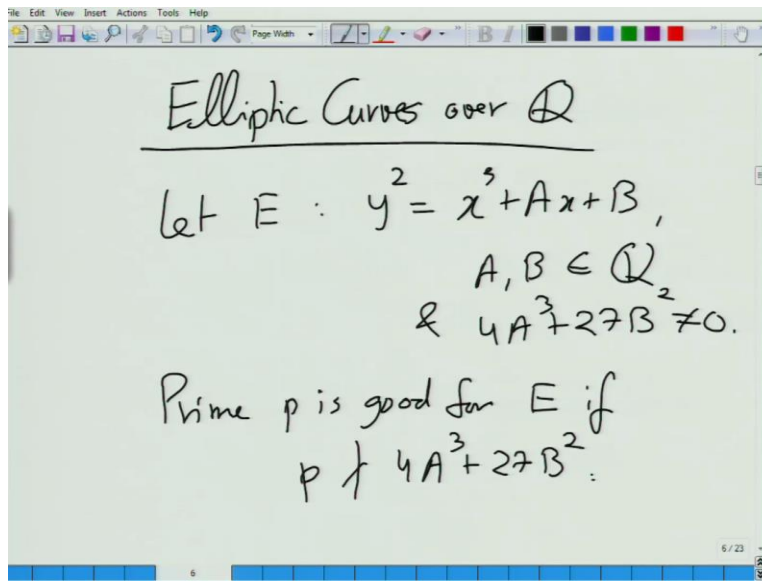


**Riemann Hypothesis and its Applications**  
**Prof. Manindra Agrawal**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kanpur**

**Lecture – 29**

(Refer Slide Time: 00:18)



So let us talk about elliptic curves over  $\mathbb{Q}$ . Actually yesterday we did part of it. So  $E$   $y$  square equal to  $x$  cube plus  $Ax$  plus  $B$ ,  $A, B$  are rational numbers and  $4A^3 + 27B^2$  is not equal to 0. So these would prime  $p$  is good for  $E$  if  $p$  doesn't divide.

(Refer Slide Time: 01:07)

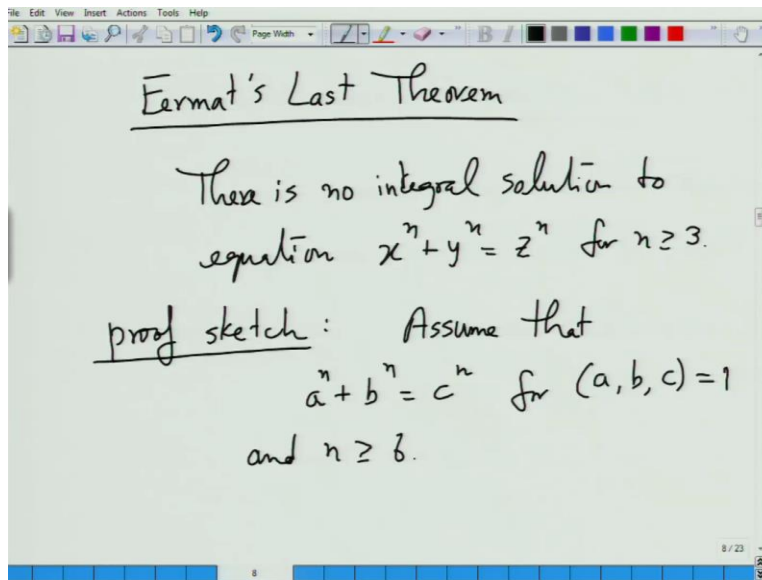
$$\zeta_E(z, \mathbb{Q}) = \prod_{p \text{ good}} (1 - a_p p^{-z} + p^{1-2z})$$

$$(\ast) = \prod_{p \text{ bad}} (1 - a_p p^{-z}), \quad a_p \in \{-1, 0\}$$

And we define the zeta function for the elliptic curve over  $z$  rational, so unique as a product over  $p$ ,  $p$  good of simply one minus  $a_p p$  to the power minus  $z$  plus  $p$  to the power one minus two  $z$  that's right, and times something else which is product over bad prime just for the sake of completeness let me give you what is  $p$  product over bad primes of 1 minus  $a_p p$  to the power minus  $z$ . Very simple, but  $a_p$  is not well define for bad primes ah that is not define the same way for bad primes. So this  $a_p$  is actually without going (( )), it is either minus 1 or 0, depending on what is the type of badness.

So the type of badness could be there is repeated that two roots would be or all three roots would be depending on what kind of badness (( )). So this is the zeta function for the elliptic curve where the rational. Like I said last time, this is closely connected with the Eermat's Last theorem, (( )). So, what is the connection?

(Refer Slide Time: 03:11)

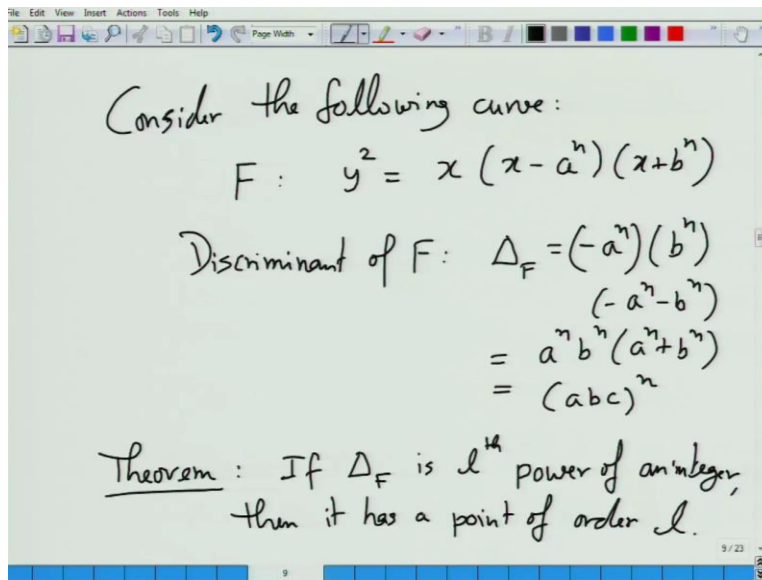


So let us start with that connection. What?

Student: (( ))

Professor: It's depend on a type of badness, so when there are anybody have two types two roots would be or all roots would be, but within that there are classification. So Eermat's last theorem is all of you know this is there is no integral solution to  $x$  to the  $n$  plus  $y$  to the  $n$  equal to  $z$  to the  $n$  for  $n$  greater than or equal to three. So how to do the proof (( )). Now I will just provide a very brief proof sketch. Assume that  $a$  to the  $n$  plus  $b$  to the  $n$  equal  $c$  to the  $n$  for for number integers  $a$ ,  $b$  and  $c$  whose residues is one (( )). And  $n$  greater than equal to 6 ok. For  $n$  less than 6, you already know the solution, by the result 3, 4 and 5 1 can prove these in very simple methods and there are no solutions. With these are proved by (( )), proved it for equals (( )) in 4, 5 or like anything.

(Refer Slide Time: 05:25)



Consider the following curve:

$$F: y^2 = x(x - a^n)(x + b^n)$$

Discriminant of  $F$ :  $\Delta_F = (-a^n)(b^n)(-a^n - b^n)$

$$= a^n b^n (a^n + b^n)$$
$$= (abc)^n$$

Theorem: If  $\Delta_F$  is  $l^{\text{th}}$  power of an integer, then it has a point of order  $l$ .

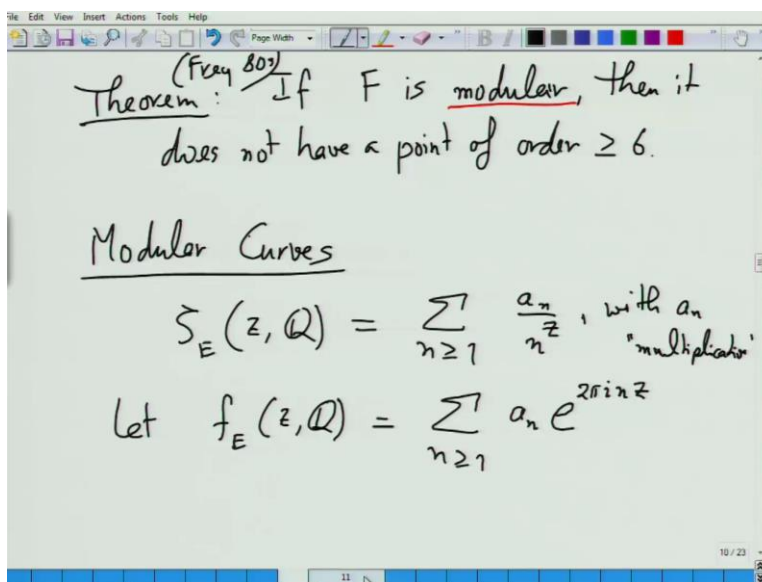
Now consider these elliptic curve, which is very simple and we define using this solutions, one of these solutions to be this equal to a b, we are using n b and make a to the n and b to the n, a to the n and minus b to the n two roots of the right hand side. Now for this curve, which is elliptic curve, it is discriminant, discriminant is same as the four a Q plus twenty seven b square. And if you remember that is non-zero if and only could be no repeated roots. So alternative description of discriminant in terms of root is, discriminant is delta F equal to it's product of different sets. If any two roots repeat in product is zero, discriminant. And it is actually easy to show that for an elliptic curve, the discriminant that the definition idea is equivalent equal to product of the roots. So what is the product of different roots of this curve?

Well, one is zero, one root is 0 then other root is a to the n, the third root is minus b to the n. So the difference between a this two roots, a to the n, first two roots, 0 minus, minus a to the n, 0 minus minus b to the n that is b to the n. And the third one will be minus b to the n, minus a to the n... ok So this is equal to a to the n b to the n a to the n plus b to the n, and because a b c is the solution of that formers equation, so a to the n plus b to the n (( )). So I can write to this a b c to the n, a b c is the integers. So this is showing that the discriminant of ah this particular elliptic curve is n eth power. So what (( )) that means many things but one of the things is the following theorem that if delta F, this is the more general theorem which is specializing for the case of this elliptic curve, delta F is l th power integer, then it has a point of order l. This theorem is

conditional let us keep as it is sense, it is n eth power of an integer with point of order l. The point of order l is, ah the group associated with the elliptic curve right, which is group of rational point, these are all rational.

At the point of order l simply means a point for that if we add the point to itself n times we get 0 or infinity that is the identity of this. And no smaller number of addition will be infinity (( )). So the power of discriminant in relates to the order of a particular point that's all.

(Refer Slide Time: 10:17)



And then there is a theorem miller theorem that if the F is modular, then so if the curve is modular which I will define so, if the curve is modular, then it does not have a point of order greater than equal to 6. So if we can prove that F is modular whatever that means then we are done. Because when we say that it cannot have a point of order greater than equal to 6. Therefore either all points of order less than equal to 5 or have infinite to all, it keep on adding the point, it never get infinity.

So there is a point of, (( )) point of order greater than equal to 6, then discriminant cannot be 6 for higher power of an integers by this theorem, which means in turn a to the n plus b to the n equal c to the n, there is no such solutions (( )). That's the collection, so this ah whole part of these things were known already, but this was the this connection was put together by Frey in late eighties. I think he proved this non hiding away certain details, strictly speaking these

statements I am making are not true, could approximately, there are some small small twist then one has to give even the discriminant description changes by  $(\Delta)$  divided by certain  $(N)$ , but will not get into this, just mix the whole thing will mix, without adding anything to our understanding.

So the challenge at this point was can we prove  $F$  to be  $(\Gamma)$ . So what is it means, for a curve to be modular. So let us go back to the elliptic curves, and let's go back to those the zeta function, so it is called zeta  $E, z$  of  $Q$ , if you remember last time we wrote it as also as a  $n$  by  $n$  to the  $z$  correct with certain multiplication properties of a  $n$ . This came out of the product form is which we expand it to get this form. So this is one series, we associated with an elliptic curve. And like I said the couple of lectures ago, there is another series we can associate with an elliptic curve which is the natural power series. So let's define to be  $f \in z \in Q$ . Instead of writing  $z$  to the  $n$ , I am going to write slight differently this is the Fourier series form of the power series. We can derive it naturally from the power series by whatever the variable in power series replace that variable by  $e$  to the  $2\pi i x$  and then we have this Fourier series form.

So these two we can see coefficients are really common to these two series and therefore there are some relationship clearly between these two. Now we so far looked at the zeta function, focused on this alternative form – the Fourier series of this. Can you identify some interesting properties there? There is one very simple, but nice property. The name Fourier series,  $(\Gamma)$  periodicity, the function  $f$  is periodic. What is period?

$(\Gamma)$

(Refer Slide Time: 15:58)

Observation:

$$\begin{aligned} f(z+1) &= \sum_{n \geq 1} a_n e^{2\pi i n (z+1)} \\ &= \sum_{n \geq 1} a_n e^{2\pi i n z} \cdot e^{2\pi i n} \\ &= f(z). \end{aligned}$$

Let  $z = \alpha + i\beta$ ,  $\beta > 0$ .

$$\begin{aligned} \text{Then } f(z) &= \sum_n a_n e^{2\pi i n (\alpha + i\beta)} \\ &= \sum_n a_n e^{2\pi i n \alpha} \cdot e^{-2\pi n \beta} \end{aligned}$$

What?

(( ))

One? One is any period of this function (( )) because  $f(z+1) = f(z)$  because  $f(z) = \sum_{n \geq 1} a_n e^{2\pi i n z}$  and  $f(z+1) = \sum_{n \geq 1} a_n e^{2\pi i n (z+1)} = \sum_{n \geq 1} a_n e^{2\pi i n z} \cdot e^{2\pi i n} = f(z)$ , so this is the periodic function, that's why any periodic function there is an actual Fourier series. So that's one(( )) obvious property of this function. And the another very interesting property which is so this function clearly is the way to define. Now look at ah what shall I say where is the function define.

This function may or may not for various point on the complex plane, this function may or may not be defined. Suppose  $z$  is on the upper half of complex plane, which means the real, no the imaginary part is positive. So let  $z$  ah  $\alpha + i\beta$ , and  $\beta > 0$ . Then what is  $f(z)$ ,  $\sum_n a_n e^{2\pi i n (\alpha + i\beta)}$ .

(Refer Slide Time: 18:22)

$$\Rightarrow |f(z)| \leq \sum_n |a_n| e^{-2\pi n \beta}$$

$$\leq \sum_{n \geq 1} \frac{O(n)}{(e^{2\pi \beta})^n} < \infty$$

Möbius Transformation

$$\tau: \mathbb{H}_+ \rightarrow \mathbb{H}_+, \quad \mathbb{H}_+ : \text{upper half of } \mathbb{C}$$

$$\tau(z) = \frac{az+b}{cz+d}, \quad \begin{array}{l} a, b, c, d \in \mathbb{C} \\ \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1. \end{array}$$

So if you look at the absolute value of  $z f z$  is less than equal to sum over  $n$  absolute value of  $n$ , actually  $n$  is an integer, is the positive times all these course away. And this is  $n$  always positive, it is less than equal to summation  $n$  greater than equal to one, what is upper bond of the  $n$  like order  $n$ , a  $p$  is  $p$  plus one plus minus two square root  $p$   $h$ , and the multiplicative properties shows there a  $p$   $Q$  is a  $p$  times a  $Q$   $(( ))$   $p$   $Q$ . And the a  $p$  square also, I am not giving the definition one can show the order  $p$  is one. So this would be order  $n$ ,  $O$   $n$  would be order  $n$  divided by  $e$  to the two  $\pi$   $\beta$  this purely converges that because the denominator of  $(( ))$ .

The same argument can be used to show that when you are in the lower half of complex plane then this diverges, because then this would be positive and that will really shoot up no matter what their coefficient root  $(( ))$ . And on the real line, may or may not converge depending on how these coefficients are sort of, so that's the sort of the structure of the  $(( ))$  has been defined, essentially upper half of complex plane. Now comes the interesting transformation on the upper half of the transformation on the upper half of complex plane, which is called Möbius transformation. So here,  $H$  plus is upper half of the complex plane,  $\tau$   $z$  goes to  $a$ ,  $b$ ,  $c$ ,  $d$  and determinant of  $a$ ,  $b$ ,  $c$ ,  $d$  is one. So these matrices 2 by 2 matrices which determinant is one, they form a group, with usual identity and so on,  $(( ))$  under multiplication not addition. And this is very well-known group called the symmetry linear group  $ah$   $(( ))$  size of order two.



(Refer Slide Time: 22:31)

The image shows a whiteboard with handwritten mathematical derivations. The first part shows the transformation  $\tau(z) = \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}$ , which is simplified to  $\frac{ac|z|^2 + bd + adz + bc\bar{z}}{|cz+d|^2}$ . The second part shows the imaginary part  $\text{Im}(\tau(z)) = \frac{(ad-bc)\text{Im}(z)}{|cz+d|^2}$ , which is further simplified to  $\frac{\text{Im}(z)}{|cz+d|^2}$ . The whiteboard has a toolbar at the top and a status bar at the bottom showing '13 / 23'.

$$\tau(z) = \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}$$

$$= \frac{ac|z|^2 + bd + adz + bc\bar{z}}{|cz+d|^2}$$

$$\text{Im}(\tau(z)) = \frac{(ad-bc)\text{Im}(z)}{|cz+d|^2}$$

$$= \frac{\text{Im}(z)}{|cz+d|^2}$$

So essentially this is  $\tau(z)$  operating on this, so  $\tau(z)$  is simply  $\tau$  operating on the complex, someone in this form. The interesting thing is this maps upper half of complex plane to upper half of complex plane.  $\tau(z)$  slightly some more  $az + b$  times  $c\bar{z} + d$  bar  $z$  multiplied with complex conjugate. And what do you get here, now let me make a simplification here. Just make like simple, I just use this  $Z$ , because this is what I am going to be interested. So  $a, b, c$ , we are going to be integers, there is no  $c$  bar, no  $d$  bar. So this comes as  $ac|z|^2 + bd + adz + bc\bar{z}$ ... Now if you look at the imaginary part of  $\tau(z)$  what is that. This is real, so this is for this contribute the imaginary part then they got the real part, the imaginary part of that bar is negative of the imaginary part of this, so you get  $ad - bc$  times imaginary part of  $z$  divide by  $|cz + d|^2$ . Now  $ad - bc$  by this definition is one. So this is imaginary part of  $z$ , divided by  $|cz + d|^2$ . So it is sign is exactly same as  $\left(\frac{\text{Im}(z)}{|cz+d|^2}\right)$ .

So that's where I am going to stop, because I don't have time; but tomorrow I am going to finish this half. So this  $\tau$  is going, it's very interesting transformation. It's looks so what funny that you mapping this in this fashion, but it say the most general transformation that preserves  $ah$  for example circles. You make a circle and apply a  $\tau$  on it, then look at the curve that you get, it will be a circle. If we take a line, then apply  $\tau$  on it, what happens to a line, a line also goes to circle. So circles and lines together go the circles. So basically, in general like this, if we take

two lines with certain angles, and look at the corresponding curves on the tau and point where the intersect, you look at the corresponding point wherever the corresponding tau curves intersect. Look at the angle of intersection there that the angle will represent and this is this how we can actually characterize the mobius transformation, all the class of entire transformation which preserve this property. So it is very interesting sub class of transformation which preserve lot of properties and these are going to be useful for us also, because the property that we want from this function  $f$  is essentially invariance under tau. So  $f$  of  $z$  or say  $f$  of tau  $z$ , you would want to be roughly equal to  $f$  of  $z$  not completely (( )).