A Basic Course In Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 07
Stories around primes

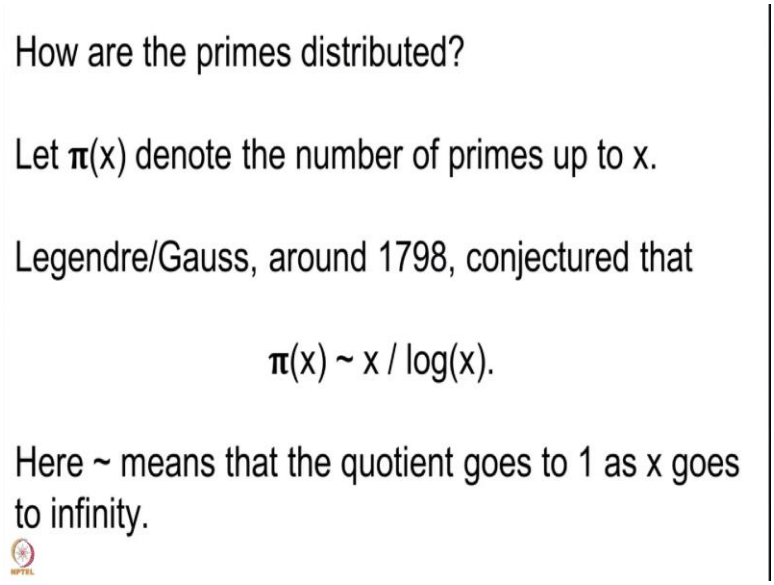
Welcome back it is great to see you back. We proved the fundamental theorem of arithmetic in our last lecture, which said that if you take any natural number n bigger than 1, then it can be written as a product of primes in a unique way. If you are agreeing with me to write the primes in the increasing order. And then when you have the same prime appearing many times you just combine the whole bunch of those same primes and put a power to the head of the prime.

So the decomposition is n equal to p1 power n1 p2 power n2 dot dot dot p k power nk where p1 is less than p2 which is less than p3 dot dot dot less than pk and ni are natural numbers. So this is a very unique decomposition and which says that primes work like atoms if you are looking at naturals numbers. The concept of primes actually goes beyond the realm of natural numbers and this is the study of what is called algebraic number theory.

But, we will restrict ourselves with the notion of natural numbers and so we will be looking at only the natural primes the primes that we all know. And one question would be how are these primes distributed in the set of natural numbers? We know already that the number of primes is infinite so it is not a finite set the set of primes is infinite. So you have a prime after any given natural number.

On the other hand, as I told you there are sets of any given length which do not contain primes. So you can actually construct sequences of consecutive integers of any length you want, such that there is not even a single prime in that sequence of integers natural numbers. On the other hand I have been talking about this twin prime conjecture which says that there are infinitely many primes such that the very next odd number is also a prime.

(Refer Slide Time: 02:37)



So the question is how are primes distributed and this has this is the question which has been troubling which has been bothering mathematicians since quite some time. Two major mathematicians two well-known mathematician by name Legendre and Gauss they studied this question in the 8 in the 19th century. So to explain this let me build a small notation for any real number x positive I will denote by pi x the number of primes up to x. So pi of 2 will be 1 because there is 1 prime up to 2 which is 2 itself.

Pi of 3.5 will be 2 pi of 4 will be 2 pi of 4.5 will be 2 pi of 5.1 will be 3, because now you have 2, 3 and 5 three primes up to 5.1. Pi of 1.5 will be 0 because there is no prime up to 1.5. So this is a function it is set function if you draw the graph of this function, the question is how do we understand this function pi x? So this is a very irregular function because it is step function it will be constant for a length.

And then, it will suddenly jump to 1 high or high level up then again it will be constant for sometime then it will jump and so on. So, in number theory what one does is that one averages the function what we would do is that you would pi x by x which is some sort of average. And try to understand the function pi x upon x. Now understanding is that you know function x quite well and if also known pi x upon x then you will know the function pi x that is the hope.

So, this is how one starts thinking about it and as I told these mathematician Legendre and Gauss in 1798 the end of 18th century that is when they thought about it independently. And both of

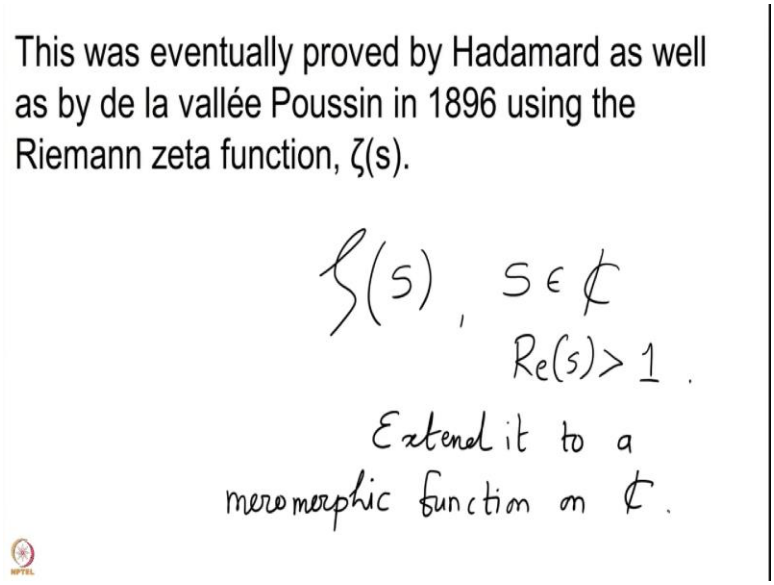
them conjectured a formula, what was the formula? They both conjectured that pi x is equivalent to x upon log x. Here this equivalence means that the quotient of these two functions goes to 1 and x goes to infinity. So we will divide pi x by x upon log x and then we say that this quotient goes to 1 as x goes to infinity.

Which is the same of looking at pi x upon x and dividing that by 1 upon log x that quotient goes to 1. So we want to understand the function pi x and we would do it by understanding pi x upon x the averaging function. And this averaging function as x goes to infinity behaves like 1 upon log x. So these two functions are what are asymptotic to each other. We learn about asymptotes vertical asymptotes, horizontal asymptotes, slanted asymptotes there the asymptotic function is taken to be a straight line.

So it is a linear function but we here allow the other to be any other function just that we hope that the function be well understood. So here pi x upon x is asymptotic to 1 upon log x or which is the same thing as saying that pi x is asymptotic to x by log x. So this was still a conjecture this it was not proved neither by Legendre nor by Gauss and meaning this result is very peculiar in the sense that every time there is something new happens to the result, there are always two people working independently about it.

So here we have Legendre and Gauss working independently and getting the result getting the conjecture that pi x is equivalent to or asymptotic to x upon log x. It took 50 years to prove this result.

(Refer Slide Time: 07:18)



This was eventually proved by Hadamard as well as by de la vallée Poussin in 1896 using the Riemann zeta function, ζ(s).

It is known as the Prime Number Theorem.

In 1948, Selberg as well as Erdős proved it without using any complex analysis.

Which was proved by Hadamard and de la vallee Poussin this was proved in 1896. No, it took more than 50 years it about hundred years 1798 was the time when it was conjectured and 1896 hundred years later. This was proved and the proof used this function called Riemann zeta function Riemann had introduced this function this zeta is a Greek symbol, which is written like this.

So here you have S to be complex number and normally what we assume is that real part of S is bigger than 1. This is when the function has very nice properties but of course we would like to extend it to the whole complex plain to which is called a meromorphic function on C. And there

is this famous line real part of it is equal to 1 by 2 which where we are suppose to have lots of non-trivial zeros. And in fact, all the so called non-trivial zero they are suppose to lie only on this line. This is the part of the famous Riemann hypothesis but anyway. So this function zeta S was used to prove the result conjectured by Legendre and Gauss hundred years back.

And then, once the result is proved and then quote the results several times how do quote it? Do you called Hadamard do you call it Hadamard's result or de la vallee Poussion theorem or Legendre conjecture or Gauss conjecture, how do you call it? Since there well where several people involved in it mathematicians simply decide to call it Prime Number Theorem. So this result later came to be known as the Prime Number Theorem. So this was proved in 1896 and in the early part of the 19th century Hardy and others these were the prominent mathematicians both in number theory and as well as analysis.

So they started wondering so you know a philosophy of mathematics was also being developed then. And so people started comparing different proofs as per there difficulty level. And the prime number theorem because it used complex analysis which is supposed to be a higher level. So you have the theory you have the system of natural numbers which is the set of integers. This is contained in the real numbers which will give you real analysis. This is further contained in complex numbers giving you complex analysis.

So if there was a result which can prove using only integers, then one would say that such a result is elementary compare to a result which uses real analysis or calculus. And, a result which uses real analysis will be called elementary compared to the result which uses complex analysis. And something which uses properties of the Riemann zeta function which is a very difficult function actually defined only on the upper half plain on the right half plain. Then one would say that this problem is very difficult.

So, Hardy and others were wondering where whether there can be an elementary prof of the prime number theorem. And people had different opinions and they were all stunned saying 50 years after the result was first proved in 1948 when Selberg and Erdos gave an elementary prove. Elementary prove means that it did not use complex analysis it did not uses any contour integration or ((11:29)) formula or any such thing. However, the prove is quite intricate it is quite involved and there is a small story involved here which proves that mathematicians are also humans.

And you will notice that again there are two people so the result was conjectured by two people Legendre and Gauss in 1798 it was proved first by Hadamard and de la vallee Poussin in 1896 independently. And again, Selberg and Erdos in some sense there work was also independent they proved it without using any complex analysis. So Selberg was working Erdos is a mathematician Erdos was a mathematician who worked on a Platero of problems he worked on several problems. He was a problem solver whereas Selberg was the person who was a developer of a theory.

He would really think about a concept and develop the whole theory. Erdos would try to prove problems would try to solve problems and the movement there was any new tool which was made available to him he had the knack of solving it. Solving new problems with solving problems with the help of the new tools, which were made available to him. So the story goes as follows that in 1946 or 1947 Selberg proved one very fundamental asymptotic equality which is really an inequality.

And he proved this inequality he was at university of Princeton that time and he had to travel to Mountrail for few days and before going he told one of his assistance, assistance meaning a person who has completed his PhD but was visiting Princeton University for a while. He told this assistance about the inequality or the asymptotic equality and then he went to Montreal. Meanwhile Erdos arrived in Princeton and he got to know about the inequality from this assistance whose name was Turan by the way. So Turan and Erdos knew each other from Hungary days and the movement Erdos heard about this he thought let me use to it prove Prime Number Theorem.

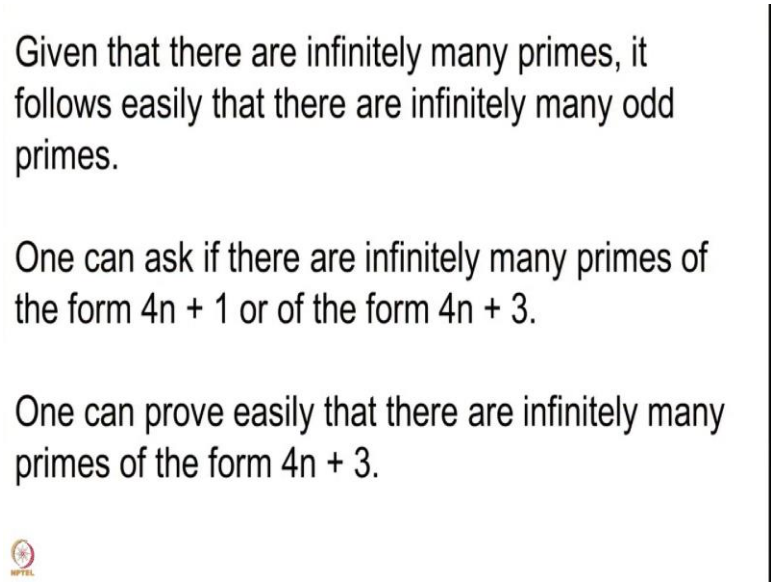
When Selbreg returned from Montreal to Princeton Erdos told him that he thinks prime number theorem can be proved with the help of the fundamental inequality that Selberg had proved. But Selberg said I proved the inequality because I wanted to prove Prime Number Theorem. Meaning it would not be fair if somebody else did it with his inequality he had the very much aim he was going to prove prime number theorem using the inequality. However, Erdos had almost completed his proof of the Prime Number Theorem by then and so it turned out that Selberg heard Erdos's proof.

He observed that there could be some more improvements that could be done. And finally, Selberg understood that he can proof Prime Number Theorem without using any of results of the

Erdos any of the result's that Erdos had proved. Finally, it was settled in some sense by Selberg agreeing to lead Erdos prove his proof first and then Selberg will prove his proof. But mathematical community was mostly on Selberg side there were some mathematician on Erdos side also. However, it is always called Selberg Erdos proof of the Prime Number Theorem.

So this is the interesting story about the prime number theorem which says that pi x the function which calculates primes up to x behave like x by log x when you go to infinity in the sense that the quotient becomes 1. There are more functions which were developed which were suppose to have given you a better asymptotic result. But we will not go into all that we will go to a another problem regarding primes once again.

(Refer Slide Time: 15:42)



Now, that we have established that there are infinitely many primes out there one would ask how many of them are even and how many of them are odd?

So we know that there is only one even prime the oddest of them that prime is 2. And, once you take 2 all its multiples which are the even numbers cannot be primes because 2 divides them. So all other primes have to be odd. So because we have infinitely many primes it follows very easily that there are infinitely many odd primes. So odd numbers which are of the form 2 n plus 1 contain infinitely many primes in fact they contain almost all primes except the prime 2.

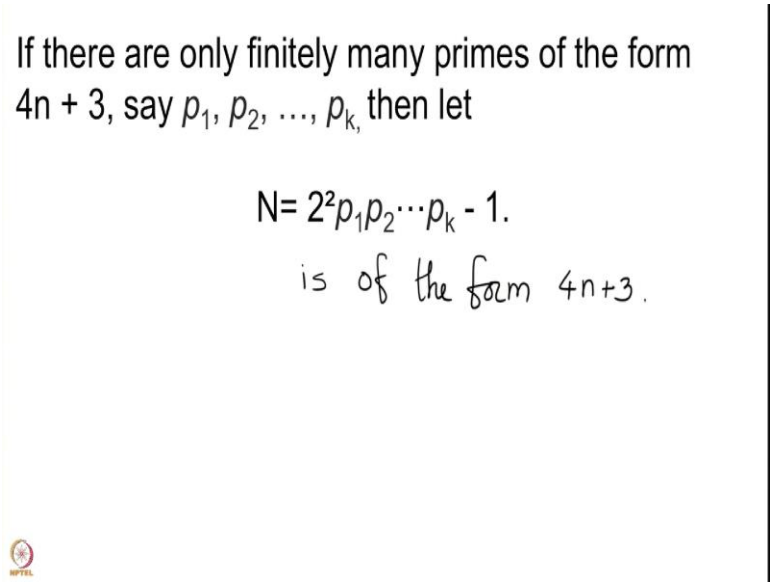
Then you can ask further. Every odd number can be written as 4 n plus 1 and 4 n plus 3. So the infinitely many primes which are in the odd numbers where do they go and sit? Do these go and

sit in the 4 n plus 1 or do these go and sit in the 4 n plus 3? You may imagine that there are two lines one is of the type 4 n plus 1 other is of the type 4 n plus 3 and the moment you observe a new prime you check whether it is of the form 4 n plus 1 or 4 n plus 3 and write it in the corresponding line.

Which line grows faster? That is the question, but do we at least have that there are infinitely many primes in each line? That is the question first, we should ask. Are there infinitely many primes of the form 4 n plus 1 or are there infinitely many primes of the form 4 n plus 3? And we would like to have a proof of this result which ever went is. Mathematicians are not unhappy about the result which is proved they just want to have a proof about it.

So we will first prove that there are infinitely many primes of the form 4 n plus 3 let us see how the prove goes. One can prove easily that there are infinitely many primes of the form 4 n plus 3. The proof will follow on the same line we will assume that there are only finitely many. Construct a number which should have a prime of the form 4 n plus 3 dividing it and this prime cannot be part of this set of primes that you have already considered and thus you have a new prime this is the idea of the proof. How do we do it?

(Refer Slide Time: 18:46)



If there are only finitely many primes of the form $4n + 3$, say $p_1, p_2, \ldots, p_k$, then let

$$N = 2^2 p_1 p_2 \cdots p_k - 1.$$

Since N is odd, all its prime factors are odd and all its prime factors can not be of the form $4n + 1$.

Hence it has a prime factor of the form $4n + 3$.

If there are only finitely many primes of the form 4 n plus 3. Let us write them p1, p2, p3 up to pk these are those primes. Now, we construct a new number from these primes. When we worked with Euclid's proof we had constructed a new number simply by taking the product and adding 1. Here we do a similar construction, the construction is take the product of these primes multiply to it by 4 and then subtract 1.

So what did we do? We constructed a new number capital N which is of the form 4 times p1 times p2 times dot dot dot up to pk and we subtracted 1 from this. So we have that our N is of the form 4 times a number minus 1 or which is of the form 4 times n plus 3 for some N. So we multiplied the primes that we had p1, p2, pk by 4 and subtracted 1. And now this number is of the form 4 n plus 3 but more importantly it is an odd integer so all its prime factors will be odd.

Since n is odd all of its prime factors are odd, 2 cannot be a prime factor here. Now since the prime factors are odd the prime factors can be of the form 4 n plus 1 or they can be of the form 4 n minus 1 or 4 n plus 3. Can all the prime factors all the prime factors of this capital N be of the form 4 n plus 1? No, they cannot be. All of them cannot be of the form 4 n plus 1 for the following reason. If you take any two numbers of the form 4 n plus 1 say 4 a plus 1 into 4 b plus 1.

The product will be of the form 4 c plus 1 because 4 a plus 1 into 4 b plus 1 will give you 16 ab plus 4 a plus 4 b plus 1. So there is a multiple of 4 and you have plus 1. So if you take any elements any number of integers of the form 4 n plus 1 and take their product, the product is

again going to be of the form 4 n plus 1. Whereas our number n that we constructed here is of the form 4 n minus 1 or 4 n plus 3.

Therefore all its prime factors cannot be of the form 4 n plus 1, so it should have one more odd prime factor and that has to be of the form 4 n plus 3. So this way we get one more prime factor of this number which is of the form 4 n plus 3 and this new prime factor cannot be equal to p1, p2, pk any of these because if it was any of the p1, p2, pk it would divide the product 2 square into p1, p2, pk it also divides n and then it will also divide 1 because 1 is obtained as 2 square p1, p2, pk minus n.

So we have a new prime of the form 4 n plus 3, if you add this call this as pk plus 1 I will repeat the process and get yet another prime of the from 4 n plus 3 and so on. So this contradicts that the assumption that there were only finitely many primes of the form 4 n plus 3. Therefore, there have to be infinitely many primes of the form 4 n plus 3. This completes the proof.

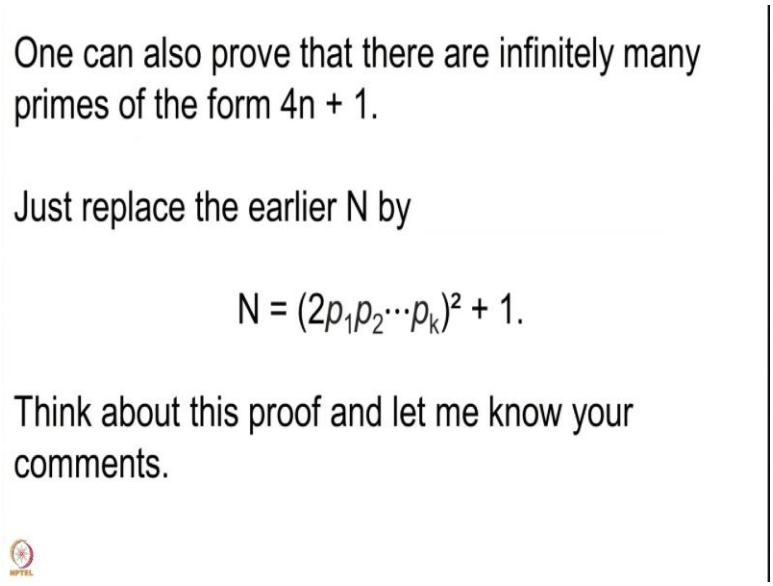
Now, that we have proved that there are infinitely many primes of the form 4 n plus 3, what about the primes which are of the form 4 n plus 1? You see we began by achieving that there are infinitely many primes would there, out of them two is a singleton even prime. So all the remaining primes which is really an infinite set has to go and sit in the odd numbers. And among odd numbers we have now found that 4 n plus 3 type of primes are infinitely many, what about 4 n plus 1 then?

Are there only infinitely many such primes of the form 4 n plus 1? Or are there infinitely many such primes? So we have to just check can you get five such primes of the form 4 n plus 3, 4 n plus 1? 4n plus 1 remember 4 n plus 3 are infinitely many, we are now wondering what about 4 n plus 1. So we have to take multiples of 4 and add 1, so 5 that is the first one that should come to your mind 4 plus 1.

4 into 2 is 8, 8 plus 1 is 9 which is not a prime. 4 into 3 is 12 plus 1 is 13 that is again a prime. So we got two primes of the form 4 n plus 1, 5 and 13. Third one is 17 which is 4 into 4 plus 1, so 5, 13, 17 after that the next one we get is all the way 29 because 21 and 25 are not primes of the form 4 n plus 1. So 29, 3 we got 5 we got 13 we got 17 and 29 and after 29 the next one we get is 37. So there are five primes of the form 4 n plus 1.

Given if you ask me to list out hundred such primes I may be able to do it given sufficient amount of time. If you ask me to do write thousand such primes I may again be able to do it given sufficient amount of time. But that does not prove that there are infinitely many primes of the form 4 n plus 1. So we have to give a proof to show that there are 4 n plus 1 type primes and that set is also infinite.

(Refer Slide Time: 25:47)



We give a similar proof to what we have done now except that we have to construct the number capital N in a slightly different way. One can also prove that there are infinitely many primes of the form 4 n plus 1 what we do is replace the earlier N by this new N which is 2 p1, p2, pk whole square plus 1. In the proof for 4 n plus 3 we had 4 into p1, p2, pk minus 1, now we have N to be 2 into p1, p2, pk square plus 1.

So it is a square plus 1, it is an odd number still but it is a square of an even quantity plus 1. This should have a prime factor which is odd it cannot be among the p1, p2, pk which are your earlier assumed finitely many primes of the form 4 n plus 1. The only thing you should prove is that any odd factor any factor of capital N has to be of the form 4 n plus 1. So think about this proof and let me know what you think about it, let me know your comments.

We will stop here now, I hope to see you in the next lecture. Thank you very much.