INDIAN INSTITUTE OF TECHNOLOGY MADRAS • सिद्धिर्भवति कर्मजा •

IIT Madras

ONLINE DEGREE

How many prime numbers are there?

Madhavan Mukund

https://www.cmi.ac.in/~madhavan

Mathematics for Data Science 1
Week 1

How many primes are there?

- A prime number p has exactly two factors, 1 and p
- The first few prime numbers are $2, 3, 5, 7, \ldots$
- Is the set of prime numbers finite?
- Equivalently, is there a largest prime?
- Euclid proved, around 300 BCE, that there cannot be a largest prime
- Hence there must be infinitely many primes

Euclid of Alexandria

A fact about divisibility

Observation

If $n|(a+b)$ and $n|a$, then $n|b$

- Since $n|(a+b)$, $a+b = u \cdot n$
- Since $n|a$, $a = v \cdot n$
- Therefore $a+b = vn+b = un$
- Hence $b = (u-v)n$

Euclid of Alexandria

There is no largest prime number

- Suppose the list of primes is finite, say $\{p_1, p_2, \dots, p_k\}$
- Consider $n = p_1 \cdot p_2 \cdots p_k + 1$.
- If n is a composite number, at least one prime p_j is a factor, so $p_j | n$.
- Since p_j appears in the product $p_1 \cdot p_2 \cdots p_k$, we have $p_j | p_1 \cdot p_2 \cdots p_k$
- From our observation about divisibility, if $p_j | n$ and $p_j | p_1 \cdot p_2 \cdots p_k$, we must also have $p_j | 1$, which is not possible
- So n must also be a prime, which is clearly bigger than p_k

Euclid of Alexandria

More about primes

- Prime numbers have been extensively studied in mathematics
- Let $\pi(x)$ denote the number of primes smaller than x
- The Prime Number Theorem says that $\pi(x)$ is approximately $\frac{x}{\log(x)}$ for large values of x
- Checking whether a number is a prime can be done efficiently — [Agrawal, Kayal, Saxena 2002]
- No known efficient way to find factors of non-prime numbers
- Large prime numbers are used in modern cryptography
- Essential for electronic commerce