Pondering the world of primes and their fascinating properties in the modern world

Simple to know yet complex to untangle. Prime numbers are to mathematicians just as elementary particles are to physicists hence why they are described as the "atoms" of mathematics where every positive integer greater than 1 can be uniquely expressed as a product of prime numbers[fundamental theorem of arithmetic].

Prime numbers have inspired mathematicians throughout time to delve deeper into a world of unsolved problems, new discoveries, and technological advancements. To understand where the real fascination of the prime numbers began, we travel around 2000 years- Euclid has just proved there are infinitely many prime numbers by simple contradiction.

Euclid's Proof

Assume there are finite number of prime numbers:
$p_1, p_2, p_3 \dots p_n$ are all of the primes.
Let $X = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1$
X cannot be divisible by $p_1, p_2, p_3 \dots p_n$
This is because there will be a remainder of 1 hence X is a prime itself OR divisible by a prime which is not on the list. Therefore, the assumption that there are finite number of prime numbers is false as the list is incomplete.

In 1737 Euler went a step further and proved that, interestingly, the series of the reciprocals of the prime numbers diverges. Euler also observed that the divergence of this series is much slower then the rate of divergence of the harmonic series:

Reciprocals of Harmonic and Prime number series

"The sum of the series of the reciprocals of the prime numbers,
$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots$
intuitively, is infinitely large, but it is infinitely many times less than the sum of the harmonic series,
$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots$
Furthermore, the sum of the former series is like the logarithm of the sum of the latter series. "

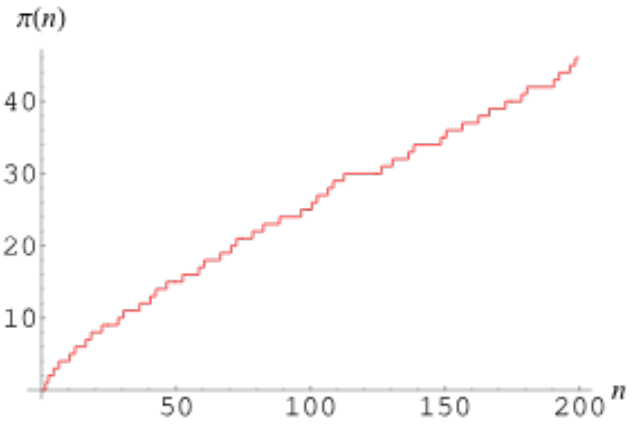
This statement appeared to be one of earliest attempt to quantify the frequency of the prime numbers among the natural numbers.

Dispersion of prime numbers compared to harmonic series

Harmonic series:
We can see that the harmonic series diverges meaning that its partial sums increase without bounds as more terms are added:
$\Sigma_{n=1}^{\infty} \frac{1}{n} = \infty$ The partial sums for the harmonic series can also be expressed as: $S_n = ln(n) + \gamma + O(\frac{1}{n})$ where ln(n) is the natural log of n, γ is the Euler-Mascheroni constant and $O(\frac{1}{n})$ shows a term decreasing to 0 as n increases.

Prime reciprocal series:
The reciprocal of prime numbers also diverges, but it diverge much slower than the harmonic series:
$P_n = ln(ln(n)) + C + O(1)$ where C and O(1) are constant terms. This slower divergence rate reflects the sparser distribution of prime numbers relative to the natural numbers.

Finding regularities and trying to understand the patterns and distributions in the prime sequences became one of the greatest mathematical endeavours. Another appeared as a conjecture written by a French mathematician Adrien-Marie Legendre where on the basis of his study of a table of primes up to 1 million, Legendre stated: If x is not greater than 1, 000, 000 then $\frac{x}{ln(x)} - 1.08366$is very close to $\pi(x)$ [the prime counting function]. This was further conjectured by the mathematician Gauss until the theorem was finally proved by Hadamard and la Valee Poussin who independently showed that: $\pi(x) \approx x\frac{}{ln(x)}$



Plot of π(X)

Where $\pi(x)$ is the number of primes less than or equal to x. If you select a natural number randomly, the likelihood of P(x) being a prime number is approximately $\frac{1}{ln(x)}$. This shows us that the the average gap between consecutive prime numbers is about $ln(x)$. This concept of finding the density of prime numbers provided a statistical framework for understanding the distribution of primes. However,the apparent regularity in their distribution, the precise structure and behaviour of prime numbers using this approximation was still far from understanding the fluctuations and irregularities of the distribution of primes.

Puruit of patterns

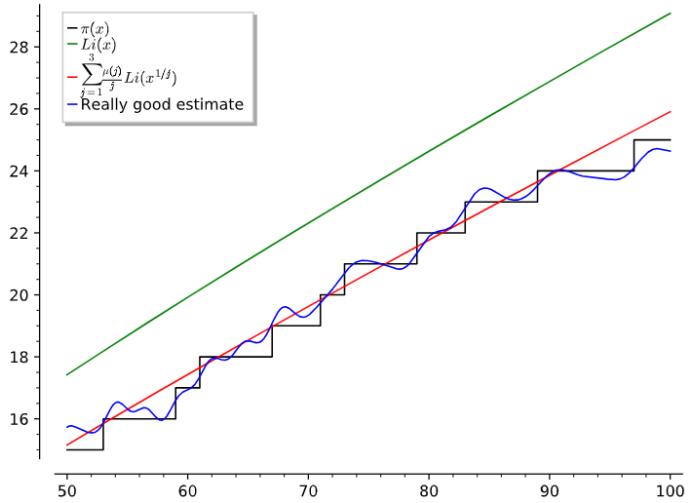
We consider the extent to which we can find 'order' in the primes to be a measure of our understanding of patterns in the prime sequence. Finding patterns and possible sequences in this infinite and unpredictable list is still one of the greatest mathematical challenges. Unlike the sequence of squares, where the n^{th} square is given by n^2 , we have no usable formula allowing us to explicitly determine the n^{th} prime. The closer and closer mathematicians get to untangling this infinite array of these unique properties, the more intriguing discoveries we have made. What's even more exhilarating is the fact that Riemann was able to refine the prime number counting function $\pi(x)$ by minimizing the discrepancies between predictions and empirical data. His work sought to align the graph of the refined function, often denoted as $R(x)$, more closely with the actual distribution of prime numbers:

Reiman's explicit function

J(x) = Li(x) - Σ_p^{∞}Li(x^{ρ}) - log2 + $\int_x^{\infty} \frac{1}{t(t^2-1)logt}\,dt$

-Reimann's prime number theorem approximating the number of primes under a given | x | .

- - Li(x) is the logarithmic integral which is a better estimation of $\pi(x)$
- - Second term - sum of the logarithmic integral of of x^{ρ} summed over ρ which are the non-trivial zeros of the Riemann zeta function.
- - Final term is an integral which returns a value of 0 when x < 2 because no primes are less than 2.



The prime counting step function $\pi(x)$ and other approximations compared to the explicit formula for the Reimann prime counting function (really good estimate) using the first 100 non-trivial zeros ρ of the Riemann Zeta function

This mathematical thought proved to be more accurate for values of x compared to the prime number theorem's approximation. We can see from the graph that the periodic term causes the function to begin to approach the shape of $\pi(x)$!

Reinman's ground breaking analysis of prime numbers has continued to stand as a cornerstone in the realms of prime and analytic number theory and there no doubt what Reinmann has done is one the greatest successes in finding order of primes as well as opening doors to the properties of prime numbers in modern day cryptography.

Primes in Crytography

Prime numbers aren't just the backbone of mathematics but also the heart of modern technology. The use of prime numbers in modern day cryptography was first devised in 1977 and called the RSA Public Key System. The mathematics behind the encryption utilises classical number theory: Fermat's Little Theorem and the Chinese Remainder Theorem.

Fermat's little theorem in cryptography

Fermat's Little Theorem states that if p is prime then $a^p \equiv a(mod p)$ for all a.
For Example, is it true that: $p = 5 \Rightarrow a^5 \equiv a(mod 5)$?
for all a = 1, 2, 3 or 4(mod5)?
Check: if a is itself a multiple of 5, the both a^p and a are equal to 0(mod 5) so identity will hold. So we need to check cases where a is not a multiple of 5:
a = 1 $\rightarrow$ Holds true trivially
$a = 2 \Rightarrow a^5 = 32 \equiv 2(\text{mod } 5)$
$a = 3 \Rightarrow a^2 = 32 \equiv 4(\text{mod } 5)$
$a = 4 \Rightarrow a^2 = 16 \equiv 1(\text{mod } 5)$
In Crytography: The public and private keys in RSA encryption are generated using this theorem. Fermat's Little Theorem take advantage of the the fact that, while it's easy to multiply two numbers (encryption), factorising the number into its prime factors without the decryption key is computationally infeasible.

Chinese Remainder Theorem in Cryptography

The Chinese Remainder Theorem [CRT] and Fermat's Little theorem [FLT] coincide when it comes to crytography. FLT is applied during key generation in RSA to ensure security of encryption and decryption operations whereas CRT is used to speed up decryptions. CRT is applied during decryption to break down modular exponentiation into more managable computations. In essence, CRT helps you unlock a complicated "lock" by dealing with simpler "locks" separately and combining the results to access the contents of the "package" which was inside the bigger "lock".

It's not only the use of these two theorems but many more which have enabled the development of secure encryption methods forming the backbone of modern digital communication and online transactions. Prime numbers will always be the forefront of ensuring the security of sensitive information such as bank transactions to safeguarding personal data. I hope to many of us, there is still this hope as future mathematicians that soon, prime numbers will be understood to a point where their pattern can truly be untangled.

References

"Complex Analysis - Riemann's Explicit Formula – Proof and Convergence." Mathematics Stack Exchange, 2020, math.stackexchange.com/questions/3591648/riemanns-explicit-formula-proof-convergence.

"NTIC the Riemann Explicit Formula." Math.gordon.edu, math.gordon.edu/ntic/ntic2021-7/section-riemann-formula.html. Accessed 30 Mar. 2024.

Kumchev, Angel. The Distribution of Prime Numbers. 2005.

Li, Hao. The Series of Reciprocals of the Primes Diverges.

Mazur, Barry, and William Stein. Prime Numbers and the Riemann Hypothesis. 4 Nov. 2016.

Veisdal, Jørgen. "The Riemann Hypothesis, Explained." Www.privatdozent.co, 12 Nov. 2021, www.privatdozent.co/p/the-riemann-hypothesis-explained-478.

"Why Are Primes Important in Cryptography?" Stack Overflow, Jan. 2024, stackoverflow.com/questions/439870/why-are-primes-important-in-cryptography.