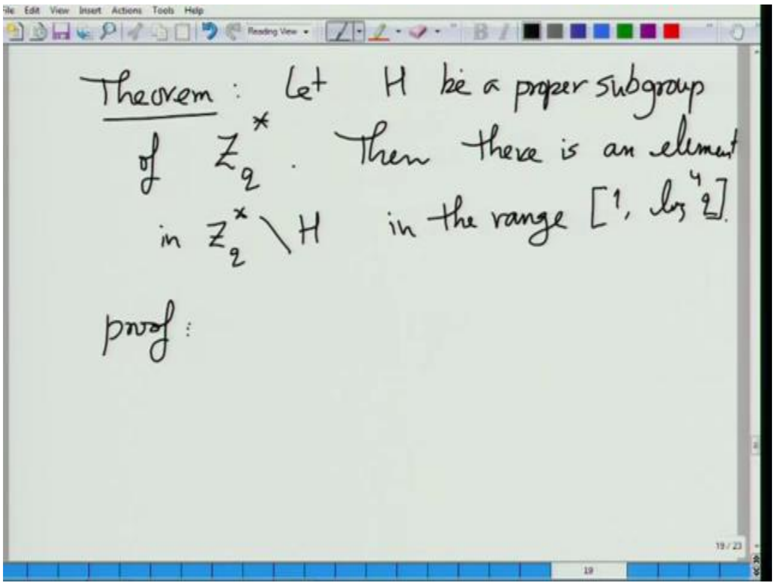
Riemann Hypothesis and its Application

Prof. Manindra Agrawal
Department of Computer science and Engineering
Indian Institute of Technology, Kanpur

Lecture – 25

(Refer Slide Time: 00:22)

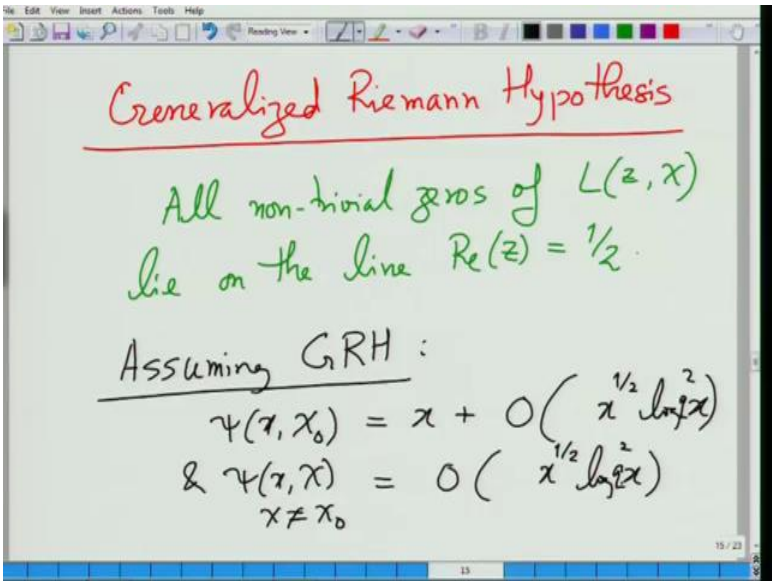


Theorem : Let H be a proper subgroup of Z_q^*. Then there is an element in $Z_q^* \setminus H$ in the range $[1, \log^4 q]$.

proof :

Just small simple break that is that has to strike you, so that it will become straight clear. So, we have this H is a proper sub group by the way I think I have yes I have made a mistake.

(Refer Slide Time: 00:40)



Generalized Riemann Hypothesis

All non-trivial zeros of $L(z,\chi)$ lie on the line $Re(z) = 1/2$.

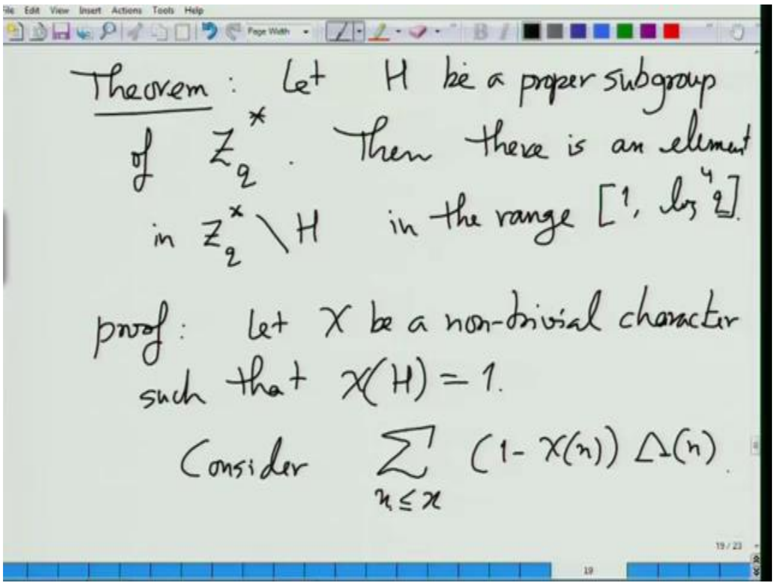
Assuming GRH :

$$\psi(x,\chi_0) = x + O(x^{1/2}\log^2 qx)$$

$$\& \ \underset{\chi \neq \chi_0}{\psi(x,\chi)} = O(x^{1/2}\log^2 qx)$$

In stating of the G R H the consequence of G R H when I say q square root x log square x this is not true the q is here, square root x square root x log square x here may be this is what stopped you from proving it yes.

(Refer Slide Time: 01:11)



Theorem : Let H be a proper subgroup of Z_q^*. Then there is an element in $Z_q^* \setminus H$ in the range $[1, \log^4 q]$.

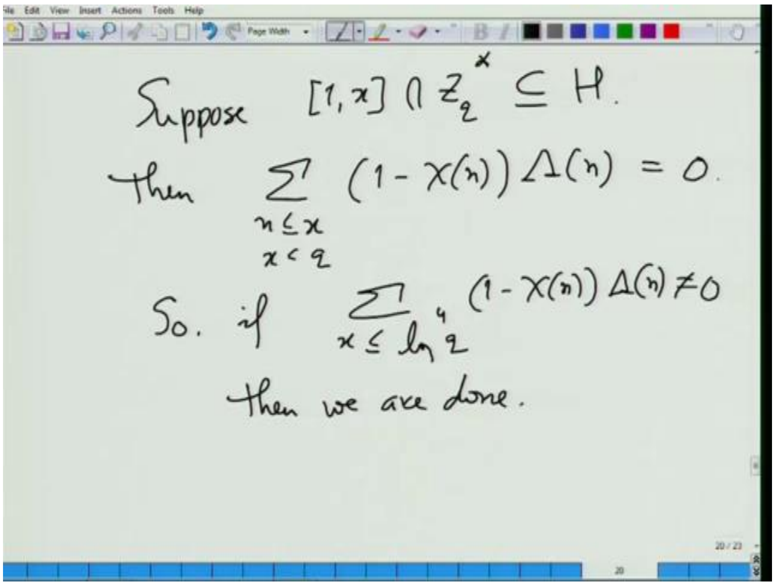
proof : let χ be a non-trivial character such that $\chi(H) = 1$.

Consider $\sum'_{n \leq x} (1 - \chi(n))\Lambda(n)$.

So, what H is a sub group of z q star a proper sub group, so let us define a character or not define there are character already defined the copy character which o one on entire H. But, it is not trivial such a character always exists you just H is the subgroup you sent H to 1 and define to get that there are many possibilities for choosing that character.

So, these character groups are as same as the q star, so fix this, now consider this quantity this is sum of one minus psi n whole time lambda n and n is less than equal to x. Now, think about this quantity sum for a moment and what we are interested in knowing is when is this sum is all 0, let me put it in slight differently suppose between one and n all elements of z q star are in H.

(Refer Slide Time: 03:10)



Suppose $[1, x] \cap \mathbb{Z}_q^{\times} \subseteq H$.

then $\displaystyle\sum_{\substack{n \le x \\ x < q}} (1 - \chi(n))\,\Lambda(n) = 0$.

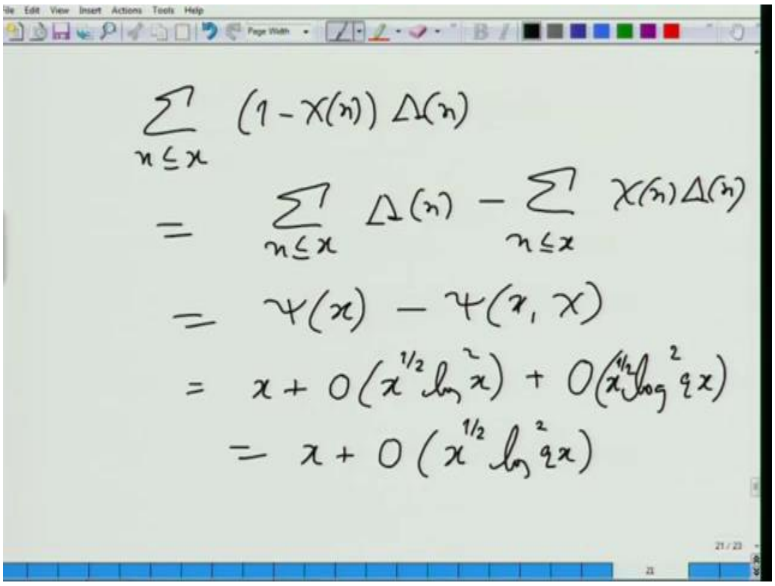
So. if $\displaystyle\sum_{x \le \ln^4 q} (1 - \chi(n))\,\Lambda(n) \neq 0$

then we are done.

So, 1 and x in q star is sub set of H then what is this sum 0 when ever is n is in zq star psi n is one so this is zerowhenever n is not in z q star lambda n is 0, lambda n is non zero only when n is prime power. But, when n is not in z q star it is not trivial in G C D with q yes and we are saying that x is less than x is less than q, q is smaller than anyway that is not an issue. Now, this is 0, this happens, now for all what if you want to show is that in the range 1 to log n, log q to 4 there is a element which is not in z, not in group H.

So, if you can show this sum is non zero when x is log q to the 4 and clearly it is less than q. So, that the condition we want to enjoy just to reveal each, therefore if to the 4 q then, now let us see what this is equal to.

(Refer Slide Time: 04:50)



$$\sum_{n\le x}(1-\chi(n))\Lambda(n)$$

$$= \sum_{n\le x}\Lambda(n) - \sum_{n\le x}\chi(n)\Lambda(n)$$

$$= \psi(x) - \psi(x,\chi)$$

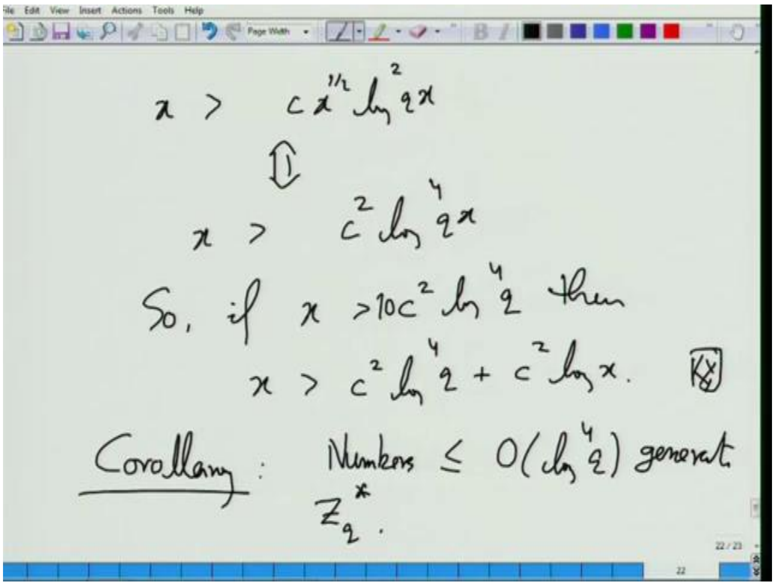
$$= x + O(x^{1/2}\log^2 x) + O(x^{1/2}\log^2 qx)$$

$$= x + O(x^{1/2}\log^2 qx)$$

We already know this is equal to what is this, the first quantity, the first sum equal to what x psi x and the second one psi of x of psi that is by definition. Now, use G R H if G R H is true then psi x equals x plus order square root x log s square x and the G R H is true. The n what is psi x of psi is not trivial for trivial character it is the same quantity x plus order square root x log square q x.

But, psi is not trivial then this is simply order square root x log square q x which is x plus order square root x log square q x. Now, this would be 0 when this a term is equal to the principle term as it, so opposite sign. But, certain see for asymptotically the principle term is much bigger than a theorem at what point does it become bigger it stays bigger forever.

(Refer Slide Time: 06:44)



$$x > c\, x^{1/2} \log^2 qx$$

$$\Updownarrow$$

$$x > c^2 \log^4 qx$$

So, if $x > 10c^2 \log^4 q$ then

$$x > c^2 \log^4 q + c^2 \log x. \quad ☒$$

Corollary: Numbers $\leq O(\log^4 q)$ generate $\mathbb{Z}_q^*$.

So, when x is less than square root x log square q x we cannot leave x is bigger than log to be four q x. So, if x is bigger than let us say c q of log to 4 q is that would be sufficient it would log 4 q x that is sufficient it instead of c q we can say what 10 c square something which is not really very important. So, that is it that means if we look at interval 1 to x, so x is order log to 4 q I am guarantee to find an element which is outside any sub proper subgroup of any proper sub group of H z q star.

So, when you said the sum should be 0 the element for which n is n is some G C D with q and still it can be a prime power and it has G C D with q that is true. So, how do you handle this if n is a prime power and that prime, this prime, that prime should divide q that is the requirement. So, that will have a non trivial G C D and, therefore lambda n is not 1 psi n, what is psi n then psi n is 0 psi n by definition is 0.

So, this is not, then there is certainly sum will be non zero then I will have to count number of occurrences the sum will not be 0. But, what one can see that sum will be very small the x is going to the log to 4 q, we are looking at prime devisers of q which are very small and each such prime deviser lambda n is log of that. So, if you sum it up the sum of logarithm of all prime devisers of all small prime devisers of q that is going to be very small quantity or is it necessarily small quantity yes.

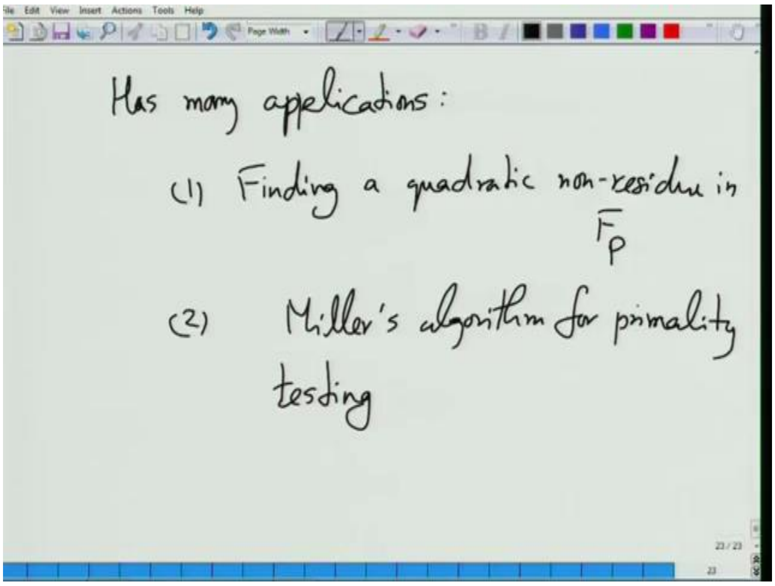
So, it has to be a prime power, so there are a small prime number and we are going up to the only log to 4 q. So, that will say prime devisers which prime devisers may be very small it divides q, so we will go up to a small power of p only. So, the power of p go up to its log q I will agree that does not matter that the power of p will go up to is because this is only log p that we will get counted. So, log p, p itself is less than equal to the log to 4 q, so log p is log q and how many such primes will existsit may be at least log q such primes because their product is going to be q.

So, log q times log q is the maximum value of this sum and then we go here again and do the same thing, so 0 is not that important. So, because this gap is going to be clearly large for appropriately chosen constant here this gap would be log to the 4 q which is very beyond what is allowed it does not matter. But, that is a good point that you are to be carefullycorollary of this is that you look at e the elements of all z q star lesser than equal to the order log to the 4 q. Then it must generate the entire group if it s not then it must generate a sub group and then and that is not possible.

So, there are many other corollary like quadratic, non residue, modular prime if you that, if you want to find given prime pyou want to find quadratic, non residue model of p which is used in factoring quadratic polynomial. So, if whatever if you are take factor polynomial like x square minus a over f p then you are the one convenient algorithm is said to be if you have available. So, one quadratic non residue and using that non residue you can polynomial in polynomial you can factor the polynomial.

Now, how do you get a quadratic non residue well use this theorem start searching from 1, 2, 3, 4 and checking if a number is quadratic non residue. Now, if a number, how do you check if a number is quadratic, no residue p minus 1 modulus of p and see plus 1 or minus 1 that is the correct, p minus 1 by 2 that is how we always get. So, 1 p minus 1 by 2 then get plus 1 or minus 1, keep checking one of the 4 log of 4 to the number has to be quadratic non residue if G R H is true for set of quadratic non residue form a proper sub group of z p star.

(Refer Slide Time: 13:55)



Has many applications:

(1) Finding a quadratic non-residue in F_p

(2) Miller's algorithm for primality testing

So, finding quadratic non residue in f p the other application is millers algorithm for primarily testing I am not going to describe the algorithm. So, you go and look it up if a deterministic algorithm it is polynomial time and claim that if G R H is true and the reason for this claim is and again try to do the same thing. So, it compute the sub group of z p star or the number the z n star, the n is the number which is checking prime or not. So, look at z n star then identify the sub group proper sub group of xn star looking for an element outside the group.

So, if at the element is available then the algorithm becomes polynomial time and this is the way tofind that elementis that this know throwing a big hammer of G R H at you will get polynomial time. So, any questions without G R H this log 4 q, no without G R H the best one is square root q. So, there are lots and lots of problems which will solution will become easy if G R H is true in all kind of field’s diversified case.

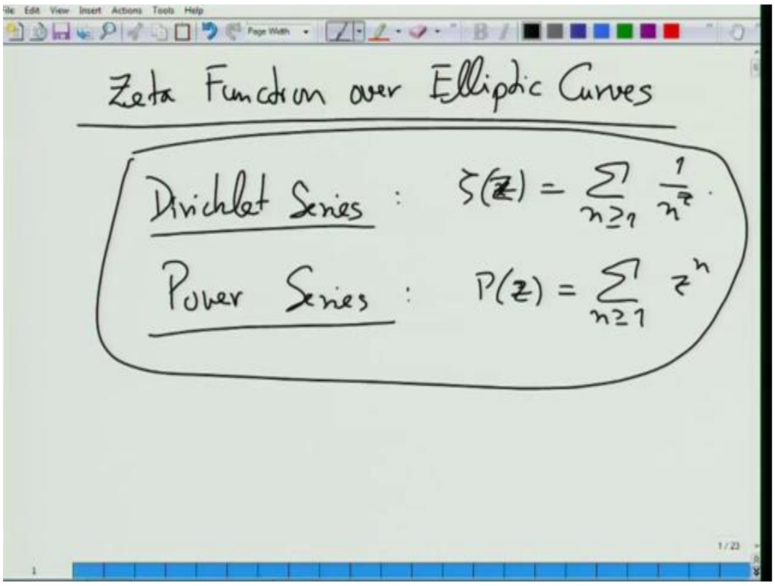
So, for example finding that we know that between n and 2 n there exists a prime for every n, but what one would like to do is shrinkthis interval and show this between n and 2 n. so, obviously there was exists a prime and the one must able to shrink this interval and say that between n and n plus 1 thing there must be always a prime.

Now, G R H is true then you can show that n and n plus and into the 1 plus asylum if I am remembered correctly there must be a prime asylum now what am I saying. Here, what I am saying between n and n plus n asylum there must be 1, so the internal gap will be only n to the asylum by intact G R H if not strong enough to fully satisfy our scale because what is believed to be. Here, n to n and n plus order log square there must be a prime that does not follow from G R H ha it may led to be correct.

Now, I said already much about this hypothesis, one final thing I want to say is that as some apart from its fundamental importance to mathematics seems to have very curious connections with physics. So, there is a theory called quantum field theory in physics I do not know about that anything, but what I read is it is basically models the quantum phenomena and in that there is a particular governing matrix. So, it is a huge matrix and the Eigen value infinite matrix by the way and Eigen values of that matrix are precisely 0 of the zero function.

So, that connection was discarding not too long and it was a quite remarkable insight that zero function has something to say about physical theory as well. So, anyway if you are interested feel free to read the theorem I still have time which is good, now I want to change track I have full lectures. So, in this I want to like to do the following, I will give you an example of the zero function or different kinds of zero function that is the example is elliptic curves and let me create a new template.

(Refer Slide Time: 19:24)



Zeta Function over Elliptic Curves

Dirichlet Series : $\zeta(z) = \sum_{n \geq 1} \frac{1}{n^z}$.

Power Series : $P(z) = \sum_{n \geq 1} z^n$

So, in fact there is a full theory of this zeta function can be defined over as many different objects particular over all 2 dimensional curves. So, there is a corresponding Riemann hypothesis associated with it and that hypothesis actually did not proven and in fact I will prove the Riemann hypothesis for elliptic curves remaining all is same. So, there is also all the zeros, not trivial zeros lie on the line real z equals of, now elliptic curves are interesting formany other reasons as well. S

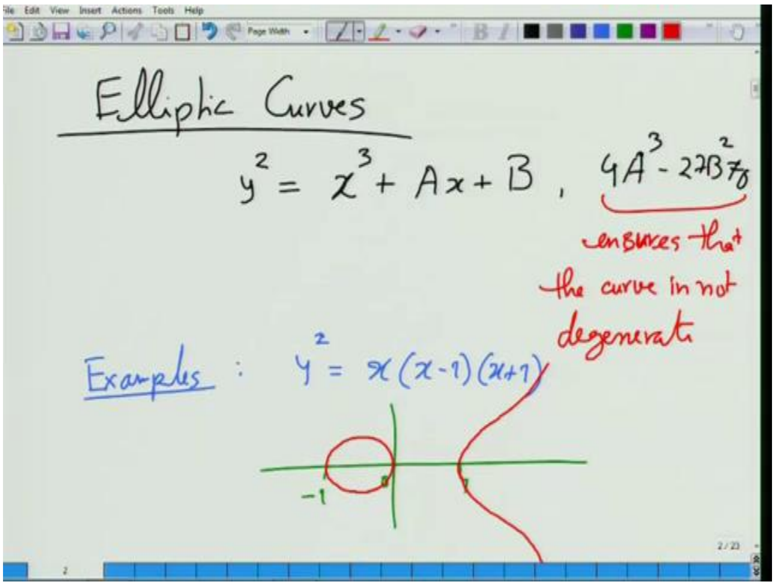
o, I thought, I will do this because once I prove this I will show you the connection between the zeta function for elliptic curve. But, not just theta function actually any Dirichlet series, Dirichlet series is the zeta function original expression all the kind of sigma. So, we have that is for example for this theta z 1 over, so this is infinite sum is calling Dirichlet series and the reason it is called Dirichlet series. But, is a infinite series and there is some another quantity called power series this is more familiar quantities.

So, I guess would be corresponding to this powers series would be p of z equals sigma n greater than equal to 1 z to the n. So, z to the n is familiar in infinite power series, if I keep increasing the Dirichlet series is an end to this type. So, keep this thing andtakes into denominator and in general there could be coefficient in case whatever coefficient are.

Here, we can stick to that coefficient are here these Dirichlet series and power series create these duality between the two and what has been shown that the Dirichlet series has a certain structure. So, that is metaphorphic over the entire complex strain whatever function can be extended to a metaphorphic to the entire complex scan and it has a functional equation like the zeta function. So, does one or one more property I think this size of the coefficient should not be very large in this corresponding power series becomes what you called modular form and vice versa.

So, we should not jump to all these things right away, let us forget about I will come back to this. But, let me first focus of on the zeta function or the elliptic curves eventually, in the last lecture I want to connected to this column up to deforms last theorem and how that was shown using the ideas of elliptic curves modular function and theta function.

(Refer Slide Time: 23:16)



Elliptic Curves

$y^2 = x^3 + Ax + B$, $4A^3 - 27B^2 \neq 0$

ensures that the curve in not degenerate

Examples : $y^2 = x(x-1)(x+1)$

So, now what are elliptic curves do all of you know the definition you know few of you forget.

Student: I forget.

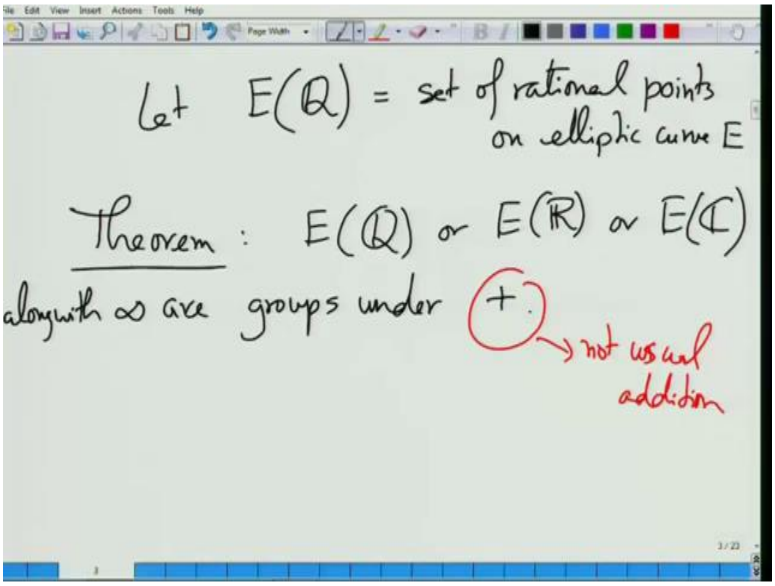
So, elliptic curves are cubic curves in the order the quadratic curves cycle parabolahyperbola ellipse these are the 4 types of quadratic curves. So, the simplest next curve is elliptic curve typically given by equation square equals a y square equals a x cube plus a x plus b and another condition which has to be added to this 4 a cube minus 22 b square should be non zero. So, that is essentially to ensure that right hand side will it is the degree 3 polynomial in x in degree 3 polynomial will have three roots in x.

So, I can rewrite the right hand side as x minus alpha x minus beta x minus gamma, so this condition is equal to saying that the right hand side does not have repetitive roots because if there is repeated roots on that the power of curve will degenerate. But, we do not want that situation that all, so this reasonable condition to assume how do a elliptic curve look like. So, let us take some example suppose y square equals x, x minus 1, x plus 1, so I am writing it in this form of course this if you multiply this how hope it is in this form.

So, this is x square minus 1 times x how does this curve look like, I now realize am not much complex real curve look like. So, clearly at x equals to 1 and y 0 x equal to 0 y equal to 0 x equal to minus 1 and y 0 all these represent for x between minus 1 and 0. So, what happens I should ask for that for x less then minus 1 what happens for x less than 1 is it negative, this is negative and this is negative and product is a negative number. So, y square is equal to a negative number and real and there is no solution because x is does not exist because x exists minus 1 where between 0 and 1 same this is power to negative again the curve does not exists between 0 and 1.

So, to eliminate this anything about it, so the curve will look like this something like this, so this part is a closed curve. So, this part is, this is an infinite curve the general no form of a elliptic curve whatone piece which is closed curve one which is infinite curve. Now, these look like ellipse and parabola these are cubic curve not really an ellipse, but it is symmetric alone x axis because of y square. Now, elliptic curves are justprobably the most mark able curves in whole of mathematics it is just unbelievable kind of properties. So, they have and the all arise because of a group structure which sits on this curve one can define, so we look at let see.

(Refer Slide Time: 28:07)



Let $E(\mathbb{Q})$ = set of rational points on elliptic curve E

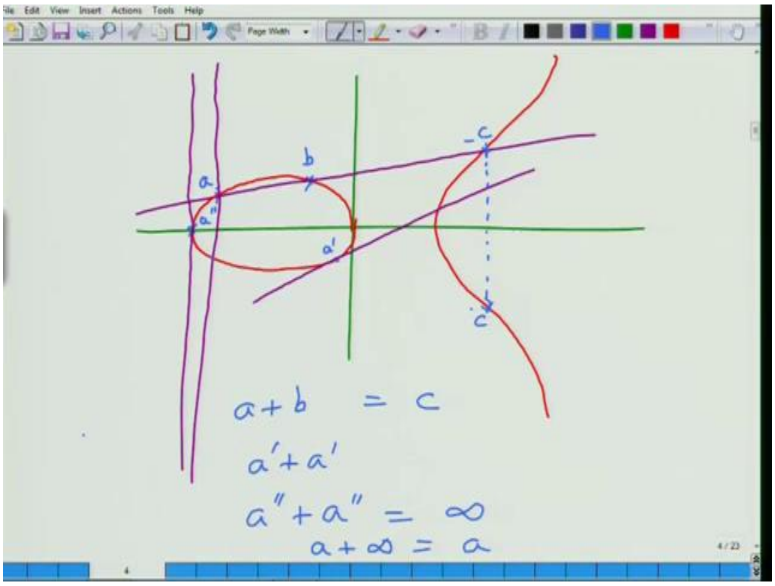
Theorem : $E(\mathbb{Q})$ or $E(\mathbb{R})$ or $E(\mathbb{C})$ alongwith ∞ are groups under $\oplus$ → not usual addition

So, let us take E of Q, so that is our real set, so we can say take any Q is a set of, so we use these notations E of Q to denote the set of rational points lying on the elliptic curve given by E. So, when I say rational point I meant point here the coordinates are rational E of R this is of course can be generalized E of R. So, E of R for the entire curve all the points E of Q is sub set of those points which are rational, so the remarkable property of elliptic curve is that E of Q are E of R.

Now, R when if of gone E of C when even we can put this equation more complex somewhere look at all the complex solutions of this. So, those are complex points laying on the elliptic curve, so these forms a group under addition operation and the addition is not is not usable addition.

So, this is also slightly cheating because E of Q itself does not from a group we have one more to point to this. So, I would say a pointed infinity alone with infinity all three any of the, three basically look at the point and we are throwing one point in pointed infinity. So, it is an abstract entity we I will make it precise later on but a sort of intuitively imagine the point being lying on the curve which is that infinity, now so let me say what is the addition operation to the elliptic curve.

(Refer Slide Time: 30:49)



$a + b = c$

$a' + a'$

$a'' + a'' = \infty$

$a + \infty = a$

Now, that we draw the elliptic curve which I described earlier, so this is the elliptic curve and to add two points. So, let us say this is point a, this is point b we want to add a and b to add a and be the process is draw a line through a and b this line is going to intersect the curve at the third point. So, this is guaranteed why it is guaranteed because it is a cubic curve, so it is guaranteed to intersect. So, the equation of the line is equal to y is equal to some c x n x plus c, so plug that n into y square equal to x cube q plus a x square plus b.

So, we get a cubic in x it has 3 solutions, careful one has to be careful either it has three solution of one solution these are the two possibilities. So, if it has three solutions because its line is running through 2 points we cannot have one solution it should have 3 solutions that is a guarantee. So, third point must exists there is a third point let us call it minus c, the reason I call it as minus c is we will clear anymore and this is symmetric alone the x axis.

So, there is a reflection of this point below which will call c and this point is the addition of a and b, so a plus b equals c. So, this process can be followed and there are some degenerate cases one has to worry about what if this point is here or let us say this the point is I want to add a with itself.

So, let us call it a prime, so a prime plus a prime because it has a group addition it has to satisfy for all pears of it. Then again the geometric answer is simple you draw a tangent on a prime, so this tangent is also guarantee to intersect the curve at second point again reflected. So, these are three intersection scenarios, but there is also one intersection scenario, for example this if you take this point here. Here, we try to develop and if you add a prime with itself by now just what I defined you will draw a tangent at double prime which is going to be a vertical line.

So, it intersects the curve exactly at one point which is the double prime there is no third point it intersects. So, this is where the point infinity comes to our help because this is vertical line going to infinity it is pretend that it intersecting the curve at that infinite point. So, this will only allow when the line is vertical the line is joining two points is vertical then we say that the third point is because any line that joint is that is vertical is not going to intersect a third point on the curve.

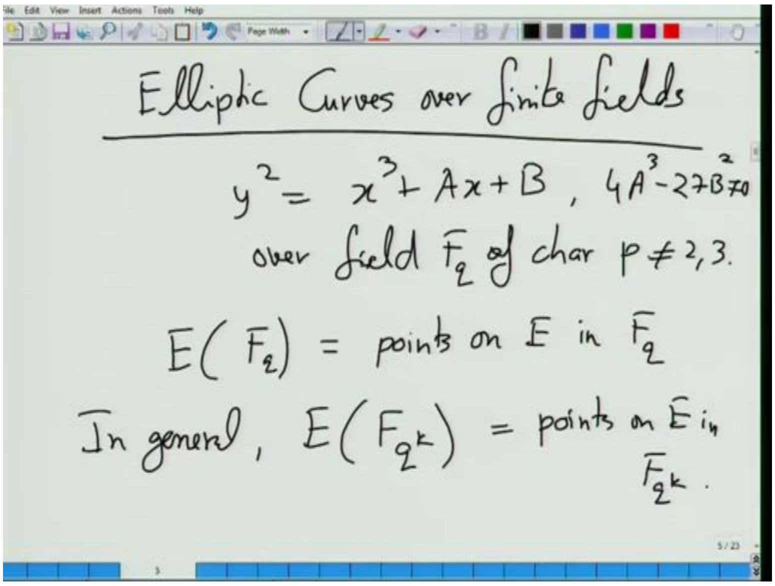
So, that we pretend that is intersecting that at the point infinity here it is prime, but it is not infinity point in infinity is actually unique point. Now, in infinity for this group exact as identity alone, so readable prime is also infinity readable prime is also its own inverse. So, through one can easily verify that infinity is the identity because if you take any point a and add infinity to it you should get point a. So, how do you add a with infinity such infinity associated with the vertical line, so we want to add a and infinity you draw a vertical line at it.

Now, see that is the other point intersect in it will intersect it at this point which is minus a and the algorithm will tell us reflected back reflecting it back you come back to it. So, that is the sum a prime a plus infinity is a and the same thing you can verify infinity plus infinity. So, how do you visualize that infinity plus infinity must be infinity, you just you can visualize it like anything it is like point line intersect line here which is not intersecting it anywhere.

So, that we pretend it as intersecting infinity at 3 times no interesting, yes 3 times as many times as you want. So, these are all de generate cases which you can fix and this geometric realization is just for our own understanding. Now, really one can give much more precise and rigorousalgebraic definitionon to this and they are because some of these things shouldbe in outer which am giving if you look at it algebraically it all works.

So, this is the group that sits on a elliptic curve and there are lots of group which sits on the elliptic curve I have already identified three of them. So, the group holds complex numbers group of real numbers and the group for rational the group of rational points group of real points and the group of the complex numbers.

(Refer Slide Time: 37:10)



Elliptic Curves over finite fields

$y^2 = x^3 + Ax + B$, $4A^3 - 27B^2 \neq 0$

over field F_q of char $p \neq 2,3$.

$E(F_q)$ = points on E in F_q

In general, $E(F_{q^k})$ = points on E in F_{q^k}.

So, one can go further and define elliptic curves or finite fields and again this is simply y square equals to x cube plus a x plus b 4 a cube minus 27 b square equal to 0 not necessarily. So, we can close this algebraic we can get different group from the field curve as we proceed towards the closure. But, just like as in case of real and complex or real are also its defined that is not algebraic equation I can close it to complex somewhere and get another set of points and those set of points also form this.

Similarly, this is our field f of characteristic of p and p I do not want p to be 2 or 3, if p is 2 or 3 then this form of equation does not quite exists. Now, because you see that this gets missed out the y square and x cube these all get missed out, so there are alternatives forms of the curve which are forms the characteristics of 2 and 3. But, for the sake of simplicitywe will not consider them, so let us just concentrate on higher characteristics note that f q need not be the base field the q, q must can be a pretty power of p.

Now, we can define this is a elliptic curve over this field, now we can talk about the set of points which are points on e in f q. So, not only in f q again as already said we can consider not all points may have not all values may nave solution in f q. So, you plug in some value of y, now you get a cubic in x you get three roots not all the three values may be in f q they may lay in the higher field extension fields. So, they will certainly lay in the algebraic function of f q, so generally we can talk about extensions of f q which are of the form k and points laying on the curve which are belong to this field.

So, e of f q is a sub set of f q square e of f q and so on, I am out of time let me just close by saying that the Riemann hypothesis which I am going to show in the next class tomorrow. Then I will prove it in the next class, it is not difficult to do you have to assume some results about elliptic curve. So, that is about it will be about this will be about elliptic curves or the finite fields and will show nice zeta function for such curves.

Now, nice functional equation and lots of properties elliptic curves over rational are a different base they are not very well understood or at least not as well understood as this. But, in fact we do not even know there is corresponding Riemann hypothesis we do not know that hypothesis is true or not we know something. Now, that is to result of this Andrew while rather we know that the zeta function have a functional equation, but that b out it.