947, and it was there that he began working on the general theory of complex

variables, which would later provide vital to many of his important works. He returned to Göttingen in 1849 to pursue his Ph.D., and later became a lecturer at the University of Göttingen, [8]. In 1859, Riemann wrote a paper titled “On the Number of Prime Numbers Less Than a Given Quantity.” Riemann discussed the function: $\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots$, which is known today as the Riemann zeta function. Riemann conjectured that this function has an infinite number of zeroes with real part between 0 and 1, and gave a formula for the number of zeros of the function. His conjecture is considered to be the most important unsolved problem in mathematics, [1].

Hilbert included the problem of proving the Riemann hypothesis in his list of the most important unsolved problems which confronted mathematics in 1900, and the attempt to solve this problem has occupied the best efforts of many of the best mathematicians of the twentieth century. It is now unquestionably the most celebrated problem in mathematics and it continues to attract the attention of the best mathematicians, not only because it has gone unsolved for so long but also because it appears tantalizingly vulnerable and because its solution would probably bring to light new techniques of far reaching importance.

H.M. Edwards - Riemann’s Zeta Function, [10]

4.2 Conjectures Proven within a Limit

Like the New Mersenne Prime conjecture, some prime conjectures have been proven up through a certain number, but still have yet to be verified for all prime numbers. These conjectures cannot be considered true until they have been proven for all primes.

Romanian mathematician Dorin Andrica (1956–) is currently a professor at “Babes-Bolyai” University in Romania. Andrica proposed that $\sqrt{p_{n+1}} - \sqrt{p_n}$ is less than 1 for all n . Andrica’s conjecture was more about the gaps between prime numbers than the prime numbers themselves, with the largest value of the difference for $n < 1000$ being $\sqrt{11} - \sqrt{7} = 0.670873\dots$. Imran Ghory has verified this conjecture up to $1.3002 \cdot 10^{16}$, but it still has yet to be completely proven true, [1].

Belgian mathematician Eugéne Charles Catalan conjectured that 8 and 9 are the only pair of consecutive prime numbers; thus, saying for prime numbers p and q and positive integers x and y , the equation $x^p - y^q = 1$ has one solution, $3^2 - 2^3 = 1$, [9]. Catalan’s and Fermat’s conjectures are special cases of the Fermat-Catalan conjecture which states that there are finitely many solutions to the equation $x^p + y^q = z^r$, where x , y , and z are positive, coprime integers, and p , q , and r are all primes satisfying $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$. There are only 10 known solutions, but it has never been proven that there are *finitely* many solutions, [1]. The following are the 10 known solutions:

$$1^p + 2^3 = 3^2 \text{ for } p > 6$$

$$\begin{aligned}
2^5 + 7^2 &= 3^4 \\
7^3 + 13^2 &= 2^9 \\
2^7 + 17^3 &= 71^2 \\
3^5 + 11^4 &= 122^2 \\
17^7 + 76271^3 &= 21063928^2 \\
1414^3 + 2213459^2 &= 65^7 \\
9262^3 + 15312283^2 &= 113^7 \\
43^8 + 96222^3 &= 30042907^2 \\
33^8 + 1549034^2 &= 15613^3
\end{aligned}$$

5 Conclusion

In conclusion, prime conjectures are usually false due to the fact that mathematicians very rarely verify their prime conjectures for large prime numbers. Although there have been prime conjectures proven true and false, it sometimes takes hundreds of years to do so. And even though some of the conjectures made about prime numbers have been confirmed up through a certain number, this does not indicate that they will be true for all primes. Due to technological advances in the past few centuries, there are less false conjectures made since mathematicians can verify their conjectures more quickly and precisely. But there are still many conjectures, such as Andrica's conjecture, that mathematicians are still working to find solutions.

References

- [1] Wells, David. *Prime Numbers: The Most Mysterious Figures in Math*. John Wiley & Sons, Inc. 2005.
- [2] Ore, Oystein. *Invitation to Number Theory*. The Mathematical Association of America. 1967.
- [3] Caldwell, Chris. "The Prime Glossary: Mersenne's conjecture." <http://primes.utm.edu/glossary/page.php?sort=MersennesConjecture>. 1999-2008. 11 March 2008.
- [4] Weisstein, Eric W. "Mersenne Number." From *MathWorld*-A Wolfram Web Resource. <http://mathworld.wolfram.com/MersenneNumber.html>. 1999-2008. 11 March 2008.
- [5] Weisstein, Eric W. "Fermat, Pierre de (1601 – 1665)." From *Eric Weisstein's World of Scientific Biography*. <http://scienceworld.wolfram.com/biography/Fermat.html>. 1996-2007. 11 March 2008.

- [6] O'Connor, J. J., and Robertson, E. F.. "Marin Mersenne." University of St. Andrews, Scotland, School of Mathematics and Statistics. <http://www-groups.dcs.st-and.ac.uk/history/Biographies/Mersenne.html>. August 2005. 11 March 2008.
- [7] O'Connor, J. J., and Robertson, E. F.. "Christian Goldbach." University of St. Andrews, Scotland, School of Mathematics and Statistics. <http://www-history.mcs.st-andrews.ac.uk/Biographies/Goldbach.html>. August 2006. 5 May 2008.
- [8] O'Connor, J. J., and Robertson, E. F.. "Georg Friedrich Bernhard Riemann." University of St. Andrews, Scotland, School of Mathematics and Statistics. <http://www-history.mcs.st-andrews.ac.uk/Biographies/Riemann.html>. September 1998. 5 May 2008.
- [9] Caldwell, Chris. "The Prime Glossary: Catalan's Problem." <http://primes.utm.edu/glossary/page.php?sort=catalansproblem>. 1999-2008. 5 May 2008.
- [10] Watkins, Matthew R.. "The Riemann Hypothesis." <http://www.secamlocal.ex.ac.uk/people/staff/mrwatkin/zeta/riemannhyp.htm>. 5 May 2008.