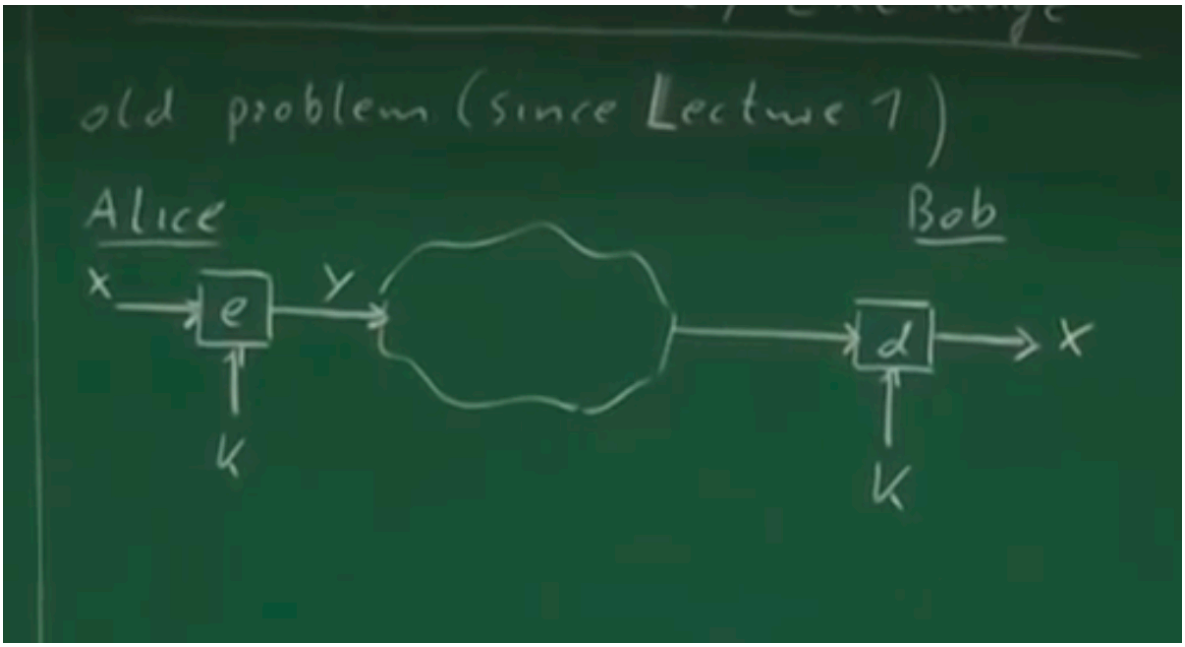
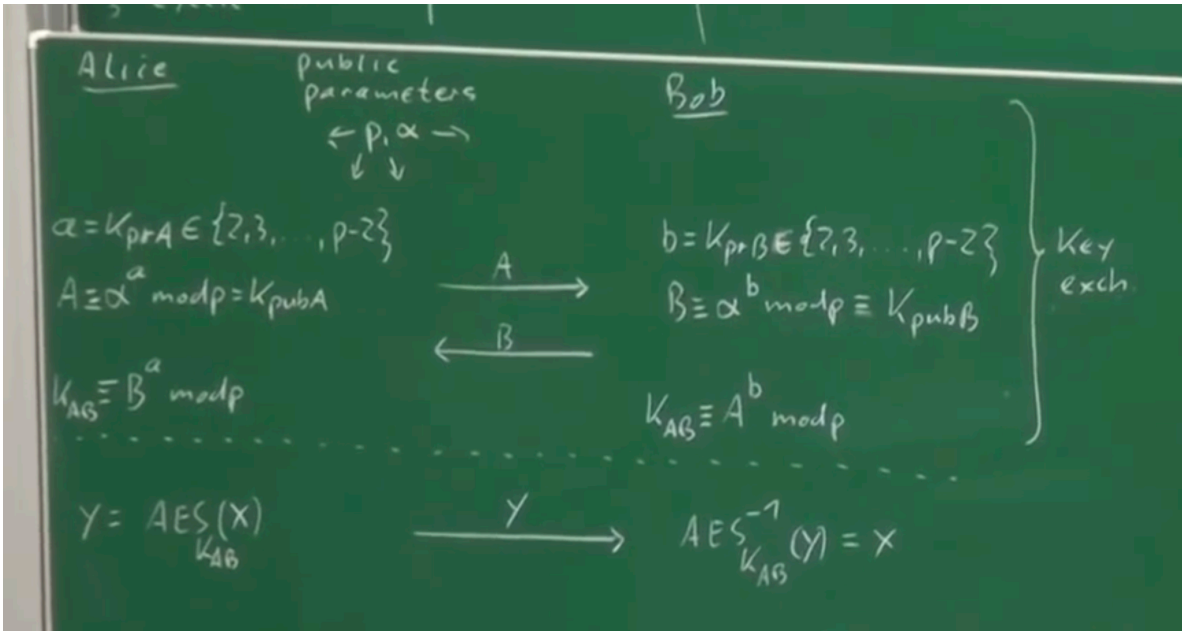
Lecture 13 Diffie-Helman Key Exchange and Discrete Log:
As we know there are hundreds and hundreds of Symmetric ciphers (stream and block ciphers) but in case of Asymmetric cryptography there are only 3 families of cryptography mainly, RSA, Discrete Logarithmic, Elliptical Crypto

1. **Diffie-Hellman Key Exchange**

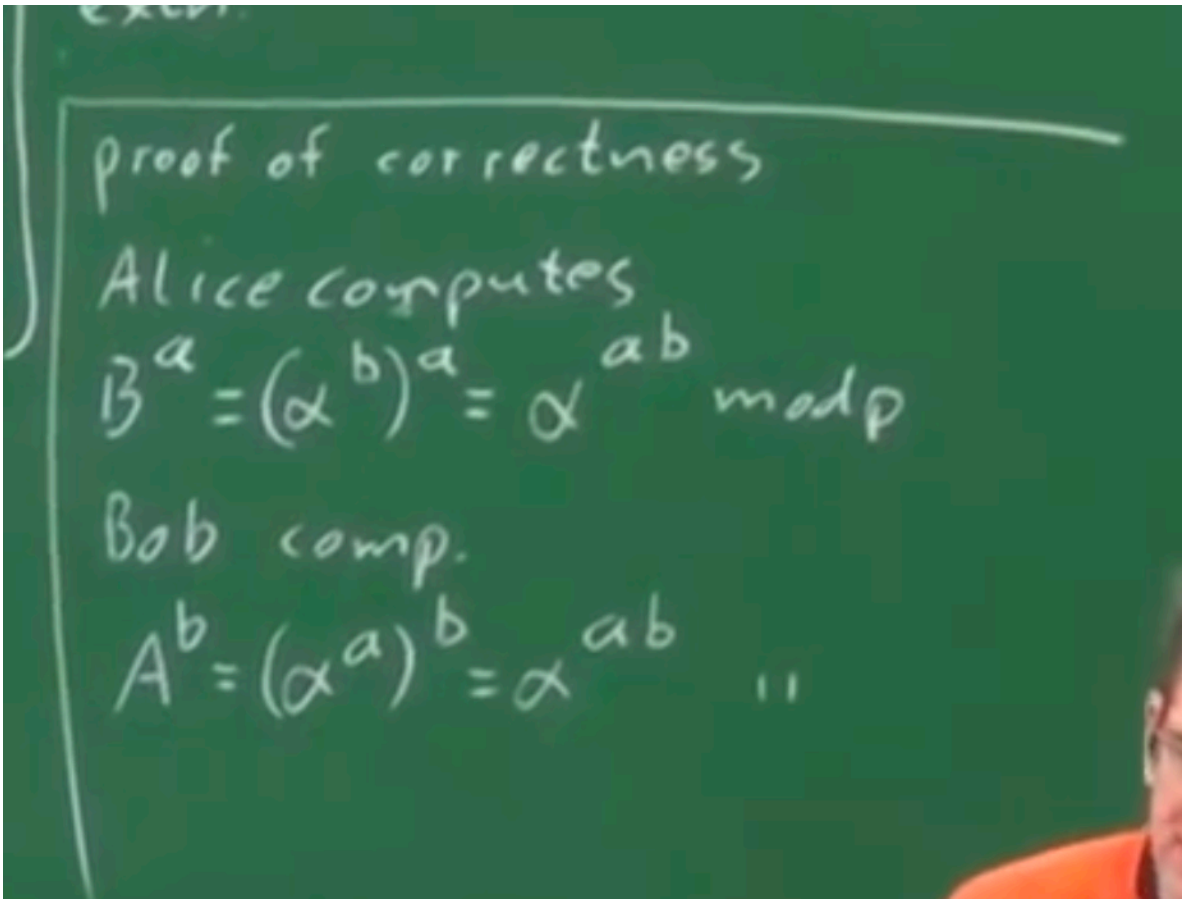


this is the picture of Symmetric Cryptography and question is what is the problem in this ?
Key Exchange is the main problem ie how Alice and Bob can share the Key ?
Main things is by exchanging certain messages over unsecured channel ie oscar can read then, Alice and Bob will be able to exchange the key and oscar cannot get the key.

1. Say we have a set of public parameters called **p and alpha**, where **p is prime and alpha is an integer**. they are publicly known ie oscar also knows about them.
2. Now say alice generates Kprivate key calling it **a** from the set of {2,3...., p-2} randomly
3. Protocol is completely symmetric so bob also does the same and generates **b** from the set of {2,3,....,p-2}
4. Now alice computes public key **A = alpha^a mod p**
5. Bob does the same and computes public key **B = alpha^b mod p** and both of them sends there public keys to each other. (**Exchange**)
6. Now alice after receiving public key from bob does one more exponentiation ie Kab = B^a mod p and same is done by bob ie A^a mod p
7. and main thing is they are the same so they are able to exchange the key.



Proof of Correctness:



Why Oscar not able to crack even after listening to the conversation:

say p = 7 and alpha is 2
now say alice choose 3 and bob chooses 2 as private key (which is **a for alice and b for bob**) and this is not known to oscar
not alice computes public key which is alpha^a mod p and same is computed by

bob:
alice = 2^3 mod 7 = A
bob = 2^2 mod 7 = B
here oscar can read both A and B
now alice computes key as B^a mod p = 64 mod 7 = 1
bob computes key as A^b mod p = 1 mod 7 = 1
so both have the key.

what does oscar have = 1 = A, 4 = B, 7 = p , 2 = alpha
now oscar doesnot have private key so he cannot compute key.

Important assumption is oscar can listen to the unsecure channel but cannot modify the data.

2. **Finite Groups**

Group roughly is a Set with elements and 1 group operation.
Formal Definition:

Definition 8.2.1 Group

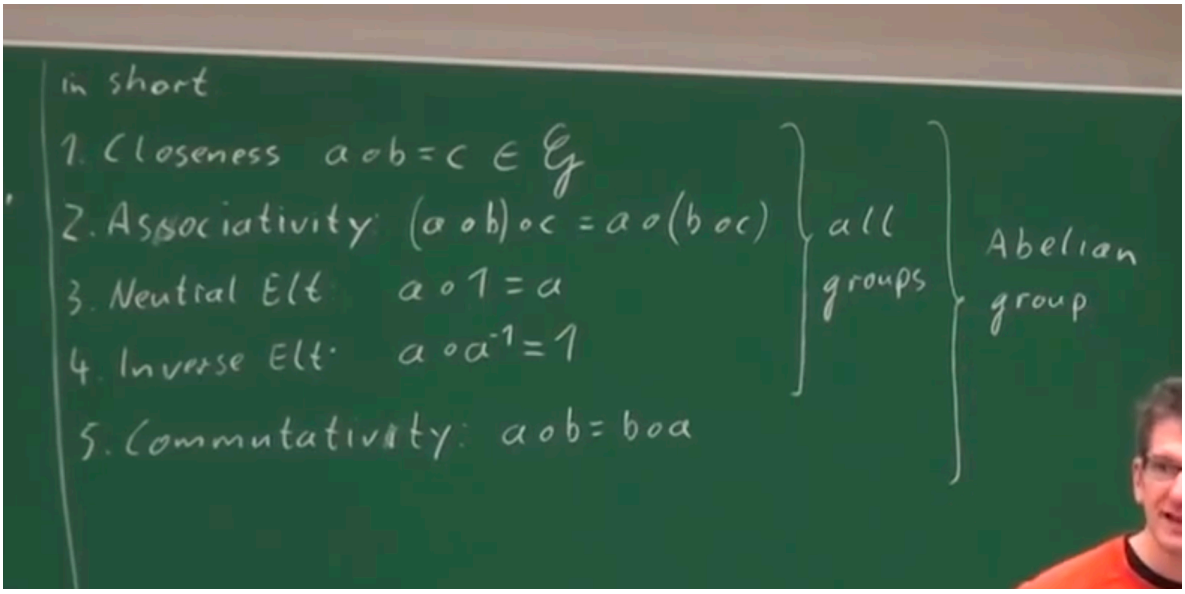
A group *is a set of elements G together with an operation* $\circ$ *which combines two elements of G. A group has the following properties.*

1. *The group operation* $\circ$ *is* closed. *That is, for all* $a, b, \in G$, *it holds that* $a \circ b = c \in G$.
2. *The group operation is* associative. *That is,* $a \circ (b \circ c) = (a \circ b) \circ c$ *for all* $a, b, c \in G$.
3. *There is an element* $1 \in G$, *called the* neutral element *(or* identity element*), such that* $a \circ 1 = 1 \circ a = a$ *for all* $a \in G$.
4. *For each* $a \in G$ *there exists an element* $a^{-1} \in G$, *called the* inverse *of a, such that* $a \circ a^{-1} = a^{-1} \circ a = 1$.
5. *A group G is* abelian (or commutative) *if, furthermore,* $a \circ b = b \circ a$ *for all* $a, b \in G$.

In Layman terms:

1. Closeness —> if a and b belong to group G then the **a dot b = c** and c belong to same group G
2. a.b.c = (a.b).c = a.(b.c) , ie sequence doesn't matter
3. a.1 = a ie 1 is neutral element
4. Inverse Element, ie every element in G has an inverse element ie a . a^-1 = 1 in elliptic curve cryptography 1 has a different meaning.
5. commutative : a.b = b.a

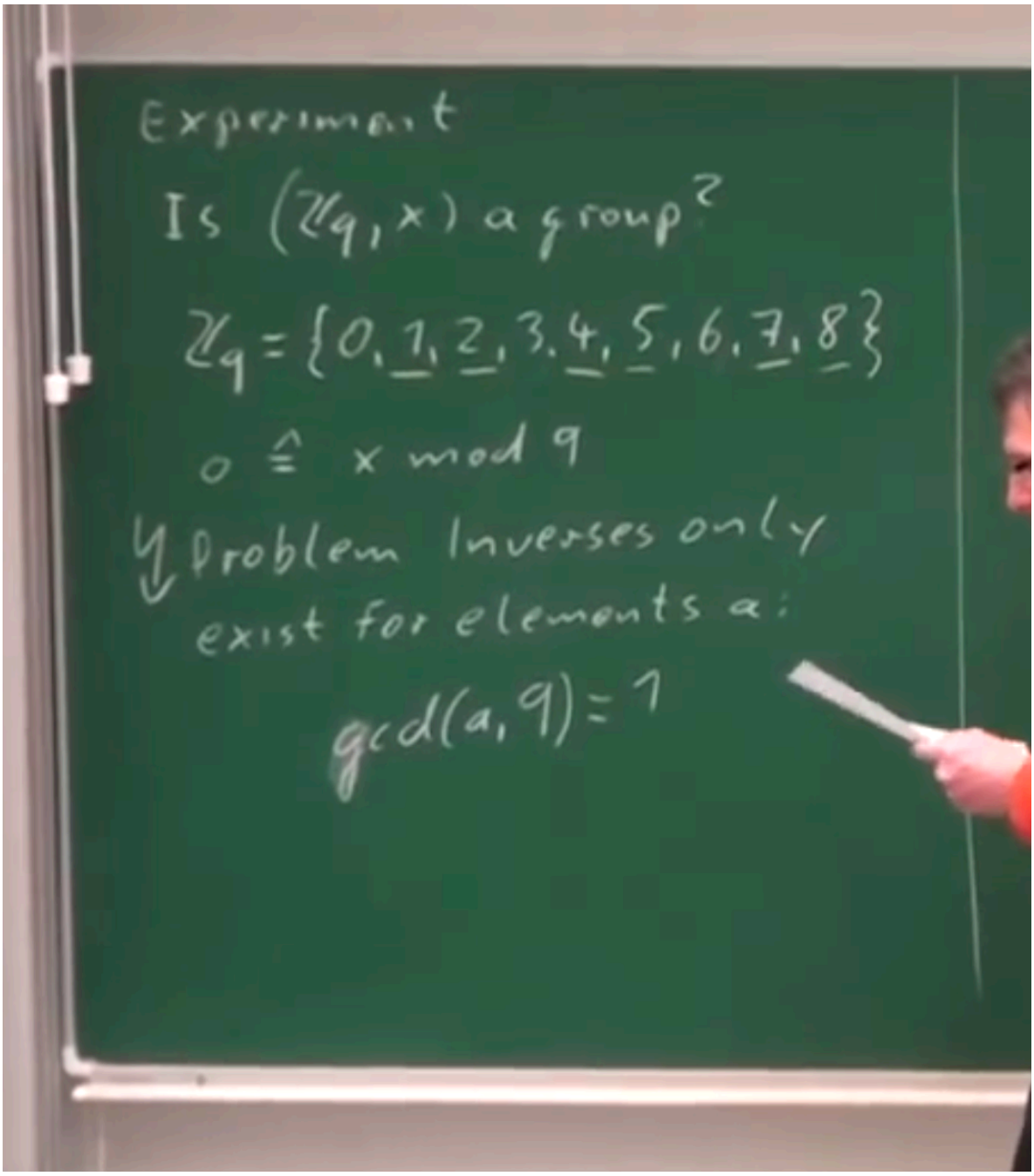
First 4 properties is group , 5th property holds then it is abelian group.



Experiment:
Question: is (Z9, MUL modulo 9) is a group ?
Z9 = {0,1,2,3,4,5,6,7,8}
let's check if the above 4 properties hold for the Z9?

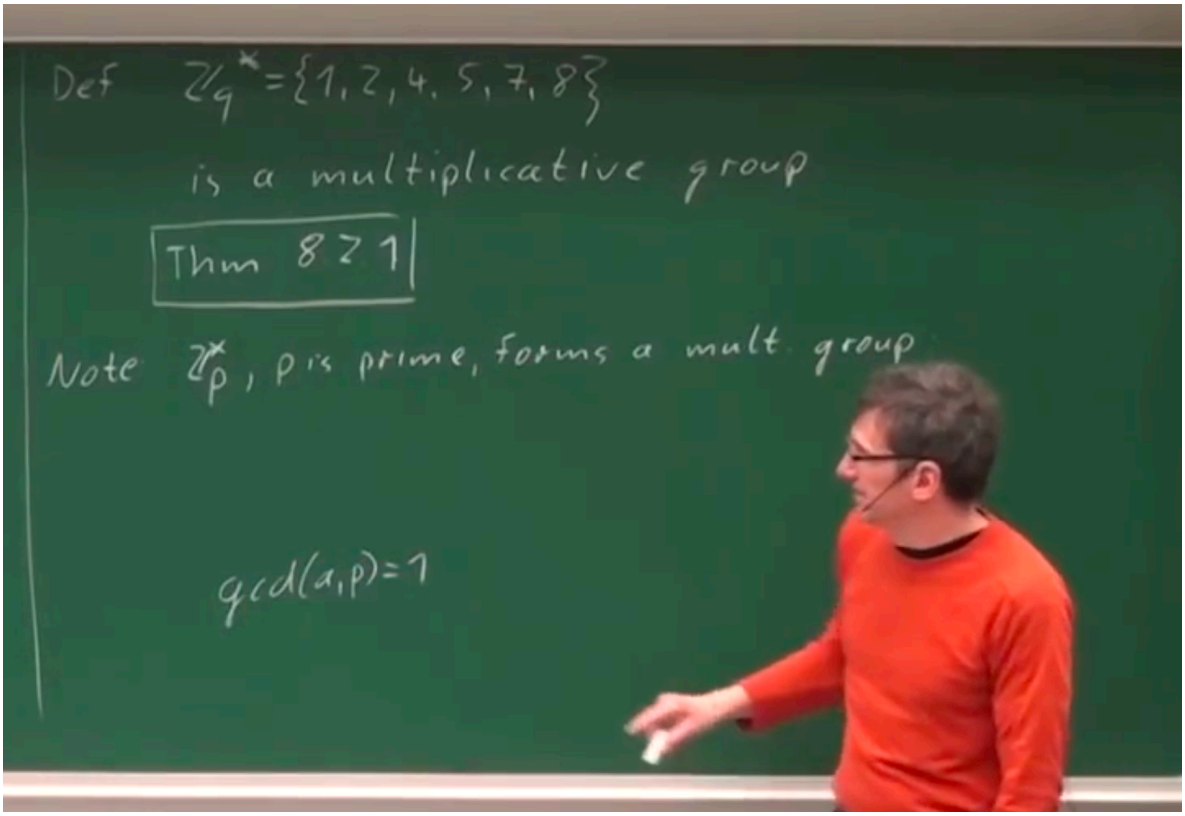
1. Closeness exists as we are doing module 9 arithmetic
2. Associativity exists
3. Neutral Element exists

But Inverse doesn't exists why ? as we know inverse only exists if
GCD(element,9) = 1
let's find the trouble makes in this set.
{
0 -> GCD (0,9) = 9 so doesn't have inverse
1 -> GCD is 1
2 -> GCD is 1
3 -> GCD is 3
4 -> GCD is 1
5 -> GCD is 1
6 -> GCD is 3
7 -> GCD is 1
8 -> GCD is 1
}
Bold characters, 0,3,6 are trouble makers.

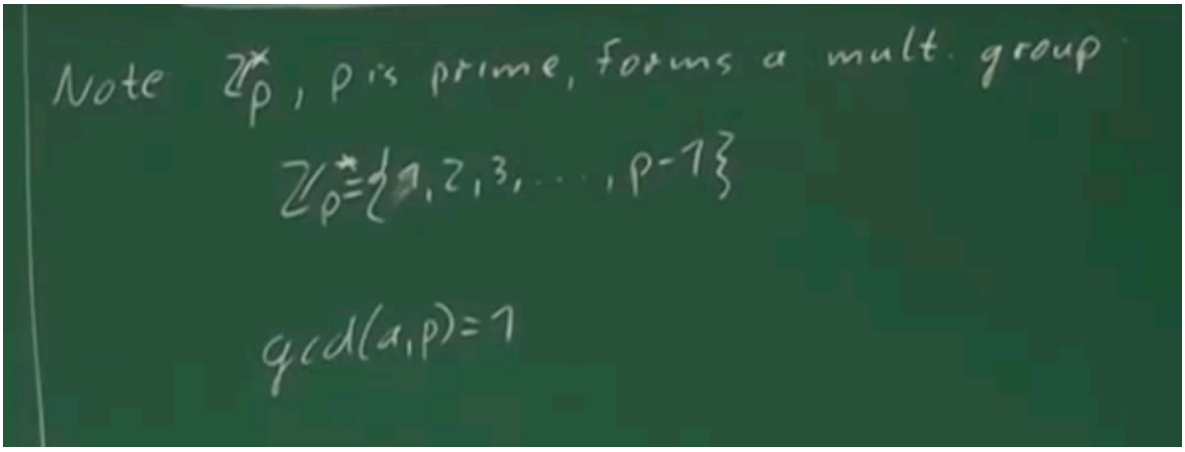


we will do something sneaky ie we define a new set and kick the trouble makers so
Z9* = {1,2,4,5,7,8}
This Z9* is a multiplicative group which is theorm 8.2.1
if we look at Z9* group, we know all the numbers have multiplicative inverses which is step 4 but we might get this feeling that closeness property ie 1st property a.b = c and c exists in same group might gets violated.

but by abelian theorem we know that after removing trouble makers, it still forms the group.

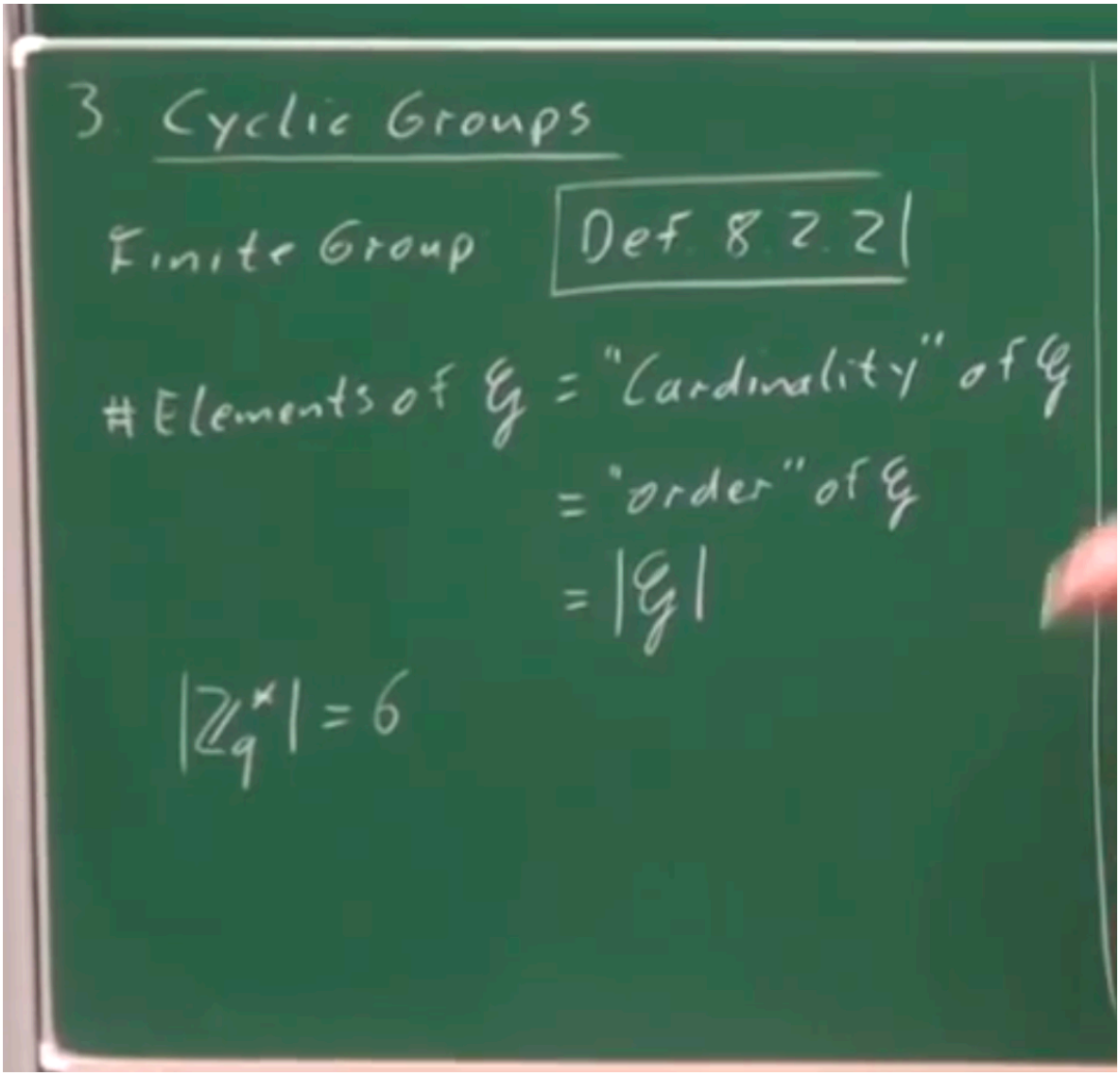


now say in Zp, p is prime then gcd of p with every other element in group is 1 except for …. “0” in Zp* is the group without 0 in the group.



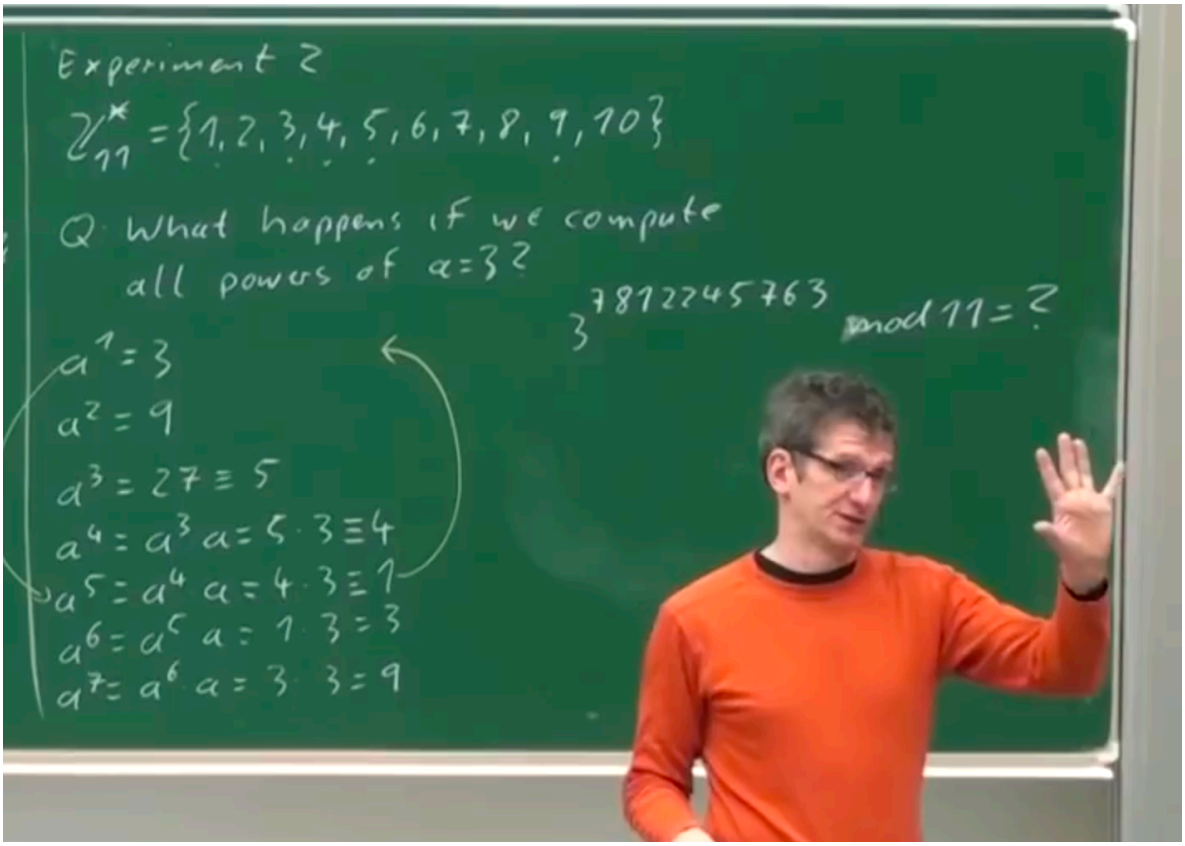
3. **Cyclic Group**

Finite Group, is the group with finite elements and Number of elements in the group G is called as the cardinality of group G or order of group G
and in mathematics it is denoted as |G|



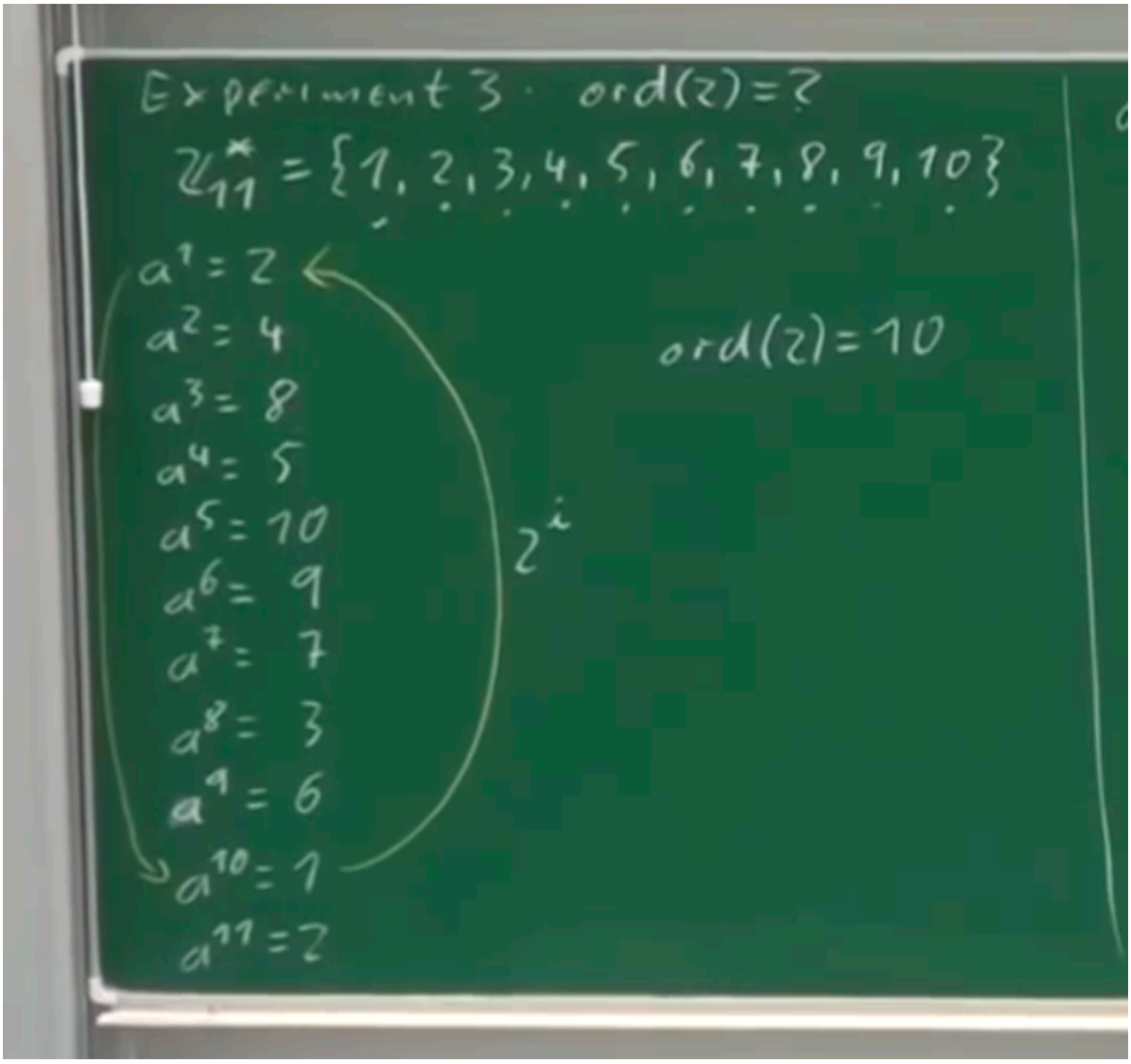
Experiment:
Z11* = {1,2,3,4,5,6,7,8,9,10}
Question: What happens if we compute all powers of a=3 modulo 11?
Answer:
a^1 = 3
a^2 = 9
a^3 = 27 mod 11 = 5
a^4 = (a^3 mod 11 * a) mod 11= 15 mod 11 = 4
a^5 = (a^4).a = 4*3 = 12 mod 11 = 1
a^6 = a^5*a = 1*3 = 3
a^7 = a^6*a = 9
and we see that all the values are starting to repeat and why is 1 exciting is because it starts the circle and hence this chapter is cyclic groups.

little bit of motivation why we are doing exponentiation is **“Diffie Hellman”** where we are doing exponentiations at every step.



so Order of 3 is 5 ie cycle length is 5.

Experiment 3:



so Order of 2 is 10 ie it generated the entire group.

Definition 8.2.3 Order of an element

The order *ord(a) of an element a of a group (G, ∘) is the smallest positive integer k such that*

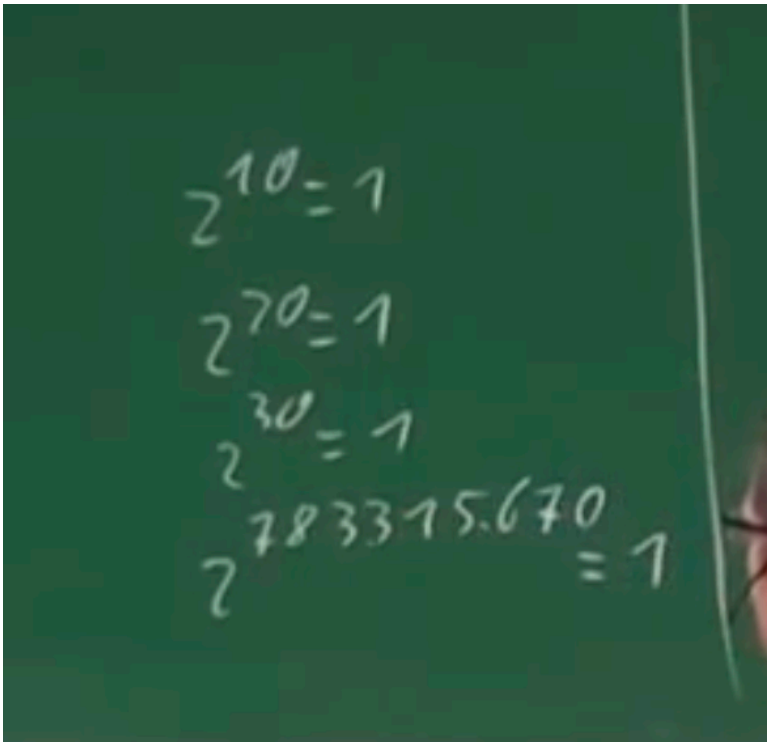
$$a^k = \underbrace{a \circ a \circ \ldots \circ a}_{k \text{ times}} = 1,$$

where 1 is the identity element of G.

Question is why smallest positive integer k ? reason is there will be other

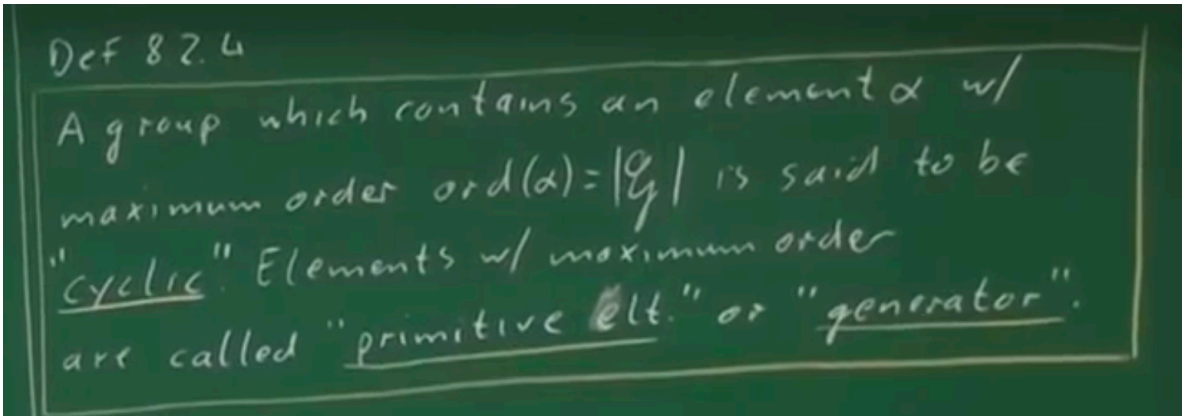
exponents where a ^ p = 1

eg. in experiment 3 , a^10 is 1 same way a^20 is also 1 and so on....



Def 8.2.4: A group G which has an element alpha such that order of alpha is maximum ie order(alpha) = |G| is called **cyclic group** and elements with maximum order are called **primitive elements or Generators**.

eg above Z11 is a cyclic group because there is such element ie 2.

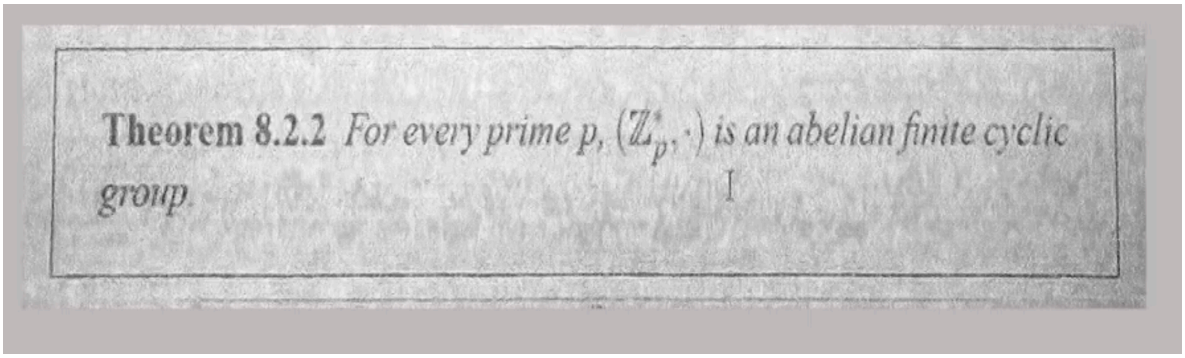


Definition 8.2.4 Cyclic Group
A group G which contains an element α *with maximum order* $ord(\alpha) = |G|$ *is said to be* cyclic. *Elements with maximum order are called* primitive elements *or* generators.

so we can say 2 is the generator for Z11*

Cyclic groups are the basis of discrete logarithm cryptosystems.

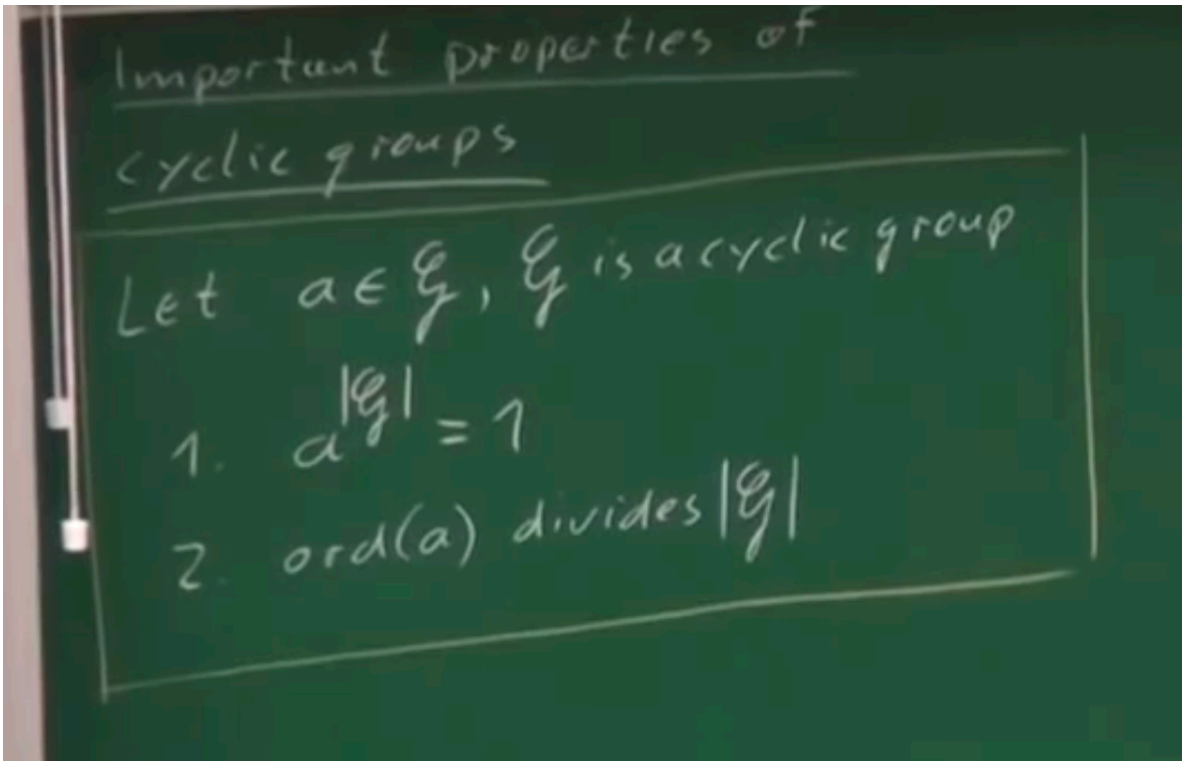
Theorem: for every prime number p, Zp* is a cyclic group.



Theorem 8.2.2 *For every prime p, $(\mathbb{Z}_p^*, \cdot)$ is an abelian finite cyclic group.*

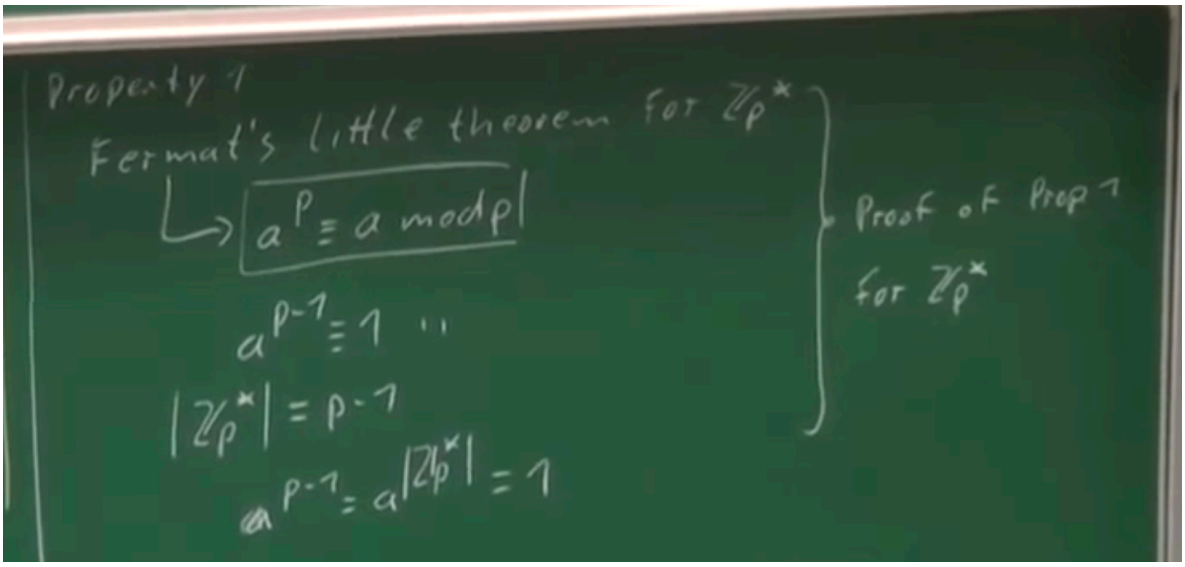
Properties of Cyclic Groups (Cyclic groups are the onces which has an element with maximum order ie |Zp*|):

1. say a is an element of G then a^|G| = 1
    1. as we know G is a cyclic group and as per theorem 8.2.2, for every prime p Zp* is a cyclic group so length of Zp* is p-1 as we know from the above so “a^p-1 = 1 “ we need to prove this.
2. Order(a) divides |G|



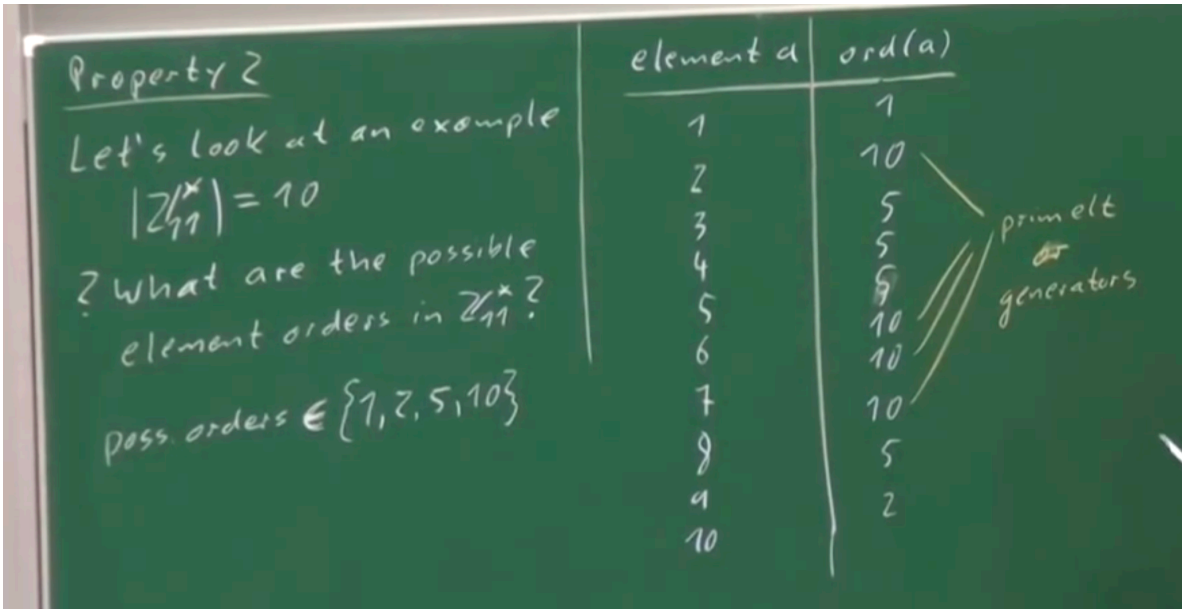
Proof of Property 1.
Fermat little theorem for Zp*:
Actual theorem is a^p = a mod p
dividing with a : a^p-1 = 1 mod p
How many elements in Zp* ? {1,2,3,4,5,6,7,... p-1}

a^p-1 = a^|Zp*| = 1 mod p hence proved property 1 for cyclic groups.



Above property is true for prime/abelian cyclic group.there are many types of other groups but this group is very important for us from crypto stand point.

Property 2:



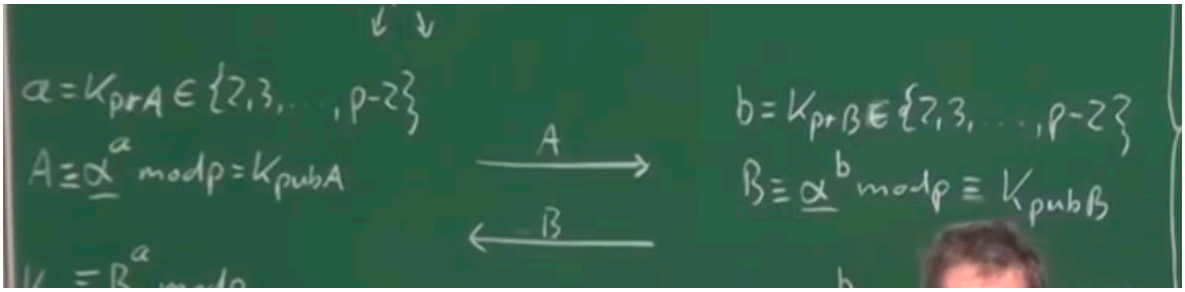
as per property 2, each element's order in cyclic group divides |G| or length of Zp* and same is depicted in the above image.

Little Hint for next lecture:
Cyclic groups can make "nice" Discrete Logarithm problems.
What is Discrete Logarithmic problem:
Take Z47*
a = 5 is the generator for Z47*

5^x will generate all the numbers from 1 to 47.

5^x = 41 mod 47
if you look at diffie hellman you will know it is same as what is diffie Hellman.
in Diffie helman **Alpha** is a generator and A or B are transferred over unsecured channel so both Alpha and A or B are known to oscar so **Alpha^a = A mod p**

if we compare x is same as “a” which is the private key.



we need to find the x ? how can we find that ? we can take logarithm on both sides to solve 5^x = 41 mod 47