

Riemann Hypothesis and its Application
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture – 23

That one thing I want to do, another thing I wanted to do was very quickly give you overview of the last theorem see that course via this modular forms and modular forms essentially come out of zeta forms. Once you keep generalizing these properties of zeta function, you essentially end up with modular forms and their connection with firstly elliptic curves and then secondly last theorem. So let us see how much I can cover. So, today we will start with our first step towards the generalizing whatever we have done.

(Refer Slide Time: 01:31)

Dirichlet's Theorem

Theorem: Let $a, q \in \mathbb{N}$ and $(a, q) = 1$.

Let $\psi(x, a, q) = \sum_{\substack{\text{prime } p \leq x \\ p \equiv a \pmod{q}}} \Lambda(p)$.

Then, $\psi(x, a, q) = \frac{1}{\phi(q)} x (1 + o(1))$.

That would be for Dirichlet's theorem this state's equal what would you expect. So, a and q are two numbers which are relatively prime to each other and define $\psi(x, a, q)$ as the number of not quite number. But sum over all primes p less than equal to x such that p equals a modular q.

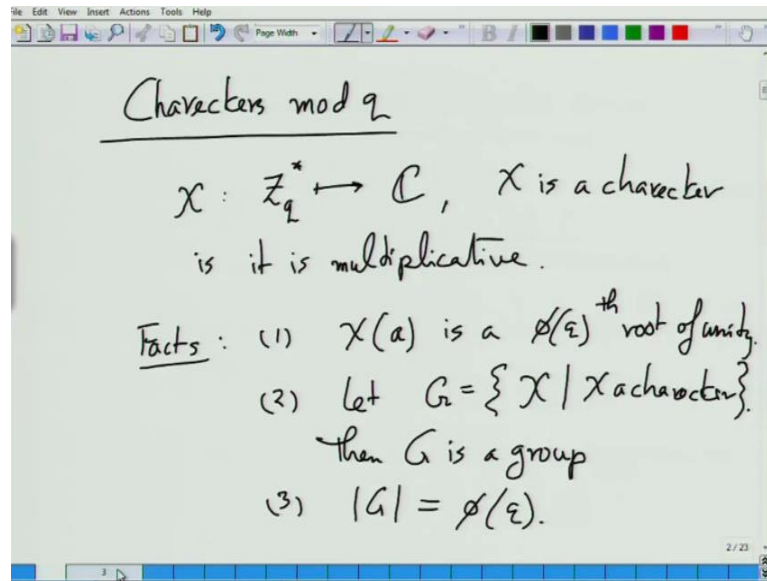
If you are now not counting all the primes you are only counting primes which are a modular q and less than equal to x and summing over the weight we sum with. So, what would you expect this quantity to be see now all the primes less than equal to x fall into different conjugacy classes with respect to q, how many such conjugacy classes are

there? It must be relatively prime to q , so if q is prime, then $q - 1$, but if q is not prime, then certainly not $q - 1$ it is ϕ of q . So, that many conjugacy classes, so if everything all the primes fall roughly equally in all of those. Then, you expect this to be the leading term of ψ to be divided by ϕ of q because now you falling in different these many different classes.

Dirichlet's theorem says that is basically what you get up to an error, so this exactly same as prime number theorem it is actually generalization of prime number theorem because it is dividing the primes into different conjugacy classes. We are saying that the count in each conjugacy class is what you would expect if things were uniformly distributed. Now, this can be proven essentially used, not essentially completely following or almost completely following the tools. We have developed the entire strategy of writing this ψ in front in form of what did you do we started with ψ and connected it with a zeta function where the count to ψ .

We wrote in terms of an integral which involved zeta prime over zeta and then we did a contouring integral and said this contouring integral is essentially this sum of the poles of the zeta functions and some other ones and that gives this estimate. So, we do exactly the same thing, the difference is that now this becomes a little messier sum because we are counting only primes which are a modular q not all primes. So, we need sum way of just pin pointing primes a module q so for that what we will do is we will add some new ideas into this, then we follow essentially the whole methodology.

(Refer Slide Time: 06:28)



So the new ideas are well one of them actually there is only one new idea characters module q . So, characters q is a map, which is a from \mathbb{Z}_q^* to complex numbers, all the classes then it should be x by $\log x$, but this is ψ this is not π for p you just divide by $\log x$. So, it is a map for \mathbb{Z}_q^* which is set of all numbers less than q relatively prime to q to complex numbers and \mathbb{Z}_q^* happens to be a group under multiplication module q and is character. If it is multiplied, there is a b is now some properties of characters are pretty evident, first is that of a is a by q the root of infinity. This is because of any a and \mathbb{Z}_q^* a to the $\phi(q)$ is one because the size of this group is $\phi(q)$.

So, a to the $\phi(q)$ is 1, therefore since it is multiplied, one is 1, therefore X of a is a to the $\phi(q)$ is 1, which means that X of a is $\phi(q)$ root infinity, which obviously implies that the characters always map to unit circle on the complex number. If you let g , set of all characters, then g is a group, so that is a multiplication of two characters is another character. It follows simply by the fact that firstly multiplication of two characters is obviously multiplied and it again maps \mathbb{Z}_q^* to complex numbers more interestingly size of g is also $\phi(q)$, this is a group of same size as the group on which it operates. I am not going to prove this you guys can work out on this none of this is difficult to prove at all.

(Refer Slide Time: 10:20)

$$(4) \sum_{a \in \mathbb{Z}_q^*} \chi(a) = \begin{cases} \phi(q) & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases}$$

where $\chi_0(a) = 1$.

$$(5) \sum_{\chi \in G} \chi(a) = \begin{cases} \phi(q) & \text{if } a = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then, if you sum take a character of a and sum over all a 's in \mathbb{Z}_q^* , then one of the two things happen. This is pretty straight forward to see because these are $\phi(q)$ th root of units different a is different a 's will be mapped to different $\phi(q)$ th roots of a . If they are mapped to the same, then there will be a same amount of a mapping into the, so this is either $\phi(q)$ if is 0, where 0 is 1. So, this is a trivial character which maps every element to 1, so if that is the case that is obviously something $\phi(q)$ and that is not the case, then it just basically summing of all roots of unit $\phi(q)$ th root of unit and they will all cancel each other out this is standard.

Finally, in sum over all characters in the group G of X of a , again one of the two things happen if you look at $\phi(q)$ if a is 1 0 otherwise. So, these are purely basic factors about characters, which some of which we will use, so how does this relate to the problem we have. Well, if you recall we wanted to identify the those primes which are exactly equal to a modular q , now one way of thinking about it is a is a residual class modular q and which is this. So, the characters operating on \mathbb{Z}_q^* which sent it to complex numbers, which is essentially the domain that we are going to work on eventually.

So, they can take this transform this problem of you know looking at residual class of a module q to that of looking at certain roots of unit a 's in the complex, so that is the broad picture and that is how it works out.

(Refer Slide Time: 13:21)

$$L(z, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^z}$$

where $\chi(n) = \begin{cases} \chi(a) & \text{for } a = n(q) \\ 0 & \text{for } (n, q) > 1. \end{cases}$

$$L(z, \chi_0) = \sum_{\substack{n=1 \\ (n, q)=1}}^{\infty} \frac{1}{n^z}$$

In fact, what I am going to do now is define or recall χ functions which are generalization of zeta functions before that I should have defined what χ of n is. So, this is a generalization of zeta function, almost we have χ , where now an additional parameter which takes is χ defined with respect to χ , the numerator is now χ of a . Now, here I am using χ of n on all numbers, I have just defined only on z q star, so I have to extend that definition and that is whatever is the obvious definition. We just use it χ of n is equal to χ of a or say if q and n are not relatively prime, then χ of n is 0, if they are relatively prime. Then, we just take n go modular q take the residual class to which it belongs and that χ of a value of χ of n .

So, this is basically cycles the value of n cycle in a cycle length of q of 0, we can also define χ of 0 as 0 χ of 1 is 1, χ of 2, whatever χ of 2 is you go up to any point, where you hit a number which is relatively not relatively prime to q χ of that number is 0. Otherwise, χ of that number is defined as by the definition we reach up to q minus 1.

Then, you go to q χ of q is 0 and then you cycle back into this exactly the same pattern, so that pattern keeps on repeating. Now, these functions play the same role as a zeta function, so when we translate that ψ of x a q as an integral over complex range, we find is L function. I will show you that, but maybe not today tomorrow, but let us spend some time in trying to understand, what these χ functions look like. So, what about how does L z χ_0 look like, which is the simplest of these χ functions χ_0 is 1, but it is not 1

everywhere, so it is not quite the zeta function $\chi(0)$, is it is 1 precisely when n is not coprime to q .

So, this is n greater than equal to 1 and q is 1, 1 over n to the power z , now is there a way of writing that with certainly more complicated function, but can we write it as in the same form with the multiplicative form that.

(Refer Slide Time: 17:35)

The image shows a whiteboard with handwritten mathematical formulas. At the top, there is an equation:
$$= \prod_{\substack{\text{prime } p \\ (p, q) = 1}} \frac{1}{1 - \frac{1}{p^z}}$$
 Below this, the word "Similarly," is written. Then, the Dirichlet L-function is defined as:
$$L(z, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^z}$$
 This is followed by its multiplicative form:
$$= \prod_{\substack{\text{prime } p \\ (p, q) = 1}} \frac{1}{1 - \frac{\chi(p)}{p^z}}$$
 The whiteboard also shows a standard software toolbar at the top and a page number '5/23' at the bottom right.

We could do for zeta function, e comma q is 1 of 1 over 1 minus 1 by q to z , so it has although it is a little more complicated than the zeta function. It still has that same multiplicative expression and that is really the one of the key points of studying the effect almost all the results we used about zeta function came out of this order.

Then, we took log of zeta, which translated these into sum and then the derivative χ , so all of that comes from the equation, which does exist in this case, which is good to know so that you can play around with this more easily. Similarly, let us take a general character does this have a multiplicative form, it does and that is exactly this as you would expect why this is a bit of justification. If you write this down or rather write as a infinite power sum you get one plus χ p over p to the z in the denominator and so on, χ of p whole square is same as χ of p square.

So, that infinite sum can be written as χ of p by p to the z somewhat and then when you multiply with this all primes p which are relatively prime to q , you just get all numbers

of n and divided by n to the z for all n which are relatively prime to q . So, n is 0 whenever n is not relatively prime to q , so here we are crucially using the fact that the character χ is multiplied. If it is not multiplicative, this factorization does not work because it is multiplicative it is working and that is a second that is really the defining property in the sense or a key property in order to such a factorization to a prime for the infinite sum.

So, later on we will see we will put in more complex things here than just characters, but that is the key property, we will always want to have that whatever we put in here factorizes. So, both of in general functions help in such a factorization, now very quickly because again for zeta function, we know that it has a pole at z equals 1, what about these do they have poles at z equals 1. So, again let us go back to the first the trivial characters as it is called χ_0 does it have poles at z equals 1.

(Refer Slide Time: 21:46)

$$L(z, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^z}$$

where $\chi(n) = \begin{cases} \chi(a) & \text{for } a = n(q) \\ & \chi(n, q) = 1 \\ 0 & \text{for } (n, q) > 1. \end{cases}$

$$L(z, \chi_0) = \sum_{\substack{n \geq 1 \\ (n, q) = 1}} \frac{1}{n^z}$$

So, you just put z equals 1 in this sum, so this is like a log, what it is called the harmonic series, but some pieces are missing, so what are the pieces which are missing? So, the pieces which are missing are for all the n 's for which n q is greater than 1.

(Refer Slide Time: 22:16)

Handwritten mathematical derivation on a whiteboard:

$$L(1, \chi_0) = \sum_{\substack{n \geq 1 \\ (n, q) = 1}} \frac{1}{n}$$

Let $p_1, p_2, \dots, p_\ell \mid q$, and no other prime.

$$\sum_{\substack{n \geq 1 \\ (n, q) = 1}} \frac{1}{n} = \zeta(1) - \sum_{i=1}^{\ell} \frac{1}{p_i} \zeta(1) + \sum_{\substack{i, j=1 \\ i \neq j}}^{\ell} \frac{1}{p_i p_j} \zeta(1) - \dots$$

Now, does that make any significant difference in the sum that is the question, something in which you do not have a prime number. There will be a finite number of primes that will be prime factors of X , now all those n 's in which I do not have those prime factors. They can be only mapped to another set in which the total number of primes is all the primes infinite primes minus those constant number of primes. You are saying that the sum is sum is the full sum minus a finite number no that is not true, not a finite number the primes that is in use they will be finite, primes will be finite that is true.

So, the product of sum of their product is something like a geometric series or say two three and five geometric series of two into geometric series of three into geometric series of five the product of finite such series. The sum is finite, no series is infinite, but the sum is finite, why the sum would be finite no this is for example, let us say q is 2 times t , so what are we excluding, we are excluding all ends which are multiples of either 2 or 3. So, what we are excluding is one plus one by summation 1 by 2 n , we are also excluding summation 1 over 3 n and we are we are counting their product twice. So, we are we are add, so this is like inclusion exclusion principle add summation 1 by 6 n .

So, let us do that, so let us say $p_1 p_2 \dots p_\ell \mid q$ and no other prime, so all multiples n all n 's which are multiples of any of this are excluded, but now we are having. So, we basically write it as you know it is zeta 1, then we are to subtract what do we subtract summation how you are going one to $L \frac{1}{p_i}$ times zeta 1. Now, you are over

subtracting, now we have to add back and i not equal to here, again zeta 1 minus something, so this inclusion exclusion that goes on here.

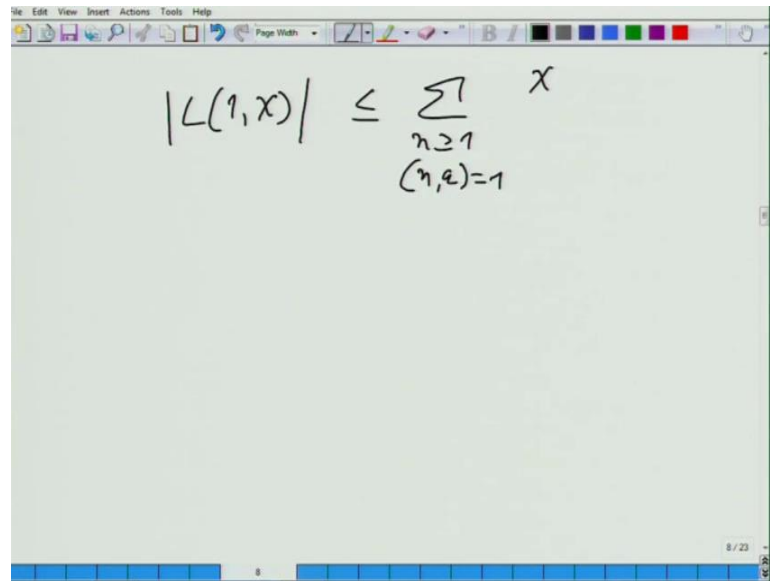
(Refer Slide Time: 25:51)

The image shows a whiteboard with handwritten mathematical expressions. At the top, the Riemann zeta function at s=1 is expressed as an alternating sum of reciprocals of prime powers:
$$= \zeta(1) \left[1 - \sum_i \frac{1}{p_i} + \sum_{\substack{i,j \\ i \neq j}} \frac{1}{p_i p_j} - \dots \right]$$
 This is then simplified to an infinite product over primes:
$$= \zeta(1) \prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i} \right)$$
 Below this, it is stated: "Hence, $L(1, \chi_0)$ diverges." A question is posed: "What about $L(1, \chi)$, $\chi \neq \chi_0$?" The Dirichlet L-function is then defined as:
$$L(1, \chi) = \sum_{\substack{n \geq 1 \\ (n, q) = 1}} \frac{\chi(n)}{n^z}$$

So, basically zeta 1 is always there it is always present times 1 minus summation i 1 over p i plus summation i j 1 over p i p k i not equal to j minus and so on. It is this a recognizable quantity as long as 0, we are done because zeta 1, we know is infinite, this is what it is and that is it the problem solved. Now, what about when you have non principle character or non trivial character then what about X zeta 1 times the series. The lower series are greater than the number of terms in the previous series number of terms is same we are running n and q.

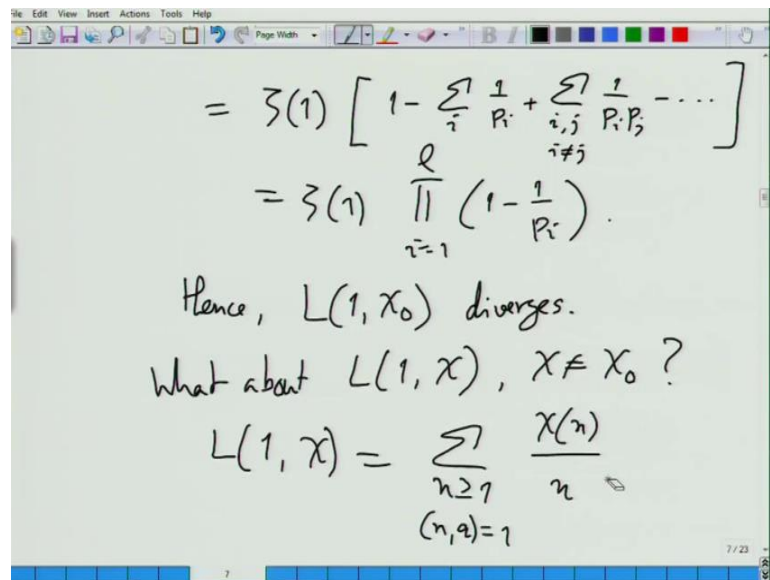
I am taking it, so basically instead of 1, we have a number greater than 1, so it will be the original series plus some other constant series it will diverge. It will diverge, why is this, how does the original series come from no it is a complex number that is always on the unit circle, it could be minus 1 also it converges a very simple look at the absolute value.

(Refer Slide Time: 28:46)


$$|L(1, X)| \leq \sum_{\substack{n \geq 1 \\ (n, a) = 1}} X^n$$

I need to be there, I do not want, that is why I do not want to look at absolute values of X , but it is no problem.

(Refer Slide Time: 29:20)


$$\begin{aligned} &= \zeta(1) \left[1 - \sum_i \frac{1}{p_i} + \sum_{\substack{i, j \\ i \neq j}} \frac{1}{p_i p_j} - \dots \right] \\ &= \zeta(1) \prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i} \right). \end{aligned}$$

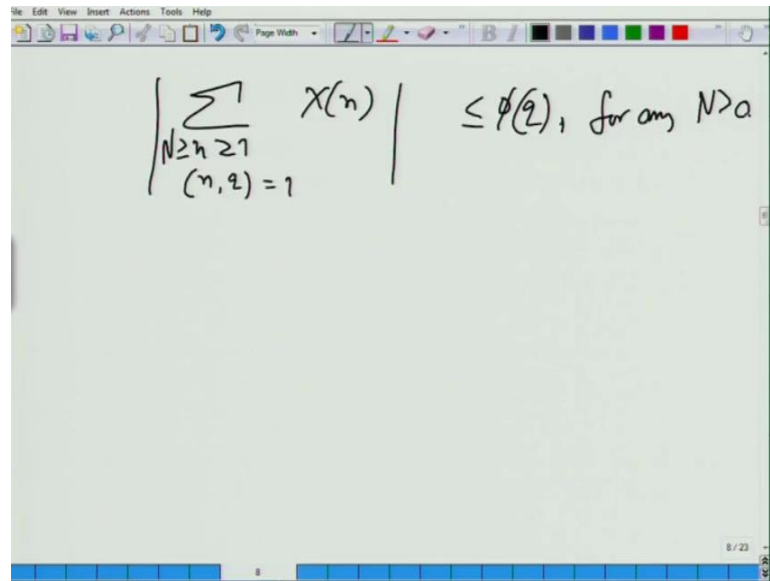
Hence, $L(1, \chi_0)$ diverges.

What about $L(1, \chi)$, $\chi \neq \chi_0$?

$$L(1, \chi) = \sum_{\substack{n \geq 1 \\ (n, a) = 1}} \frac{\chi(n)}{n}$$

Let us forget for the time being the denominator and suppose we are just summing up the numerators over all n does, this sum diverge, is it diverged?

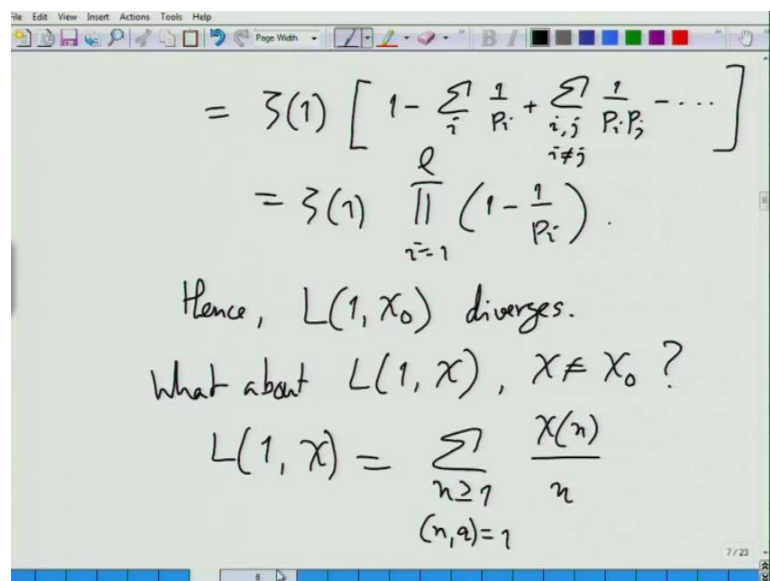
(Refer Slide Time: 29:40)



$$\left| \sum_{\substack{N \geq n \geq 1 \\ (n, q) = 1}} X(n) \right| \leq \phi(q), \text{ for any } N > a$$

Now, that is basically being undefined that is correct, but since that I am not saying. It converges with that I am asking if it diverges, so if you sum it up in usual sense of using the prefixes this is always less than equal to $\phi(q)$ actually 5 because the first q when you sum up the first q you get 0. These are roots of units non trivial roots of units circle around X , at the end you will get 0, the next q 0 again the next q 0, again so whatever is the segment which is left out. Actually, I should not try this strictly speaking what I should try is put an upper and then for any n this is bounded by this quantity.

(Refer Slide Time: 31:06)



$$= \zeta(1) \left[1 - \sum_i \frac{1}{P_i} + \sum_{\substack{i, j \\ i \neq j}} \frac{1}{P_i P_j} - \dots \right]$$

$$= \zeta(1) \prod_{i=1}^q \left(1 - \frac{1}{P_i} \right).$$

Hence, $L(1, X_0)$ diverges.

What about $L(1, X)$, $X \neq X_0$?

$$L(1, X) = \sum_{\substack{n \geq 1 \\ (n, q) = 1}} \frac{X(n)}{n}$$

Now, let us come to this sum, what can we say about this sum?

(Refer Slide Time: 31:15)

$$\left| \sum_{\substack{N \leq n \leq 2N \\ (n, q) = 1}} x(n) \right| \leq \phi(q), \text{ for any } N > 0$$

Consider $\sum_{\substack{Nq < n \leq (N+1)q \\ (n, q) = 1}} \frac{x(n)}{n}$

Assignment

$$= \sum_{\substack{0 < n \leq q \\ (n, q) = 1}} \frac{x(n)}{Nq + n}$$

$$= \frac{1}{Nq} \left(\sum_{\substack{0 < n \leq q \\ (n, q) = 1}} \frac{x(n)}{1 + \frac{n}{Nq}} \right)$$

prove that $f(n, x)$ is formally

I want to show that this is also convergent; there is only few of q non zero term in that segment of length q . I am just adding them all up of course, it is not the case it is correct, now when you stick a n in the denominator what happens to this you should see the bonding. Let us take segment of length q after several initial large number of initial ones, so what happens to that, let us say $n q$ less than n less than equal to n plus $1 q$. This would be if you see the denominator here, it will vary from $n q$ to n plus $1 q$, so denominator will roughly be the same when n is large.

Then, the difference is just between the denominator value is $n q$ to $n q$ plus q and the q is of course, the fixed quantity. So, it is going to be very minor difference in the denominator and if the denominators are equal then this sum is 0. Here, successive terms are still less than 1 because that series diverges, which series diverges. Now, if you look at other series they have the successive terms, then I think the ratio can be written in terms of the original series times some quantity.

That is less than 1, but the originals ones those are complex numbers, so I do not know how to write that. So, I mean this is rough this should be very close to 0 and as n grows bigger and bigger, they should approach 0 quite rapidly I would say, let me write it in the following way.