Prime Numbers: From Euclid to AKS

by Manjil Saikia - Tuesday, June 30, 2015

http://gonitsora.com/prime-numbers-from-euclid-to-aks/

> **Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the mind will never penetrate.** - Leonhard Euler

Prime Numbers Image by Shutterstock

Prime numbers have taken the fancy and imagination of almost every mathematician in the world at some point or the other in his or her lifetime. We first encounter these numbers when we are in school and they are defined as the numbers which are indivisible into smaller factors. But why are these numbers important and why do mathematicians love them so much?

The first result on prime numbers that is available to us is from Euclid. In his *Elements*, he states and proves what is perhaps the most beautiful proof of any mathematical result that I have seen. Euclid proves that there are infinitely many primes. That is, the sequence of prime numbers $$2, 3, 5, 7, 11, 13, 17, 19, ldots$$ never ends. This result has inspired for many generations mathematicians to study these class of numbers. The next natural question to ask is how many primes are there upto a given number? For example there are $$25$$ primes upto $$100$$ and $$125$$ primes upto $$1000$$. As we go higher and higher along the number line, we shall notice that the primes goes on decreasing in numbers relatively. This observation is the basis for one of the most fundamental and widely known result in all of mathematics, called *The Prime Number Theorem*. This result also ties up very closely with one of mathematics' other famous result called *The Riemann Hypothesis* which is still unpoved.

Another important facet of prime numbers in our normal number system is that, they are the fundamental building block of all integers. Much like atoms which make up all matter, prime numbers make up all of the integers. Each positive integer can be expressed as the product of some powers of primes in a unique way. Hence, it is not a very bad idea to study the prime numbers. A natural question might arise at this point: Whether the prime numbers have any pattern? The simple answer is 'no'. The primes have no pattern that has been discovered so far, but they do satisfy many interesting properties which have baffled centuries of mathematicians. For example, a famous conjecture is mathematics says that every even number greater than $$2$$ can be written as the sum of two primes. This is called the *Goldbach Conjecture* and recently much work has been done in this direction. But that is a different story, one which we shall not discuss here and is left for a future post.

This now brings us to the most important application of prime numbers: cryptography. We have become so used to computers and the internet that not many of us know how much non-trivial mathematics hides behind simple stuff that we take for granted. Almost everyone of us have used our Debit or Credit cards

to make a purchase online. How do you know that such a transaction is safe? The reason behind this is something called RSA cryptosystem, which is named after the people who invented it: Rivest, Shamir and Aldeman. The main idea is that the merchant has two very large prime numbers (say of $$300$$ digits each) and they multiply them together to get a composite number $$X$$ (a non-prime number) and then do some mathematical operations on $$X$$ with your card number and then send the details over the internet to the merchant so that they can figure out what your card details are. The process looks deceptively simple, but the main reason why this works is because given an arbitrary number it is generally very difficult to determine whether that number is prime or not, but it is close to impossible with present computational power to determine large prime factors of a number like our $$X$$ here.

With today's best computing skills, we still cannot factor a $$1000$$ digit number into its prime factors in a finite amount of time. This is why such crypotsystems work. But there has been some research into what is called *quantum computing* and in 1994, a mathematician named Shor proved that a quantum computer will do a much better job at factoring numbers than a classical computer. Such a computer is still largely theoretical and only very small such quantum computers have been built in labs. But there is a distinct possibility that such a computer may come into existence in our lifetime. If such a thing happens, then perhaps RSA will be rendered useless.

The final thing that I would like to mention here is about the problem of determining whether a given number is prime or not. This is normally a very difficult thing to do. This problem has been around for centuries and many great mathematicians like Gauss, Fermat, etc have worked on this. Before 2003, the methods that were used to find whether a number was prime or not either were very slow and cumbersome or were randomised in the sense that it gave an answer with some amount of chance or probability associated with it. But all this changed when in 2003, three Indian computer scientists solved this long standing problem of finding a test to determine whether a number was prime or not in polynomial running time. The test called AKS test after the inventors: Manindra Agarwal, Neeraj Kayal and Nitin Saxena is one of the most significant contributions by Indians to mathematics in the recent years. It must be mentioned that Kayal and Saxena were undergraduates at IIT Kanour and there undergraduate project work was on devising this test. Also, Kayal was born and brought up in Guwahati, Assam.

The AKS primality test is very simple to state and prove and it uses only mathematics at a very elementary level. The running time of the test has been since improved by a lot of mathematicians including Pomerace, Lenstra, etc. and is now almost twice as fast as when it was originally proposed. However, this is not the end of the story of prime numbers as there is much work to be done. These numbers have been the obsession of many mathematicians since time immemorial and have been wrapped in a certain mystery and charm of its own. In this short note, we have not discussed any details specifically, the idea was just to give a brief overview of the topic. We hope to address some of the things mentioned in this article in future posts.

[This article was solicited for an in house magazine of the School of Engineering, Tezpur University, India and is published here without any significant changes.]
