

Mathematical Quest 4: More about Primes

by Gonit Sora - Saturday, September 07, 2013

<https://gonitsora.com/math-quest-more-about-primes/>

The following was published in Young NE, Vol. 1, Issue 5 (September 2013). We thank the editor of Young NE for permission to post this here.

In the [last issue of this column](#) I discussed about prime numbers and why they were so useful for us. In this issue I shall focus again on primes and say how different they can be even if they belong to the same class of numbers.

It is a widely recognized truth that the primes are seemingly random and patternless. Mathematicians have been trying very hard for more than two millenia to find a pattern that shall describe primes. But so far they haven't been able to find such a pattern.

There have been many wrong claims about prime numbers and there have been claims which till now no one has been able to verify or refute. Such is the saga of primes that every mathematician in whatsoever field he or she may work, is always fascinated by prime numbers. The story that began with Euclid is far from being over and every passing month or year we get to know something new about the prime numbers.

A very famous name in number theory and in whole of mathematics is Pierre de Fermat, who was a lawyer by profession and did mathematics as an amateur. Fermat's name is associated with a very famous problem in mathematics called Fermat's Last Theorem which states that the equation $x^n + y^n = z^n$ cannot be solved for non-negative numbers x , y and z if n is greater than two. This assertion made by Fermat in the margin of a book he was reading took almost 358 years to prove. The proof of this result was given by Prof. Andrew Wiles of Princeton University in 1994 using very sophisticated techniques and the proof runs for more than 100 pages and infact even now only a select few mathematicians understand the whole proof. Fermat believed that the numbers of the form $F_n = 2^{2^n} + 1$ were all primes, where a^b means a^b and n is a natural number. Fermat checked the first four cases and found that they were all primes, and so he conjectured that maybe all such numbers were primes. Thus primes of the form F_p are called Fermat primes in his honour.

It was almost a 100 years later that the famous Swiss mathematician Leonhard Euler refuted Fermat's claim by showing that the number 641 divides F_5 . It is believed but yet not proved that there are infinitely many Fermat primes. Infact we cannot even prove that there are infinitely many Fermat numbers which are composites.

This is just a simple case of a class of primes that share the same property. There are many other such classes like Mersenne primes, $M_n = 2^n - 1$ which are primes. These Mersenne primes have given rise to an Internet project called GIMPS (Great Internet Mersenne Primes Search), where users from all across the globe use their computers in parallel to find Mersenne primes. The largest known prime numbers are

normally Mersenne primes. The largest known prime at present is $\dots 2^{57,885,161} - 1$, a number with 17,425,170 digits. This is a Mersenne prime. It is worth mentioning that Mersenne was a Catholic priest, whose hobby was mathematics.

Now we turn our discussion to pairs of prime numbers that satisfy some property. The most famous such pairs are what we call twin primes. Say we have a pair of consecutive primes (p, q) where $p - q = 2$. Then such pairs of primes are called twin primes. Examples are $(3, 5)$, $(5, 7)$, $(17, 19)$ and so on. It is believed by mathematicians that there are infinitely many such pairs of primes, but no one has been able to prove it yet. The closest result about such pairs of primes that we know now is due to Yitang Zhang, a virtually unknown mathematician who in April of this year proved that there exists infinitely many consecutive primes (p, q) such that $p - q = N$, where N is a very large number, but not exceeding 70 million. This result may seem like a trifle compared to what we need to know, where N should be 2, but mathematicians are working on decreasing the estimate of N in Zhang's result. It is believed that they might bring it down to 16 from 70 million. Infact at the time of writing this article (June, 2013) the bound for N has been decreased upto almost 12,000. Its amazing how mathematics is created and at what speed.

I would like to close this column with a brief discussion about a very famous unsolved problem in mathematics, called the Goldbach Conjecture. This conjecture states that any even number greater than 2 can be written as the sum of two primes. For example $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 7 + 3$, and so on. Mathematicians have been trying to prove this assertion for many centuries now with utter failure. They have yet to find a counter-example to this statement and via computers they have checked for millions of numbers to see if there are any even numbers which do not satisfy this property, but they have not yet found one such number. It is generally believed that the Goldbach Conjecture is true, and in case you solve it then it will not only make you immortal but also will fetch you a lot of money, as important problems like this have a lot of cash reward for a proof or disproof.

What is known is a weaker version of Goldbach Conjecture which says that every odd integer greater than 7 can be written as the sum of at most three primes. This result was proved conditionally by the famous Russian mathematician I. M. Vinogradov using techniques developed by G. H. Hardy and Srinivasa Ramanujan. Recently, in May 2013 a mathematician named Helfgott has given an unconditional proof of this assertion thus settling it completely. He also uses techniques of Hardy and Ramanujan called the Circle Method.

Thus, we see that even innocent sounding questions about primes can be very hard to crack. Mathematicians and lovers of mathematics are attracted to these questions like a bee to a flower, and only the true follower will understand the pleasure one gets when one solves a very hard problem.