The Hidden Structure of the World Revealed Through Prime Numbers

Chen mi

1 Introduction

Imagine a security system so secure that even with an army of the world's most powerful computers, it would take them years to crack it. This level of security is built on a seemingly simple topic covered in school: prime numbers.

Prime numbers are one of the most important concepts in mathematics and form the foundation of number theory. They are defined as follows:

$$p \text{ is prime if } p > 1 \text{ and its only positive divisors are 1 and } p.$$

Despite this simple definition, prime numbers remain unpredictable, and much of their behaviour is still beyond our understanding. Euclid was the first to publish a definition of prime numbers, in *The Elements* around 300 BCE. He treated numbers as line segments, saying that one line "measures" another if a whole number of copies fits into it exactly without remainder; this is the modern idea of division. In this framework, he defined a prime as a number "measured by a unit alone", meaning it is divisible only by 1 and itself.

This article explores how primes are the "atoms" of all integers, key discoveries about them, how they are distributed, and how they underpin modern cryptography and online security. It then turns to one of the most famous unsolved problems about primes, the Riemann Hypothesis, whose solution would deepen our understanding of how primes are distributed and could improve cryptography and computer algorithms.

2 The Structure of Numbers

The importance of primes derives from the fact that they are the "atoms" or "building blocks" of all integers. This idea is first stated in the *Fundamental Theorem of Arithmetic*, which explains that the structure of numbers can be expressed using prime factorisation, where any integer greater than 1 can be expressed as:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i}. \tag{1}$$

Here, p_i are distinct prime numbers and a_i are positive integers.

Take, for example:

$$120 = 2^3 \times 3 \times 5.$$

Prime factorisation is the foundation of modern cryptographic security as this prime factorisation is difficult to reverse in the sense that while it is simple to multiply primes to obtain 120, it is much harder to start with 120 and recover its prime factors. This asymmetry between factorisation and multiplication creates a "one-way" system, where multiplying primes together to obtain a number is easy, whereas factorising that number to find the original prime factors is much more difficult. Therefore, this relationship between multiplication and factorisation forms the foundation of modern cryptography, most notably in RSA (Rivest–Shamir–Adleman), which utilises this phenomenon by using the product of two large primes as part of a public key, while keeping the original primes

secret. Thus, efficiently decrypting data without the private key becomes extremely difficult, as factorising the large number would take an excessive amount of time using known classical methods. This can be mathematically illustrated through simple number theory:

Let p and q be very large prime numbers. In cryptographic systems, they are multiplied; let this result be N. So,

$$N = pq. \tag{2}$$

In trial division, one would need to check possible divisors up to $\sqrt{N}$ to establish the prime factors in the worst case. For sufficiently large, carefully chosen primes, this difficulty helps provide security.

3 Euclid and the Infinity of Primes

The first major breakthrough in prime numbers was by Euclid, who proved that there are infinitely many prime numbers in *The Elements* around 300 BCE.

Euclid proved this through contradiction. First, he assumed that there are only a finite number of primes, meaning that we are able to write a complete list:

$$p_1, p_2, p_3, \ldots, p_n.$$

Consider the number:

$$N = p_1 p_2 p_3 \cdots p_n + 1. \tag{3}$$

N is either prime or not prime (composite). If N is prime, then it is a new prime that is not on this finite list, suggesting that the list is incomplete. If it is not prime, then it is made up from prime factors since they are the "building blocks" of all integers, meaning that those prime factors of N will divide N exactly. Here arises the problem. None of the primes on the finite list divide N exactly, because every p_i divides $p_1 p_2 p_3 \cdots p_n$, but leaves remainder 1 when dividing N. Therefore, since an integer $N > 1$ must have a prime factor, there must be a prime factor that is not on this finite list. So, the list is incomplete. The assumption that there are only finitely many primes leads to a contradiction; therefore, there are infinitely many prime numbers.

4 The Distribution of Primes

Prime numbers, despite being infinite, do not occur at regular intervals. The general trend of their distribution is that they get increasingly sparse as numbers get larger. Their distribution is described in the *Prime Number Theorem*, which states:

$$\pi(x) \sim \frac{x}{\ln x} \qquad (x \to \infty). \tag{4}$$

Where:

- $\pi(x)$ is the number of primes less than or equal to x;
- $\ln x$ is the natural logarithm of x;
- $\sim$ means that the ratio of the two sides approaches 1 as x becomes large.

From this expression, we can deduce that the approximate probability that an integer near x is prime is:

$$\frac{1}{\ln x}. \tag{5}$$

This implies that prime numbers get progressively rarer as numbers get larger, but always exist. This expression gives us only an approximation of prime number locations, but not their exact locations. Understanding their precise distribution remains a challenge for mathematicians.

5 Attempts to Find Prime Numbers

5.1 The Sieve of Eratosthenes

The Sieve of Eratosthenes is one of the earliest methods for finding prime numbers. It is an algorithmic procedure used to systematically identify prime numbers by filtering out composite numbers like a sieve. While none of his original works remain today, he is later credited with a method by Nicomachus of Gerasa in his *Introduction to Arithmetic*. This method is carried out by iteratively marking integers as composite that are multiples of primes, starting with the first prime number, 2, and working one's way upwards. Subsequently, the next unmarked number on the number line is then marked as prime and all of its multiples are marked. This algorithm is repeated until all necessary multiples have been eliminated. As a result, the remaining unmarked numbers greater than 1 are prime numbers. This is a highly efficient method for finding all primes up to 10^7; however, it becomes impractical for obtaining extremely large primes, as it requires storing numbers up to the specified bound as well as continuously calculating multiples. This can require an immense amount of memory and time when the bound becomes very large.

5.2 Mersenne Numbers

Mersenne offers another way of finding large prime numbers by observing that some prime numbers can be expressed as

$$M_n = 2^n - 1, \tag{6}$$

where n represents a positive integer. He sought patterns or rules for values of n that would yield prime numbers. One of the largest known primes, discovered in 2024, is the Mersenne prime

$$2^{136\,279\,841} - 1. \tag{7}$$

Using this expression, mathematicians have found many exceptionally large primes in the hope of discovering patterns in their distribution. Despite this amazing feat, there remains no simple formula that identifies every prime number. One famous unsolved problem related to the distribution of primes is explained below.

6 The Riemann Hypothesis

The Riemann Hypothesis posits that all non-trivial zeros of the Riemann zeta function have a real part equal to $\frac{1}{2}$. The zeta function is initially defined by the series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots, \qquad \mathrm{Re}(s) > 1. \tag{8}$$

The function can then be extended to other complex values of s by analytic continuation (except at $s = 1$).

Where:

- s is a complex number;
- n ranges over the positive integers.

Riemann suggested that complex numbers can be written in the form

$$s = a + bi, \tag{9}$$

where a is the real part and b is the imaginary part. His hypothesis concerns the non-trivial solutions of

$$\zeta(s) = 0. \tag{10}$$

These zeros reveal properties of the function and are linked to the distribution of prime numbers. The Riemann Hypothesis states that all non-trivial zeros lie on the vertical line

$$\mathrm{Re}(s) = \frac{1}{2} \tag{11}$$

in the complex plane. If proven, it would give mathematicians a much more precise understanding of the errors in estimates of the distribution of primes, although it would not reveal the exact location of every prime.

Proving the Riemann Hypothesis would be a major advance in number theory and could have indirect implications for algorithms involving prime numbers. However, it would not automatically make RSA encryption more secure or provide a direct method for decrypting encrypted information.

7 Conclusion

Prime numbers—the building blocks of all positive integers greater than 1—hold secrets that continue to interest mathematicians. Their unique structure as the "atoms" of numbers, shown through prime factorisation, reveals the asymmetry between multiplication and factorisation, thus creating the foundation of modern cryptography. It allows systems like RSA encryption to secure communication and support online banking. We know quite a great deal about prime numbers, but at the same time prime numbers remain mysterious, with questions about their distribution and unsolved problems like the Riemann Hypothesis that, if solved, could open the door to many more discoveries.

References

Bischoff, Manon. "The Biggest Problem in Mathematics Is Finally a Step Closer to Being Solved." *Scientific American*, 1 July 2024. https://www.scientificamerican.com/article/the-riemann-hypothesis-the-biggest-problem-in-mathematics-is-a-step-closer/.

"Euclid's Theorem." *Wikipedia*, Wikimedia Foundation. https://en.wikipedia.org/wiki/Euclid%27s_theorem.

"Fundamental Theorem of Arithmetic." *Wikipedia*, Wikimedia Foundation. https://en.wikipedia.org/wiki/Fundamental_theorem_of_arithmetic.

"Infinite Primes." *YouTube*, uploaded by Numberphile, 23 April 2013. https://www.youtube.com/watch?v=ctC33JAV4FI.

"Mersenne Prime." *Wikipedia*, Wikimedia Foundation. https://en.wikipedia.org/wiki/Mersenne_prime.

"Prime Number." *Wikipedia*, Wikimedia Foundation. https://en.wikipedia.org/wiki/Prime_number.

"Prime Number Theorem." *Wikipedia*, Wikimedia Foundation. https://en.wikipedia.org/wiki/Prime_number_theorem.

"Riemann Hypothesis." *Wikipedia*, Wikimedia Foundation. https://en.wikipedia.org/wiki/Riemann_hypothesis.

"Riemann Zeta Function." *Wikipedia*, Wikimedia Foundation. https://en.wikipedia.org/wiki/Riemann_zeta_function.

"RSA (Cryptosystem)." *Wikipedia*, Wikimedia Foundation. https://en.wikipedia.org/wiki/RSA_(cryptosystem).

Shivakumar M. D. "The Riemann Hypothesis and Its Implications." *World Journal of Advanced Research and Reviews*, vol. 10, no. 3, 2021, pp. 493–498. https://doi.org/10.30574/wjarr.2021.10.3.0287.

Watkins, Matthew R. "Prime Quotes." *Inexplicable Secrets of Creation*, University of Exeter. https://empslocal.ex.ac.uk/people/staff/mrwatkin/isoc/quotes.htm.