INDIAN INSTITUTE OF TECHNOLOGY MADRAS

सिद्धिर्भवति कर्मजा

IIT Madras

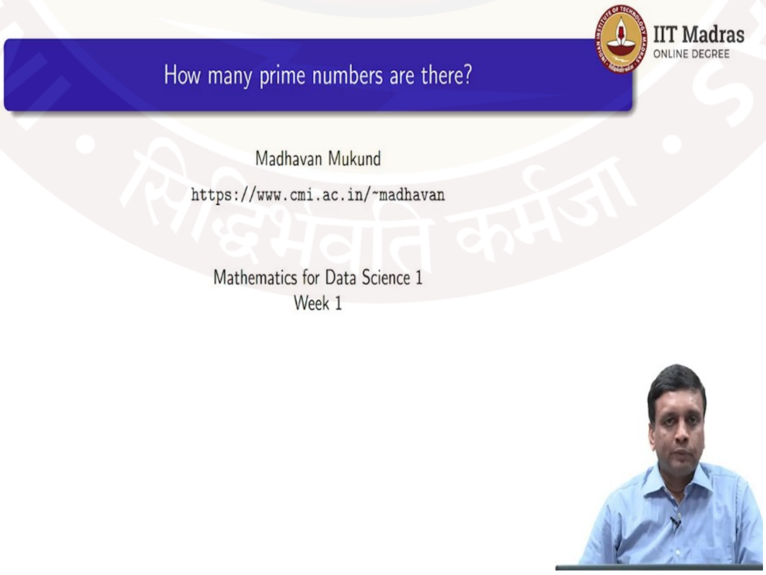
ONLINE DEGREE

Mathematics for Data Science 1
Prof. Madhavan Mukund
Department of Computer Science
Chennai Mathematical Institute

Week - 01
Lecture – 08
Prime Numbers

(Refer Slide Time: 00:06)

(Refer Slide Time: 00:14)



How many prime numbers are there?

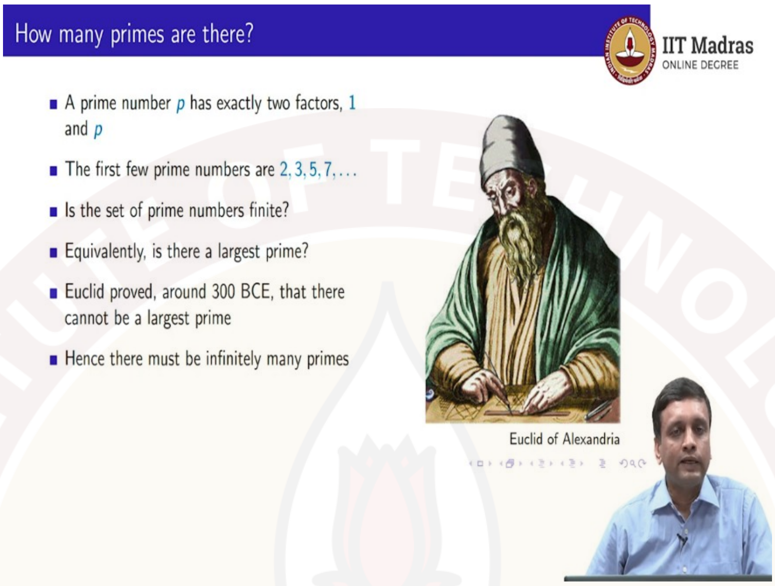
Madhavan Mukund

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

Mathematics for Data Science 1
Week 1

So, when we looked at the natural numbers, we talked about divisibility and we talked about the prime numbers. So, we know that the prime numbers start with 2, 3, 5, 7 and so on. So, how many prime numbers are there?

(Refer Slide Time: 00:25)



How many primes are there?

IIT Madras
ONLINE DEGREE

- 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

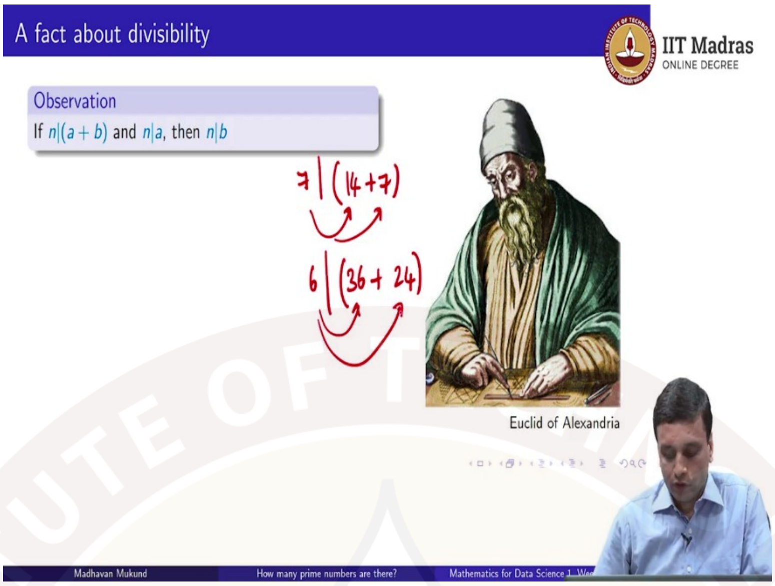
Euclid of Alexandria

So, remember that a prime number is something that has only two factors 1 and itself. Now, it must have exactly two factors. So, 1 is not a prime. So, the first few prime numbers are 2, 3, then 4 is not a prime – because 4 is divisible by 2, then 5, again 6 is not a prime and so on. So, the question is, is this set of numbers these prime numbers is it a finite set or are there infinitely many prime numbers?

Now, if there is a finite set of prime numbers, there will be a largest prime number. So, the same question can be asked by asking is there a largest prime? So, if it is a finite set, in that finite set, there will be a largest one. And if there is a largest one, then below that largest one there are only finitely many numbers, so there can only be finitely many primes. So, asking whether the set of primes is finite is the same as asking whether there is a largest prime.

So, what we are going to see is a version of a proof that goes back to Euclid from about 300 BCE, which shows that there cannot be a largest prime. And as we argued if there is no largest prime, then it must be that the set of primes is actually an infinite set.

(Refer Slide Time: 01:35)



A fact about divisibility

IIT Madras ONLINE DEGREE

Observation

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

$7 | (14+7)$

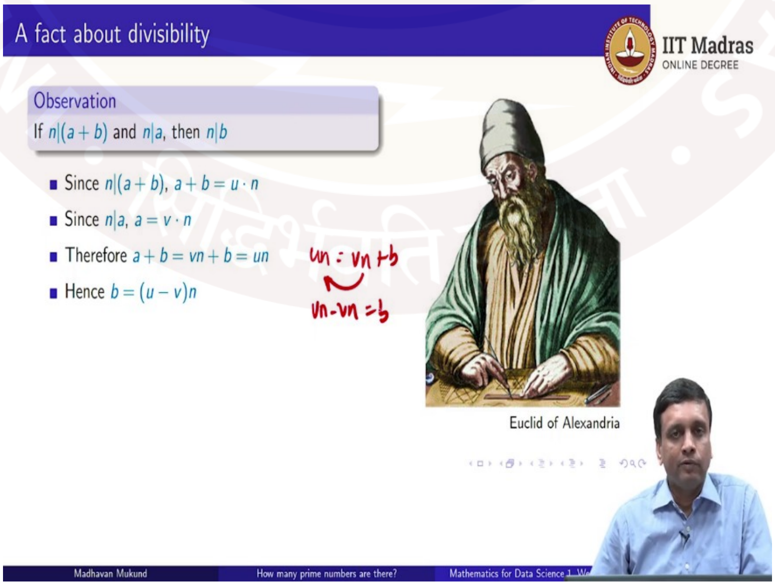
$6 | (36+24)$

Euclid of Alexandria

Madhavan Mukund How many prime numbers are there? Mathematics for Data Science 1, We

So, to go ahead with this we need a basic fact about divisibility. So, this says that if a number divides a+b and it also divides a, then it must divide b. So, let us look at an example. So, supposing you say that 7 divides 21, and I write 21 was 14+7 then 7 also divides 14, and therefore, it also divides 7. Similarly, if I say 6 divides 36+24 which is 60; then since 6 divides 36, it must also divide 24 right. So, this is not very difficult to prove. So, let us prove it just to get a feel of how such proofs go.

(Refer Slide Time: 02:17)



A fact about divisibility

IIT Madras ONLINE DEGREE

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 $b = (u-v)n$

$un = vn + b$

$un - vn = b$

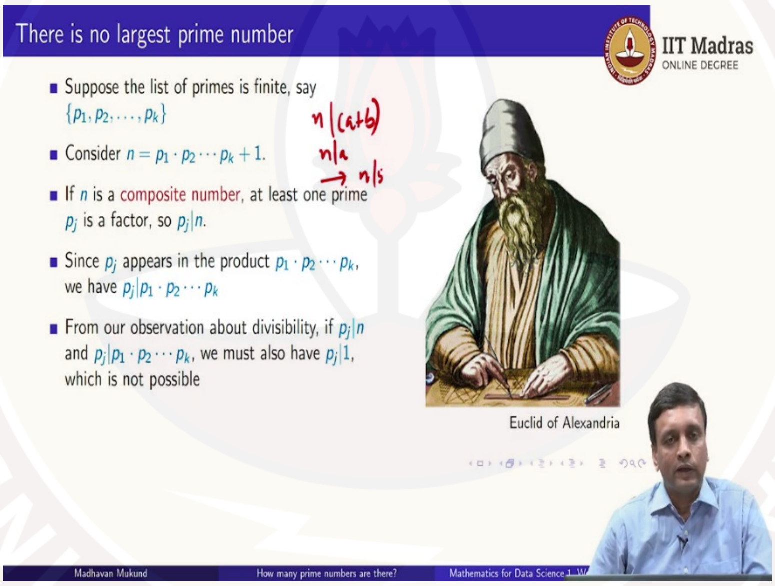
Euclid of Alexandria

Madhavan Mukund How many prime numbers are there? Mathematics for Data Science 1, We

So, since n divides the sum a+b, a+b can be written as a multiple of n. So, let us call it u times n. Similarly, since we have assumed that n divides a, a can also be written as a multiple of n; let us call it v X n. So, what we are told is that any a + b is u X n for some u, a itself is v X n for some v. And the question is b also some multiple of n does n divide b?

Well, because of what we have just discussed a + b can be written as v n + b, because a is v n, and the sum v n + b which is the same as a + b is in fact u n. So, now, we can do some simple rearrangement. So, we can take u n = v n + b, and just take the v n to the other side and we get u n - v n = b and so b is (u – v) times n. So, this simply proves to us that if a number divides a sum and it divides one part of that sum, it also must divide the other part of the sum. And we will use this in order to show Euclid's result.

(Refer Slide Time: 03:21)



There is no largest prime number

- Suppose the list of primes is finite, say $\{p_1, p_2, \ldots, p_k\}$
- 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

$n | (a+b)$

$n | a$

$\rightarrow n | b$

Euclid of Alexandria

IIT Madras
ONLINE DEGREE
Madhavan Mukund
How many prime numbers are there?
Mathematics for Data Science 1, W

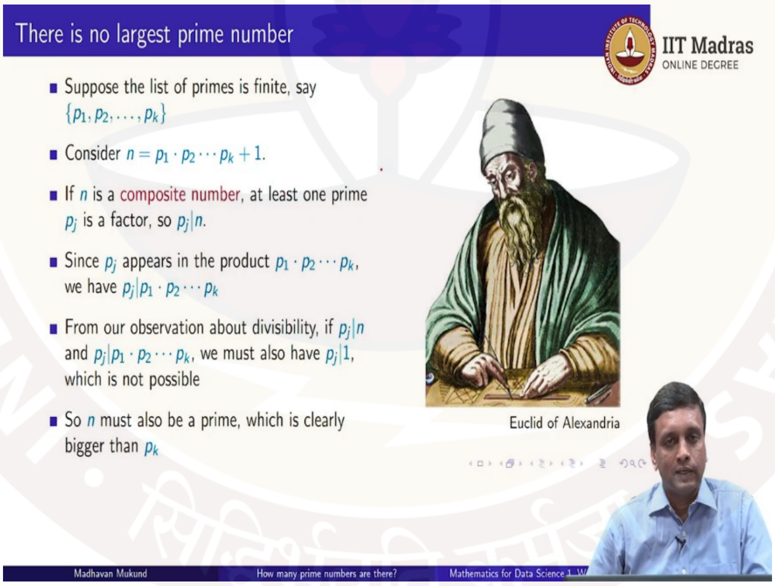
So, what Euclid said is that suppose the list of primes is finite. So, if it is finite, then we can list them out and it is a finite set, so it is some $p_1$to p_k. We do not have to be in any particular order. we can assume that p_1 is the smallest one; it is 2, $p_2$is 3 and so on. But it does not really matter as long as this exhaustively completes all the primes.

Now, we construct a new number which is the product of all these primes, you multiply all these primes by themselves to each other and then we add 1 right. So, n is p_1X p_2X ...X p_k+1. So, now, the question is what is the status of n? So, since we have assumed that the list of primes is finite, n must be a composite number, because this is not one of the primes that we had before right, it is bigger than all of them because it is the product of all of them plus 1.

Now, since it is a composite number it must have a factor other than 1 and itself. And because we have listed out all the primes one of the primes among them must be a factor. So, let us assume that $p_j$is a factor. So, $p_j$divides n right. So, there is one in this $p_1$to p_k, there is a p_j which divides n. But on the other hand, let us look at this part right. The first part the first part is the product of all the prime So, $p_j$appears in that product.

So, if it is one of the factors of the product, it must divide the product right. So, $p_j$divides n, and $p_j$also divides one part of the sum. So, remember what we said that if some number n divides a + b and if some number n divides a also, then n must divide b. So, in this case a+b is the product of the primes plus 1, and a itself is a product of the primes and we have argued that there is one prime p_j which divides both of these. So, therefore, by that divisibility result that we showed in the previous slide $p_j$must divide 1. But of course, we know that $p_j$is a number bigger than 1, it cannot divide 1. And so we have a contradiction right.

(Refer Slide Time: 05:21)



There is no largest prime number

IIT Madras
ONLINE DEGREE

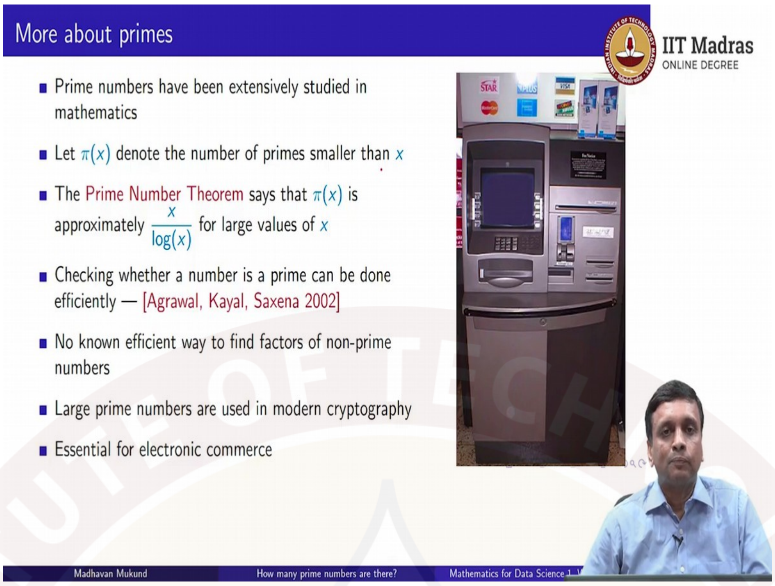
- Suppose the list of primes is finite, say $\{p_1, p_2, \ldots, p_k\}$
- Consider $n = p_1 \cdot p_2 \cdots p_k + 1$.
- If n is a composite number, at least one prime p_j is a factor, so $p_j | n$.
- Since p_j appears in the product $p_1 \cdot p_2 \cdots p_k$, we have $p_j | p_1 \cdot p_2 \cdots p_k$
- 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

Madhavan Mukund How many prime numbers are there? Mathematics for Data Science 1, W

So, what is the contradiction? Well we assume that n was a new number was a composite number because we have exhausted all the primes, but in fact, it cannot be composite because then we cannot find a proper divisor for it among the primes. Therefore, n itself must be a prime. And notice by construction n is actually bigger than all these. So, it also shows that there is no largest prime, because for any set of primes we can always construct a larger prime. So, this is essentially what Euclid did.

(Refer Slide Time: 05:47)



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

IIT Madras
ONLINE DEGREE
Madhavan Mukund
How many prime numbers are there?
Mathematics for Data Science 1

So, we know more about prime numbers. So, prime numbers are very mysterious because their distribution is kind of unclear, but they also have important properties as we will see. So, prime numbers have been extensively studied in mathematics in an area called number theory. So, one of the things that is studied about prime numbers is how they are distributed. So, as we go a larger and larger in the set of natural numbers, how frequently do we find primes?

So, π(x) is supposed to denote the number of primes that is smaller than any given number x. So, for instance, π (4) would be 2, because 2 and 3 are the only 2 primes below 4; π (10) would include 2, 3, 5 and 7. So, π (10) would be 4 and so on.

Now, as you go larger and larger, the gaps between the primes become larger. And in fact, you can prove amazing things like the prime number theorem which says that π(x) is approximately x / log x for large values of x. Now, it does not matter if you do not understand what this means, but it is important to understand that this is a very significant type of argument that you can give about the distribution of a set of numbers which is quite in a way randomly distributed.

Now, in terms of modern applications of primes, it might seem that primes are very strange things, and we would only need to study them a number theory. In fact, the famous mathematician G. H. Hardy once said that he was very proud of the fact that he did number theory and nothing that he studied had any application. Well, it is not quite true because primes as we will see are actually quite useful.

So, one of the questions that you might want to ask is given a number check whether it is a prime. Now, of course, there is a brute force way of doing it which is to try and enumerate all the factors by looking at all the numbers below n and dividing n by them, but that is not considered to be an efficient way to do it. And in fact, this was proved by three Indian computer scientists from IIT Kanpur, Manindra Agrawal, Neeraj Kayal, and Nitin Saxena in 2002, and it is one of the breakthrough results in theoretical computer science in the history of the subject.

So, checking whether a number is prime can be done efficiently. But what about the other question, if I know a number is not a prime, can I factorize it? So, we know number is not a prime, but how do I find two non-prime, two non-trivial factors that is not 1 or itself. Now, it turns out that there is no efficient way to do this. So, this is quite paradoxical. We can check whether a number is prime or not, but if it is not a prime we can factorize it fast. And this in fact is the reason why we are so concerned about prime numbers, because we would like to find numbers which are not prime, but which are actually products of large primes. So, their factors are only large prime numbers, and this is a very important in cryptography.

And cryptography in this sense is something which affects not just you know military secrets, but it affects us in day-to-day life because whenever we do electronic commerce our transactions are protected by cryptography to prevent unauthorized transactions from being executed on our behalf or to prevent them from being tampered with they are all encrypted. And a lot of this encryption is based on the existence of large prime numbers, and the fact that factorizing the product of two large primes is difficult. So, prime numbers though they are very exotic in number theory are actually a very, very important part of our day-to-day life.