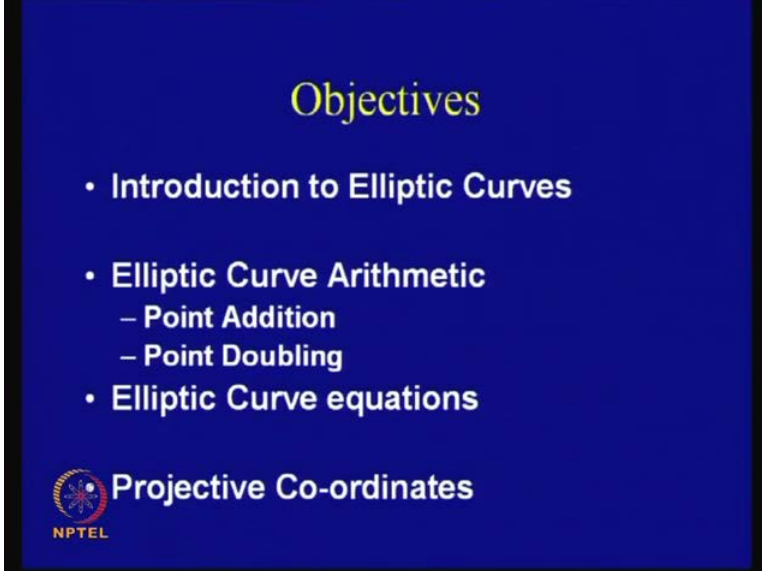


Cryptography and Network Security
Prof. D. Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Module No. # 01
Lecture No. # 34
An Introduction to Elliptic Curve Cryptography


So, welcome to **this** today's lecture on elliptic curves cryptography. So, in continuing with public key ciphers, today we shall discuss about a special type of cryptographic technique, this is actually is employed based upon, **I mean** geometrical interpretations.

(Refer Slide Time: 00:27)



Objectives

- Introduction to Elliptic Curves
- Elliptic Curve Arithmetic
 - Point Addition
 - Point Doubling
- Elliptic Curve equations

 **Projective Co-ordinates**
NPTEL

So, it is a classic combination of algebraic properties with geometric techniques. So, we shall discuss about two fundamental elliptic curve arithmetic operations, namely point addition and point doubling, and then discuss about some of the forms of elliptic curve equations, which are used in cryptography. And then, discuss about projective coordinates, which are often useful for implementing elliptic curves.

(Refer Slide Time: 01:05)


Lets start with a puzzle...

- **What is the number of balls that may be piled as a square pyramid and also rearranged into a square array?**
- **Soln:** Let x be the height of the pyramid...

$$\therefore 1^2 + 2^2 + 3^2 + \dots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

We also want this to be a square:

Hence, $y^2 = \frac{x(x+1)(2x+1)}{6}$

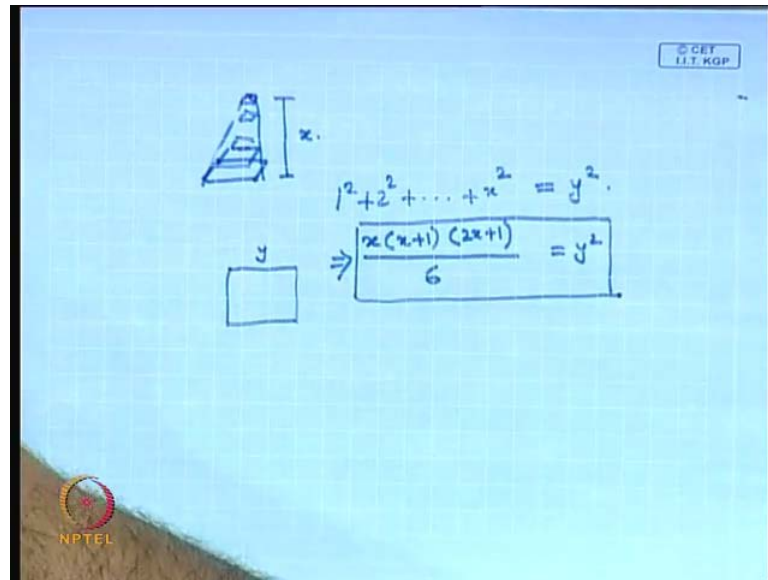


To start with, let us start with a puzzle, that is let us consider this question, that is what is the number of balls that may be piled up as a square pyramid and also rearranged into a square array. So, this problem is a kind of deceptively simple problem, which can be solved easily in this fashion.

That is, let us assume that x be the height of the pyramid, so if you assume that x is the height of the pyramid then, **so we can** we can essentially try to compute the total number of balls in this fashion.

So, for example, if you consider that your pyramid is arranged in various squares, and you start on building up the pyramid, then you can count the number of balls in this fashion, right.

(Refer Slide Time: 01:49)

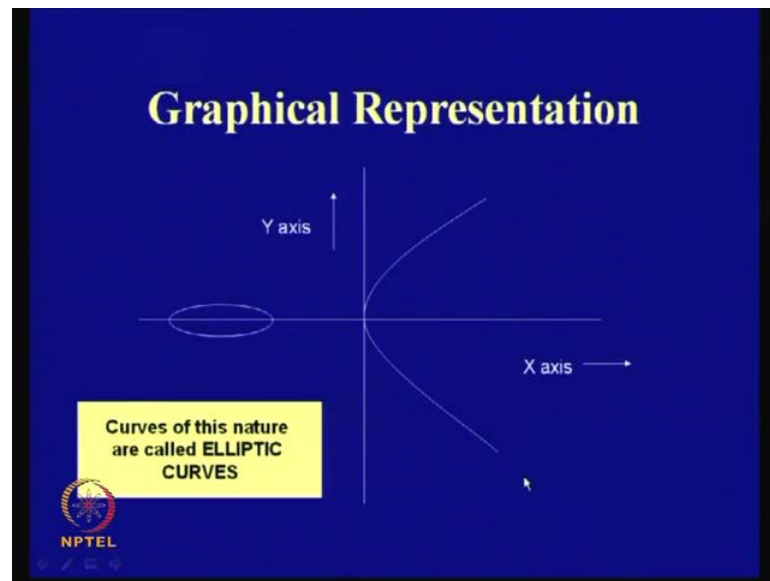


So, you can count, you can imagine that the pyramid is made of squares of balls, and suppose this is the height of the pyramid, and the height of the pyramid is denoted in this case by x , ok. So, what is the total number of balls in the first layer? It is one by one, so it is 1 square, so there are 1 square numbers of balls. In the second, **there** it is 2 square number of balls, so if I continue like this, the last layer has got x square number of balls. So, therefore, total number of balls can be computed in this fashion as 1 square plus 2 square and so on till x square.

Now, these balls by the question can also be rearranged in to square array, so we can actually rearranged these balls and rearrange them in the form of the square. So, the square also has a dimension of y by y and therefore the total number of balls can also be written to be equal to y square.

So, if you solve these two equations, then, therefore we know that the left hand side computes to x into x plus 1 into $2x$ plus 1 by 6 and that is equal to y square. Now, this form of equations is referred to as the elliptic curves, ok.

(Refer Slide Time: 03:30)




So, it may be remembered at this point, that **it has, it** its name actually derived from the word, from the terms elliptic integrals and it has nothing to do with ellipses. So, therefore, if we solve or rather write or rather draw this kind of this graph, then the graph would look like this. So, therefore, we can actually obtain certain, we can observe certain properties.

So, for example, it is symmetric over the x-axis and there are two distinct loads here. So, this is a kind of form, and this is kind of curves, which are commonly known as elliptic curves. So, these are cubic curves in the variable x , and they are also symmetric above the y-axis, this is a kind of distinct property. And purely we see that it has got more similarity with ellipses, so therefore, it should not be mistaken that elliptic curves have got any similarity with ellipses.

(Refer Slide Time: 04:02)

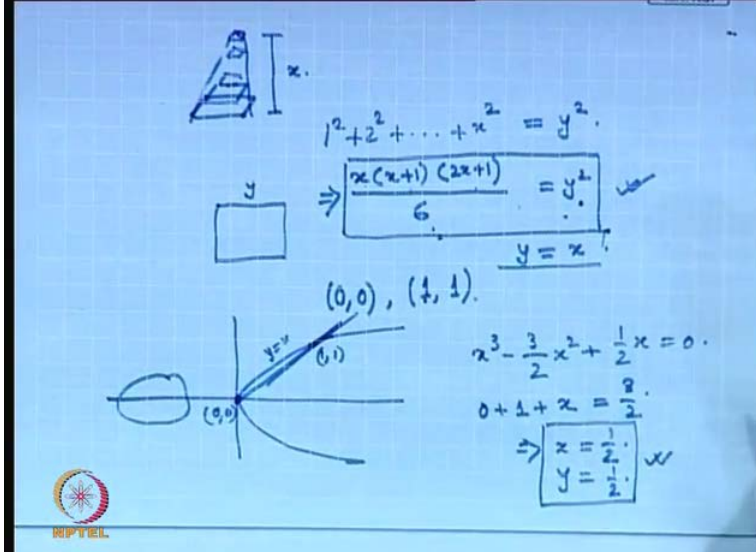
Method of Diophantus

- Uses a set of known points to produce new points
- (0,0) and (1,1) are two trivial solutions
- Equation of line through these points is $y=x$.
- Intersecting with the curve and rearranging terms:
$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0$$
- We know that $1 + 0 + x = \frac{3}{2} \Rightarrow$
 $x = \frac{1}{2}$ and $y = \frac{1}{2}$
- Using symmetry of the curve we also have (1/2, -1/2) as another solution



So, now, there was famous method, which is known as the method of diophantus, which is **which is** often used to, it uses a set of known points to actually produce new points. For example, from this graph, immediately we know that there are two common, that there are two trivial solutions, like for example, 0, 0 satisfies this equation, similarly 1, 1 also satisfies this equation.

(Refer Slide Time: 04:29)



$1^2 + 2^2 + \dots + x^2 = y^2$

$\frac{x(x+1)(2x+1)}{6} = y^2$


$y = x$

$(0,0), (1,1)$

$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0$

$0 + 1 + x = \frac{3}{2}$

$\Rightarrow x = \frac{1}{2}$
 $y = \frac{1}{2}$



It can be easily seen like if i substitute 0 and 0 on both sides, will be satisfied, if we substitute 1, 1, then the left hand side computes $1^2 \cdot 1^2 = 1$ into 2 into 3, that is 6 divided by 6, and the right hand side also 1 square, which satisfies this equation.

Now, starting from these two trivial roots, like 0, 0 and 1, 1, diophantus methods gives us new nontrivial values, which will satisfy this curve equation. So, how does it work? It is like this, so the technique is like this, that is we take a line through these points, like we take 0, 0 and 1, 1, and we draw a line which connects 0, 0 and 1, 1. So, $y = x$ it is easily understood that the equation of the line through these points is $y = x$.

So, now, let us take this $y = x$ and find out where does this line intercept the elliptic curve, because since it is a cubic curve in x , it can be easily seen that if I take two points on the curve and draw a line, then it should definitely meet the curve on a third point. So, therefore, let us try to find out that equation or whether that coordinates of the third point, and it can be found out by substituting $y = x$ into the curve, and the curve therefore takes the form of $x^3 - 3x^2 + x - 2 = 0$, it can be checked and that is equal to 0. So, now, we would like to find out the roots for this equation to obtain the x -axis of the third point, third intersecting point.

So, what we have done is essentially like this, we have taken, suppose this is the curve equation, we start with this point 0, 0, we start with the point that the other point, that is 1, 1 and we draw a line through these two points, and it is believed. Therefore, since it is a cubic curve in x , this should definitely intersect the curve again at another point, and we are trying to find out x coordinate of that point ok.

So, if we do so, that is if we substitute this, then we see that we get this equation $x^3 - 3x^2 + x - 2 = 0$. So, therefore, what we have done is that we have taken this $y = x$ equation of the line, and substituted it into the equation of the curve, which is given by this. So, basically we are trying to solve simultaneously $y = x$ and the equation of the curve.

Now, we know from the theory of the equations that since we know that this equation has got three roots, out of them two of them has got a value of 0 and 1. So, that means, 0 plus 1 plus the third point which we are trying to find out, let us call it x , this should add up to the value of 3 by 2, right.

Because **that is** that follows from the theory of equation, that is if we sum up the all the roots, then it is the negative of the first **first first** coefficient, which is here in this case minus 3 by 2 and therefore, this is equal to plus 3 by 2. So, therefore, from this we get that x is nothing but equal to half, ok.

So, therefore, what is the value of y, since it lies also on the x equal to y line or y equal to x line, therefore y is also equal to half, **right**. So, therefore, you obtain another point, which is 1/2, 1/2 **right**. So, that means, now this is a third point on the curve, and you just see **its is** it is a more kind of, we can say it is a more nontrivial root, then the roots **that which** with which we started with **ok**.

Now, immediately we know that if 1/2, 1/2 is a point on the curve, then by the symmetry of the curve 1/2, minus 1/2 is also a point on the curve **right**, so that means, **that** we know that if 1/2 and 1/2 are points on the curve, then by the symmetry city of the curve, 1/2, minus 1/2 is also a point in the curve.

(Refer Slide Time: 08:23)

$\left(\frac{1}{2}, \frac{1}{2}\right)$ By symmetry of the curve:
 $(1, 1), \left(\frac{1}{2}, -\frac{1}{2}\right) : y = 3x - 2.$
 $x^3 - \frac{51}{2}x^2 + \dots = 0$
 $1 + \frac{1}{2} + x = \frac{51}{2} \Rightarrow x = 24. \checkmark$
 $y = 70 \checkmark$
 $\# \text{ balls} = 70^3 = 4900$

So, now, we shall try to find out, that is, what is the line which joins 1/2, minus 1/2 and 1, 1? We will again similarly continue this approach, and we will obtain further and further points. So, **we** our objective is to obtain further and further points, and ensure that the value of x is an integral value, because if we obtain a value of x, which is an integral

value, then that gives us a nontrivial solution to the puzzle that which we started with, right.

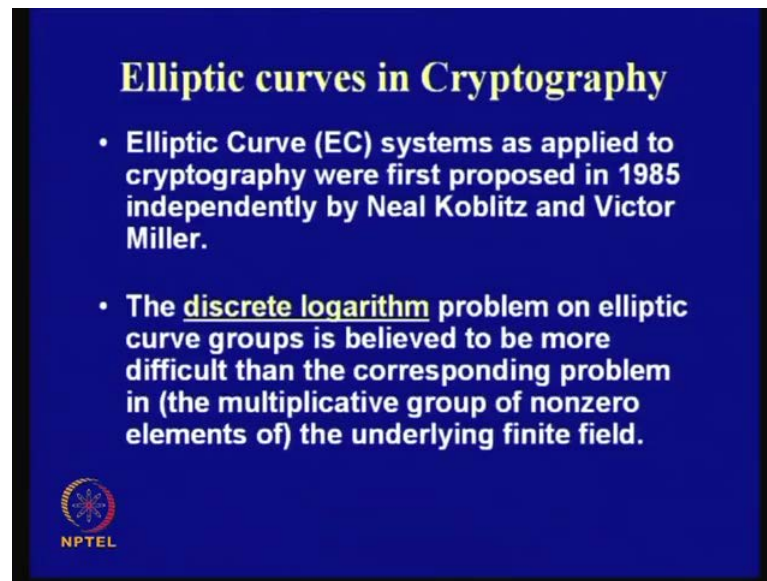
So, therefore, what we do is that we take this $1/2$ and minus $1/2$, and we draw a line through $1/2$, minus $1/2$ and 1 , 1 . So, we already knew that 1 , 1 is your point, we have got a $1/2$, minus $1/2$ point and we want further points. So, what we do is that we take these two points, and we draw a line, and if we can easily check that the line which joins 1 , 1 and $1/2$, minus $1/2$, we will have the equation of y equal to $3x$ minus 2 , ok.

So, this is quite trivial, I am not going through this, but we can obtain the equation of the straight line in this fashion. Now, we will intercept this with the curve again, that is we will substitute y equal to $3x$ minus 2 into the original curve equation, and we obtain an equation, in that in that in that case which has the form of this. So, we are not actually bothered about the higher terms, because what we need is the value of this, right, because we need to find out the value of x .

So, we know that one value is 1 ; the other value is $1/2$, so that means 1 plus $1/2$ plus x should give us 51 by 2 . So, this means that the value of x in this case comes out to be 24 , and if we substitute this value of x into the equation, we obtain the value of y as 70 . So, that means, that we remember that in our case this is, this gives the height of the square pyramid, and this gives the dimension of the square arrangement of the ball. So, this what is the number of balls? Therefore, the total number of balls is therefore, in this case 70 square or that is 4900 , right.


Anyway this is not so important in the perspective of cryptography, but what is important is that using this technique of diophantus you can produce more and more number of points on the elliptic curve, right. And this technique is actually employed in computing arithmetic or performing arithmetic on the elliptic curve points, that is point addition and point doubling, which we will soon we will see. And is the same technique this is still being adopted for elliptic curve operations.

(Refer Slide Time: 11:36)



Elliptic curves in Cryptography

- Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller.
- The discrete logarithm problem on elliptic curve groups is believed to be more difficult than the corresponding problem in (the multiplicative group of nonzero elements of) the underlying finite field.

 NPTEL

So, therefore, now we come into the application of elliptic curve or rather talk about elliptic curves in the context of cryptography. So, this was essentially first proposed or first found in the literature and **in the** on cryptography, in around 1985, developed independently by Neal Koblitz and Victor Miller. And the fundamental problem of on which elliptic curve cryptography is based is commonly known as the discrete logarithm problem, like what we have seen is discrete logarithm problems on finite fields in the last class.

Similarly, we can actually develop elliptic or discrete logarithmic problem on elliptic curve groups, and it is believed to be more difficult than the corresponding problem in the underlined finite fields, and that actually leads to a significant, I mean significant important in cryptography, because this reduces the sizes of the operations **that which that**, which you are doing. And therefore, elliptic curve cryptography is probably the most efficient public key ciphers, at least one of the most efficient public key ciphers that we have seen, and therefore it is quite important.

(Refer Slide Time: 12:45)

Elliptic Curve on a finite set of Integers

- Consider $y^2 = x^3 + 2x + 3 \pmod{5}$
 - $x = 0 \Rightarrow y^2 = 3 \Rightarrow$ no solution $\pmod{5}$
 - $x = 1 \Rightarrow y^2 = 6 = 1 \Rightarrow y = 1, 4 \pmod{5}$
 - $x = 2 \Rightarrow y^2 = 15 = 0 \Rightarrow y = 0 \pmod{5}$
 - $x = 3 \Rightarrow y^2 = 36 = 1 \Rightarrow y = 1, 4 \pmod{5}$
 - $x = 4 \Rightarrow y^2 = 75 = 0 \Rightarrow y = 0 \pmod{5}$
- Then points on the elliptic curve are $(1, 1)$ $(1, 4)$ $(2, 0)$ $(3, 1)$ $(3, 4)$ $(4, 0)$ and the point at infinity: ∞

Using the finite fields we can form an Elliptic Curve Group where we have a Elliptic Curve DLP problem: ECDLP

NPTEL

So, first of all let us try to see some elliptic curves, or let us try to conceptualize how elliptic curve looks like. So, consider this field of modulo 5, that is if you consider the x field to lie between modulo 5 x and y values, to lie between modulo 5, that means it can take the value of 0, 1, 2, 3, 4, and that's it.

So, that means, now we are going to start with some points like x equal to 0, so immediately if I substitute y square equal to 3, you see that in modulo 5 there is no solution, that is if I take the value of say 0, 1, 2, 3, 4, then if I square them, none of them will be equal to 3, so that means there are no solutions for this.

Consider x equal to 1, if you substitute this, you will get x square equal to 6 and therefore modulo 5 this is 1, immediately you know that both 1 and 4 are solutions, because you know that 1 squared is 1, and 4 squared is 16, modulo 5 is again one, so therefore these are solution.

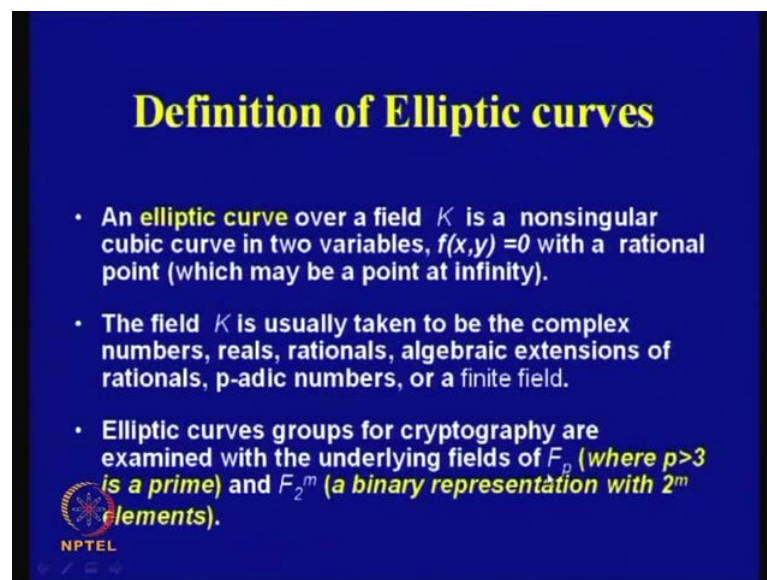
Similarly, you can obtain the other solutions, and what you find is that therefore the points on elliptic curves are actually $(1, 1)$, $(1, 4)$, $(2, 0)$, $(3, 1)$, $(3, 4)$ and $(4, 0)$, so let us now not consider this point the infinity, which I will define later on, but actually we can say these are some discrete points on the elliptic curve.

Now, the reason why we are actually considering this example is to understand that although we are actually drawing continuous elliptic curves, they are actually not

continuous, but they are discrete curves. That is the curves are actually defined on certain finite elements, that is they are not actually continuous curves, but they are actually discrete collection of points.

So, using the finite field, we can actually form a elliptic curve groups, where we have got an elliptic curve discrete lock problems, this is often commonly called as the elliptic curve discrete logarithm problem, but I will define that later on. But first of all let us at least try to understand that elliptic curves on a finite set of integers are actually a cluster of discrete points and not continuous points.

(Refer Slide Time: 14:42)



Definition of Elliptic curves

- An **elliptic curve** over a field K is a nonsingular cubic curve in two variables, $f(x,y)=0$ with a rational point (which may be a point at infinity).
- The field K is usually taken to be the complex numbers, reals, rationals, algebraic extensions of rationals, p-adic numbers, or a finite field.
- Elliptic curves groups for cryptography are examined with the underlying fields of F_p (where $p>3$ is a prime) and F_{2^m} (a binary representation with 2^m elements).

NPTEL

So, a definition as elliptic curve would look like this, that is an elliptic curve **over** is defined generally over a field k , like what we have seen in the previous example, it was defined over the points on, **it was** it was defined over the points on the modulo 5 field, right.

So, similarly it is always defined about a field k , and it is a non singular cubic curve, it is non singular, I will define what is mean by non singular, but it is it is non singular cubic curve, it is cubic curve in x . And in this, **in** generally in two variables $f(x,y)$ is equal to 0 with a rational point, so there is an additional point which is called as a point at infinity. Now, what is the purpose or what is the definition of the point in infinity? You will see soon.

The field k is usually taken to be the complex numbers, real numbers, rationals, algebraic extensions of rationals, p -adic numbers, or a generally a finite field, so it can be various kind of, it can be a various kind of algebra with, I mean, based upon the field k can be defined.

So, elliptic curve groups for cryptography are examined generally with underlying fields on F_p , so it is F_p , means it is a prime field, where P is greater than 3. And it is a prime or it is a binary extension, where there are 2^m elements, that is F_{2^m} fields. So, generally **when** whenever elliptic curves are applied for cryptography, then the underlying fields are either in F_p or in F_{2^m} .

(Refer Slide Time: 16:15)

General form of a EC

- An *elliptic curve* is a plane curve defined by an equation of the form

$$y^2 = x^3 + ax + b$$

Examples

$y^2 = x^3 - 1$

$y^2 = x^3 + 1$

$y^2 = x^3 - 3x + 3$

$y^2 = x^3 - 4x$

$y^2 = x^3 - x$

So, consider this is the very common general form of the elliptic curve equation, which is like this, that is $y^2 = x^3 + ax + b$. So, here this is a plane curve, which is defined by an equation of the form $y^2 = x^3 + ax + b$. Now, note that x here is again not a discrete, I mean it is not a continuous point.

Now, it is chosen from a particular field, so it is either chosen from may be F_p , where it is all prime numbers like 0 to $P - 1$, for a large prime number, or it is F_{2^m} of m , that is where the numbers or the elements can be expressed in certain discrete points again. So, that is chosen from what is known as the binary fields.

So, similar to that, we can actually like, what we have seen previously, we can actually imagine these curves, and these are some common ways of denoting this. Although they note that we have drawn continuous curve equations or try to draw continuous curve diagrams, they are actually not continuous again, they are again done discrete points, which are being joined.

So, for example, consider this line $y^2 = x^3 - 1$, $y^2 = x^3 + 1$, and there are some several points which have been, several graphs which have been drawn. So, what is important here is that this graph is a cubic graph in terms of x , and also this graph or curve needs to be non singular, which means that we have to ensure that the $\frac{\partial f}{\partial x}$, and the $\frac{\partial f}{\partial y}$ are not the same and equal to 0, which means that the graph should generally does not, I mean does not, should not have double roots in it. So, we will see more of that in our future discussions.

(Refer Slide Time: 17:55)

Weierstrass Equation

- A two variable equation $F(x,y)=0$, forms a curve in the plane. We are seeking geometric arithmetic methods to find solutions
- Generalized Weierstrass Equation of elliptic curves:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Here, x and y and constants all belong to a field of say rational numbers, complex numbers, finite fields (F_p) or Galois Fields ($GF(2^n)$).

NPTEL

Now, common or more generalized form of this elliptic curve equation is what is referred to as the weierstrass equation. Now, it is a two variable equation $f(x,y) = 0$, which forms a curve in the plane, and the generalized weierstrass equation of elliptic curves looks like this, that is $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

So, here, you know, we may note that again that the **the** cubic order is **again** again maintained, that is x is again having an order a term of x cube. And the term y has got a power of y square, so this is very important and fundamental to the definition of elliptic curves. So, here x and y and constants all belong to a field again of say rational numbers, complex numbers, finite fields F_p or galois field $G F 2^{\text{power of } n}$. So, cryptography, generally we choose them again from the finite fields or from $G F 2^{\text{power of } n}$.

Now, this weierstrass equation depending upon the characteristic of the field, actually takes various forms. So, the characteristic of a field is actually like, **the** if I take an element say one, and if I add them say lambda number of times, if I get 0, and that lambda is a minimum number of times when you have added, that is commonly referred to as the characteristic of the field.

(Refer Slide Time: 19:32)

The Curve Equations depend on the field

- **If Characteristic field is not 2:**


$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + a_4x + \left(\frac{a_1^2}{4} + a_6\right)$$

$$\Rightarrow y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

- **If Characteristics of field is neither 2 nor 3:**

$$x_1 = x + a_1'/3$$

$$\Rightarrow y_1^2 = x_1^3 + Ax_1 + B$$



For $G F 2$ fields, the characteristic is two, like if I take 1 and I add 1, I get 0; that is the minimum number of times I need to repeatedly add 1 to get a 0 in the binary fields. So, depending upon the field characteristic, its curve equation varies. For example, here what we have done is that, we have taken the original weierstrass equation, and we **are** tried to **kind of** manipulate them using the fact that the characteristic field is actually not 2.

(Refer Slide Time: 19:55)

Ch #2

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \checkmark$$

$$a_1 \left(y + \frac{a_1x}{2} + \frac{a_3}{2} \right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4} \right) x^2 + a_4x + \left(\frac{a_3^2}{4} + a_6 \right)$$

$$Y^2 = X^3 + A_2'X^2 + A_4'X + A_6'$$

Ch #3

$$x_1 = x + \frac{A_2'}{3}$$

$$Y^2 = X^3 + AX + B$$

NPTEL

So, what we have done is that we have started with this original weierstrass equation, which was like $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. So, what we are now doing is that, we are using the fact that the characteristic of the field is not two. And using that we are trying to manipulate this, and write it in this form, like $\left(y + \frac{a_1x}{2} + \frac{a_3}{2} \right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4} \right) x^2 + a_4x + \left(\frac{a_3^2}{4} + a_6 \right)$.

So, do we noted that what we have done is that, we are actually expressed this in this form. So, if I simplify this, again this original equation will be obtained. Now, you note that since the characteristic of the field is assumed not to be 2, therefore we can actually divide **with the** with the number 2, that is important.

So, therefore, if I do so **the** then we can see that this particular term here, that is $y + \frac{a_1x}{2} + \frac{a_3}{2}$ can now I replaced by a single variable. For example, I can replace this by a variable say Y , and I can call it like $Y^2 = X^3 + A_2'X^2 + A_4'X + A_6'$, ok.

So, therefore, this is the same weierstrass equation, but written in a more simpler way, assuming the fact that a characteristic field is, characteristic of the field is not two.

A $1x$ by 2.

Yeah.

Ah y plus a $1 \times y$ by 2.

y plus a $1 \times y$ by 2. So, we yeah. So, we have actually substitute the entire thing by Y , so we can basically... the entire thing is being substitute by y , here yeah, that is why when you take this two then you have got a one $\times y$ term here, right, so therefore, the entire thing is now to being replaced by y here.

Now, similarly you can actually continue simplification in further way, so what you can do is that you can assume now that the characteristic is neither two nor three. So, if we assume that, that you can make further substitutions, like you can, since if you assume that, in this case, we assume that a characteristic is not equal to 2, we make further assumption like the characteristic is not 3, and therefore we can substitute like $x + 1$ is X plus A_2 or rather A_2 dash by 3.

So, if you do that, then this further reduces to the form of Y^2 equal to X , I am just little bit... I am using the notations, but the basic form that it will be reduced to is this. And this is a very common form of the cubic curves, that is we know that it is neither characteristic two field, or neither a characteristic three field, in which you can actually, I mean, under which assumptions you can derive the curve equation in this simple form.

So, therefore, we we can actually start with the original generalized weierstrass equation, and we can actually derive them depending upon the characteristic of the field, we can actually make it more simple and you can write them, right.

(Refer Slide Time: 24:18)

Points on the Elliptic Curve (EC)

- Elliptic Curve over field L

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 + \dots = x^3 + \dots\}$$

- It is useful to add the point at infinity
- The point is sitting at the top of the y-axis and any line is said to pass through the point when it is vertical
- It is both the top and at the bottom of the y-axis

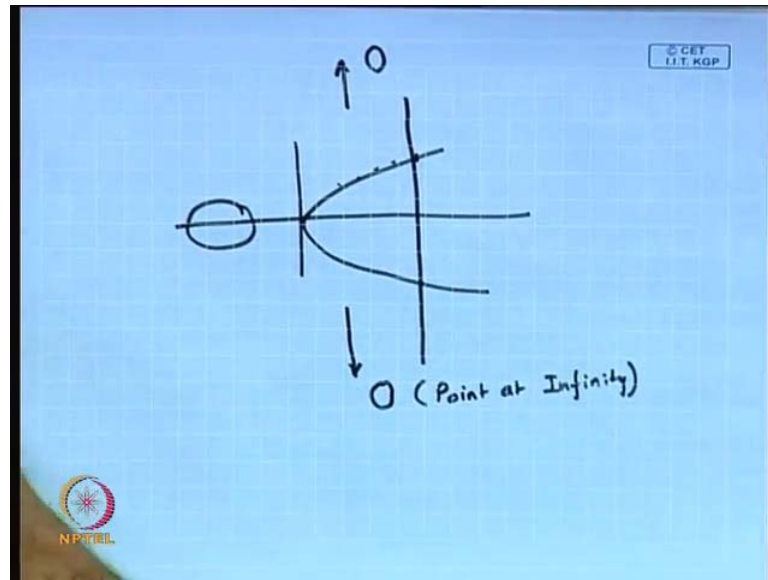
NPTEL

So, therefore, now what are the points on the elliptic curve can actually be written in a more formal way, you can say that the points on the elliptic curves, say call it an elliptic curve e , which is defined over a field which is l , to be the collection or the union of the of a point at infinity, and the or the other pairs of x, y , which belongs to l cross l , because x also belongs l and y also belongs to l .

So, therefore, it is a subset of the l cross l , the cartesian of l and l right, and all of them, I mean both x and y satisfies the original curve equation, where there are definitely these two things like y square on the x cube terms, the rest of the things may vary depending upon the characteristic of the curve.

So, it is useful to add the point at infinity, and we will see more clear in a closely y , the point is sitting, **the** this point of the infinity is a kind of point, which is generally believe like you sitting at the both the top of the y -axis and also bottom. So, therefore, it is it lies kind of at both the spaces.

(Refer Slide Time: 25:19)



So, therefore, for example, if I draw a point or rather draw an elliptic curve, an elliptic curve would essentially look like this, and it would be compassed with, encompassed with various points which lie on the curve, but we assume that there is a point which is both at the top and both at the end, and this point is also commonly known as the o point, or the point at infinity, the same point, this point o is also at the top.

So, therefore, if I draw vertical line, then we know that by the original **diophantus** technique what we have seen is that, if there are two points, and if I draw a vertical line, then it should also intersect the elliptic curve again at a third point **right**, but in this case, since it will not actually intersect on the elliptic curve, we assume that it intersects the elliptic curve again at a point on infinity and that is the concept of the point o.

So, therefore, it both at the top and at the bottom of the y-axis, and any line is said to pass through this point when it is vertical, so any vertical line will intersect this point at infinity, which is also assumed to lie on the elliptic curve based on this definition, **ok**.

And it is a very useful point, because it helps us to define the concept of a group, because it helps us to create a group, which is very much needed in order to apply this elliptic curve for various applications, right.

(Refer Slide Time: 26:42)

The Abelian Group

Given two points P, Q in $E(F_p)$, there is a third point, denoted by $P+Q$ on $E(F_p)$, and the following relations hold for all P, Q, R in $E(F_p)$

- $P + Q = Q + P$ (commutativity)
- $(P + Q) + R = P + (Q + R)$ (associativity)
- $P + O = O + P = P$ (existence of an identity element)
- there exists $(-P)$ such that $-P + P = P + (-P) = O$ (existence of inverses)

NPTEL

So, let us see some of the reasons why the elliptic curve should form an abelian group. Now, this is slightly a recapitulation of the abelian group and we know that given two points P and Q , which lies saying E of F_p , so it is an elliptic curve, it is defined about the say finite, say on the plane fields.

Then there is a third point, which is denoted by P plus Q , which also lays on E of F_p , that is if I take P and if I take Q , we have to define an operation, call it a class operation, or an addition operation on these two points, such that it also lies on E of F_p , that is it should be closed, right and the following relations also has to hold for all P, Q and R , which lies on E of F_p .

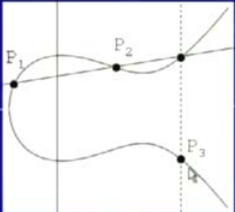
So, what are the fundamental requirements? The first thing is the commutativity property, that is we know that if I add P and Q , this should be the same as adding Q and P , it also should satisfy the property of associativity, which means that if I take P plus Q , and then I add R , it is a same as giving P and adding it to the sum of Q and R , **ok**.

That is, it does not matter in which order we are doing the addition operation. Similarly, there should be an identity element, that is if I take P and if I add O , then I should get back, and it is the same as O plus P , because of the commutativity property, and both of them should actually go back to P , that is there O , that is essentially here with the identity element, and O is generally referred to as the point of infinity.

So, that means, the point of infinity is assumed to be the identity element in the plus operation that we are trying to define here. Similarly, **the** I mean another point is that there exists a minus P, such that if I take P and I add minus p, that is the additive inverse of P, then I should get back O, that is the point on infinity again. So, therefore, minus P is the additive inverse of P.

(Refer Slide Time: 28:36)

Elliptic Curve Picture



- Consider elliptic curve
 $E: y^2 = x^3 - x + 1$
- If P_1 and P_2 are on E , we can define
 $P_3 = P_1 + P_2$
as shown in picture
- Addition is all we need

NPTEL

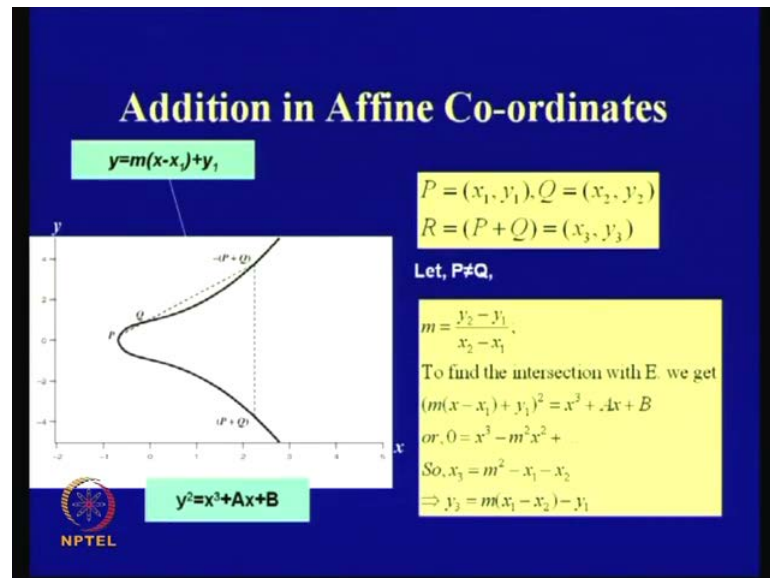
So, let us try to see how we can do this operation. So, consider an elliptic curve $y^2 = x^3 - x + 1$, this is the form of an elliptic curve that we have chosen here. So, if P_1 and P_2 are two points on this curve, so consider that there is another point called P_3 , and let us try to define an addition operation on P_1 and P_2 , **ok**.

So, what we essentially expect by the diophantus technique is that if I take P_1 and P_2 and draw a straight line through this, it should intersect the elliptic curve on a third point like. So, do the same technique which we had, what we have seen in context to solving the first puzzle that we started with, **right**.

So, now, for our addition purpose, instead we do not take this as the sum, but we take the reflection of this point on the x-axis as the sum, that is we call P_3 to be the sum of P_1 and P_2 . So, we take P_1 and P_2 , and remember that when we started with was taking $(0, 0)$ and $(1, 1)$, and it intersected the curve at a point $(\frac{1}{2}, \frac{1}{2})$ and instead of telling $(\frac{1}{2}, \frac{1}{2})$, we

actually took the point of $1/2$ minus $1/2$. So, this has got a very close relationship with the diophantus technique, right, so we take this point and we draw this line.

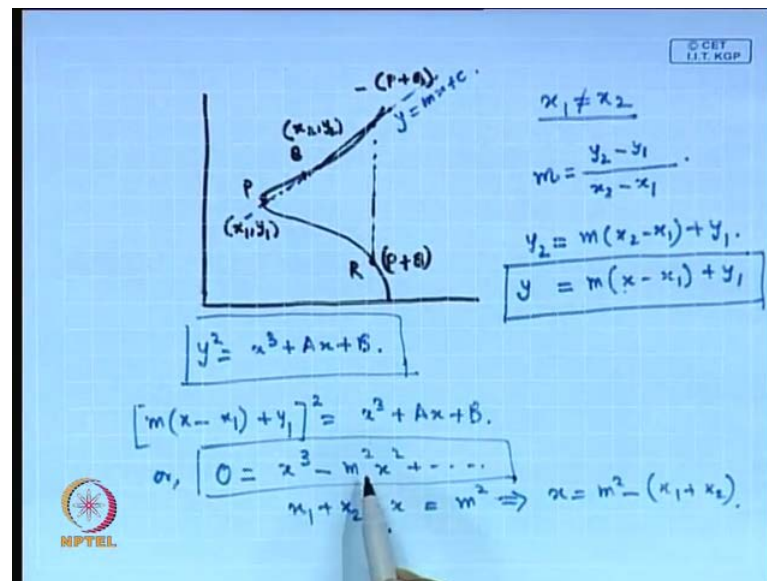
(Refer Slide Time: 29:47)



So, now we will try to make it more formal, so therefore immediately you understand that. If I tell that P 3 is a sum of P 1 and P 2, and then we can actually obtain the ordinates of P 1 of P 1 plus P 2 by using the techniques of coordinate geometry.

So, that actually, I mean motivates us to apply coordinate geometric techniques here. So, consider that there is a point p, and there is a point Q, and the point P at Q, and Q have got the ordinates as shown in the diagram as x_1, y_1 and x_2, y_2 .

(Refer Slide Time: 30:25)



So, what we have to telling is that we have got say a curve, and this curve has got two points, say one point is P, the other point is Q, and we are considering this line, that is the sum of P and Q. So p, the ordinate of P is x_1 , y_1 and the ordinate of Q is x_2 , y_2 , and it is intersecting the curve again at a third point, so call it minus P plus Q, because you will consider the reflection of these point on the x-axis as the sum of P plus Q.

So, therefore, this point is the point R, which is the sum of P and Q. So, what we do is that we actually consider the slope of this line first, that is considering the slope of this particular line, which is actually used to join this P and Q. So, therefore, call this line as some line like y equal to $m x$ plus c , ok.

So, what is the value of m here, which is the slope? m is immediately obtained as y_2 minus y_1 divided by x_2 minus x_1 . So, therefore, of course, here when you are writing the m like this, we are making an assumption that x_1 and x_2 are not the same. So, under these assumptions we know that we can write the value of m like this.

So, now we will try to find out the intersection of this line with the cubic equation. So, we started with the cubic form and the equation of the curve is like y^2 equal to x^3 plus $a x$ plus p . So, what we do is that we take this and we substitute this that is we take y_2 as m into x_2 minus x_1 plus y_1 , so is that straight away

from the equation. So, we know that if in this equation, if there is a point which has got a coordinate of x or ordinate of x , then the y ordinate is obtained by this, right.

So, therefore, if we substitute x here, this is the corresponding ordinate for y . So, we can take this y and substitute this in the equation right, so that means that we can actually take this and this, and we can combine these two equations, and we can write them as $m^2 - x_1 + y_1^2 = x^3 + ax + b$, right, we can write them in this form. And therefore, we can actually rearrange them, and we can write them as $0 = x^3 - m^2x + \text{some more terms}$, which we are not actually bothered with. So, again you see that there is a very close similarity with the diophantus method, right.

Because, what we are now doing is that we have and we know that there are two points x_1 and x_2 , and the third sum, if I believe it to be x , right is if I add these two things I get m^2 , so that means that x is nothing but $m^2 - x_1 + x_2$ right. So, if I know that this particular curve is satisfied by three experts because of the cubic thing, right.

So, two of them are x_1 and x_2 , the third point if it is x , then if I add them, then it is nothing but the minus of minus m^2 , which is m^2 that is x , is nothing but $m^2 - x_1 + x_2$, right. So, we take this x , and that is why my essentially the ordinate of the of the third point of minus P plus Q ok.

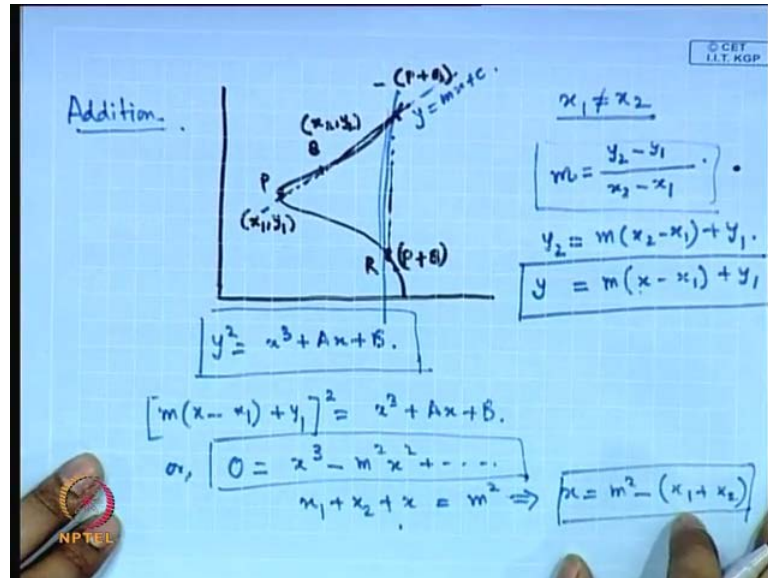
So, that is the way, I mean, so therefore we know that if we can obtain this point, similarly we can obtain the x coordinate of this one also, because it is the same, right. The x -axis is the, it is since we are taking a reflection here, this point x x value and this point's x value are the same x values.

So, therefore, the x is given by this $m^2 - x_1 + x_2$, where m is actually obtained by this equation. So, if we combine this, this will essentially look like this, that is I will come to this actually later on, I mean, the combined form do you know when we summarize the results.

Now, the obvious question is what about the case when P and Q are actually the same point. That is if the point P and Q are actually the same point, then we cannot write an m

value like this, right. So, the obvious answer to this is, since we are drawing a tangent here we do a differentiation, **right**, we tend to, we differentiate the value of **of** y with respect to x to obtain the corresponding equation of the tangent **ok**.

(Refer Slide Time: 35:34)



So, what we do is that we take this line, that is **y square equal to** $y^2 = x^3 + Ax + B$, which is the equation of the curve, and we draw a line, like we what we do is that we take a line and write $2y \frac{dy}{dx}$ is nothing but $3x^2 + A$ right. So, therefore, $\frac{dy}{dx}$ at the point at any point x_1, y_1 is defined as $\frac{1}{2} \frac{3x_1^2 + A}{y_1}$ divided by 2 of y_1 .

That means that if I take this equation of the curve here, then if I draw a tangent here, and the tangent is defined at the point of x_1, y_1 then this is the slope **which is we are** which we are defining here, right. So, therefore, this becomes the slope of this tangent, **right**

So, therefore, now the question is, **that is what** how do I **[actu/actually]** actually obtain the third point. So, therefore, after this we can do a similar technique as what we have seen previously, and we can actually obtain the ordinate of the third point, right. So, what we do is that we again assume that this particular equation $y = mx + c$ is substituted $y = mx + c$, is substituted into the curve equation, ok.

And we again solve for the three point sum, and we obtain the coordinate of the third point. So, in this case, if I do so, then again I get this form like 0 equal to x cube minus m square x square plus so on. So, therefore, in this case the two points that is x plus x, if I take that this point is x 1, y 1, so it is 2 x 1 actually, x 1 plus x 1 plus the third point is x sums to m square, like what we have seen previously. So that means that x is nothing but m square minus 2 of x 1, where m is actually obtained by 3 x 1 square plus A divided by 2 y 1, right.

So, therefore, this is the way how we can actually obtain the value of x, and similarly again we can draw reflection of the of this point and obtain the corresponding some point right, of this of the same x and y. So, actually this particular I mean way of obtaining the third point is called there is a doubling of two points, the this is actually commonly called as a doubling, this particular operation, whereas this is called commonly as the addition operation or the point addition operation. And these are actually forms two fundamental operations of the elliptic curve, of elliptic elliptic curve cryptography.

(Refer Slide Time: 38:13)

Doubling of a point

- Let, $P=Q$

$$2y \frac{dy}{dx} = 3x^2 + A$$

$$\Rightarrow m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

If, $y_1 = 0$ (since then $P_1 + P_1 = \infty$).

$$\therefore 0 = x^3 - m^2 x^2 + \dots$$

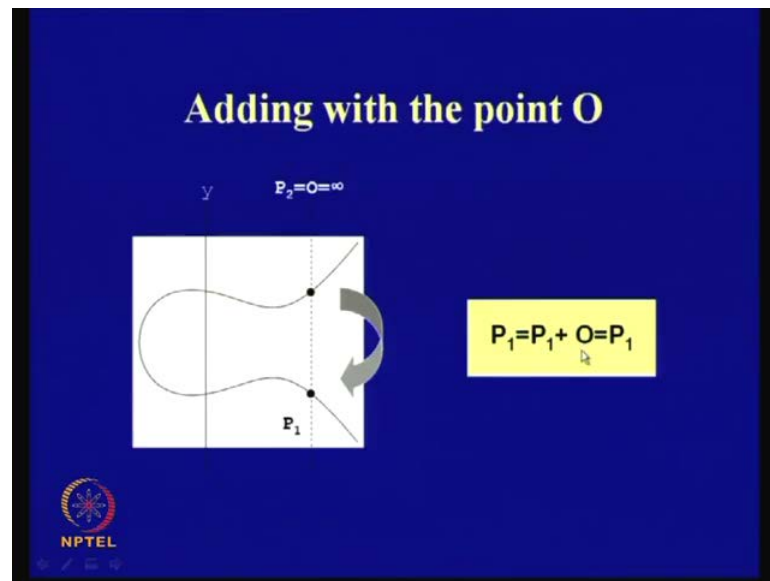
$$\Rightarrow x_2 = m^2 - 2x_1, y_2 = m(x_1 - x_2) - y_1$$

- What happens when $P_2 = \infty$?

NPTEL

So, now, we again have this question like what happens when P 2 is equal to the point at infinity, then what happens. So, that means that what we are saying here is that, we will take P 1 and the second point is the point at infinity.

(Refer Slide Time: 38:18)



So, we basically what we do is that we take P_1 and we draw a vertical line through P_1 , and therefore it intersects the P_1 at the the third point. So, what we need to do after this is, we need to reflect this point, and if I reflect this point then we get back the value of P_1 .

So, therefore, this is actually I mean, means that the point at infinity satisfies whether behaves as the, it it behaves as what the group property should should should, would want it to satisfy, right.

That is, O is essentially serving as your you're your inverts, because we are adding P_1 to O , and you are getting back the value of P_1 . So, therefore, this means that the point at infinity with the additional point of infinity, we are actually ensuring that the point on the elliptic curve satisfies the group properties.

(Refer Slide Time: 39:20)

The Abelian Group

Given two points P, Q in $E(F_p)$, there is a third point, denoted by $P+Q$ on $E(F_p)$, and the following relations hold for all P, Q, R in $E(F_p)$

- $P + Q = Q + P$ (*commutativity*)
- $(P + Q) + R = P + (Q + R)$ (*associativity*)
- $P + O = O + P = P$ (*existence of an identity element*)
- there exists $(-P)$ such that $-P + P = P + (-P) = O$ (*existence of inverses*)

NPTEL

So, actually there are, there is a, so what we fundamentally required is these four properties, we need that it should essentially satisfy the property of commutativity, which follows from the way the addition has been done, because if I draw two lines it does not matter which way you are drawing it. Similarly the point or rather the existences of an identity element is also understood by the way what **what** we saw just now.

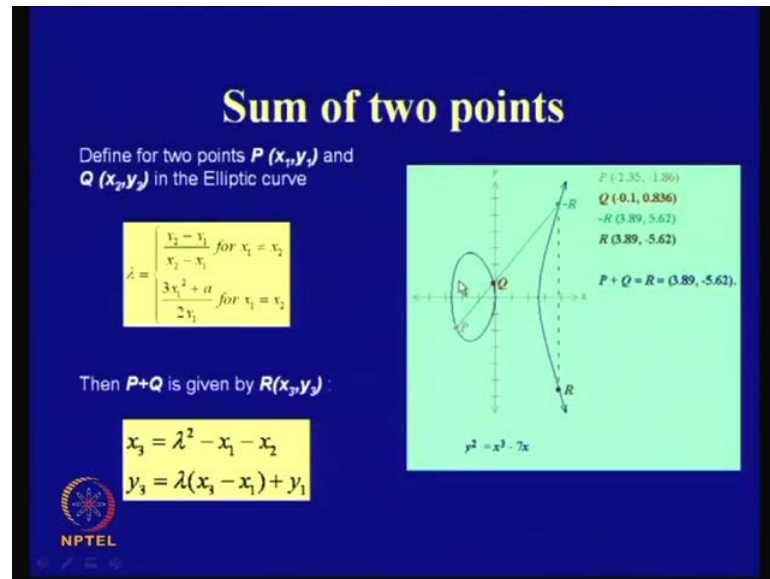
Similarly, the point of inverse is also understood, because if you take P and minus P , it will again intersect the point at infinity, if you reflect that point at infinity, you still get that infinity, because **the** it is assumed that the point infinity exist both at the top and both at the bottom, **right**.

But what is not so obvious is this **associativity...** why it is associative also? But, this is actually a quite lengthy proof, and it is actually beyond the scope of this discussion. So, therefore, we will assume that it also satisfies the associativity property, and therefore the elliptic curve elements **at**, where the elliptic curve points satisfies the group properties or **or** other forms a group, forms an abelian group on that the addition operation.

And how is the addition operation defined? Now, we take two points, and we draw a straight line through it, intersect if there any third point, reflect that point on the x-axis to obtain the corresponding sum, or if the point P and Q are the same, then we draw a

tangent through that point, again obtain the **the** point of intersection, reflect that and obtain the corresponding output. So, that is the corresponding, either how we do a P plus Q, where P and Q are different, or we do Q P, or that is how we do the **addition proper[ty]**- addition operation or how we do the doubling operation. So, that is how it is defined, **ok**.

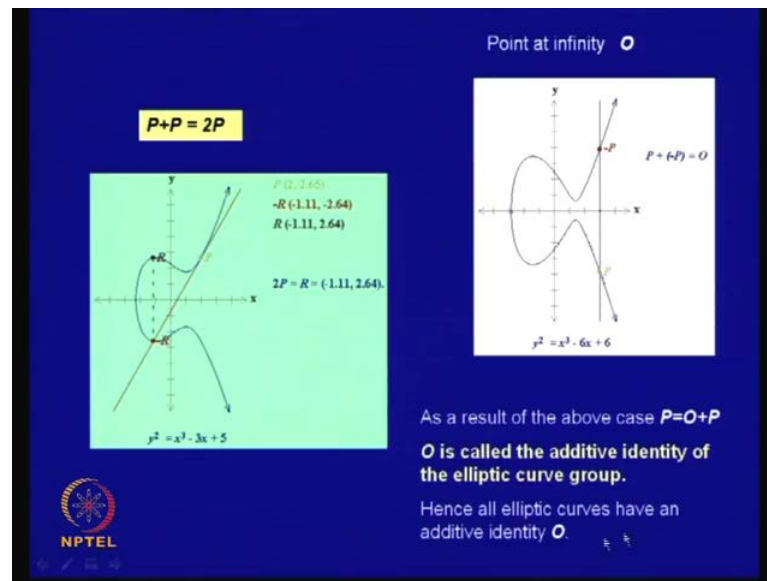
(Refer Slide Time: 41:06)



So, therefore, this is a summary of what we have seen, that is if that points are different, that is if I take two points like x_1, y_1 and x_2, y_2 in elliptic curve, then your slope is defined like this, where x_1 and x_2 are not the same, but if x_1 and x_2 are indeed the same, then this is the way the slope is defined, and for both these cases your third point is actually $\lambda^2 - x_1 - x_2$, and the corresponding y ordinate is obtained like this.

So, therefore, we users take this and you substitute this and obtain the corresponding y sum. So, this is a cryptographic description, **of** you take P and Q, you add it, it intersects at the third point R, you again reflect that point to obtain the corresponding R. So, therefore, you can actually engage coordinate geometry to do this operation.

(Refer Slide Time: 41:57)

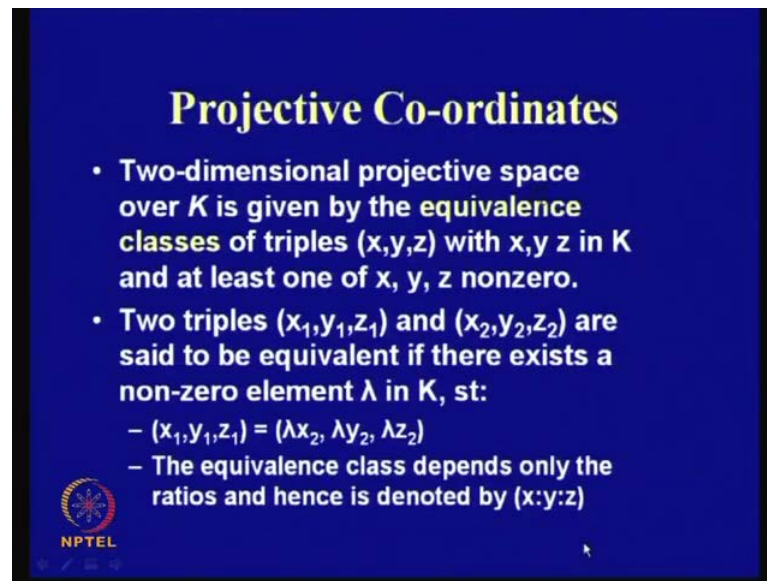


Similarly, for **for** other cases like this, so this is a case of a doubling operation, like we take a P point, and we do want to do a 2 P operation, **we are we are** what we have done is that we have considered a tangent at this point, intersects at a point R, meant of reflecting it to obtain the corresponding some value. So, therefore, this can be similarly performed.

So, this is again like doing P plus minus P, so therefore you take P and you add with this additive inverse minus P, it intersects at the point at infinity, and the point at infinity is, if we again reflect this, we again obtain point at infinity.

So, as the result of the above cases, you have got this property. So, O is called the additive identity of the elliptic curve group, and hence all the elliptic curves have an additive identity O.

(Refer Slide Time: 42:48)



Projective Co-ordinates

- Two-dimensional projective space over K is given by the equivalence classes of triples (x,y,z) with x,y,z in K and at least one of x, y, z nonzero.
- Two triples (x_1,y_1,z_1) and (x_2,y_2,z_2) are said to be equivalent if there exists a non-zero element λ in K , st:
 - $(x_1,y_1,z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$
 - The equivalence class depends only the ratios and hence is denoted by $(x:y:z)$

NPTEL

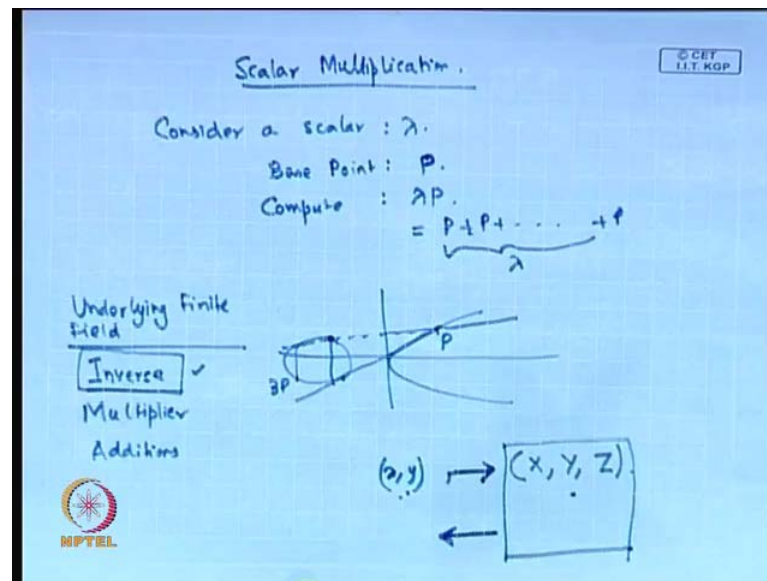
So, now we will come to the concluding part of this that is talking about, discussing about projective coordinates. Now, we shall see in our few **unix** linux class, that when we discuss that, when we are actually talking about the scalar operations, then what we essentially need to perform is repeated additions and repeated doubling.

Now, because of this, we essentially, **we** I mean if we try to understand the elliptic curve operations that are underlying, we have actually **to** perform the finite field arithmetic operations, like we have to either perform finite field multiplication, finite field addition, finite field inverses and such kind of operations.

So, therefore, if you **if you** want to make our implementations efficient, which is also very important, it is important that the underlying field operations need to be done in a clever way, that is we need to minimize the underlying field operations.

So, one of the most complexes underlying field operations is the multiplicative inverse. So, therefore, it is always an objective of how when we are implementing or finite elliptic curve scalar multiplication, is actually by repeatedly **is by** reducing the number of inverses. Now, **what is** scalar multiplication is like, is defined like this.

(Refer Slide Time: 44:11)



That is, see consider a scalar quantity, which is defined as lambda. So, what we are interested in, is in performing, so we consider a point or base point p , and we are interested in computing λp , that is we need to multiply this P with this scalar quantity called lambda.

So that essentially we know that we can do it by doing P plus P and so on lambda number of times that is we can perform this addition lambda number of times. That means if I take or start with an elliptic curve, and I take another a point p , then the first in which I have do is P plus p .

So, that means I need to draw a tangent through this, and this intersects the curve at a point, you take a deflection, this becomes twice p . So, now we take this, and we want to add this with further p , so that means that I take this, and I again intersect this line with this point p , this again intersects the curve at a third point, we again take its deflection, that becomes $3p$, right, so we continue this process, right.

That is we performed repeated additions or repeated doublings on additions to compute the value of λp . Now, there is, I mean we can actually do it in a efficient way, like by as we have seen in the case of raising value to its exponent, we have used the square and multiply in a if we in order to do it efficiently. Similarly, here we can actually engage a double on addition algorithm to do this efficiently.

But that we will see in the next class, but what is important to understand is that, when you are doing this $P + P$ or P plus a third point as different point, then underlying operations which we are doing actually encompasses finite field, multiplies finite fields inverses and so on.

So, what is important is that when you are doing this operation, it is to reduce the cumbersome operations, **right**. So, what we will try is if we consider that **the underlying**, the underlying finite field operations, the underlying finite field operations, because elliptic curve is always defined on a finite field **right** in this case. So, therefore, the underlying finite field operations are inverses multipliers and additions. So, if we assume that this is the most cumbersome operation, then our objective will be to reduce these inverse operations as much as possible.

So, in order to do that, there is a very effective transformation of the elliptic curves, which is from the affine coordinates, that what we have seen into a coordinate system, which is called the projective coordinate systems, which is actually very helpful in reducing the number of inverse operations.

So, what we do here in this projective coordinate system is that, instead of considering a point x, y , we actually elaborate this and consider a point has to be made up of three important component that is x, y and z , **ok**.

So, it is assumed that various points which are actually lying on the curve, or instead of having two ordinates, have got three ordinates x, y and z . And this transformation from the affine coordinates to this projective coordinates, so what we first do is that we take the affine coordinates, transform it into the projective coordinates, perform all the operations in a projective coordinates, and then finally again bring it back to the affine coordinates.

Now, what has been seen is that in this process the number of inverses gets completely removed, that is when you are doing your addition and doubling operation in the projective coordinate system, then it is completely divide of the multiplicative inverse. It is **made of...** multiplications are required, but there are no multiplicative inverses which are employed here.

But of course, when you are doing this final transformation back into the affine coordinate, you require to do one finite field inverse operation at that point. That means, that the entire purpose, or entire efficiency of these coordinate, system transformation is that we are actually reducing the number of multiplicative inverse at the cost of some extra multiplication operations.

So, therefore, more formally this looks like this, that is the two dimensional projective space over k is given by the equivalence class of triples x, y, z , with x, y, z in k and at least one of **where** where, at least one of this x, y, z is non zero, **ok**. So, therefore, this essentially is actually made up of equivalence classes, so x, y, z these are the three points, and they are actually equivalent **when** under certain conditions, that is with x, y, z in k and at least one of the x, y, z being non zero.

Now, **when do** we say that two points like x_1, y_1, z_1 and x_2, y_2, z_2 are equivalent, we say two triples like this to equivalent, if there exists a nonzero element λ , which is also in k , such that x_1, y_1 and z_1 is equal to λx_2 into λy_2 into λz_2 , that is if I take x_2, y_2 and z_2 and multiply each of them by λ , I get the **I get the** second point, **ok**.

So, therefore, it is also commonly referred or this equivalence class, is actually defined only by the ratio of x, y and z and therefore, it is also commonly referred or written as x is to y is to z , which indicates that we are actually interested in the ratio of the x ordinate, y ordinate and the z ordinate.

So, therefore, **all the all the** all such triples where this ratio is maintained are actually believed to, belong to one particular equivalence class, if there is another point which also maintains a ratio, then that belongs to another equivalence class. So, similarly, you can actually divide your entire coordinate or rather entire set of points into equivalence classes, so that is how it is defined.

(Refer Slide Time: 50:28)

Projective Co-ordinates

- If $z \neq 0$, $(x:y:z) = (x/z:y/z:1)$
- What is $z=0$? We obtain the point at infinity.
- The two dimensional affine plane over K :

$$A_k^2 = \{(x, y) \in K \times K\}$$

Hence using,

$$(x, y) \rightarrow (X : Y : 1)$$
$$\Rightarrow A_k^2 = P_k^2$$

There are advantages with projective co-ordinates from the implementation point of view

NPTEL

So, for example, I mean continuing further, like if z is not equal to 0, then you can always write x is to y is to z as same as that of x by z is to y by z is to 1, because that also maintains the same ratio, right, here x is to y is to z here and here are the same.

But what about the point at z equal to 0, then you **can** cannot write like this, **right**. So, therefore, **it is** we obtain, so we say that this is the point at infinity, so we obtain the point of infinity if we do like that. So, therefore, the two dimensional affine plane, so what we have seen previously was this, that is x, y was the corresponding affine plane, and that we defined, and x also belongs to k , and y also belongs to k , so therefore, the ordered pair x, y is the subset of the cartesian product of k and k , **right**.

Now, if we use a transformation like this, where we transform this x and y to x is to y is to 1, there actually this gets transformed into the projective coordinate system. That means, what we are trying to say here is that the A_k^2 and the P_k^2 , both of them **are actually** you can actually define a 1 to 1 relationship, **right**. You can transform any element here into this, and you can actually take any element here and **and** convert it back into the affine space. Now, there are some advantages as I told you, is that with projective coordinates which we will see in the next class also, there are certain distinct advantages of using projective coordinates, that is it reduces the number of inverse operations, which are required from the implementation point of view, **ok**.

(Refer Slide Time: 51:58)


Sum of two points

Define for two points $P(x_1, y_1)$ and $Q(x_2, y_2)$ in the Elliptic curve

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{for } x_1 \neq x_2 \\ \frac{3x_1^2 + a_1}{2y_1} & \text{for } x_1 = x_2 \end{cases}$$

Then $P+Q$ is given by $R(x_3, y_3)$:

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_3 - x_1) + y_1$$

 NPTEL

That is, for example, **if you need**, if you see these operations like when we have considered these equations, then instead of, when we are **when we are** performing this right, that is all of them are finite field elements. So, therefore, we need finite field squarers, we need finite field multiplies, we need finite field division operation, which is nothing but based **based** on finite field inverse operations.

So, the objective of transforming into the projective space and then performing operations is to reduce the number, is **to** basically it is to reduce the number of multiplicative inverses. So, that is the objective of y, I mean **one of the impor[tant]**- one of the important advantages of transforming a elliptic curve system into projective coordinates and performing the operations in the projective space.


(Refer Slide Time: 52:40)

Singularity

- For an elliptic curve $y^2=f(x)$, define $F(x,y)=y^2-F(x)$. A singularity of the EC is a pt (x_0,y_0) such that:

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$$

or, $2y_0 = -f'(x_0) = 0$
or, $f(x_0) = f'(x_0)$
 $\therefore f$ has a double root

 It is usual to assume the EC has no singular points

So, I would like to, just going to make some comments about the **about the** similarity of an elliptic curve, so for an elliptic curve y square equal to $f x$, **where we defined**, we can actually find out the similarity in this fashion, that is you actually rewrite the equation as $F(x, y)$ is equal to y square minus $f x$, and a singularity of the elliptic curve is a point x_0, y_0 such that your $\Delta f \Delta x$ and $\Delta f \Delta y$ are the same, **ok**.

So, we actually find out $\Delta f \Delta x$ with **respect...** so this is basically differentiate this curve y square minus $f x$ with respect to x . So, if we do so, then we actually obtain, so we can actually do that, similarly **we can also** we also differentiate this in **respective** with y . For example, here we differentiate, if we differentiate this with respect to y , what do we get? We get $2 y$, right, so we get $2 y_0$, because that is the point. So, what we are doing is that, we get x , because in that case, the effects if we differentiate this with respect to y , that is 0 . So, therefore, we get $2 y_0$ and the other thing is $f x_0$ minus $f x$ is here. So, what we are doing is this, that is we are taking the curve $F(x, y)$ and that is equal to y square minus f of x , we are differentiation Δf with respect to Δx , so Δf with respect to Δx will be equal to $2 y_0$.

(Refer Slide Time: 53:52)

$$F(x,y) = y^2 - F(x).$$
$$\frac{\partial F}{\partial y} = 2y_0 \quad \frac{\partial F}{\partial x} = -F'(x).$$
$$2y_0 = -F'(x) = 0.$$
$$f(x_0) = f'(x_0) = 0.$$

Similarly, your del f with respect to, sorry del f with respect del y, del f with del with respect to del x will be minus of f dash x, **right**. So, therefore, here what we are saying is that $2y_0$ and minus of f dash x is equal to 0 at the singularity point. So, we say that $2y_0$ is equal to minus f dash x equal to 0, now when we are saying that $2y_0$ is 0, that is y_0 is equal to 0, it means that y_0 square is also 0, **right**. That means, **your** if you substitute this in this graph right, then it means that your $f(x_0)$ is also equal to 0, that means we can write that... **f** we can write $f(x_0)$ and $f'(x_0)$, both are equal to 0 here. So, **that** that is why we call this point at singularity as a double root, where it **is** also satisfy this and also the differentiation is satisfied, **ok**.

So, if you draw a curve like this, which has actually **has** got a singularity point and then you will find that it is quite distinctly defined from the other elliptic curve operations. So, it may have something like this kind of edge over there, **right**, so it is this point basically.

(Refer Slide Time: 55:27)

If Characteristics of field is not 3:

$y^2 = f(x) = x^3 + Ax + B$

- Hence condition for no singularity is $4A^3 + 27B^2 \neq 0$
- Generally, EC curves have no singularity

Mathematical Derivations:

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$$

or, $2y_0 = -f'(x_0) = 0$
or, $f(x_0) = f'(x_0)$
 $\therefore f$ has a double root

$$y^2 = x^3 + Ax + B$$

For double roots,
 $x^3 + Ax + B = 3x^2 + A = 0$
 $\Rightarrow x^2 = -A/3$
Also, $x^4 + Ax^2 + Bx = 0$,
 $\Rightarrow \frac{A^2}{9} - \frac{A^2}{3} + Bx = 0$
 $\Rightarrow x = \frac{2A^2}{9B}$
 $\Rightarrow 3\left(\frac{2A^2}{9B}\right)^2 + A = 0$
 $\Rightarrow 4A^3 + 27B^2 = 0$

NPTEL

So, it is evenly assumed that the elliptic curve has got no singular point. So, therefore, I mean, we can go through this, and we can find out that if we go through this, then if we assume that f has got double roots, then if we take this x cube plus Ax plus B , and the for double roots, therefore we know that we will actually equate the differentiation of this equation with respect to x , this is $3x^2 + A = 0$, and therefore your x^2 is minus $A/3$ from this equation, right.

So, if you substitute this, therefore you know that $x^4 + Ax^2 + Bx$ is equal to 0, because that is also a root right. So, therefore, if $x^3 + Ax + B = 0$, you can always multiply this by x , and that is still 0, right. So, therefore, you get $x^4 + Ax^2 + Bx = 0$, if you take this, and now substitute this one into this, then you get a square by 9 minus A^2 by 3 plus $Bx = 0$ and therefore, $x = \frac{2A^2}{9B}$.

So, now, if you take this value of x , and substitute back into this equation of $3x^2 + A = 0$, then you get that $4A^3 + 27B^2 = 0$. Now, this is commonly referred as the discriminant of an elliptic curve, that is, what we have seen in quadratic equations, we know that when it as when the discriminant is 0, then the two roots are same.

Similarly, in cubic curves, when f has got double roots for the singularity conditions, that it satisfies four A cube plus $27 B$ square, is also equal to 0.

(Refer Slide Time: 57:00)

Elliptic Curves in Characteristic 2


- **Generalized Equation:**

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
- **If a_1 is not 0, this reduces to the form:**

$$y^2 + xy = x^3 + Ax^2 + B$$
- **If a_1 is 0, the reduced form is:**

$$y^2 + Ay = x^3 + Bx + C$$
- **Note that the form cannot be:**

$$y^2 = x^3 + Ax + B$$


 NPTEL

So, this we can prove in a slightly different way also, but I mean one of the very important curve equation is for characteristic two, and it is useful for implementations. So, we can consider again the weierstrass equation, and depending upon the facts right, we can actually again modify and we can actually reduce it into various forms, like one of the various very common forms is again y square equal to x cube plus Ax plus B .

(Refer Slide Time: 57:32)

Points to Ponder

- **Suppose that the cubic polynomial $X^3 + Ax + B$ factors as $(X - e_1)(X - e_2)(X - e_3)$. Show that $4A^3 + 27B^2 = 0$ iff two or more of e_1, e_2 and e_3 are the same.**
- **Sketch the curves:**
 - $E_1: Y^2 = X^3 - 7X + 3$
 - $E_2: Y^2 = X^3 - 3X + 2$
 - note that the curve E_2 is not an elliptic curve. It has a singular point.

 NPTEL

So, I am not going into these detailed deductions or it can also be done in the similar fashion, as we have seen for the other characteristic. Now, I just throw some points to think on, like we have thought about the discriminant point, so you see that, suppose that the cubic polynomial, this is factored as this, then we can actually show that $4A^3 + 27B^2$ is equal to 0, if and only if two and more of the E_1 , E_2 and E_3 are the same, so you can actually reduce both the curve equations and this one, and **and** compare the coefficients. If you simplify, you will again get back these equations, this is another way of proving the discriminant that is if two roots are same, then you'll get this equation to be satisfied.

The other thing is that we can sketch these two curves, and we can note that the second curve E_2 is actually not an elliptic curve, because it has a singular point. So, if you do this, you will get one feel about the singular point, the singularity of the curve.

So, we stop at this point, and here are some of the references that I have used in my video, so I have used the stinson's book and the washington's book and also this book. And in next day, we can actually discuss about the applications of elliptic curves to cryptography.