A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics,
Indian Institute of Technology, Bombay
Lecture 03
Infinitude of Primes

Welcome back, I hope you remember the definition of a prime number from our last lecture, let us revise it. A prime is a natural number P which has exactly 2 divisors, we saw this definition yesterday in the previous lecture and we also saw several examples of primes, you know in mathematics, definitions and examples are the most important things.

You should never compromise with the definition, the definition should be there in your mind to the T, the full definition has to be there and you should have many examples as well as some at least 2, 3 non-examples. So, we saw that 1 is not a prime because the number of divisors of 1 in the set of natural numbers is 1, 1 does not have any other divisors than itself.

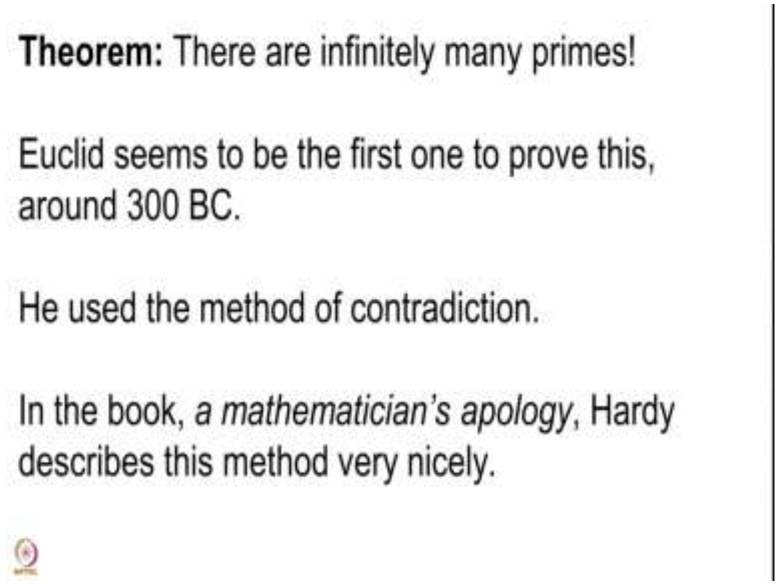
So 1 is not a prime, 2 is a prime, 3 is a prime, 5 is a prime but 4 is not. The reason for 4 not being a prime is that there are now 3 divisors for 4, 1 divides 4, 2 divides 4 and 4 also divides 4 and then we continue, we actually also saw that we could list all primes up to 100 that was a good set it had 25 elements, many primes.

But if you go from 100 to 1000 the number of primes actually went down by a bit, it was not quite multiplied by 10, but we got 168 primes up to 1000, after that we went up to 10000 and we saw that there were 1229 primes.

So, the rate of getting primes is decreasing a bit, but still we are getting more primes and the question that we asked after that was whether we can just go on and on? And I also told you that yes, we can. Meaning there are infinitely many primes. So, now this statement which is one of the most important statements in the study of primes has to be proved.

A statement needs a proof, as it would happen for any basic theorem in any area most importantly number theory there are many proofs, this theorem about infinitude of primes is proofed in any different ways by many people. We will see the very first proof, this is by Euclid.

(Refer Slide Time: 03:23)



Theorem: There are infinitely many primes!

Euclid seems to be the first one to prove this, around 300 BC.

He used the method of contradiction.

In the book, *a mathematician's apology*, Hardy describes this method very nicely.

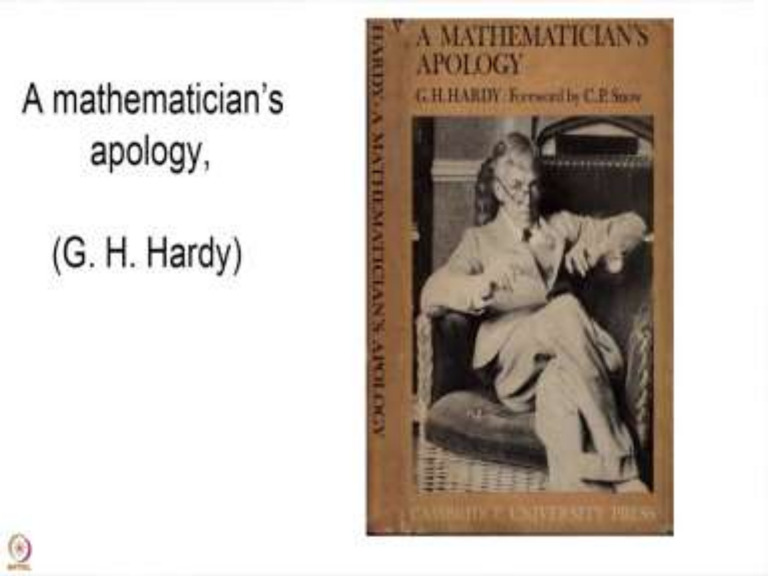
So, the theorem says that there are infinitely many primes and Euclid is the one who was the first one, he seems to be the first one to prove this around 300 BC so more than 2300 years back. The proof that Euclid uses to prove this theorem is by a method of, the method of contradiction. What is the method of contradiction?

The method of contradiction starts by assuming that you do not have what you are claiming to have. So, in this case, we would start with the assumption that we have only finitely many primes, we know that up to 10000 there are 1229 primes, so we know that at least 2029 primes are there, but suppose there is some number capital N such that we have only N many primes. Then we would deduce some statements logically from this statement and arrive at a contradiction.

Therefore if you start with some assumption and reach by logical conclusions to a contradiction that would mean that the first statement that you had assumed has to be wrong, this is the method of contradiction. I should also tell you that there is this book by the great mathematician G.H. Hardy, Hardy is the one who introduced Ramanujan to the world, he is the one of the very few mathematicians who encouraged Ramanujan in the very beginning and showed what a true talent he was.

So, in his book, which is called a Mathematician Apology, he describes this method very nicely, he gives the analogy of a chess game. Sometimes to win a chess game or to checkmate the opponent's king, we may sacrifice upon, sometimes a bishop or sometimes even a queen, then Hardy says that mathematician surrenders the whole game, the mathematician sacrifices the whole game, he says that okay, let us assume that what I am saying is not true and then we deduce some statements logically. This is how he describes the method of contradiction.

(Refer Slide Time: 06:02)



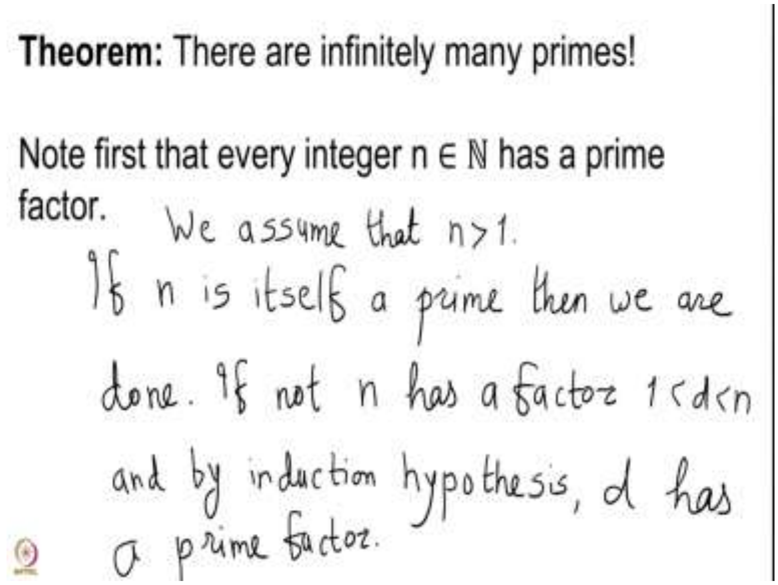
A mathematician's apology,

(G. H. Hardy)

HARDY · A MATHEMATICIAN'S APOLOGY
A MATHEMATICIAN'S APOLOGY
G. H. HARDY · Foreword by C. P. Snow
CAMBRIDGE UNIVERSITY PRESS

I will show you the cover of a book, the A mathematician’s Apology, by G. H. Hardy, it is an interesting read and I would really suggest many of you in fact all of you to do give it a chance read this book, it will be a very interesting reading. Alright, so we now go towards proving that there are infinitely many primes, so we will give a proof of this theorem.

(Refer Slide Time: 06:41)

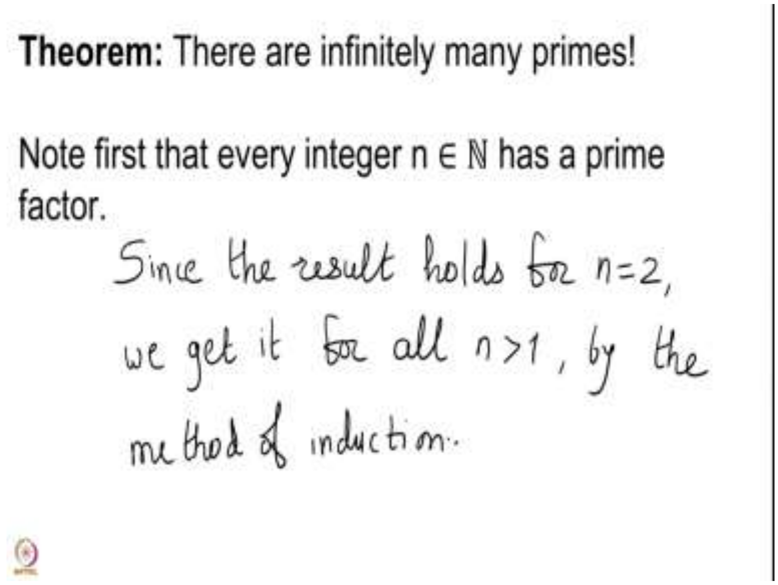


Theorem: There are infinitely many primes!

Note first that every integer n ∈ ℕ has a prime factor.

We assume that $n>1$.

If n is itself a prime then we are done. If not n has a factor $1<d<n$ and by induction hypothesis, d has a prime factor.



Theorem: There are infinitely many primes!

Note first that every integer n ∈ ℕ has a prime factor.

Since the result holds for $n=2$, we get it for all $n>1$, by the method of induction.

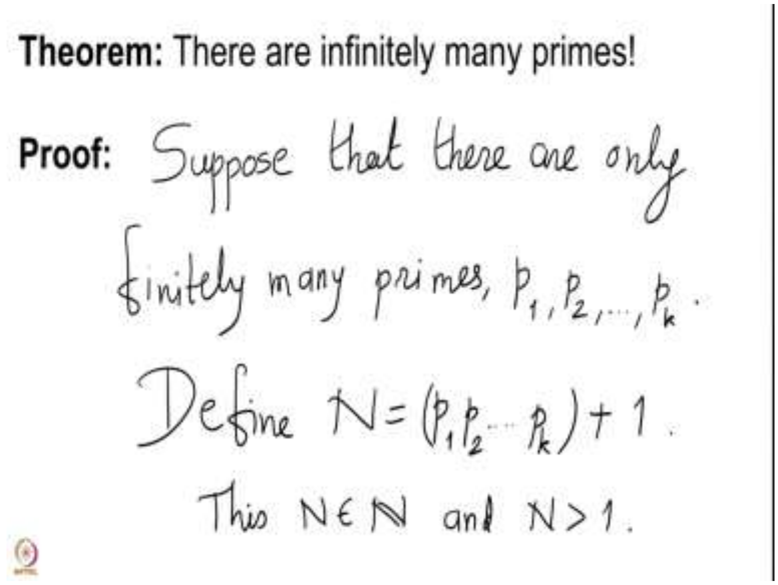
However, before giving the main proof we will have to note that every integer n has a prime factor. So, how do we prove this that every integer n has a prime factor? Let us, see. If n is itself a prime then we are done. We wanted to show that every integer n has a prime factor, if your n is a prime then we are done. If not n has a factor 1 less than d less than n.

So, what I am saying here is that this d which is not equal to 1 and not equal to n is a factor of n, this is because n is not a prime, so it should have at least one more factor. We will, ofcourse we assume that n is bigger than 1, this is an assumption that we will have. So, with this assumption if your n is not a prime it should have 3 or more factors.

So we start with d being this factor and by induction hypothesis d has a prime factor. What is the induction hypothesis? Induction hypothesis is assuming that the statement holds for everything smaller than n and then we deduce the statement for n. But induction hypothesis needs to be proved for the beginning stage, the beginning stage here for n bigger than 1 would be for n equal to 2.

Since the results holds for n equal to 2 we get it for all n bigger than 1 by the method of induction. Okay so we will assume, we want to prove that there are infinitely many primes and what we have noted already is that if you take any n bigger than 1 then there is at least 1 prime factor, alright we all agree on this. Let us, now go on and prove that there are indeed infinitely many primes. So, I want to prove this and the (condt) we assume that this is not true.

(Refer Slide Time: 10:28)

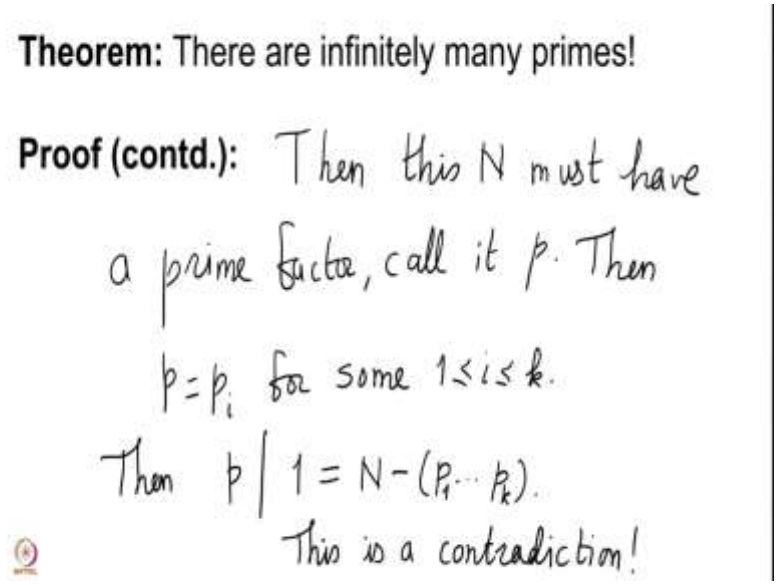


Theorem: There are infinitely many primes!

Proof: Suppose that there are only finitely many primes, $p_1, p_2, \ldots, p_k$.

Define $N = (p_1 p_2 \cdots p_k) + 1$.

This $N \in \mathbb{N}$ and $N > 1$.



Theorem: There are infinitely many primes!

Proof (contd.): Then this N must have a prime factor, call it p. Then

$p = p_i$ for some $1 \leq i \leq k$.

Then $p \mid 1 = N - (p_1 \cdots p_k)$.

This is a contradiction!

So, suppose that there are only finitely many primes, so we assume that the result that we want to prove is not true. So, suppose there are only finitely many prime, so we can write them, so we assume that there are only k primes, k can be a very big number does not matter, but there are still only finitely many primes, that is our assumption. Define capital N equal to p1, p2 up to pk plus 1.

So, we have defined a new natural number. Remember product of natural numbers is again a natural number, once you add 1 to it you get yet another natural number, so this N belongs to our set of natural numbers and we have that N is bigger than 1. Now, what did we see just now? We saw that any natural number which is bigger than 1 has to have a prime factor.

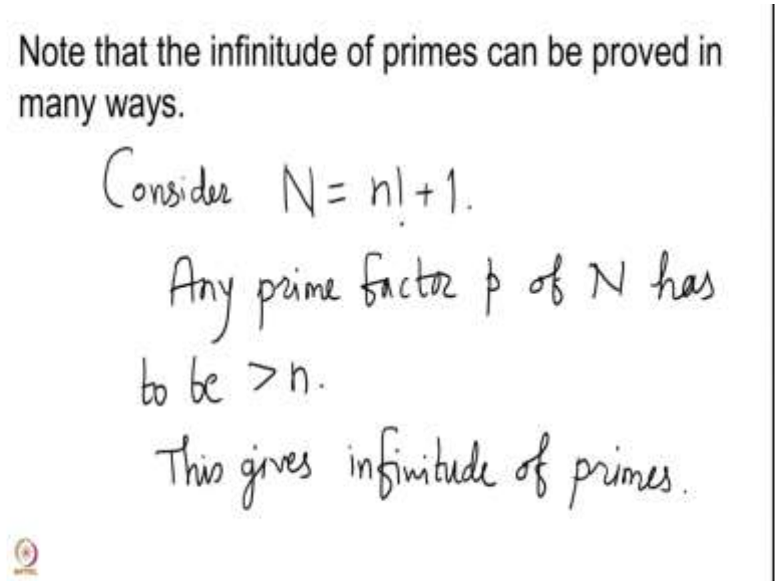
Then this N must have a prime factor, call it p. We have already assumed that there are only k primes p1, p2, p3 up to pk and now here we have a prime since we had assumed that only k many primes are there and we labelled them as p1, p2, p3 up to pk, so this p has to be one of them, because those are the only primes that we have heard so far, that is our assumption. Then p equals pi for some i from 1 to k.

But what was our definition of N? N was product of pi's, so our p which is some pi divides that product and it also divides n so it should divide 1, you have a prime and that divides 1 that is a contradiction because then it gives you that p has to be less than or equal to 1, you have a natural number which is less than or equal to 1 it should be 1 but 1 is not a prime, so this is a contradiction. Once you reach contradiction, the result is proved.

So, what we have done is that we started by assuming that there are only finitely many primes say p1, p2, p3 all the way up to pk and after that we constructed a number capital N which is product of all these primes, this is where we have used the finiteness. If you have finitely many numbers, you can take the product of them and you will still have a natural number, you cannot take product of infinite many natural numbers and hope to get a natural number.

So, once you have capital N which is p1, p2, pk plus 1, now such an N should have a prime factor call it p, this p has to be one of the pi that you had initially labelled, then this p must divide 1 which is the difference of N and product pi. And p dividing 1, p being a prime gives you a contradiction. So, this is the way we prove the theorem of infinitude of primes. This theorem says that there are infinitely many prime elements.

(Refer Slide Time: 15:55)



Note that the infinitude of primes can be proved in many ways.

Consider $N = n! + 1$.

Any prime factor p of N has to be $> n$.

This gives infinitude of primes.

Note that the infinitude of primes can be proved in many ways. I told you that this is one very basic theorem and such an interesting theorem basic theorem should have in my opinion many interesting ways to prove. So this theorem also has some other ways to prove. So, let me quickly talk about another such proof.

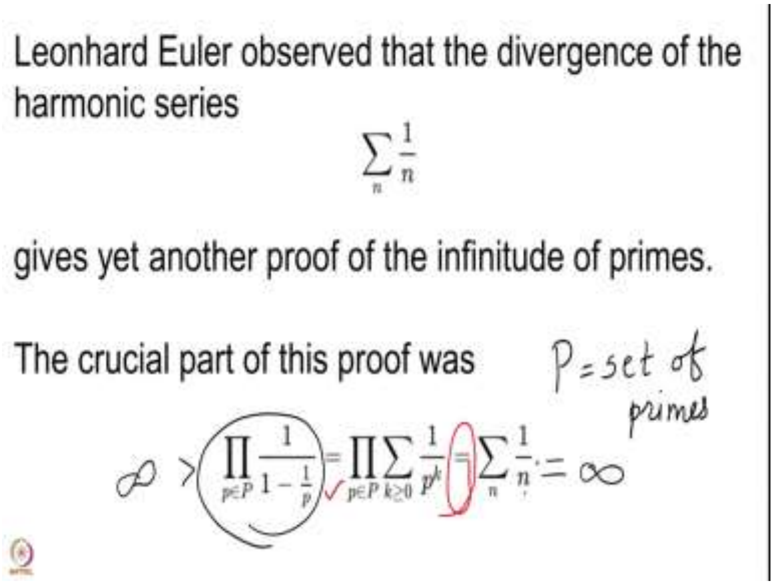
So, consider capital N to be n factorial plus 1, what is n factorial? N factorial is the product of 2, 3, 4, 5, 6, 7 all the way up to n, it is the product of all natural numbers up to and including N. So, 2 factorial will be 2, 3 factorial will be 6, because it is 2 into 3 into 1, but we will not mention 1. 4 factorial is 24, 2 into 3 which is 6 into 4 you get 24. 5 factorial is 120. 6 factorial is 720 and so on. So, we can compute these n factorials add 1.

Now, any prime factor of n has to be bigger than n, any prime factor of capital N we know that capital N should have a prime factor, capital N is a natural number and it is bigger than 1, so it should have a prime factor. But this prime factor cannot divide n, it will not divide the n factorial for the small n, because otherwise it would then divide 1.

So the prime factor p which is the prime factor of capital N cannot divide n factorial therefore it cannot be less than or equal to n. If it was less than or equal to n it would figure in those products that you obtain that you have to obtain n factorial. So this p has to be bigger than n and you can do this for every n, for every n you have capital N the corresponding capital N which is n factorial plus 1 and then it gives you a prime factor of this number which is bigger than n.

Since for every natural number you have a prime bigger than that natural number there has to be infinitely many primes. So, this gives infinitude of primes. There are many other proofs, there is a proof using topology, if you search on Wikipedia for proof of infinitude of primes using topology, then you will find that proof, I am going to do I am just going to mention one more interesting proof. So, this was by Euler the greatest mathematician one of the greatest mathematician Leonhard Euler.

(Refer Slide Time: 19:31)



Leonhard Euler observed that the divergence of the harmonic series

$$\sum_n \frac{1}{n}$$

gives yet another proof of the infinitude of primes.

The crucial part of this proof was

P = set of primes

$$\infty > \prod_{p\in P}\frac{1}{1-\frac{1}{p}} \overset{\checkmark}{=} \prod_{p\in P}\sum_{k\geq 0}\frac{1}{p^k} = \sum_n \frac{1}{n} = \infty$$

He observed that the divergence of the harmonic series, what is the harmonic series? Harmonic series is the series summation 1 upon n where n goes from 1 to Infinity, one knows that this series diverges, this is a proof in analysis, which we use right now. Euler observed that the divergence of this series gives one more proof of the infinitude of primes. So, he used one equality which is a very crucial part of his proof, this crucial part was to observe this equality.

Now note what we have here is the following thing. We have summation, we have product 1 upon 1 minus 1 upon p capital P belongs to small p belongs to capital P, so here capital P is the set of primes. And if on this side if you had only finitely many primes to play with, if the capital P was a finite set then this quantity would be finite.

You have only finitely many primes, so 1 minus 1 upon p is some number you take its reciprocal and you still get some real quantity real number, but you are taking a product of only finitely many quantities. So, this number has to be finite, but we get that this on the other hand is infinite, this is the contradiction you have on one hand some quantity which is finite but on the other hand this is an infinite quantity.

However, in this crucial part we are using this equality, how do we get this equality? The equality says, this equality is okay, because we are using the geometric series expansion for 1 upon 1 minus 1 by P, that geometric expansion would give you this geometric series, but to go from here to summation n, 1 by n this uses the fundamental theorem of arithmetic which says that given any natural number n bigger than 1 you can write n as product of primes in exactly one way.

The uniqueness is only up to the order of the factors that you may write. So, this proof will require more concepts to be developed, but we will develop those concepts and also prove the fundamental theorem, of arithmetic in the next lecture. Thank you.