

Hardware Security
Prof. Debdeep Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 19
Hardware for Elliptic Curve Cryptography – I

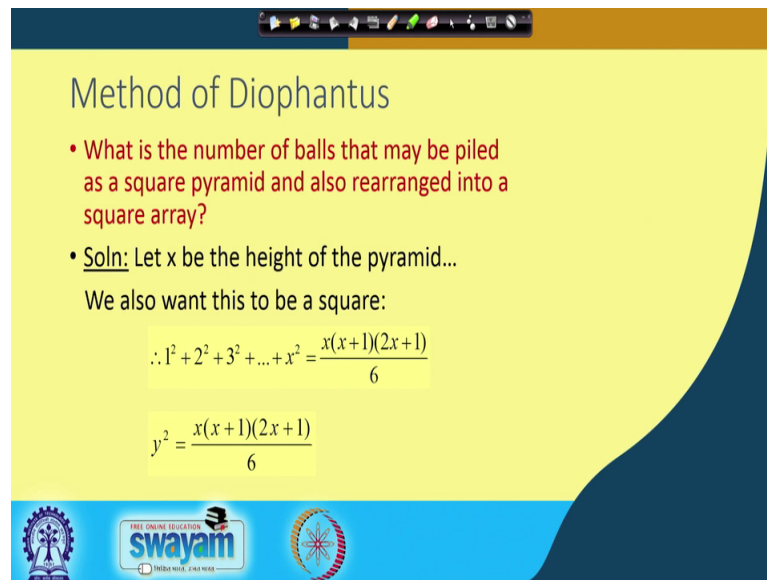
Welcome to this class on Hardware Security. Today we shall be studying about Elliptic Curves which is a kind of de facto public key cryptosystem. And we shall be trying to understand eventually the hardware design on or how to do a hardware architecture for this algorithm. So, we shall be trying to start with some on the basics and trying to introduce them in the class

(Refer Slide Time: 00:41)



So, in today's class we shall be covering or we shall be getting an introduction to elliptic curves we shall be trying to understand the elliptic curve arithmetic. We shall be trying to understand how point addition and point doubling which are essentially two important operations in the elliptic curve group are being performed. We shall be trying to understand the concept of projective coordinates which are essentially used to reduce the computations the required to perform elliptic curve operations. And in particular we shall be trying to look into characteristic two elliptic curves which are very conducive for hardware design.

(Refer Slide Time: 01:13)



Method of Diophantus

- 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...

We also want this to be a square:

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

The slide also features logos for Swamyam and other educational institutions at the bottom.

So, let me start with an example which is essentially trying to explain an old method which is called as a method of Diophantus. So, in this example or in this sort of question be we enquire: what is the number of balls that may be piled as a square pyramid and also rearranged into a square array ok

So, basically like we have basically asking that; what is the number of balls that may be piled up in both of this arrangement. So, you can either arrange these balls you know like as a square pyramid; that means, it is essentially a pyramid where the where the top essentially has got say one square number of balls. In the second layer you have got two square number of balls in the third layer you have got three square number of balls and so on.

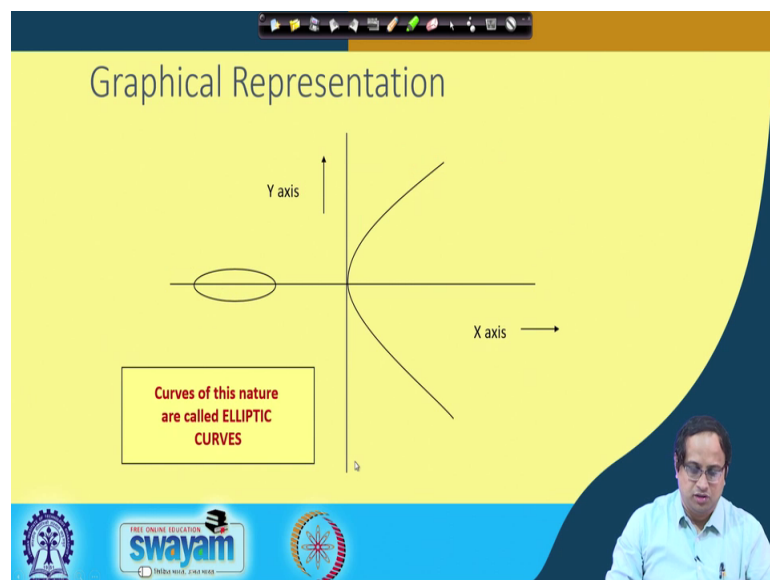
If the height is x of the pyramid then you have got 1 square plus 2 square plus 3 square plus so on till x square number of balls. And likewise you can also rearrange them in the form of a square. So, therefore, if y is the side of the square then you have got y square number of balls in the in this arrangement.

So, since that equinumerous; that means, you are essentially arranging the same number of balls then that would mean that in both the arrangements the numbers of balls are same right. So therefore, we can easily write this equality. That means, y 1 square plus 2 square plus so on till x square which is equal to x into x plus one into two x plus one by six is equal to y square ok. So, these kinds of equations which are essentially quadratic in

y and also cubic in x essentially are what are called as elliptic curves. Of course, there are lot of like definitions which have been developed over the years in elliptic curves, but this is the general form of the curve ok.

So, therefore, in order to solve this problem or this kind of problem or this class of problem there is a very famous method: which is an also an old method or an ancient method which is due to Diophantus or is often referred to as a Diophantus method. So, I will be first starting with an explanation on how it works. And gradually you will understand that how closely it is connected to the elliptic curve operations ok.

(Refer Slide Time: 03:23)



So therefore, the graphical representation of this curve is often of this form. So, you can see that it is you know like quadratic with respect to y; that means, it will be symmetric over the x axis ok. So therefore, this is a form of the curve and you can see that typically right this is essentially it looks like as if it is a curve with a single handle ok. And this is essentially are this curve or nature of the curves of this nature are called as elliptic curves ok.

So, therefore I mean if you take this curve and you can see that there as I mean typically the number of handles that you have right is essentially also a very important feature of this curves ok. So, typically this in the elliptic curve that we use for cryptography there are one such handles there is one such lobe which is essentially belong to this curve.

So, now the question is how do we solve the problem that we have in hand ok; that means, the problem of determine the number of balls. So, remember the number of balls has to be an integer of course the number of balls has to be an integer.

(Refer Slide Time: 04:31)

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 $1 + 0 + x = 3/2 \Rightarrow$
 $x = 1/2$ and $y = 1/2$
- Using symmetry of the curve we also have $(1/2, -1/2)$ as another solution

Handwritten notes on the slide include the equation $y = \frac{x(x+1)(2x+1)}{6}$ and a graph showing the intersection of the curve and the line $y=x$ at points $(0,0)$ and $(1,1)$. Other points $(1/2, -1/2)$ and $(3/2, 3/2)$ are also marked on the curve.

So, therefore the way we start is essentially from trivial solutions to this equation. So, you can easily inspect that in the curve that we essentially saw 0 0 are a trivial solutions ok.

So, if you just reflect back at the equation right; the equation was y square equal to x into x plus 1 into 2 x plus 1 by 6. So, if I may write down the equation the equation was y square equal to x into x plus 1 into 2 x plus 1 by 6 ok. So, you can easily see that 0 and 0 are solutions to this thing to this equation.

So, 0 0 is a trivial solution right, 0 comma 0 is a trivial solution. Likewise, you can also see that 1 comma 1 is also trivial solution 1 comma 1 is also a trivial solution. So, if I plug in 1 here this is 1 left hand side is 1 and the right hand side is 1 into 2 into 3 that is 6 divided by 6 which is also 1. So, 1 comma 1 is also a trivial solution of this equation.

So, now what we will do is that we will basically draw a straight line through these two points that is 0 0 and 1 1 ok. So, you can easily see that in that case write the line is nothing, but y equal to x . So that means, like if I believe that in the curve that we have ok. So, we basically kind of say consider that your curve is something like this right. I

take this point $(0, 0)$ and I take the point $(1, 1)$ and I draw a straight line through these two points ok. So that means, this is my $(0, 0)$ point and this is my $(1, 1)$ point and I draw straight line and the straight line is y equal to x ok.

So, now you can you can basically see that since equation is cubic with respect to x . So, if I plug in y equal to x into the curve equation and I do a few rearrangements then you will get this equation which is $x^3 - 2x^2 + 2x - 1 = 0$ ok. So, this essentially or this equation is cubic with respect to x which means that there are three possible roots. So, we already know that $(0, 0)$ and $(1, 1)$ are two roots; that means, x equal to 0 and x equal to 1 are already two roots we need to determine the third root ok.

So, therefore from the theory of equations if we add up the roots that means what we do like $1 + 0 + x$; that means, we add up the three roots of this equation. Then that should be the negative of this coefficient ok; that means it is equal to $3 - 2$. And therefore, we easily can obtain that x is equal to $\frac{1}{2}$. Now you note that x equal to $\frac{1}{2}$ implies y equal to $\frac{1}{2}$ and therefore, the number of balls right is y^2 . So, you can easily see that since y is a fraction that is not the solution that where we where we should stop.

But at the same time this is nevertheless a non trivial root of the equation. So, you can similarly we generate non trivial roots. So, what you can do is you can start with $\frac{1}{2}$ and you can easily see that if $\frac{1}{2}$ is you know like 1 root. Then since the curve is symmetric over the x axis then; that means, like if (x, y) is a root of this curve then that would also imply that $(x, -y)$ is also root on the curve is also point on the curve. So, that means write $\frac{1}{2}, -\frac{1}{2}$ is also a point on the curve.

So, now we can essentially take $\frac{1}{2}, -\frac{1}{2}$ and continue this exercise. So, that is essentially the broad idea of a Diophantus methods. So, let us see if we do that then what happens.

(Refer Slide Time: 08:33)

Method of Diophantus

- Consider the line through $(1/2, -1/2)$ and $(1, 1) \Rightarrow y = 3x - 2$
- Intersecting with the curve we have:

$$x^3 - \frac{51}{2}x^2 + \dots = 0$$

- Thus $\frac{1}{2} + 1 + x = 51/2$ or $x = 24$ and $y = 70$
- Thus if we have 4900 balls we may arrange them in either way

swayam
INDIA WISE, LEARN WISE

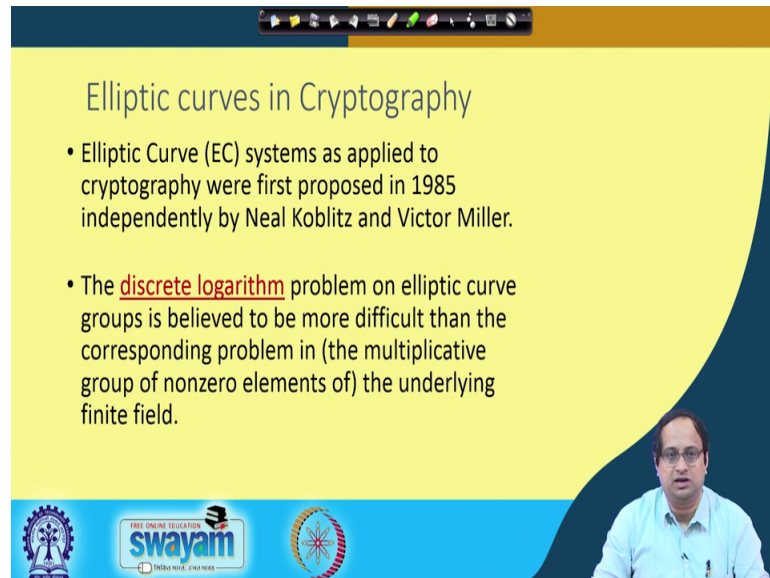
So therefore, if I take now a straight line through half minus half and 1 comma 1 then my equation in this case is y equal to $3x$ minus 2 ok. So, now I take y equal to $3x$ minus 2 and again plug in to the curve; that means, I intersect the straight line with the curve. Now I can equation which is x cube minus 51 by 2 x square plus some terms ok. Again I apply the theory of questions I know that half on 1 are 2 roots I need to obtain the third root ok.

So, therefore, I add half with 1 with x which is my unknown root and that is equal to the negative of this coefficient which is 51 by 2 ok. So, now I obtain an integer integral value of x ; that means, in this case x is equal to 24 ok. And I am lucky that this is an integer and therefore, I obtain that y is equal to 70. So, I can tell that y equal to or y square which is 4900 is a number of balls which can be arranged in both of this manner with both this manner.

So, while this problem can have it is own implication and statement what essentially I am trying to kind of illustrate out of this example is that if you take curves of this nature. Then you can essentially have this nice you know like technique of starting with trivial roots and obtaining further points on the curve by using this technique of you know like drawing straight lines, and finding out the third point of intersection ok. So, this is essentially precisely like one of the techniques which leads to something which is called

as the chord and tangent rule in context to elliptic curve cryptography or elliptic curves in general ok.

(Refer Slide Time: 10:13)



The slide features a yellow background with a dark blue curved border on the right side. At the top, there is a navigation toolbar. The title 'Elliptic curves in Cryptography' is centered. Below it, two bullet points are listed. The second bullet point has the word 'discrete' underlined. In the bottom right corner, there is a small video inset showing a man in a light blue shirt speaking. At the bottom of the slide, there are three logos: a circular emblem on the left, the 'swayam' logo in the center, and another circular emblem on the right.

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.

So therefore, I mean elliptic curves in cryptography you are just to give an little bit of background was essentially kind of made popular in around 1985. And essentially forms the basic like basic structure on which elliptic curve cryptography has been design ok.

So, there is a problem in this case or essentially heart problem like all public key cryptography systems like these also relies on the notion of some heart problems. And the notion is called as a discrete log problem or discrete logarithm problem on elliptic curves; which is believed to be more difficult than corresponding problems in the multiplicative groups of non 0 elements of the underlying finite fields ok.

And therefore, elliptic curve cryptography can often afforded with much shorter keys compare to the other counterparts like say RSA ok. And that is essential precisely the reason why elliptic curve cryptography is essentially kind of has become very popular and is often considered as a de facto public key cryptosystems for many you know like resource constrained environments ok. Because, you can essentially operate with shorter key sizes; and therefore you can do the arithmetic with smaller finite field operations.

Also if you want performance these also can give you quite fast operations again precisely because of the same reason. And therefore, you can also have high performance

public key cryptography which can be used in data centers and cloud and other kind of infrastructure where performance is key criteria.

(Refer Slide Time: 11:48)

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 an Elliptic Curve Discrete Logarithm Problem: ECDLP

swayam

So therefore, let me try to look at now in more formally in to a form of elliptic curve again this is a toy example. So, consider that I write y square equal to x cube plus $2x$ plus 3 . So, you see that this is precisely the curve that or form of curve that we have been seeing in context to a Diophantus example, but one thing that we need to kind of keep in mind when you are considering elliptic curve cryptography is that you know like that it often operates on finite fields ok. That means, that the basic elements or the basic points or the basic points means the you know like the x coordinate and the y coordinate of the points they often belong to finite fields ok.

So therefore, I mean let me take an example of very toy finite field in this case which is same modulo P field; that means, say $z \pmod{P}$ ok. So, $z \pmod{P}$ imply that may elements can be 0 1 2 3 and 4 ok. So therefore, in this case since the space is small we can see that whether you know like what are the possible points on the curve ok.

So therefore, let me start with x equal to 0 . You see that if I plug in x equal to 0 I get y square is equal to 3 and it turns out that field modulo 5 there are no solutions of y . That means, there are no solutions of y we belongs to 0 1 2 3 and 4 which if I square I get 3 ok. That is because 3 is a non quadratic residue ok. So, it is not a quadratic residue in this

field. So, I do not get any solution with x equal to 0 I start with x equal to 1 I get y squared equal to 6 it turns out that there are two solutions ok.

So, therefore, in this case either y is equal to 1 all y equal to 4. Likewise a plug in x equal to 2 I get y square equal to 15 and 15 is essentially 0 in this case and therefore, y is equal to 0 mod 5 ok. Likewise if I plug in x equal to 3 then y square is equal to 36 which is equal to 1 and this implies that y is equal to 1 comma 4 modulo 5. And likewise x equal to 4 also leads to y equal to 0 modulo 5.

So; that means, the points on the curve or I would say like the finite points on the curve are; 1 comma 1, 1 comma 4, 2 comma 0, 3 comma 1, 3 comma 4, and 4 comma 0. So, the elliptic curve, although we are drawing as a continuous line is actually an array of points or discrete points. Along with it be also define a point at infinity which I will be briefing very soon or detail in very soon just give me an idea about the point at infinity is also another point which we release is at the top of the Cartesian coordinate are also the below of the Cartesian coordinate ok. So, this is often called as a point O in context to elliptic curves ok.

So therefore, I mean this is a very important point. So therefore, whenever we consider elliptic curves right we essentially considered some finite points and also one infinite point ok. Together the define what is called as a elliptic curve group ok. And now, what we essentially try to formalize is essentially a problem which is analogous to the discrete log problem in context to you know, like normal finite field operations which we called as a elliptic curve discrete log problem or the ECDLP problem which is believed to be a heart problem if the parameters are properly chosen ok.

(Refer Slide Time: 15:05)

The slide is titled "Definition of Elliptic curves" and contains the following text:

- 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).

The slide also features a video feed of a presenter in the bottom right corner and logos for "swayam" and "INDIA WISE, LEARN WISE" at the bottom.

So, now we basically are all set to essentially define an elliptic curves. So therefore, elliptic curves over a field K is a nonsingular cubic curve. So, I will be again defining what nonsingular means at the end of this class is; that is a nonsingular cubic curve in two variables $f(x,y)=0$ with a rational point which may be a point at infinity ok. So therefore, I mean if you just ignore a few terms that we mentioned here. The basic idea is that it is essentially a cubic curve; that means, it is a cubic curve with respect to x quadratic curve with respect to y it is a nonsingular curve which I will be defined in shortly.

And it has got you know like a it has got some finite points and also point on infinity ok; together they are called as an elliptic curve. There are different elliptic curves that you can define, but what will be considering here in this course on hardware security is essentially elliptic curve which are defined and characteristic prime fields and also characteristic two fields ok.

So, typically these are the two popular alternatives which are used in hardware architectures, they either belong to $GF(p)$; that means, the underlying field is either $GF(p)$ or $GF(2^m)$ to the power of m ok. So, the architecture that will be starting in details will be on $GF(2^m)$ simply because they are more conducive for a fusion architectures ok. So therefore, elliptic curves for groups are examined with the underlying fields of $GF(p)$

and also f_2 to the power of m which is a binary representation with 2 to the power of m elements ok

(Refer Slide Time: 16:39)

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, now we essentially are let me take an elliptic curves of this nature. So, it is equal to say y squared equal to x cube plus a x plus b . So, this is the general form of the elliptic curve and which is defined on. So, essentially a plane curve defined by an equation of this form. And it can look these are various curves that we have taken say y square equal to x cube minus 1 y square equal to x cube plus 1 y square equal to x cube minus 3 x plus y square equal to x cube minus 4 x y squared equal to x cube minus x . So, you can take different curves of this nature by choosing, different values of a and b and it would be a fun exercise kind of to plot this curves and see how they look like ok.

So, you can see sometimes this globe is kind of separated from this part sometimes you know like it is connected as well. So, it is very interesting to see how this curve kind of you know like varies depending upon the choice of a and b ok. One thing we should always keep in mind is that this is not a continuous curve if you define this over finite fields in that case this is the discrete points.

(Refer Slide Time: 17:39)

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 ($GF(2^n)$).

swamyam
FREE ONLINE EDUCATION
TRIED & TRUE. LIVE HERE

So, there is a general form of the curve which is called as the Weierstrass equation from which all these curves are derived ok. So, this is a two variable equation $f(x,y) = 0$. And this looks like this $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

So, now what we will be trying to look into is that depending upon the characteristic of the underlying finite field this curve can take various forms ok. So therefore, what I mean is that sometimes these curves can be of I say the underlying field can be an F_p field which is a prime field ok. And it can have different characteristic ok. So, if you remember characteristic then; that means, that the minimum number of elements that number of times they need to add 1 in that field to get 0 ok. So, the characteristic can be 2 can be 3 can many other thing. So, we will see that how depending upon the characteristic the form of the curve also differs ok.

(Refer Slide Time: 18:46)

The Curve Equations depend on the field

- If Characteristic field is not 2:
$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + a_1x + \left(\frac{a_5}{4} + a_6\right)$$
$$\Rightarrow y_1^2 = x^3 + a_2x^2 + a_1x + a_6$$
- If Characteristics of field is neither 2 nor 3:
$$x_1 = x + \frac{a_2}{3}$$
$$\Rightarrow y_1^2 = x_1^3 + Ax_1 + B$$

So, there are some examples. So you can start doing this that is I will not go into too many details about this derivations, but these are something that you can also verify subsequently is that suppose you know like let me state that if the characteristic field is not 2 ok. That means, the characteristic is not 2; that means, right I mean I can do this operation; what I can do is that I can take this equation and I can rewrite it in this form ok.

So, here you see that I have divided by 2 certain terms this division is legal here or is allowed here simply, because the characteristic is not 2. If the characteristic was 2 then I cannot do it this division because in that case 2 is equivalent to 0 and I cannot divided by 0 ok. But here since the characteristic is not 2, I am free to do this division and you can easily verify that this is exactly the same equation as this equation except that I have you know like added few terms, and I have kind of adjusted few terms ok. So, I leave it to as an exercise to verify that this equation is essentially exactly equal to the Weierstrass equation ok.

So, once you can if you write this in this format then I can take this part which is inside this square you know like and raise to the power of 2 and replace it by a new y dash or y 1. So, therefore, I get y 1 square which is equal to x cube plus this is a new constant I write this is a 2 dash plus this is again a new constant say a 4 dash although it is a same in this case and I write this as a 6 dash ok.

So, you see that the curve right essentially kind of transforms into a simpler equation, because of this assumption that the characteristic field is not 2 ok. I can make a further assumption that the characteristic is neither 2 nor 3; so that means, now division by 3 is also allowed ok. So, if I therefore, plug in you know like $x^2 = x^2 + a$ and you know like if I substitute in this case then I will get the equation further simplified into this form.

And this is a very common form often used in several standards ok. So, that is $y^2 = x^3 + ax + b$, but remember that whenever this equation comes then it is implicitly assumed that the characteristic is neither 2 nor 3 only then we get this form of the equation. If the characteristic is 2 then we get a different form as we will see subsequently.

So, now let us assume that the characteristic is neither 2 and nor neither 3 and without loss of generality. Let us try to define an elliptic curve group and also some operations on the elliptic curve group. Because, we need to do at the end of the day arithmetic based using which we will be doing our cryptographic operations.

(Refer Slide Time: 21:36)

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

swamyam
FREE ONLINE EDUCATION
INDIAN NATIONAL OPEN UNIVERSITY

So therefore, as I is already mentioned that the elliptic curve therefore, over the field L will consist of a point at infinity along with some points x comma y which satisfy this curve. So, this x comma y I taken from L square; that means, x belongs to the field L y also belongs to the field L and they are satisfying this equation. That is $y^2 + \dots = x^3 + \dots$

some terms equal to x^3 plus some terms and this x comma y is a point on the curve. So, with this we called as finite points on the curve and this is the point at infinity.

So, why do we add the point at infinity is that it is often you know like just we can understand in this way either it is useful to at the point at infinity ok. The apparently the point is you can imagine that is are sitting at the top of the y axis and also you know like is kind of a point which is very far away from this coordinate system. But the introduction of the point at infinity essentially completes the definition on my group without it I do not I cannot defined the group.

So, that is essentially you can also you conceive in this way it is essentially nothing, but the identity of or you know like it is essentially my 0 element of the group ok. So, this notion will be clear very soon. So, it is kind of sitting at the top and also the bottom of the y axis ok.

(Refer Slide Time: 22:54)

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*)

swayam
Indira Gandhi Centre for Women Studies

So therefore, let us try to define the group and this is a quick recapitulation of what Abelian groups essentially imply. So, if I considered you know like two points P comma Q which belongs to $E F p$. So, $E F P$ means that now I am defining elliptic curve on the finite fields $E F P$ ok. Similarly I can define it on any field any finite field ok. So, there is a third point which is denoted by P plus Q . So now, you see that I am taking two points on the elliptic curve say P and Q and I am trying to define an operation which is plus.

Note that, this operation plus is not a normal plus ok. So, it is essentially a plus or plus symbolizes some operation ok. So, you can if you are confused or if you don't want plus you can very well replace it by any notation ok. So therefore, I want to define some P operation with Q. So, that I again get another point which is R which also belongs to the field I mean belongs to the elliptic curve. So, here you see that the Diophantus method is exactly the same because I start with two points P and Q and I want to obtain a third point on the curve ok. So therefore, if I want to define an Abelian group then I need these properties. That means I need the property of commutativity. That means, if I take P and Q the operation should be same as P plus Q is equal to Q plus P it should be associative; that means, P plus Q then added with R should be same as P plus with Q and R ok.

Similarly, write the there should be an identity element with exist; that means, P plus a point O should be equal to O plus P. And I should get back P and there should exist inverse; that means, P plus minus P should be equal to O ok. So, all these things has to be satisfied for us to have a complete definition of what is called as an Abelian group.

(Refer Slide Time: 24:41)

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

The slide features a yellow background with a blue header and footer. The header contains a navigation bar with icons. The main content area shows a coordinate system with an elliptic curve. Points P_1 , P_2 , and P_3 are marked on the curve. A red line connects P_1 and P_2 , and a vertical dashed line connects P_2 and P_3 . The footer includes logos for Swamyam and other educational institutions, along with a small video inset of a man in a white shirt.

So, if I start with an elliptic curve picture therefore, so this is essentially an elliptic curve equation. So, you see that it is y square equal to x cube minus x plus 1 and we want to set so we want to define this operation plus. So therefore, let me start with two points on the elliptic curves say P 1 and P 2 and I and I want to define what is P 1 plus P 2 ok. So, the usual way it is done is again by applying a curve through P 1 and P 2. So, again

remember that since it is a cubic equation in x this intersects the curve on a third point and now I take this point and I reflect this point ok.

So, if I reflect this point I get this point which is P 3. So, this is P 3 is essentially nothing, but the addition of P 1 and P 2 ok; from Diophantus technique or in general also you easily understand the P 3 should be a point on the curve So, likewise so now you can essentially are all set to obtain you know like some details about you know like about how the addition works. And we will be kind of seeing like how you can get these equations ok.

(Refer Slide Time: 25:52)

Addition in Affine Co-ordinates

$y = m(x - x_1) + y_1$

$P = (x_1, y_1), Q = (x_2, y_2)$

$R = (P + Q) = (x_3, y_3)$

Let, $P \neq Q$,

$m = \frac{y_2 - y_1}{x_2 - x_1}$

To find the intersection with E we get:

$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$

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

$\therefore x_3 = m^2 - x_1 - x_2$

$\Rightarrow y_3 = m(x_1 - x_2) - y_1$

Handwritten notes on the right:

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

$\Rightarrow y = \frac{Ax^2 + Bx + C}{x - y}$

$-y_3 = m(x_2 - x_1) - y_1$

$y_3 = m(x_1 - x_2) - y_1$

Now, we essentially can derive the equations for doing this addition operation. So, what I essentially kind of said now we can see in a more mathematical way. So we can take P and Q so imagine that the point P is nothing but x 1 comma y 1. So, the point P is let me try to write it here. So, the point P essentially is this point. So, let me write this point as x 1 comma y 1 and likewise this is my point Q which is nothing but x 2 comma y 2 ok.

So, we draw a chord through these two points and therefore, this is your minus P plus Q if I reflect this I get P plus Q ok. So, what we are interested is now is in the coordinates of P plus Q ok. That means, how do I get P plus Q basically. So, you can easily understand from the simple theory of coordinate geometry that is the slope of these curve so this is suppose m ok. So, the slope of this straight line is m which means at the straight

line equation is nothing, but y equal to $m x$ minus x_1 plus y_1 because of straight line passes through x_1 and y_1 . So, therefore, m is nothing, but y_2 minus y_1 divided by x_2 minus x_1 note that we are assuming here that the point P and Q are distinct. If the point P and Q are distinct then this m is not defined. So, therefore, we cannot apply this equation ok.

So, now if I want to find out the intersection with E then what we will do is that will take the straight line y equal to $m x$ minus x_1 plus y_1 and plug in into the curve equation. And therefore, with little bit of adjustment again I will get this equation I will get like x cube minus m square x square plus some terms this will be equal to 0. So, you can see that I have replaced y with this equation that is $m x$ minus x_1 plus y_1 .

So therefore, now again you know like if I arrange these terms then and I know that since there are three roots of this curve. So, two roots are already x_1 and x_2 I want to obtain this root. So, suppose this root is x_3 which is essentially the same as you know the x coordinate of this inverse. Then I can write that x_3 plus x_1 plus x_2 is nothing, but the negative or negation of minus m square which is m square.

So, therefore, I can obtain x_3 which is equal to m square minus x_1 minus x_2 and from there I can obtain y_3 and I can negate y_3 to get this equation I mean this coordinate ok. So, you know easily see that I can essentially you know like obtained say you know like minus of y_3 is equal to you know like m of x minus x_1 . So, m is nothing but as we have already obtained that is m into x minus x_1 plus. So, in this case you know like this x will be replaced by x_3 ok. So, x minus x_3 plus y_1 ok.

So therefore, I will get y_3 as $m x_1$ minus x_3 minus y_1 ok. So, you can I hope you understand that if x_3 if this point is x_3 comma minus y_3 then this point is which I am inverting over the x axis is x_3 comma y_3 ok. So this, you can easily understand by you know like if I can take a straight line. So, this line is say you know like x equal to say h right and I draw it with the curve; that means, my curve is y square equal to x cube plus a x plus b . So, if I plug in x equal to h here then I get y square equal to h cube plus $a h$ plus b ok.

So; that means, right there are two roots of this equation ok. So, I already note that so the so the idea is that you know like I mean seen this is you know like symmetric over the x axis then; that means, if y is a root then minus y is also a root ok. So that means, like if x

3 comma y 3 is a root then x 3 comma minus y 3 is like also falling on the curve. And that is a inverse of that point ok. So, that way you can calculate the inverse.

So therefore, the first thing that we did here was obtain this point and then we kind of you know like reflected this point and obtain the negative which is essentially nothing but the addition of P and Q. So, this is a simple you know like operation and you can essentially extend this also 2 over the case where x and P and Q are same ok.

(Refer Slide Time: 30:53)

The slide is titled "Doubling of a point" and contains the following content:

- Let, $P=Q$
- $$2y \frac{dy}{dx} = 3x^2 + A$$
- $$\Rightarrow m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$
- If, $y_1 \neq 0$ (since then $P_1+P_2=\infty$):
- $$\therefore 0 = x^3 - m^2 x^2 + \dots$$
- $$\Rightarrow x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1$$
- What happens when $P_2=\infty$?

The slide also features a video feed of a presenter in the bottom right corner and a footer with the Swayam logo and "FREE ONLINE EDUCATION" text.

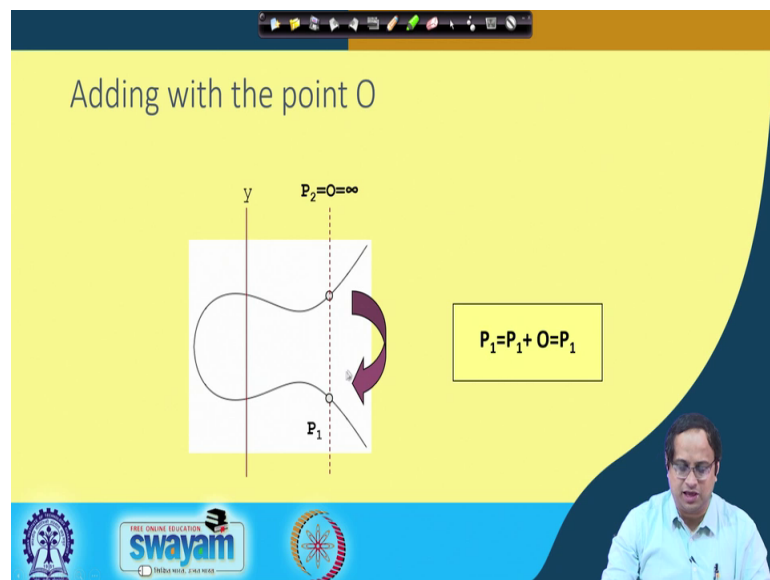
That means, in that case we will not draw I mean we cannot obtain m in the way we saw. But we can obtain m by taking derivative or obtain the different differential at the point x comma y. So, now if I you know like derivate my curve then I can obtain 2 y d y by d x is equal to 3 x square plus a. And therefore, m which is the slope is nothing, but d y by d x and at the point x 1 comma y 1. So, if I obtain these are the points x 1 comma y 1 then is equal to 3 x 1 square plus a divided by 2 y 1 ok. So, if you are particular then we should actually right here that this derivative is taken at the point x 1 comma y 1 ok.

So, then this is equal to 3 x 1 square plus a divided by 2 y 1 and again we apply the same thing. So, I know, but in this case you know like there are 2 2 roots and both of them are same. So, therefore, that is x 1 plus x 1 that is 2 x 1. Note that, the characteristic is neither 2 nor 3. So, I can obtain 2 x 1 and therefore, my x 3 nothing, but m square minus 2 x 1 ok. So, likewise I can obtain y three exactly like what we saw in the previous case and we can obtain this equations ok.

So, now the question is write what happens when one of the points is the point infinity or is the O. So, there we can we can easily we can easily see that when we consider that we essentially you know like ok. So, essentially right so, what we see therefore, I mean once we have derived the point and addition the point at doubling, but we remember that we have we have been operating on finite points.

But, as I mention that in the curve that is also point an infinity on which also I need to do these operations. So, what essentially happens you one of these points is that point; that means, it is the point at infinity. So, that means like what happens when P_2 is equal to infinity or is a point O ok.

(Refer Slide Time: 32:46)



So, let us see that; therefore, if I want to add with O remember O is a point which is kind of at conceive to be as the top and at the bottom both sides kind of as a point at infinity. So therefore, if I take a point say P 1 and if I want to added add with O then the way we do that is as if like drawing a vertical line through P point P 1 ok.

So therefore, this is a assume that I am I am essentially you know like trying to kind of you know like draw a line which goes through P 1 and the point at infinity. So, that essentially you can imagine is as if like a vertical line. So therefore, this will cut the curve at this point which is essentially nothing but minus minus of P 1 so the minus of P 1. And therefore, if I reflect it back I get back P 1. So, that also defines you know like

what I need in my definition for elliptic curve group; that means, if I add P_1 with O I will get P_1 ok

So, likewise right you can also imagine that if I take P_1 and if I add with minus of P_1 which is essentially this point then also it will intersect at the point O ok. So, that also defines that that I have got an inverse ok; that means, inverse also exist. So therefore, right the point O essentially kind of completes the definition of what is required in a Abelian group.

So, now you have got some points there like finite fields on the curve and also like that point at infinity which is O . And therefore, you are all set to define your elliptic curve operations you are you have got a group on which you can you have also define to operations like addition and doubling through which you can do your computations.

So, let me stop here. And, we will continue from this point in the next class, will be try to look at some more details about elliptic curves.

Thank you for your attention.