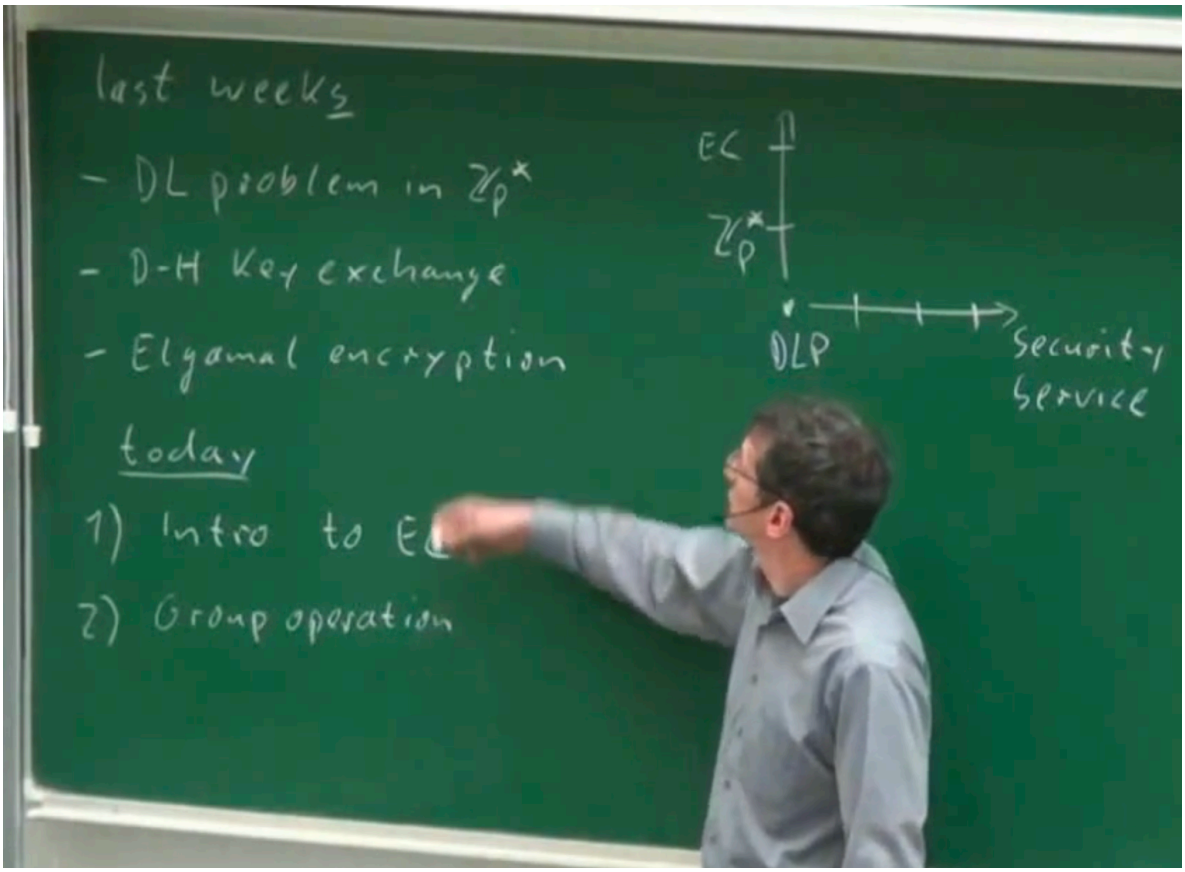
Chapter 16. Introduction to Elliptic Curves.

Last weeks:
- DL Problem
- D-H key exchange
- Elgamal encryption

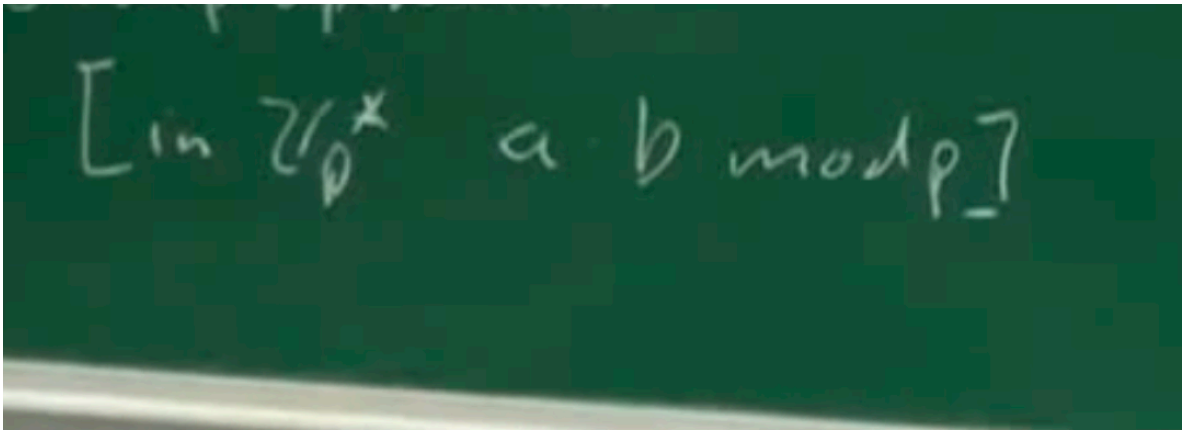
Best thing about DL problem is that we can develop different crypto systems like Key Exchange, Encryption and there is one more thing called Digital Signatures.

we can do all the above with this but there is one more dimension so we need not to compute in Zp*, we will using very different mathematics to build similar protocols.



Today we are going to talk about:
1. Introduction to EC
2. Group operation.

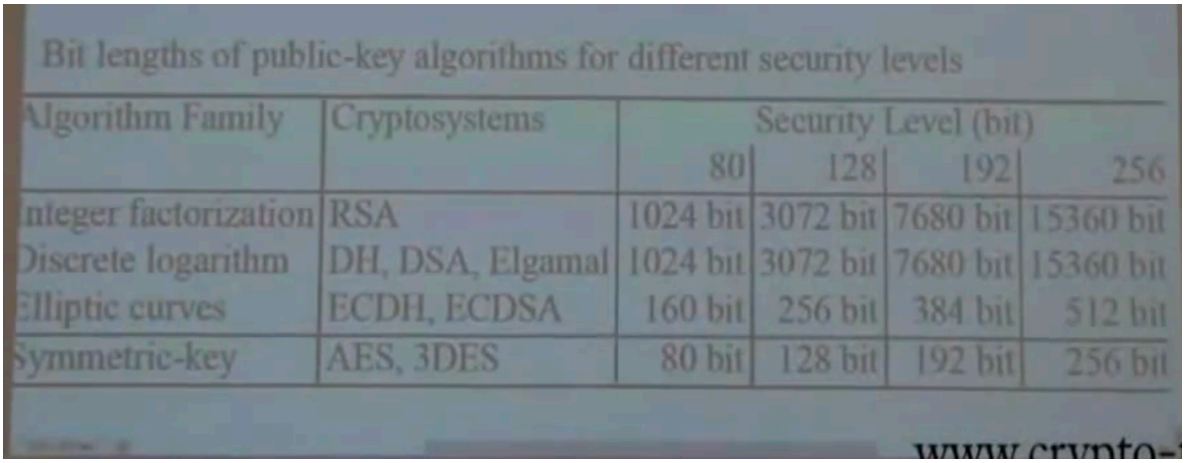
Question: What is the group operation in DL in Zp* ?
it is Multiplicative group.



Today we discuss about the group is also cyclic group, We will do today very different type of Arithematics:

Introduction of Elliptic Curves -> it also is a cyclic group
Motivation:
Question is why are we doing this? Why is this even necessary ? in Zp* we are able to do all the things then why ?

Actually the bigger motivation is:



Bit lengths of public-key algorithms for different security levels

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete logarithm	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric-key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

www.crypto-

in the above table you can find that for block cipher like AES the security we get with 80 bits require 1024 bits of RSA and DH and 160 bits of EC and if we want to go to 256 bits of security then general public key cryptosystems require very large key lengths which means a large/very complex computation so we want to find a public crypto system which is comparable key length and security so we have **EC.**

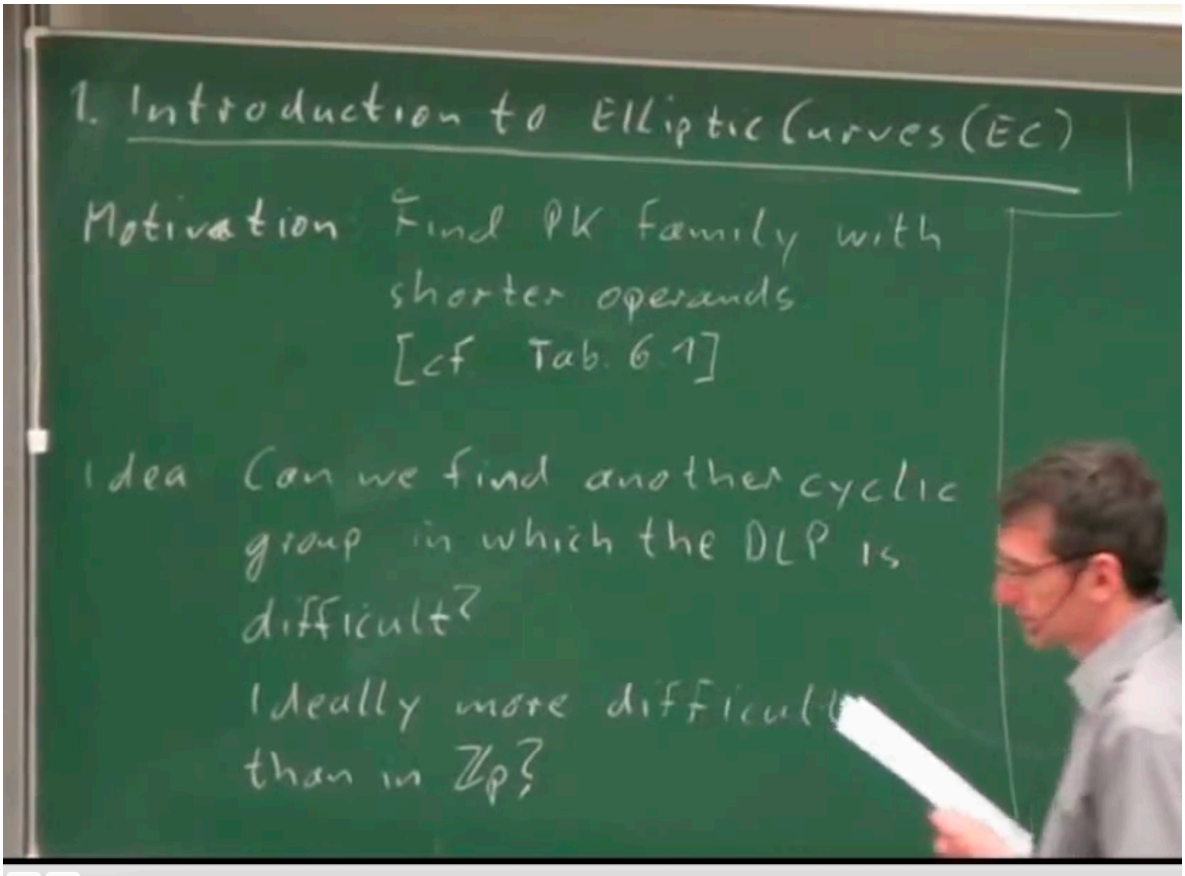
Here we are not concerned about key lengthbut the kind of computations involved by multiplying such large numbers. Most of the new applications, use EC opposed to RSA.
Say in case you want to add public key crypto into smart cards which are 8bit processors so you cannot do that using such big key length as computations

are too difficult as the key length increases.
Actually all the modern application most of them is having EC implemented instead of RSA.
This will be the crypto system of the future.

Motivation is : find a public key family with shorter operands. we are not looking for only encryption instead we are looking for Encryption, Key exchange and Digital Signature.

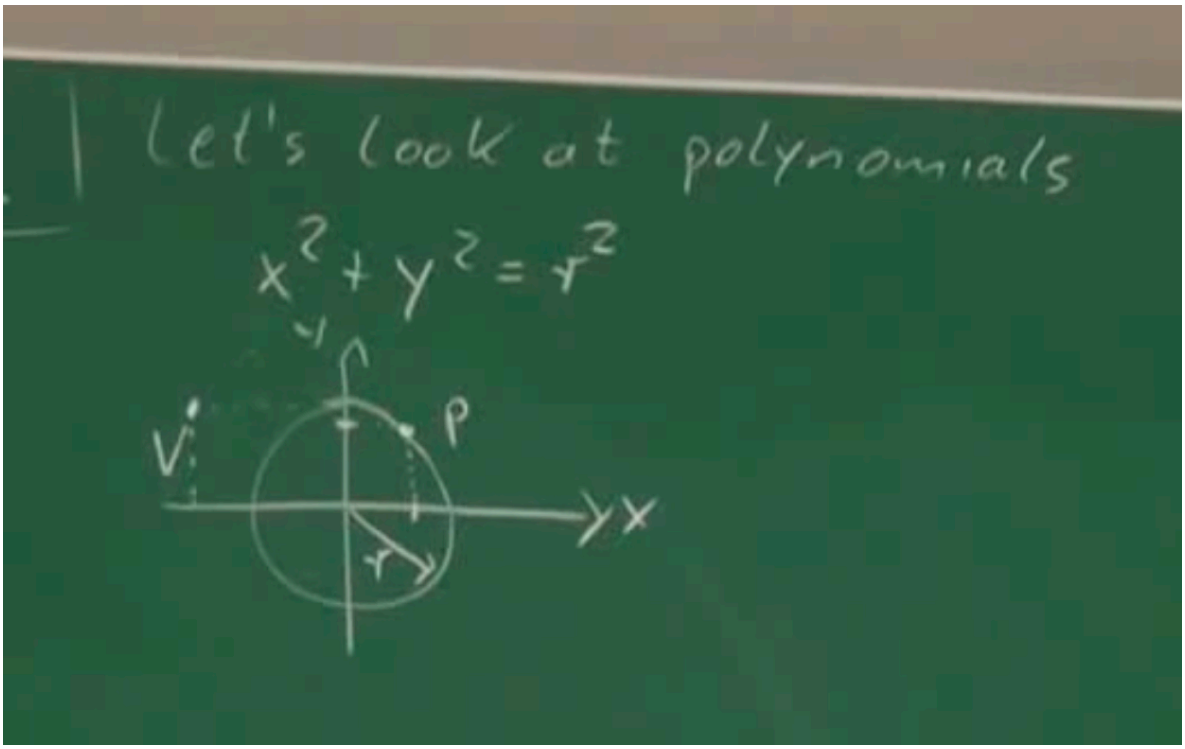
Idea: idea is to find another cyclic group in which DLP is difficult ? ideally more difficult than in Zp*.
Answer is Yes, and reason is why do we choose 3000 bits ? because there are fairly powerful attacks exists which are forcing us to go upto 3000 bits.

this means this is a hard problem but it is not as hard as it is like to. For EC it is different case where best attack against EC is much much weaker and requires only 256 bits and it takes 2^128 steps to solve the EC problem.



EC is very complex.
Let's look at polynomials :

X^2 + Y^2 = R^2
above equation is circle equation.

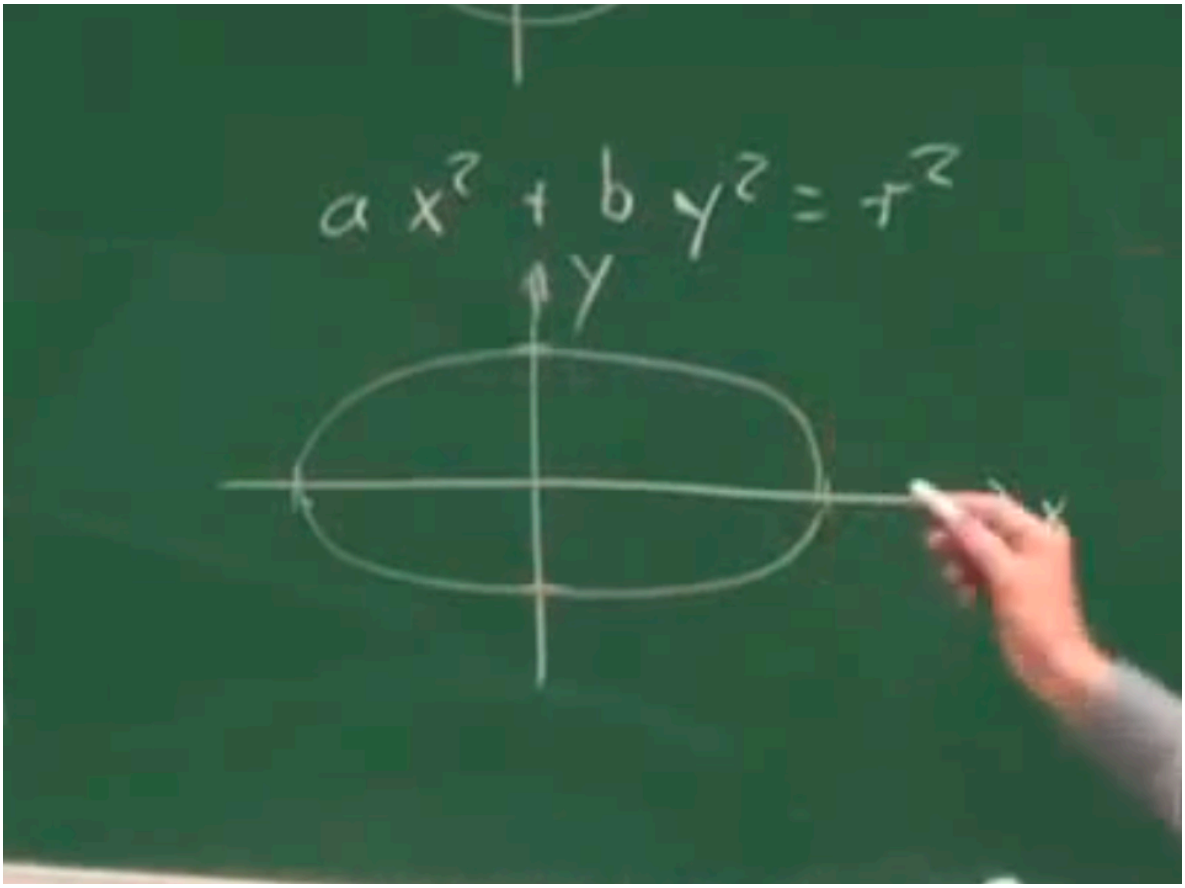


P is on the circle is because it satisfy the equation but V is outside of the circle because it doesn't satisfy the equation.

Now say we have introduced variables a and b in the circle equation ie

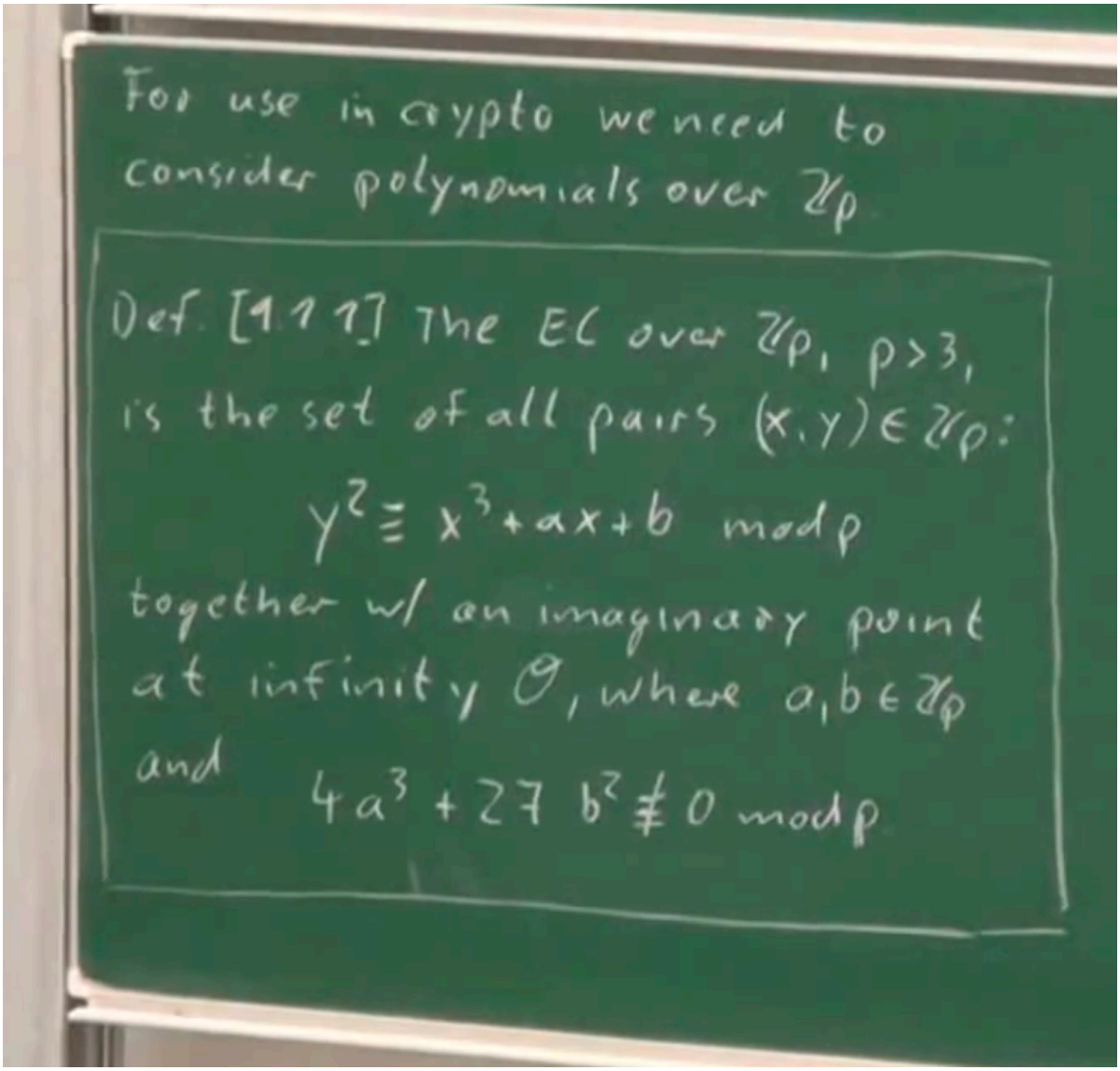
a*X^2 + b*Y^2 = R^2;

what is this equation ?
it is Elliptical curve.



both the above equations are on **Real Numbers**.
For use in crypto we need finite fields so we need to consider polynomials in Zp ie modulo p.

Definition of Elliptical Curve cryptography:
The Elliptic curve over Zp where p > 3 , is the set of all the pairs which fulfill
Y^2 = X^3 + a*x + b mod p
together with an imaginary point infinity where a,b belongs to Zp and 4*a^3 + 27*b^2 not equal to 0.



Definition 9.1.1 Elliptic Curve
The elliptic curve *over* $\mathbb{Z}_p$, $p > 3$, *is the set of all pairs* $(x,y) \in \mathbb{Z}_p$ *which fulfill*

$$y^2 \equiv x^3 + a \cdot x + b \bmod p \tag{9.1}$$

together with an imaginary point of infinity $\mathcal{O}$, *where*

$$a,b \in \mathbb{Z}_p$$

and the condition $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \bmod p$.

Lets start breaking this definition to understand more:

1. Lets talk about the condition, actually certain curve have undesirable properties which we cannot use in cryptography and these are these curves.

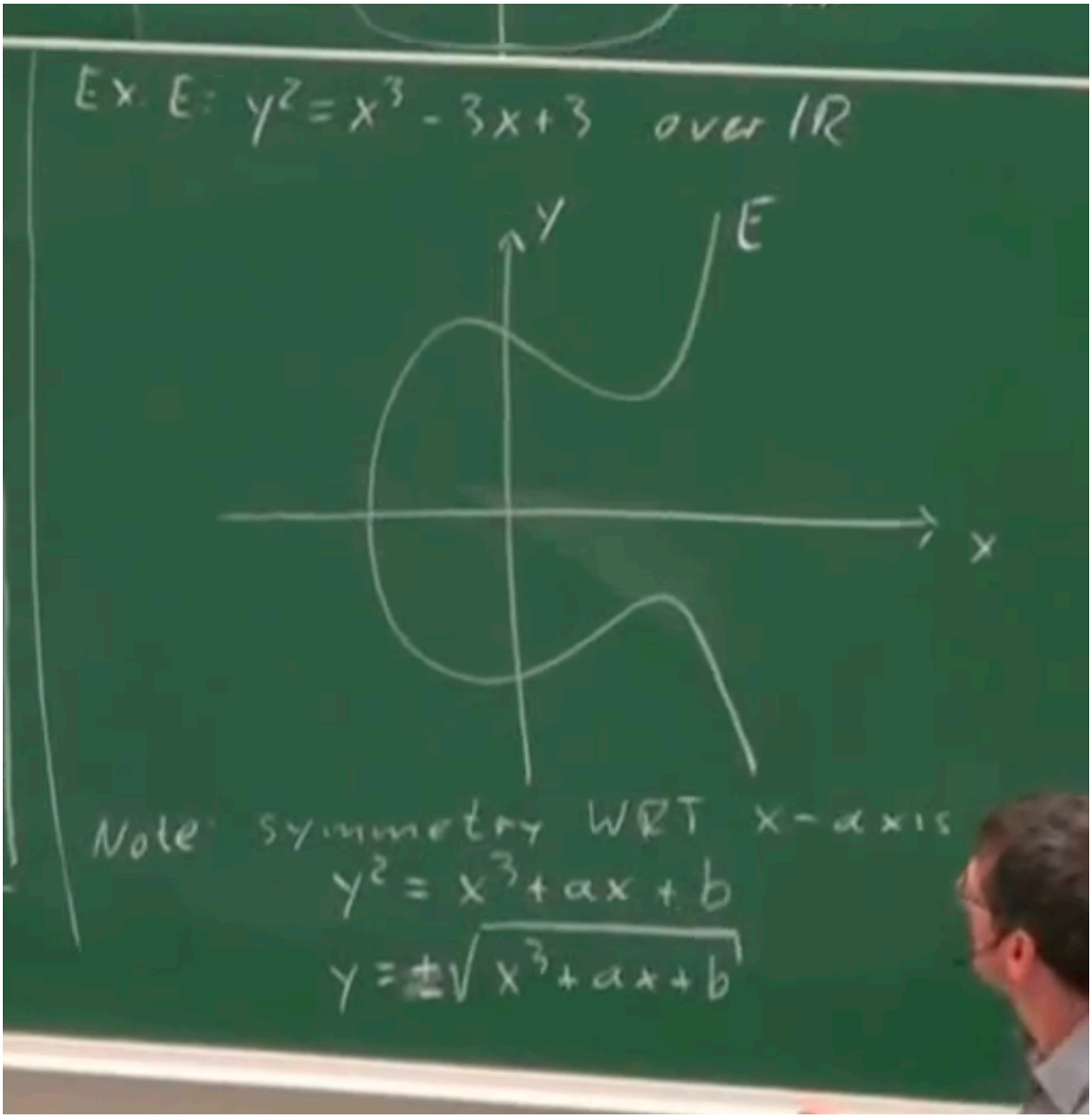
so the elliptic curves which are not fulfilling this condition , then that is not the

curve which we are using in cryptography.
it is out of course.

If you are looking at the definition purely mathematically then it is really hard to understand and it looks very arbitrary but nice thing is there is a very nice geometric interpretation to this.

Looking at geometric interpretation of EC:
e.g.
$y^2 = x^3 - 3x + 3$
to use this equation in cryptography, we need to do Modulo P operation ie say modulo 17.
but as soon as we introduce this modulo P arithmetic, we cannot draw diagram as it becomes distorted.
Nice thing is just take same equation over R ie Real Numbers and understand it and then we can do this with modulo operations.

Someone who has studies Crypto knows that this corresponds to following shape:

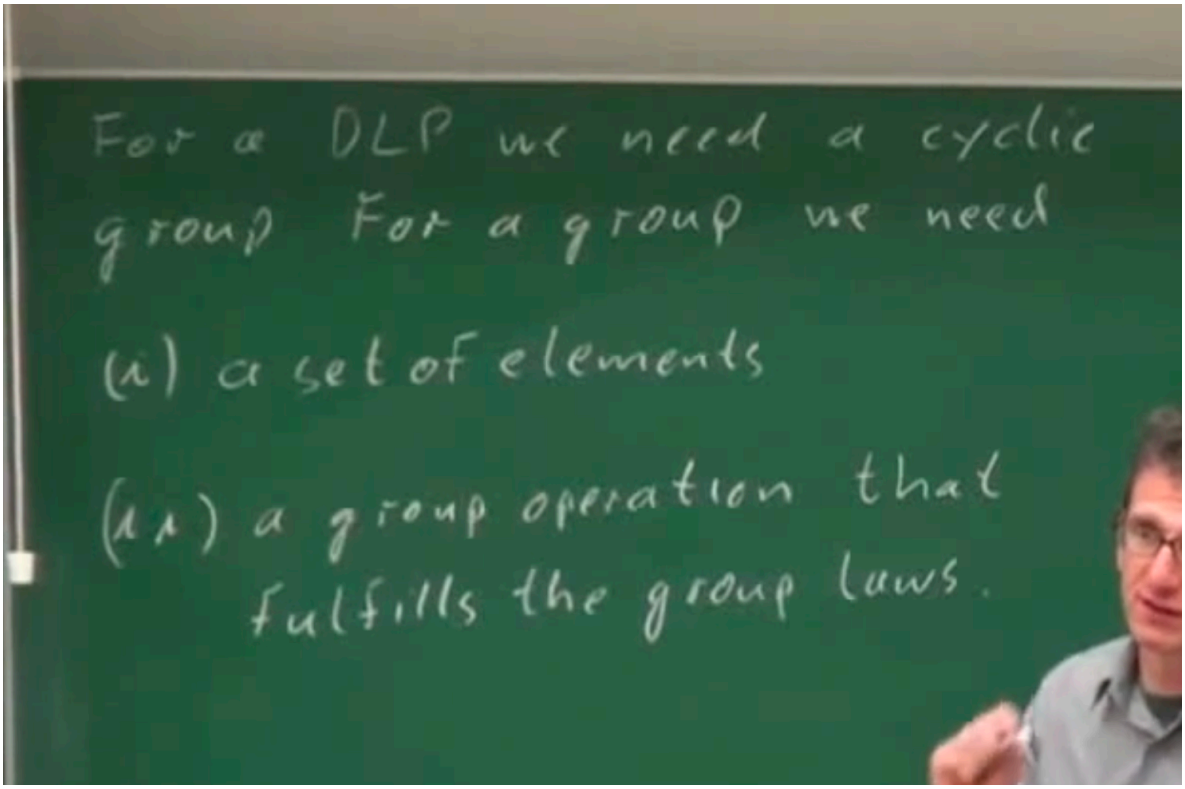


Note that it is symmetric with respect to X axis and why is that ?
answer: as if we try to find y then we get + and - roots of the the equation as depicted above in the diagram.

Question: Why elliptic curves are only considered not other curves like circle/cone etc are considered. what is so special about EC?

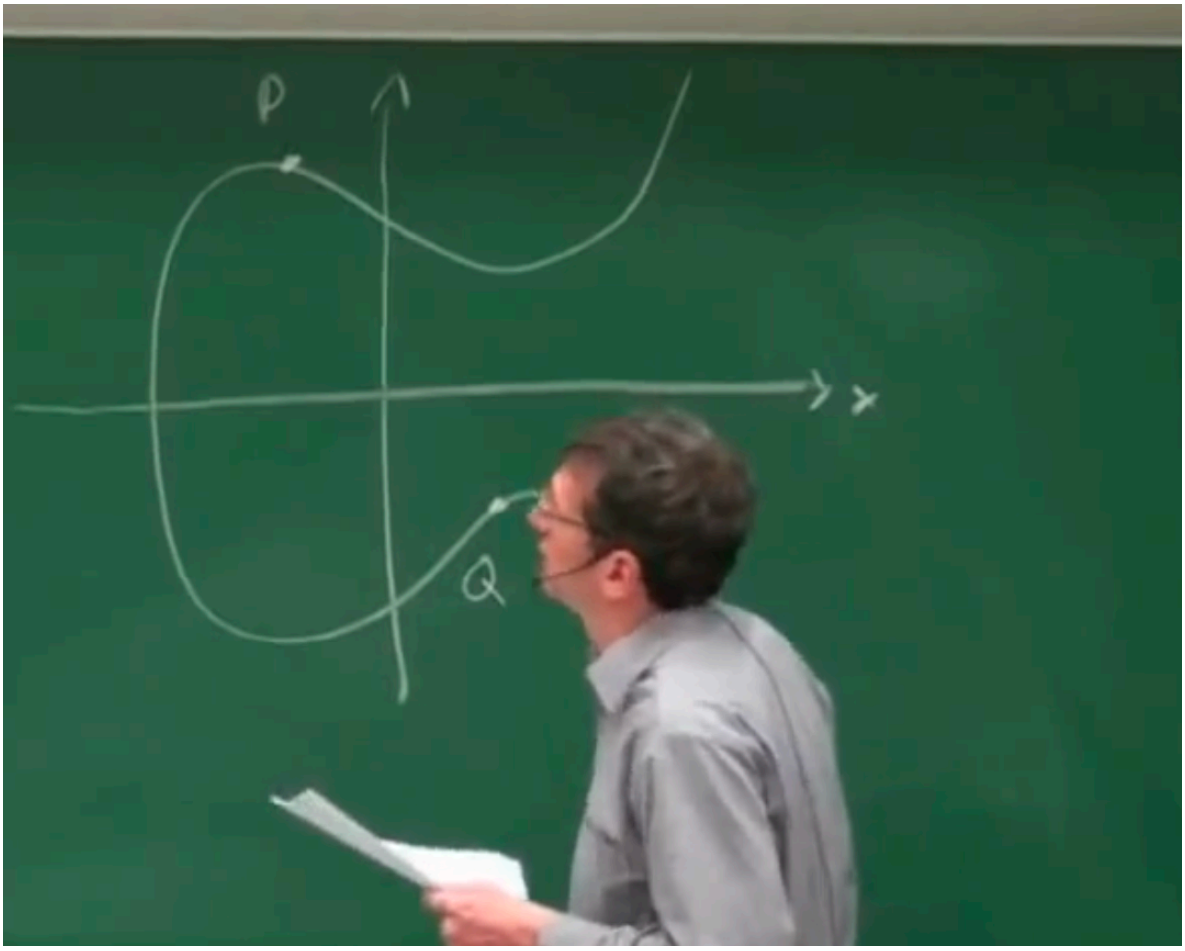
Now for DLP we need a cyclic group so we need :

1. Set of Elements and in case of EC it is points on the Curve but in Zp* the elements are Integers ie so far the group elements are integers but in EC group elements are the points in the curve.
2. Compute on the curve or compute in the set ie A group operation that fulfils group laws.



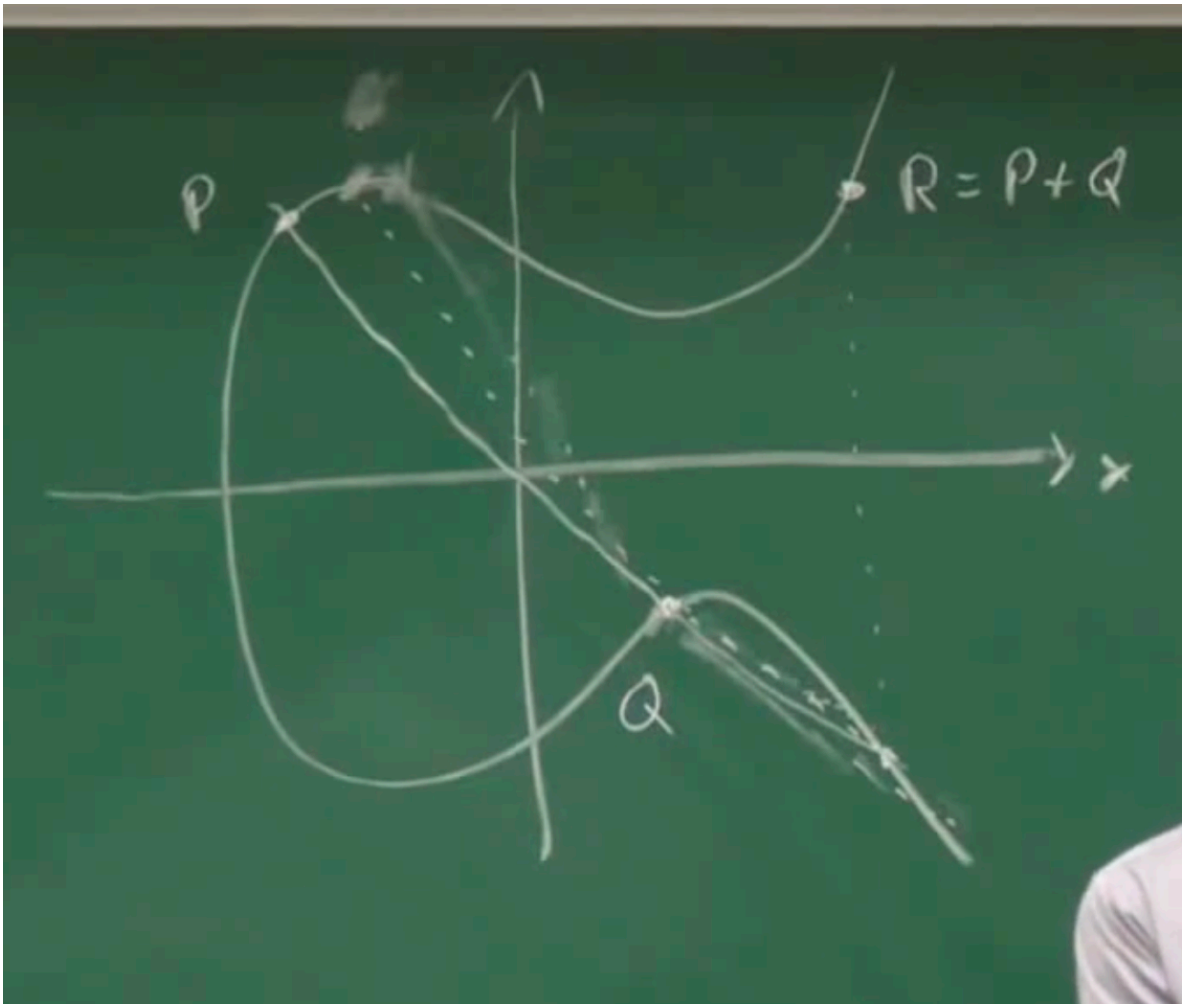
Important:

Group Operations:
Say following is the Elliptical curve diagram:



In this diagram we have 2 points P and Q now **Question is how to compute the group operation ? ie P + Q = R ? How to add 2 points ?**

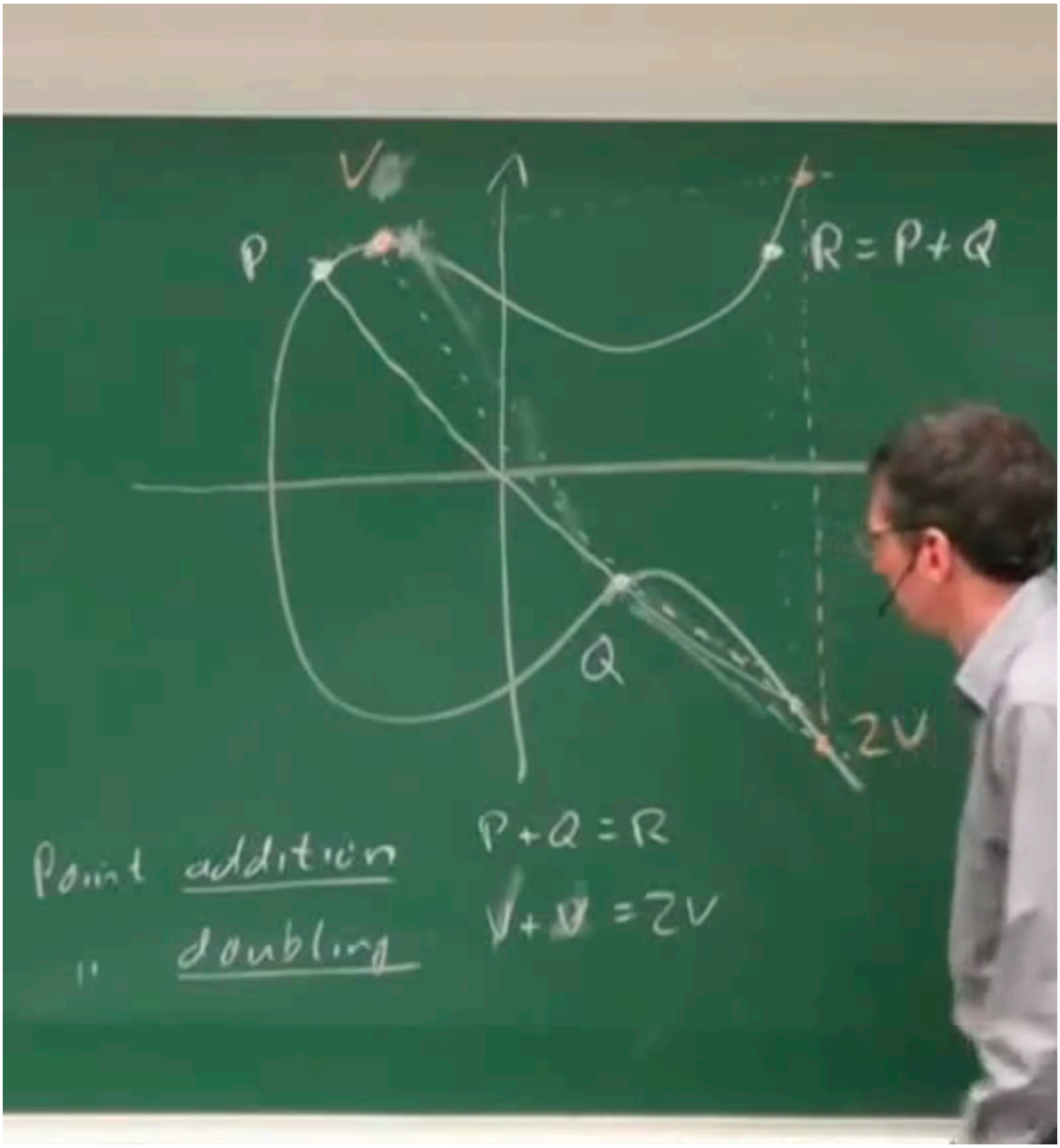
To add 2 points you are going to draw line in 2 points (Connect the 2 points), you get the 3rd point of Intersection and mirror to that intersection point is P + Q



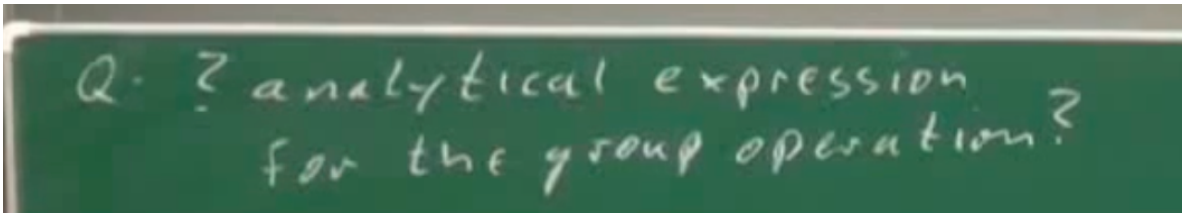
So say 2 points are given and group operation is Addition then compute the line and find the third point and then mirror the point and the resulting point by definition is R.

If you want to compute P + Q where P != Q then you follow the above approach but that if we want to do Point Doubling ie V + V ?

this construction might not work so we need to draw tangent and then we get the intersection and then mirror that.



So now question is how does black berry does all this ? it is surely not computing all this geometry ?
so all the devices are doing this using computations and not using geometry.
Analytical Expression:



Idea is Given E (Elliptic Curve) : Y^2 = X^3 + a*x + b,
P = (X1, Y1)
Q = (X2, Y2)

Find R ?

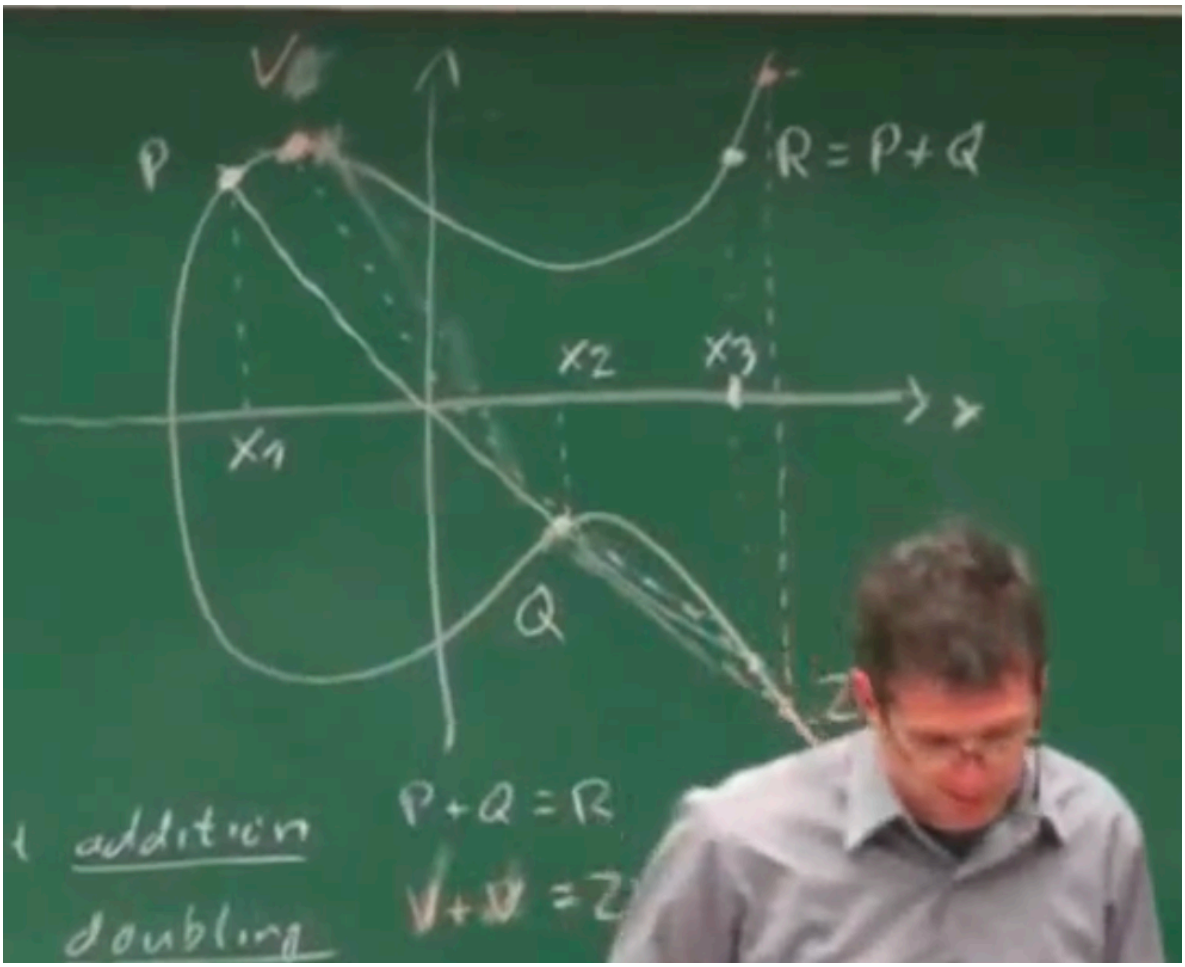
Question: How are we doing this Geometric construction ?
We are drawing line ie connecting the points so the line **L**
equation of line is : Y = s*X + m where s is slope and m is coefficient.

Now we have an Elliptic curve and a line and we want to find the intersection of both. This is quite simple as we just need to equate.

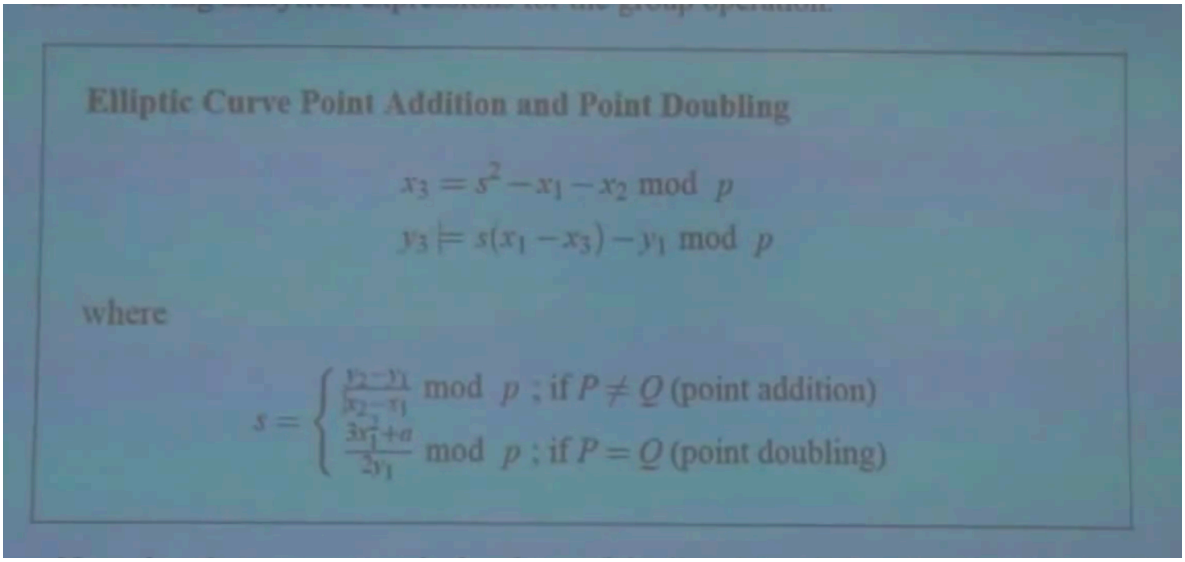
replacing Y with s*X + m in equation so equation becomes:

(s*X + m)^2 = X^3 + a*x + b

now if you look at the equation so how many roots of the equation. Because equation is of degree 3 so maximum real distinct roots will be 3.
as we are already having 2 roots so we can find the third one easily.
we know X1, X2 and we need to find X3 i.e.:



After computing all the steps we will reach at the following formula:

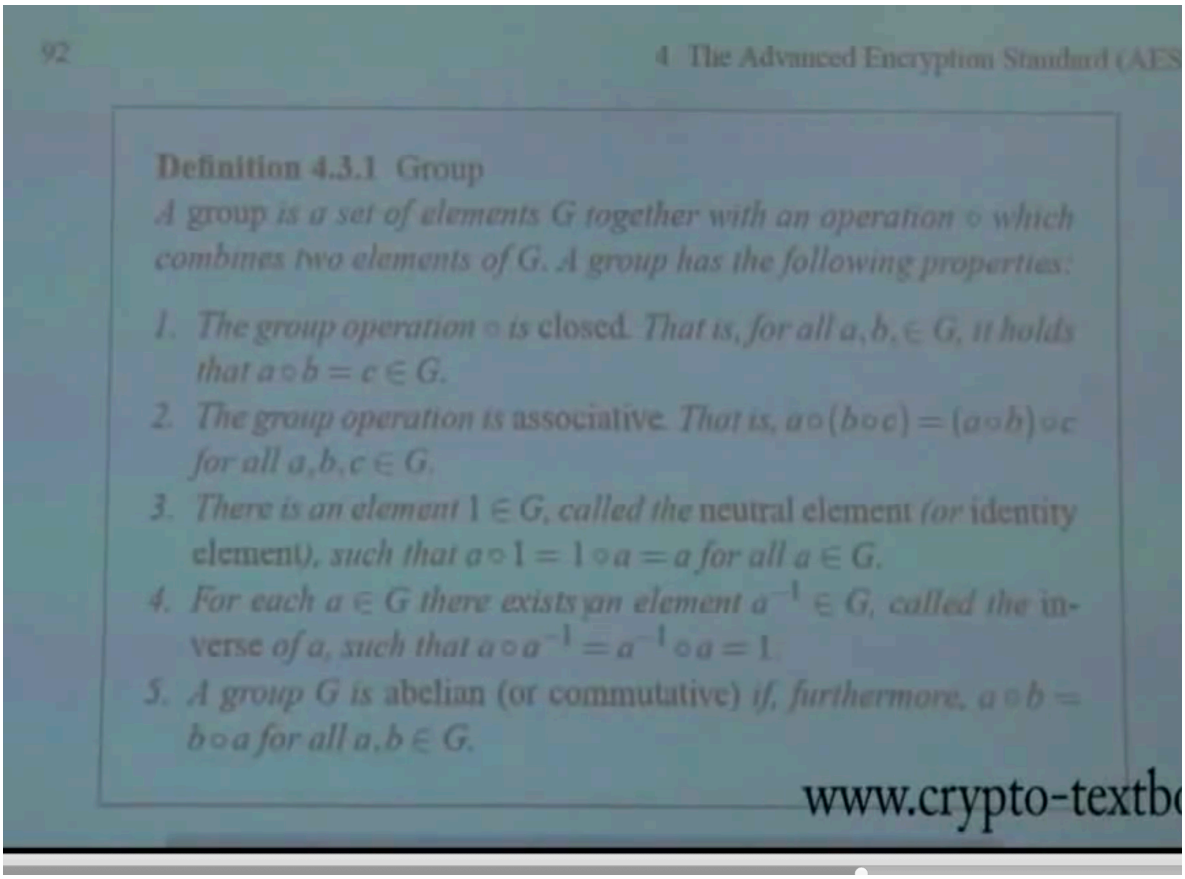


you get the formulae in page 244 cristof paar book.

For finding slope the formula is Y2 - Y2/X2 - X1 mod p but if we do direct division we will get the rational number or say decimal number so instead we use (Y2 - Y1)* (X2 - X1)^-1 mod p ie we compute the modulo inverse and multiply instead of dividing.

So question is which algorithm is used for finding the inverse ? **EEA**

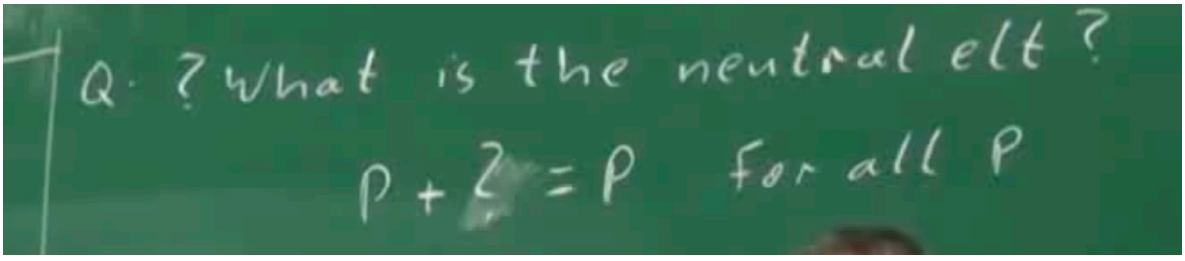
As we see that Addition operation follows the group laws
Little information about group laws again:
so we need to fulfil all the below laws :



First law says that group operation is closed ie A dot B = C and C also belongs to the Group.
In our case dot is addition and as we know that P + Q gives R which is also on the curve so it satisfy the statement.
Better argument for this is that we are considering the points of intersection and intersection always on the curve so **First Law satisfy.**

For Second Law ie associative ness, we cannot see that but as per Paar it is associative.

Now 3rd and 4th laws are quite tough and hard part. we are looking for identity element in case of 3rd law so what we need is:



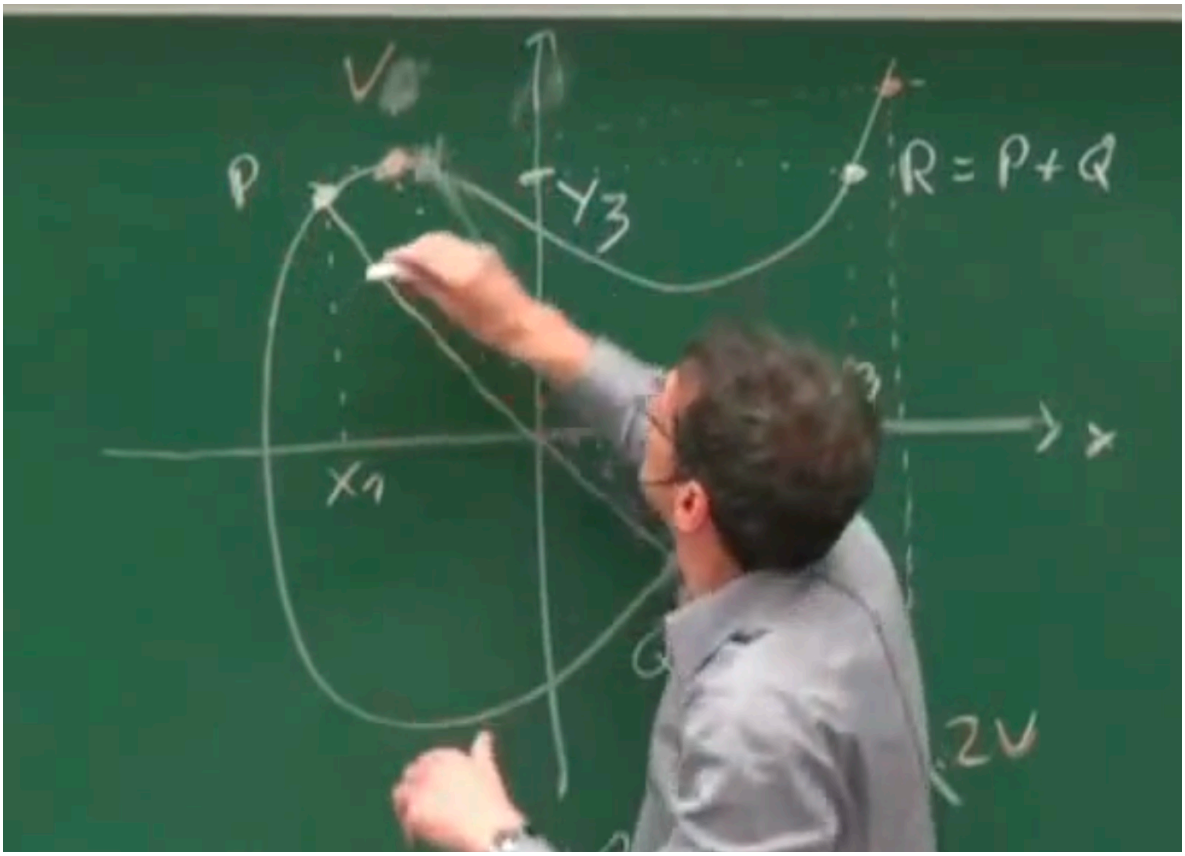
ie we need a point added to P gives P only ie a null element.

So what we are trying is that we can find a point on curve which once added to P gives P again but actually there is no point on the curve that serves as a null element or identity element or null point so **what we do is, we artificially**

define a point (Dirty trick).
=> We define a “Point at Infinity”
Property 3 of definition 4.3.1 is now P + Infinity = P for all P in Elliptic curve

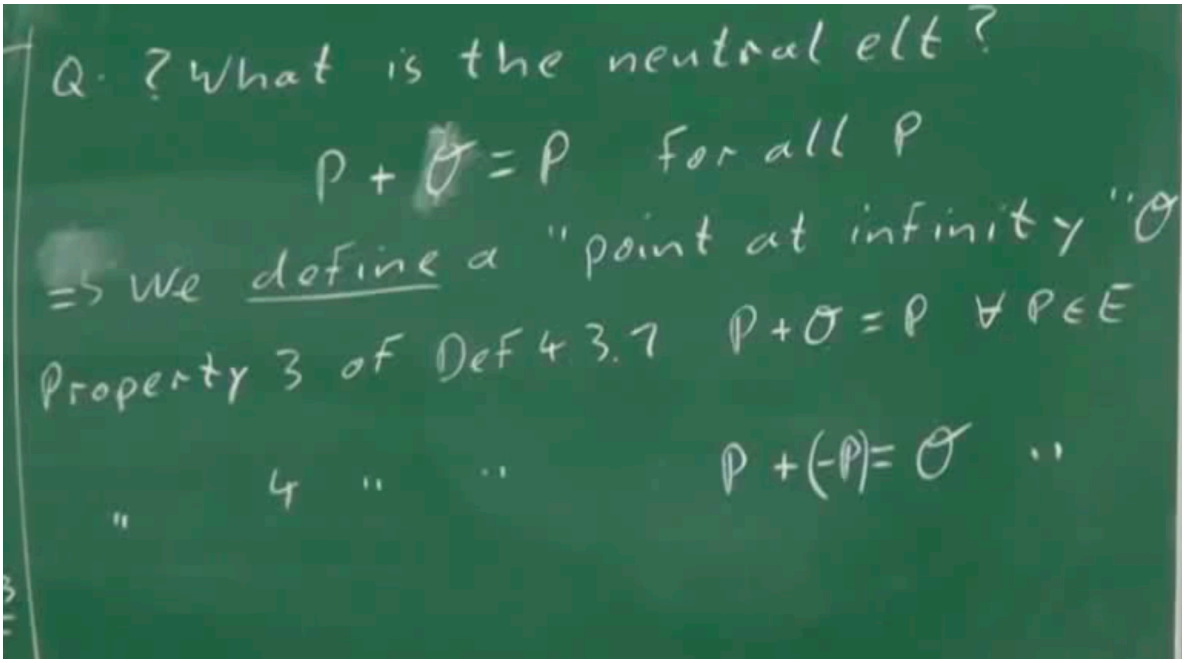
Now Question comes what is this Point Of Infinity ?
Geometrically what works is say a point is + or - infinity along Y axis then if you imagine this you can see it works.

Experiment:

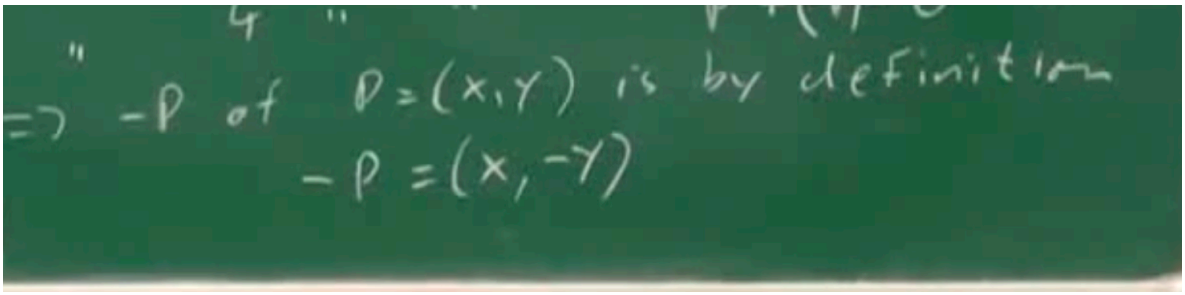


Think point of infinity is + infinity on Y axis then if we connect P and Infinity them that line becomes parallel to Y axis almost and then **Question is what is the 3rd point of intersection ?**
Answer is -P which is on the curve and then taking mirror image of -P we will get P again and it holds the 3rd property of group law.

once we have the identity element which is “Point of Infinity” we need to fulfil property 4 of the group definition which is **P + ? = Point of infinity ie we need to find the inverse of Point “P”** Which is -P



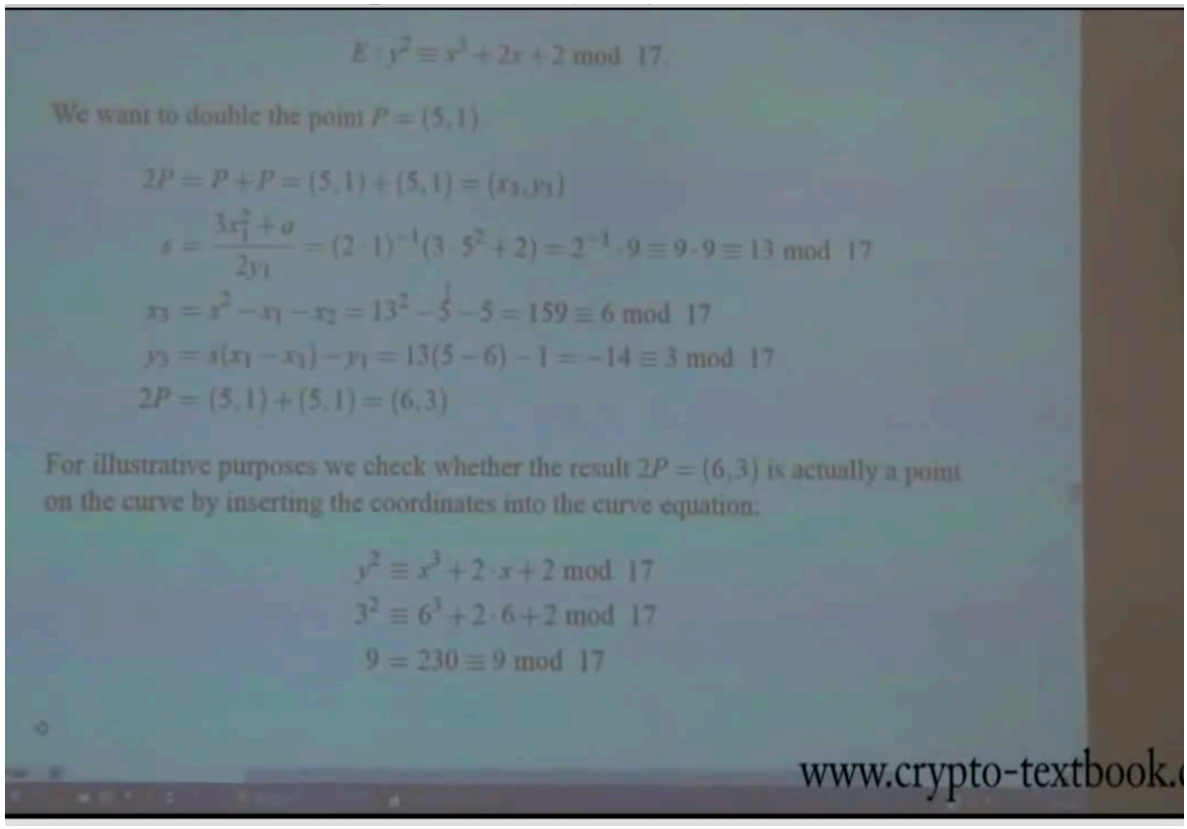
Now this -P is not something like imaginary point but actually it is point on the curve.
Actually it is the mirror point of P.



-P is actually mirror on X axis of -P = (X, -Y) if P is (X,Y)

One nice property of Elliptic cryptography, finding inverse in group is really easy in EC which is very tough in Zp* which needs EEA.

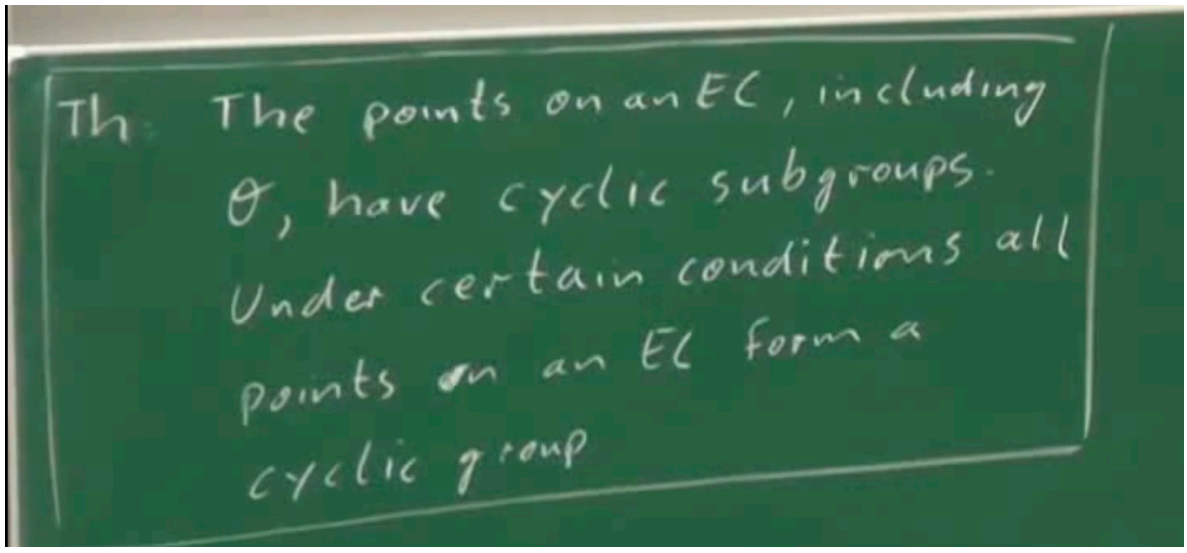
Lets look at an example:



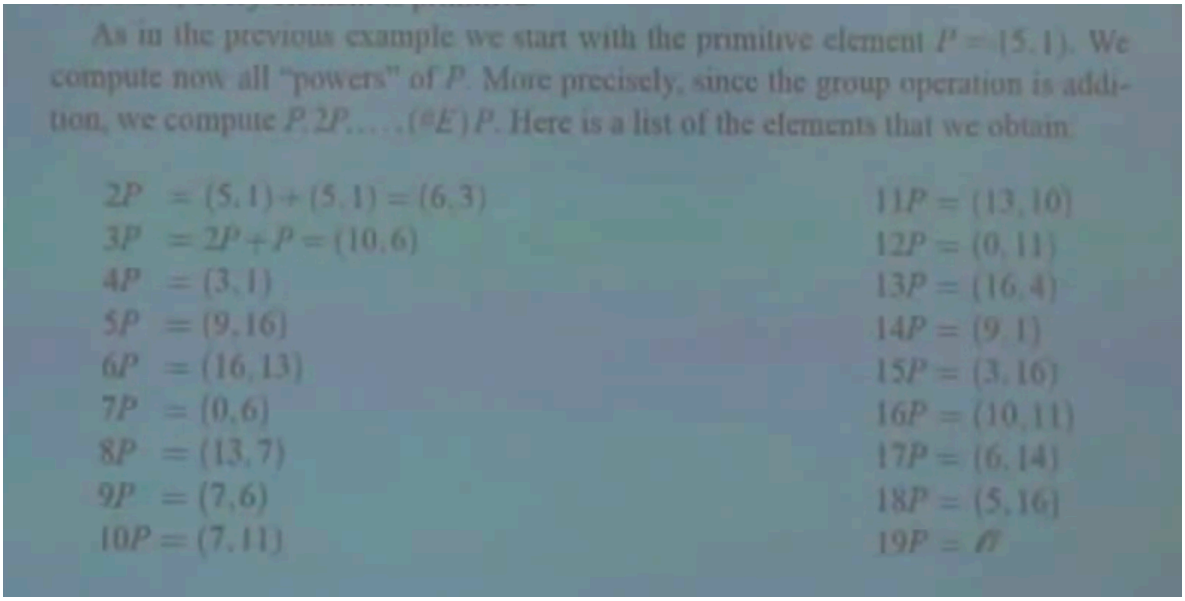
in above example as P == Q so we are doing tangent slope formula.

Final Theorem:
Before that one question, we are talking that we need a group and fulfil the group properties but question is what kind of group we need ?
We need Cyclic Group.

Proving that EC gives cyclic group requires a lot of learning about number theory so this is the theorem.



example: However next week professor par is going to repeat it.



As in the previous example we start with the primitive element $P = (5, 1)$. We compute now all "powers" of P. More precisely, since the group operation is addition, we compute $P, 2P, \ldots, (^{\#}E)P$. Here is a list of the elements that we obtain:

$2P = (5,1) + (5,1) = (6,3)$
$3P = 2P + P = (10,6)$
$4P = (3,1)$
$5P = (9,16)$
$6P = (16,13)$
$7P = (0,6)$
$8P = (13,7)$
$9P = (7,6)$
$10P = (7,11)$
$11P = (13,10)$
$12P = (0,11)$
$13P = (16,4)$
$14P = (9,1)$
$15P = (3,16)$
$16P = (10,11)$
$17P = (6,14)$
$18P = (5,16)$
$19P = \mathcal{O}$

Didn’t understood last 1 minute, may be in next lecture we can understand much.

Research is needed in the below point
|
|
\ /
Question which is still not clear is, Infinity point is considered as the identity element but does that infinity point exists on the the curve and if so then how ?