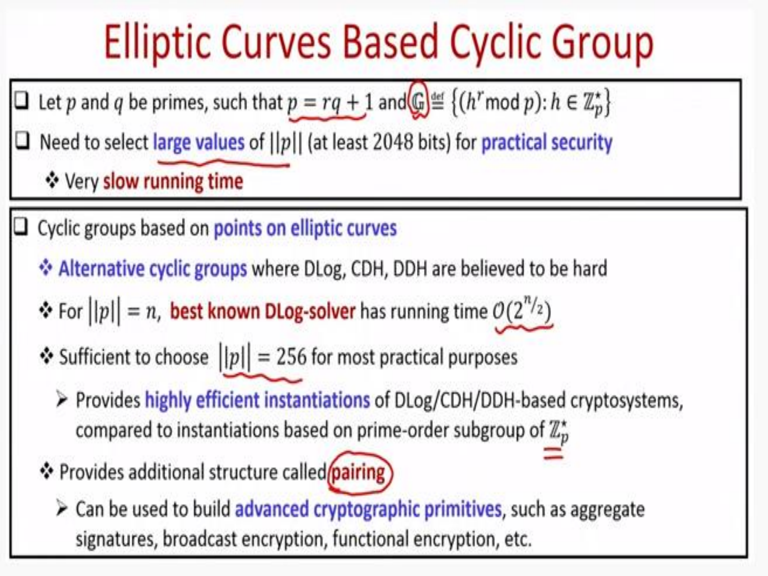
Foundations of Cryptography
Dr. Ashish Choudhury
Department of Computer Science
International Institute of Information Technology – Bangalore

Lecture – 41
Candidate Cyclic Groups for Cryptographic Purposes Part II

(Refer Slide Time: 00:44)



Elliptic Curves Based Cyclic Group

- ❑ Let p and q be primes, such that $p = rq + 1$ and $\mathbb{G} \overset{\text{def}}{=} \{(h^r \bmod p) : h \in \mathbb{Z}_p^*\}$
- ❑ Need to select large values of $||p||$ (at least 2048 bits) for practical security
  - ❖ Very slow running time

- ❑ Cyclic groups based on points on elliptic curves
  - ❖ Alternative cyclic groups where DLog, CDH, DDH are believed to be hard
  - ❖ For $||p|| = n$, best known DLog-solver has running time $O(2^{n/2})$
  - ❖ Sufficient to choose $||p|| = 256$ for most practical purposes
    - ➢ Provides highly efficient instantiations of DLog/CDH/DDH-based cryptosystems, compared to instantiations based on prime-order subgroup of $\mathbb{Z}_p^*$
  - ❖ Provides additional structure called pairing
    - ➢ Can be used to build advanced cryptographic primitives, such as aggregate signatures, broadcast encryption, functional encryption, etc.

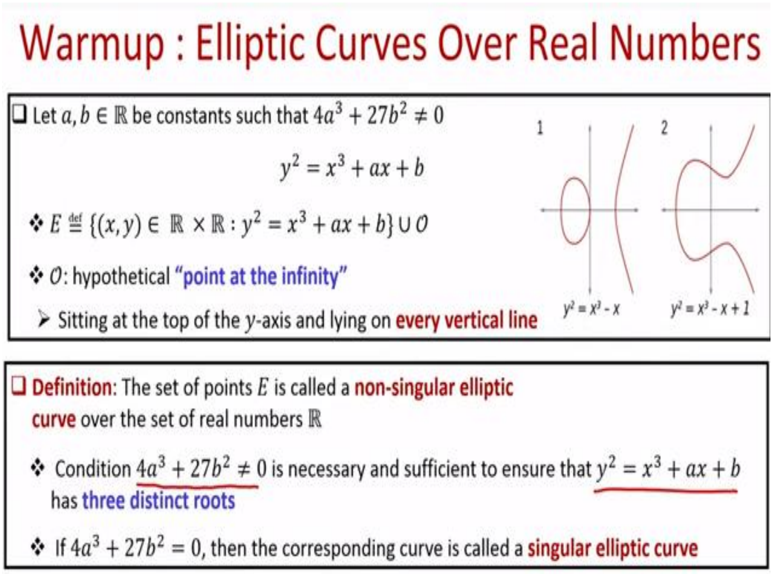
Hello everyone, welcome to this lecture in this lecture we will continue our discussion on the candidates cyclic groups for cryptographic purposes and in this lecture, we will introduce specifically the cyclic groups based on elliptic curves. So let us start with the discussion on elliptic curves based cyclic groups. So remember in the last lecture we had seen that if p and q are primes where p is of the form r times q + 1 and if we take all the rth residues modulo p then the resultant set which we denote as G constitutes a subgroup of Z_p* and we can prove that this set G along with the operation multiplication modulo p constitutes a cyclic group.

However, it turns out that for practical security we have to operate or select very large values of this prime p namely we have to ensure that the p is at least 2048 bit prime numbers which actually ends up ensuring that the resultant time of the sender and the receiver is also very slow. So what we are now going to do is in this lecture we will see cyclic groups based on the points on elliptic curves and these are basically alternative cyclic groups where the DLog problem the CDH problem and the DDH problems are indeed believed to be hard.

More specifically if the size of prime that we are going to operate with is of size n bits, then the best known DLog solver that we know for these groups is of order $2^{n/2}$ and that means its sufficient to operate with a prime number which is a 256 bit prime number for most practical purposes and that gives us highly efficient instantiations of DLog, CDH and DDH based crypto systems compared to instantiations based on prime order subgroups of Z_p* right.

So that is plus point of this groups compared to the instantiations based on the prime order subgroups of Z_p*. Another interesting property of the cyclic groups based on the elliptic curves is that it provides us with additional structures what we call as pairings which we are not going to discuss in this course. Because these are advanced concept but just for your information this additional structure which we call a pairing can be used to build highly advanced cryptographic primitives such as aggregate signatures, broadcast encryption, functional encryption and so on.

(Refer Slide Time: 02:59)



Warmup : Elliptic Curves Over Real Numbers

❑ Let $a, b \in \mathbb{R}$ be constants such that $4a^3 + 27b^2 \neq 0$

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

❖ $E \overset{\text{def}}{=} \{(x,y) \in \mathbb{R} \times \mathbb{R} : y^2 = x^3 + ax + b\} \cup \mathcal{O}$

❖ $\mathcal{O}$: hypothetical "point at the infinity"

➢ Sitting at the top of the y-axis and lying on every vertical line

❑ Definition: The set of points E is called a non-singular elliptic curve over the set of real numbers $\mathbb{R}$

❖ Condition $\underline{4a^3 + 27b^2 \neq 0}$ is necessary and sufficient to ensure that $\underline{y^2 = x^3 + ax + b}$ has three distinct roots

❖ If $4a^3 + 27b^2 = 0$, then the corresponding curve is called a singular elliptic curve

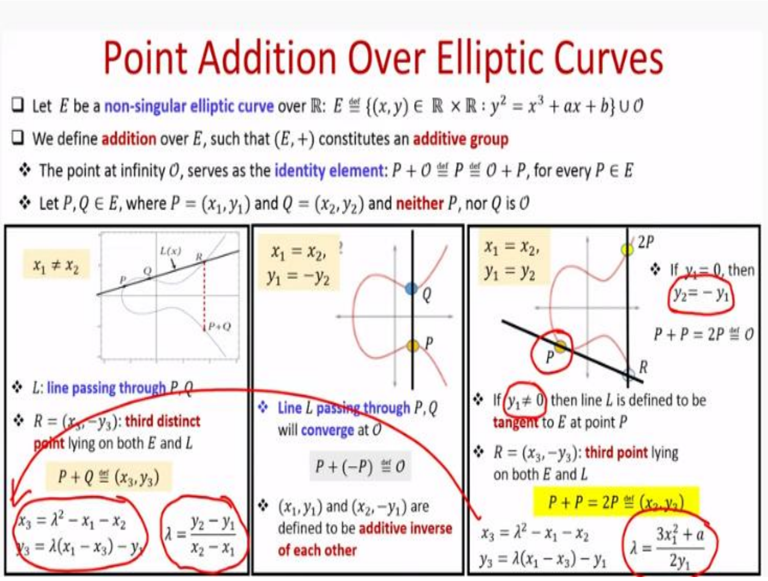
So before going into the exact elliptic based cyclic group that we are going to use for the cryptographic purpose let us do a warmup and see how exactly elliptic curves over the real numbers look like. So let R be the set of real numbers and let a and b be 2 real numbers or constants publicly known such that this relationship whole namely $4a^3 + 27b^2$ is not 0.

The reason for this constant will be clear soon and imagine we have such an a and b constants a and b consider this equation in x and y, $y^2 = x^3 + ax + b$ then if I plot the points on this equation or if I plot x, y value satisfying this equation and if you take all those x, y pairs which are real numbers satisfying this equation and along with that if I take a special point which I did not as O then the resultant set I call as E.

So for instance if I take the curve or the equation $y^2 = x^3 - x$ and plot all the real x, y satisfying this equation then I obtained this curve in the same way if I take the curve $y^2 = x^3 - x + 1$ and plot all the real x, y satisfying this equation then I obtain this curve. So what E is basically once we have fixed the equation we take all the x, y real numbers which satisfies this equation and along with that a special point which we denote as O and this special point O is called as the point at the infinity which is kind of an imaginary point which you can imagine sitting at the top of the y-axis and lying on every vertical line.

So you can imagine that every vertical line will eventually meet at a horizon at a single point and that point where all the vertical lines are going to meet is considered as the point at infinity which would be denote by this special notation O. So that is how I construct the set E now the set of points E that we have defined above is called a non-singular elliptic curve over the set of real numbers and why it is called non-singular, is because we have ensured the condition $4a^3 + 27b^2 \neq 0$ which is a necessary and sufficient condition to ensure that the resultant curve that we have defined here namely $y^2 = x^3 + ax + b$ has 3 distinct roots because it is an equation of degree 3 in x. However, if we do not ensure this condition namely $4a^3 + 27b^2 \neq 0$ if we let it to be 0 then the corresponding curve or the set of points that we obtain is called a singular elliptic curve it will not have 3 distinct roots.

(Refer Slide Time: 05:55)



Point Addition Over Elliptic Curves

- □ Let E be a **non-singular elliptic curve** over $\mathbb{R}$: $E \overset{\text{def}}{=} \{(x, y) \in \mathbb{R} \times \mathbb{R} : y^2 = x^3 + ax + b\} \cup \mathcal{O}$
- □ We define **addition** over E, such that $(E, +)$ constitutes an **additive group**
  - ❖ The point at infinity $\mathcal{O}$, serves as the **identity element**: $P + \mathcal{O} \overset{\text{def}}{=} P \overset{\text{def}}{=} \mathcal{O} + P$, for every $P \in E$
  - ❖ Let $P, Q \in E$, where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ and **neither** P, nor Q is $\mathcal{O}$

$x_1 \neq x_2$

- ❖ L: **line passing through** P, Q
- ❖ $R = (x_3, -y_3)$: **third distinct point** lying on both E and L

$P + Q \overset{\text{def}}{=} (x_3, y_3)$

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

$\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

$x_1 = x_2,$
$y_1 = -y_2$

- ❖ **Line L passing through** P, Q will **converge** at $\mathcal{O}$

$P + (-P) \overset{\text{def}}{=} \mathcal{O}$

- ❖ (x_1, y_1) and $(x_2, -y_1)$ are defined to be **additive inverse of each other**

$x_1 = x_2,$
$y_1 = y_2$

- ❖ If $y_1 = 0$, then $y_2 = -y_1$

$P + P = 2P \overset{\text{def}}{=} \mathcal{O}$

- ❖ If $y_1 \neq 0$ then line L is defined to be **tangent** to E at point P
- ❖ $R = (x_3, -y_3)$: **third point** lying on both E and L

$P + P = 2P \overset{\text{def}}{=} (x_3, y_3)$

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

$\lambda = \dfrac{3x_1^2 + a}{2y_1}$

So that is the definition of elliptic curves. Now what we are going to do here is we are going to find a very sophisticated way of doing performing operation : addition operation on the points on this elliptic curve. So imagine you are given a non-singular elliptic curve over the real numbers and we define the additional operation on these points such that the way we are going to define the addition operation it satisfies all of our group axioms namely it will satisfy the closure property, associativity property, it will be ensured we have an identity element and an additive inverse for every point on the curve and which ensures that the set E along with the plus operation that we are going to define now constitutes an additive group. So the plus operation is defined as follows so we define the point at infinity to be the identity element that is our definition. So we define that if you we defined a + operation on any point p on this elliptic curve and a point at infinity to give the result as p.

So if you take any point p which could be the point at infinity itself and to that point if you add the point at infinity the result is defined to be the point p itself. So that is a first property of the addition operation that we have defined here. On the other hand, if you are given 2 points P and Q lying on the curve E and say the coordinates of the point P are (x_1, y_1) and the coordinates of the point Q are (x_2, $y_{2)}$ and neither P nor Q is the point at infinity then the way we are going to define the plus operation on these 2 points P and Q is as follows.

So we can have 3 of the possible cases depending upon the relationship that holds between the coordinates of P and Q. So the first case is when $x_1 \neq x_2$ in this case the way we define the result of P + Q is as follows. So we define L of x to be the line passing through the points P and Q. So its a straight line passing through the P and Q so you have the pictorial representation here and let R be the third distinct point which lies both on the straight line as well as on the elliptic curve.

So I am denoting the x and y coordinates of the third point to be x_3, $-y_3$ and I call that point to be R. So pictorial is say this curve the straight line passes through P and Q and it intersects the elliptic curve at the third point say at R whose coordinates I denote it as x_3 and $-y_3$. So in this particular example in the pictorial representation the y coordinate of R is actually positive but that need not be always the case.

So that is why I am just representing it as $-y_3$ because if for instance if your Q would have been here then on passing the straight line or through P and Q it would have met somewhere here, and y coordinate of R would have been a negative coordinate. So irrespective of what exactly is the case. It is just a notational issue the third distinct point at which the line intercepts the elliptic curve is denoted as R and its x coordinate is x_3 and the y coordinate is $-y_3$.

Now what we do here is we just reflect the point R along the x axis and if we reflect the point R along the x axis the x coordinate is going to remain the same, but the y coordinate its sign will get changed. If it was $-y_3$ it will become $+y_3$ whereas if we would have been plus, then it becomes minus. And the result of the addition of P and Q is defined to be that reflected point. So that is the way we define the plus operation on points P and Q both neither P and Q are infinity point and $x_1 \neq x_2$.

So now if we want to mathematically compute the exact value of x_3 and y_3 here is how we can compute: it turns out that x_3 and y_3 are related to the coordinates x_1, x_2, y_1, y_2 by this relationship $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ and here λ is basically the slope of the straight line passing to the points P and Q and the slope of the line passing to the points P and Q comes through this formula $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and since we are in the case where $x_1 \neq x_2$ that means the denominator is not 0 and hence the λ is well-defined.

So that is the way operation of addition (plus) operation on points P and Q is defined for this case for the case where $x_1 \neq x_2$ now let us take the second case where $x_1 = x_2$ but the y coordinates of P and Q are just opposite of each other right. So in this case what we do here is the line that we make pass through P and Q it basically ends up converging at the point at infinity right.

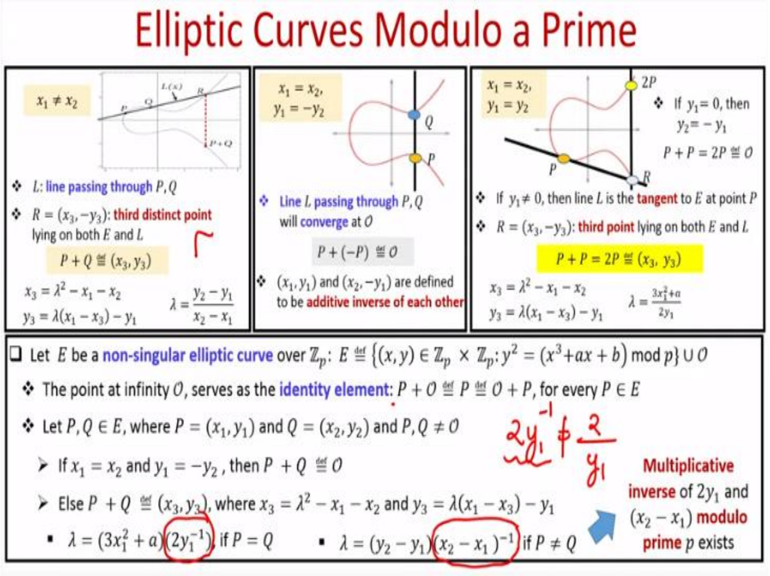
So the idea here is also the same we actually pass a line pass into the points P and Q and see where exactly it meets the elliptic curve. But in this case since the x coordinates of P and Q are same but only their y coordinates are different in the in the sign the straight line passing through P and Q basically meet the point at infinity, converge at point at infinity and that is why we define the P + Q operation in this case to give the result the point at infinity that means we can interpret 2 points x_1, y_1 and x_2, $-y_1$ where x_1 and x_2 are same to be the additive inverse of each other.

Right whereas for the third case where $x_1 = x_2$ and $y_1 = y_2$ we have 2 sub-cases if $y_1 = 0$ then we can interpret y_2 to be $=-y_1$ because 0 and + 0 and - 0 as same right? so if $y_1 = 0$ then we can interpret y_2 to be $= - y_1$ and then we basically come to the previous case where $x_1 = x_2$ and y_1 is $-y_2$. In that case the way we have defined the plus operation we get that the summation of P with the same point which is basically 2P gives you the point at infinity.

On the other hand if y_1 is not 0 that means say we have a point like this P and we want to add P to itself then the line passing through this point is defined in a different way : the line here is basically the tangent to this curve E passing through the point P and we see where exactly the tangent touches the curve we call that point as say R and say the coordinates of R is x_3 and $-y_3$ which is the third point, 2 of the points are P and the third point lying on the curve is R and what we now do is we just reflect the point R along the x axis and that is the result of adding P to itself.

So the result P + P, which is 2P in this case will be x_3, y_3 and mathematically again x_3 and y_3 are exactly the same as it was defined for the case where x_1 was not equal to x_2 the only difference now is that the slope of the line is different here compared to the first case. Because in the first case the points P and Q are distinct points but here are the points P and Q are the same points and that is why the line is the tangent and the slope of the tangent is computed by this formula $\lambda = \frac{3x_1{}^2 + a}{2y_1}$.. And since y_1 is not 0 right we are in the case where y_1 is not 0 the denominator 2 times y_1 is non 0 and that is why the slope is well defined.

(Refer Slide Time: 13:55)



Elliptic Curves Modulo a Prime

$x_1 \neq x_2$

- L: line passing through P, Q
- $R = (x_3, -y_3)$: third distinct point lying on both E and L

$P + Q \stackrel{\text{def}}{=} (x_3, y_3)$

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

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

$x_1 = x_2$, $y_1 = -y_2$

- Line L passing through P, Q will converge at $\mathcal{O}$

$P + (-P) \stackrel{\text{def}}{=} \mathcal{O}$

- (x_1, y_1) and $(x_2, -y_1)$ are defined to be additive inverse of each other

$x_1 = x_2$, $y_1 = y_2$

- If $y_1 = 0$, then $y_2 = -y_1$

$P + P = 2P \stackrel{\text{def}}{=} \mathcal{O}$

- If $y_1 \neq 0$, then line L is the tangent to E at point P
- $R = (x_3, -y_3)$: third point lying on both E and L

$P + P = 2P \stackrel{\text{def}}{=} (x_3, y_3)$

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

$\lambda = \frac{3x_1^2 + a}{2y_1}$

❑ Let E be a non-singular elliptic curve over $\mathbb{Z}_p$: $E \stackrel{\text{def}}{=} \{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p : y^2 = (x^3 + ax + b) \bmod p\} \cup \mathcal{O}$

- The point at infinity $\mathcal{O}$, serves as the identity element: $P + \mathcal{O} \stackrel{\text{def}}{=} P \stackrel{\text{def}}{=} \mathcal{O} + P$, for every $P \in E$
- Let $P, Q \in E$, where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ and $P, Q \neq \mathcal{O}$
  - If $x_1 = x_2$ and $y_1 = -y_2$, then $P + Q \stackrel{\text{def}}{=} \mathcal{O}$
  - Else $P + Q \stackrel{\text{def}}{=} (x_3, y_3)$, where $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$
    - $\lambda = (3x_1^2 + a)\boxed{(2y_1^{-1})}$ if $P = Q$
    - $\lambda = (y_2 - y_1)\boxed{(x_2 - x_1)^{-1}}$ if $P \neq Q$

$\underline{2y_1^{-1}} \neq \frac{2}{y_1}$

Multiplicative inverse of $2y_1$ and $(x_2 - x_1)$ modulo prime p exists

So that is the way we perform the addition operation for elliptic curves defined over the set of real numbers but as I said earlier for cryptography primitives we want to operate on a set which has a finite size that is why now what we are going to do is we are going to compute perform operations on elliptic curves modulo prime number which will not have nice geometrical representations as we had for elliptic curves over the real numbers but property wise we can extend the definition of the plus operation as we have done for the case of real numbers here as well.

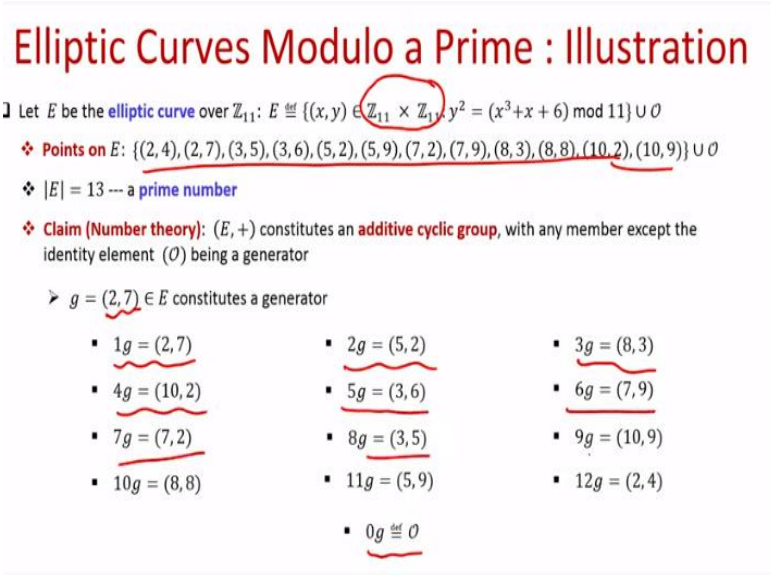
So here is how we define elliptic curves modulo a prime : so let E be a non-singular elliptical over the set Z_p basically what it means is we form an elliptic curve equation here namely the equation is $y^2 = x^3 + ax + b$ modulo p and we take all x,y elements or x , y pairs from the set Z_p x Z_p and take all the elements of the form x,y where x is in the range 0 to p - 1 and y is also in the range 0 to p-1 which satisfies this equation and along with those x , y pairs we take the special imaginary point namely the point at infinity.

So as it was the case for elliptic curves defined over the set of real numbers the point at infinity serves as the identity element namely we define that any non any point P belonging to the state E if we perform the plus operation with respect to the point at infinity then we get back to the same point P whereas if we have 2 points P and Q belonging to the set E which are not the points at infinity and say the coordinates of P are x_1, y_1 and x_2 , y_2 where x_1, $y_{1,}$ x_2, y_2 are all elements of the state Z_p then the plus operation is defined as follows.

For the case where $x_1 = x_2$ and $y_1 = - y_2$ we define P + Q to be infinity, this is exactly the case this is the same as in the case 2 for the elliptic curves over the real numbers. Whereas if otherwise if $x_1 \neq x_2$ or $y_1 \neq y_2$ then we define P + Q to be (x_3, y_3) where x_3 and y_3 are elements of Z_p and where x_3 will be this value namely it will be $\lambda^2 – x_1 – x_2$ of course everything modulo p and y_3 will be λ times $(x_1 – x_3) – y_1$ modulo p right and the λ will be computed in a different way for 2 sub-cases : if P = Q then λ is defined in this way namely $(3x_1^2 + a) * (2 y_1^{-1})$ and this basically corresponds to this case that is how we have defined x_3, y_3 for the real number case and if P $\neq$ Q then the λ is basically the slope of the line passing through the points P and Q which basically is similar to the first case for the elliptic curves over the real number.

And it turns out that all the plus operations and all the multiplications operation that we are performing here are modulo p when we are actually performing operation on the elliptic curves modulo p and if you see here the way we have defined λ this is the element 2 times y_1^{-1} is not $2/y_1$. That is not the case. This should be interpreted as the element 2 times y_1's multiplicative inverse which exists because we are performing modulo prime p operation and in the same way for the second case where λ is of this form $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, this $(x_2 - x_1)^{-1}$ is the multiplicative inverse of the element $(x_2 - x_1)$ modulo p which is also guaranteed to exist because $x_2 - x_1$ will be a non 0 value. So that is the way we naturally extend the definition of the plus operation for elliptic curves defined over modulo prime.

(Refer Slide Time: 18:18)



Elliptic Curves Modulo a Prime : Illustration

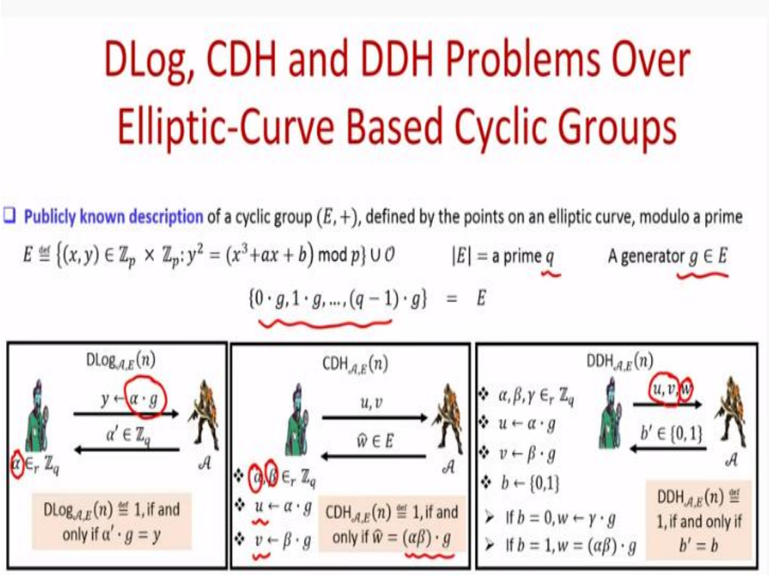
- Let E be the elliptic curve over $\mathbb{Z}_{11}$: $E \overset{\text{def}}{=} \{(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11} : y^2 = (x^3 + x + 6) \bmod 11\} \cup \mathcal{O}$
  - Points on E: $\{(2,4), (2,7), (3,5), (3,6), (5,2), (5,9), (7,2), (7,9), (8,3), (8,8), (10,2), (10,9)\} \cup \mathcal{O}$
  - $|E| = 13$ --- a prime number
  - Claim (Number theory): $(E, +)$ constitutes an additive cyclic group, with any member except the identity element $(\mathcal{O})$ being a generator
    - $g = (2,7) \in E$ constitutes a generator
      - $1g = (2,7)$
      - $2g = (5,2)$
      - $3g = (8,3)$
      - $4g = (10,2)$
      - $5g = (3,6)$
      - $6g = (7,9)$
      - $7g = (7,2)$
      - $8g = (3,5)$
      - $9g = (10,9)$
      - $10g = (8,8)$
      - $11g = (5,9)$
      - $12g = (2,4)$
      - $0g \overset{\text{def}}{=} \mathcal{O}$

And for an illustration let us take this example say I perform all my operations on Z_{11}. I take my curve to be equation $x^3 + x + 6$ modulo 11 and I take my set E to be the set of all x, y belonging to the set Z_{11} x Z_{11} satisfies this equation along with the point at infinity. So if you take all x, y belonging to the set Z_{11} x Z_{11} and see which of them satisfies this equation then we obtain the set E to consist of these values all the pairs satisfies this equation modulo 11 and along with that we have a point at infinity.

So since the size of this E is a prime number namely we have 13 entities in this set E it follows from a basic fact from the number theory that the set E along with the plus operation that we have defined constitutes an additive cyclic group and since the order of this group is a prime number every element in this group except the identity element which is the point at infinity can be treated as the generator for this group.

So for instance we can take the element (2,7) belonging to the set E which is a non-identity element and you can verify that indeed it constitutes a generator namely different powers of this element (2,7) will give you all the elements of the state E. So 0 times g as per the definition it gives you the identity element namely the point at infinity and if we perform the operation 1 times g, 2 times g, 3 times g then the way we have defined additive group operation we will get back each of the elements from the state E namely the non-identity elements of the set E once, that means the element 2,7 indeed constitutes a generator of the set E.

(Refer Slide Time: 20:12)



DLog, CDH and DDH Problems Over Elliptic-Curve Based Cyclic Groups

❑ Publicly known description of a cyclic group $(E, +)$, defined by the points on an elliptic curve, modulo a prime

$E \overset{\text{def}}{=} \{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p : y^2 = (x^3 + ax + b) \bmod p\} \cup \mathcal{O}$ $|E|$ = a prime q A generator $g \in E$

$\{0 \cdot g, 1 \cdot g, \ldots, (q-1) \cdot g\} = E$

$\mathsf{DLog}_{\mathcal{A},E}(n)$

$y \leftarrow \alpha \cdot g$

$\alpha' \in \mathbb{Z}_q$

$\alpha \in_r \mathbb{Z}_q$

$\mathcal{A}$

$\mathsf{DLog}_{\mathcal{A},E}(n) \overset{\text{def}}{=} 1$, if and only if $\alpha' \cdot g = y$

$\mathsf{CDH}_{\mathcal{A},E}(n)$

u, v

$\widehat{w} \in E$

$\mathcal{A}$

❖ $\alpha, \beta \in_r \mathbb{Z}_q$

❖ $u \leftarrow \alpha \cdot g$

❖ $v \leftarrow \beta \cdot g$

$\mathsf{CDH}_{\mathcal{A},E}(n) \overset{\text{def}}{=} 1$, if and only if $\widehat{w} = (\alpha\beta) \cdot g$

$\mathsf{DDH}_{\mathcal{A},E}(n)$

❖ $\alpha, \beta, \gamma \in_r \mathbb{Z}_q$

❖ $u \leftarrow \alpha \cdot g$

❖ $v \leftarrow \beta \cdot g$

❖ $b \leftarrow \{0,1\}$

➢ If $b = 0, w \leftarrow \gamma \cdot g$

➢ If $b = 1, w = (\alpha\beta) \cdot g$

u, v, w

$b' \in \{0, 1\}$

$\mathcal{A}$

$\mathsf{DDH}_{\mathcal{A},E}(n) \overset{\text{def}}{=} 1$, if and only if $b' = b$

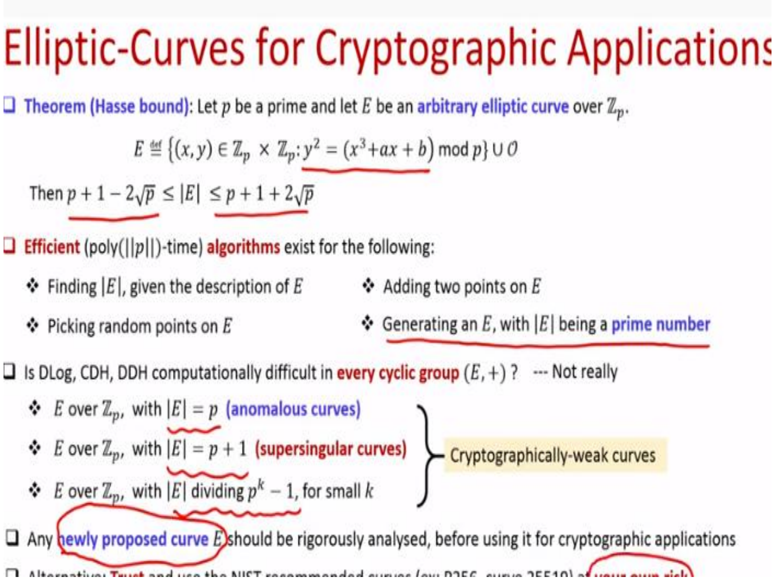
Now we have another candidate group namely the elliptic based cyclic groups and let us see how exactly the DLog problem, CDH problem and DDH problem will look like over these groups because in the description of the DLog, DDH and CDH problem that we had seen in the last lecture we assumed that underline group operation is the multiplicative operation but now we just want to recast those definitions in the elliptic curve based cyclic groups.

So what you are given here is the given description of a cyclic group based on the points on the elliptic curve modulo prime and say the size of the group is a prime number q and you are given a generator that means different powers of g namely up to q – 1th power of g would have given you the all the set E. Then the DLog problem is as follows the challenger here picks a random index from the set 0 to q – 1.

And it gives g^{α} which basically is α times g which is nothing, but the element g added to itself (α – 1) times and the challenge for the adversary is to find out the index α. There is a CDH problem is the challenger has picked 2 random points from the elliptic curve by picking the indices α and β and computing α times g and β times g and the goal of the advisory is to compute the Diffie Hellman function without knowing α and β.

And the DDH problem is the challenger prepares a triplet where the first 2 components are random points from the elliptic curve and the third component is either the output of the DH function the Diffie Hellman function with respect to the first 2 components or a random point from the curve and the goal of the adversary is to find out whether he is seeing a Diffie Hellman triplet or a non-Diffie Hellman triplet

(Refer Slide Time: 22:06)



Elliptic-Curves for Cryptographic Applications

❑ **Theorem (Hasse bound):** Let p be a prime and let E be an **arbitrary elliptic curve** over $\mathbb{Z}_p$.

$$E \stackrel{\text{def}}{=} \{(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p : \underline{y^2 = (x^3 + ax + b)} \bmod p\} \cup \mathcal{O}$$

Then $\underline{p + 1 - 2\sqrt{p}} \leq |E| \leq \underline{p + 1 + 2\sqrt{p}}$

❑ **Efficient** (poly($||p||$)-time) **algorithms** exist for the following:

- ❖ Finding $|E|$, given the description of E
- ❖ Picking random points on E
- ❖ Adding two points on E
- ❖ Generating an E, with $|E|$ being a **prime number**

❑ Is DLog, CDH, DDH computationally difficult in **every cyclic group** $(E, +)$? --- Not really

- ❖ E over $\mathbb{Z}_p$, with $|E| = p$ **(anomalous curves)**
- ❖ E over $\mathbb{Z}_p$, with $|E| = p + 1$ **(supersingular curves)**
- ❖ E over $\mathbb{Z}_p$, with $|E|$ dividing $p^k - 1$, for small k

Cryptographically-weak curves

❑ Any **newly proposed curve** E should be rigorously analysed, before using it for cryptographic applications

❑ Alternative: **Trust** and use the NIST recommended curves (ex: P256, curve 25519) at **your own risk**

So now we have seen the definition of elliptic curves for cryptography applications so the next question that we would like to answer is, is it the case that all elliptic curves modulo prime suitable for cryptographic applications? So before answering that let us see an interesting result for elliptic curve based on elliptic curve modulo prime. So let p be a prime and say E be an arbitrary elliptic curve defined over Z_p which could be a singular curve, non-singular curve namely say E is the collection of all x, y pairs satisfying this equation along with the point at infinity then a very well-known bound which is called as Hasse bound gives you a lower bound as well as upper bound on the number of points which we have on this elliptic curve. So this is the lower bound $(p + 1 - 2\sqrt{p})$ and this is your upper bound $(p + 1 + 2\sqrt{p})$ and interestingly we have poly time algorithms polynomial in the number of bits that we need to represent a prime p which can give you the cardinality of the elliptic curve, we also have poly time algorithms for picking random points from the curve, we also have poly time algorithms for adding 2 points and we also know how to generate an elliptic curve where the size of the elliptic curve is a prime number. So the next question that we would like to answer is that is the DLog, CDH and DDH problem computationally difficult to solve in every elliptic curve based cyclic group and answer is not really.

So there are certain curves which we should completely avoid for instantiating cryptographic primitives. So we cannot take the curves defined over Z_p where the size of the curve or the number of points on the curve is exactly p which because there are well known algorithms for solving the DLog problems in those groups, so these such curves are called as anomalous curves.

In the same way we should avoid curves where the size of the curve p + 1 which are called a super singular curves and we should also avoid curves where the size of the curve is p^k - 1 for a small group. All these curves are cryptographically weak curves because as I said earlier the instances of DLog problem is very easy to solve in this group.

That means if tomorrow you are proposing a new elliptic curve based modulo prime then we have to very rigorously analyze the security property of those elliptic curves before we take those elliptic curves and perform operations on those curves to instantiate any cryptography primitive say for example a Diffie Hellman key exchange protocol and it turns out that analyzing any newly proposed elliptical is a very challenging task.

So an alternative that you can do is that you can trust and use any of the NIST recommended curves if for example P256 curve, curve 25519 which have been rigorously analyzed by NIST and they claim that they have not found any weaknesses in those curves in terms of solving the DLog problem that means there exists no polytime algorithms to solve the DLog problem for computing the DLog of any randomly given point on those curve.

But you should trust the claim of NIST at your own risk and that is why when a government of any country tries to adopt any cryptographic primitive where the underlying cyclic group is based on elliptic curves then they become very skeptical of using or trusting the curves which are recommended by NIST because they believe that there might be some loopholes which only NIST knows, but it is not known in the public domain and that is why the government for such critical application pushes to come up with new curves and try to analyze those curves and use those curves for instantiating the cryptography primitives. But it turns out that for many practical purposes these curves are very popularly used for instantiating the elliptic curve and the cyclic groups for instantiating the cryptography primitives.

So that brings me to the end of this lecture just to summarize in this lecture we have introduced the second class of cyclic groups where we believe the DLog, CDH and DDH problem to be difficult namely the cyclic groups based on elliptic curves modulo prime. The advantage of these groups compared to the cyclic groups Z_p* multiplicative modulo p is that here the best known algorithms for solving DLog problem is of the order $2^{n/2}$.

So we do not have to operate with very large modulus namely 2048 bit modulus which was the case for cyclic subgroups of Z_p* its suffice to set the model as size to be 256 bits and we get the same level of security as you could expect from AES 128 and not only that the cyclic groups based on elliptic curves gives you another additional structure which we call as pairings which can be used for constructing advanced cryptographic primitives. Thank you