Investigating the Primes*

Kaneenika Sinha

The aim of this expository article is to introduce the reader to some of the fundamental milestones in the study of prime numbers across several centuries. Among the important developments in the study of prime numbers, we review the history of the prime number theorem, the Riemann zeta function (in relation to prime number theory), and some recent investigations into spacings between consecutive primes. We also present an important application of prime numbers in safe data transmission, namely the 'RSA public key cryptosystem'.

Kaneenika Sinha is a mathematician at IISER Pune. She works on problems that lie at the interface of analytic number theory and arithmetic geometry.

Introduction

In 300 BCE, Euclid of Alexandria wrote a series of 13 volumes under the title *Elements*. These volumes contain a systematic presentation of several mathematical concepts through precise definitions, theorems, and their deductive proofs. They form the structural foundation of logic and mathematics as we study it today; in fact, much of what we learn in high school mathematics today goes back to the contents of these volumes. The topic of this article is a fundamental notion in *Book 7* of *Elements*, which has fascinated humanity for the last 2300 years, namely prime numbers.

Euclid defined a prime number as "that which is measured by the unit alone". In modern parlance, a prime number is a natural number $n > 1$ which is not divisible by any natural number other than 1 and itself. School textbooks typically make a passing reference to the notion of prime numbers, with some computational exercises on deriving prime factors of 'large' numbers (which, by

Keywords
Prime numbers, sieve methods, Riemann zeta function, cryptography.

*DOI: https://doi.org/10.1007/s12045-019-0784-6

real-world standards, are not that large!).

It is only in college that a mathematics student revisits prime numbers in some detail. We learn, for instance, the fundamental theorem of arithmetic which states that "every natural number other than 1 is either a prime or can be uniquely written as a product of primes". We also learn that there are infinitely many primes. Both these theorems go back to Euclid's *Elements*. At this stage, a student is naturally led to ask further questions about primes. How are primes distributed on the number line? Are they distributed in some sort of uniform pattern or not? Do they become sparse as one proceeds on the number line?

How do we recognize a prime when we see it? If we are given a large number, how long could it take to determine whether it is prime? If we need a large prime for some reason, how quickly can we generate it? If a number is not a prime, do we have nice (and efficient) methods to break a number down into its prime factors?

One can also ask some explicit questions. How do we recognize a prime when we see it? If we are given a large number, how long could it take to determine whether it is prime? If we need a large prime for some reason, how quickly can we generate it? If a number is not a prime, do we have nice (and efficient) methods to break a number down into its prime factors? Such questions and more about prime numbers have interested and inspired several seekers of knowledge over the last three millennia.

Answers to these questions are not immediate and in many cases, are known partially after several centuries of deep thought. Advancement in the study of prime numbers has less to do with answers and more to do with questions; questions that progressively reveal what prime numbers meant to seekers at every stage. The journey from Euclid's discovery that there are infinitely many primes to the sophisticated investigation of prime numbers in the twenty-first century has many important milestones, and we hope to describe some of them in this article. This article does not claim to contain a complete history of primes. Instead, we review some key developments and provide useful references with the hope that an interested student will explore the world of primes in greater detail.

Organization of the Article

In Section 1, we summarise some classical developments that enhance our perspective of prime numbers. This section culminates in a fundamental 1859 article of Riemann which provided a 'vision document' to answer questions about prime numbers with the help of what is called the *Riemann zeta function*. Section 2 takes forward the study of distribution of primes and describes questions about spacings between prime numbers. Many interesting developments in this aspect have taken place within the last 15 years, and we describe some of them. Finally, in Section 3, we shift gears and turn towards an important application of prime numbers – security in our online transactions. These applications, developed in the 20th century, use properties of primes that were discovered more than 200 years ago.

1. Prime Counting: From Arithmetic to Analysis

In this section, we describe four important milestones, which take us from Euclid's demonstration of the infinity of primes to a more refined study of primes using modern tools of mathematics. These also mark the conversion of arithmetic counting questions about prime numbers into the language of real and complex analysis. This is the language in which various problems about primes are currently studied.

Roughly speaking, the four developments that we touch upon in this section are as follows:

1. **The sieve of Eratosthenes**: This refers to an idea described by the Greek scholar Eratosthenes in the third century BCE to determine if a number is prime. This method is more efficient than the trivial method of checking divisibility by every number smaller than a given number. All the way until the 19th century, progressively larger records of prime numbers were built by several people using this sieve and its variants. This is described in Section 1.1.

2. **Gauss and the prime counting function**: A major shift in the

study of primes occurred when the German teenager Gauss, with a penchant for observing patterns in extensive data, made a conjecture in the 1790s about the asymptotic density of prime numbers. A big chunk of modern number theory was developed to understand and prove the conjecture of Gauss. This conjecture, also known as the prime number theorem, forms the content of Section 1.2.

3. **Chebyshev and the smooth analogue of prime number theorem**: In the early 1850s, Chebyshev defined some functions which 'smoothen' out the prime counting function and make way for the application of calculus to study what was heretofore seen as an arithmetic problem. Developments around this theme are described in Section 1.3.

4. **The zeta function of Riemann**: The introduction and study of zeta functions mark a very important development in the prime number theory. A breakthrough article written in 1859 by Riemann on this topic became the foundation for much of the number theory as we know it today. A brief overview of this function and relation to the prime number theorem is provided in Section 1.4.

1.1 *Sieves: The Earliest Tools to Capture Primes*

How does one determine if a number n is prime? The first method that comes to mind to determine primality is, of course, trial division. We simply attempt division by all the numbers between 2 and $n-1$, and if neither of them divides n, we declare it a prime. But, in this method, the number of steps needed is equal to the size of n. Some time in the third century BCE, the Greek scholar Eratosthenes had a clever idea. If n is not a prime number, then it must have a factor not bigger than the square root of n. Therefore, to test the primality of n, it would be sufficient to check the divisibility by all the primes less than or equal to the square root of n. Take, for example, $n = 101$. We just need to check if n is divisible by all the primes up to 10, that is, 2, 3, 5 and 7. This reduces the number of steps to check the primality of 101 from 99 to 4. What's more, among the numbers 2 to 100, if we cross

Some time in the third century BCE, the Greek scholar Eratosthenes had a clever idea. If n is not a prime number, then it must have a factor not bigger than the square root of n.

out all the multiples of 2, 3, 5 and 7, we will be left with a table of all the prime numbers up to 100. This method is famously called the 'sieve of Eratosthenes'. Early records of primes were created through a systematic use of this sieve. Mathematicians used physical tools like adjustable sliders and stencils to locate and eliminate multiples of primes by this method (see [1] for a detailed description of how early tables of primes were created).

The simple sieve method of Eratosthenes has now evolved into more sophisticated sieves developed in the 19th century and afterward. However, the fundamental insight of Eratosthenes remained a primary tool for tabulating primes for a long time until the advent of computers.

1.2 *Counting the Primes: Beyond Prime Tables*

Several centuries after the observation of Eratosthenes, the study of prime numbers received a new impetus. In the 1790s, a young German teenager by the name of Johann Carl Friedrich Gauss, who would later earn the title of the "prince of mathematics", wanted to understand the distribution of primes. He made some interesting guesses by looking carefully at existing records of prime numbers. He asked a fundamental question that brought a fresh perspective to the study of primes: Can we count the number of primes up to a number x? More precisely, can we approximate the function

$$\pi(x) = \#\{p \leq x,\ p \text{ prime}\}?$$

Based on existing data, Gauss conjectured that

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

That is, as x takes larger and larger values, the value of the prime counting function $\pi(x)$ comes closer to $\frac{x}{\log x}$, and the error margin between $\pi(x)$ and $x/\log x$ decreases. The journey of this conjecture to become a theorem (now famously known as the prime number theorem) was to take a 100 more years, and it gave birth to a beautiful amalgamation of analysis and number theory.

1.3 *Logging the Primes: Interface Between Analysis and Number Theory*

Questions in the theory of numbers often attract attention from amateurs as well as professional mathematicians. Many of these problems can be explained in simple language and look appealing for this reason. Unfortunately, the 'elementary' approach often does not go far, and it could take decades, or even centuries of concerted efforts before new light is shed on such problems. In some cases, this new light comes simply by reinterpreting the problem in a different language, which opens it up to the use of other tools.

We often study the prime counting function by attaching suitable weights at the primes. This approach allows us to bring in analytic tools to study primes.

In the case of the conjecture of Gauss on the prime counting function $\pi(x)$, this new interpretation came when the French mathematician Joseph Bertrand went through the table of primes up to 3×10^6 and conjectured in 1845 that for any natural number $n \geq 2$, one can find a prime number lying between n and $2n$. That is, $\pi(2n) - \pi(n) > 0$ for any $n \geq 2$. This conjecture was soon proved by the Russian mathematician Pafnuty Chebyshev in 1852. While studying the primes, Chebyshev modified the prime counting function by attaching logarithmic weights to the primes. That is, he replaced the function

$$\pi(x) = \sum_{p \leq x} 1,$$

by what is called the first Chebyshev function,

$$\vartheta(x) = \sum_{p \leq x} \log p.$$

Bertrand's conjecture is equivalent to saying that $\vartheta(2n) - \vartheta(n) > 0$ for all $n \geq 2$. This logarithmically weighted function yields itself to readily available tools in analysis. Therefore, it is natural to try and state the conjecture of Gauss in terms of this function. In fact, using an important tool from an analysis that was independently discovered by Leonhard Euler and Colin Maclaurin in the 1730s, one can approximate the sums $\sum_{p \leq x} \log p$ by integrals of appropriate functions. In terms of this new function, the conjecture of

Gauss is equivalent to the assertion that

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1.$$

Another related function is one in which we isolate, not just the primes, but all the prime *powers* less than or equal to x. The second Chebyshev function is defined as

$$\psi(x) = \sum_{p} \sum_{\substack{m\geq 1 \\ p^m \leq x}} \log p.$$

For large values of x, the functions $\vartheta(x)$ and $\psi(x)$ are very close to each other. Moreover, for reasons described in Section 1.4, $\psi(x)$ is better suited to study the prime numbers. In fact, the prime number theorem is also equivalent to the assertion that

$$\lim_{x\to\infty} \frac{\psi(x)}{x} = 1,$$

and it is in this new form that the prime counting function was henceforth studied.

1.4 *Prime Numbers and the Zeta Function of Euler and Riemann*

The fundamental theorem of arithmetic, which says that every natural number $n \geq 2$ can be uniquely written as a product of prime powers, can be restated in terms of infinite series. Let us consider the infinite series, also known as Euler's zeta function,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

which converges for a real number $s > 1$. By unique factorization of every n into a product of prime powers, we see that for $s > 1$,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots \frac{1}{p^{ms}} + \ldots\right) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

This analytic restatement of the fundamental theorem is due to Leonhard Euler and is called the 'Euler product formula'. It gives

an indication that the study of primes is linked to the behaviour of the series $\zeta(s)$, which in turn can be studied using standard tools of calculus, since it is an (absolutely) convergent series in the interval $(1, \infty)$.

In fact, since $\frac{1}{p^s} < 1$ for $s > 1$, using the Taylor series expansion:

$$-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n} \text{ for } |x| < 1,$$

we deduce,

$$\log \zeta(s) = -\sum_p \log\left(1 - \frac{1}{p^s}\right) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}.$$

Since $\lim_{s\to 1^+} \zeta(s) = \infty$, we have, $\lim_{s\to 1^+} \log \zeta(s) = \infty$. Thus,

$$\lim_{s\to 1^+} \log \zeta(s) = \lim_{s\to 1^+} \left(\sum_p \frac{1}{p^s} + \sum_p \sum_{m\geq 2} \frac{1}{mp^{ms}} \right) = \infty.$$

But, for $s \geq 1$, the second series on the right hand side,

$$\sum_p \sum_{m\geq 2} \frac{1}{mp^{ms}} \leq \sum_p \sum_{m\geq 2} \frac{1}{p^m} = \sum_p \frac{1}{p(p-1)} < \infty,$$

Therefore,

$$\lim_{s\to 1^+} \sum_p \frac{1}{p^s} = \infty.$$

This shows that there are infinitely many primes; otherwise, the above limit would be finite.

The above calculation can be refined as follows. Differentiating the identity,

$$\log \zeta(s) = -\sum_p \log\left(1 - \frac{1}{p^s}\right),$$

we get,

$$-\frac{\zeta'(s)}{\zeta(s)} = -\frac{\mathrm{d}}{\mathrm{d}s} \log \zeta(s) = \sum_p \frac{\mathrm{d}}{\mathrm{d}s} \log\left(1 - \frac{1}{p^s}\right).$$

Further, applying the chain rule for diffentiation,

$$\sum_p \frac{\mathrm{d}}{\mathrm{d}s} \log\left(1 - \frac{1}{p^s}\right) = \frac{\log p}{p^s - 1}.$$

Thus,

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log p}{p^s - 1} = \sum_p \sum_{m=1}^{\infty} \frac{\log p}{p^{ms}}.$$

This explains the use of the function

$$\psi(x) = \sum_p \sum_{\substack{m \geq 1 \\ p^m \leq x}} \log p,$$

in the study of the prime number theorem. This is a prototypical example of an important point of view in number theory first elucidated by Dirichlet – the study of arithmetic sums $\sum_{n \leq x} a(n)$ by investigating the analytic properties of the Dirichlet series,

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s},$$

in the region where it converges. In the case of the prime numbers, the relevant function that needs to be investigated is $\sum_{n \leq x} \Lambda(n)$ where the von Mangoldt function $\Lambda(n)$ is defined as:

$$\Lambda(n) := \begin{cases} \log p & \text{if } n = p^m,\ m \geq 1 \\ 0 & \text{otherwise} \end{cases}.$$

Note that the partial sum $\sum_{n \leq x} \Lambda(n)$ equals $\psi(x)$ and the associated series to be investigated is:

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},\ \mathrm{Re}(s) > 1. \qquad (1)$$

Henceforth, the zeta function was to be a primary tool to study prime numbers.

In 1859, Bernhard Riemann built on this point of view and wrote a famous nine-page article whose title can be translated into English as 'On the Number of Primes Less Than a Given Magnitude' [2]. The fundamental innovation in this work was to view Euler's zeta function as a function of *a complex variable*. That is, the zeta function of Riemann is a complex-valued function defined as:

Riemann wrote a breakthrough paper on the prime counting function and linked it to the study of the Riemann zeta function.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

for complex numbers s with the real part $\mathrm{Re}(s) > 1$. Since this series converges absolutely in the region $\{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}$ and uniformly in all compact subsets therein, it can be viewed as a complex-analytic function in this region.

Riemann's paper describes an idea that lies at the heart of what is called the analytic number theory today, namely analytic continuation. He derives a function on a larger domain of complex numbers, which is equal to $\sum_{n=1}^{\infty} \frac{1}{n^s}$ when $\mathrm{Re}(s) > 1$. This new function is complex-analytic on all points of the complex plane except $s = 1$. This extension of the zeta function to $\mathbb{C} \setminus \{1\}$, is called Riemann's zeta function.

Riemann then goes on to provide a 'vision document' that has guided research on this topic in the last two centuries. Owing to (1), the function $\psi(x)$ and therefore, the prime counting function $\pi(x)$ are inherently linked with the analytic properties of the function $\frac{\zeta'(s)}{\zeta(s)}$, and this naturally leads to questions about the complex zeroes of the zeta function, that is, those points s on the complex plane where $\zeta(s) = 0$. Riemann stated all these connections precisely and one of the key statements in his paper is *the explicit formula*, an explicit description of the relation between $\psi(x)$, and the location of the complex zeroes of the zeta function.

An important observation of Riemann was that the prime number theorem is equivalent to showing that all non-trivial zeroes of $\zeta(s)$, (that is, zeroes of the form $s = \rho + it$ with the imaginary part $t > 0$) must lie inside the critical strip, that is, the region $\{s \in \mathbb{C} : 0 < \rho < 1\}$. This idea was independently used by Hadamard and de la Vallée Poussin to prove the prime number theorem in 1896.

Properties of the prime counting function can be translated into explicit complex-analytic properties of the zeta function.

Even more refined estimates about $\psi(x)$ and $\pi(x)$ can be made with better knowledge about the location of the zeta zeroes inside the critical strip. In fact, in his paper, Riemann makes a conjecture that all zeta zeroes lying in the critical strip must have real part $1/2$. This conjecture is famously known as the 'Riemann hypothesis' and remains unproven till date. It is in the list of Millennium Prize Problems announced by the Clay Mathematics Institute that

promises an award of 1 million US dollars for a correct resolution.

Further explanation of Riemann's article will take us well beyond the scope of this article. Hence, we conclude this section by referring the reader to an excellent exposition [3] of Andrew Granville on the techniques and ideas in Riemann's work. For further reading, we also refer the reader to the 1974 book *Riemann's Zeta Function* by H M Edwards [4] which contains an English translation of Riemann's original German paper and a chapter-wise description of its contents.

2. Gaps Between Primes

In this section, we focus on another statistical aspect of the distribution of prime numbers, namely, gaps between consecutive primes. This is an exciting topic in the study of prime numbers, and some of the most important advances in this theme have come about within the last 15 years.

How far apart can two consecutive primes be? For starters, we observe that for any natural number n,

$$n! + 2,\ n! + 3,\ n! + 4, \ldots n! + n,$$

is a string of consecutive composite numbers. That is, for any number $n \geq 2$, we can find consecutive primes which are apart by at least n numbers. Thus, the gaps between consecutive primes can be arbitrarily large. What about small gaps? Do we have infinitely many pairs of primes with gaps below a fixed bound?

Let us start with listing the first few primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349 and so on.

In this listing, we immediately observe that the gaps between consecutive primes seem to oscillate. For several pairs, we have a gap of 2, they gradually increase to 4, 6, 8, 10 and so on, but keep

jumping back to 2. This pattern seems to repeat several times even in the limited list we have above. Similar observations for much larger sets of primes motivate the following questions.

As the primes grow larger and larger, do we have infinitely many pairs of consecutive primes with gap 2?

1. As the primes grow larger and larger, do we have infinitely many pairs of consecutive primes with gap 2?
2. Does there come a stage beyond which the gaps between consecutive primes increase and do not fall back to smaller numbers?
3. Can we predict how large the gaps can be at any stage? How much can these gaps differ from the average?

The twin prime conjecture is the assertion that there are infinitely many pairs of consecutive primes with gap 2. This is a special case of a more general 1849 conjecture of the French mathematician Alphonse de Polignac. This general conjecture states that for any even number K, there are infinitely many pairs of consecutive primes with gap K. This conjecture, if proved, would immediately address the first two questions (yes to the first and no to the second). The third question 'averages out' the first two questions: What is the variation among gaps between consecutive primes with respect to the average gap? An underlying question behind the above questions is whether the prime numbers are distributed among the natural numbers in a discernible pattern.

To check the infinity of twin primes, an immediate 'analytic' idea that comes to mind (inspired by Euler's use of zeta function) is to check if the series

$$\sum_{\substack{p \\ p,\, p+2 \text{ prime}}} \frac{1}{p}$$

diverges. In 1919, Viggo Brun showed that this sum is finite, which, unfortunately, tells us nothing about the finiteness or infinity of twin primes.

Mathematicians continued to grapple with the above questions in various ways. It was only in 2005 that three mathematicians – Dan Goldston, János Pintz and Cem Yildirim – made a remarkable observation that brought us a little closer to the twin prime

conjecture. They showed that there are infinitely many pairs of consecutive primes with gap arbitrarily small relative to the average gaps between consecutive primes. The question that now remained was if we could have infinitely many pairs with the absolutely smallest possible gap, namely, 2.

Yitang Zhang showed that there are infinitely many consecutive prime pairs with a gap bounded by 70 million.

In 2013, Yitang Zhang made a giant stride in this direction. He announced that there is a number N less than 70 million such that there are infinitely many pairs of consecutive primes with gap N. At first sight (to the layman), 70 million may come across as a ridiculously large bound. But that is not how the experts saw Zhang's theorem; instead, they recognized it as the first instance of a finite and explicit bound for infinitely many consecutive prime gaps. This is sufficient to see that the answer to the second question listed above is no. Stunned and impressed by Zhang's work, the mathematical community challenged itself to reduce the gap from 70 million to 2. Thus started the international Polymath Project with several contributors, some of the notable names being James Maynard and Terence Tao. As of today, the bound has been reduced to 246. Is it just a matter of time before 246 can be taken down to 2? Or does 246 represent the limit that can be obtained by current knowledge? We do not know. It is, however, widely believed that further reduction of gaps will require completely new insights.

We now make some comments on how the third question mentioned above is interpreted. We start by recalling the prime number theorem, which predicts that the number of primes up to x is asymptotic to

$$\frac{x}{\log x},$$

as $x \to \infty$. We now arrange the primes in an ascending order and let p_n denote the n-th prime number. We leave it as an exercise for the interested reader to deduce from the prime number theorem that:

$$p_n \sim n \log n \text{ as } n \to \infty.$$

That is,

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1.$$

Furthermore, if we list out the gaps between consecutive primes up to p_{N+1} as:

$$p_2 - p_1,\ p_3 - p_2, \ldots p_{N+1} - p_N,$$

the prime number theorem also tells us that the 'expected' or the 'average' gap

$$p_{n+1} - p_n$$

is asymptotically $\log p_n$. That is,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{p_{n+1} - p_n}{\log p_n} = 1.$$

For large values of N, one wonders whether, one can predict the proportion of values among

$$\left\{ \frac{p_{n+1} - p_n}{\log p_n} :\ n \leq N \right\}$$

that lie in a fixed interval $[a, b]$ of positive real numbers as $N \to \infty$. The answer is believed to be yes. In fact, it is conjectured that the 'normalized' gaps

$$\frac{p_{n+1} - p_n}{\log p_n}$$

can be modelled by the Poisson distribution. That is, for any two positive real numbers $a < b$,

$$\lim_{N\to\infty} \frac{1}{N} \#\left\{ 1 \leq n \leq N :\ a \leq \frac{p_{n+1} - p_n}{\log p_n} \leq b \right\} = \int_a^b e^{-t} dt.$$

In recent developments, building upon the ideas of Riemann, connections have also been made between the distribution of gaps among consecutive primes and gaps among consecutive zeroes s of the Riemann zeta function lying on the line $\mathrm{Re}(s) = 1/2$.

An investigation of this conjecture and its implications is a foundational theme in the subject of probabilistic number theory. We are nowhere near a resolution of this conjecture, but once again, we see how a difficult question about twin primes has evolved into a related question about the distribution of all consecutive prime gaps. In recent developments, building upon the ideas of Riemann, connections have also been made between the distribution of gaps among consecutive primes and gaps among consecutive zeroes s of the Riemann zeta function lying on the line $\mathrm{Re}(s) = 1/2$.

A comprehensive and detailed discussion of the probabilistic models that can predict the distribution of gaps between consecutive primes is present in the expository article [5] of K Soundararajan. We also refer the interested reader to the survey article [6] of M R Murty for an explanation of the recent developments around the twin prime problem, particularly the strategy of Zhang and how it was improved upon by Maynard and Tao.

3. Big Prime Numbers and Big Secrets

Prime numbers help in the safe digital transfer of information between two parties.

The study of prime numbers is not all about 'data analysis' of records of prime numbers. Prime numbers also have a very important use for us in the real world. They help us to transfer sensitive information over the internet between valid parties without being intercepted by an unauthorised third party. We describe this application below.

To begin with, imagine walking on the hour points of a clock. You may walk millions of steps, and yet, you will find yourself among the 12 points. In effect, therefore, the 'net' result of your walk is between 1 and 12. This is an example of a circular form of counting called 'counting modulo 12'. One can, of course, replace 12 with any number N and count modulo N. In this sense, each time we walk over N points on an N-hour clock, we find ourselves at the same point where we started. That is, any multiple of N steps amounts to a walk with zero change.

In October 1640, the French lawyer-mathematician Pierre de Fermat made an observation in a letter to a friend.

Let p be a prime number. If we take any number A of our choice and walk A^p steps on a p-hour clock, we will find ourselves at the same point as if we had merely walked A steps. For example, on a 13-hour clock, whether you walk 11 steps or a whopping 11^{13} steps from the same starting point, you will find yourself at the same end point. In mathematical language,

$$A^p \equiv A \pmod{p}.$$

Equivalently, p divides $A^p - A$.

This theorem, at the heart of number theory, is famously known as 'Fermat's little theorem', even though it was proved almost a hundred years later by Leonhard Euler.

Theorem. [Fermat–Euler Theorem]: *Let N be a natural number and A be an integer such that A and N are coprime, that is, the greatest common divisor of A and N is 1. Let $\phi(N)$ denote the number of integers lying between 1 and N which are coprime to N. Then,*

$$A^{\phi(N)} \equiv 1 \,(\mathrm{mod}\, N).$$

Thus,

$$A^{\phi(N)+1} \equiv A \,(\mathrm{mod}\, N).$$

The RSA cryptosystem depends on the fundamental Fermat–Euler theorem discovered three centuries ago.

Around two hundred and forty years later, in 1978, Ron Rivest, Adi Shamir, and Leonard Adleman, three computer scientists at the Massachusetts Institute of Technology (USA), exploited the Fermat–Euler theorem and developed a method to share information between two parties safely. Typically, when a message is sent from a sender to a receiver, the sender has to disguise or 'encrypt' the message and the receiver has to decipher or 'decrypt' it. The method (or *k*ey) for the encryption and decryption is discussed privately between these parties or is shared between them through other safe sources. The RSA method (named after its creators) is set up in such a way that the key to encrypt a message is made public. While anyone can encrypt a message, sign it and send it across, only the intended receiver has the knowledge to decrypt a message and deduce whether it comes from a genuine sender. Such a system is called a *p*ublic key cryptosystem.

The method is easy to understand and we attempt to present it below in a simple form.

1. Instead of a prime p, an online merchant takes a semi-prime number N, which is a product of two primes p and q, roughly of equal size. The reader can quickly check that for this chosen N, $\phi(N)$ equals $(p-1)(q-1)$. Thus, the Fermat–Euler theorem tells us that for any number A,

$$A^{(p-1)(q-1)+1} \equiv A \,(\mathrm{mod}\, pq).$$

The merchant then chooses two numbers E and D, so that $(p-1)(q-1)+1 = ED$. The merchant makes N and E public and keeps D private.

2. You, the buyer, will typically take your credit card number A (which will be smaller than N) and encrypt it as the net value of $A^E \pmod N$. You don't do it yourself, of course. You enter the number and the website does it for you since the encryption key E is public.

3. The number D is not public. It is known privately to the merchant. On receiving the encrypted message $A^E \pmod N$, the merchant raises it again to the power D and calculates $A^{ED} \pmod N$. By basic congruence arithmetic and by the Fermat–Euler theorem,

$$\begin{aligned}(A^E)^D \equiv A^{ED} &\equiv A^{(p-1)(q-1)+1} \pmod N \\ &\equiv A \pmod N.\end{aligned}$$

This gives back the number A to the merchant. The credit card number (or intended message) therefore gets decrypted back to A.

But, you may ask: If N and E are public, can D really stay secret? The answer is an emphatic yes.

The safety of the RSA algorithm lies in the fact that it is very, very difficult to break down or to factorise a large number N into its prime factors p and q. Thus, even if the 'encryption' key E is public, to find out D, an unscrupulous third party will have to know the value of $\phi(N) = (p-1)(q-1)$, and this is not possible unless one is able to factor N into its constituent primes p and q. This makes it practically infeasible to find out the decryption key D (which only the intended receiver knows) within a reasonable time.

In their 1978 paper [7] on the RSA algorithm, the authors estimated that the computing resources of those days could take, for example, 74 years to factor a number with 100 decimal digits and 38,00000000 years to factor a number with 200 decimal digits! Today, we have more sophisticated computing resources and

methods to factor numbers of this size. These methods originate from abstract ideas in mathematics like the number field sieve and elliptic curves. But, we now use even larger numbers for encryption with unfeasible factoring times using current technology.

A lot of research has gone into factoring large numbers. For example, between 1991 and 2007, the RSA Laboratories, a company formed by Rivest, Shamir, and Adleman, ran the factoring challenge. They listed out semi-primes of various sizes with cash prizes for those who could factor them.

A lot of research has gone into factoring large numbers. For example, between 1991 and 2007, the RSA Laboratories, a company formed by Rivest, Shamir, and Adleman, ran the factoring challenge. They listed out semi-primes of various sizes with cash prizes for those who could factor them.

The fact that it takes much longer to factorise numbers than to generate primes and multiply them keeps our information safe. In fact, the interested reader can go to secure websites (for example their email provider) and check the digital certificates. These clearly state the encryption algorithm (most likely, the RSA algorithm), the public key as well as the key sizes. The certificate also mentions its expiry dates. This is to ensure that the keys are updated before an unscrupulous party gets hold of an existing private key.

Conclusion

Prime numbers have fascinated us for a long time. We saw in this article that developments in this study are rather abruptly distributed over the last three millennia. Sometimes, centuries would elapse before any new development would take place. On the other hand, occasionally there would be intense periods of activity when in a matter of decades, breakthrough ideas would appear and create a major impact on prime number theory. In retrospect, some of these ideas may look simple to us, but to discover them from scratch requires great intellectual power and ingenuity in thinking. Sometimes, ideas would be expressed in letters among friends and would motivate people with fresh points of view to

jump into the subject. Last, but not the least, even though the study of some of these ideas would appear to be theoretical in the short term, a few centuries down the line, they would lead to innovations with a major impact on how the world functions today, for example, Fermat's little theorem and its use in safe internet transactions without which many of us cannot imagine a life . We hope that we could give a small flavour of some of these ideas in this article and hope that the interested reader will find at least one of them interesting enough to pursue in greater detail.

Suggested Reading

[1] M H Weissman, Why Prime Numbers Still Fascinate Mathematicians, 2,300 Years Later, *The Conversation*, April 2, 2018. https://theconversation.com/why-prime-numbers-still-fascinate-mathematicians-2-300-years-later-92484.

[2] B Riemann, *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*, *Bernard Riemann's Gesammelte Mathematische Werke Und Wissenschaftliche Nachlass*, Zweite Auflage, pp.145–155, Teubner, Leipzig, 1892; reprinted, Dover, New York, 1953.

[3] A Granville, What is the Best Approach to Counting Primes? A century of Advancing Mathematics, *Math. Assoc. America*, pp.83–116, , Washington, DC, 2015.

[4] H M Edwards, *Riemann's Zeta Function*, Reprint of the 1974 original [Academic Press, New York], Dover Publications, Inc., Mineola, NY, 2001.

[5] K Soundararajan, Small Gaps Between Prime Numbers: The Work of Goldston–Pintz–Yildirim, *Bulletin of the American Mathematical Society (N. S.)*, Vol.44, No.1, pp.1–18, 2007.

[6] M R Murty, New Developments on the Twin Prime Problem and Generalizations, *Hardy–Ramanujan Journal*, Vol.37, pp.13–19, 2014.

[7] R L Rivest, A Shamir and L Adleman, A Method for Obtaining Digital Signatures and Public-key Cryptosystems, *Communications of the Association for Computing Machinery*, Vol.21, No.2, pp.120–126, 1978.

Address for Correspondence
Kaneenika Sinha
IISER Pune
Dr Homi Bhabha Road
Pashan, Pune 411 008, India.
Email:
kaneenika@iiserpune.ac.in