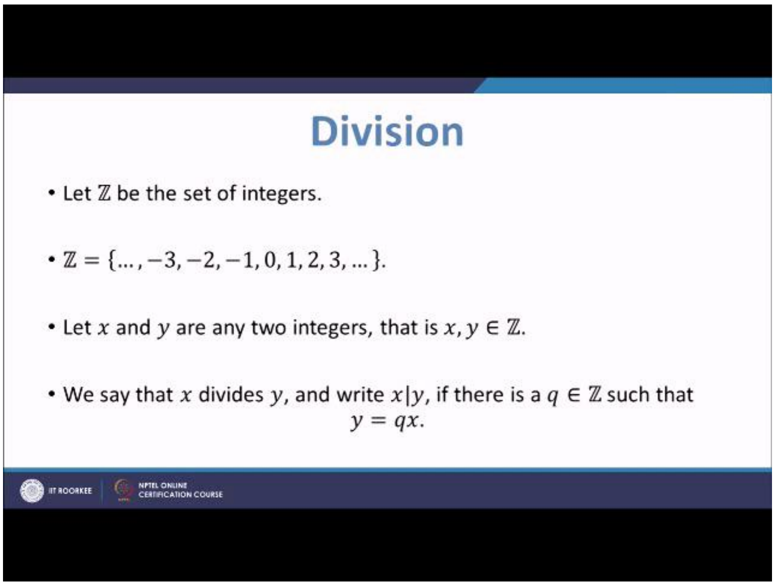
# Introduction to Cryptology
## Dr. Sugatha Gangopadhyay
## Department of Computer Science and Engineering
## Indian Institute of Technology, Roorkee

## Lecture - 02
## Modular arithmetic, shift cipher

Hello. Welcome to our course on Introduction to Cryptology, Lecture 2 of the first week. In this lecture we will study Modular Arithmetic, but before that we study division. We already know what division is, but we will study that again and see some salient points.

(Refer Slide Time: 00:53)



Division

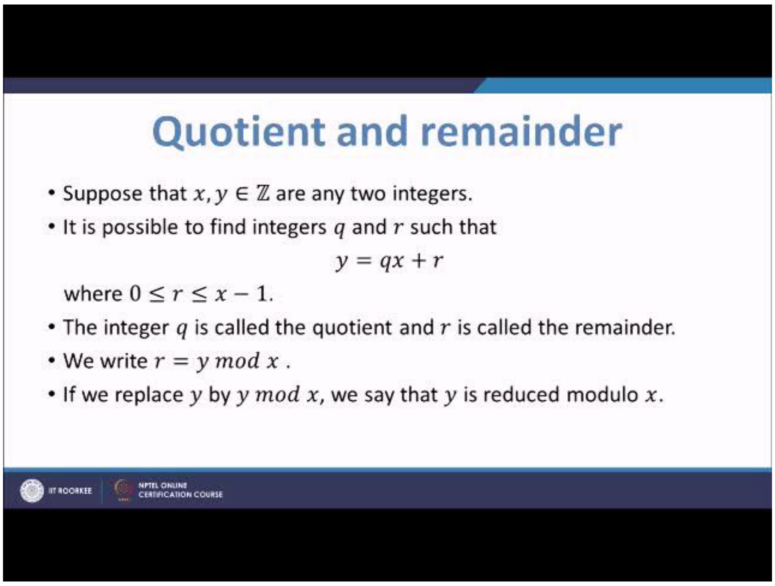
- Let $\mathbb{Z}$ be the set of integers.
- $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- Let $x$ and $y$ are any two integers, that is $x, y \in \mathbb{Z}$.
- We say that $x$ divides $y$, and write $x|y$, if there is a $q \in \mathbb{Z}$ such that $y = qx$.

IIT ROORKEE
NPTEL ONLINE CERTIFICATION COURSE

Our starting point is the set of integers Z which is 0, 1, 2, 3 onward and on the negative side minus 1, minus 2, minus 3 and so on.

Now, let x and y be two integers, that is to say x y belongs to Z then we say that x divides y if there is another integer q such that y is equal to q plus x. I write it here y equal to q plus x, if this happens then we say that x divides y and we write symbolically as x and a vertical line and y.

(Refer Slide Time: 01:55)



## Quotient and remainder

- Suppose that $x, y \in \mathbb{Z}$ are any two integers.
- It is possible to find integers $q$ and $r$ such that

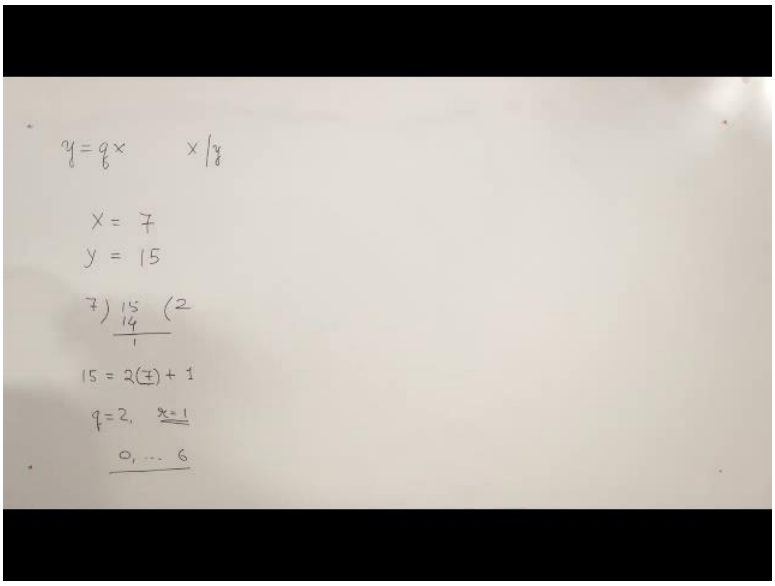
$$y = qx + r$$

where $0 \leq r \leq x - 1$.
- The integer $q$ is called the quotient and $r$ is called the remainder.
- We write $r = y \ mod \ x$ .
- If we replace $y$ by $y \ mod \ x$, we say that $y$ is reduced modulo $x$.

IIT ROORKEE
NPTEL ONLINE CERTIFICATION COURSE

Now let us go one step forward this is quotient and remainder. Suppose, we have two integers x and y belonging to Z, that is a set of integers. Now we know that we can write y equal to q times x plus r that is we know that we can find two integers q and r such that y equal to q x plus r.

(Refer Slide Time: 01:32)



$y = qx \qquad x | y$

$X = 7$

$y = 15$

$$7 \overline{)\ 15\ } (2 \\ \underline{14} \\ 1$$

$15 = 2(\boxed{7}) + 1$

$q = 2, \quad \underline{\underline{r = 1}}$

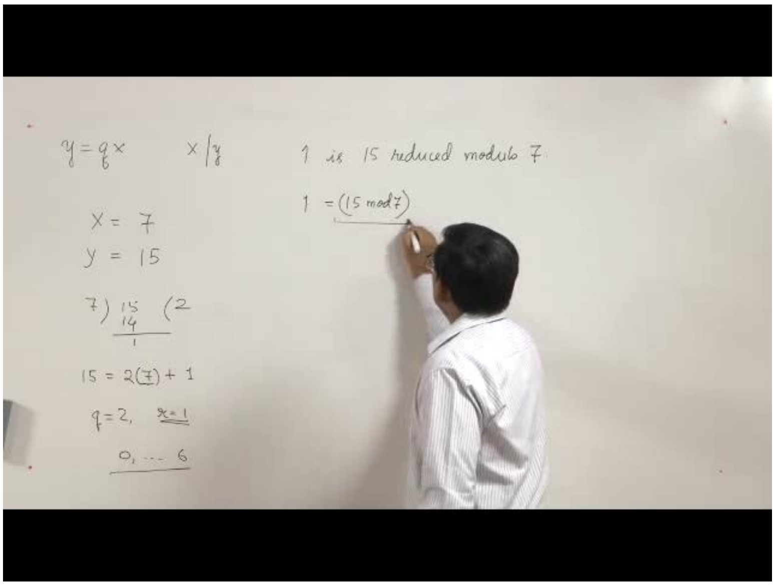
$\underline{0, \ldots 6}$

This is nothing new because we know that suppose we have got x equal to 12 and y equal to let us say 7, I am sorry let us move with the other way around. So, x equal to 7 and let us say y equal to 15, then we know that the usual division goes like this 7 15 and

7x2 are 14 then 1, so I can write 15 equal to 2 times 7 plus 1. In this case my q is 2 and r is equal to 1. We also know that we can always manage q in such a way that r falls between 0 and x minus 1, that is in this case if I fix x then this r is always going to be between 0 and 6, this is not surprising we know this.

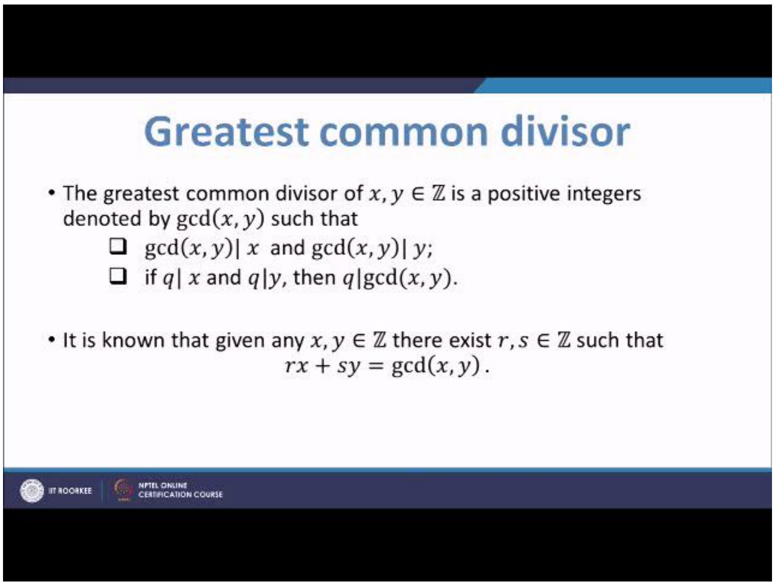
Now, this thing is written as symbols in this way. Now, there is a name for r it is called remainder after division by x. And there is a name for q it is called the quotient and we give another name we say that r is y reduced modulo x.

(Refer Slide Time: 04:34)



So, here in this example let say 1 is 15 reduced modulo 7. If I divide 15 by 7 then the remainder is 1 and I force the remainder to be between 0 and 6. I write this as a symbol 1 is equal to 15 mod 7, this is a single entity 15 mod 7 which I write over here r equal to y mod 7. Now next step, we also know what a greatest common devisor between two integers is.

(Refer Slide Time: 05:40)



## Greatest common divisor

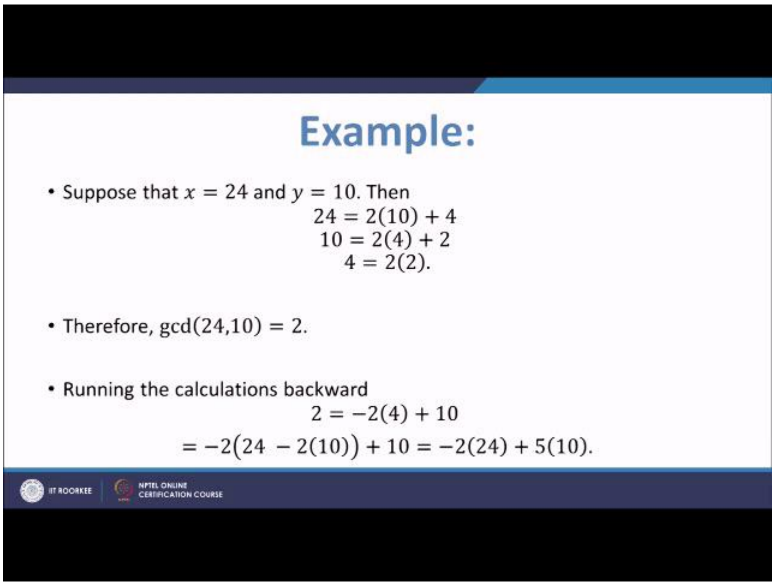
- The greatest common divisor of $x, y \in \mathbb{Z}$ is a positive integers denoted by $\gcd(x, y)$ such that
  - ❑ $\gcd(x, y) | x$ and $\gcd(x, y) | y$;
  - ❑ if $q | x$ and $q | y$, then $q | \gcd(x, y)$.
- It is known that given any $x, y \in \mathbb{Z}$ there exist $r, s \in \mathbb{Z}$ such that
$$rx + sy = \gcd(x, y) .$$

IIT ROORKEE
NPTEL ONLINE CERTIFICATION COURSE

So, suppose we have got two integers x and y greatest common devisor of x and y is written as gcd of x and y and it is a it is a positive integer by definition which divides both x and y, and if we have any other integer dividing both x and y then definitely that integer is going to divide gcd of x and y.

So, let us look at an example. For example let us come here. Suppose x is equal to 24 and y is equal to 10.

(Refer Slide Time: 06:47)



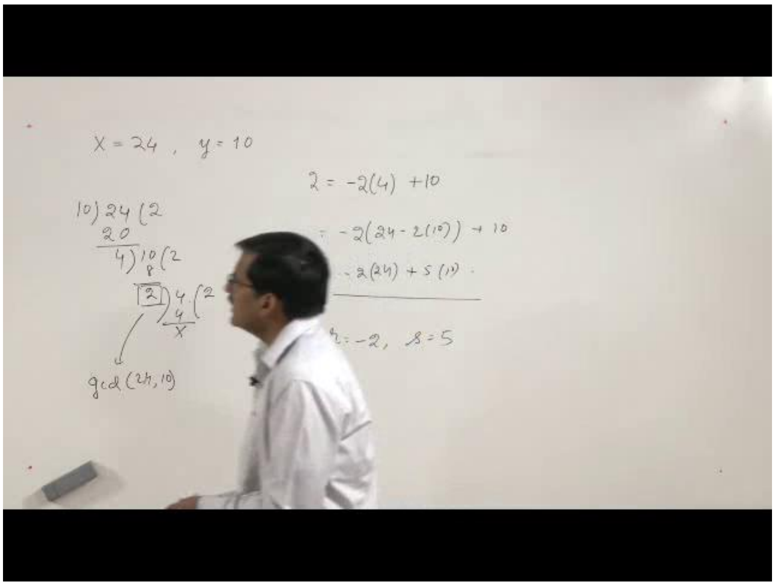
## Example:

- Suppose that $x = 24$ and $y = 10$. Then
$$24 = 2(10) + 4$$
$$10 = 2(4) + 2$$
$$4 = 2(2).$$
- Therefore, $\gcd(24{,}10) = 2$.
- Running the calculations backward
$$2 = -2(4) + 10$$
$$= -2\big(24 \; - 2(10)\big) + 10 = -2(24) + 5(10).$$

IIT ROORKEE
NPTEL ONLINE CERTIFICATION COURSE

Now we would like to find out the greatest common devisor of 24 and 10 for that we will have to start like this, we take 24 and then divide it by 10 first so I am writing here in a different way we will see that this way is easier to handle in some in our contest, but we know that in school arithmetic we do like this.

(Refer Slide Time: 06:22)

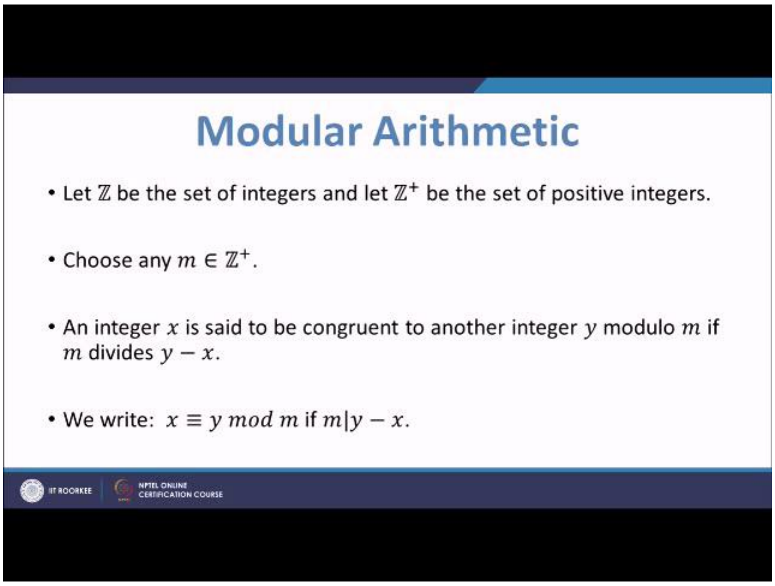


We take y and then we write 24 we divide this so I have got 20 this is 4 and then I take 4 we do this, so I have got 2 this is the remainder. And then we divide 4 by 2, so I will have 2x2 are 4 so I have got nothing, I have got no remainder. So, I come to this step 4 2 divides 4 and we know that this is the greatest common devisor of 24 and 10, so gcd of 24 and 10.

Now there is a surprising fact, we can say something more with greatest common devisors and that is this; if we have two integers x and y then there exist two more integers r and x such that rx plus sy is equal to gcd of x and y. Now we will say how we know that, there is an algorithm for computing r and s and gcd which is called the Extended Euclidean Algorithm we are not going to details about extended Euclidean algorithm, but we will see how to find this coefficients r and s and that is here. So, we have already seen that these steps are true 24 is equal to 2 times 10 plus 4, 10 is equal to 4 times 4 plus 2, 4 is equal to 2 times 2. So, I know that gcd is 2.

Now what about r and s we can run the calculations backward. If we run backward then we get something like this let us see. We have got 2 over there this is 2 we can transpose this term to the other side so we will get something like, this 2 equal to minus 2 times 4 plus 10 and then I can replace 4 by looking at this term. So, 4 equal to 24 minus 2 times 10 and we have got 10 here, so minus 2 4 is equal to 24 minus 2 times 10 plus 10 and this gives me minus 2 times 24 and here it is plus 5 times 10, we come over here. So my r is minus 2 and s is 5 and that is what we set out to find, rx plus sy is equal to the greatest common devisor. This was the background. After this background we come to the topic of today that is called Modular Arithmetic.

(Refer Slide Time: 10:45)

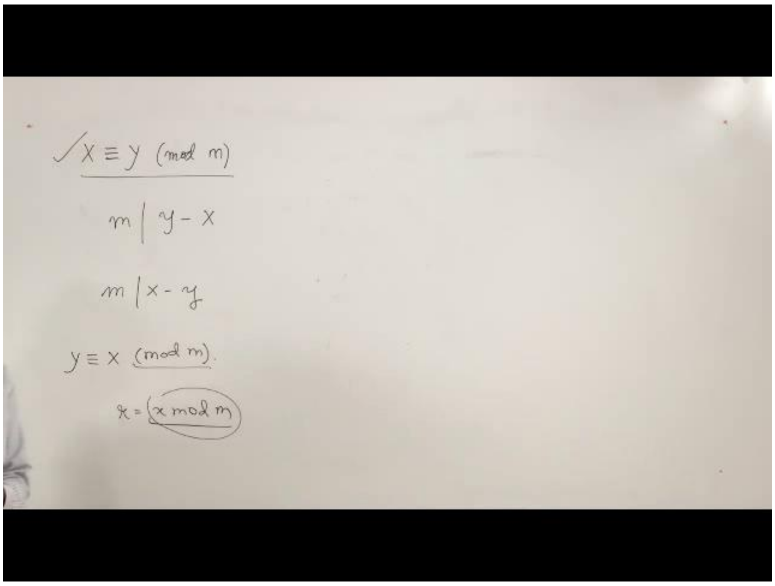


# Modular Arithmetic

- Let $\mathbb{Z}$ be the set of integers and let $\mathbb{Z}^+$ be the set of positive integers.
- Choose any $m \in \mathbb{Z}^+$.
- An integer $x$ is said to be congruent to another integer $y$ modulo $m$ if $m$ divides $y - x$.
- We write: $x \equiv y \bmod m$ if $m | y - x$.

Now, again our starting point is z and we denote the set of positive integers by z superscript plus. Now we choose a positive integer m. Nice we have chosen an m we say that an integer x is congruent to another integer y modulo m if m divides y minus x that is to say in symbols.

(Refer Slide Time: 11:25)



✓ $x \equiv y \pmod{m}$

$m \mid y - x$

$m \mid x - y$

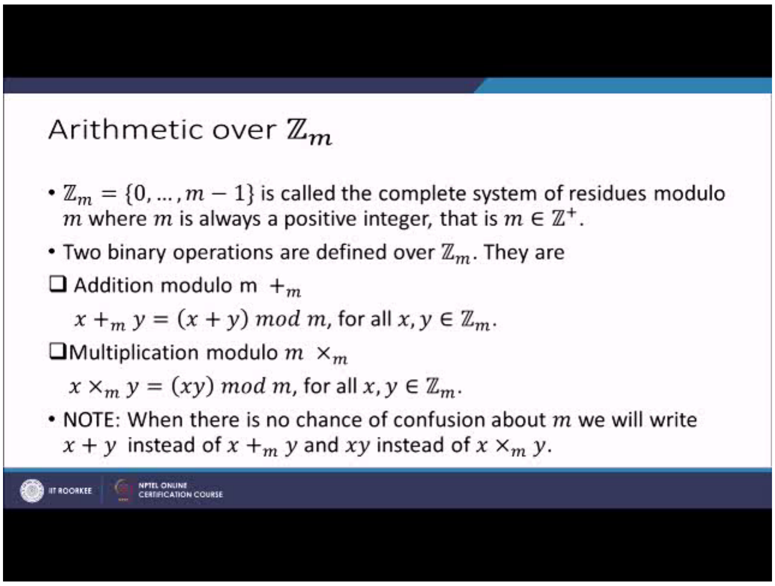
$y \equiv x \pmod{m}$

$r = (x \bmod m)$

I will write x is congruent to y mod m, I will put a bracket here later on and if this happens I write this if m divides y minus x. It is needless to say that if m divides y minus x then m divides x minus y therefore if x is congruent to y modulo m then y is congruent to x modulo m. We will be always writing like this, we will put a bracket over here to which is not written over here but later on we will be careful. Why do we put a bracket here, to distinguish between r equal to x mod m and y congruent to x mod m or x congruent to y mod m.

This means that m divides y minus x, but if I write x mod m that means I am reducing x modulo m that is to say that I am dividing x by m and then taking the remainder.

(Refer Slide Time: 13:17)



## Arithmetic over $\mathbb{Z}_m$

- $\mathbb{Z}_m = \{0, \dots, m-1\}$ is called the complete system of residues modulo $m$ where $m$ is always a positive integer, that is $m \in \mathbb{Z}^+$.
- Two binary operations are defined over $\mathbb{Z}_m$. They are

❑ Addition modulo m $+_m$

$x +_m y = (x + y)\ mod\ m$, for all $x, y \in \mathbb{Z}_m$.

❑ Multiplication modulo $m$ $\times_m$

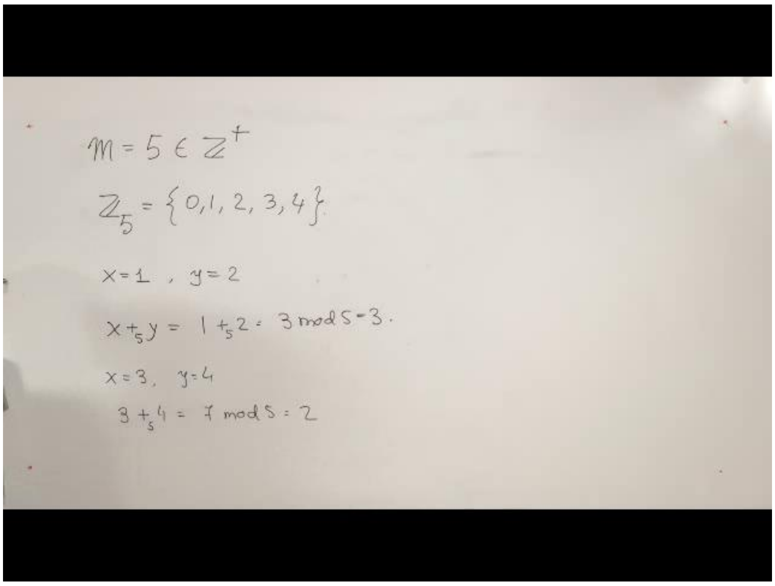
$x \times_m y = (xy)\ mod\ m$, for all $x, y \in \mathbb{Z}_m$.

- NOTE: When there is no chance of confusion about $m$ we will write $x + y$ instead of $x +_m y$ and $xy$ instead of $x \times_m y$.

IIT ROORKEE NPTEL ONLINE CERTIFICATION COURSE

Arithmetic over z m; now what is z m, you give an m it can be anything, it can be 2 3 5 4 whatever I can always construct a set of 0 to m minus 1, so if you give me 5 I will construct the set 0 to 4. So, let me write it an example.

(Refer Slide Time: 13:45)



$m = 5 \in \mathbb{Z}^+$

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$x = 1$ , $y = 2$

$x +_5 y = 1 +_5 2 = 3 \bmod 5 = 3$.

$x = 3$, $y = 4$

$3 +_5 4 = 7 \bmod 5 = 2$

So, if you give m equal to 5, 5 is of course a positive integer then I can always write z subscript 5 which is 0, 1, 2, 3 and 4. And now I define an addition. So, what I do is I take any two integers in z m, in this case it might be z 5 so something between these two 0, 1, 2, 3, 4, and once I do that I will add them as a integers and then reduce modulo m.

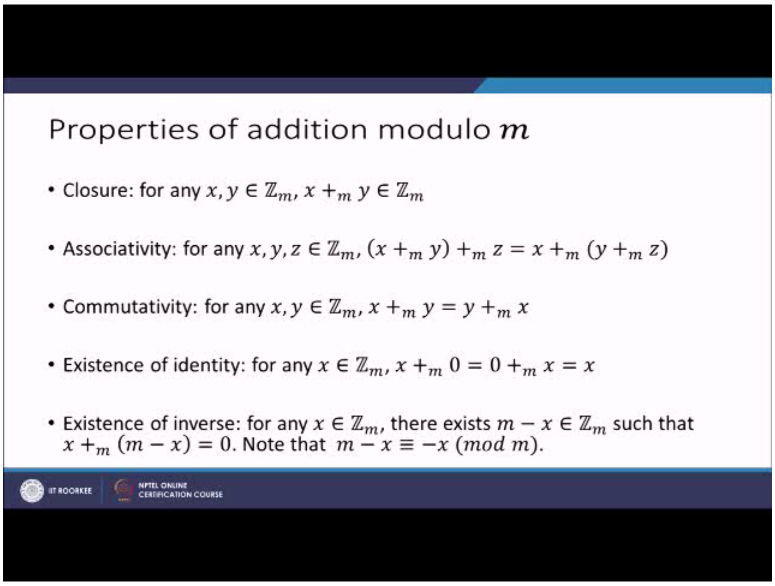
So that is exactly what I am doing over here. I am taking x and here this sum it is different, so I am writing a plus I am tagging it by m, so once I tag it by m I see that I can basically write x plus subscript y then I can write equal to x plus y mod m, I now know what is x plus y mod m just take the addition divide by m take the remainder. Once I do this I call this result sum modulo m or addition modulo m.

I can do exactly the same thing with multiplication. I am now considering elements in z m I am taking x multiplication modulo m y which is simply ordinary multiplication then you reduce it modulo m, so you are pushing it back to z sum m that is exactly what we are doing here. And we have to note something more, that if we have no confusion about m and when we are doing lot of calculations then we are not going to write that subscript we are just going to write plus instead of plus subscript m and we will write nothing in place of multiplication modulo m will just write x y that is what we are going to do.

So, as an example let us look at this. Suppose my x is 1 and y is 2 then what is x modulo 5 y this is 1 modulo 5 2 when this is 3 reduced mod 5, but that is 3. We see that this is a case where x addition modulo 5 y that is same as x usual addition y. Sometimes modular addition and is going to give me the same result as the usual addition but of course sometimes not, we can easily find out a scenario like that. I mean for example, if I take 3 plus 4 it is going to give a pretty large number. So if I take x equal to 3 and y equal to 4 then I am going to get 3 plus modulo 5 4 which is by definition 7 mod 5 and which is equal to 2, because if I divide 7 by 5 the remainder is 2.

Now there are several properties of modular addition and modular multiplication. We will list these properties, we have to know these properties and we can check these properties on our own with small numbers. So, let us see what properties are there. We can always check that if we have two numbers inside z m that is it mean 0 and m minus 1 the sum the modularation, modulo m is of course going to be inside z sub m.

(Refer Slide Time: 18:25)



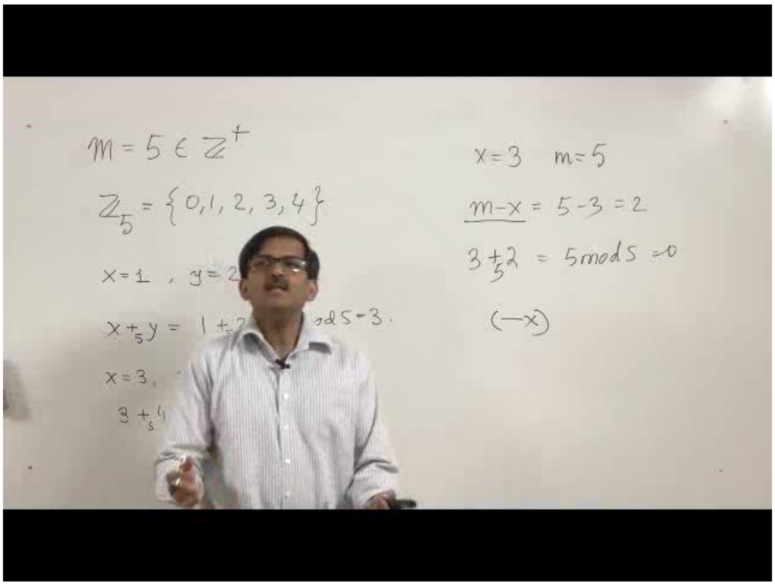
## Properties of addition modulo $m$

- Closure: for any $x, y \in \mathbb{Z}_m$, $x +_m y \in \mathbb{Z}_m$
- Associativity: for any $x, y, z \in \mathbb{Z}_m$, $(x +_m y) +_m z = x +_m (y +_m z)$
- Commutativity: for any $x, y \in \mathbb{Z}_m$, $x +_m y = y +_m x$
- Existence of identity: for any $x \in \mathbb{Z}_m$, $x +_m 0 = 0 +_m x = x$
- Existence of inverse: for any $x \in \mathbb{Z}_m$, there exists $m - x \in \mathbb{Z}_m$ such that $x +_m (m - x) = 0$. Note that $m - x \equiv -x \ (mod\ m)$.

And then we have something called Associativity, that is x plus y plus z is going to be x plus y plus z. And then we have commutativity, that is x and y in z m. So, x addition modulo m of y is going to be y addition modulo m of x these are very easy consequences or these are easy properties basically. At the end there are two interesting properties; one is extremely easy because we say that we will always have 0 because we will always have this one. So if I add any x to 0 or 0 to x modulo m I am going to get x.

And the last one, that if you give me an x I can find out or I can compute m minus x and then if I add them this is going to be 0 modulo m; why is very natural. So let us take an example over here.

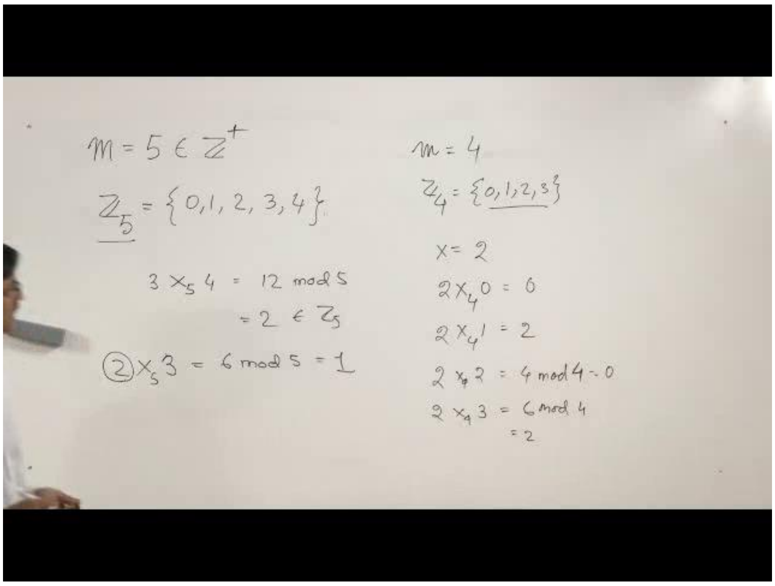
(Refer Slide Time: 19:47)



So, well let us take 3. If you give me 3, suppose my x is 3 now and the modulus is 5, so I compute m minus x which is equal to 5 minus 3 which is 2 now see if I add 3 modulo 5 2 I get 5 mod 5 and if I divide 5 by 5 the remainder is 0 so I am going to get 0. This particular quantity m minus x is called the additive inverse of x modulo m. Sometimes we write in just minus x without thinking much, understanding that at minus x has to be put inside z m.

We now come to the properties of multiplication modulo m. Now, again the multiplication modulo m is closed that is to say if I take two integers x and y in z m, if I product the modulo m of course I am going to get another integer between 0 and m minus 1 that is not difficult to see we can we can check that over here.

(Refer Slide Time: 21:25)



$m = 5 \in \mathbb{Z}^+$

$\underline{\mathbb{Z}_5} = \{0, 1, 2, 3, 4\}$

$3 \times_5 4 = 12 \bmod 5$

$= 2 \in \mathbb{Z}_5$

$\textcircled{2} \times_5 3 = 6 \bmod 5 = 1$

$m = 4$

$\mathbb{Z}_4 = \{\underline{0, 1, 2}, 3\}$

$x = 2$

$2 \times_4 0 = 0$

$2 \times_4 1 = 2$

$2 \times_4 2 = 4 \bmod 4 = 0$

$2 \times_4 3 = 6 \bmod 4$

$= 2$

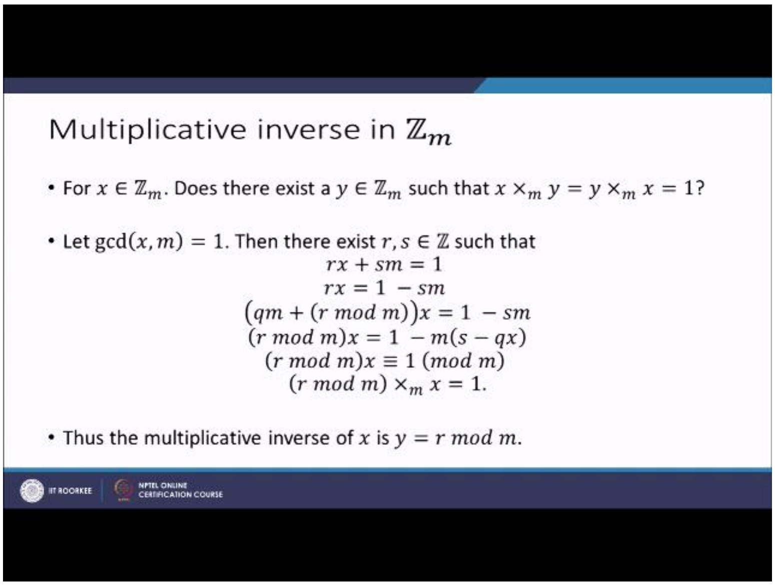
If you have let us take 3 and 4 so I will get 3 multiplication modulo 5 4 this is 12 and of course this is reduced mod, well what 5 and so it is 2 it is of course inside. I made a mistake; I know I did not make any mistake over here. So, it of course 2 and of course this is inside z sub 5. And then associativity, commutativity, existence of identity, so let us looks here.

So, associativity is of course x times y times z is equal to x times y times z.; Commutativity we know is x modulo multiplication modulo m y is going to y multiplication modulo x and here is going to be 1 over here. This 1 works as a identity in the sense that if you multiply 1 modulo x, if you multiply 1 and x with multiplication modulo m we are going to get x and the other way around. And lastly we have a property which connects addition and multiplication modulo m which is this that is x addition modulo m y, multiplication modulo m z is going to be x multiplication modulo z plus modulo m plus and then we have got y multiplication modulo z and is other way around.

Finally, we come to this question that how do we compute multiplicative inverse in z m. First of all what is a multiplicative inverse. We might have certain numbers in z m, let us look at this z 5 for example, I have got 2 and if I multiply modulo 5 3 I will get 6 if mod 5 6 1, what does it mean? It means that when we are given a number in z mod z 5 I have got another number 3 such that their product is going be 1.

But this is not always true. Let us consider where the modulus is 4, so z sub 4 is 0, 1, 2, 3, and now let us take x as 2. Now we can multiply 2 by all the other integers here so 2 modulo 4 0 is of course 0, then 2 multiplication modulo 4 1 is 1, 2 multiplication modulo 2 now this is 4 4 mod 4 is going to give me 0, and 2 multiplication mod 4 3 this is going to be 6 which is mod if we do mod 4, I made a mistake over here this is going to be 2 and this is going to be 6 mod 4 that is going to be 2 again.

(Refer Slide Time: 25:29)



Multiplicative inverse in $\mathbb{Z}_m$

- For $x \in \mathbb{Z}_m$. Does there exist a $y \in \mathbb{Z}_m$ such that $x \times_m y = y \times_m x = 1$?
- Let $\gcd(x, m) = 1$. Then there exist $r, s \in \mathbb{Z}$ such that

$$\begin{gathered} rx + sm = 1 \\ rx = 1 - sm \\ (qm + (r \bmod m))x = 1 - sm \\ (r \bmod m)x = 1 - m(s - qx) \\ (r \bmod m)x \equiv 1 \pmod{m} \\ (r \bmod m) \times_m x = 1. \end{gathered}$$

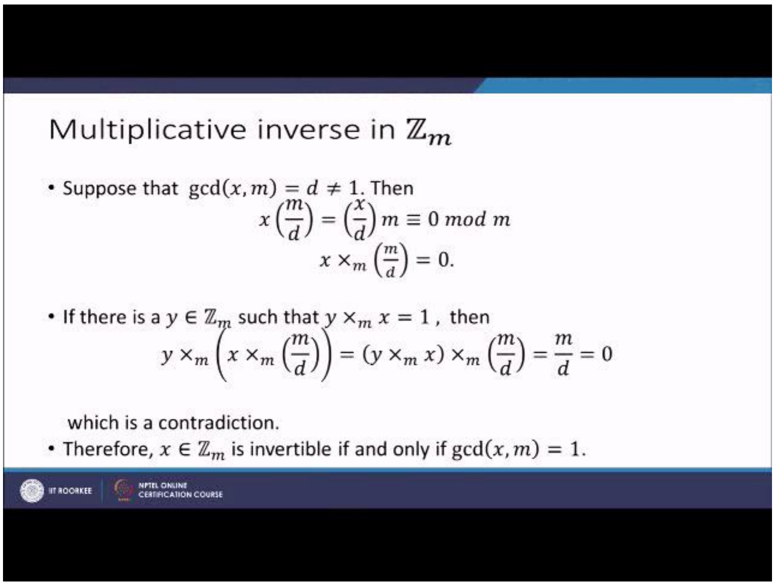
- Thus the multiplicative inverse of $x$ is $y = r \bmod m$.

So, always we do not have always we do not have inverses, but sometimes we have inverses. Now our question is that when do we have an inverse. Suppose, the greatest common devisor of x and m is equal to 1, there exist r and s belonging to z such that r x plus s m is equal to 1.

This is something that we have seen with the greatest common devisor because 1 is the greatest common devisor of x. And m and if you have that we can write r x equal to 1 minus s m, and therefore what I can do is that I can reduce r modulo m so I get q m plus r mod m into x equal to 1 minus s m and then I can take x times q m over here on the other side so I will ultimately have r mod m x plus 1 is equal to 1 minus m s minus q x. And therefore, if I reduce modulo m I will get r mod m times x is congruent to 1 mod m.

So I can say here that r mod m multiplication modulo m of x is going to be 1, not only that where r times x plus s times y is equal to 1 which is g, sorry it is not y it is s times m is equal to 1 where 1 is a gcd of x and m. So one thing is clear here that if the gcd of x and m is 1 then you will get another integer in z m such that, that integer let us say y times x is going to give you 1.

(Refer Slide Time: 28:14)



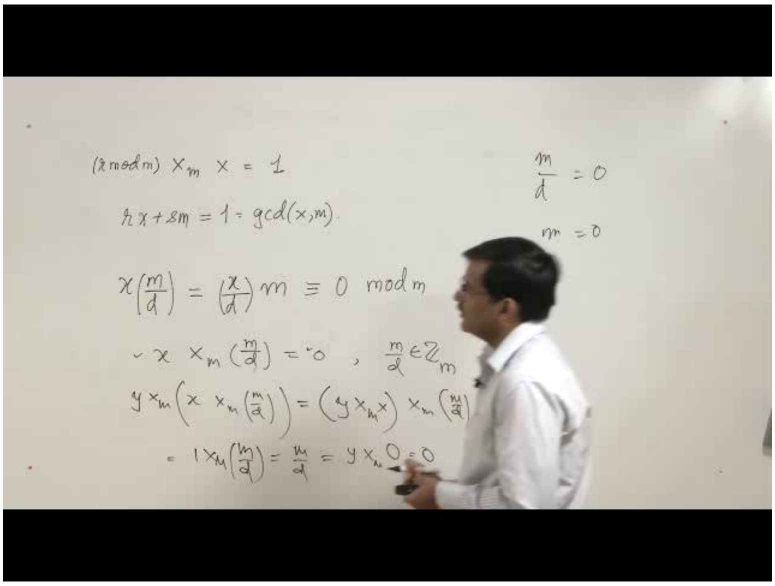
## Multiplicative inverse in $\mathbb{Z}_m$

- Suppose that $\gcd(x, m) = d \neq 1$. Then
$$x\left(\frac{m}{d}\right) = \left(\frac{x}{d}\right)m \equiv 0 \; mod \; m$$
$$x \times_m \left(\frac{m}{d}\right) = 0.$$
- If there is a $y \in \mathbb{Z}_m$ such that $y \times_m x = 1$, then
$$y \times_m \left(x \times_m \left(\frac{m}{d}\right)\right) = (y \times_m x) \times_m \left(\frac{m}{d}\right) = \frac{m}{d} = 0$$

  which is a contradiction.
- Therefore, $x \in \mathbb{Z}_m$ is invertible if and only if $\gcd(x, m) = 1$.

On the other hand if you have an integer x inside z m with gcd to m is not one that is d something that is greater than 1 then, we have a sequence of argument like this I have got x times m by d.

(Refer Slide Time: 26:58)

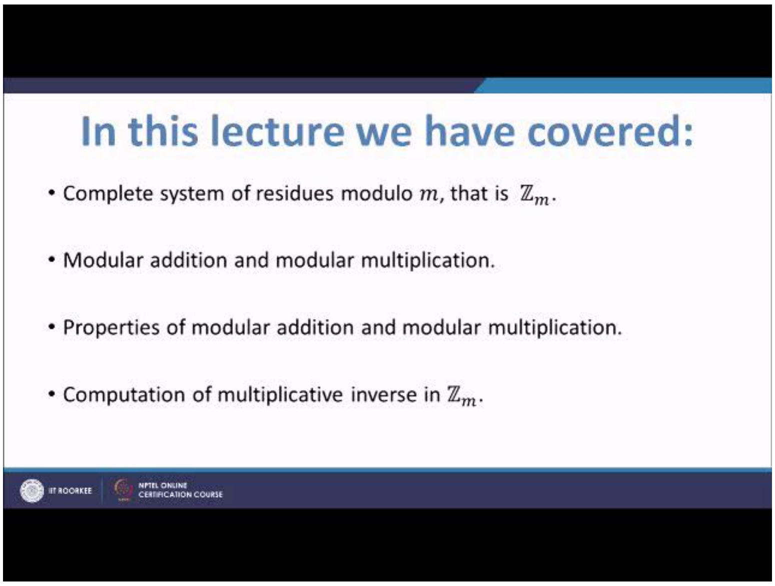


$$(r \bmod m) \times_m x = 1$$
$$rx + sm = 1 = \gcd(x,m)$$
$$x\left(\frac{m}{d}\right) = \left(\frac{x}{d}\right)m \equiv 0 \mod m$$
$$x \times_m \left(\frac{m}{d}\right) = 0 \quad , \quad \frac{m}{d} \in \mathbb{Z}_m$$
$$y \times_m \left(x \times_m \left(\frac{m}{d}\right)\right) = (y \times_m x) \times_m \left(\frac{m}{d}\right)$$
$$= 1 \times_m \left(\frac{m}{d}\right) = \frac{m}{d} = y \times_m 0 = 0$$
$$\frac{m}{d} = 0$$
$$m = 0$$

So what I am doing here, is that I have got x times m by d I know that d is the gcd so d divides m it is an integer, this is equal to x by d times m and I know that this is an integer because d divides x also because d is a gcd and this is congruent to 0 mod m. Therefore, we can say that x wait a minute m by d is equal to 0, where m by d is inside z sub m. And now suppose if possible x has an inverse, that means suppose there is an integer inside z m such that y mod multiplication modulo m x is 1 then I can multiply this equation both sides by y, so I get something like this y multiplication mod m into x multiplication mod m m by d and here I can use the associative law of modular multiplication so I will write something like this.

That is exactly what I have written over here, but this is nothing but 1 multiplication modulo m m by d, well this is equal to m by d. So I have started from here I can always do this, but you know this is equal to y multiplication mod m of 0 which is 0. This force is m by d to be equal to 0, but this is possible only if m equal to 0. So, the calculation steps are over here. If I multiply both sides by y then one use of associative law gives me m by d equal to 0 and which is a contradiction. Therefore, I come to the conclusion that an element x inside z sub m is invertible that is it has another elements as that the product multiplication module m is 1 if and only if the greatest common devisor of that element with m is 1.

(Refer Slide Time: 31:44)



## In this lecture we have covered:

- Complete system of residues modulo $m$, that is $\mathbb{Z}_m$.
- Modular addition and modular multiplication.
- Properties of modular addition and modular multiplication.
- Computation of multiplicative inverse in $\mathbb{Z}_m$.

IIT ROORKEE
NPTEL ONLINE CERTIFICATION COURSE

So, we stop here. In this lecture we have covered something called complete system of residues modulo m which is essentially z m that we have been dealing with. Modular addition and modular multiplication, properties of modular addition and modular multiplication and, probably most importantly the computation of multiplicative inverse in z sub m.

So that is all for today, see you in the next lecture.