CS300 - Odd Semester 2022

INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

Lecture : Infinitude of Prime numbers

30 August, 2022

Lecturer: Rajat Mittal *Scribe: Jhaansi Reddy*

What are prime numbers? We all are familiar with prime numbers and have been using them as a special set of numbers in various mathematical problems.

Let us recall them by firstly defining them.

Definition 0.1. Prime numbers are natural numbers which have exactly two divisors, that is '1' and the number itself. The set denotation for these numbers is $\mathbb{P}$.

$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47..\}$

Let us also recall that any composite number ($\mathbb{N} - \mathbb{P}$) can be represented as product of primes.
Example :

- $22 = 2 * 11$
- $48 = 2 * 2 * 2 * 2 * 3$
- $45 = 3 * 3 * 5$

How many such numbers? Now that we know what prime numbers are, it makes sense that we think and discuss about the count of primes. Cardinality of natural numbers is infinite. *Are the prime numbers infinite too?* **There are infinite number of primes.** We, kind of, have accepted the fact that there are infinite primes, but in this lecture let us proceed to prove this fact with three different approaches.

1 Euclid's proof for infinite primes

Let us assume that there are finite number of prime numbers and that be n in count.

So, $\mathbb{P}' = \{P_1, P_2, P_3, ..., P_{n-1}, P_n\}$

Take a natural number k such that $k = P_1.P_2.P_3...P_n + 1$

Since P_n is the largest prime, k is a composite number, and there must exist a prime, P_i that divides k.

That would mean that P_i must also divide 1, however there doesn't exist such a prime. This suggests us that there must exist another prime not in $\mathbb{P}'$ that divides k.

Hence, our assumption that there are finite prime numbers is false.

2 Proof using Lagrange's Theorem

Lagrange's Theorem

For any finite group G the order of any of its subgroup divides the order of G.

Let us assume that there are finite prime numbers, and the largest among them is p. Consider a number $2^p - 1$ and its prime divisor q.

From *Fermat's Theorem*, firstly, it can be deduced that the sub group generated by 2 has order p, since there is no other smaller number that divides p. Also, since 2^p will leave a remainder 1 when divided by q, p has to divide $q - 1$.

This will imply

$p \leq q - 1 \implies p < q$.

Showing us that there exists a prime number q larger than p, which contradicts our assumption.

3 Erdos proof for infinite primes

Let $\mathbb{P} = \{P_1, P_2.....P_n\}$

Now consider a sequence $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + ...\frac{1}{P_n}$.

If this sequence (which is sum of reciprocals of primes) diverging, it is implied that the cardinality of the set of primes is infinity.

Let us proceed by assuming that this sequence is converging.

So, by definition of a converging sequence sum, we can say

$$\exists k \quad \text{s.t} \sum_{n \geq k+1} \frac{1}{P_n} \leq \frac{1}{2} \tag{1}$$

Multiplying N both sides we get,

$$\forall N \in \mathbb{N} \quad \sum_{n \geq k+1} \frac{N}{P_n} \leq \frac{N}{2} \tag{2}$$

Let us now categorize the natural numbers into n as big and $small$.

Definition 3.1. A natural number $n \leq N$ is big, if $\exists P_m, m \geq k+1$ s.t $P_m | n$. Let these numbers be N_{big} in number.

Definition 3.2. A natural number $n \leq N$ is $small$, if all its factors are small. Let these numbers be N_{small} in number.

This means a number which is not big, has to be $small$. i.e. these sets are complementary to each other.

$$N_{big} + N_{small} = N \tag{3}$$

Number of numbers in set A divisible by k is $\frac{n}{k}$, where n is cardinality of set A.

Here, N_{big} is the number of numbers divisible by P_m for $m \geq k+1$. So,

$$N_{big} \leq \sum_{m \geq k+1} \frac{N}{P_m} \tag{4}$$

From (2) and (4),

$$N_{big} \leq \frac{N}{2} \tag{5}$$

For, numbers which are $small$, each of them can be represented as $a_n.b_n^2$, where a_n and b_n are taken from $\{P_1, P_2.....P_k\}$.

While b_n represents the product of primes which taken as pairs (to make even power) a_n constitutes the rest of it, meaning that a prime can either be present once or none in product representation of a_n. Hence a_n can take 2^k values. Whereas b_n, at the most can take $\sqrt{N}$ values.

So, for large N

$$N_{small} \leq 2^k.\sqrt{N} \leq \frac{N}{2} \tag{6}$$

This brings us to

$$N_{big} + N_{small} < N \tag{7}$$

Contradiction.

Hence there are infinite primes.

References

[1] W. L. Hosch. Fermat's theorem. https://www.britannica.com/science/Fermats-theorem.

[2] G. M. Z. Martin Aigner. *Proofs from THE BOOK*. Springer, 1998.

[3] Wikipedia. Fermat's theorem. https://en.wikipedia.org/wiki/Lagrange%27s_theorem_(group_theory).

[2] [1] [3]