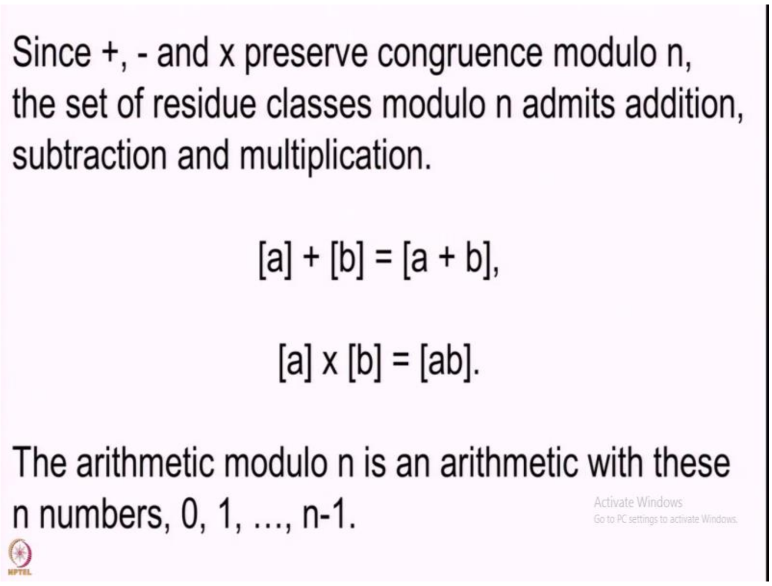
**A basic Course in Number Theory**
**Professor Shripad Garge**
**Department of Mathematics**
**Indian Institute of Technology Bombay**
**Lecture no, 11**
**Arithmetic modulo n, theory and examples**

Welcome back, we are talking about arithmetic in this set of residue classes modulo any given interior n, a natural number n. And we saw that this arithmetic means that we can add two classes that we give us a class. We can multiply two classes that will again give us a class residue class modulo n. In the last lecture towards the end I made some noise about these operations being well defined. So, why it is so much important?

(Refer Slide Time: 1:02)



Since +, - and x preserve congruence modulo n, the set of residue classes modulo n admits addition, subtraction and multiplication.

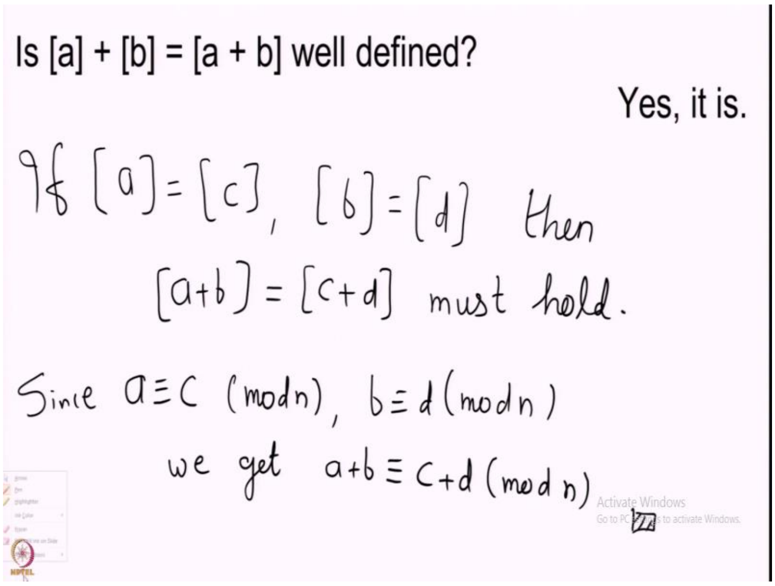
$$[a] + [b] = [a + b],$$

$$[a] \times [b] = [ab].$$

The arithmetic modulo n is an arithmetic with these n numbers, 0, 1, ..., n-1.

Let us go and see what we have done in the end. That whenever we have congruence modulo n, addition subtraction and product is going to preserve the congruence. And therefore I said that we have addition as well as subtraction and multiplication on the set of residue classes. And indeed in the last lecture I asked and answered this question that this addition and multiplication is a well-defined operation. So, what does one mean by this? So, let us go through these two operations one by one. And to really understand the concept of well definedness properly we will also see an example of an operation where the well definedness does not hold.

(Refer Slide Time: 1:54)



Is [a] + [b] = [a + b] well defined?

Yes, it is.

If $[a] = [c]$, $[b] = [d]$ then

$[a+b] = [c+d]$ must hold.

Since $a \equiv c \pmod{n}$, $b \equiv d \pmod{n}$

we get $a+b \equiv c+d \pmod{n}$

So, let us go to the very first property we have, we are asking whether this addition is it well defined? Answer is that yes, it is. But how do we check this. So, what it means is that if you have the class of a to be equal to class of c and the class of b is equal to class of d. If these two hold, then we must have that the class of a plus b is the same as the class of c plus d. Because, you know I told you that I may look at the class of a as given by the element a and the class of b as given by the element b.

We are defining the summation of these two classes and we are picking up one single element from the class. As we saw in the last lecture that the class really has infinitely many elements. So, we have infinitely many choices. And if we are taking two classes then we have doubly infinitely many choices which is again just a number of infinite number of choices.

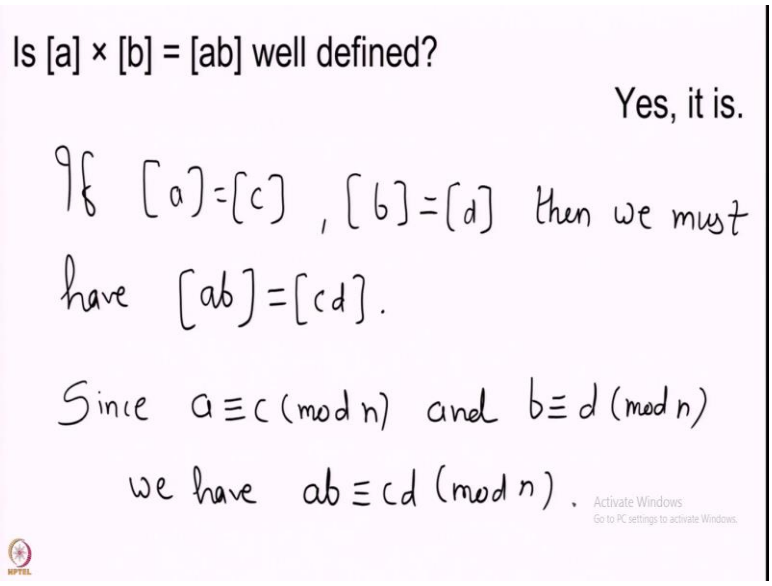
And then we say that the sum of these two classes is the class of a plus b. So, here we are making a choice. We are choosing the element A from the class a and we are choosing the element b. Take the sum and then take the corresponding class. So, to make sure that this is well defined or that it does not depend on the choices that we have made; we have to ensure that if someone else chooses a different element in the class.

So, if class a is class c, then the other person may actually choose the element to be c. And if class b is class d, then the other element may, other person may choose the element d. And then the summation for the other person will be the class of c plus d. For me it is a plus b and its class for the other person may be the class of c plus d. And to have the mathematics well-defined, to have no confusion at all these two classes; the class of a plus b and the class of c plus d should be the same.

Only then we say that the addition makes sense. Only then do we say that the addition is well-defined. It does not depend on the person, does not depend on the place. We are taking addition, the date, time, etcetera. So, how do we ensure that this holds so first of all because class a is class c we have that a is congruent to c mod n. This is something which is given to us.

And we have that b is congruent to d mod n. But then we have seen that whenever a is congruent to c mod n, b is congruent to d mod n, we get A plus B is congruent to c plus d mod n. That is all that we needed to check. Because a plus c mod n, and c plus d mod n, are same and that means that these two classes happen to be the same class. So, the addition is well defined.

(Refer Slide Time: 5:42)



Is $[a] \times [b] = [ab]$ well defined?

Yes, it is.

If $[a]=[c]$, $[b]=[d]$ then we must have $[ab]=[cd]$.

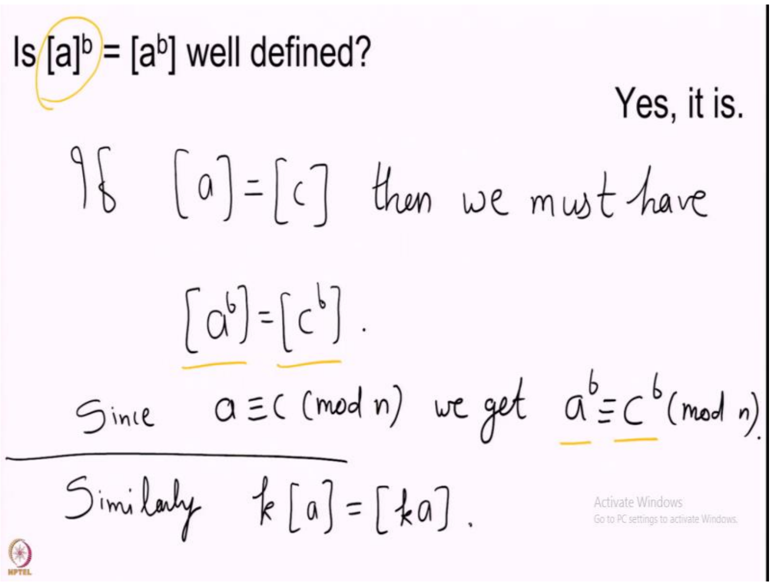
Since $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$ we have $ab \equiv cd \pmod{n}$.

Let us go over to the next slide to check whether the multiplication is well defined. So, indeed multiplication is also well-defined and for that we need to check the same thing. So, if the class of a is the class of c, the class of b is the class of d then we must have class ab to be equal to the class cd. This is what we should have to have the product to be well-defined. Because once again someone may say that c is my element in the first class, which is the class of a, and d is my element in the class of b.

And then for that person the multiplication will be the multiplication of c and d, and then taking its class. And to have these two multiplications to give you the same class we should have that ab and cd give you the same class. But this is again a simple checking. So, since a is congruent to c mod n and b is congruent to d mod n we do have that ab is congruent to cd mod n. This was also one of the initial problems which I had given you and I had also invited you to think about.

And since we have the ab and cd congruent to each other mod n, we have that these two classes are indeed the same. So, we have that the addition is well-defined. We have that the product is well-defined. Once you have product you can take powers, so we can talk about power of an element in the set of residue classes. So we have the, we will start with one residue class and we define the power of that class. So, our definition is as follows.

(Refer Slide Time: 8:10)



Is $[a]^b = [a^b]$ well defined?

Yes, it is.

If $[a]=[c]$ then we must have

$[a^b]=[c^b]$.

Since $a \equiv c \pmod{n}$ we get $a^b \equiv c^b \pmod{n}$.

Similarly $k[a]=[ka]$.

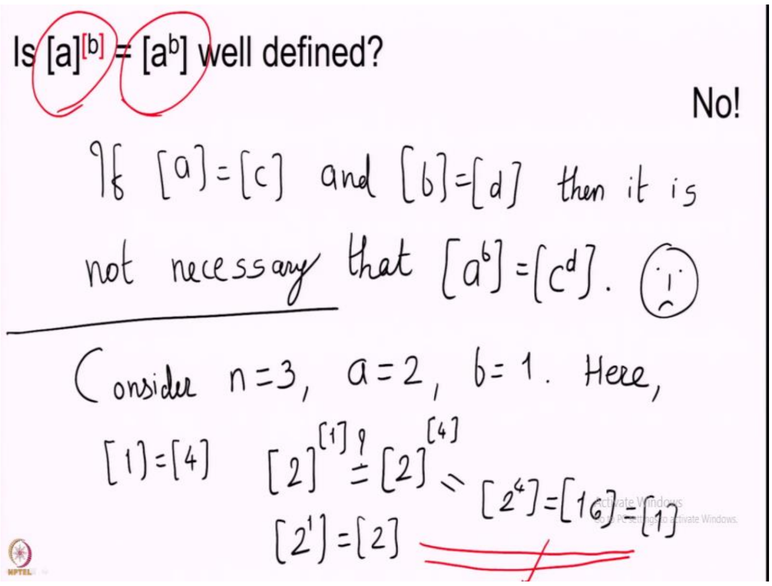
We start, so left hand side we have a residue class and we are taking a power of that, which should again be a residue class because we want to have arithmetic within the set of residue classes. To have an arithmetic does not mean that you are allowed to go out. So, here we want to give the definition of the power of the residue class A and we say that this, our definition is that this is same as the class of a power b. Is this well-defined? So, of course, here we have to check something very simple.

We need to check that if the class a is the class c, then we must have the class of a power b to be equal to the class of c power b. This is all that we need to check. And is this true? So, this is clearly true. So, since a is congruent to c mod n, I will consider this congruence ab many times take the product of left hand side elements which are all aaa.

The product taken b times, so I get a power b and the element on the right side of the congruence is ccc, b times taking the product will give you c power b. So, we get a power b is congruent to c power b mod n. And this is all that we wanted because once we have a power b congruent to c power b mod n we get that these two classes are the same. So, just like from multiplication we went to power similarly from addition we can go to taking multiples.

But that is a very basic case of the multiplications. So, let me just write it here for you. Similarly, k times the class of a is the class of ka. So, these were the 3 or if you consider the last operation we had 4 operations which are well defined on the set of residue classes. Now, I want to give you an example of a operation which is not well-defined. So, here the operation is given.

(Refer Slide Time: 11:10)



Is $[a]^{[b]} = [a^b]$ well defined?

No!

If $[a]=[c]$ and $[b]=[d]$ then it is not necessary that $[a^b]=[c^d]$. ☹

Consider $n=3$, $a=2$, $b=1$. Here,

$[1]=[4]$ $\quad [2]^{[1]} \overset{?}{=} [2]^{[4]} = [2^4]=[16]=[1]$

$[2^1]=[2]$ $\neq$

We want to define power of a residue class by another residue class. We want to define power of the class a by the class b so look at that. The b in the slides has the square brackets given in red to tell you that we are looking at the power of a residue class by another residue class. This is what we are doing. And we have no choice but to define it in this way because this is the most natural way to define it. Or let us say that our example is that if we define it in this way.

The class of a power class of b to be equal to class of a power b, then this operation or this definition that we are giving is not well-defined. It does not make sense. So, why does it not make sense? Let us look at why this does not hold? So, what I am saying is that if you have a class of some element a to be equal to the class of an element c and the class of b is the class of d. Then it is not necessary that the class of a power b is equal to the class of c power d. This is really the problem.

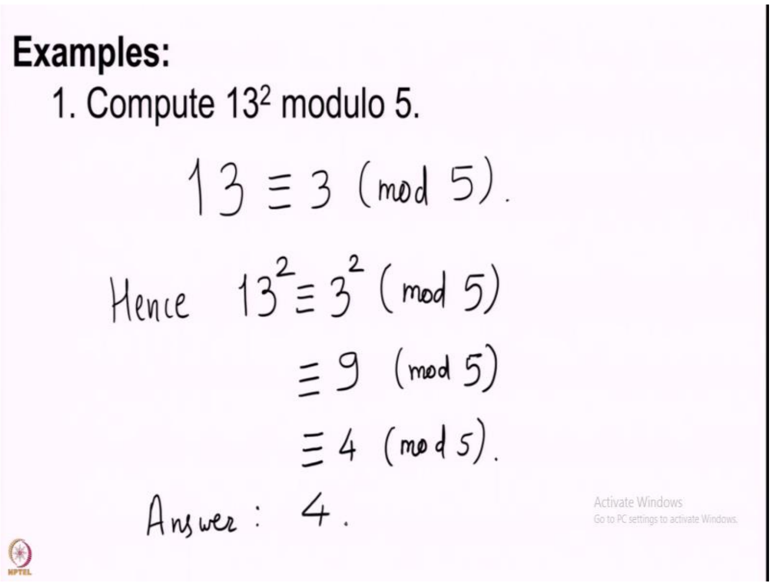
So, to say that it is not necessary that this happens, we need to just give an example where this does not happen. So, we consider the example where n is 3, let us say. Let us take a equal to 2 and I will take b equal to 1. Now modulo 3, the class of 1 is the class of 4 because 1 is congruent to 4 modulo 3. And now if I want to take the power of this, we want to know whether these 2 are the same. This is class of 2 power 1, which is class of 2. And this on the other hand is class of 2 power 4. 2 power 4 is 2 into 2 into 2 into 2 which is 4 square which is 16.

And, since your n is 3 class of 16 is class of 1, but class of 2 is not equal to the class of 1 modulo 3. These are not same. So, we get that these two are also not same. The class of 2 power class 1 and the class of 2 power class 4 these by the definition that we have made here are not the same. So, indeed we will have to think about and ensure that the operations that we define. So, what we have done here is that we have defined operations where our elements were some sets.

Remember the classes, the residue classes modulo n, are themselves sets and we want to talk about what it means to sum 2 sets modulo n. And we said that the sum of 2 sets is given to be yet another set where the set is obtained by choosing 2 elements from these two sets, taking their sum in the integers and then looking at the corresponding class. This is how we had defined.

Similarly, we defined for the product. Thankfully, these two operations are well-defined and therefore, we have a nice arithmetic on the set of residue classes modulo n. So, we have done a bit of theory until now. It is time to get our hands dirty and do some problems. So, I am going to give some examples. I will give you a minute or 2 to think about them and we will solve them together after that.

(Refer Slide Time: 16:28)



**Examples:**

1. Compute $13^2$ modulo 5.

$13 \equiv 3 \pmod{5}$.

Hence $13^2 \equiv 3^2 \pmod{5}$

$\equiv 9 \pmod{5}$

$\equiv 4 \pmod{5}$.

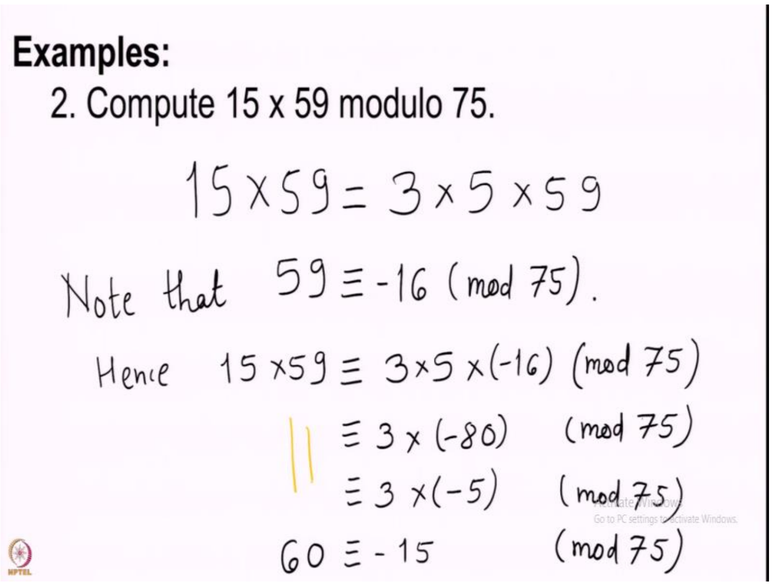
Answer: 4.

So, very first problem. So, simple problem – Compute 13 square modulo 5. So, we are working in the arithmetic of congruence classes, residue classes, modulo 5. 13 will give it is own class. I want you to compute the class which is the square of the class of 13. Your minute starts now. So, since your time is up. Let us compute these things together.

So, we have first of all 13 is congruent to 3, modulo 5. Therefore, if I wanted to compute the square of 13 this would be same as computing the square of 3. Of course, many of you would know what is the square of 13 right away, but if you do not know be at ease because we are doing the arithmetic modulo 5. And therefore, it is enough to compute the square of 3 which is 9.

So, you may say that the square of 13 modulo 5 is 9 that would also be okay, but since we are looking at the residue classes we will look at elements which are between 0 and 5. So, we are going to look at only the five elements 0, 1, 2, 3, 4, and among these 5 elements 9 is congruent to 4, mod 5. So, our answer is 4. Quite easy, so let us go and do some more problems.

(Refer Slide Time: 19:41)



**Examples:**

2. Compute 15 x 59 modulo 75.

$$15 \times 59 = 3 \times 5 \times 59$$

Note that $59 \equiv -16 \pmod{75}$.

Hence $15 \times 59 \equiv 3 \times 5 \times (-16) \pmod{75}$

$\equiv 3 \times (-80) \pmod{75}$

$\equiv 3 \times (-5) \pmod{75}$

$60 \equiv -15 \pmod{75}$

Second problem is slightly difficult. It says compute 15 into 59 modulo 75. So, now, earlier we had arithmetic modulo 5, we had only 5 numbers 0, 1, 2, 3, 4 and we wanted to take square of one of those and again get the answer to be equal to one of those. Here we have 75 elements. So, here we have to be slightly careful about taking this product. Do not use calculator, calculator is not going to be needed for this computation, so your minute starts again at this moment.

So, let us do this problem together. There are two things that I would do to solve this problem. 15 into 59 is actually 3 into 5 into 59, because 15 is nothing but 3 into 5, so the product 15 into 59 is same as 3 into 5 into 59. And further we note that 59 is congruent to a smaller number modulo 75. If you add 16 to 59 that is adding 1 first and then adding 15, so you will be adding 15 to 60, you will get 75.

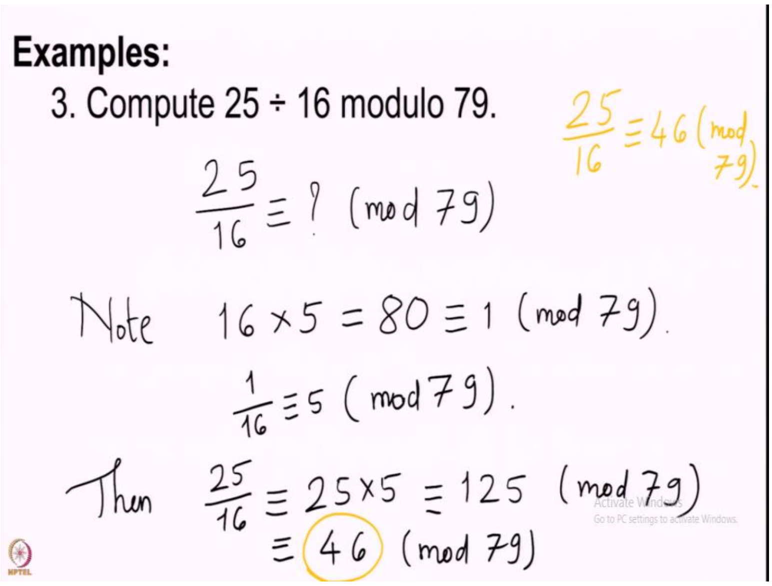
So as much, as long as the arithmetic is happening modulo 75, we can replace 59 by minus 16. That makes our problem much simpler. So, I will first of all write 15 as 3 into 5 and then I replace minus, then I will replace the 59 by minus 16. Now this is simpler because this is 3 into minus 80 mod 75. 16 into 5 is 80 and we have to keep that minus sign. But 80 is same as 5 mod 75. This is nothing but

3 into minus 5 which gives you minus 15 mod 75. So, answer is minus 15 or 60.

So, the answer that we obtain in this case is that 15 into 59 modulo 75 is 60. So, this was a slightly involved computation, but because we had 59, we could replace it by minus 16 and then do out the calculation by also observing that 15 is product of 2 smaller elements. So, there are two things that we can do here, which is that once you have one number into another number you can write one of the numbers as product of smaller numbers and do the product in steps.

Or, if you have a number which is bigger than n by 2; here 59 was bigger than 75 by 2, so we could replace it by a negative of a smaller number. These are the two things which we can do when we are doing arithmetic modulo natural number n. This is why this arithmetic is simpler compare to the usual arithmetic, which we do inside n, q, r, which is the real numbers or complex numbers. Let us go n do one more thing, after doing summation product the very next natural thing is division.

(Refer Slide Time: 25:15)



**Examples:**

3. Compute 25 ÷ 16 modulo 79.

$\frac{25}{16} \equiv 46 \pmod{79}$

$$\frac{25}{16} \equiv ? \pmod{79}$$

Note $16 \times 5 = 80 \equiv 1 \pmod{79}$.

$$\frac{1}{16} \equiv 5 \pmod{79}.$$

Then $\frac{25}{16} \equiv 25 \times 5 \equiv 125 \pmod{79}$

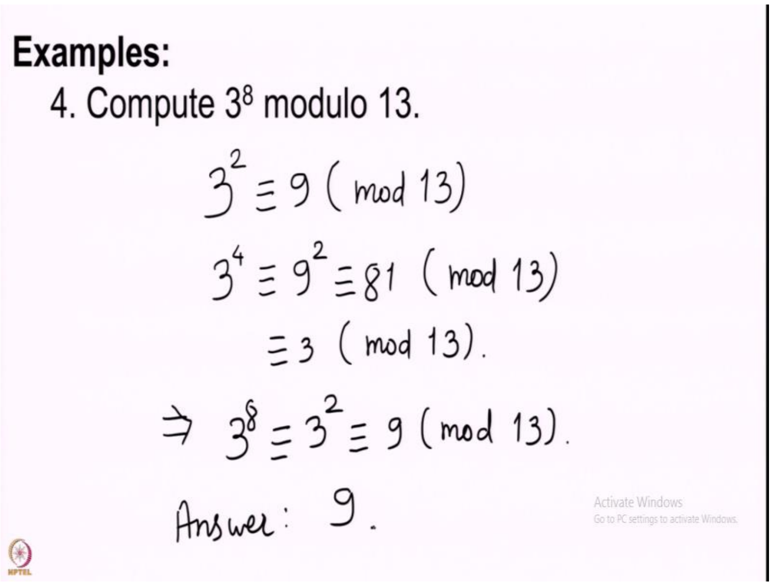
$$\equiv \boxed{46} \pmod{79}$$

So, I want you to tell me what is 25 divided by 16 modulo 79? Observe that I am asking you to divide by 16 mod 79. The GCD, the greatest common divisor of 16 and 79 is 1. In fact, 16 is 2 power 4. So, the only prime that will divide 16 is 2 and 2 does not divide 79, so there is no prime which will divide both of them and therefore the GCD has to be 1. Of course, you may also say that 79 is itself a prime. So, your minute starts now. So let us do this computation, we want to know what is 25 divided by 16 modulo 79? So, we want to understand this.

But it will be useful to note the following thing. Just like we had replaced the earlier 59 by negative of 16 to have a simpler thing, here we have a division which is a somewhat difficult operation. And so we would like to replace this division by multiplication by another number. So, what is that another number? Note that 16 into 5 is 80. And this is congruent to 1 mod 79. So, 1 upon 16 is congruent to 5 mod 79.

That makes our job quite simple because we then have 25 by 16 this is congruent to 25 into 5 modulo 79 and this is equal to 125. And then you just need to go modulo 79 and find once you remove 80 from this 125 you get 45 and to remove 79 you have to remove 1 more so we get that this is equal to 46. So, our answer is this 25 divided by 16 is 46 mod 79. Let us go and do one more problem.

(Refer Slide Time: 29:15)



**Examples:**

4. Compute $3^8$ modulo 13.

$$3^2 \equiv 9 \pmod{13}$$

$$3^4 \equiv 9^2 \equiv 81 \pmod{13}$$

$$\equiv 3 \pmod{13}.$$

$$\Rightarrow 3^8 \equiv 3^2 \equiv 9 \pmod{13}.$$

Answer: 9.

Compute 3 power 8 modulo 13. Your minute starts now. Alright, so let me do this problem as well. Let us compute all powers of 3, so we know that 3 square is congruent to 9 modulo 13. Therefore, 3 power 4 is going to be congruent to 9 square modulo 13. 9 square is 81 and 81 is we need to remove multiples of 13, 13 into 6 is 78. And once we remove 78, we get that this is congruent to 3, modulo 13. And hence, 3 power 8 which is the square of 3 power 4 is same as 3 square modulo 9, modulo 13.

So, our answer is that the class of 3 power 8 modulo 13 the residue class modulo 13 of the element 3 it is 8th power is the residue class of 9. We will see some more interesting problems in the next lecture. What we have to do is to keep in mind that the moment we do addition, subtraction, multiplication, or taking powers, we have to remove the multiples of n, and work with the smaller number. We are actually only working with elements 0, 1, 2, 3, 4 up to n minus 1. Have this with you and see you next time. Thank you.