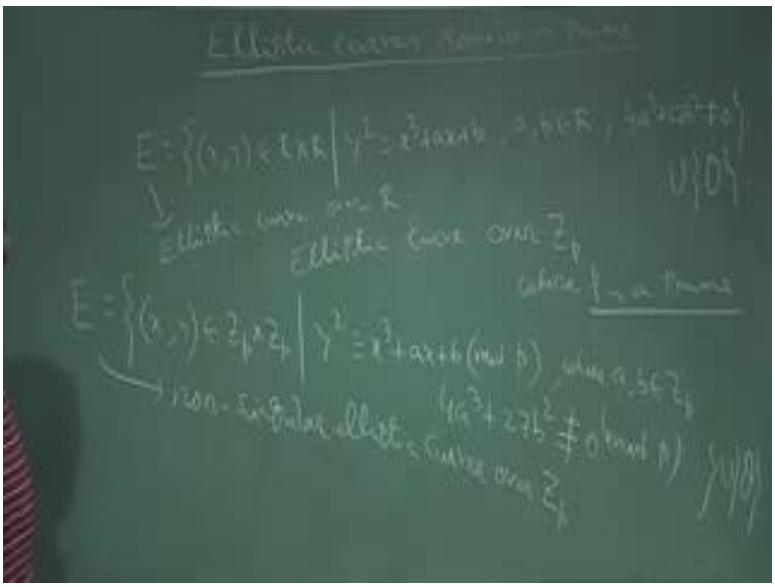
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 30
Elliptic curve Modulo a Prime

(Refer Slide Time: 00:29)



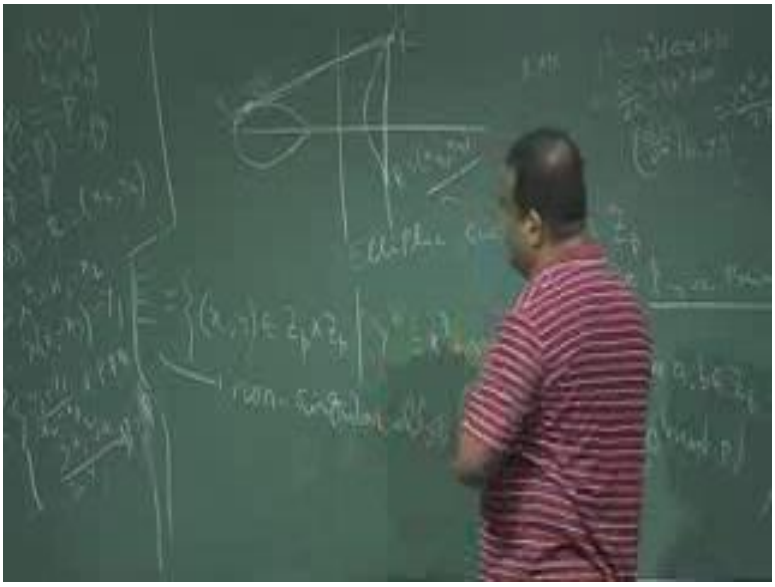
So, we will talk about elliptic curve over a prime Z p. So, elliptic curve points over Z p. So, so far we have seen the elliptic curve over R. So, this is defined as E is the set x, y. So, these are coming from R cross R. So, this is the elliptic curve over R such that y square equal to x cube plus a x plus b where a, b are also real constant satisfy that non singularity condition 4 a cube plus 27 b square is not equal to 0; along with this point at infinity this is the elliptic curve over R, elliptic curve this set is elliptic curve points over R.

So, now, we will talk about elliptic curve points over Z p. So, instead of R, so we want to discuss there is over Z p elliptic curve, points elliptic curve over Z p, where p is a prime, p is a prime number. So, this want to discuss now. So, elliptic curve over Z p similar to this we can define like this, it is the set of all points, there are points x, y such that they are coming from Z p both x and y. And y square is congruent to x cube plus a x plus b, so mod p, so every operation is under mod p. And this a, b; and a, b are coming from Z p

such that this non-singularity condition will satisfied such that 4 a cube plus 27 b square is not congruent to 0 mod p.

So, this set along with the point at infinity. So, this set, and all the points are coming from Z p earlier it was coming from R. So, now our set is from Z p. And these points are satisfying this modulo equation like Y square equal to x cube plus a x plus b mod p and this a, b are coming from Z p again, and we have a non-singularity condition. This is the elliptic curve – non-singular elliptic curve over Z p. So, now if we having this is congruent to 0 mod p then the corresponding elliptic curve is a singular elliptic curve over Z p. What we will talk about non-singular elliptic curve over Z p and we will see that it will form a group under the addition. Like we have seen that this e along with the plus will form a group and under the addition, so we have to define the addition operation over here on the Z p.

(Refer Slide Time: 04:18)



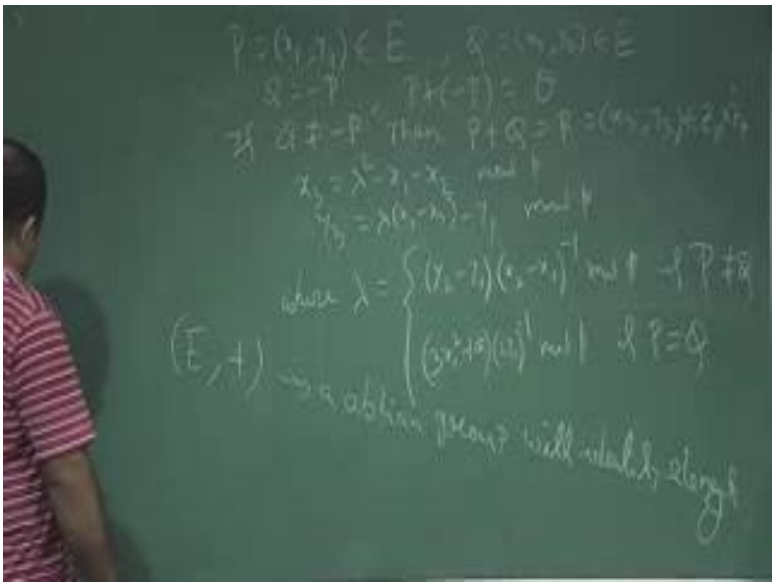
So, let us travel we call the addition operation over R. So, if we are considering this elliptic curve over R then if we take two point P, Q; P is equal to x 1, y 1, and Q is equal to x 2 y 2. And if Q is equal to minus P, we know that P plus or minus P, it is the point at infinity. And if Q not equal to minus P then we know that P plus Q is equal to R which is basically x 3, y 3. And we have the formula for x 3, y 3 like this. So, x 3 is basically lambda square minus x 1 minus x 2; and y 3 is basically lambda into x 1 minus x 3 minus y 1. And lambda is the slope is either it is a cot or the tangent in the curve. So, depending

on whether this P equal to Q or P not equal to Q; P not equal to Q then this will be a call like.

So, this was the picture for R. So, this is the x-axis, y-axis and this is the curve. So, this is two points P, Q. So, this is P, this is Q and this is the third point of intersection and this is our, so if this is R prime this is our R, the mirror image on of this point with respect to x-axis. And this is our x 3, y 3. This is in over R cross R elliptic curve point over R. So, this is basically if P not equal to Q if their different point then this is a cot and then the slope of this is basically 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 they are basically same point, and this will be basically if P is equal to Q they are same point and this will be a tangent on that point. And in that case, we need to take the derivative of this equation y square equal to x cube plus a x plus b. So, 2 y dy dx is equal to 3 x square plus a. 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 basically 3 x 1 square plus by plus a by 2 y 1 if P is equal to Q. So, this is the formula for P plus Q.

Now we want to have the same kind of thing for over this Z p. Now, our points are coming from Z p.

(Refer Slide Time: 08:25)



So, if you take two points from this set of curve, now our points are coming from Z p. So, if you take two points P, Q, x 1, y 1 which is basically from E and Q is also x 2, y 2 which is basically from E. Now, this x 1, y 1; x 2, y 2 are basically coming from Z p. So,

then we define this addition if P is equal to minus Q or Q is equal to minus P then we know P plus this is the point at infinity. Now if P is not equal to minus Q or Q is not equal to minus P then we define the addition as P plus Q is equal to R which is x 3, y 3 which is a pointing Z p cross Z p and which is defined similar to this. So, x 3 is equal to lambda square minus x 1 minus x 2. So, these all operations are under mod p. So, this is mod p. And then y 3 is equal to lambda into x 1 minus x 3 minus y 1 mod p. And now the lambda is basically the slope, but the here points are form Z p. So, lambda will be equal to y 2 minus y 1 then x 2 minus x 1 inverse mod P, if P not equal to Q. And it is 3 x 1 square plus a into 2 y 1 inverse mod p small p, if P is equal to Q. So, this is the formula we have to use to find the addition points of P, Q.

So, this is the addition how we define the addition over two points to elliptic curve points over Z p. And now the question is this will also form a group we have seen that E along with this addition is the Abelian group with the identity element that point an infinity. Now, the question is how we can find the points of the elliptic curve over Z p, so that is the next step we will do. So, how to find the points on the elliptic curve, what are the points.

(Refer Slide Time: 12:18)

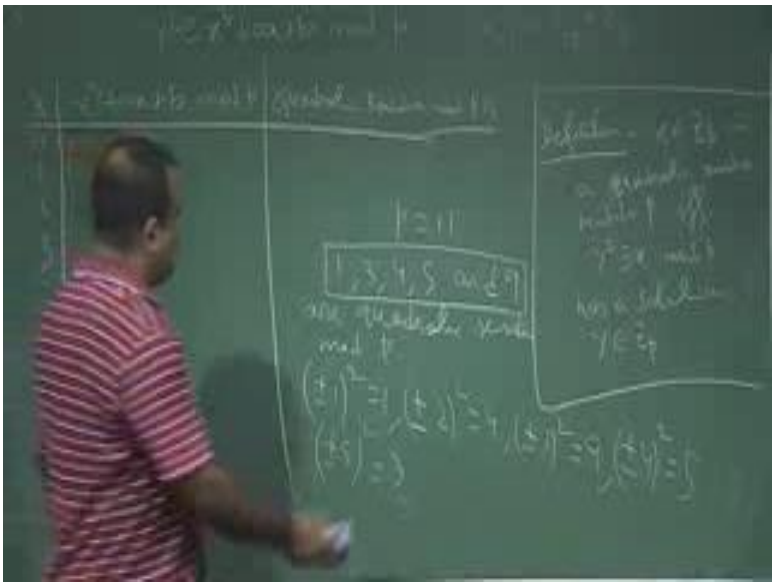
So, suppose we have this elliptic curve y star equal to x cube plus a x plus b curve mod p. So, these x, y's are coming from Z p. So, x is coming from Z p, y is coming from Z p. So, what we do. So, we form a table of x. So, x is Z p means what are the values x can

take, so x can take value 0, 1, 2, 3 up to p minus 1, so 0, 1, 2, 3 up to p minus 1. And then corresponding to x we compute this x cube plus a x plus b mod p. We compute this value by putting these values of x and we have values z 1, z 2 like these are corresponding y's, so y 1, y 2 like this these are corresponding y's.

Now, the question is now we have to check whether this is a quadratic residue or not. So, if you recall the quadratic residue we have to check whether this is a quadratic residue mod p or not so that checking, so we will come to the what is the quadratic residue we have seen that we will again recap that the quadratic residue. So, we check whether this quantity is quadratic residue would not that means, we say x is a quadratic residue. So, this is the definition x belongs to Z p is a quadratic residue modulo P modulo P if and only if y star is congruent to x mod P has a solution y in Z p. So, this is the definition of quadratic residue.

We say a point x from Z p is a quadratic residue if and only if it has a square root sort of. So, if and only if there exists a y such that y square equal to x has a solution in Z p. Now, suppose we take P is equal to 11, for example, if you take P is equal to 11 then we have to check what the quadratic residue under this. So, if you take P is equal to 11, so now, if we just calculate this, so plus minus 1 square is 1 we considered all the points before 11. So, plus minus 5 square is basically 3 plus minus 4 square, so these are all under plus minus.

(Refer Slide Time: 16:08)



So, we can check that they quadratic this 1, 3, 4, 5 and 9, these are all the quadratic residue mod P, for this we have a square root. So, basically that that plus minus 1 square is 1, plus minus 2 square is 4, plus minus 3 square is basically 9. So, 9 is basically again 1. So, 9 is a plus minus 3 square, so sorry it is 9, so this z 11 actually. So, plus minus 4 square, so it is basically 16. So, 16 means 5 and plus minus 5 square like this is basically 25, then it is basically 3 like this. So, if you continue like this we will check we will get only this numbers 1, 3, 4, 5, 9. So, these are the quadratic residue under mod 11. So, these are the points which is having the square root.

Now, the question is how we can check a number is a quadratic residue or not, so that we know we can check this from Euler criteria. So, what is that Euler criteria? This is to check whether a point y is a quadratic residue or not.

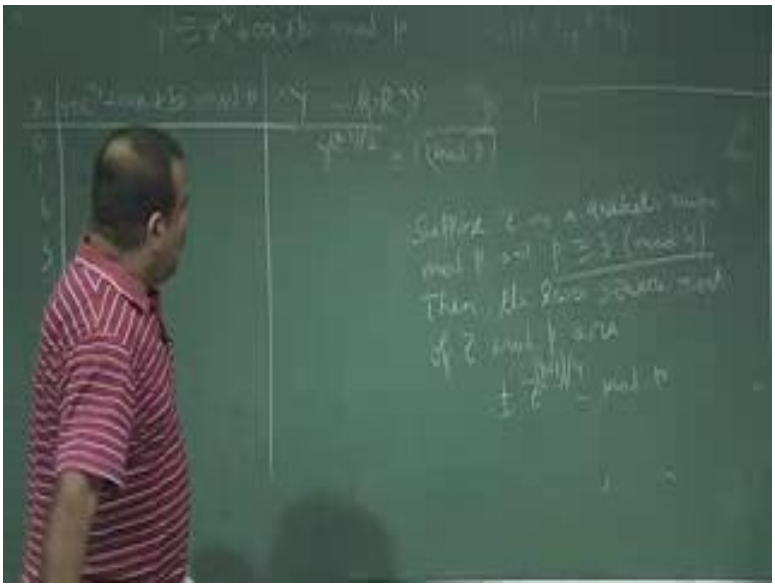
(Refer Slide Time: 18:24)

So, the problem is this to check the quadratic residue, the problem is we have given integer x from Z p and we need to check whether is Z y is a quadratic residue mod p or not. So, this is we can check using what is called Euler criteria. So, this is telling this is theorem x is a quadratic residue mod p if and only if this is the necessary and sufficient condition, if and only if this x to the power p minus 1 by 2 x to the power P minus 1 whole divided by 2 is congruent to 1 mod p or not. This proof of this theorem we have seen. So, this is not to talk to prove, because this is the one way we have seen this

because if we assume x is a quadratic residue that means, x there exists a y such that y square equal to x so that means, we can just put it here.

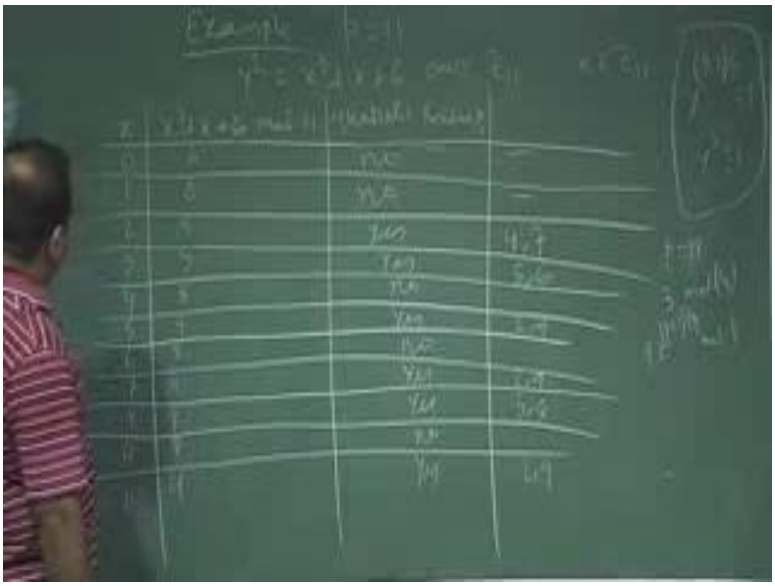
So, y x to the power p minus 1 by 2 is basically y square and y is belongs to Z p and p is a prime. So, y square, so this is basically p minus 1. So, this is basically congruent to 1 mod P by that Fermat's theorem this you have seen. Now, the reverse also true, if this is true then we can show that it has a square root. So, this proof we have seen. So, now, this way we can check whether this is a quadratic residue or not so that means so this is our y, so we have to check that.

(Refer Slide Time: 21:22)



So, we calculate this y, now we have to check whether y is a quadratic residue or not. So, to check this we will use the Euler criteria. We will just check y to the power p minus 1 by 2 whether this is congruent to 1 mod p or not; if this is 1 mod P then it is a quadratic residue otherwise not. So, suppose it is a quadratic residue then how to get the square root. So, here is the theorem, it is telling suppose z is a quadratic residue mod p and p is congruent to 3 mod 4 suppose in particular case then the 2 square root of Z mod P are basically plus minus Z to the power p plus 1 by 4 mod p. So, this is the way we get the square root provided p is in this form. Now let us take an example and we will see how we can find the points over elliptic curve points over Z p. So, let us take that P is equal to 11 and let us take a curve over Z 11 and calculate the points on that curve.

(Refer Slide Time: 23:31)



So, this is an example. So, here we are taking p is equal to 11 and we are taking this curve y square equal to, so you need to choose a b from Z 11 we are taking this curve y square equal to x cube plus a x, a is 1 plus 6 over Z 11. Now what we do? We compute, so x is coming from Z 11, so we compute all the values of for all the values of x. So, x is taking value of 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. So, these are the values x can take. Now, we have to compute this x cube plus x plus 6 mod 11. So, if you put 0 over here, it is basically 6. It is better to draw a separate line for this. So, now, if you put a 1 over here, so this is 1 plus 1 2 plus 6 it is basically 8. If you put 2 over here 2 cube 8 plus 2 10 plus 1, 16, 16 mod 11 this is basically 5.

So, similar way if you calculate we are getting this 3, then for 8, then 4, then for 6 we are getting 8; then for 7 we are getting 4. So, just put the value and take the mod 11; for 8 we are getting 9, and then for 9 we are getting 7; and for 10 we are getting 4. So, these are my y's. Now, we need to check whether this is a quadratic residue or not. So, to check that we need to check this is a quadratic residue or not. So, we need to apply the Euler criteria so that means, we need to check that whether that y to the power p minus 1 by 2 this congruent to 1 mod p or not. So, here p is equal to 11. So, y to the power 5 is congruent to 1 mod p or not. So, we just take this value we to the power 5 and we take mod and we check with that this is 1 or not.

So, if we check that then we can say this is no, this is no, this is yes, this is yes, no, yes, no, yes, yes, no, yes. Now, this is the quadratic residue or not we check using this Euler criteria. Now, we need to find out this square root. So, this is no, this is no, so this is a quadratic residue, so we need to find out the square root. So, square root formula if here p is equal to 11 which is basically 3 mod 4 so that means, square root will be z to the power p plus 1 by 4 mod p.

So, if you do so then we are getting this point as 4 minus 4 and that is basically 7 then 5 minus 6. So, this is 2 comma 9 and this will be again 2 comma 9 and this will be 3 comma 8 and this will be 2 comma 9. So, this is the square root corresponding to this plus minus z. So, for minus, so minus 4 is basically 7, minus 5 is 6 like this. So, we got the points. So, points are basically. So, this is x this is x and we have two option for y. So, these are the point 2 comma 4, 2 comma 7 then 3 comma 5 then these are the points on the elliptic curve.

(Refer Slide Time: 29:09)

So, let us just write the points. So, just quickly let us write the points. So, the points are basically 2 comma 7, then 2 comma 4 sorry 2 comma 7 and 2 comma 4 and 2 comma 4 and then we have 3 comma 5, 3 comma 6, and we have 5 comma 2, then 5 comma 9 and then we have 7 comma 2, and 7 common 9, and we have 8 comma 3, 8 comma 8 and finally, we have 10 comma 2, and 10 comma 9. So, these are my elliptic curve points along with this. This is the elliptic curve that elliptic curve y square equal to congruent to

x cube plus x plus 6 mod 11 so that means so these are the points. So, there are total 13 points. So, there are total 13 points 12 plus 1 - 13 points on this curve.

So, this is the elliptic curve points over Z p over Z 11. Now, the question is how we can from the groups using that points and how we can have a cryptosystem based on this point. So, this will discuss in the next class.

Thank you.