

## Mathematical Quest 3: Prime Numbers

by Gonit Sora - Tuesday, July 09, 2013

<https://gonitsora.com/mathematical-quest-3-prime-numbers/>

*The editor of the English section of Gonit Sora, writes a monthly column devoted to mathematics in a teen magazine called Young NE. The editor of Young NE was kind enough to grant us permission to republish the column after it appears on print. Below is the column that appeared in Vol 1, Issue 3, July 2013 of Young NE.*

In this column, I shall talk about a very very special class of numbers called *prime numbers*. You probably know these classes of numbers, but didn't think them to be very useful. My goal in this column is to give you some flavours of what these numbers have in store and why are they important?

First let us define these prime numbers. *Numbers which have only two positive factors are called prime numbers*. For example, 2, 3, 5, 7 and 11 are the first five prime number. 9 is not a prime number because it has three positive factors, not two. Prime numbers have been a source of wonder, mystique and much deliberation for more than three to four millenium now. It all started when **Euclid**, the famous Greek mathematician wrote down his classic textbooks called '**The Elements**'. Therein Euclid stated and proved a theorem which we now know as the fundamental theorem of arithmetic. What does this theorem say? It says that given any positive natural number, we can always break it down into product of prime numbers or powers of prime numbers in a unique way. For example if we consider the number 100, then we have  $100=2 \times 2 \times 5 \times 5$  and this representation is unique. This happens for any positive natural number.

In light of the above discussion we see that these prime numbers are the building blocks of all our numbers that we normally use. Thus their importance can neither be denied nor overlooked. But this is not the sole reason why prime numbers are important. They have a vast use in our day to day life also.

Have you seen someone use an ATM? Or perhaps you yourself have used one? Or maybe you bought the latest Dan Brown book on flipkart.com? Or perhaps some of you might have recharged your mobile phone online? Whatever be the case, you had to write in your Debit/Credit card number and then voila your bill was paid and you needn't worry about anyone stealing your information. But have you wondered how this information goes from the website to the merchant and then that merchant determines what amount to deduct and return you the message? All this happens in a fraction of a second, and that is because of the beauty of mathematics. In this whole scenario of online transactions or ATM withdrwals, prime numbers play a major role. What happens is that there will be two very very large prime numbers, and then they will be multiplied together to get a huge number say X. Now X will be given by the merchant to the bank and then the bank will send in another large number, say Y to the merchant. If one party knows one of the prime numbers originally used then the number Y so generated can give you X

that the merchant or the bank sends. This is infact a very famous system called the RSA cryptosystem and this system is used almost in every online transactions and is considered one of the safest ways to send in such information so that only the person for whom the information is meant to will be able to extract it, while the rest of the people won't be able to learn anything.

Now that we have seen the importance of primes, then do we know how many prime numbers are there exactly? In fact, we do. The answer is infinite, that is the primes are a never ending sequence of numbers. This was again proved by Euclid in his Elements. It is also known that the primes become rarer and rarer as we go on. For instance between 1 and 100 there are 25 primes, that is 25% of the numbers are primes. Between 1 and 1000 there are about 16.8% primes and so on. We see that the density of primes goes on decreasing as we increase our interval of obeservation. This fact, combined with a lot of ingenuity led to what is called the prime number theorem, a very important theorem in modern mathematics. Unfortunately, we need to understand a lot of math before we can state this result, so I shall skip it.

Now that we know there are infinitely many primes, then is there any way in which we can determine whether a given number is prime or not? For small number it is a relatively easy task and there are many ways in which we can do it. But for larger numbers this becomes a major issue and requires lots of computation. For a long time, no such method existed to check whether a number was prime or not in a finite amount of time. But in 2001 there came a landmark paper by three Indian computer scientists where they showed that an algorithm existed which allowed a computer to determine whether a given number is prime or not in a time that is efficient. These three men were Prof. Manindra Agarwal, Neeraj Kayal and Nitin Saxena from IIT Kanpur. Kayal and Saxena were then final year engineering students when they found this remarkable result.

It is also worth noting that Neeraj Kayal was born and brought up in Guwahati. Kayal did his schooling from Don Bosco, Guwahati and then Cotton College before going to IIT Kanpur where he also did his PhD, then he went to Princeton University, Rutgers University and many other places of repute before finally settling as a researcher in Microsoft Research, Bangalore.

These were just a glimpse of what prime numbers are, there are many more such prime facts and oddities to share which I leave it for some other time. You can call/SMS me at +91-80119-02141 or email me at [manjil@gonitsora.com](mailto:manjil@gonitsora.com) with your comments, queries, corrections, criticisms, etc.