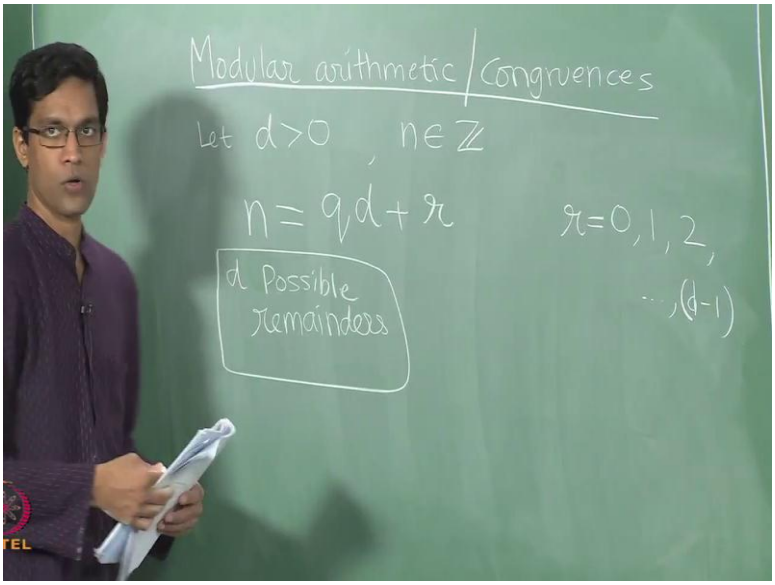
An Invitation to Mathematics
Prof. Sankaran Viswanath
Institute of Mathematical Sciences, Chennai

Unit
Number theory
Lecture - 34
Congruence's, Modular arithmetic

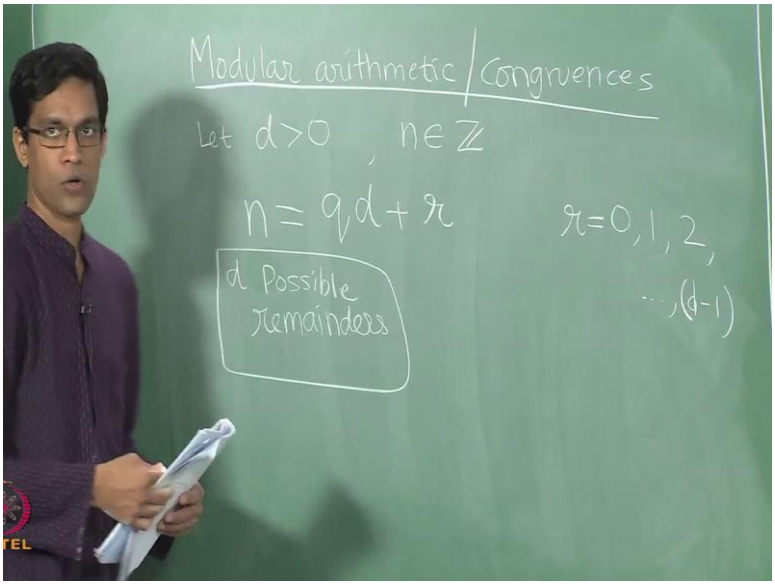
Now, we will talk about Modular arithmetic or the equivalent notion of Congruence's. So, this goes back to reminder that we obtain on division. So, division on reminder recall was the following.

(Refer Slide Time: 00:31)



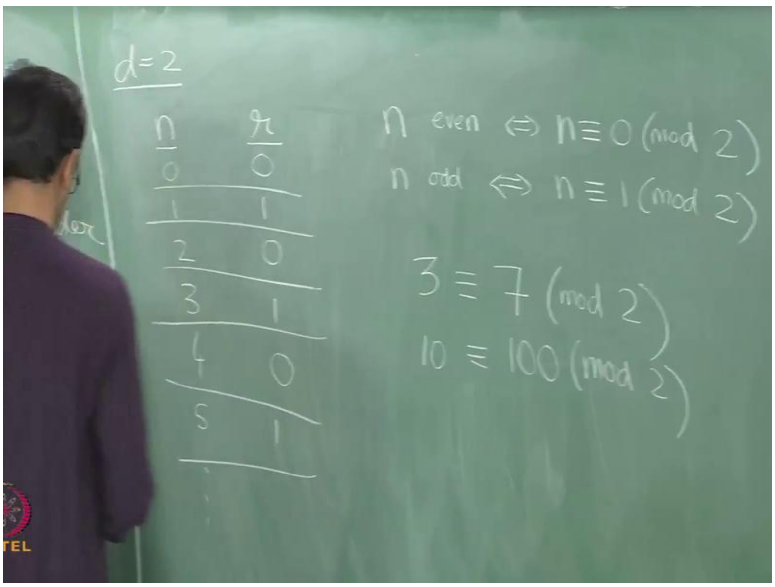
If you had a number d, a natural number d and you had any integer n, then we could divide n by d to produce a quotient and a reminder. And the reminder had the following property or the following requirement; that it is a number between 0 and d minus 1. So, the reminder can be 0, 1, 2, 3 all the way till d minus 1. So, these are the possible values of the reminder, so that there are d different reminders possible. So, observe that the reminders, the number of possible reminders are d, so possible reminders are d in number. So, now, here is a notion, we say the two numbers are congruent modulo d.

(Refer Slide Time: 01:38)



So, we say that, we say the two integers n and m are congruent modulo d, if they leave the same reminder on division by d. So, if they have the same reminder on division by d and thus a notation for this, it is again very useful. So, the notation if m and n are congruent modulo d, we would write this as m is this three lines here and we read this as m is congruent to n mod d, so that is how we denote this relation of being congruent.

(Refer Slide Time: 02:56)



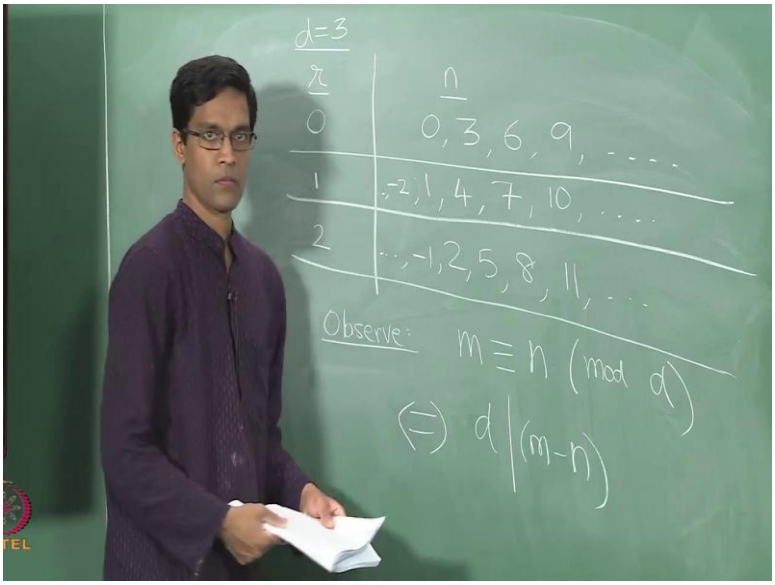
So, let us just do examples, if you take d equals 2, so what does division with reminder, when you divide by 2 mean, you can either get a reminder 0 or a reminder of 1. So, what are the varies numbers, if I have a number n, let me tabulate the reminders that I get on division by 2. So, if I have 0, 1, 2, 3, 4, 5 and so on, I could also write them out for the negatives.

So, observe that if I have an even numbers 0, 2, 4, 6, and so on, when I divide those numbers by 2, of course, they leave a reminder of 0. So, these guys would give me a reminder of 0 on division by 2, because they all even numbers, whereas the odd numbers, when I divide by 2 would give me a reminder of 1. So, roundly 2 possible reminders and if I sort of collect together all numbers which give me a reminder of 0; that gives me the evens and the 1's with reminder 1 give me the odds.

So, observe that if, so n is even would mean the following, if only if n is congruent to 0 mod 2, so remember, what is this mean that, if I divide n by 2, the reminder I get is the same as what I get when I divide 0 by 2. So, when I divide the number 0 by 2, of course it leaves reminder 0. Similarly, the odd numbers of the property that they give you a reminder of 1, when I divide by 2 and another way of expressing it is as follows, n is odd is the same thing as seeing; that n is congruent to 1 mod 2.

So, the reminders are odd or reminders are 1 and that also other things, you can also express relationships among numbers. For instants, 3 and 7 are congruent to each other modulo 2; that is just saying that the reminders are the same, when you divide both of them by 2. This case the reminder is a 1, similarly 10 is congruent to 100 if you wish modulo 2, because both give you a reminder 0 and so on, you can sort of see how this concept works by working out many examples.

(Refer Slide Time: 05:27)



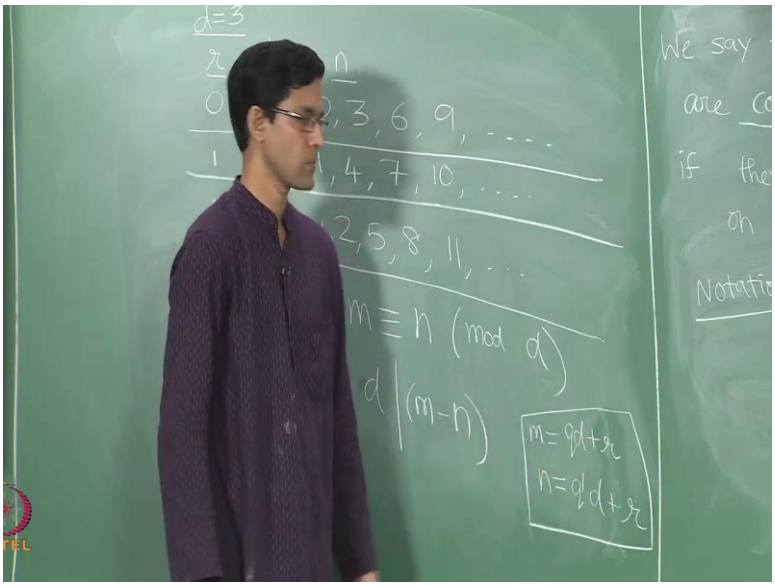
And look at the possible reminders and now we will write out all the values of n. So, the reminders are in this case, when I divide a number by 3, I can either get 0, 1 or 2 as reminders. And let us now, let us do a table little differently, let me now write down all values of n, which would give me a reminder 0 on division by 3, of course that just mean that n is a multiple of 3. So, what numbers would give me 0, when I divide by 3, it is just the 0, 3, 6, 9 and so on; that is the list.

Now, similarly if I want a reminder of 1 on division by 3, then well here are those numbers, if I take 1, 4, 7, 10 and so on similarly I could do things on the negative side as well. So, here for instants the preceding number is minus 2, and so on, all these numbers observe, when you divide them by 3, give you reminder 1. Similarly, here I have 2, 5, 8 or 11 and so on.

And observe thus a very easy way of getting these guys, so once you know one of them which is a 1 here, you just get there as by adding multiples of 3, so I add 3, I get 4, I add 3 again I add 3, subtract 3, and so on. So, all these numbers just differs from each other by multiples of 3. So, observe, sort of an easy observation here, if m and n are congruent to each other mod d, in other words they both give you the same reminder. Here, is an alternate way of saying this, this is same thing as saying that d divides their difference.

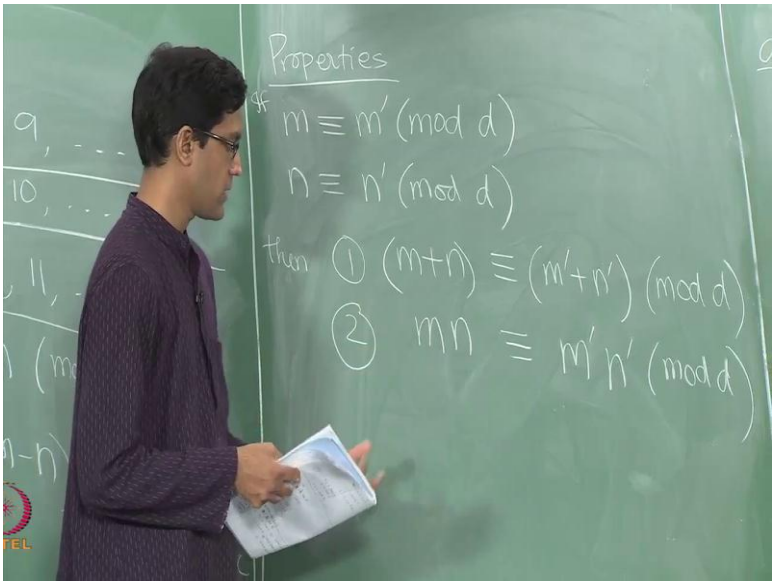
So, we already seeing it by example in this case, if I take any two numbers which give me the same reminder. So, I take any two numbers for instants in the second row here, they both give me reminder 1, their difference is always a multiple of 3. So, the difference very much is going to be divisible by d and it is very easy to see, why this is true.

(Refer Slide Time: 07:50)



So, let me just briefly sketch the proof and leave it for you to complete formally, let say m gives you some reminder, m is so I write it out as q d plus r, where r is a reminder when m is divided by d. Similarly, if n is divided by d, I get let say some other quotient q prime, but the reminder is the same; that is what being congruent means. So, here is what I have and now, observe if I subtract m minus n, the reminders will just cancel each other. So, the r cancels the r and what is left is just the multiply of d; so that is the sketch of the proof, why the two numbers are congruent to each other the differences is divisible by d.

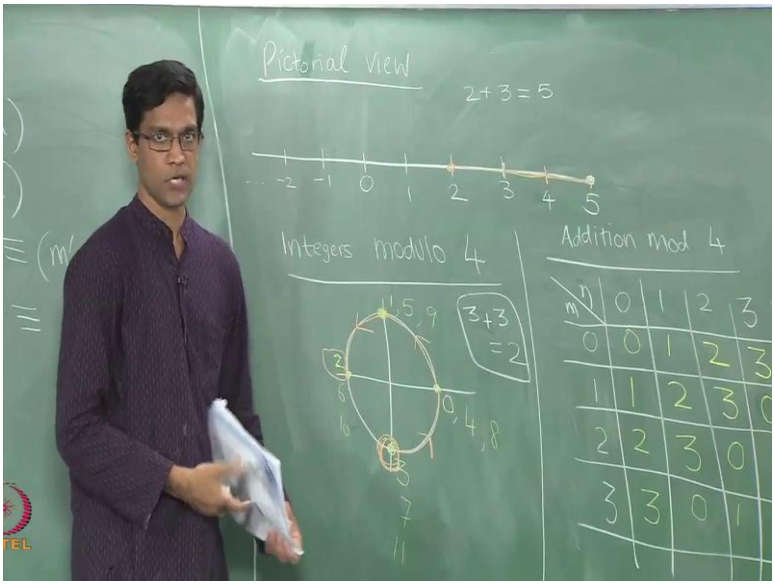
(Refer Slide Time: 08:37)



And there are lots of other interesting properties of congruence's, especially let me just single out of few of them, specifically related to addition and multiplication. So, if m is congruent to m prime mod d and let us say n is congruent to n prime mod d. Then, here is what I can say, the sum of these two numbers m and n is congruent to the sum of the other two numbers m prime and n prime. And so the congruence's with respect addition is one way of stating this.

Similarly, I can also put minus there if you wish or multiplication, if I multiply m and n, it is again going to be congruent to m prime and n prime. So, these are very easy to prove and I leave them as exercises for you, but they have very you know they really useful they have very interesting consequences, they also make computations with congruence's very, very simple. So, for that reason this addition and multiplication properties are extremely important.

(Refer Slide Time: 10:03)



So, this whole discuss of congruence's has this rather. So, here is a pictorial point of view or how one should think in terms of pictures and one thinks of congruence's modulo d and so on. So, observe that one possible pictorial representation of the set of integers is just has points on the number line. So, this is one of our standard picture when we think about integers, we just drawn number line and mark of things at equal intervals and you think of integers as being represented by this.

So, one nice thing here is, this picture also tells you how to do addition for instance. So, if you wanted to add 2 and 3 is sort of only using this picture, here what you do, you would start with one of the two numbers. Let say you start with 2 and you go three steps from there, so 2 plus 3 gives you the number 5 pictorially becomes the following, you start at say 2 and then you take three steps.

So, three steps would mean 1, 2, 3 and where you land is exactly the answer, so 3, 4, 5. So, that is going to be what you get, when you add 2 with 3. So, addition really represents moving along those many steps starting with, let say one of the two numbers. Now, similarly we want to think of integers modulo d, for instance. So, let me do it again by an example, let me look at integers modulo 4, so I will take d equals 4, just as an example, we just makes a picture here.

So, how should want really thing of this ways, you should thing of them as being points on a circle. So, when I say integers modulo 4, what is it mean, when a divide a number by 4, I can either get reminder 0, 1, 2 or 3. So, there are four possible reminders. So, I will thing of it as being four points equally spaced on the circle. So, here for instance in side that have four points, they just kind occupy the four axis.

So, think of this as the number 0 on the circle, this is the number 1; that is a number 2, this the number 3, and now what happens for the life keep going thing of the next number, which is the 4. But, what I am doing here is only keeping track of reminders that I get, when I divide integers by 4. So, and I take the number 4, well 4 when divided by 4 gives me reminder 0. So, I should really thing of 4 as again being the same point. So, this is really also represents 4, if you wish.

And then again one more step, I go to 5, but I do not think a 5 as 5, but only as what I get when I divided by 4, what is the reminder obtain when I divide 5 by 4, well that is a 1. So, I should real thing of 5 has sitting here, similarly I should of thing 6 has sitting here, 7 has sitting here, 8 has sitting here and so on 9, 10, 11 and so on and so forth. So, should really thing of the set up all integers has somehow having being the wrapped around the circle in this fashion.

So, when you keep going round and round, you still get all the integers except that main of the integers occupy the same spot. So, that is really how you want to think of integers, when you go modulo something. Now, the nice thing with this is you can actually just like I talk about how addition has a nice interpretation in terms of the picture, you can also thing of addition modulo 4 are multiplication modulo 4.

So, what does addition modulo 4 mean? So, let us do this once draw the table for addition modulo 4. So, what is it mean to draw the table, well I will draw, so let me thing of two numbers m and n, 4, so that is the table. Now, m and n are integers, but I only keep track of things modulo 4, which means I only worry about a reminders. So, let me say m is numbers between 0 and 4, 0 and 3 and can take values 0, 1, 2, 3.

And now I want to add them, except when I write the answers down, I will only write

down the reminders that the answers give. For instance, so let us do one of the, let us do the first row from instance, if I add 0, 0 plus 0 is of courses 0, 0 plus 1 is 1, 0 plus 2 is 2, 0 plus 3 is 3. Similarly, I add 1 to everything, 1 plus 0 is 1, 1 plus 1 is 2, 1 plus 2 is 3 and now, 1 plus 3 which suppose to be a 4.

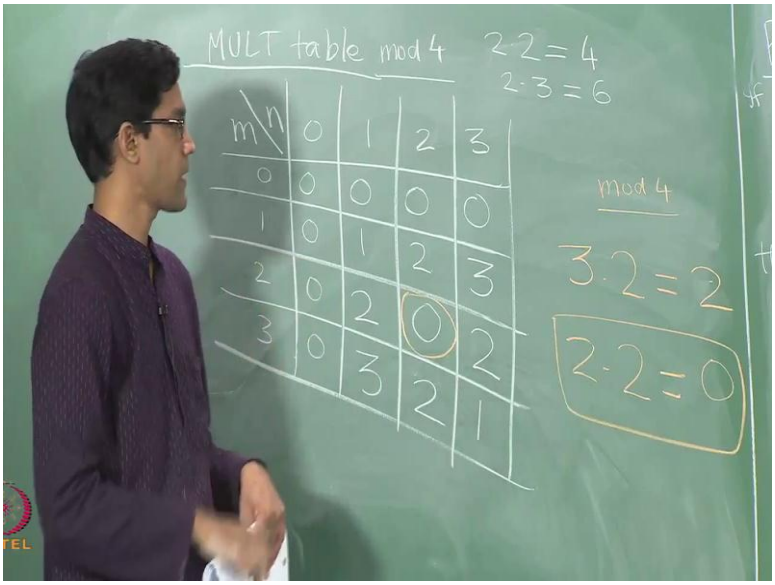
So, if I where sort of just doing regular integers, I would think of that as the 4, because I am adding 1 and 3, but now I am doing things modulo 4, which means I only look at the reminder that I get. So, this answer 4, when I divided by 4, it gives me a reminder 0. So, this guy should really be as. So, similarly if I add 2 plus 0 is 2, 2 plus 1 is 3, 2 plus 2 should be a 4 morally, but a 4 is really as a 0, because that is the reminder, similarly 2 plus 3 is 5, but 5, when divided by 4 gives me reminder 1.

So, similarly this is 3, 0, 1 and 2. So, this is what the addition table modulo 4 means and observe that in fact this has the exact same interpretation has the interpretation for addition that we talk about on the number line. So, for instance, let me pick on something here a 3 plus 3 was 2, according to this, so 3 plus 3 is a two. So, this is modulo 4, so that is the equation, 3 plus 3 is actually a 2.

Now, let see what; that means, so let start on the circles. So, what a we supports to do we started 3; that is a starting point and then we go three steps and wherever we land up is the answers. So, here is the starting point, now going three steps has to be d1 on the circle, so I go one step, two steps and three steps. So, I traverses three steps along the circle and when I do that well I land up exactly a 2.

So, when as I 3 plus 3 is 2, what it means as I need to the really traverse may distances on the circle rather than thing of it as distances traverse on the straight line. So, that is really the addition table, and similarly one can do a multiplication table, you can right out a products of numbers and only worry about, what the reminders are.

(Refer Slide Time: 17:28)



So, similarly let us do the multiplication table here. So, I will write out these numbers and n as before, case a 0 time 0 is 0, well 0 time any things is a 0's. So, that is easy. So, all 0's similarly anything times is 0 is a 0. Now, let us to 1 times 1 is 1, 1 times 2 is 2, 1 times 3 is 3. Similarly, two times each of these guys 2 times 1 is 2 2 times 2, so what is 2 times 2, well morally it is a 4, but a 4 as we just set modulo 4.

So, I am doing this multiplication table mod 4, 4 when I look at the reminder, it gives on division by 4; that is a 0 again. So, that is the 0 and 2 into 3 should really be a 6, but 6 when I divide by 4 gives me reminder 2. So, here it is somewhat funnier, it is 0 2, 0 2 those of the 4 numbers and similarly, if a multiply 3 by each of these, 3 into 1 is 3, 3 into two is 6, but 6 is really a two modulo 4 and 3 into 3 is 9 and 9 modulo 4 is 1.

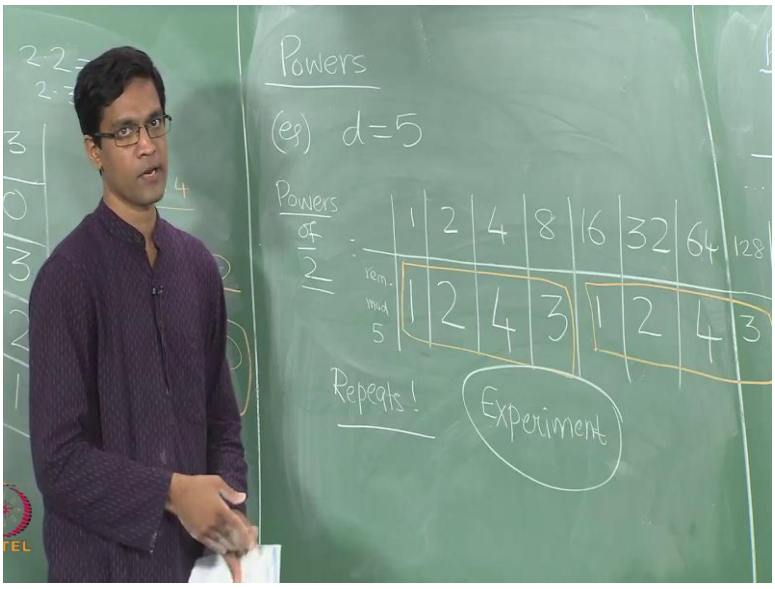
So, here some multiplication table modulo 4, if you wish and in of course, if you just literately write it out, it seen somewhat funny into give you funny answers. So, for instance 3 into 2 is 2, so we get things to at this 3 into 2 is actually at 2, but remember this is all modulo 4, we are not writing out you know things for just a regular integers, but here thus already something very interesting to sort of. Observe, what happened write here we had these two numbers 2 and 2, we multiplied them together and what we actually got this is 0.

So, this already a very new and interesting phenomenon that is, work out of this new arithmetic. So, this way of do in things is what is called a modular arithmetic, it is like regular arithmetic, in the sense, we do addition multiplication, but the rules for addition multiplication are more rules on the circle, rather than rules on the straight line. So, here for instance if we multiply 2 with itself the answer is a 0, why is this very counter in tutor well we are already is used to thinking of numbers as having the following property.

So, if for instance this where the number x, so some real number, this is the non-zero number, so 2 is of course not 0, it is a non-zero number, but when you multiply it with self, it gives you a 0. So, observe the also when we now look at things to like this back in the talk to about the matrices, if you have the 2 cross 2 matrix a, it was perfectly possible for a to be non-zero, but a times a to give you the 0 matrix.

In case, one non-zero things can have square 0 here is again another somewhat different examples in the contacts of modular arithmetic where something squares to 0, but the thing itself is non-zero. So, some strange things tend a happen in this business and so one loss thing which is the again related to multiplication is powers.

(Refer Slide Time: 21:09)



So, what do you mean by this, we could take for instance d to the 5 and let us to the following, let us write out all powers of 2, you keep rising 2 to higher and higher powers and what you study, well you study the reminder that you get, when you go modulo 5. So, what I am going to do is the follow and I am go to write out all powers of 1, 2, 4, 8, 16, 32, 64 and so on.

So, I write those down and below what I do is, I write out the reminders, when I go modulo 5. So, this is now when to the reminders modulo 5 are a division by 5. So, 1 when divided by 5 gives me reminder 1, 2 when divided by 5 gives me reminder 2, 4 gives me a 4, constancy, 8 when divided by 5, well 8 is 5 plus 3, so gives me reminder 3 and so I have 1, 2, 4 and 3. Now, let us do the next 16, when divided by 5, 16 is one more than 15, 15 is a multiply 5.

So, it is a 1, 32 is well reminder 2, 64 is a reminder 4 and let see, what is the next one 128 is reminder 3 again and so on. So, if we keep continuing in this, this what you will find that a just keep repeating like this, 1, 2, 4, 3, 1, 2, 4, 3, and so on. So, repeat in the block of. So, this repeats, now this is a very go thing to try out one self. So, try doing the same thing for other choices of d and for other furthers.

So, instead of 2, you know even for d equals 5, try is same thing with the d equals 3 and are with this number instead of 2 things of it as 3 and 4 and so on in similarly changes this number d and see, what happens. So, and all instances you will always see that it repeats after at certain a block size, but it interesting to study you know when does it repeats what is the what is the size of this block that repeats in each case.

So, I am going to leave this without saying to much more be on this, there are theorems, such as what called Fermat's little theorem and so on, which are relevant in this contacts, but for now I would say, this is quite right thing for experimentation. So, experiment with various choices of d and for and with various numbers here and try and make your own conclusions on what seems to be happened.

What are the reminders, when do they repeat in a with what perceptional size, you get and how do things change, if d is say a prime numbers, say 5 or 7 or 11 would behave in

a certain way as suppose to numbers which are not prime. So, considered those two cases and experiments to this and see what you get.