Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 29
Elliptic Curve over the Reals

We will talk about elliptic curve over real then I talk about elliptic curve over Z p.

(Refer Slide Time: 00:29)

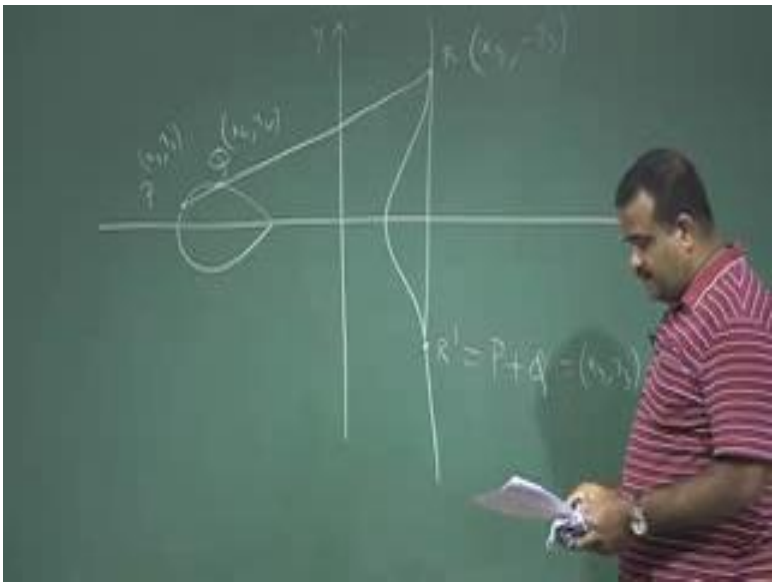
Basically the definition is we take 2 real number a b such that 4 a cube this is the non singularity condition of a of a elliptic curve, this curve is not equal to 0 then we take this equation y square equal to x cube plus ax plus b for this a b and this will give us a elliptic curve over R. So, the collection of the points this x y such that this and a b are coming a b's are coming from R such that this condition 4 a cube plus 27 b square is not equal to 0.

This collection; this is the elliptic curve along with a point which is denote; which is called point at infinity. So, this is denoted by, this is called we will talk about what we mean by point at infinity; point at infinity. So, this is a; this curve is called elliptic curve over R along with this point at infinity and this condition is required in order to have this is called non singular elliptic curve and if this is 0 then that is if 4 a cube plus 27 d square is 0 then it is called singular elliptic curve, singular curve and this is coming from the I mean if we this is the Extremum, I mean like if we take the partial derivative of this, if

we take this, this side and then it is a function of f x y. So, if you take f x y equal to 0, this will give us the solution. So, it is the extreme point condition. So, to have the 3 real roots of this equal to something we will need this condition to satisfy. So, this will ensure that we have third point of intersection with the curve.

Let us draw the curve; let us draw the curve and let us define addition over operation over this elliptic curve points.

(Refer Slide Time: 03:53)



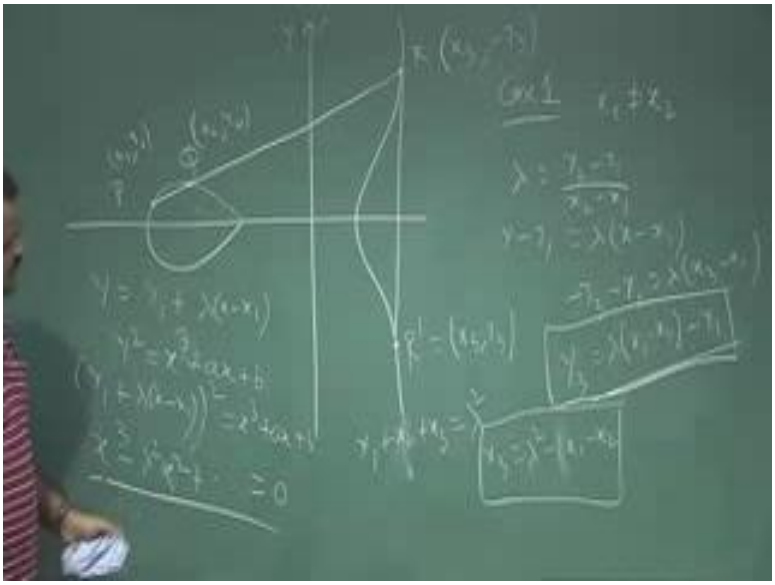
Let us draw the curve. So, suppose this is x axis, this is y axis and our curve is y square equal to x cube plus ax plus b, this is our real. So, if we draw, it has 2 part, this and another part is this symmetric. So, if we draw this equation y square equal to; y square equal to x cube plus ax plus b where we have this non singularity condition of on the a b; that means, we choose a b such that 4 a cube plus 27 b square is not equal to 0. So, this has to part, this one and this one.

Now how we define a addition? So, let us to take 2 points on the curve, P Q. So, this is P this is Q, let us take 2 points P Q on the curve. Now let us draw the line joining P Q and suppose it is touching another point R in the curve and we take the mirror image of R with respect to x axis and this is basically R prime and this we defined as P plus Q, this is how we define the addition over 2 points, P Q. So, we take any 2 points P Q, it could be 1 point is here, 1 point is here, but for simplicity to visualize, we are taking 2 points on here and we join this curve, join; we join the straight line, we draw the straight line

joining P Q. So, it is touching the third; this is the third point of intersection with the curve with this line and if you take the mirror image on this based on the x axis and that is our R; R prime and that is how we define P plus Q, this point.

Now we want to know the coordinate of this P plus q. So, suppose this is P is say x 1, y 1 and Q is say x 2, y 2 and we want to know what is P Q. So, this is x 3, y 3 and. So, this will be then. So, this is the mirror image of this. So, x 3 minus y 3, so, this is just the mirror image based on the x axis. So, now, how to define this? How to get, so there are 3 cases, case 1 is if x 1 is not equal to x 2, I mean if P Q are same and if x 1 is not equal to x 2, P Q are different and if they are; if x 1 is so, there are 3 cases, basically let us just write the cases, we will come back to this picture again.

(Refer Slide Time: 07:34)



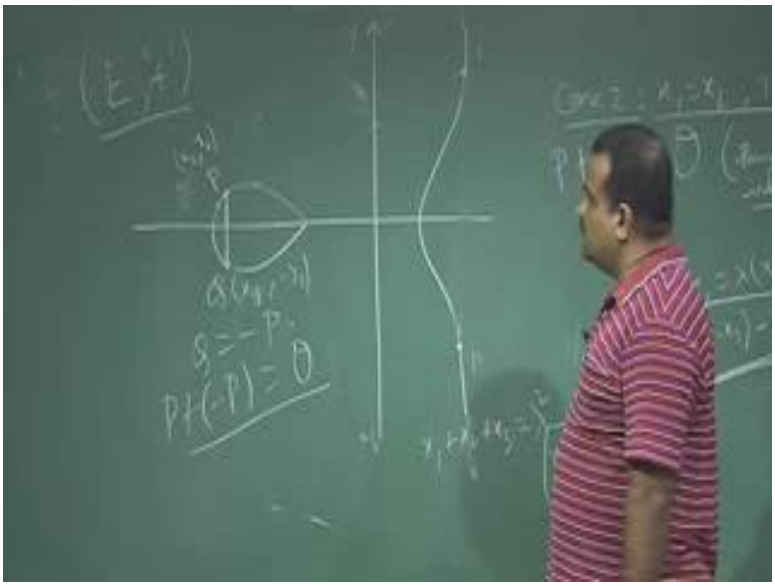
Case 1 if x 1 is not equal to x 2, so in this case, so this is say this is R prime or we came so, this is basically x 3, y 3 then how we calculate x 3, y 3? We can take this, we can take this line and slope of that line is basically lambda is equal to y 2 minus y 1 by x 2 minus x 1, this is the slope of the line and the equation of this line is y minus y 1 is equal to lambda into x minus x 1 and this line is passing through this point. That means, so this is the equation of the straight line and since x 1 is not equal to x 2, this will be a caught. So, this is perfectly so, this slope of this line is y 2 minus y 1 by x 2 minus x 1 and this is the equation of the line and now this line is passing through this. So, if you put this value, we are getting basically minus y 3 minus y 1 is equal to lambda into x 3 minus x 1.

From here we can just write y 3 is equal to so, y 3 is equal to so, we take y 3 is equal to take this, this side lambda into x 1 minus x 3 minus y 1. So, this is 1 equation, based on this y coordinate. So, this is involved x 3. So, now, how to get this x 3? Now if we put this value y in this equation, so this is basically y is basically y 1 plus lambda into x minus x 1, this is y, now this is passing through this curve x 3 plus x plus b. So, we can just put this value y over here y 1 plus lambda into x minus x 1 square is equal to x 3 plus ax plus b.

Now this is a cubic equation in terms of x. So, this is basically so, this is x 3, now this is x 3 and then some term will be in x square. So, this lambda into x square so, if we take this lambda this side so, this will be basically lambda square x square then plus some no order terms equal to 0. So, this is a cubic equation in x. So, it basically has 3 roots and this roots are basically one is x 1, another one is x 2, another one is x 3, these roots of this cubic equation, there are some terms if we just simplify this, we will get the other terms no order term. So, this is x square because this will give us x square. So, there is no x square over here. So, if you take this side, it will be minus lambda square x square. So, this is the cubic equation in x and so, cubic equation means it has 3 roots and these roots are basically x 1, excuse me, x 1, x 2, x 3.

We know some of the roots is basically minus b by a. So, that will give us so some of the roots x 1 plus x 2 plus x 3 is basically minus this by 1. So, this will give us lambda square so; that means, x 3 is basically lambda square minus x 1 minus x 2. So, lambda square minus x 1 minus x 2, this is x 3 and this is y 3. So, this is x 3; this x 3 and this is this x 3 and this is y 3. So, this is the coordinate for the R, plus a P plus Q, if P Q are not equal and P is not equal to minus Q. So, this is case 1 or lambda is this one, this is case 1.

(Refer Slide Time: 13:04)

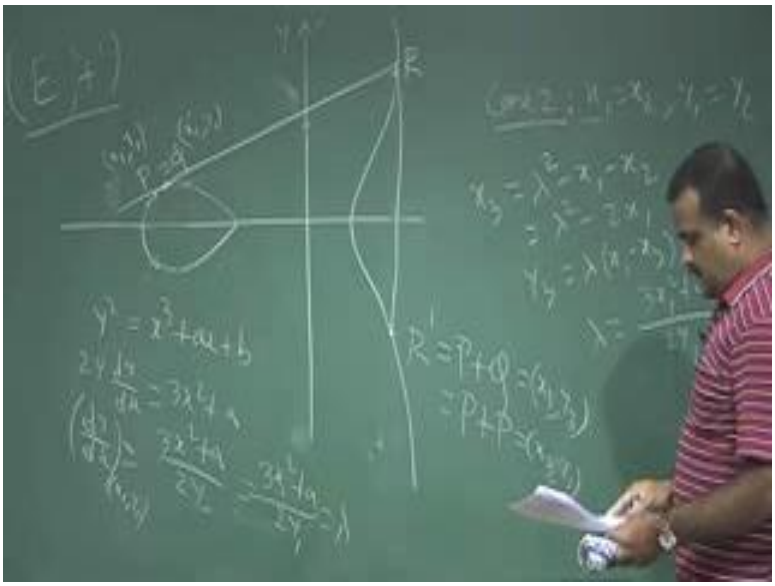


Now, case 2 is telling us so this is Ok no, so you can write case 2. So, case 2 is basically where x 1 is x 2 and y 1 is minus y 2. So, how it is looks like if x 1 is x 2 and y 1 is minus y 2. So, that means, let us just rub this. So, this is the curve we have. So, this is case 2. So, this means P is here P is x 1. So, x 1 this and Q is basically telling us Q is x 2 and minus y 1. So, this is parallel basically x this is x 1 minus y 1. So, this is parallel, parallel to other part of the curve.

Then where is the third intersection because third intersection is the sum. So, where is the third intersection? So, third intersection will be we assume this is at the point at infinity. So, that is why we will take for this case, P plus Q is we define this symbol which is called point at infinity, point at infinity as if they are meeting at infinity because there are parallel to the other part of the curve. So, this is third point of intersection is as if point at infinity. So, this is basically, this Q is basically minus P so, then P plus Q of minus P is basically this.

Later on, we want to see whether this is along with this E; the elliptic curve. So, E along with this will form a group or not. So, for that we need to have the inverse. So, basically and this is the identity element will talk about that, but this is the addition when P is equal to Q is equal to minus p. So, they are meeting at the point at infinity. So, this is case 2.

(Refer Slide Time: 16:05)

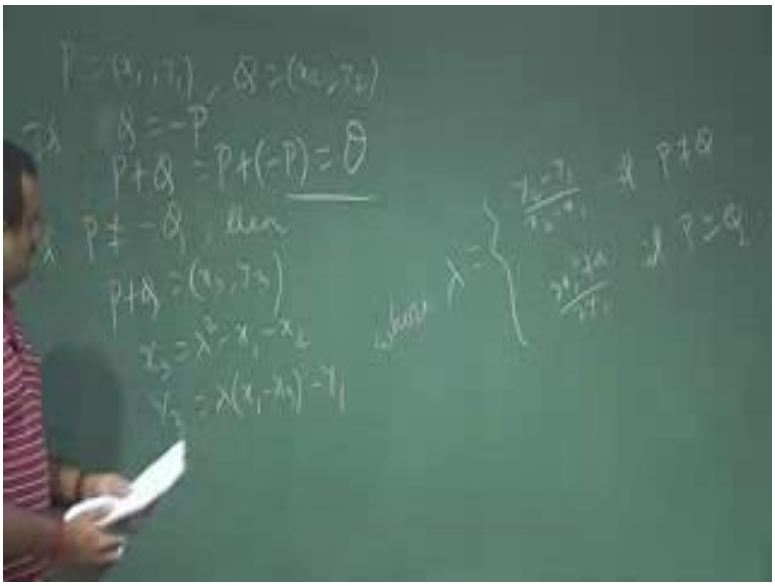


Now, case 3 when they are same, when P Q are same, so when P Q are same, when x 1 equal to x 2 and y 1 equal to y 2, so in this case, so this is P and this is also q, so, this is also x 1 y 1 I mean basically both points are same then it will be a tangent, it is meeting here and this is the other part of the caught. So, this is R and this is R prime which is P plus Q.

Now, if you denote this x 3 y 3 so, this is basically a P plus Q actually P plus P both are same so, in this case, so, what is the x 3 y 3 then? x 3 is basically we know x 3 is lambda square minus x 1 minus x 2, but x 1 x 2 is same, so it is basically lambda square minus 2 x 1 and y 3 is basically I mean the straight line equation, from here we are getting x 1 minus x 3 minus y 1 and here lambda is basically slope of this line, so this is a tangent. So, slope will be d y d x. So, equation is y star equal to x cube plus ax plus b. So, if you do that 2dy dx 2 y; 2 y dy dx is equal to 3x square plus a.

So, dy dx is basically 3x square plus a by 2y. So, dy dx at the point x 1 y 1 is basically 3 x 1 square plus a by 2 y 1. So, this is our lambda for this case because this is a tangent. So, lambda here is 3x 1 square plus a by 2 y 1. So, this is basically P plus Q. So, if you combined this and we can write this. So, there are 3 cases, one first one is P Q at different. So, it is a basically straight line, it is a caught and the second one is there are P Q is equal to minus P then they will meet at point at infinity and third case is this is the case number 3. So, third case is when they are same.

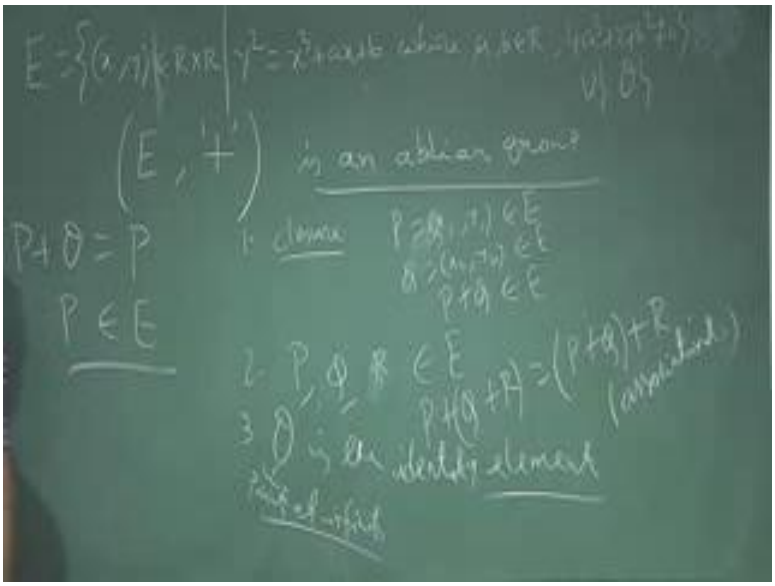
(Refer Slide Time: 19:24)



Let us just summarize this, if P is equal to say x 1 y 1 and Q is equal to x 2 y 2 and how we defined the sum, we defined the sum in this way if P if Q is equal to minus P, then the sum is which is basically P plus or minus P, this is basically theta, this point at infinity and if P is not equal to minus Q or Q is not equal to minus P then P plus Q will denoted by coordinate x 3 where x 3 is nothing but lambda square minus x 1 minus x 2, this is coming from the sum of that 3 roots and this y 3 is equal to lambda into x 1 minus x 3 minus y 1 and where lambda is basically so, where lambda is basically if it is a caught then lambda is y 2 minus y 1 by x 2 minus x 1 if P not equal to Q and if P is equal to Q then it is a tangent then we have 3x minus 4 plus a by 2 y 1, if P is equal to Q then it is a tangent.

This is the formula for finding the P plus Q. So, now, this plus operation we defined over this elliptic curve points.

(Refer Slide Time: 21:37)



We have an elliptic curve E which is basically set of all points such that this is coming from R square R plus R x y, this is elliptic curve over R. So, such that y square equal to x cube plus ax plus b where a b are coming from R such that that non singularity conditions 4 a cube plus 27 b square is not equal to 0 along with a symbol which is called point at infinity.

This along with point at infinity, so this set this is a setup, the points; elliptic curve points. So, this set along with this operation class which is just now seen the question is whether this will form a group or not. So, whether this is forming a group or not in particular with this is an Abelian group or not. So, it can be proved that this is an Abelian group or commutative group, Abelian group. So, if it is an Abelian group. So, prove to prove that we need to have, for group we need to have a closer property closer property means if you take any 2 points P cube from this. So, P is equal to x 1 y 1 from this set E and if you take another point x 2 y 2 from E then P plus Q should also belongs to E so closer property is ok.

Now, the second property for group is associativity. So, associativity means if you take 3 points P Q R or P Q S, P Q R from E then we must able to see that P plus Q plus R should be same as P plus Q plus R. So, this is called associativity; associativity property. So, and this must be true for all P Q R then we have a and this also can be proved geometrically, this is not very straight forward, but it can be proved and then the third

should be the existence of identity element. So, who is the identity element, this phi is the identity element, phi is the identity element, sorry! This phi means point at infinity; this is the point at infinity. So, this sharp as the identity element; that means, P plus this is P and this is true for all P belongs to E.

This is the things and the inverse. So, this is the identity element and the inverse. So, each element should have inverse that is another property for a group. So, each element should have inverse so such that if we do the operation on that inverse, it should give us this group so E identify element.

(Refer Slide Time: 26:02)

For each P we have so, this is the inverse. So, identity 4 is inverse, so, for a P which is say x 1 y 1 then we have Q which is basically minus P which we are telling the x 1 minus y 1 such that we know that P plus of minus P which is identity element. So, this is the inverse. So, every element has the inverse and this is also you are telling Abelian group; that means, it is commutative, commutative means P plus Q should be equal to Q plus P this is quite obvious. So, this will form a group. So, this group this is coming from elliptic curve points. So, E along with this is an Abelian group. So, this is our R.

In next class, we will talk about how we can get these points over Z p.

Thank you.