Bertrand's Postulate

What is the Bertrand's Postulate

- It states that for any integer $n > 1$, there is always at least one prime p such that $n < p < 2n$.
- The conjecture was proposed by Joseph Bertrand in 1845 and was later proven by the Russian mathematician Pafnuty Chebyshev in 1852.
- It was also later proven in a simpler method by Paul Erdös.
- Chebyshev's proof showcased the power of analytic techniques in addressing problems in number theory while Erdös' proof utilized combinatorial methods rather than complex analysis.

Definitions

Binomial Coefficient $\binom{n}{k}$ represents the number of ways to choose k elements from a set of n elements and is given by: (particularly used in Erdös' proof)

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Important Functions

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

where the sum is over all primes $p \leq x$.

$$\psi(x) = \sum_{p^k \leq x} log(p)$$

extends the first Chebyshev function by including logarithms of all prime powers. This function smooths out the contributions of primes and provides a more detailed picture of prime distribution.

Erdös' Proof

First Lemma:

$$\binom{2n}{n} \geq \frac{4^n}{2n}$$

Second Lemma:

$$If \quad \sum_{i\geq 1}(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor) \quad Then \;\; p^a \leq 2n$$

Third Lemma:

$$\prod_{p\leq x} p \leq 4^{x-1}$$

1st Lemma Proof

- First let's look at the general form $(a+b)^n$ expanded:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Then let's plug in the following: Let's plug in a = 1, b = 1, and n = 2n. After plugging these values into the general form of $(a+b)^n$ expanded we get the following:

$$(1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} 1^k 1^{2n-k}$$

1st Lemma Proof

- Therefore, if we simplify the left side further we get 4^n and if we simplify the right side further it would equal to 1 which results in the following:

$$4^n = \sum_{k=0}^{2n} \binom{2n}{k}$$

- Now we can go ahead and split the right part of the equal sign (the summation) into 2 different parts which makes it simpler to find the sum of: The first part is: we should look at when k=0 and when k=2n. While doing this we can get two binomial coefficients which are respectively $\binom{2n}{0}\binom{2n}{2n}$. Then we can look at the second part of the summation as what is left after the first part being the following:

$$\sum_{k=1}^{2n-1} \binom{2n}{k}$$

1st Lemma Proof

- Due to the above information we can now conclude the following equation that:

$$(4)^n = 2 + \sum_{k=1}^{2n-1} \binom{2n}{k}$$

Now we can say that the biggest/largest part of the right part of the equal sign above is $\binom{2n}{n}$
Therefore giving us that;

$$4^n \leq 2n \binom{2n}{n}$$

Then if we divide both sides by 2n we get the following which therefore proves the first key lemma:

$$\binom{2n}{n} \geq \frac{4^n}{2n}$$

-

A quick look at Chebyshev's Proof

- Chebyshev used the concept of Chebyshev functions, specifically $\vartheta(x)$ and $\psi(x)$, which are related to the distribution of prime numbers. These functions sum the logarithms of primes and prime powers, respectively, up to a given number
- Prime Number Theorem: Chebyshev's proof relies on estimates of the Chebyshev functions. He showed that for large n, $\vartheta(x)$ and $\psi(x)$ are approximately $nlog(n)$, which helps to bound the number of primes in given intervals.

A quick look at Chebyshev's Proof

- By establishing inequalities for $\vartheta(x)$ and $\psi(x)$, Chebyshev demonstrated that :

$$\psi(2n) - \psi(n) > 2 \; for \; n > 1$$

  implying the existence of primes between n and 2n.
- Bound on Factorials: Chebyshev also used properties of factorials and binomial coefficients to show that the ratio $\frac{(2n)!}{(n!)^2}$ is an integer and grows rapidly, implying that there must be primes in the range $n < p < 2n$ to account for this growth.

Prime number cases connected to Bertrand's Postulate

There exists a proof that there is always a prime number between n^3 and $(n+1)^3$ connects to Bertrand's Postulate by reinforcing the understanding of the distribution of prime numbers within specific intervals.

By ensuring the presence of a prime within the interval n^3 and $(n+1)^3$, we see a similar principle at work: primes do not become sparse too quickly, even within much larger gaps. This consistency supports the broader theme in number theory that prime numbers, while irregular in their appearance, do follow certain predictable patterns.

Future Research and Implications

- Is there always a prime p between n^2 and $(n+1)^2$?
- Understanding prime distribution is fundamental to cryptography, particularly in public-key cryptographic systems like RSA, which rely on the difficulty of factoring large composite numbers into primes. The postulate ensures the existence of primes within specific intervals, aiding in the efficient generation of large prime numbers necessary for secure cryptographic keys.
- Block-Chain Technology: The integrity of blockchain relies on cryptographic principles, many of which depend on the properties of prime numbers.

Conclusion

- Bertrand's Postulate highlights the dense and regular distribution of prime numbers within specific intervals, reinforcing the idea that primes are never too far apart as numbers increase.
- Through the case of n^3 and $(n+1)^3$ I've learned the existence and frequency of primes in these cubic intervals, providing empirical evidence of prime distribution in non-linear ranges.

Thank you for listening!

ayaannisar12@gmail.com