Cryptography and Network Security

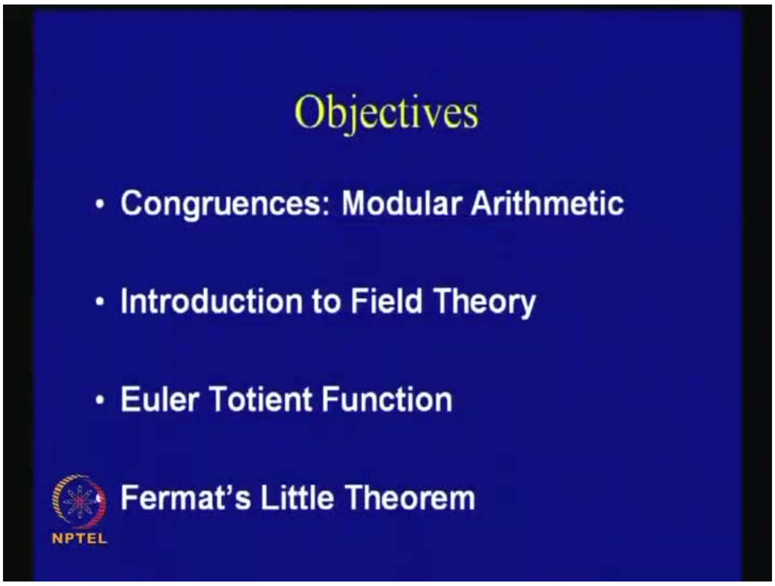
Prof. D. Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Module No. # 01
Lecture No. # 03

Introduction to Number Theory

Ok so welcome to today's talk lecture on number theory so today we shall be discussing about some elementary concepts in number theory which forms the kind of very a center i mean it is very central to the field of the cryptology so we shall i mean it is a really fascinating field and quiet a big vast field but, today we shall essentially understand some of the basic concepts

(Refer Slide Time: 00:51)

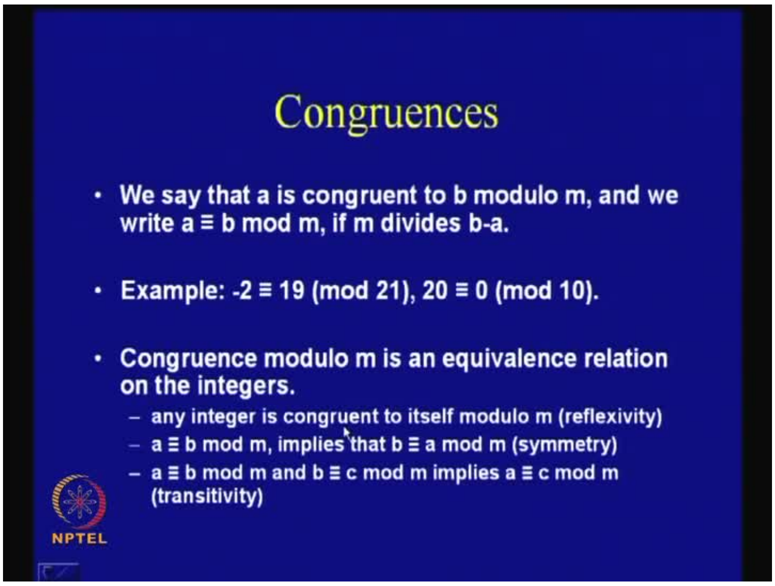


Objectives

- Congruences: Modular Arithmetic
- Introduction to Field Theory
- Euler Totient Function
- Fermat's Little Theorem

So today's objective of this particular talk shall be on congruences modular arithmetic introduction to field theory euler totient function and fermat's little theorem so we shall be talking about these topics so one of them is congruences which is modular arithmetic which is very important to understand field of cryptology and then we shall try to give the define the concepts of what is meant by mathematical field which is very again very central idea to the study and then discuss about a particular function which is called as euler totient function very popular and very useful kind of parameter and then conclude the talk with discussion on fermat’s little theorem so we will be actually discussing about fermat’s euler theorem

(Refer Slide Time: 01:29)



Congruences

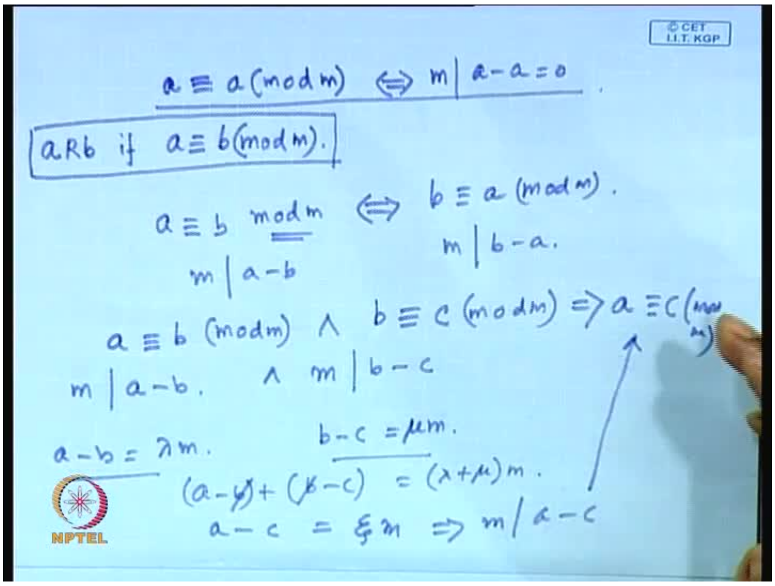
- We say that a is congruent to b modulo m, and we write $a \equiv b \bmod m$, if m divides b-a.
- Example: $-2 \equiv 19 \pmod{21}$, $20 \equiv 0 \pmod{10}$.
- Congruence modulo m is an equivalence relation on the integers.
  - any integer is congruent to itself modulo m (reflexivity)
  - $a \equiv b \bmod m$, implies that $b \equiv a \bmod m$ (symmetry)
  - $a \equiv b \bmod m$ and $b \equiv c \bmod m$ implies $a \equiv c \bmod m$ (transitivity)

So starting so essentially we will find that when we’re doing cryptology or when we’re doing a normal kind of computation i mean in in related to the ciphers then we essentially do not with deal with infinite sequences so we for example, we do not have a set which rather we do not have a set which is which can be which can take infinitely large number of values so which means that there is a finite number of values and we are supposed do our computations on finite values so therefore, there is i mean we have to define our arithmetic in a finite set of values so for that or rather in order to study such kind of operations one basic concept or one very important concept is something which is called as congruences

So we say that a is congruent to b modulo m so a and b are supposed to be integral integer numbers and we say that a is congruent to b modulo m and we denote them as them as follows that is a is congruent to b mod m if m divides a minus b or b minus a so that is the basic idea therefore, let us see some examples like minus two will be is equal to will be congruent to nineteen modulo twenty one the reason being that twenty one divides nineteen minus of minus two that is twenty one and similarly, twenty will be zero mod ten because if you take or rather one way of thinking is that ten will divide twenty minus zero or zero minus twenty

So i mean so therefore, i mean the idea is that if you just think in terms of numbers then this number if we divide by the modulus of operation and then this particular number on the right hand side is nothing but, the remainder therefore, so that is the way of how to kind of compute modular computations so this is nothing but, the simple modulo computation now you may note it that congruence modulo m is actually an equivalence relation why now because it is an equivalence relation on the set of integers so let us try to reason it out

(Refer Slide Time: 04:11)



$$\underline{a \equiv a \pmod{m} \iff m \mid a-a=0}.$$

$$\boxed{aRb \text{ if } a \equiv b \pmod{m}.}$$

$$a \equiv b \ \underline{\underline{\bmod m}} \iff b \equiv a \pmod{m}.$$

$$m \mid a-b \qquad m \mid b-a.$$

$$a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

$$m \mid a-b. \quad \wedge \quad m \mid b-c$$

$$\underline{a-b = \lambda m.} \qquad \underline{b-c = \mu m.}$$

$$(a-\cancel{b})+(\cancel{b}-c) = (\lambda+\mu)m.$$

$$a-c = \xi m \Rightarrow m / a-c$$

© CET
I.I.T. KGP
NPTEL

So we know that for in order for a particular relation to be satisfying their properties of an equivalence relation it has to satisfy three important concepts of reflexivity symmetricity and also transitivity so let us try to first of all argue why it is reflexive so we see that reflexive its reflexive because any integer is congruent to itself modulo m therefore, if you take a number a or other integers take any number then this number is also congruent to itself so why it is because of this if you take a number a and discus that whether and i say that a is kind of a is congruent a mod m right therefore, this is perfectly why now because this means that m divides a minus a which is zero ok

So this is true therefore, a is congruent to a modulo m therefore, the reflexivity relationship holds therefore, if i define my relation by congruency which means that number a is related to b if a is congruent to b modulo m this is the basic definition of the of of the relation that we are considering of the congruence relation then this relation satisfies the property of reflexivity because of this reason

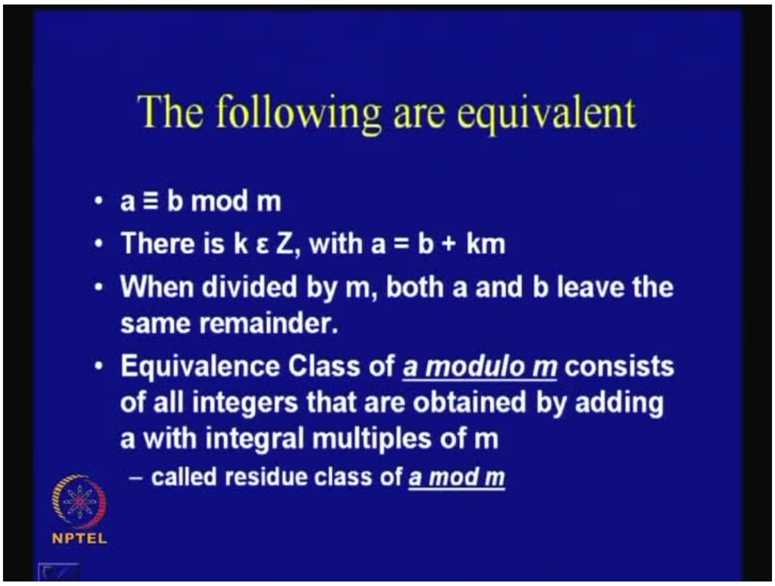
Now what about symmetricity now you see that in terms of symmetricity also it holds because as we say that if a is congruent to b modulo m then it also holds that b is congruent to a modulo m why now because this says that if m divides a minus b then m also divides b minus a therefore, the symmetric the symmetricity relation also holds and this is also true for all all a and b therefore, it is true for all integer values a and b now this is really important it holds for this relation holds the symmetricity properties holds for all values of a and m b hm

What about transitivity so you see that in it is also transitive why because if a is related to b mod m and i tell u that b is congruent to c mod m then this implies that a is congruent to c mod m why now because you see that m divides a minus b and m divides b minus c so from there we can conclude that m also divides a minus c why now because you could have written this a minus b mod simply as some multiple of m similarly, you could have written b minus c as some other multiple of m ok

So now if you have added these two equations right if you have simply added these two equations then you would have got a minus b plus b minus c is nothing but, lambda plus mu which is again another integer times m now form here b and b cancels and we have got a minus c is equal to some other constant we can call that to be some epsilon or something so it is something some integer multiplied with m and therefore, this means that m divides a minus c and therefore, this this also holds true so we see that this relation is also transitive and therefore, since it is and this will hold for any such a b and c right and therefore, since it satisfies the properties of reflexivity symmetricity and also of transitivity we say that this particular relation of congruence also satisfies the i mean it is an equivalence relation ok

So therefore, it basically induces a partition on the set of integers we know that equivalence relation induces a set of parti[tion]- i mean induces a induces a partition on the set on the set right therefore, it holds this property holds true

(Refer Slide Time: 08:03)

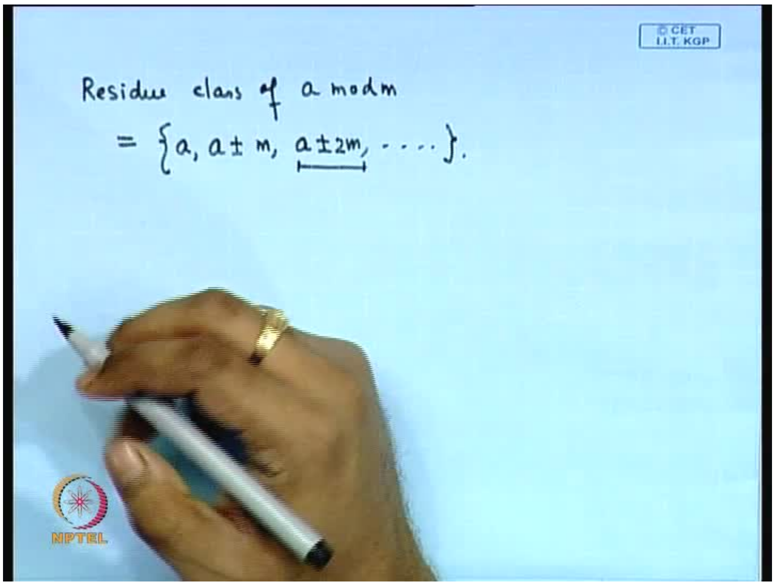


The following are equivalent

- $a \equiv b \bmod m$
- There is $k \in Z$, with $a = b + km$
- When divided by m, both a and b leave the same remainder.
- Equivalence Class of *a modulo m* consists of all integers that are obtained by adding a with integral multiples of m
  - called residue class of *a mod m*

Now the following are actually some equivalence statements and you can easily verify them it says that a is congruent to b mod m is same as saying that there is an integer value of k which satisfies that a is equal to b plus k m so this is what i just just wrote in the previous slide so you see that m divides a minus b because a minus b is k which is an integer multiplied with m it is an integral multiple of m now when divided by m then both a and b leave the same reminder so these is also same as saying as a is congruent to b modulo m now equivalence class of a of a modulo m that is a modulo m consists of all integer that are obtained by adding a with integral multiples of m now this is called or defined as the residue class of a mod m so which means that if i say that the class which is called the residue class of a mod m

(Refer Slide Time: 09:15)

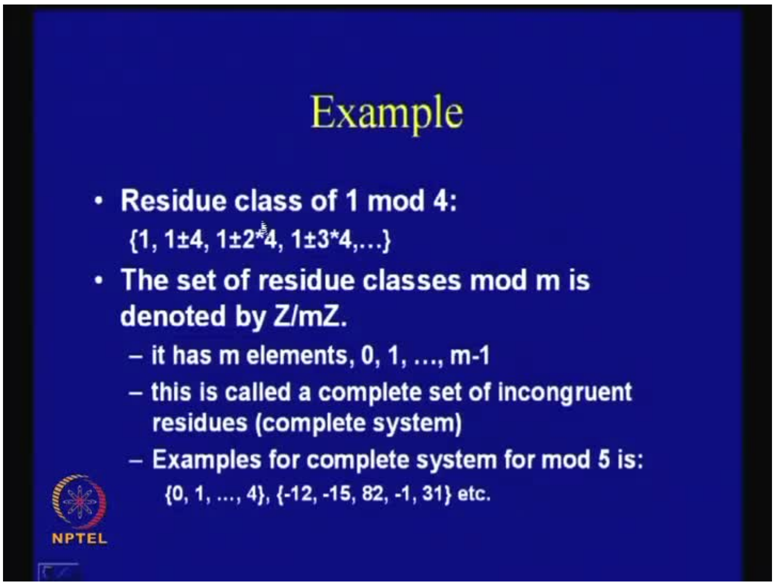


Residue class of a mod m

$$= \{a, a \pm m, \underline{a \pm 2m}, \ldots.\}.$$

Then what we do is that we take a and we add all possible integral multiples of m therefore, therefore, by saying you that there is a residue class of there is a residue class of a mod m thin it means that this consists of all integer so it is basically a set of all integers which are obtained by adding a integer multiples of of m therefore, it could be like a plus minus m a plus minus two m and so on so the basic idea is that if we just take any number from here and you divide it by m then the remainder which you obtained is a therefore, the remainder defines that particular class therefore, this class is a residue class of a mod m and it is also an equivalence class because it satisfies i mean it it satisfies the properties of equivalence class we are just seeing that right

(Refer Slide Time: 10:11)

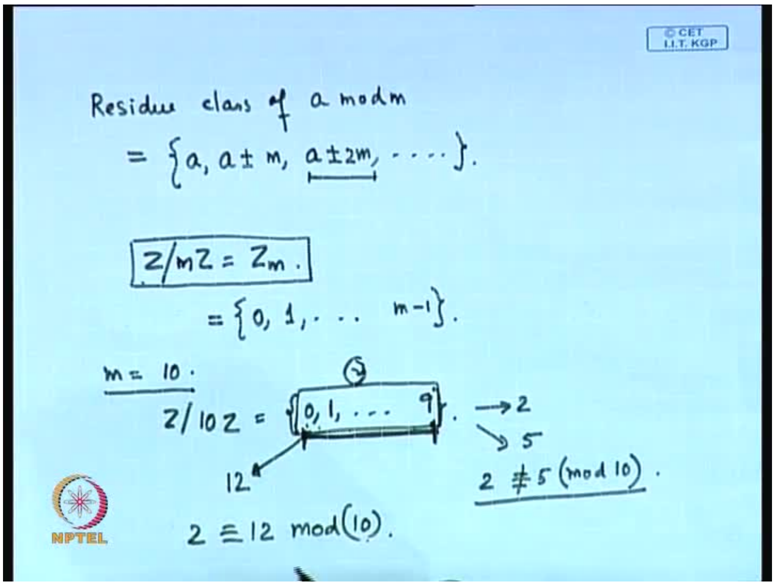


Example

- Residue class of 1 mod 4: {1, 1±4, 1±2*4, 1±3*4,…}
- The set of residue classes mod m is denoted by Z/mZ.
  - it has m elements, 0, 1, …, m-1
  - this is called a complete set of incongruent residues (complete system)
  - Examples for complete system for mod 5 is: {0, 1, …, 4}, {-12, -15, 82, -1, 31} etc.

So therefore, so here is an example for residue class of one modulo four so one modulo four will be one and then one plus minus four therefore, and again one plus minus two multiplied four and then one plus minus three multiple multiplied by four and so on so the set of residue classes mod m is denoted by z m z so z this is also denoted in this in this fashion

(Refer Slide Time: 10:42)



Residue class of a mod m

$= \{a, a \pm m, \underline{a \pm 2m}, \cdots\}.$

$\boxed{Z/mZ = Z_m.}$

$= \{0, 1, \ldots m-1\}.$

$\underline{m = 10.}$

$Z/10Z = \{0, 1, \ldots 9\}.$ $\to 2$ $\searrow 5$

12

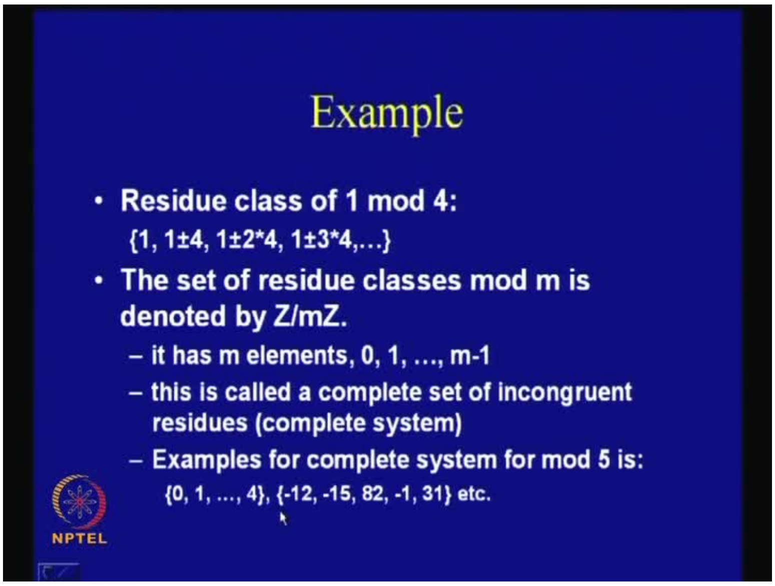
$2 \equiv 12 \text{ mod}(10).$

$\underline{2 \not\equiv 5 \text{ (mod 10)}}.$

So this particular notation is also,metimes known as z m it is also denoted as z i mean the you can also denote it as like this so it is also an equivalent way of may be shorter way of representing this z so this this just defines that this is the set of residue classes mod m and it is denoted by z slash m z and that equal to z m therefore, now now this particular set we will have all the possible all the possible values so it'll essentially have m values so what are the m values possible the m values will run from zero one and till m minus one so this is the set which essentially comprises of this values that is from zero two m minus one now this is also called an a complete system or a complete set of incongruent residues therefore, you see that if you just take a number so an example of this would like let us take the example of ten and then define like what is z by ten z so then this will comprise of numbers from zero one till m till nine that is ten minus one is nine

So that means that if we just take m is equal to ten then these are the possible values of numbers which are which are possible i mean maximally possible and which also have which are also incongruent to each other so that means that if you take any numbers from this from this set for example, let us take like one example one one random choice could be like two and another arbitrary choice could be say five then two and five are never congruent to each other modulo ten so that is why why is two not congruent to five modulo ten because ten will not divide two minus five or five minus two so that means all the elements in this set are actually incongruent to each other and this is the maximal possible possible number of incongruent values that can that can happen ok

(Refer Slide Time: 13:10)

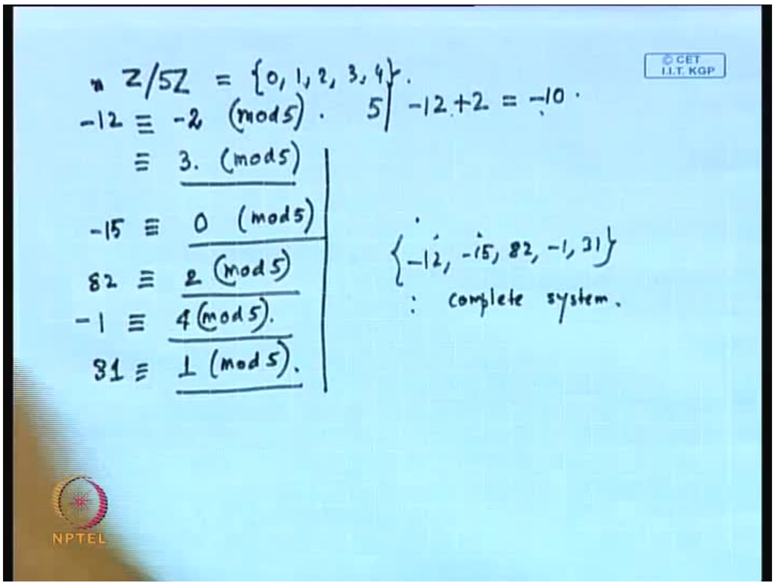


Example

- Residue class of 1 mod 4:
  {1, 1±4, 1±2*4, 1±3*4,...}
- The set of residue classes mod m is denoted by Z/mZ.
  - it has m elements, 0, 1, ..., m-1
  - this is called a complete set of incongruent residues (complete system)
  - Examples for complete system for mod 5 is:
    {0, 1, ..., 4}, {-12, -15, 82, -1, 31} etc.

You can take any number of outside this particular set for example, if you just take an arbitrary choice like say twelve then you'll find one number in this set which is congruent to this number modulo ten which is that number for example, you can choose two so you see that two and twelve are congruent to each other modulo ten why now because ten will divide twelve minus two right therefore, you'll find that this particular set which is like z defined by z slash m z is also called a complete set of incongruent residues for a complete system

(Refer Slide Time: 13:45)



$Z/5Z = \{0, 1, 2, 3, 4\}$.

$-12 \equiv -2 \pmod 5$. $\quad 5 \mid -12+2 = -10$.

$\equiv \underline{3.} \pmod 5$

$-15 \equiv \underline{0 \pmod 5}$

$82 \equiv \underline{2 \pmod 5}$

$-1 \equiv \underline{4 \pmod 5}$.

$31 \equiv \underline{1 \pmod 5}$.

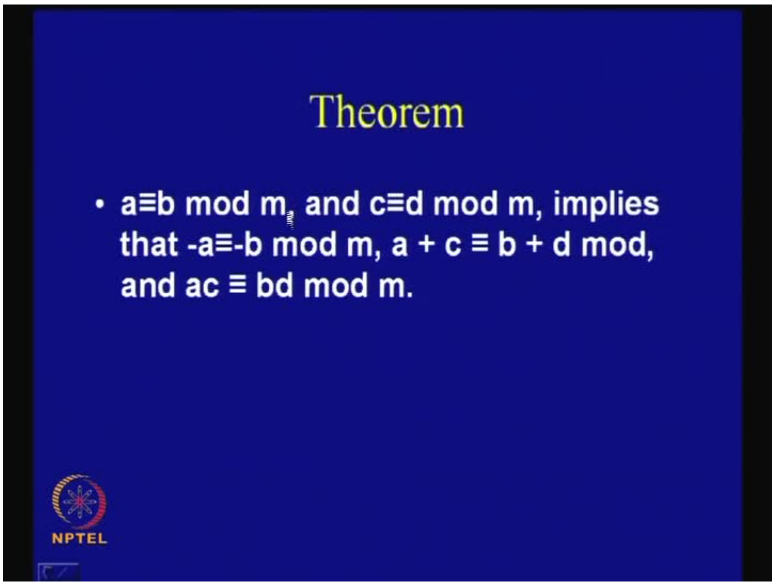
$\{-12, -15, 82, -1, 31\}$

: complete system.

Now there are example this is an example given here for complete system for modulo five so we know now for mod five it will be like from zero to five minus one that is zero one till four and this an another example you can verify like that this is minus twelve minus fifteen eighty two and minus one and thirty two this set is also a complete system why now this is also a complete system because if you just take these numbers like you take minus twelve so we what we are considering is z slash five z right so you see that in this set if we just take twelve then twelve is actually so it is minus twelve right so minus twelve if you take modulo five so what does it mean what is this value so if you divide twelve by five therefore, you will get that this is equal to is it correct yes because if you just take this number five then five you divide minus twelve plus two because that is minus twelve plus two is nothing but, minus ten so five divided minus ten ok

Now what is minus two if you if you would like to bring in this among this numbers like from zero one [till/two] three and four then this particular number minus two will be actually equal to three therefore, because it is you can verify this because five will agian divide minus two minus three so this is same as minus two modulo five will be same as three modulo five what about the next number the next number here in this set was given as minus fifteen so minus fifteen if you take modulo five what will be it it will be zero so similarly, you can do it for the other once also like eighty two will be equal to two modulo five because five will divide it into minus two and minus one will be congruent to four mod five and thirty one will be congruent one mod four one one mod five so you see that the numbers that i obtain after taking the modulo five essentially are nothing but, another order of the numbers zero one two three and four therefore, you see that this is also a kind of these numbers like this set like minus twelve minus fifteen eighty two minus one and thirty one is also another example of a complete systems and any two numbers from this set are are incongruent to each other they are not congruent we can check this

(Refer Slide Time: 16:17)



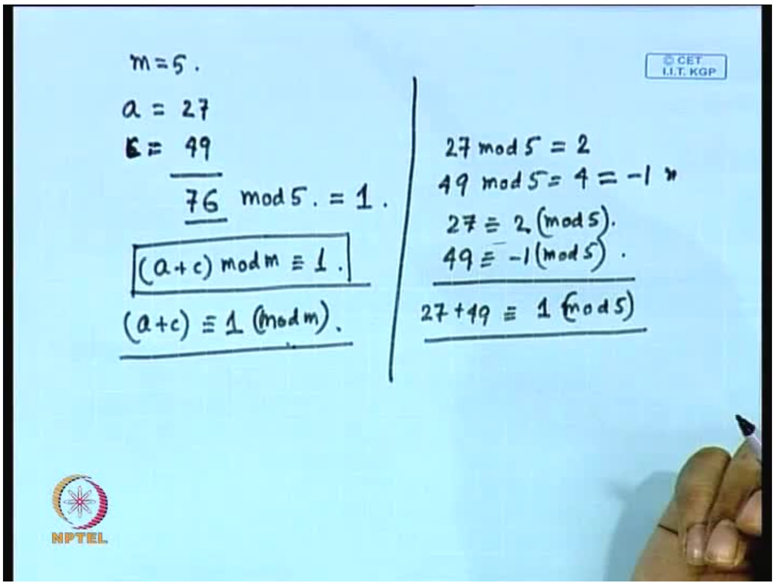
Theorem

- a≡b mod m, and c≡d mod m, implies that -a≡-b mod m, a + c ≡ b + d mod, and ac ≡ bd mod m.

So there is a theorem i mean i am i- i really do not have i- i am not going the proof but, its very simple you can verify it like if a is congruent to b modulo m and c is congruent to d modulo m then this implies that minus a and minus b are congruent to each other modulo m we can also add like a plus c is congruent b plus d modulo m there should be a modulo m here and a c is congruent to b d modulo m so you can verify this and its very simple like what you can do is that you can start like writing as a is equal to b plus some constant multiple of b of m and c is equal to d plus some constant times m and then try to find out minus a and (( )) and this is very simple so this is this is quite trivial to prove

Now what is the implication of this result now the[re]- there is a very is strong implication of this result so let me reflect on this see for example, what we understand here is that this number a may be quite a large value and this number c maybe also another quite large value and suppose you’re actually interested in computing doing computation on large values now if you would like to do computation of large values but, you always have this modulo m then the idea is that what it says is that instead of taking a plus c or rather adding a plus c and then doing a modulo m is same as doing a modulo m on a doing a modulo m on c and reducing this numbers between zero to m minus one and then adding these two numbers so let me kind of illustrate this with a very simple example

(Refer Slide Time: 17:57)



$m = 5.$

$a = 27$

$c = 49$

$76 \bmod 5. = 1.$

$\boxed{(a+c) \bmod m \equiv 1.}$

$(a+c) \equiv 1 \pmod{m}.$

$27 \bmod 5 = 2$

$49 \bmod 5 = 4 = -1$ *

$27 \equiv 2 \pmod{5}.$

$49 \equiv -1 \pmod{5}.$

$27 + 49 \equiv 1 \pmod{5}$

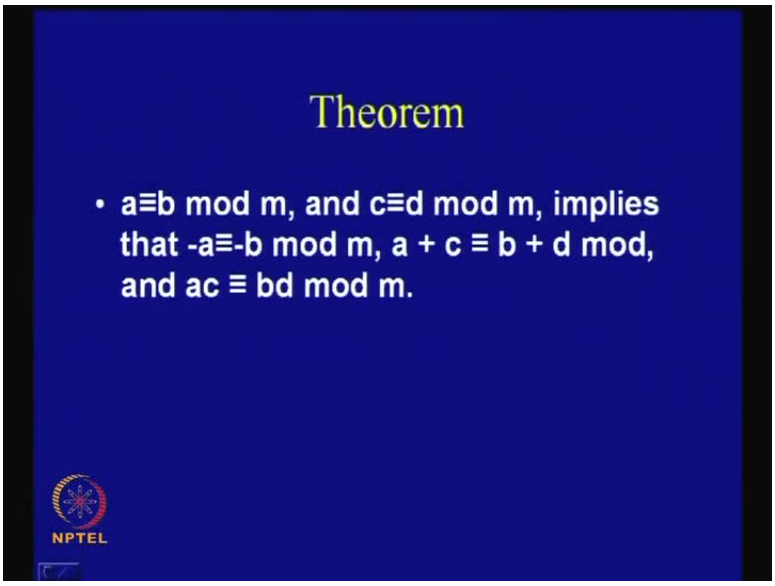
© CET
I.I.T. KGP
NPTEL

So let us take a large value of a so for example, you consider that a is again let us consider that our m value is five and let us see that a is supposed a large value like may be larger than this so it may be like twenty seven and let us consider another value which is say b or rather c and consider that this is say something like forty nine now let us try to add these two numbers so we know that if we add these two numbers then we get seventy six and therefore, if i do a modulo five here that means that i divide this by five and my remainder is one ok

So therefore, i write that a plus c modulo m is nothing but, equal to one it is congruent to one so another way of writing this is rather the way we are writing this a plus c is equal to one mod m now let us try to do i mean apply the previous result so what we will do is that we will take twenty seven and perform a modulo five operation so if i do that then i see that twenty five is divisible by five so the remainder is two similarly, i take forty nine and do a modulo five operation so we see that forty five is divisible so this is actually is equal to four now you see that four also can be written as minus one right so therefore, we write the twenty seven is equal to two mod five and forty nine is minus one mod five now if i add these two numbers like twenty seven plus forty nine then i can obta[in]- add this instead of these two numbers and reducing what i can do is that i can actually add these two small numbers and i get one modulo five which matches with this result

So which means that i need not do the additions with large number when i am doing a modular operation right when then i really do not need to add these large numbers but, what i can do it is that i can reduce this numbers modulo five reduce this number modulo five and then add these two numbers so this particular particular technique can actually make our computations quite simple and this is actually applied in the implementation of cryptosystems quite regularly to make your implementations easier ok

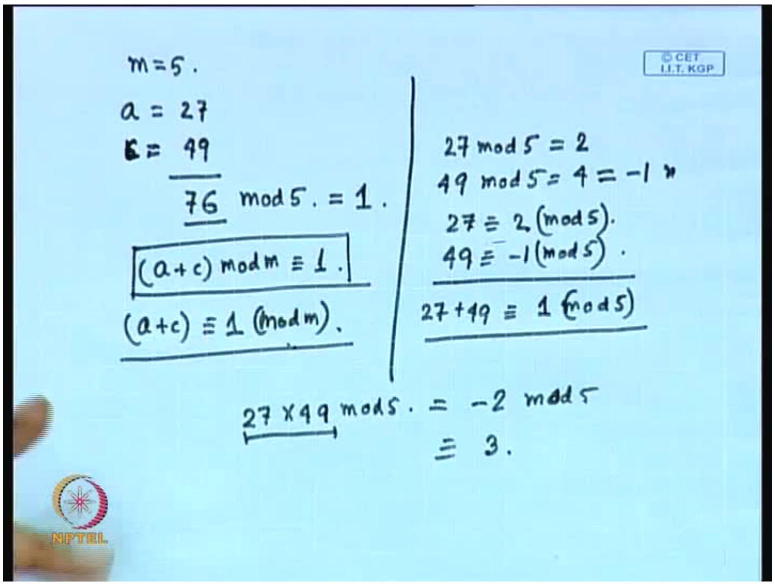
(Refer Slide Time: 20:26)



Theorem

- $a \equiv b \bmod m$, and $c \equiv d \bmod m$, implies that $-a \equiv -b \bmod m$, $a + c \equiv b + d \bmod$, and $ac \equiv bd \bmod m$.

(Refer Slide Time: 20:46)



$m = 5.$

$a = 27$

$c = 49$

$\underline{76}$ mod 5. $= 1.$

$\boxed{(a+c) \bmod m \equiv 1.}$

$(a+c) \equiv 1 \pmod{m}.$

$27 \bmod 5 = 2$

$49 \bmod 5 = 4 = -1$

$27 \equiv 2 \pmod{5}.$

$49 \equiv -1 \pmod{5}.$

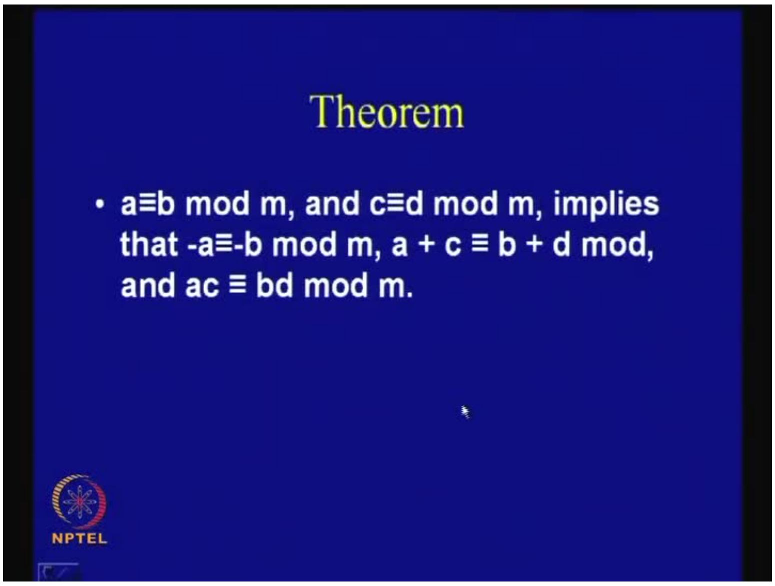
$27+49 \equiv 1 \pmod{5}$

$27 \times 49 \bmod 5. = -2 \bmod 5$

$\equiv 3.$

So we will squarely get this idea or rather find more examples of this as we proceed but, this is a very interesting and very important results which we should understand similarly, when we’re talking about multiplication we can also again instead of multiplying two large numbers which is even more complicated we can actually reduce these numbers mod m and then just multiply this small numbers for example, imagine like if you have to multiply twenty seven and forty nine and then do a modulo five operation right then this this multiplication is not i mean it is not proceeding well you have to do it and you can make mistake right and most importantly when your computer does it it may not make mistakes but, what it may do is it may require large number of time right so the resource may be useful may be used up so instead of that what you can do is that you can reduce it it becomes two and this becomes minus one and you know that this result is very simple this resulting is nothing but, minus two mod five which is nothing but, three ok

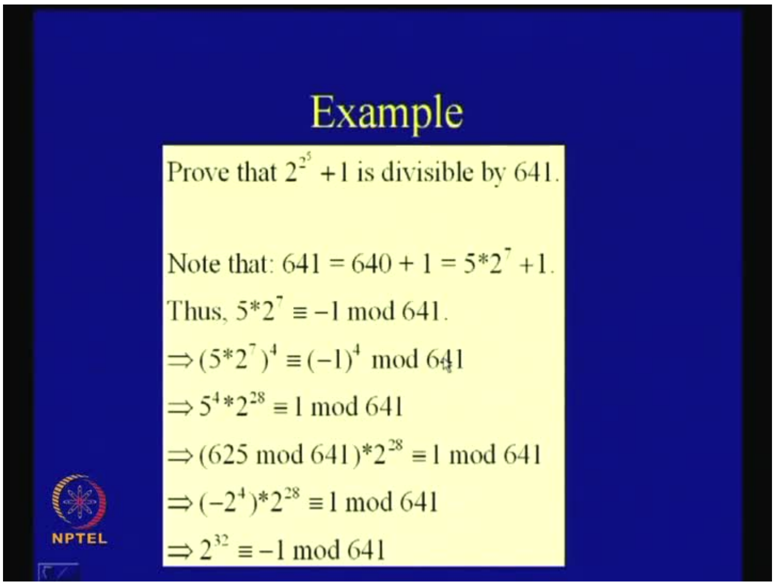
(Refer Slide Time: 21:31)



Theorem

- $a \equiv b \bmod m$, and $c \equiv d \bmod m$, implies that $-a \equiv -b \bmod m$, $a + c \equiv b + d$ mod, and $ac \equiv bd \bmod m$.

(Refer Slide Time: 21:33)



Example

Prove that $2^{2^5} + 1$ is divisible by 641.

Note that: $641 = 640 + 1 = 5*2^7 + 1$.

Thus, $5*2^7 \equiv -1 \bmod 641$.

$\Rightarrow (5*2^7)^4 \equiv (-1)^4 \bmod 641$

$\Rightarrow 5^4*2^{28} \equiv 1 \bmod 641$

$\Rightarrow (625 \bmod 641)*2^{28} \equiv 1 \bmod 641$

$\Rightarrow (-2^4)*2^{28} \equiv 1 \bmod 641$

$\Rightarrow 2^{32} \equiv -1 \bmod 641$

So you can just straight away from these two results we can obtain this product that actually makes your computations much easier otherwise you would have it would have become a little more difficult right so this result has got lot of impact therefore, and here is a another example so you can probably try to understand the impact of the previous result from this example so let let us consider so this is the very important number in number theory but, let us not go into that say is the two to the power two to the power of five plus one is divisible by six forty one and a proof is required for that so one way of doing it like it will be two to the power of five is thirty two therefore, let us compute two to the power of thirty two and then add one and then divide by six forty one and then see that whether it is divisible or not

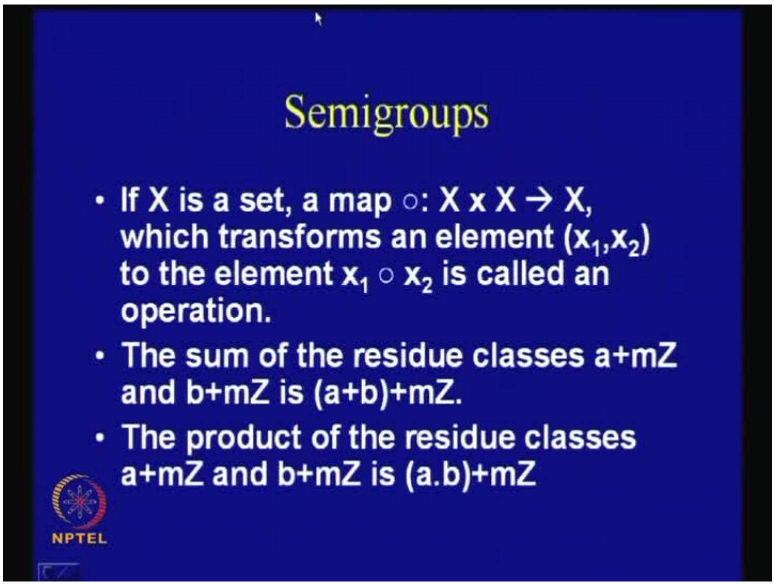
But this is quite tedious approach instead of that lets see this we know that six forty one can be actually written as six forty plus one and six forty can be factorized as five multiplied by two to the power of seven plus one now this factorial (( )) is quite easy right because its divisible by five and the others are just powers of two therefore, we can write as five multiplied by two to the power of seven is nothing but, minus one modulo six forty one why now because we know that five two to the power of two to the power of seven will be equal to six forty one minus one right so we can rearrange this as five into two to the power of seven is equal to six forty one minus one

Now if take modulo six forty one then this vanishes and therefore, minus one remains as a remainder now from the previous result we know that if i raise this to the left hand side to the power of four it is same as write i mean raising the right hand side to the power of minus one hole to the power of four when you're doing modulo six forty one operation because this means that we are multiplying this four times and therefor the right hand side also needs to be multiplied four times therefore, straight away from here we get five to the power of four multiplied by two power of twenty eight is nothing but, congruent to one modulo six forty one

So now we see that five to the power of four is nothing but, six twenty one six twenty five and we know we know that need not actually require to multiply these two numbers but, we can actually deduce this number modulo six forty one so that should be make our computations easy right and then multiplied by two power of twenty eight and that is congruent one modulo six forty one so this equation is not disturbed by this now we see that six twenty five modulo six forty one is nothing but, equal to minus sixteen therefore, this result is nothing but, minus two (( )) power of four multiplied by two power of twenty eight is congruent to one modulo six forty one and that means that two power of thirty two is nothing but, equal to minus one modulo six forty one so that means that six forty one divides from the definition of congruence we know that six forty one divides two power of thirty two minus of minus one that is six forty one divides two power of thirty two plus one so this particular thing is proved

But you see that throughout this we are actually not done a single bit large computation and that is the advantage of previous theorem therefore, idea that when you need do multiplications or additions or computations on large numbers and when you're doing a modular operation then it is better to reduce each individual numbers and perform the operations that'll you're your computations easier

(Refer Slide Time: 24:40)



Semigroups

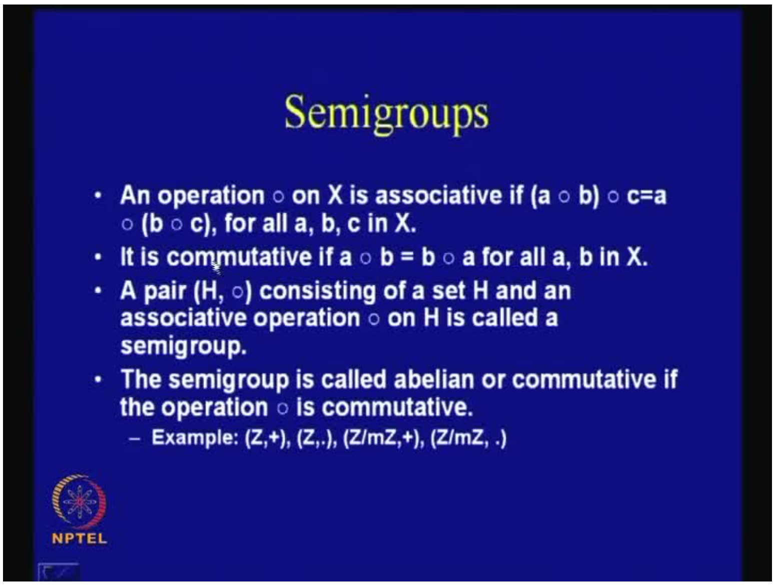
- If X is a set, a map ○: X x X → X, which transforms an element (x_1,x_2) to the element $x_1 \circ x_2$ is called an operation.
- The sum of the residue classes a+mZ and b+mZ is (a+b)+mZ.
- The product of the residue classes a+mZ and b+mZ is (a.b)+mZ

So now we actually i mean so this is we actually shift our focus and go into a little bit of field theory now we fields are actually very central to the understanding of crypto that is for example, the common that is the recent standard which is known as the advanced encryption standard relies heavily on finite fields therefore, we will try to understand some of the basic of fields that is what are what are the fields and what are the properties of a mathematical field ok

So let us start with something which is called semi groups so first of all let us define something which is called a transformation or an operation so here is an x is a set and let us define a map which is defined by this circle has nothing but, a transformation which takes two numbers from this set x let let it be x one and the other one is x two and perform an operation therefore, this example of this could be an addition that is just a simple plus in the integer domain or multiplication so, the so you can generalize it means that i just take two numbers from the set x and i perform these computations and therefore, this element therefore, this transforms an element x one coma x two to the element x one operation x two and this is [vocalize-noise] so this is just this is a simple transformation ok.

So now the sum of the free residue classes that is so here is an example like examples of this transformation as i told you that integer is one example similarly, you can also define in the residue classes like that we just take two residue classes a plus m z and b plus m z so this was so we know that a plus m z and b plus m z and if i just need to find out the some of these residue classes then this is nothing but, a plus b plus m z similarly, the product of the residue classes a plus m z and b plus m z is equal to a multiplied b plus m z so this is the same thing which i just told you before this that is if i need to kind of multiply or add two large numbers in the modulo m domain then i just find the remainders right and just add the remainder or multiply the remainders this is perfectly defined ok

(Refer Slide Time: 26:56)



Semigroups

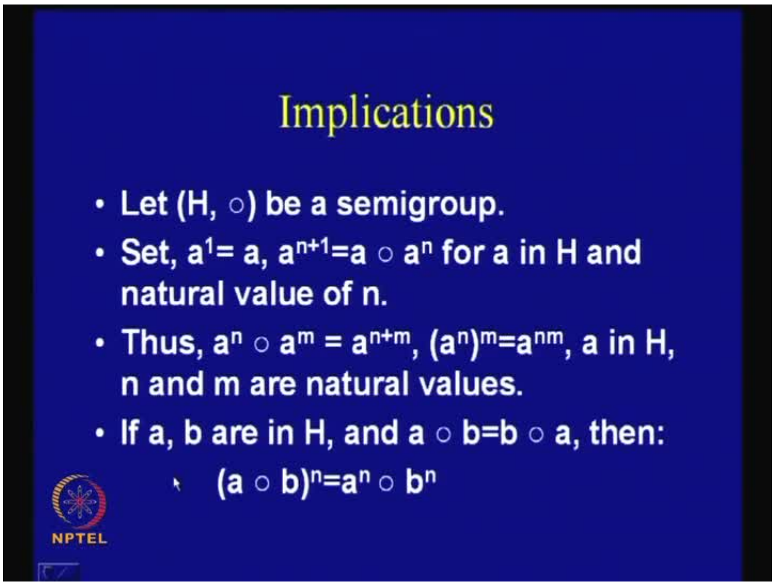
- An operation $\circ$ on X is associative if (a $\circ$ b) $\circ$ c=a $\circ$ (b $\circ$ c), for all a, b, c in X.
- It is commutative if a $\circ$ b = b $\circ$ a for all a, b in X.
- A pair (H, $\circ$) consisting of a set H and an associative operation $\circ$ on H is called a semigroup.
- The semigroup is called abelian or commutative if the operation $\circ$ is commutative.
  - Example: (Z,+), (Z,.), (Z/mZ,+), (Z/mZ, .)

So now an operation this circle on x is associative so we now we would like to define the associativity of this it means that a operation b operation c and if i do this it can also be associated as a this operation can also be performed as this that is a operation b operation c being given a priority and this holds for all a b c in x so this is how associativity is defined ok

And we know what is commutativity which means that if a operation b is same as b operation a for all a and b in x then it is said to be commutative (( )) so examples we know that integer addition is an associative operation right and it is is it commutative also it is also commutative but, what about an example which is not commutative for example, matrix multiplication is not commutative we know that if i take two matrix a and another matrix as b and if i multiply a and b then it may not be the same as that b and a ok

So now we define what is meant by a semi group so it says that there is a pair of h so it is a set so we define a transformation as just as we told right now so it consists of a set h and an associative operation so that means if the operation is also associative on h and then it is called a semi group so of semi-groups means simply that there is a set h with an operation circle and this operation is also associative so if the operation is also associative then if the operation is associative then we say it to be a semi-group now the semi-group is also called abelian or commutative if the operation is also commutative and examples of this could be like integer set the addition defined over it integer set multiplication defined over it residue class set and addition defined over this and the residue class set and multiplication defined over this ok

(Refer Slide Time: 29:04)



Implications

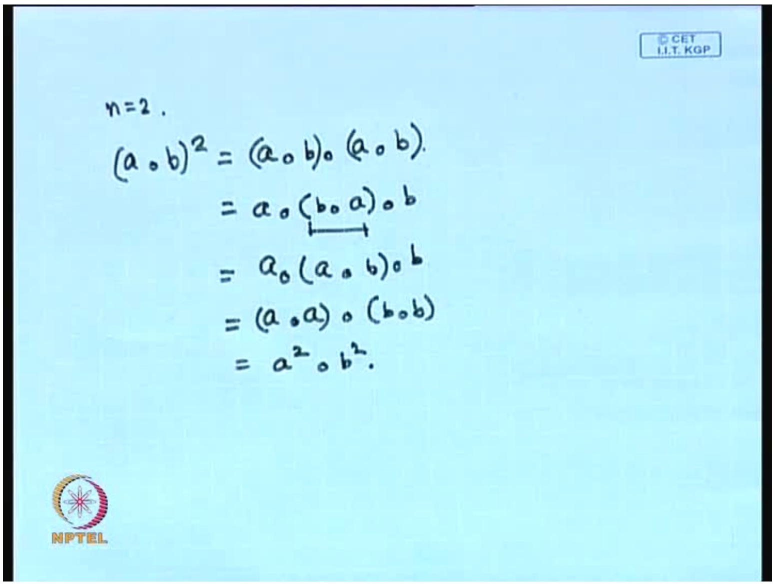
- Let $(H, \circ)$ be a semigroup.
- Set, $a^1 = a$, $a^{n+1} = a \circ a^n$ for a in H and natural value of n.
- Thus, $a^n \circ a^m = a^{n+m}$, $(a^n)^m = a^{nm}$, a in H, n and m are natural values.
- If a, b are in H, and $a \circ b = b \circ a$, then:
  $(a \circ b)^n = a^n \circ b^n$

So we know that these are examples of abelian or commutative semi-groups because this is also associative because it is a semi-group and also further its abelian or commutative so which means you can do it either as a operation b or as b operation a for all a and b which belongs in the set so, implications are as follows so there are some interesting implications

So let h and this operation be defined as a semi-group and let us define like a let us define some powers of a as follows so a power one is nothing but, a and a power n plus one is defined as a operated with a power n so this is the recursive definition of a power n plus one for a which is in h and natural value of n so this is a natural number n now if i need to compute a power n and operate it with a power m then it is same as doing as a power n plus m or if i do as a power n and take a whole power m then this is same as doing a power n m and where a is in h and n and m are nothing but, natural values or natural numbers

Now you see that it is a further interest result which says that a and b are in h and we perform and if a and if the operation is commutative that is if a operation b is same as b operation a then a power the a operation b and if i raise it to power of n is same as a raise to power of n operated with b raise to power of n so we can actually reflect upon these are kind of definitions and we can actually i mean we can actually reflect upon this definition by by for example, choosing the value of n to be two ok

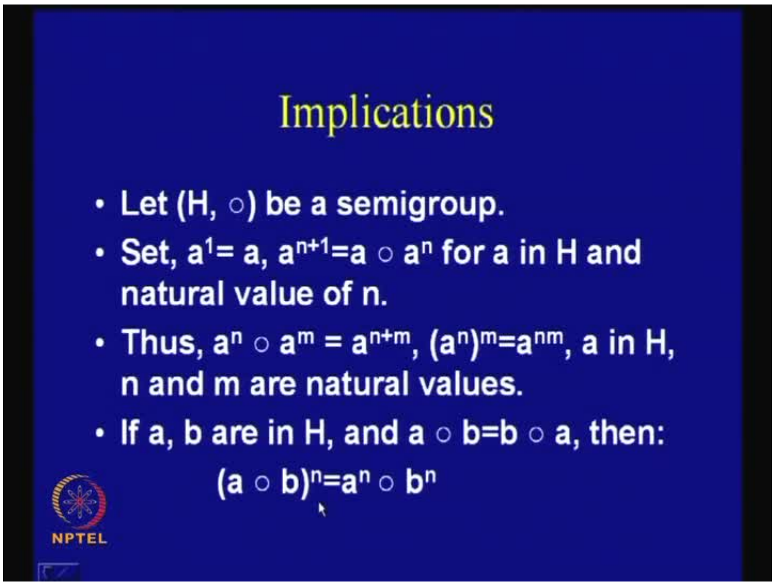
(Refer Slide Time: 30:28)



$n=2.$

$$\begin{aligned}(a \circ b)^2 &= (a \circ b) \circ (a \circ b). \\ &= a \circ \underbrace{(b \circ a)}_{} \circ b \\ &= a \circ (a \circ b) \circ b \\ &= (a \circ a) \circ (b \circ b) \\ &= a^2 \circ b^2.\end{aligned}$$

(Refer Slide Time: 31:25)



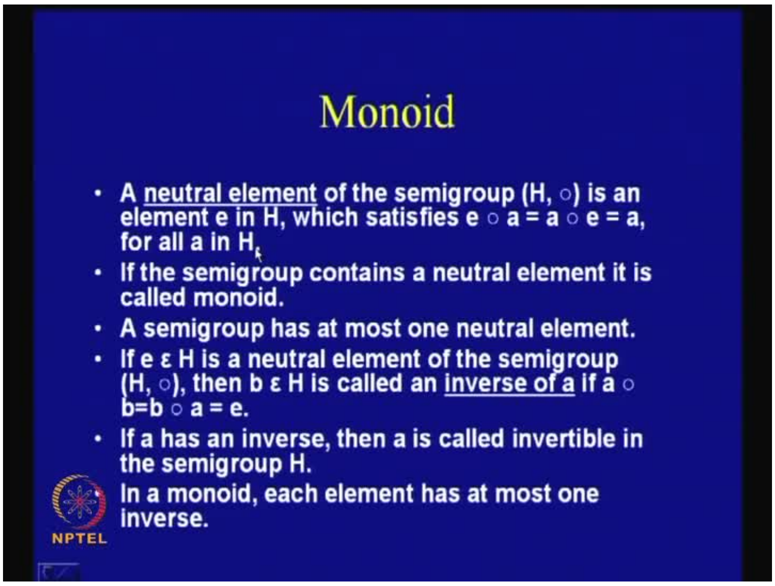
Implications

- Let (H, $\circ$) be a semigroup.
- Set, $a^1 = a$, $a^{n+1} = a \circ a^n$ for a in H and natural value of n.
- Thus, $a^n \circ a^m = a^{n+m}$, $(a^n)^m = a^{nm}$, a in H, n and m are natural values.
- If a, b are in H, and $a \circ b = b \circ a$, then:

$$(a \circ b)^n = a^n \circ b^n$$

So let us take n is equal two and consider the operation as a transformation b raise the power of two so we now that we can actually write this as a power of b by our recursive definition as a power b now we apply we know that this is this operation is so the first thing that we start with is this so that is the first definition but, since this is a semi-group so we know that it is associative so we can actually do like a b operation a operated with b and we know that because if i apply commutativeity then we actually write this as a with b and we know that again we can actually do this that is a apply associativity and perform this operation like this and this is nothing but, a square operated with b square therefore, this we can actually inductively apply and obtain the results that is a operated operation b if i raise it to the power of n is same as a raise to the power of n operation operated with b power n

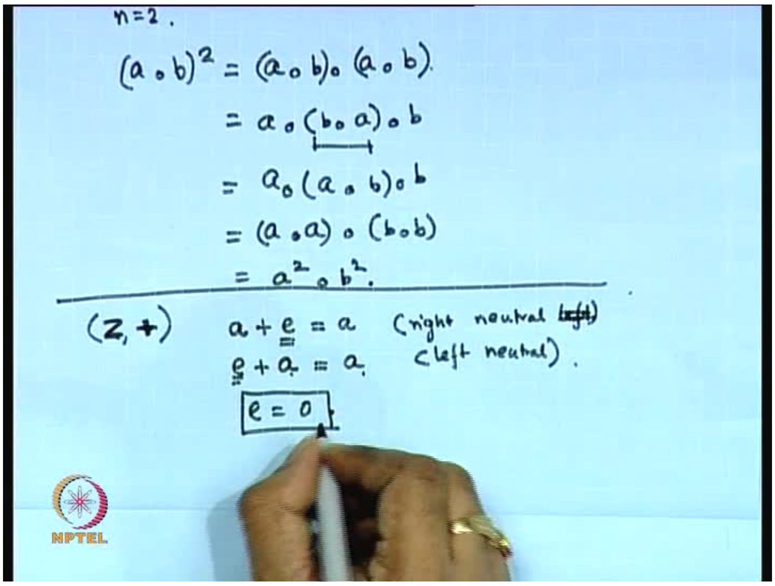
(Refer Slide Time: 31:32)



Monoid

- A neutral element of the semigroup (H, ○) is an element e in H, which satisfies e ○ a = a ○ e = a, for all a in H.
- If the semigroup contains a neutral element it is called monoid.
- A semigroup has at most one neutral element.
- If e ε H is a neutral element of the semigroup (H, ○), then b ε H is called an inverse of a if a ○ b=b ○ a = e.
- If a has an inverse, then a is called invertible in the semigroup H.
- In a monoid, each element has at most one inverse.

(Refer Slide Time: 32:10)



n=2.

$$(a \circ b)^2 = (a \circ b) \circ (a \circ b)$$
$$= a \circ \underbrace{(b \circ a)} \circ b$$
$$= a \circ (a \circ b) \circ b$$
$$= (a \circ a) \circ (b \circ b)$$
$$= a^2 \circ b^2.$$

(Z, +) $\quad a + \underline{\underline{e}} = a$ (right neutral ~~left~~)

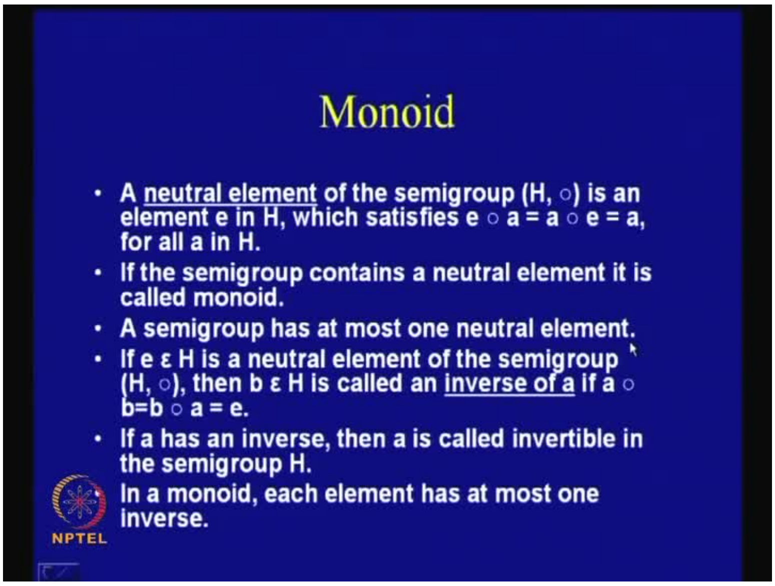
$\underline{\underline{e}} + a = a$ (left neutral).

$\boxed{e = 0}$

So now we let us the define some something which is called monoids so first of all one of the definition the central definition of the monoids is something which is called a neutral element a neutral element of the semi-group h operation is an element e in h which satisfies e operation a as same as a operation e and that that means that this is equal to a for all a in h therefore, we see that an easy way of understanding the neutral element would be to consider an example so let us consider the example of let us consider the example of for example, a field of z and so this is an integer set this is an integer set and there is a plus operation defined so we so we have just defined that this is a this is an example of if so this was an example of semi-group so we have defined what is meant by a semi-group

And let us consider this particular example and see that how or rather what is the neutral element in this set so i think all of us know what is the neutral element in this set so if i so the by the definition it means that if i take a and if i apply the opera[tion]- operation plus and there should be a neutral element a so that i get back a or so this is called a right neutral element and similarly, there is something which is called a left neutral element which says that if i add e with a and if i obtain a so this is the left neutral element so this is the right right neutral element this is the left neutral element that i get back here now you see that this defines that so this actually gives us an idea that this e is nothing but, zero right so for example, if i add a with zero then i get back a and if i add zero with a i also get back a so zero is the neutral element in the semi-group z plus

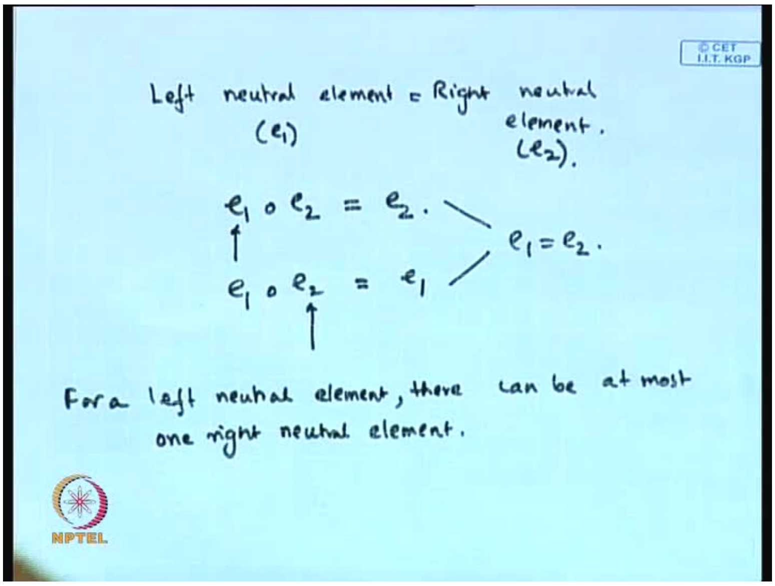
(Refer Slide Time: 33:43)



Monoid

- A neutral element of the semigroup (H, ○) is an element e in H, which satisfies e ○ a = a ○ e = a, for all a in H.
- If the semigroup contains a neutral element it is called monoid.
- A semigroup has at most one neutral element.
- If e ε H is a neutral element of the semigroup (H, ○), then b ε H is called an inverse of a if a ○ b=b ○ a = e.
- If a has an inverse, then a is called invertible in the semigroup H.
- In a monoid, each element has at most one inverse.

(Refer Slide Time: 33:55)



Left neutral element = Right neutral element.
(e_1) (e_2).

$e_1 \circ e_2 = e_2$.

$e_1 \circ e_2 = e_1$

$e_1 = e_2$.

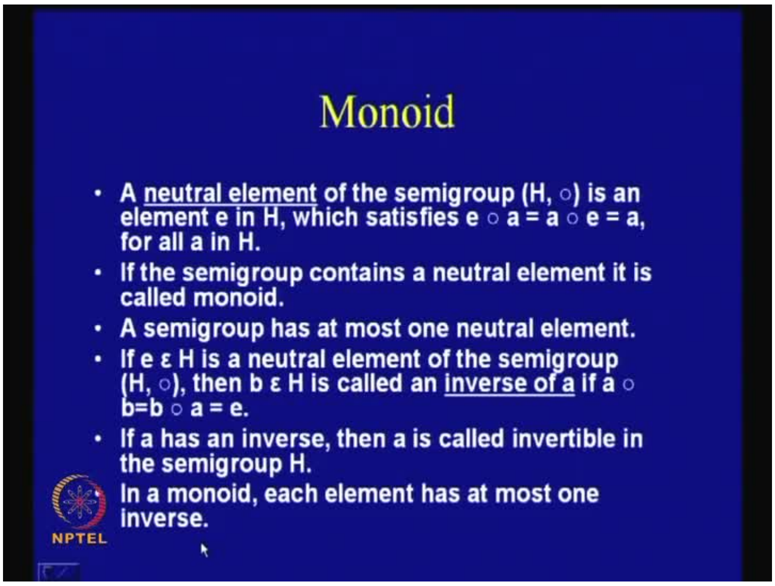
For a left neutral element, there can be at most one right neutral element.

Similarly all so therefore, if the semi-group contains a neutral element like this then it is actually defined to be something which is called a monoid so, a semi-group has there is a result which says that a semi-group has at most one neutral element and this is actually not very difficult to prove so the first result that we can actually kind of reflect is that the left neutral element and the right neutral element are the same so if i just consider the left neutral element so the left neutral element and the right neutral element are the same why

Now you can just say that the left the left neutral element be e one and let the right neutral element be e two so what about e one operation e two now you see that if i just think that this is the left neutral element then by the definition i know that e one operation with e two should be e two because this is the left neutral element now what what if i think this to be the right neutral element like if i just think that e two if i think that e two is the right neutral element then i know that e one operation e two will be e one therefore, from here i understand that e one and e two are the same right

So therefore, the left neutral element and the right neutral element are the same now the other thing that holds is that if there is one neutral element then there can be at most one right neutral element so this proof i i mean it is quite easy actually you can follow the similar principle but, i leave this as an exercise that is if there is a left neutral element that is for a left left neutral element there can be at most one right neutral element so therefore, so from here we know that if there can be at most one right neutral element then this right neutral element is again same as the left neutral element by this definition so there can be at most so from these two results we can conclude that there can be at most one neutral element ok

(Refer Slide Time: 36:14)

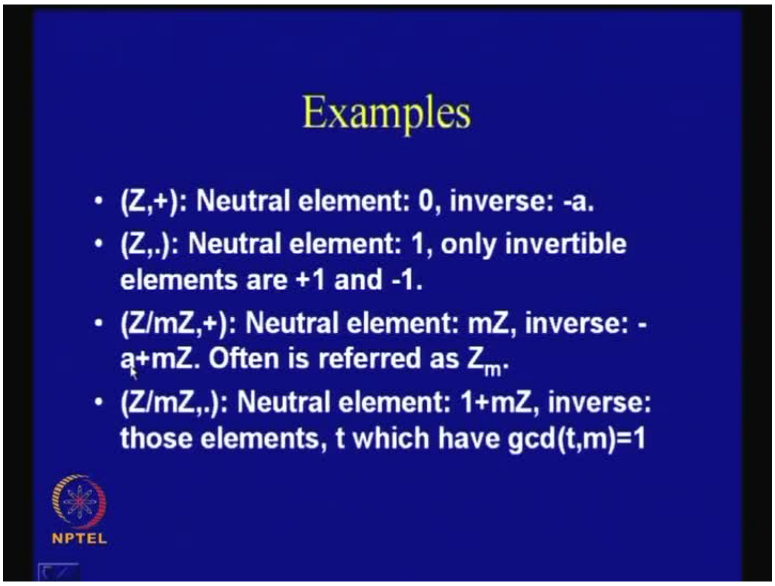


Monoid

- A neutral element of the semigroup (H, ○) is an element e in H, which satisfies e ○ a = a ○ e = a, for all a in H.
- If the semigroup contains a neutral element it is called monoid.
- A semigroup has at most one neutral element.
- If e ε H is a neutral element of the semigroup (H, ○), then b ε H is called an inverse of a if a ○ b=b ○ a = e.
- If a has an inverse, then a is called invertible in the semigroup H.
- In a monoid, each element has at most one inverse.

So therefore, if the semi-group which essentially has a neutral element which is called a monoid has can can have at most one neutral element therefore, this result holds true that is semi-group has got at most one neutral element now if e which belongs to h is a neutral element of the semi-group and and of the semi-group and then b also belongs to h then there is a definition of inverse like this that is if i take a and if i operation operate it with b then this is same as and it is same as b being operated on a and i obtain e so for example, when i am doing when i consider the semi-group z coma plus then what will be the inverse of a it will be minus a so because if i know that if i add with minus a that i obtain back the neutral element which is zero

(Refer Slide Time: 37:05)

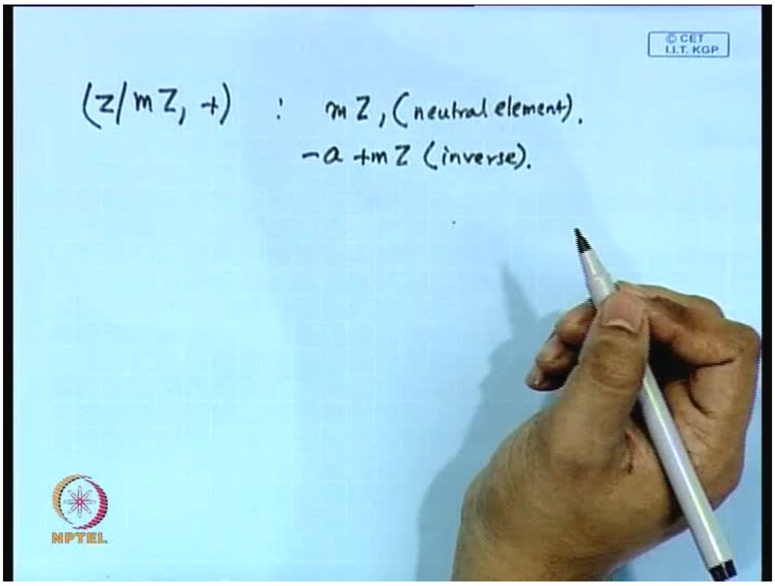


Examples

- (Z,+): Neutral element: 0, inverse: -a.
- (Z,.): Neutral element: 1, only invertible elements are +1 and -1.
- (Z/mZ,+): Neutral element: mZ, inverse: -a+mZ. Often is referred as Z_m.
- (Z/mZ,.): Neutral element: 1+mZ, inverse: those elements, t which have gcd(t,m)=1

So if a has an inverse then a is called invertible in the semi-group h and in a monoid each element has at most one inverse so this also result can be proved that is if there is a monoid so in the monoid then each element has at most one inverse so examples are like this that is if i consider z coma plus the neutral element is zero and inverse is minus a if you consider z under multiplication the neutral element is one and the only invertible elements are plus one and minus one because if i just consider any other integer le[t's]-says five then there is no integer say integer number if you multiply with which you will obtain back the neutral element except therefore, the neutral element exists only for plus one and minus one

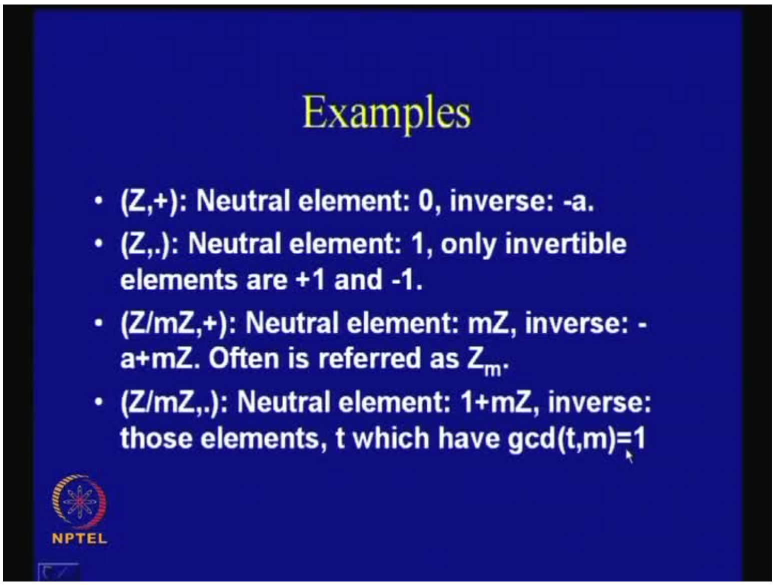
(Refer Slide Time: 37:53)



$(Z/mZ, +)$: mZ, (neutral element).

$-a + mZ$ (inverse).

(Refer Slide Time: 38:24)

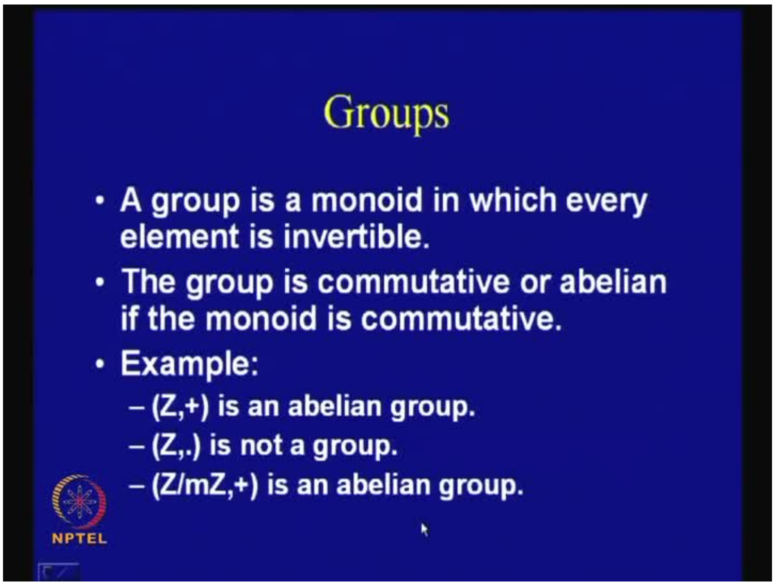


Examples

- (Z,+): Neutral element: 0, inverse: -a.
- (Z,.): Neutral element: 1, only invertible elements are +1 and -1.
- (Z/mZ,+): Neutral element: mZ, inverse: -a+mZ. Often is referred as Z_m.
- (Z/mZ,.): Neutral element: 1+mZ, inverse: those elements, t which have gcd(t,m)=1

What about the residue class z slash m z plus and operation is plus then neutral element is m z itself and the inverse is minus a so this should be actually minus a plus m z so it means that if i take if if i just consider this particular set that is z z m z which is a semi-group and then the operation is defined as plus then a neutral element is m z so that is the neutral element and the inverse is so this is the neutral element and the inverse is minus a plus m z so that is the inverse and you can verify this it is quite simple so, what about z m z and product z m z coma product in this case the neutral element is one plus m z and the inverse and this result we will see actually is are those elements t which are actually which are actually co-plained to m that is every element does not have an inverse but, only those elements for only those elements inverse exist which are actually co-plained to m so which means that the g c d or the greatest common devisor of that number and m is actually equal to one so we will see this as we go ahead

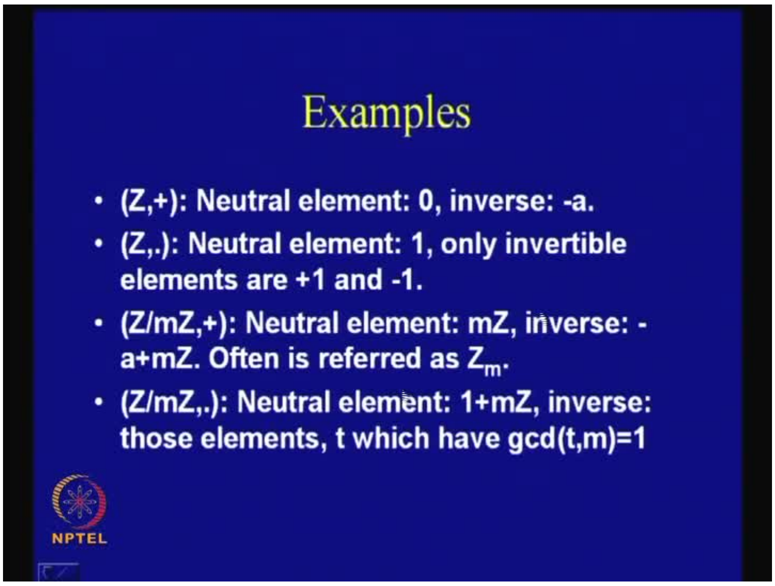
(Refer Slide Time: 38:50)



Groups

- A group is a monoid in which every element is invertible.
- The group is commutative or abelian if the monoid is commutative.
- Example:
  - (Z,+) is an abelian group.
  - (Z,.) is not a group.
  - (Z/mZ,+) is an abelian group.

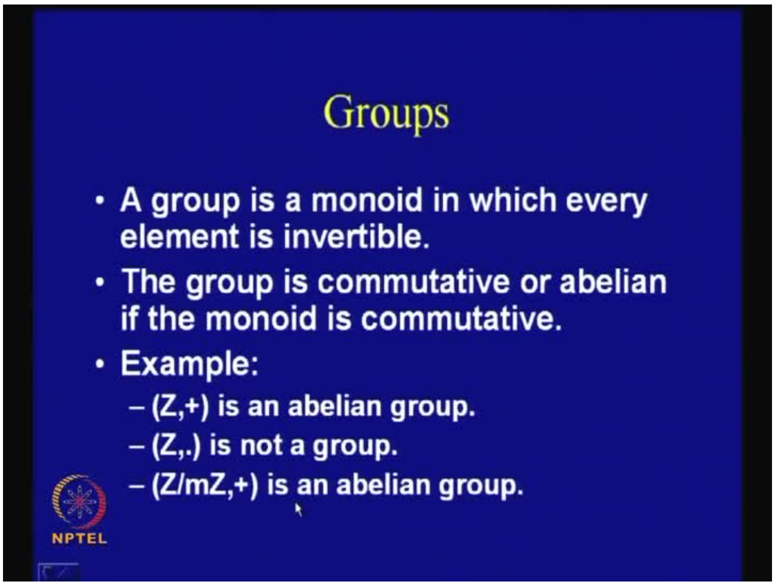
(Refer Slide Time: 39:33)



Examples

- (Z,+): Neutral element: 0, inverse: -a.
- (Z,.): Neutral element: 1, only invertible elements are +1 and -1.
- (Z/mZ,+): Neutral element: mZ, inverse: -a+mZ. Often is referred as Z_m.
- (Z/mZ,.): Neutral element: 1+mZ, inverse: those elements, t which have gcd(t,m)=1

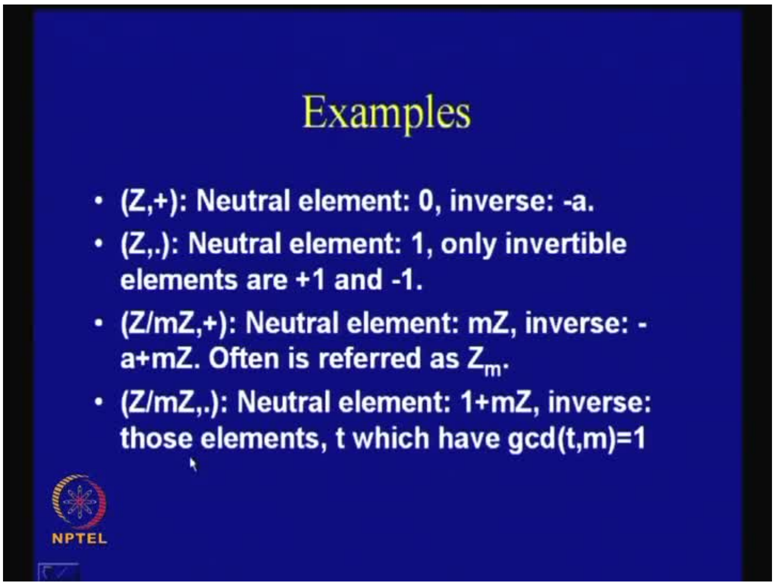
(Refer Slide Time: 39:41)



Groups

- A group is a monoid in which every element is invertible.
- The group is commutative or abelian if the monoid is commutative.
- Example:
  - (Z,+) is an abelian group.
  - (Z,.) is not a group.
  - (Z/mZ,+) is an abelian group.

(Refer Slide Time: 39:53)

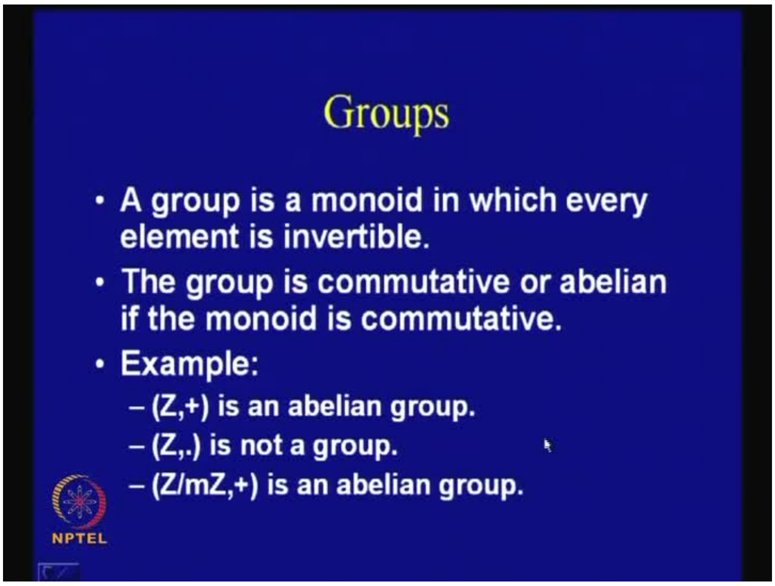


Examples

- (Z,+): Neutral element: 0, inverse: -a.
- (Z,.): Neutral element: 1, only invertible elements are +1 and -1.
- (Z/mZ,+): Neutral element: mZ, inverse: -a+mZ. Often is referred as Z_m.
- (Z/mZ,.): Neutral element: 1+mZ, inverse: those elements, t which have gcd(t,m)=1

So then we define what is called a group a group is a monoid in which every element is invertible so a group is a monoid in which every element is invertible and the group is commutative or abelian if the monoid is also commutative so examples of this will be like z coma plus which is an abelian group and z product which is not a group so so this is actually not an example of a group and then we have got z coma m m z and plus z slash m z and plus which is an abelian group so why is this not a group this is not a group because from the definition of a group a group is a monoid in which every element is invertible and we have just defined just discussed in the previous slide that is in this particular set only invertible elements are plus one and minus one so every element does not i mean rather every element does not have does not have an inverse therefore, z coma multiplication is actually not a group because every element does not is not invertible in this is not invertible in these semi-group ok

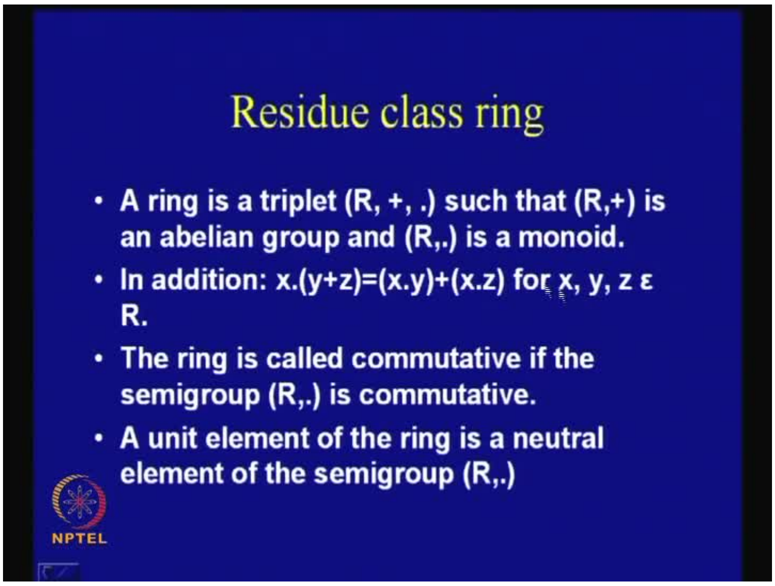
(Refer Slide Time: 39:56)



Groups

- A group is a monoid in which every element is invertible.
- The group is commutative or abelian if the monoid is commutative.
- Example:
  - (Z,+) is an abelian group.
  - (Z,.) is not a group.
  - (Z/mZ,+) is an abelian group.

(Refer Slide Time: 40:01)

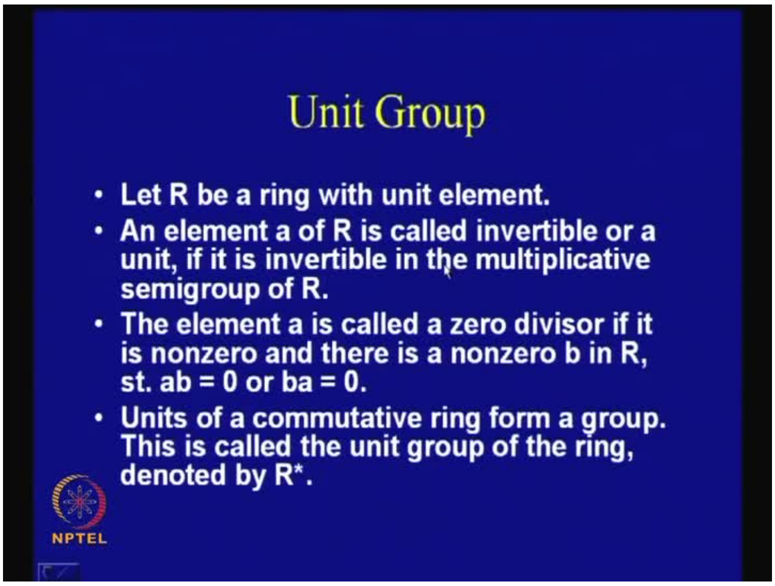


Residue class ring

- A ring is a triplet (R, +, .) such that (R,+) is an abelian group and (R,.) is a monoid.
- In addition: x.(y+z)=(x.y)+(x.z) for x, y, z ε R.
- The ring is called commutative if the semigroup (R,.) is commutative.
- A unit element of the ring is a neutral element of the semigroup (R,.)

So therefore, that is that is the definition of a group and there is higher concept to this which is called ring and ring is nothing but, r and they are actually triplets so there is not only one operation as plus and there is another operation also along with it such that r coma plus is an abelian group the way we have defined and r coma product is r coma the second operation is actually a monoid in addition it satisfies the properties of distributivity which says that x if we mul[tiply]- i mean product if we take product with y plus z then which is same as x dot y plus x dot z for x y z which belongs to this ring the ring is also called commutative if the semi-group r coma dot that is this one is also commutative and a unit element of the ring is the neutral element of the semi-group r coma dot so a unit element of the ring is a neutral element of the semi-group r coma dot therefore, a neutral unit element of this ring will be as defined as the neutral element of this of the monoid r coma dot.

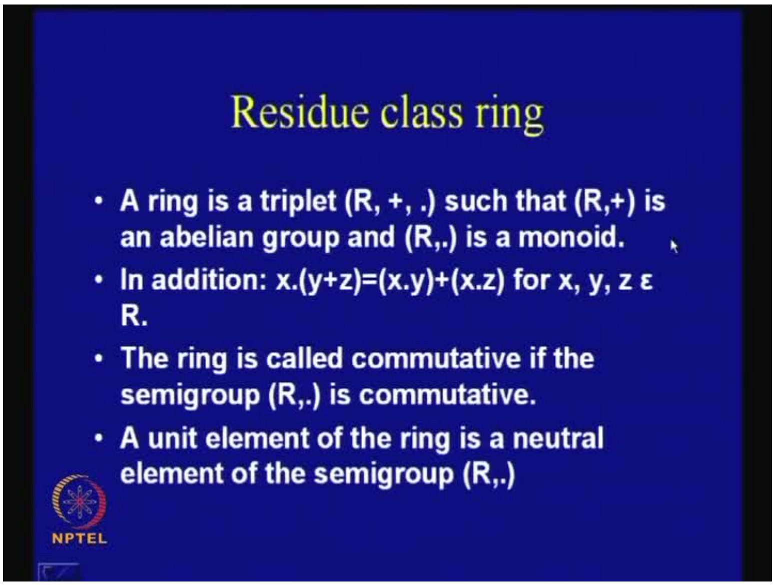
(Refer Slide Time: 41:01)



Unit Group

- Let R be a ring with unit element.
- An element a of R is called invertible or a unit, if it is invertible in the multiplicative semigroup of R.
- The element a is called a zero divisor if it is nonzero and there is a nonzero b in R, st. ab = 0 or ba = 0.
- Units of a commutative ring form a group. This is called the unit group of the ring, denoted by R*.

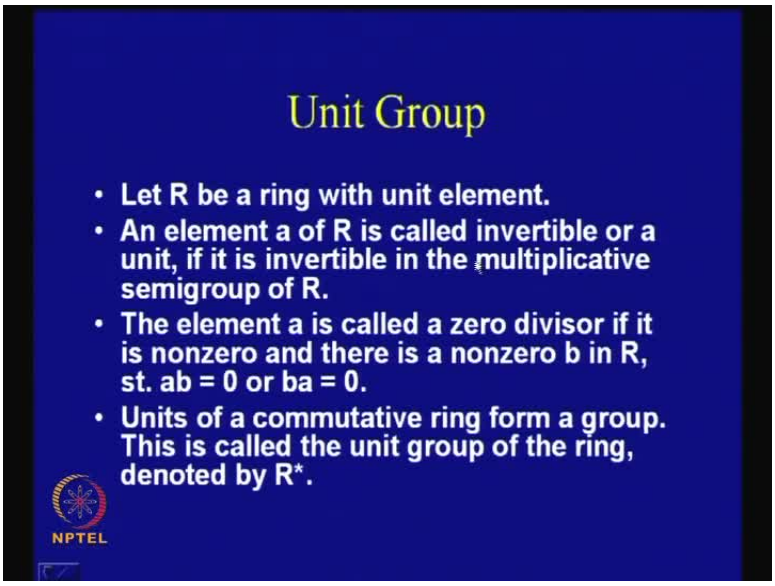
(Refer Slide Time: 41:30)



Residue class ring

- A ring is a triplet (R, +, .) such that (R,+) is an abelian group and (R,.) is a monoid.
- In addition: x.(y+z)=(x.y)+(x.z) for x, y, z ε R.
- The ring is called commutative if the semigroup (R,.) is commutative.
- A unit element of the ring is a neutral element of the semigroup (R,.)

(Refer Slide Time: 41:36)

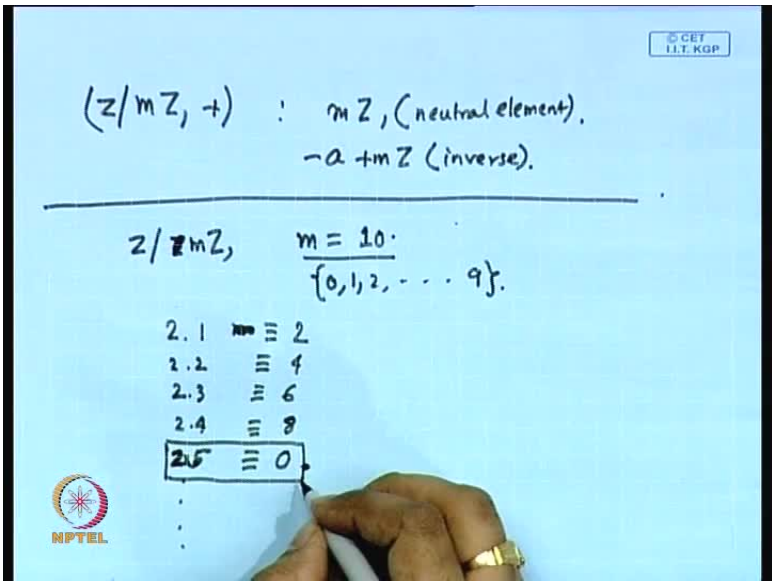


Unit Group

- Let R be a ring with unit element.
- An element a of R is called invertible or a unit, if it is invertible in the multiplicative semigroup of R.
- The element a is called a zero divisor if it is nonzero and there is a nonzero b in R, st. ab = 0 or ba = 0.
- Units of a commutative ring form a group. This is called the unit group of the ring, denoted by R*.

So then we define what is called a unit group which means that let r be a ring with unit element an element a of r is called invertible or a unit if it is invertible in the multiplicative semi-group of r so an element a i repeat this definition a element a of r is called invertible or a unit if it is invertible in the multiplicative semi-group of r that means multiplicative semi-group of r will be this if it is invertible in this particular semi-group then it is said to be invertible and the element a is called a zero divisor if it is non-zero that is if the element itself is non-zero and there is a non-zero b in r such that if i take the product of a and b or the product of b and a then we get back zero now units of a commutative ring actually from a group and this is called the unit group of the ring and it is often denoted by r star ok

(Refer Slide Time: 42:15)



$(\mathbb{Z}/m\mathbb{Z}, +)$: $m\mathbb{Z}$, (neutral element).

$-a + m\mathbb{Z}$ (inverse).

$\mathbb{Z}/m\mathbb{Z}$, $\underline{m = 10}$.

$\{0, 1, 2, \ldots 9\}$.

$2.1 \equiv 2$

$2.2 \equiv 4$

$2.3 \equiv 6$

$2.4 \equiv 8$

$\boxed{2.5 \equiv 0}$

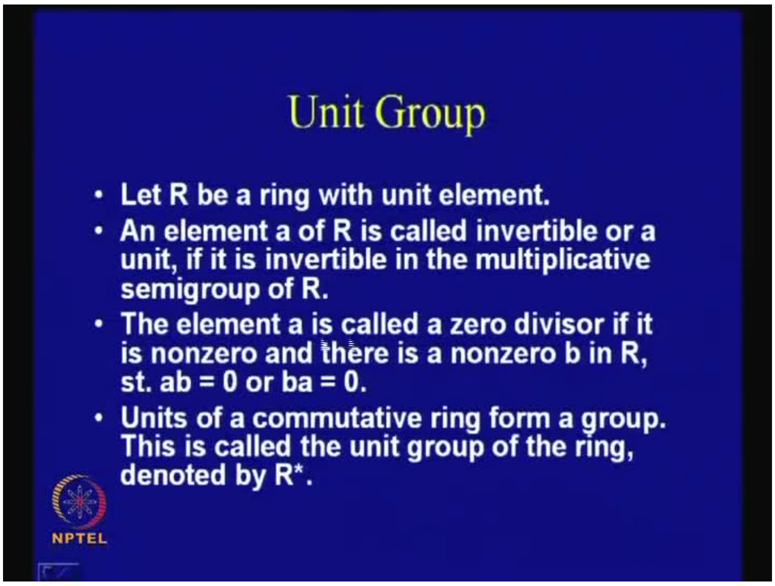
.

.

.

So that is the definition of a unit group and we can actually have one very i mean some example because i think this is little abstract so in order to understand this let us take some examples so let us consider the set or rather let us consider the ring z m z and let us define let us define rather let us take the value of m to be something like ten so we know that the elements here will be like zero one two and so on till nine now you consider like whether all the elements so let us consider like some some let us consider some interesting facts let us consider the numbers for example, two and let us consider like let us multiply two with all possible elements which are there all possible nonzero elements which are there in the set

(Refer Slide Time: 43:54)

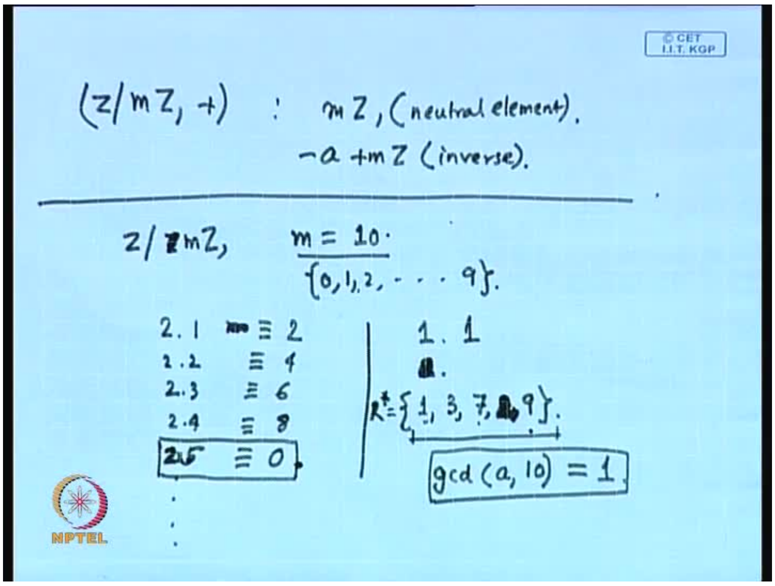


Unit Group

- Let R be a ring with unit element.
- An element a of R is called invertible or a unit, if it is invertible in the multiplicative semigroup of R.
- The element a is called a zero divisor if it is nonzero and there is a nonzero b in R, st. ab = 0 or ba = 0.
- Units of a commutative ring form a group. This is called the unit group of the ring, denoted by R*.

So let us consider two into one two into two two into three two into four two into five and so on if you consider these mult[iply]- these products and if you take the modulo ten operation that is if you take mod ten for all of them then you’ll find that this is actually equal to two this is actually equal to four this is six this is eight but, this one is zero so this shows us an example where there are two elements which are nonzero like two is nonzero and five is also nonzero but, if i multiply this and if we take i mean in these particular if i take a modulo ten then what i obtain back is zero therefore, from this definition we say that two is actually a zero divisor the element two is actually a zero divisor therefore, this particular thing i mean therefore, i mean this this is an example which shows that zero divisor exists therefore, let us come back to this and see whether element a is called a zero divisor if it is a nonzero and there is a nonzero b in r such that a multiplied with b or b multiplied with a is zero so this is an example to understand this particular aspect

(Refer Slide Time: 44:19)



$(Z/mZ, +)$: mZ, (neutral element).

$-a + mZ$ (inverse).

Z/mZ, $m = 10$.

$\{0, 1, 2, \dots 9\}$.

$2.1 \equiv 2$

$2.2 \equiv 4$

$2.3 \equiv 6$

$2.4 \equiv 8$

$\boxed{2.5 \equiv 0}$

$\vdots$

1.1

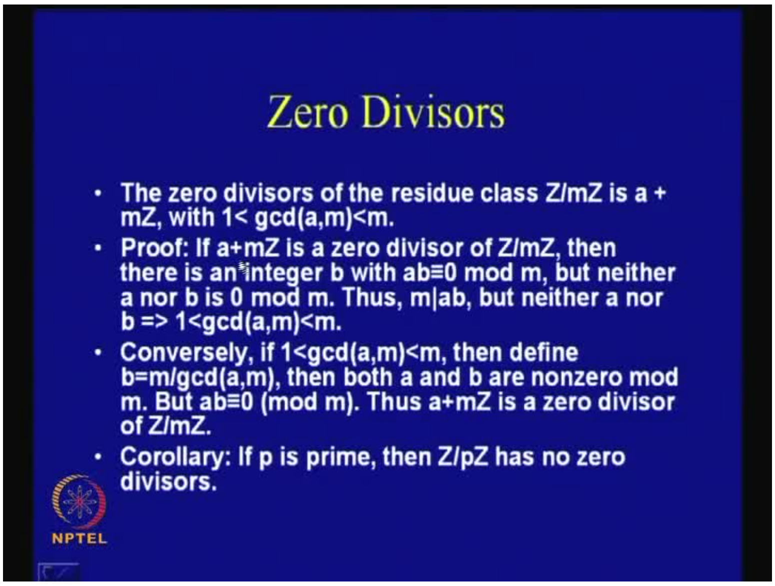
$R^* = \{1, 3, 7, 9\}$.

$\boxed{gcd(a, 10) = 1}$

Now what about this an element a of r is called invertible or unit if it is invertible in the multiplicative semi-group of r so let us see that among these particular i mean numbers like zero one two an[d]- nine what are the elements which are invertible so let us leave out zero because zero is obviously not invertible let us consider one so we know that if i take one and multiply it with one i get back one itself what about two so if i take two and if i multiply with with any of the numbers will i get back one so actually we will see that no you will not get back two is not invertible ok

So the numbers which are invertible in this particular set from zero to nine can actually be found out like this there we see one similarly, three will invertible four will not be invertible five could not invertible six will not be invertible seven will be invertible nine will be invertible eight will also be invertible sorry eight not will not be invertible nine will be invertible and the reason rather the one you see we have checking is that if i take the g c d of any of these numbers a and with ten if a is invertible then this g c d of and ten should be equal to one so if the g c d of a coma ten is equal to one then we we say that a is invertible so a is invertible if and only if the g c d of a coma ten will be equal to one so that means you'll find that this particular set that is one three seven and nine will actually form something which is called as unit-group therefore, this will form a unit-group so i mean it is often defined as r star in this ring so we will see more examples of this but, as we proceed we will see more examples of this

(Refer Slide Time: 45:58)

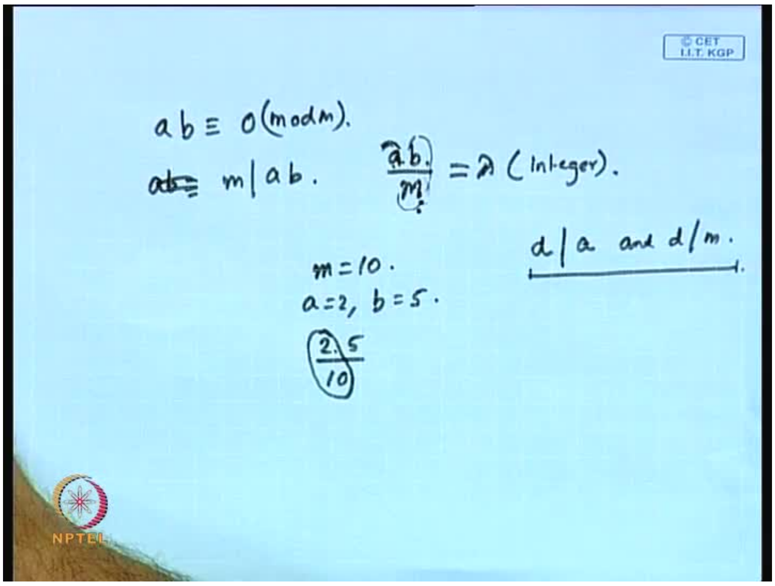


Zero Divisors

- The zero divisors of the residue class Z/mZ is a + mZ, with 1< gcd(a,m)<m.
- Proof: If a+mZ is a zero divisor of Z/mZ, then there is an integer b with ab≡0 mod m, but neither a nor b is 0 mod m. Thus, m|ab, but neither a nor b => 1<gcd(a,m)<m.
- Conversely, if 1<gcd(a,m)<m, then define b=m/gcd(a,m), then both a and b are nonzero mod m. But ab≡0 (mod m). Thus a+mZ is a zero divisor of Z/mZ.
- Corollary: If p is prime, then Z/pZ has no zero divisors.

So let us consider zero divisor therefore, the zero divisors of the residue class z slash m z is actually a plus m z and this is the generalization of what we said that is zero divisors of the residue class z slash m z is actually a plus m z such that if you take the g c d of a and with m then it is neither one nor m but, it is somewhere in between so that is nontrivial g c d of a and m and the proof is very simple it says that if a plus m z if the zero divisor of z slash m z then there is an integer b this follows take down the definition such that a b is congruent to zero modulo m but, neither a nor b is zero modulo m so which means that m divides a b so a b is congruent to zero means m divides a b but, neither a nor b is actually divisible by m

(Refer Slide Time: 47:06)



$ab \equiv 0 \pmod{m}$.

$\cancel{ab \equiv}$ $m \mid ab$. $\frac{ab}{m} = \lambda$ (Integer).

$d \mid a$ and d/m.

$m = 10$.

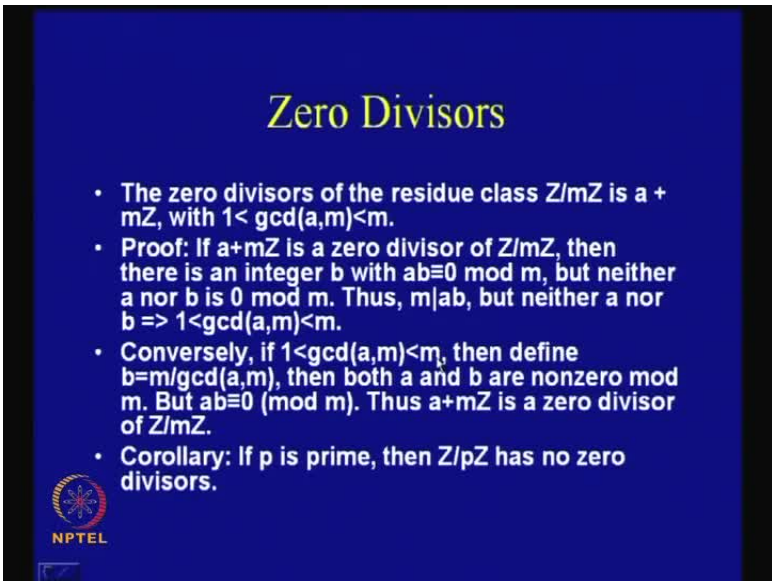
$a = 2$, $b = 5$.

$\frac{2.5}{10}$

So this atomically implies that if i take the g c d of a and m then this should be some significant value that is it means that if you take m so, say that a b is congruent to zero modulo m right so that means that a b will be equal to i mean rather m divides a b right so if a m divides a b so which means that a b divided by rather a b divided by m this should be a number right this should be an integer number this is an integer value but, we know that neither a nor b are actually divisible by m therefore, a by m is not an integer b by m is not an integer so that means that a and b definitely i mean i mean there should be a cancellation between a and m and that means that the g c d of a and m should be actually something which is between one and m so it is neither one nor m see for example, if you just consider the example just now what we considered with m is equal to ten and a being equal to two and b being equal to five ok

So now let us consider two into five divided by ten this ratio so you see that two into five by ten therefore, it means that the g c d of this particular thing is actually not equal to its not it is neither one nor ten but, it is in between therefore, this shows that there should be a i mean there should be a number d which divides both a and d also divides m there should be a number d and that number is neither d is not neither equal to one nor nor is equal to m so this proves that this shows that m divides a b but, neither a not nor nor b and therefore, this implies that the g c d of a and m lies between one and m.

(Refer Slide Time: 49:03)



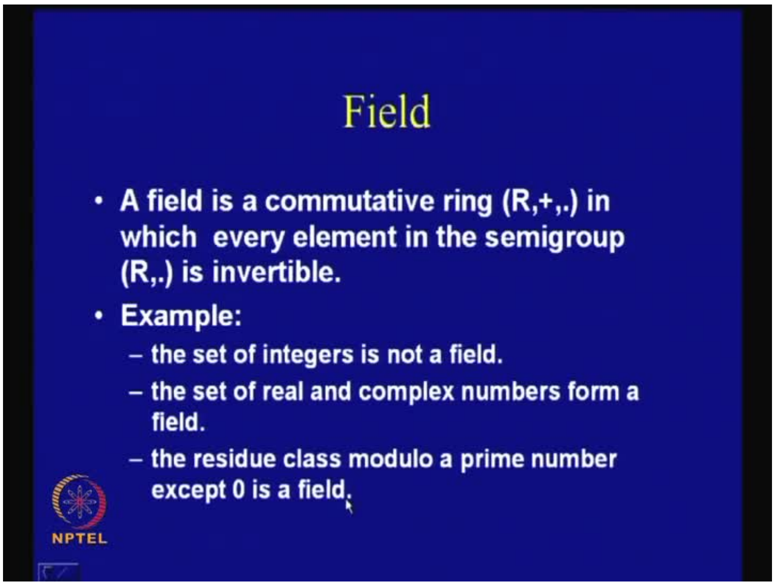
Zero Divisors

- The zero divisors of the residue class Z/mZ is a + mZ, with 1< gcd(a,m)<m.
- Proof: If a+mZ is a zero divisor of Z/mZ, then there is an integer b with ab≡0 mod m, but neither a nor b is 0 mod m. Thus, m|ab, but neither a nor b => 1<gcd(a,m)<m.
- Conversely, if 1<gcd(a,m)<m, then define b=m/gcd(a,m), then both a and b are nonzero mod m. But ab≡0 (mod m). Thus a+mZ is a zero divisor of Z/mZ.
- Corollary: If p is prime, then Z/pZ has no zero divisors.

Now conversely if one this lesser than equal to g c d is less than g c d is a coma m less than m then define then if i define a number b as m divided by g c d a coma m then both a and b are nonzero modulo m so then both a and b are nonzero modulo m that is true from the definition itself right but, if what what if i multiply a and b so if i multiply a and b then what i obtain is a so if i if i take this definition of m divided by g c d of a coma m and if i multiply this with a then i obtain zero modulo m the reason is if i if i multiply this with a and this is the g c d of a coma m then this divides a and therefore, what i obtain is an integer multiple of m and therefore, if i take a congruence or rather if i divide it by a and take the remainder then the remainder is zero so this proves that a b is congruent to zero modulo m thus a plus m z is a zero divisor of z slash m z

So therefore, we will see that i mean zero zero divisors i mean it is very easy to detect zero divisors how i mean because we just this simple test reveals the zero divisor if i take the g c d of number a and along with m and if the g c d lies between one and m then actually it forms the zero divisors so there is a natural corollary to this that if p is a prime then set z plus z slash p z will have no zero divisors because because if i take the g c d of a number with p then it is always equal to one because that is the definition of primelity right so that means that it automatically implies that there are no zero devisors if p is a prime number in this particular z slash p z

(Refer Slide Time: 50:47)

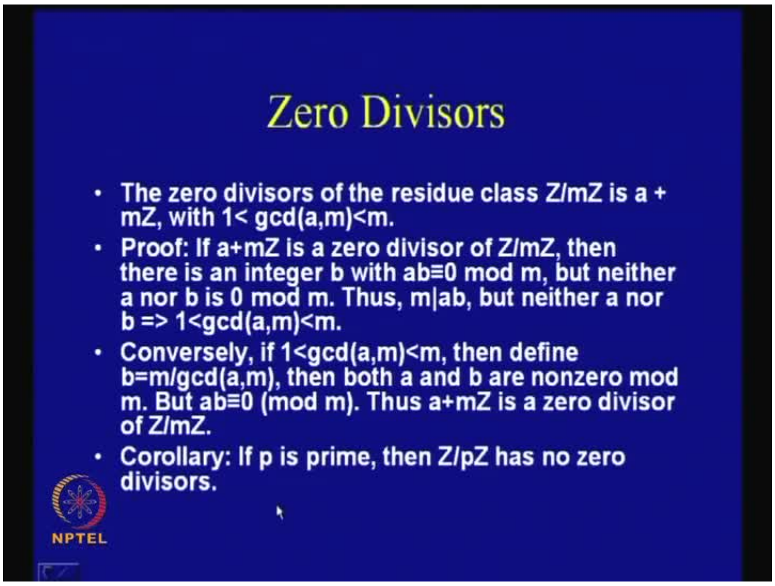


Field

- A field is a commutative ring (R,+,.) in which every element in the semigroup (R,.) is invertible.
- Example:
  - the set of integers is not a field.
  - the set of real and complex numbers form a field.
  - the residue class modulo a prime number except 0 is a field.

NPTEL

(Refer Slide Time: 51:21)

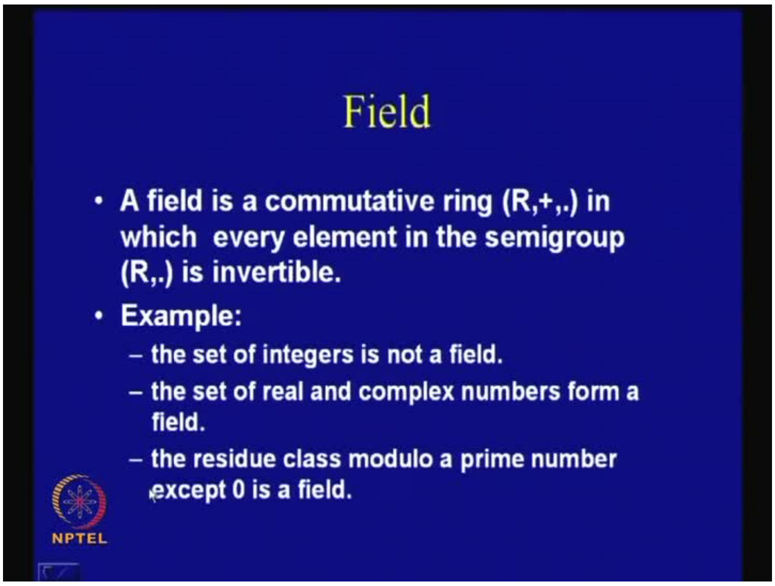


Zero Divisors

- The zero divisors of the residue class Z/mZ is a + mZ, with 1< gcd(a,m)<m.
- Proof: If a+mZ is a zero divisor of Z/mZ, then there is an integer b with ab≡0 mod m, but neither a nor b is 0 mod m. Thus, m|ab, but neither a nor b => 1<gcd(a,m)<m.
- Conversely, if 1<gcd(a,m)<m, then define b=m/gcd(a,m), then both a and b are nonzero mod m. But ab≡0 (mod m). Thus a+mZ is a zero divisor of Z/mZ.
- Corollary: If p is prime, then Z/pZ has no zero divisors.

NPTEL

(Refer Slide Time: 51:29)

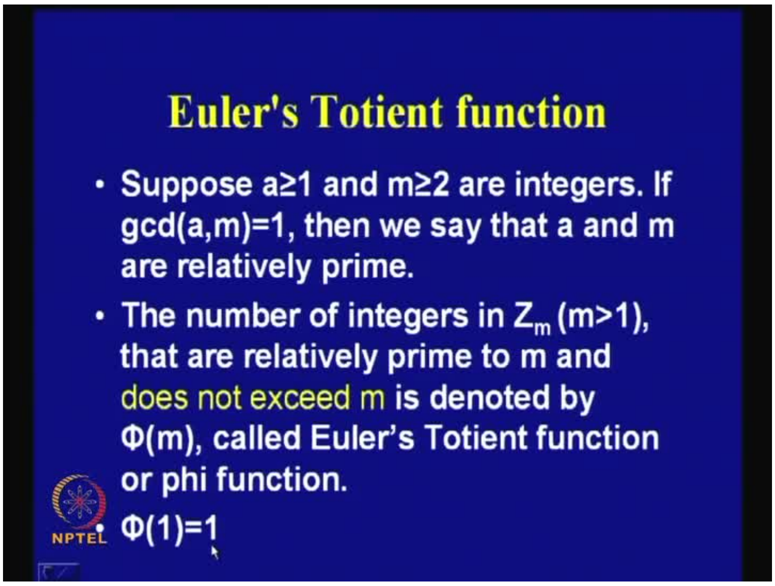


Field

- A field is a commutative ring (R,+,.) in which every element in the semigroup (R,.) is invertible.
- Example:
  - the set of integers is not a field.
  - the set of real and complex numbers form a field.
  - the residue class modulo a prime number except 0 is a field.

So then we come to the definition of field which says that a field is a commutative ring r plus multiplication in which every element in the semi-group r multiplication is invertible therefore, if every element is invertible then it is a field so examples of this would be like the set of integers is not a field because you know why i mean the set of integers cannot form a field because every number is not invertible the set of real and complex numbers from a field and the residue class modulo prime number except zero is a field why because we are seeing that because of this particular result if p is a prime then z slash p z will have no zero divisors so that automatically implies that this is not a field

(Refer Slide Time: 51:31)

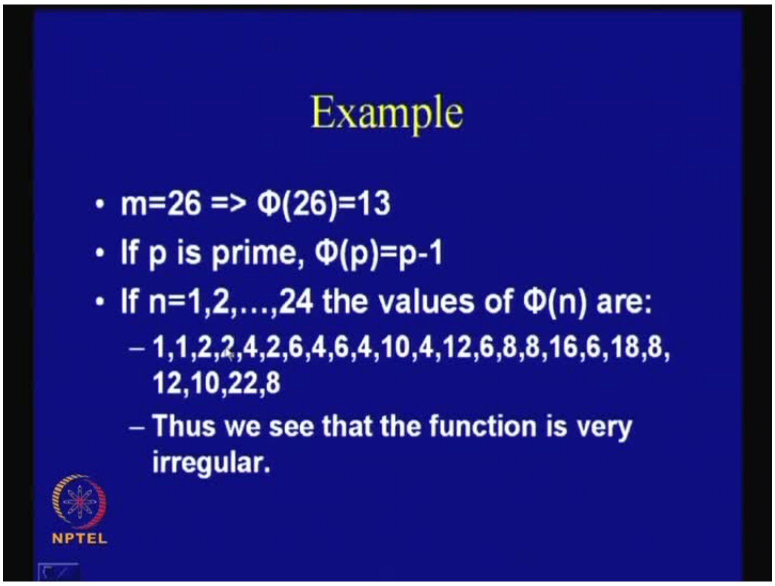


Euler's Totient function

- Suppose a≥1 and m≥2 are integers. If gcd(a,m)=1, then we say that a and m are relatively prime.
- The number of integers in Z_m (m>1), that are relatively prime to m and does not exceed m is denoted by Φ(m), called Euler's Totient function or phi function.
- Φ(1)=1

So then we come to the concept of euler's totient function which says that if a is greater than equal to one and m is greater than equal to two are integers and if g c d of a coma m is equal to one then we say that a and m are relatively prime now the number of integers in z m where m is greater than one that are relatively prime to m and does not exceed m is denoted by phi m or which is also called as euler's totient function or phi function therefore, we will we will start with this define it in a recursive fashion and it says that phi of one is equal to one ok

(Refer Slide Time: 52:06)

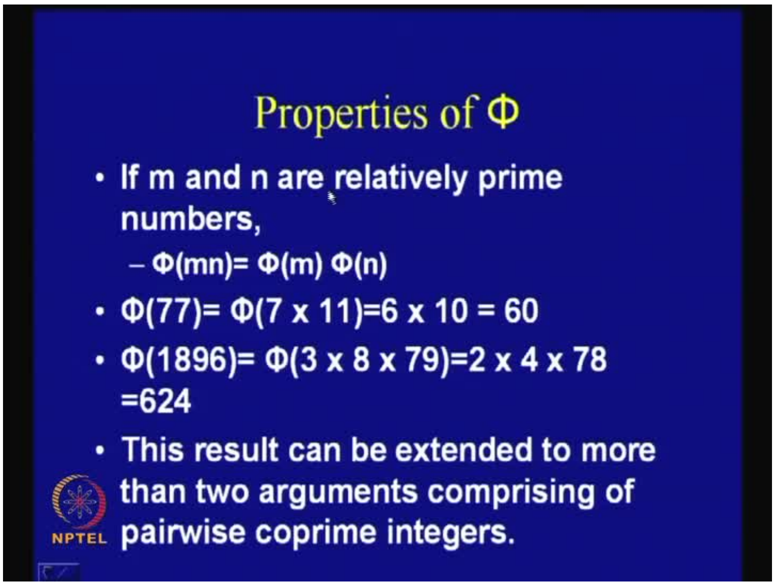


Example

- m=26 => Φ(26)=13
- If p is prime, Φ(p)=p-1
- If n=1,2,...,24 the values of Φ(n) are:
  - 1,1,2,2,4,2,6,4,6,4,10,4,12,6,8,8,16,6,18,8, 12,10,22,8
  - Thus we see that the function is very irregular.

Now what about let us consider phi of twenty six so twenty six is a number of english letters which are there and we let us consider the value of phi of twenty six we can see that phi of twenty six is equal to thirteen if p is a prime then phi of p is p minus one and if n is equal to one two twenty four then the values of phi n are as follows so this is just a enumeration so, you'll see that you can verify these results but, the fact is that this function is very irregular that is you'll not find any distinct even (( )) like it is not like as n increases phi n always increases you can see that there is defect time also ok

(Refer Slide Time: 52:44)

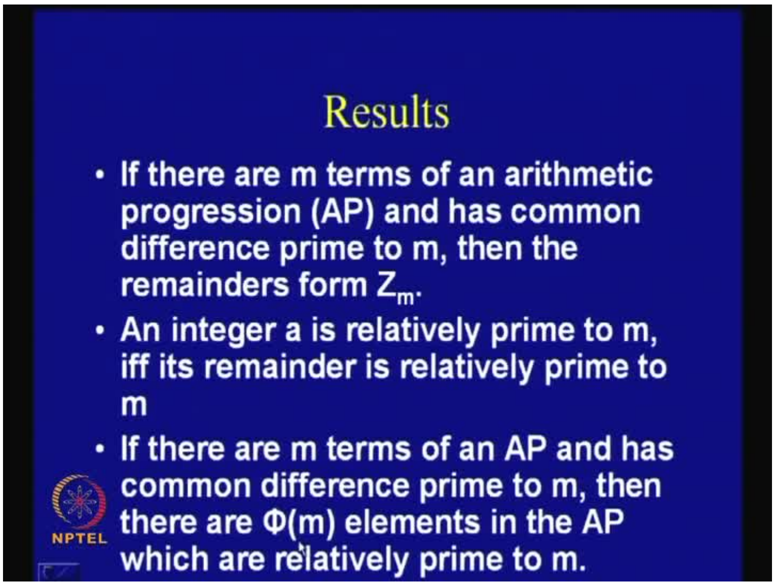


Properties of Φ

- If m and n are relatively prime numbers,
  - Φ(mn)= Φ(m) Φ(n)
- Φ(77)= Φ(7 x 11)=6 x 10 = 60
- Φ(1896)= Φ(3 x 8 x 79)=2 x 4 x 78 =624
- This result can be extended to more than two arguments comprising of pairwise coprime integers.

So now the let us see the properties of phi n so there is a very interesting result which says that if m and n are relatively prime numbers then phi of m n is nothing but, the product of phi m and phi n now this result is very interesting and helpful to compute the phi of higher numbers or larger numbers for example, phi of seventy seven is same as phi of seven multiplied by eleven which is same as phi of seven multiplied by phi of eleven and we know that if seven is a prime number then phi of seven is nothing but, six and phi of eleven is nothing but, ten so the product is sixty similarly, phi of one eight nine six divide i mean if i obtain the prime factorizations i can obtain the result of six twenty four so this result can be extended to more than two arguments comprising of pair wise co-prime integers

(Refer Slide Time: 53:28)



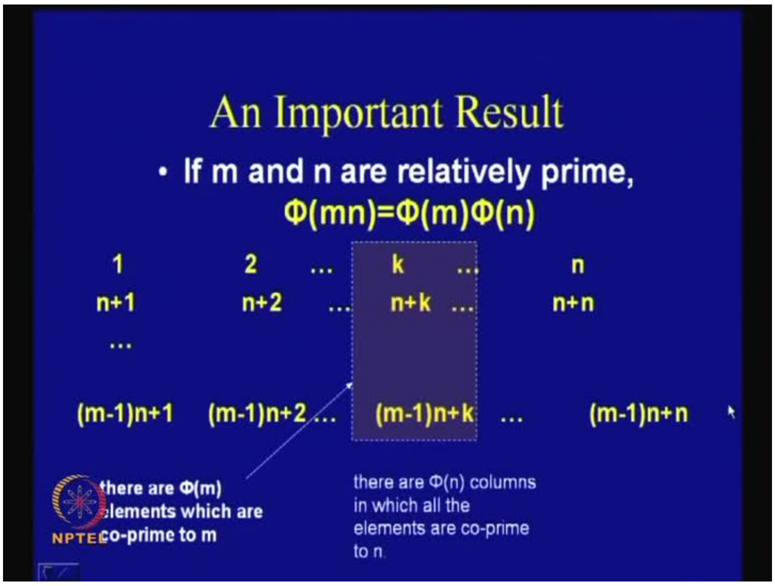
Results

- If there are m terms of an arithmetic progression (AP) and has common difference prime to m, then the remainders form Z_m.
- An integer a is relatively prime to m, iff its remainder is relatively prime to m
- If there are m terms of an AP and has common difference prime to m, then there are $\Phi(m)$ elements in the AP which are relatively prime to m.

So let us see some interesting results that is it says that if the first results says that if there are m terms of an arithmetic progression a p and has got common differences which are prime to m then the remainders form z m so if there are m terms of an arithmetic progression and has got common difference that is if the common difference is prime to m then the remainders form z m so this is a quite simple result which you can check the other one says that an integer a is relatively prime to m if and only if its remainder is relatively prime to m so if an integer a is relatively prime to m then it automatically it is an bidirectional implication is that same as saying as that its remainders is also relatively prime to m

And the other interesting results is that if there are m terms of an a p and i've got a common difference prime to m then if it is actually a combination of these two results which says that then there are phi m elements in the arithmetic progression which are relatively prime to m because so you can follow like because it says that the reminders form z m and you know that if the reminders form z m and and because i mean an integer is relatively prime to m only when the remainder is relatively prime to m so we actually need to find out the number of remainders which are relatively prime to m and that follows from the definition as phi m right therefore, if there are n terms of an arithmetic progression and the common difference is also prime to m then there are actually phi m elements in the arithmetic progression which are relatively prime to m

(Refer Slide Time: 55:05)



An Important Result

- If m and n are relatively prime, $\Phi(mn)=\Phi(m)\Phi(n)$

1	2	…	k	…	n
n+1	n+2	…	n+k	…	n+n
…					
(m-1)n+1	(m-1)n+2	…	(m-1)n+k	…	(m-1)n+n

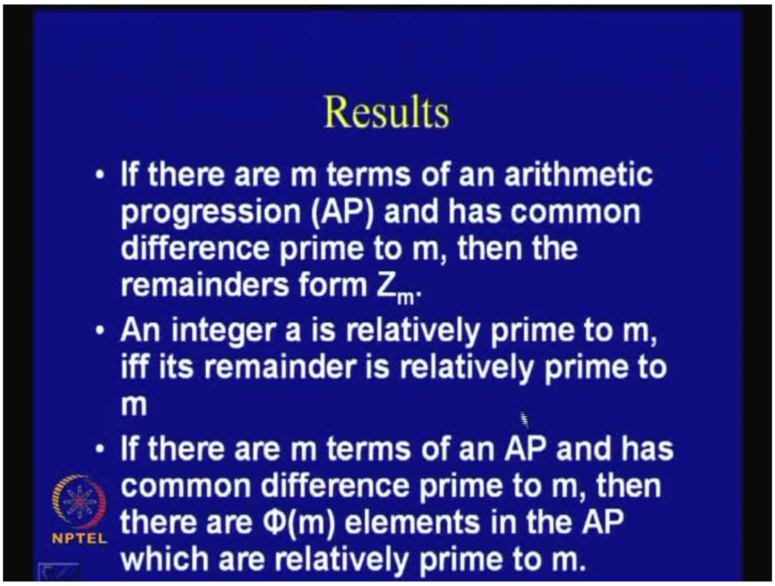
there are $\Phi(m)$ elements which are co-prime to m

there are $\Phi(n)$ columns in which all the elements are co-prime to n.

So we will apply this result to obtain this nice uh result the nice observation so let us consider phi of m n so we know from the definition phi of m n means those numbers or rather means the number of values inside from one to m minus n which are actually co-prime to m n so let us now arrange this numbers from one to m n minus so this is nothing but, m minus one i mean so this is m n minus n plus n so this is m n therefore, from one to m n all this numbers we have arranged them in this fashion so it is like one two and so on till n we arrange them in this fashion

So now you consider that among these numbers if you need to find out so if since m and n are relatively prime to both m and both n now you see that there are i mean among this numbers if you consider like this number like for example, is so, you'll find that there are phi n columns that is there are phi n columns in which all the elements are co-prime to n so if you see that for example, this particular column that is the last column that is n n plus one this this column all the elements are not co-prime to n because this is actually you will find that n multiply this n plus n this m minus one into n plus n and so on so that means that you need to find out the number of columns in which all the elements are co-prime to n and we know that there're there are actually phi n columns in which all the elements are co-prime to n

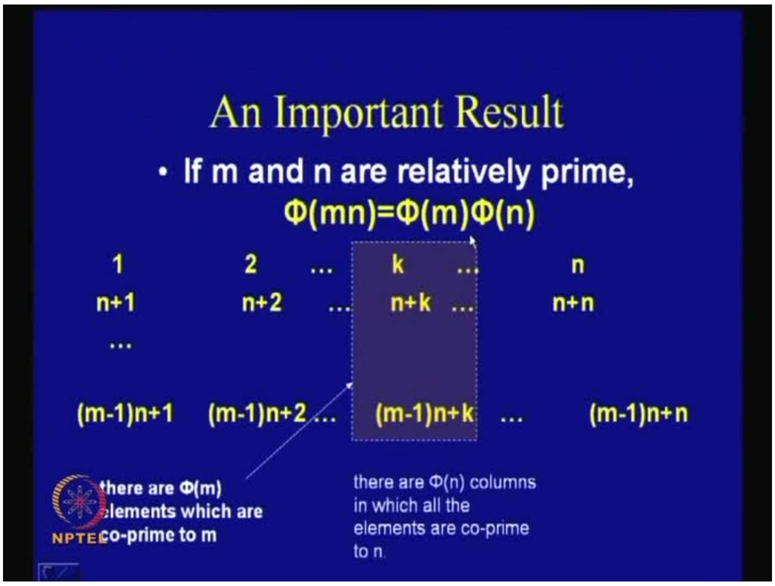
(Refer Slide Time: 57:16)



Results

- If there are m terms of an arithmetic progression (AP) and has common difference prime to m, then the remainders form Z_m.
- An integer a is relatively prime to m, iff its remainder is relatively prime to m
- If there are m terms of an AP and has common difference prime to m, then there are $\Phi(m)$ elements in the AP which are relatively prime to m.

(Refer Slide Time: 57:28)



An Important Result

- If m and n are relatively prime, $\Phi(mn)=\Phi(m)\Phi(n)$

1	2	...	k	...	n
n+1	n+2	...	n+k	...	n+n
...					
(m-1)n+1	(m-1)n+2	...	(m-1)n+k	...	(m-1)n+n

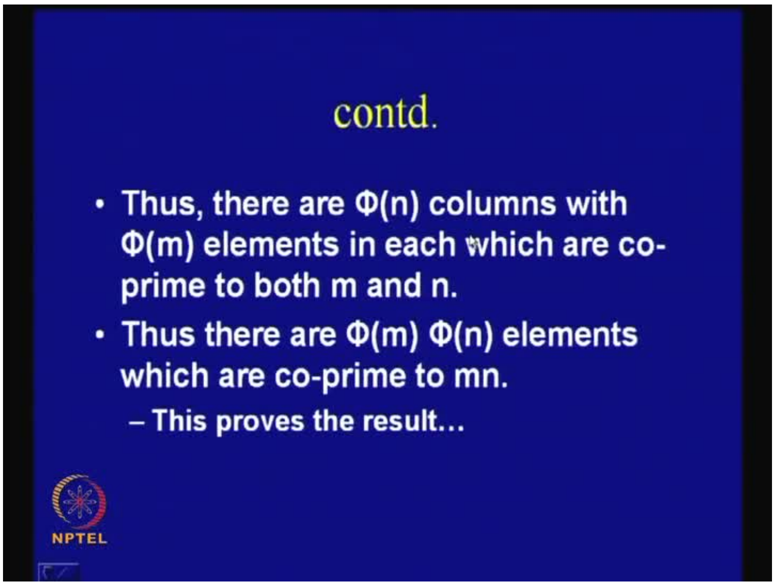
there are $\Phi(m)$ elements which are co-prime to m

there are $\Phi(n)$ columns in which all the elements are co-prime to n.

Now among this columns which are actually co-prime to n we will like to find out what are the number which are actually co-prime to m so we see that we apply the previous result and see that for example, let us consider this so in this particular column so assume that k is actually co-prime to n and consider this column and the result says the previous result says that if so what is that what is the what is the difference here what is the common difference the common difference is k now if this k is actually therefore, co-prime to m then the the previous result says that if there are m terms of an arithmetic progression and has a common difference which is prime to m then there are phi phi m elements in the arithmetic progression which are relatively prime to m so that means that these elements i mean there are phi m elements which are actually co-prime to m

So if there are phi m elements here which are co-prime to n and there are phi n five elements which are actually i mean which all the elements are co-prime to n then combining this we obtain that the phi m into phi n numbers which are actually co-prime to both m and both n and that actually forms as phi gives us the number of phi m n ok

(Refer Slide Time: 57:52)

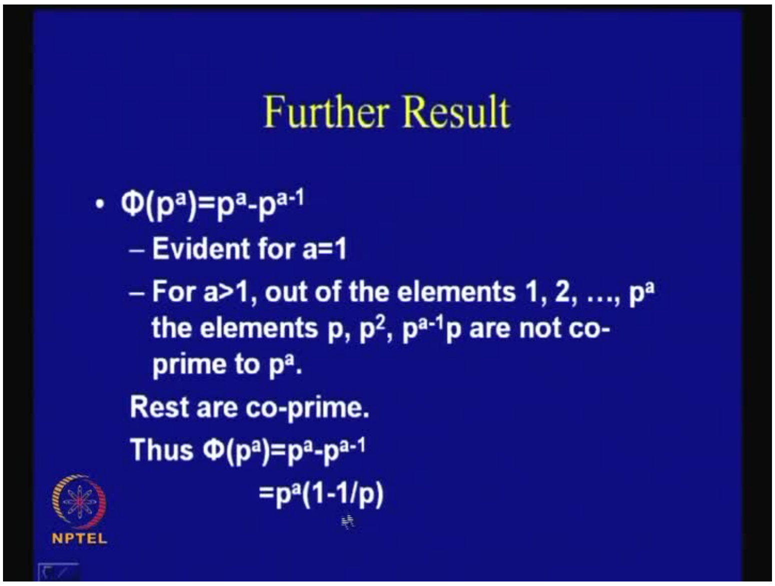


contd.

- Thus, there are Φ(n) columns with Φ(m) elements in each which are co-prime to both m and n.
- Thus there are Φ(m) Φ(n) elements which are co-prime to mn.
  - This proves the result…

So therefore, we conclude like thus there are phi n columns with phi m elements in each which are co-prime to both m and n and thus there are phi m phi n elements which are co-prime to m n this proves the result

(Refer Slide Time: 58:04)



Further Result

- $\Phi(p^a)=p^a-p^{a-1}$
  - Evident for a=1
  - For a>1, out of the elements 1, 2, …, p^a the elements p, p^2, $p^{a-1}p$ are not co-prime to p^a.

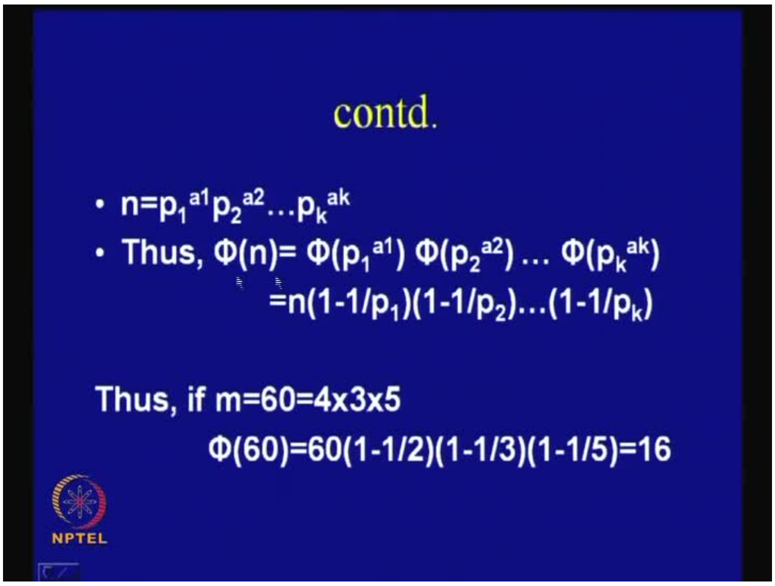
  Rest are co-prime.

  Thus $\Phi(p^a)=p^a-p^{a-1}$

  $=p^a(1-1/p)$

We can actually apply this result and we can obtain some interesting observations like phi p ot the power of a will be equal to p to the power of a minus p to the power of a minus one and these is quite evident for a equal to one but, for a greater than one out of the elements one two p p to the power of a the elements p p square p to the power of a minus one are multiplied with p are not co-prime to p to the power of a the rest will be co-prime therefore, we can obtain like phi p to power of a will be p to the power of a minus p to the power of a minus one and that is actually equal to p power of a into one minus one by p

(Refer Slide Time: 58:40)



contd.

- $n=p_1^{a1}p_2^{a2}\ldots p_k^{ak}$
- Thus, $\Phi(n)= \Phi(p_1^{a1})\ \Phi(p_2^{a2}) \ldots \Phi(p_k^{ak})$

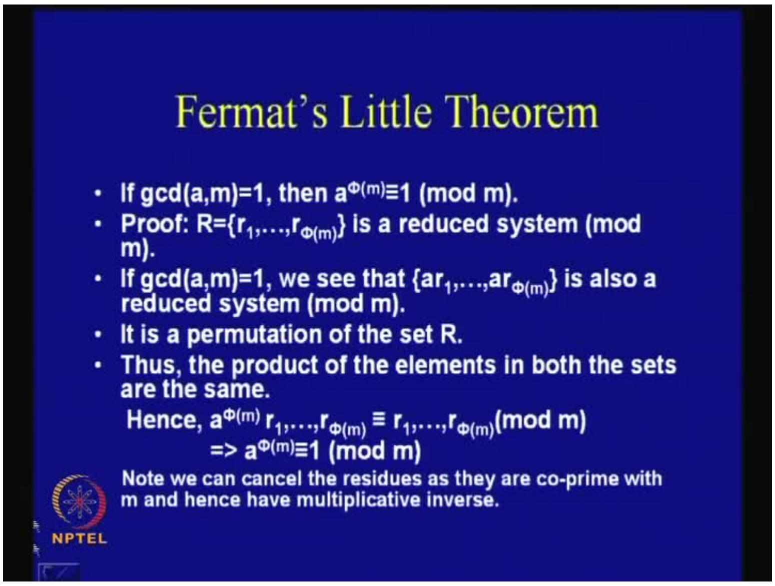
  $=n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k)$

Thus, if m=60=4x3x5

$\Phi(60)=60(1-1/2)(1-1/3)(1-1/5)=16$

We can actually extend this result and apply this like follows and compute the phi of any value in this case we know from the fundamental theory of arithmetic that we can actually take n and obtain phi if we and we can obtain this prime factorizations then it will be easy to compute the value of phi n so that means the if factorization of n is available then computation of phi n can be obtained using this this this formula so for example, if i need to the compute phi of sixty then we can and we know prime factorization of sixty as four multiplied by three multiplied by five and phi of sixty will be sixty into one minus one by two into one minus one by three into one minus one by five so that is this is equal to two square therefore, this is this is straight away application of this result

(Refer Slide Time: 59:31)



Fermat's Little Theorem

- If gcd(a,m)=1, then $a^{\Phi(m)} \equiv 1$ (mod m).
- Proof: R={$r_1,\ldots,r_{\Phi(m)}$} is a reduced system (mod m).
- If gcd(a,m)=1, we see that {$ar_1,\ldots,ar_{\Phi(m)}$} is also a reduced system (mod m).
- It is a permutation of the set R.
- Thus, the product of the elements in both the sets are the same.

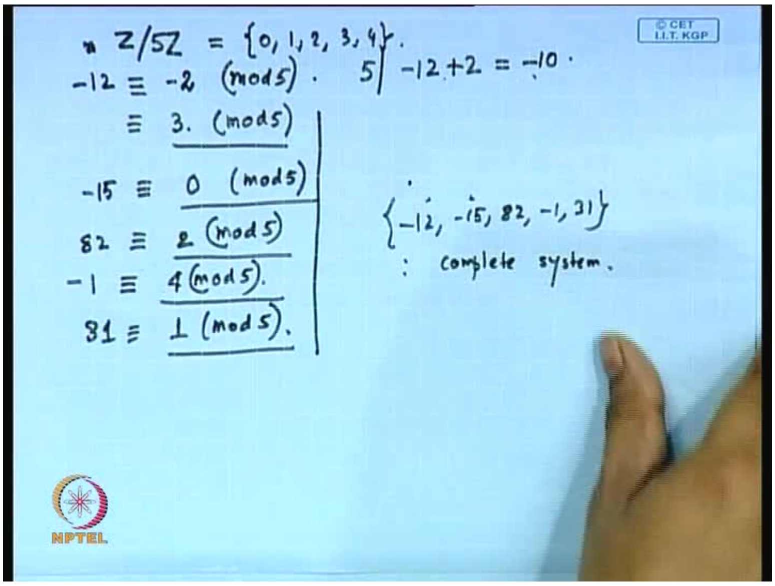
Hence, $a^{\Phi(m)} r_1,\ldots,r_{\Phi(m)} \equiv r_1,\ldots,r_{\Phi(m)}$(mod m)

=> $a^{\Phi(m)} \equiv 1$ (mod m)

Note we can cancel the residues as they are co-prime with m and hence have multiplicative inverse.

So then we see that just let us conclude our todays talk with theorem of fermat which says that it is called fermat’s little theorem and its very useful so it is so you see that if g c d of a coma m is equal to one then a power phi m is actually congruent to one modulo m actually this result is euler’s fermat’s theorem and variation of this is same as fermat’s theorem it says that if in fermat’s little theorem this this m is actually a prime number we know we know that if phi m (( )) is prime then phi of p will be equal to p minus one and therefore, a to the power of p minus one will be congruent to one modulo m so that is fermat’s little theorem but, let us consider the generalized theorem and let us consider a set r which is formed of r one to r phi m we know that there are phi m elements which forms a reduced set modulo m

(Refer Slide Time: 60:51)



$\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}.$

$-12 \equiv -2 \pmod{5}. \quad 5 \mid -12+2 = -10.$

$\equiv 3. \pmod{5}$

$-15 \equiv 0 \pmod{5}$

$82 \equiv 2 \pmod{5}$

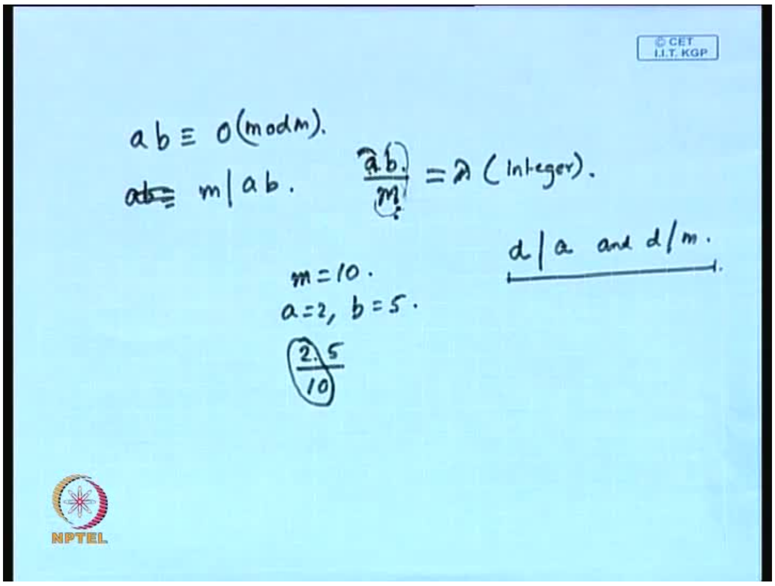
$-1 \equiv 4 \pmod{5}.$

$81 \equiv 1 \pmod{5}.$

$\{-12, -15, 82, -1, 31\}$: complete system.

Now if g c d of a coma m is equal to one we see that a multiplied with r one so we just take this numbers and you multiply each of them with a now this if g c d of a coma m is one then this results also reduced systems modulo m now this is just to be a permutation of the set r so this is we have considered na we have considered one example previously where we have seen that if you’ve taken some numbers and those numbers essentially where nothing but, rearrangement right like if you see that in the previous example of this this this particular set so this particular set was just a rearrangement of the original of the original remainder ok

(Refer Slide Time: 61:00)



$ab \equiv 0 \pmod{m}.$

~~ab≡~~ $m \mid ab. \quad \frac{ab}{m} = \lambda$ (Integer).

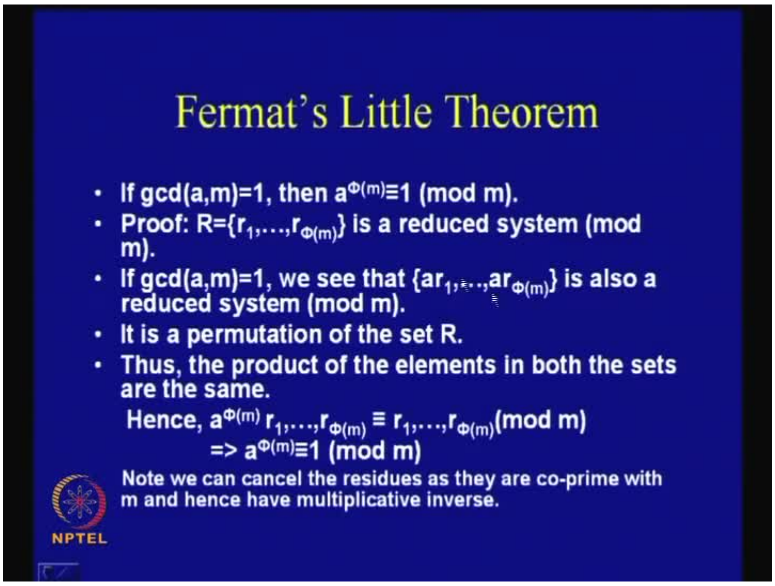
$d \mid a$ and $d \mid m$.

$m = 10.$

$a = 2, \ b = 5.$

$\frac{2.5}{10}$

(Refer Slide Time: 61:02)



Fermat's Little Theorem

- If gcd(a,m)=1, then $a^{\Phi(m)} \equiv 1$ (mod m).
- Proof: R=$\{r_1,\ldots,r_{\Phi(m)}\}$ is a reduced system (mod m).
- If gcd(a,m)=1, we see that $\{ar_1,\ldots,ar_{\Phi(m)}\}$ is also a reduced system (mod m).
- It is a permutation of the set R.
- Thus, the product of the elements in both the sets are the same.

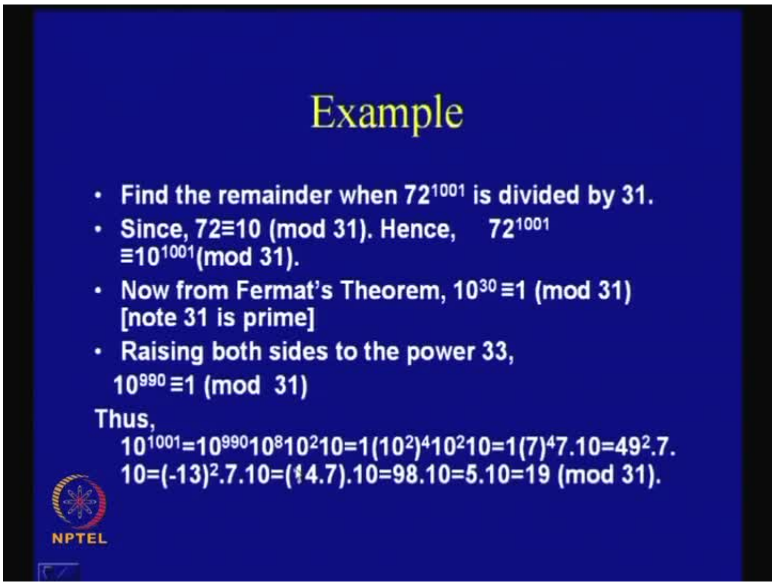
Hence, $a^{\Phi(m)} r_1,\ldots,r_{\Phi(m)} \equiv r_1,\ldots,r_{\Phi(m)}$(mod m)

$\Rightarrow a^{\Phi(m)} \equiv 1$ (mod m)

Note we can cancel the residues as they are co-prime with m and hence have multiplicative inverse.

So therefore, similarly, i mean applying this if you just take this set of remainders and if you multiply them with a number a which is co-prime to m then you obtain another order of the of the remainder now if we just take therefore, therefore, therefore, it is basically the same set of the remainders but, in some other order therefore, the product of these particular elements will of these elements will also be the same so if i just take this numbers and i multiply them this should be the same as the product of these numbers so that means writing them i mean in one this will this will work out to be a to the power of phi m because there are phi m numbers and on the left hand side you'll have r one to r phi m multiplied and the right hand side you'll also have r one to r phi m multiplied now note that since these numbers are actually co-prime with m therefore, they can be cancelled out and therefore, what remains is a power phi m is congruent to one modulo m and that is the euler's fermat's formula

(Refer Slide Time: 61:52)



Example

- Find the remainder when 72^{1001} is divided by 31.
- Since, $72 \equiv 10$ (mod 31). Hence, $72^{1001} \equiv 10^{1001}$(mod 31).
- Now from Fermat's Theorem, $10^{30} \equiv 1$ (mod 31) [note 31 is prime]
- Raising both sides to the power 33,

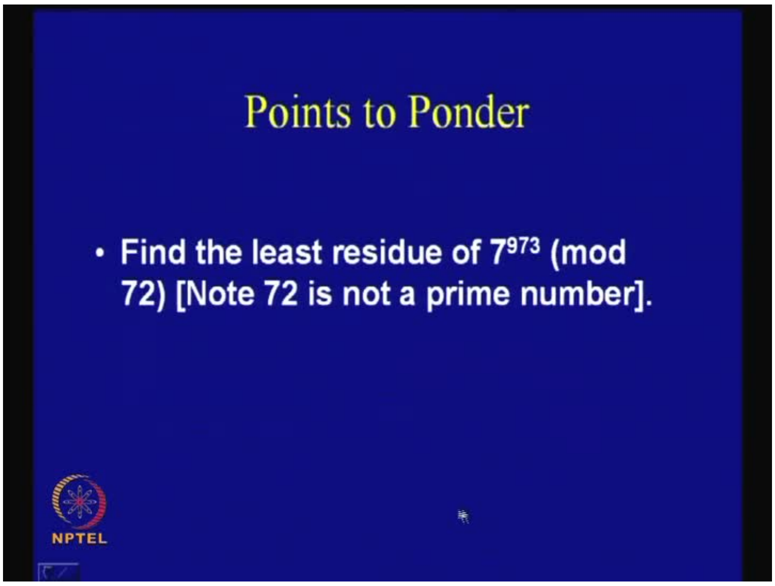
  $10^{990} \equiv 1$ (mod 31)

Thus,

$10^{1001}=10^{990}10^{8}10^{2}10=1(10^{2})^{4}10^{2}10=1(7)^{4}7.10=49^{2}.7.10=(-13)^{2}.7.10=(14.7).10=98.10=5.10=19$ (mod 31).

So example of this can be applied to find out very interesting results like suppose seventy two to the power of one thousand one is divided by thirty one and we need to go argue that so you know that seventy two is nothing but, equal to ten modulo thirty one hence seventy two to the power of one thousand one will be equal to ten to the power of thousand one mod modulo thirty one now if i apply fermat's theorem then since p is a prime number then ten to the power of thirty should be equal to or congruent to one modulo thirty one note that thirty one is prime therefore, raising both sides to the power thirty three will be ten to the power of nine hundred ninety is congruent to one modulo thirty one and therefore, we find that it it is this can be worked out like this ten to the power of thousand one will be ten to the power of nine hundred ninety which is the nearest number and these are the subsequent remaining numbers

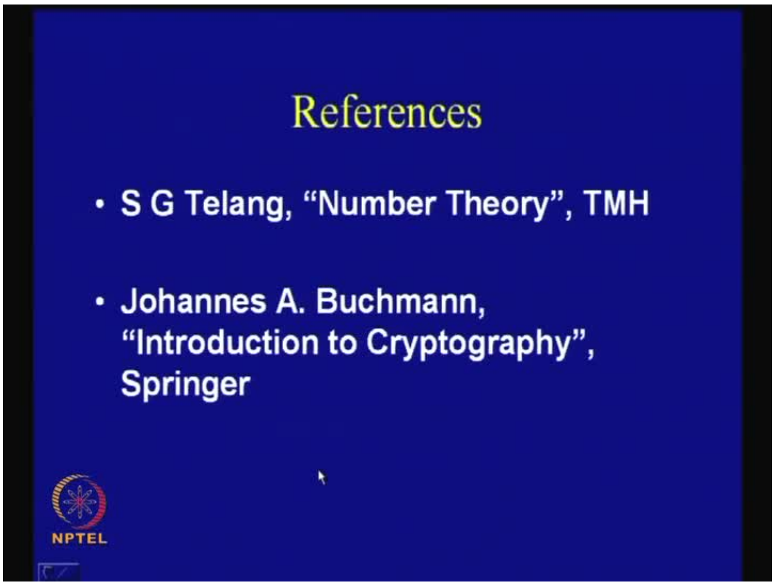
(Refer Slide Time: 62:49)



Points to Ponder

- Find the least residue of 7^{973} (mod 72) [Note 72 is not a prime number].

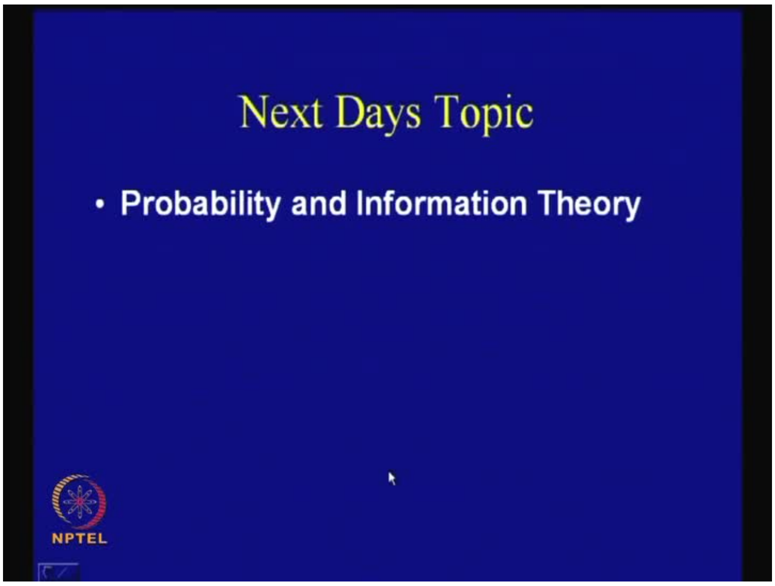
(Refer Slide Time: 62:59)



References

- S G Telang, “Number Theory”, TMH
- Johannes A. Buchmann, “Introduction to Cryptography”, Springer

(Refer Slide Time: 63:07)



Next Days Topic

- Probability and Information Theory

So similar number these small numbers you can reduce quite easily using and apply the previous results to these computations then you can see that this will work out to nineteen modulo thirteen one similarly, you can work out this example take this as an example exercise that is find the least residue of seven to the power of nine seventy three modulo seventy two note seventy two is not a prime number so i conclude here and we have followed these texts from telang and from buchmann for the i man for this part and next day's topic will be probability and information theory