John Mendribil
Math 301

A Discussion on Legendre's Conjecture

Abstract

Given that the nature of primes number—a subset of the integers that hold the property that they are only divisible by 1 and themselves. There exists no method for obtaining specific prime numbers nor is there one for determining the gap that exists in between consecutive prime numbers. This paper will discuss the properties of prime numbers and specifically Legendre's conjecture (LC). LC states that given two consecutive integers, in between the squares of those two integers exists a prime number. This paper will discuss other conjectures that are also unproven and how mathematicians have attempted to prove LC as a consequence of those proof attempts and how LC can be proven as a consequence of other conjectures. Topics discussed are Landau's Problems, Bertrand's conjecture and the prime number theorem. Also briefly discussed are methods, the toolset given to introductory proof students, that are not capable of solving LC.

Prime numbers are a very important and widely studied subset of the integers. However, they do not lend themselves to simple methods of finding consecutive or specific primes. Since prime numbers are defined to be numbers that are only divisible by themselves and the number one, finding one requires division by all primes less than or equal to the square root of any particular prime number. Larger and larger primes require more and more divisions and unlike finding numbers in a sequence, primes cannot just be found via a formula. Some of the greatest minds in the history of math have tried and failed to establish a direct algorithm for the gap between consecutive primes. People such as Gauss, Legendre and others have tried to tackle the problem but it was Legendre that conjectured that in between any two squared integers, there exists at least one prime number. His conjecture is one that has a not been proven at the time this paper was written—along with many other conjectures for which Legendre's is a just one of many conjectures involving the gaps between primes.

The set of integers are a discreet set of numbers that range from infinitely negative to infinitely positive. Zero, of course is included in that set. There are the even numbers which are divisible by 2, or in other words the set of even numbers is defined as :={x; 2|x}. Since an integer this either even or odd, we define the odd integers as :={x: x=2n-1, ∀n∈ℤ}. In English, the even numbers are those that, when divided by 2, it yields a remainder of 1. The odd numbers are those of the form 2n+1 for any integer n. Both odd numbers and even number have a definition that allows us to find not only as many of each as we wish, but also allows anyone to find the first or the fifth or the millionth odd or even number. There are even ways to find if an integer is divisible by 3. Just add the digits of an integer and if that number is itself divisible by three than the original number is divisible by three. If an integer is divisible by 5, it will either end with a 5 or a 0. Those are just a few of the many shortcuts that exist for finding integers that are divisible by another number. However, there is a special set of numbers contained within the integers for which there is not shortcut for finding itCons common divisors. That set of numbers is called the primes numbers for which we will denote as *p*. By inspection, it is easy to see that the first few prime numbers are 2,3,5,7,11,13,17,19,23,29. Each of those numbers is not the product of any smaller integers. Upon closer examination, one can see that the gap in between those numbers is 1,2,2,4,2,4,2,4,6,. That is not a sequence for which there exists an algorithm for finding the number of integers in between any two prime numbers. Instead, mathematicians have sought ways to estimate how many prime numbers exist within a given range of numbers, but first we'll refresh our memory on primes which will take us back to the days of our youth.

Recalling from elementary school, most people remember learning prime factorization. For me, it meant finding the smallest numbers that when multiplied together, their product was the original number I started with. I never thought about why the technique was called prime factorization. Take for example the number 21. There are two numbers that when multiplied together will have a product of 21. Those numbers are 3 and 7. Twenty-one just happens to be the greatest common divisor of 3 and 7. The same idea holds true for fractions, or as they are called in mathematics, the rational numbers. When an integer is not the product of any other integers except 1 and itself, we called those numbers prime. But are there always going to be prime numbers larger than the previous? Paulo Ribenboim, in his book, *The New Book of Prime Number Records,* offers a proof by Euclid, that there are indeed infinitely many prime numbers. After all, if there were not infinitely many prime numbers then Legendre's Conjecture would have an upper limit and all one would need to do to find all other primes would be to divide the largest *p* by all integers n<*p*. Ribenbiom, referencing Euclid, states, that if $p = p_n \times p_{n+1} \times p_{n+2} + 1$, then p is divisible by p_n and has a remainder of 1. That contradicts the assumption there are a finite number of primes (Ribenboim 3).

Once it was shown that there are infinitely many prime numbers, focus turned to the frequency of primes as the integers become infinitely large. Clearly, the distribution of primes numbers is more frequent for all values less than 100, and so mathematicians set out to understand those that have many more digits. Afterall, my assumption in the previous sentence could be wrong. Janos Pintz, in his article, *Landau's Problem on Primes*, states, "[that] four specific problems about primes [are] unattackable at the present state of science." He was referring to the discussion in 1912, at the Internation Congress of Mathematicians. Landau stated that there were four problems that had to be resolved when concerning primes. The first question was whether or not $n^2 + 1$ represented infinitely many prime numbers for all integers n. Second was whether or not $m = p_n + p_{n+1}$ had any solutions for m>2 that were even. The third question was whether there are there infinitely many primes *p* such that *p* − 1 is a perfect square. However it was the fourth question asked that questioned whether or not there existed a prime number between n^2 and $(n+1)^2$ (Pintz 1). Landau's problem included Legendre's Conjecture. But was

Lengedre's Conjecture a consequence of the previous three questions or was it a problem that could be solved independent? Just as Euclid's Parallel Postulate baffled geometers for centuries as to whether or not it was independent of the previous four axioms, Lengendre's Conjecture might be a consequence of other conjectures.

While a direct proof of Legendre's Conjecture has proven as difficult to prove as other similar conjectures, a young Carl Gauss, one of the most prolific mathematicians ever, proposed an amazing idea. According to Marcus du Sautoy, in his book <u>The Music of the Primes</u>, he says, "Gauss came up with a nice approximation," as to whether or not a given integer is a prime. Gauss proposed that given an integer N, the probability of that number being a prime number was proportional to the inverse of the log of that number ($1/\log(N)$) and therefore should be approximated by the function $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}$ which is stated by Riemann and is equivalent to the approximation of the number of primes less than or equal to x, which is denoted by $\pi(x)$ (Sautoy 6). This function has come to be known as the prime number theorem which is an approximation of the number of primes *p* less than x. However, both $\pi(x)$ and $\mathrm{Li}(x)$ were both approximations. Numerous mathematicians tackled a proof of the prime number theorem and eventually it was proven and is beyond the scope of this paper, but it's proof set the stage for mathematicians to tackle other problems, Legendre's Conjecture being one of them.

At present time, many mathematicians believe that Legendre's Conjecture (LC) can be proven if, using the prime counting function $\pi(x)$, Bertrand's postulate implies the LC. Bertrand's postulate states that there is always a prime number in between n and 2n. That is, $\pi(2n) - \pi(2n) \geq 1$, which is a generalization of the prime number theorem and is proposed in Tsutomu Hashimoto's paper *On a certain relation between Legendre's conjecture and Bertrands postulate* (1). Hashimoto generalizes the Legendre conjecture by stating if there exists a prime number in between n^2 and $(n+1)^2$, then $\pi((n+1)^2) - \pi(n^2) \geq 1$. Shiva Kintali, in his paper, *Towards Proving Legendre's Conjecture*, states that the proof of Bertrand's postulate "was given in 1850 by Chebychev," (2). An young Indian, auto-didactic mathematician Ramanujan, using the gamma fuction presented a simpler proof whose consequence was the introduction of the Rumanujan Primes. Just as Euler used primes to generalize Fermat's Little Theorem, mathematician Erdos further simplified Bertrand's postulate.

A consequence of Bertrand's postulate is that any positive integer can be written as a sum of primes and 1, where each prime is used only once (Hashimoto 4). Using properties of group theory, Hashimoto went on to show a relation between Bertrand's postulate and the Legendre conjecture, where once again the relationship is beyond the scope of this paper. What Hashimoto's paper does point out is that with increasing frequency, mathematicians are proving the existence of primes within a defined range of numbers.

Since there is an apparent relation between Bertrand's postulate and LC, another generalization offered by Kintali, is the generalization that given an integer n>1 and a fixed integer k≤n, does there exist and prime number such that kn<p<(k+1)n (2)? An affirmative answer has been proven for k=2. Bertrand-Chebyshev theorem answered the question for k=1, but Kintali states, "[a] positive answer to k=n would prove Legendre's conjecture," (2).

Although there has been no proof of LC by virtue of being a consequence of another theorem, one is left wondering why LC cannot be proven using basic techniques offered in an introductory proof class at any university. By inspection, anyone using basic algebra can clearly see that there is indeed a prime in between small integers and their square. Since there is no algorithm that explicitly offers one the location of any specific prime number, a proof by induction is not a valid argument. Induction to find, for example an even numbers requires a definition of the even numbers. Since even numbers are defined as being divisible by 2, then given for any n, 2|2n. The induction proofs then argue that knowing 2|2n, 2 also divides 2(n+1), however prime numbers are not a defined sequence and therefore a proof by induction is not applicable. We also know that for any integer n, n^2 is not a prime because n·n is divisible by n and therefore it is not prime. The same argument can be made for any n+1 as well. However, since there infinitely many integers and infinitely many primes, division by all number smaller than a discovered prime is not a realistic process.

So the question of whether or not the gap in between primes can be determined definitively appears to walk hand in hand with whether or not it is possible to find specific primes p_n for any $n \in \mathbb{N}$. As we've shown, some of the greatest mathematical minds have attempted to answer these mysteries and still no explicit proof for LC or the three other Landau Problems has been found. In the end it might turn out that chasing such proofs might prove a task on par with finding the smallest real number for which there is no smallest real number. Then again, given enough time, corollaries to LC might shed light on the dark mystery of prime numbers—both finding p_n for any $n \in \mathbb{N}$, which would allow mathematicians to determine the gaps in between consecutive primes, and vice versa. Black holes cannont be seen by the strongest of telescopes because they don't emit any light, but scientists know they exist by observing the behavior of the bodies within their sphere of influence. Prime numbers stand alone and therefore it might turn out that the only way to shed light on them will turn out to be a practice in having to understand them by understanding their neighbors.

Bibliography

Janos, Pintz. "Landau's Problems on Primes." *Journal De Théorie Des Nombres De Bordeaux* (2009): 1-43. *Http://www.renyi.hu/~pintz/pjapr.pdf*. 2009. Web.

Petersen, Bent E. "Prime Number Theorem." *Seminar Lecture Notes* (1996): 2-42. Print.

Du, Sautoy Marcus. *The Music of the Primes*. New York: HarperCollinsPublishers, 2003. Print.

Ribenboim, Paulo. *The New Book of Prime Number Records*. New York: Springer, 1996. Print.

Kintali, Shiva. "Towards Proving Legendre's Conjecture." 11 Jan. 2009. Web. 2 Mar. 2011. <http://arxiv.org/PS_cache/arxiv/pdf/0811/0811.4451v2.pdf>.

Hashimoto, Tsutomo. "On a Certain Relation Between Legendre's Conjecture and Bertrand's Postulate." July 2008. Web. 10 Apr. 2011. <http://arxiv.org/ftp/arxiv/papers/0807/0807.3690.pdf>.