

A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 10

Residue classes modulo n

Welcome back. We are talking about congruence relation and we saw that you can do addition, subtraction and multiplication while remaining, while keeping the congruence relation intact. Then we asked whether you can divide by things, you can divide by numbers and it was not possible to do it. We saw the example that 4 into 2 is equal to 10 into 2 if you are looking at modulo 12. It is congruent. Sometimes I may just equal. So, 4 into 2 which is 8 is congruent to 10 into 2 which is 20, modulo 12. But 4 and 10 are not congruent to each other.

(Refer Slide Time: 01:05)

Thus, it is not always possible to divide by a number modulo n.

However, if $(a, n) = 1$ then we can divide by a.

Let us see what it means.

If $ab \equiv ac \pmod{n}$ and $(a, n) = 1$ then $b \equiv c \pmod{n}$.

If $(a, n) = 1$, then a can be cancelled on both the sides of \equiv .

So, the lesson that we learn is that it is not always possible to divide by a number modulo n. Okay and I also told you in the last lecture that now there are two ways to get around this problem. You can either restrict the set of elements by which you can divide. We will put one more condition and then we will have that if your a satisfies some small condition then you can always divide by a modulo n.

Or we will reconcile with the fact that sometimes you may divide a number by another number modulo n and you may get multiple answers which happens when you divide 8 by 2 and you want to be in the arithmetic of the clock. If you want to be in the congruence relation

modulo 12 then your answer can be 4 or it can be 10 and you will then need some extra information to determine which answer you should consider.

Okay so I will first go to the restriction of the set by which we can divide. So, here is one small condition that we have. Whenever you have a relatively prime to n, whenever you have a co prime to n, whenever the GCD of a and n is 1 then we can divide by a. So, now let us put this statement in a precise form.

So, the precise form is this. If you have $ab \equiv ac \pmod{n}$ and the number a which appears on both sides of the congruence sign, if that a is co prime to n, if the GCD of a and n is 1 then b is congruent to c modulo n. You can cancel a from both sides. This is what it means.


If $(a, n) = 1$ then a can be canceled on both the sides of this, this is what it means which is quite good. Of course then the next question will come as to how many numbers are there which are co prime to n. Can you give some formula for the numbers which are co prime to n and so on? We will deal with these questions later. But let us now try to prove this statement.

(Refer Slide Time: 04:00)

If $ab \equiv ac \pmod{n}$ and $(a, n) = 1$ then $b \equiv c \pmod{n}$.

Proof: $ab \equiv ac \pmod{n}$ and $(a, n) = 1$.

Then $1 = a\alpha + n\beta$ where $\alpha, \beta \in \mathbb{Z}$.

$$b = b(1) = b(a\alpha + n\beta) = \underbrace{aba}_{=} + \underbrace{bn\beta}_{=},$$
$$c = c(1) = c(a\alpha + n\beta) = \underbrace{aca}_{=} + \underbrace{nc\beta}_{=}.$$


So, the statement is if you have $ab \equiv ac \pmod{n}$ and a is co prime to n then b is congruent to c mod n. Ideally, I should give you a minute to think about this proof. But this is slightly, very slightly, not too much, but very slightly on the level of the difficulty side compared to the other two problems which I had given you in the last lecture for thinking for

about a minute. You can of course pause this video and think about this problem but otherwise let us see the proof.

So, let us write down all the things which are given to us. So, we are given that ab is congruent to $ac \pmod n$. This is something which is given to us. You may be tempted to write it as ab minus ac is n alpha for some alpha but let us not do that for the moment. We are also given that a is co prime to n .

Let us write it down that 1 can be written as a combination of, linear combination of a and n over integers, right. We have ab congruent to $ac \pmod n$ and we also have that 1 is a alpha plus n beta for some alpha, beta in integers. This is because the GCD of a and n is 1, okay. Now, what we do is the following thing. We start with b and we multiply by b to 1. Since 1 is equal to this we have that b is equal to ba alpha plus bn beta, okay.

So, expanding this out we get ab alpha plus bn beta. Now, we also have c and we multiply by c to 1 to give us the same thing. So, we get these two equations. We got b is equal to ab alpha plus bn beta and we got c equal to, so you know, I should just write this also, c equal to ac alpha plus nc beta. Now, what we know is that ab is congruent to $ac \pmod n$. So, when you look at $\pmod n$ these two are congruent because ab alpha is congruent to ac alpha modulo n . The only thing would be to worry about are these things. But here observe that n divides both these terms.

(Refer Slide Time: 07:52)

If $ab \equiv ac \pmod n$ and $(a, n) = 1$ then $b \equiv c \pmod n$.

Proof (contd.):

$$\begin{aligned} b &\equiv ab\alpha + nb\beta \pmod n \\ &\equiv ab\alpha \pmod n \\ &\equiv ac\alpha \pmod n \\ &\equiv ac\alpha + nc\beta \pmod n \\ &\equiv c \pmod n. \end{aligned}$$




We write b is congruent to ab alpha plus nb beta mod n . This is because they were simply equal. We had that b is equal to ab alpha plus bn beta. So, b is going to be congruent to ab alpha plus nb beta or bn beta and observe that this already gives us that this is congruent to ab alpha mod n . This is because nb beta is 0 modulo n .


This further gives us congruent to ac alpha mod n because ab and ac are congruent to each other modulo n . You can multiply by alpha. So, we get that ab alpha is congruent to ac alpha mod n which is further congruent to ac alpha plus nc beta modulo n and therefore this is congruent to c modulo n .

(Refer Slide Time: 09:14)

If $ab \equiv ac \pmod{n}$ and $(a, n) = 1$ then $b \equiv c \pmod{n}$.

Proof (contd.): Thus, if $ab \equiv ac \pmod{n}$
and $(a, n) = 1$ then $b \equiv c \pmod{n}$.

Think about $8 \div 5$ modulo 12 



So, what we have obtained is indeed, if you have, thus if ab is congruent to ac mod n and $(a, n) = 1$ then b is congruent to c modulo n so quite a nice thing because in integers we were not always able to divide by something but here you can divide by elements which are co prime to n . So, if you wanted to divide 8 by 2 modulo 12 that would not be possible or you may have to accept that you may get multiple solutions. But if you were to divide 8 by 5 that would still be possible. So, think about 8 divided by 5 modulo 12.

For the moment we go to our next small construction which is that whenever we have fixed this integer n , modulo which we are looking at all the congruence relations now if I fix any other a , I can look at all other elements which are congruent to this given a modulo n .

(Refer Slide Time: 10:58)

For any $a \in \mathbb{N}$, we construct the corresponding class

$$[a] = \{b: a \equiv b \pmod{n}\}.$$

This is the set of all elements of \mathbb{N} which are congruent to a modulo n .

Clearly, this is an infinite set.

$$[a] = \{ \dots, a, a+n, a+2n, \dots \}$$



So, I will denote it by this symbol to construct this set b , so this is again coming from \mathbb{N} . You are looking at all other natural numbers which are congruent to $a \pmod{n}$. Okay this is actually a very big set that we have. This is the set of all elements of \mathbb{N} which are congruent to $a \pmod{n}$, and in fact a very simple observation will tell you that this is clearly an infinite set because your set a will consist of elements which are coming from the left-hand side of a possibly. And then you have a , $a + n$, $a + 2n$ and so on.

So, you clearly have an infinite set. So, the class of a is an infinite set. What we have done is that we have collected an infinite set and we are going to be treating this infinite set as same as the element a . This is what we are going to do.

(Refer Slide Time: 12:23)

Since \equiv is an equivalence relation, we have

$$[a] = [b]$$

or $[a] \cap [b]$ is empty.

Indeed, if $[a]$ and $[b]$ have an element in common then by transitivity of \equiv , $a \equiv b \pmod{n}$.

$$\exists c \in [a] \cap [b] \text{ then } a \equiv c \pmod{n}$$

$$\text{and } c \equiv b \pmod{n} \Rightarrow a \equiv b \pmod{n}.$$



What does it mean further? So, we had seen earlier that our triple horizontal lines, the congruence relation is an equivalence relation. Remember what it means. Let us recall it together. Equivalence relation has three properties. It should be reflexive which means that a is congruent to a modulo n for every a .

Second property is the symmetry which says that a congruent to b mod n should imply that b is congruent to a mod n . So, reflexivity is symmetry and the third property is the transitivity which says that when a is congruent to b mod n and b is congruent to c mod n then a has to be congruent to c mod n , okay. So, it this congruence relation is an equivalence relation. We have proved this fact two lectures back.

Therefore, we have, that if we take the classes a and b then you will either get that a is equal to b , the class of a is equal to the class of b . The sets that you get, the sets of natural numbers which are congruent to a mod n is the same set of natural numbers which are congruent to b mod n . You will either have this possibility or you have that the intersection of these two classes is empty. We are talking about various such subsets of natural numbers. Or you may also think about the subsets of integers.

If you were to think about the congruence relation being put on integers instead of natural numbers you may consider integers all over, the whole integers, positive as well as negative and throw in the 0 also there, okay. So, we have looked at some certain infinite subsets of integers or natural numbers whichever you are taking.

Then we say that our method of construction gives us the sets which are either equal or that they have no element in common. So, whenever you have two such classes if there is a single element in common, they should be the same. This is what we are saying. So, to prove this statement that either the class of a is equal to class of b or the intersection of class a and class b is empty.

If we want to prove this statement what we should prove is the following. If you take an element in the intersection of the two then you should prove that the class a is equal to class b , right. We are saying that there are only two possibilities that can occur about the classes. Possibility 1, classes are same; possibility 2, no element in common so if there is an element in common which is to say that the possibility 2 is not occurring then we should show that the only possibility that occurs is possibility 1. That will prove the statement.

So, let us go about proving it. If you have any element in common, if you have a c which is in a intersection b then we use transitivity. We will also use symmetry and other properties but mainly it is the transitivity which is used which will tell you that a is congruent to $b \pmod n$.

Let us see how this is done. If c belongs to the intersection of these two then a is congruent to $c \pmod n$ and I will write it as c congruent to $b \pmod n$, okay? We actually have that c is congruent to $b \pmod n$ and a is congruent to $c \pmod n$, and then the transitivity will tell you that a is congruent to $b \pmod n$. This is what we wanted to have.

So, whenever there is the common element in the classes of a and b then we get that the classes which are given by a and b have the property that a is congruent to $b \pmod n$. Now, with this we want to prove that the classes themselves are the same.

(Refer Slide Time: 17:23)

Since \equiv is an equivalence relation, we have

$$[a] = [b]$$

or $[a] \cap [b]$ is empty.

Indeed, if $[a]$ and $[b]$ have an element in common then by transitivity of \equiv , $a \equiv b \pmod{n}$.

Again transitivity gives that $[a] = [b]$.

$\exists d \in [a]$, then $d \equiv a$ and gives $d \equiv b, d \in [b]$.

$[a] \subseteq [b]$.

So, then we again go to transitivity to see that the class a is equal to class b . How does this, once again, happen? So, this thing, I am using the transitivity so if you have an element say d in class a then d congruent to a and this fact gives d congruent to b modulo n of course and so we have that d belongs to the class of b . We started with the class of a and we proved that any such element goes and sits in class b .

So, we have proved then that class a is contained in class b . But there is nothing important about ab , if I had taken the order in the reverse way I would be able to prove in the same way that class b is contained in class a . And that will tell me that both these classes are one and the same.

So, this is a very striking fact. We have used the congruence relation. We divided the whole set of integers or the natural numbers into subsets which are themselves infinite in such a way that these subsets are disjoint or they are the same, okay. So, this is what is called partitioning a set into subsets.

(Refer Slide Time: 19:14)

Thus, we can partition the whole of \mathbb{N} into these classes.

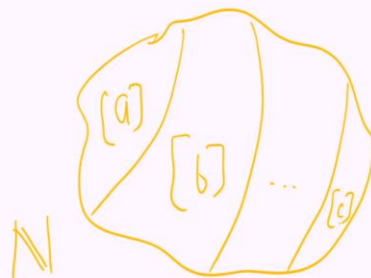


So, we have therefore been able to partition the natural numbers into these classes. Of course you will also use a reflexivity to show that every element of \mathbb{N} is contained in one of these classes. But if you take the element to be a then it is clearly contained in the class of a .

So, every element of \mathbb{N} is contained in one of these classes. So, \mathbb{N} is contained in the union of these classes and since each class is a subset of \mathbb{N} you have the other way equality also, other way containment also. So, \mathbb{N} is union of the classes but the classes are either same or disjoint. So, it is a disjoint union which is what we call as partition.

(Refer Slide Time: 20:06)

Thus, we can partition the whole of \mathbb{N} into these classes.



So, if you were to think about this in some set theoretic diagrams it will give you that if you have this as your set \mathbb{N} then we have divided this set \mathbb{N} into several of these partitions with respect to the congruence relation modulo n , alright.

(Refer Slide Time: 20:30)

Thus, we can partition the whole of \mathbb{N} into these classes.

$$\mathbb{N} = \bigsqcup [a]$$

Further, every $a \in \mathbb{N}$ is congruent to one of the following elements $\{0, 1, 2, \dots, n-1\}$.

$$\mathbb{N} = [0] \bigsqcup [1] \bigsqcup [2] \bigsqcup \dots \bigsqcup [n-1].$$

Given a , use the division algorithm to get $a = nq + r$ with $0 \leq r < n$.
 Then $a \equiv r \pmod{n}$

Further we are now saying that you do not have to look at infinitely many classes. Each class is equal to a class of one of these finitely many elements. So, earlier we saw that \mathbb{N} is union of these classes. Here we had that \mathbb{N} is disjoint union of the classes. But here we are saying that \mathbb{N} is class 0 disjoint union class 1 disjoint union class 2 disjoint union dot dot dot disjoint union class n minus 1. And this is quite simple because what we do is that, given any a , we will keep dividing by n and then there has to be a remainder. This is what our division algorithm tells us.

Division algorithm tells us that when you have any a and you want to divide by n then you have a equal to nq plus r . a equal to nq plus r where q was a natural number. r is also a natural number or it can be 0 but r has the property that it cannot be equal to a , n . It will be less than n . So, r can go from 0 to n minus 1, so that is what we have.

So, given a , use the division algorithm to get a equal to nq plus r with 0 less than r less than or equal to n minus 1. Then a is congruent to r mod n and r is in the set 0 to n minus 1. This is the proof that every a in \mathbb{N} is congruent to one of these elements 0, 1, 2 up to n minus 1. So, this is one good thing because we had an infinite set \mathbb{N} . We divided it into union of some subsets each of which was infinite. And now it turns out that there are only finitely many such partitions that you have. So, we have divided \mathbb{N} into only small n many partitions, okay.

(Refer Slide Time: 23:28)

Thus, we can partition the whole of \mathbb{N} into these classes.

Further, every $a \in \mathbb{N}$ is congruent to one of the following elements $\{0, 1, 2, \dots, n - 1\}$.

Thus, \mathbb{N} is a ^{disjoint} union of the classes $[0], [1], \dots, [n-1]$.



Thus, we can partition the whole of \mathbb{N} into these classes.

Further, every $a \in \mathbb{N}$ is congruent to one of the following elements $\{0, 1, 2, \dots, n - 1\}$.

Thus, \mathbb{N} is a union of the classes $[0], [1], \dots, [n-1]$.

These are called the residue classes modulo n .



So, \mathbb{N} is a union of these classes and in fact one can go further that it is the disjoint union. It is a disjoint union of the classes $0, 1, 2, \dots$ all the way up to n minus 1 . So, these are what are called the residue classes modulo n

(Refer Slide Time: 23:59)

Since $+$, $-$ and \times 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, $0, 1, \dots, n-1$.



And when we talk about arithmetic, we have that the addition, subtraction and multiplication preserve congruences modulo n . So, the congruence relation modulo n is preserved by these operations. Therefore, the set of residue classes modulo n admits addition, subtraction and multiplication. So, the set, the finite set that we had, the class of 0, class of 1, class of 2, class of up to n minus 1 that set admits all these operations. And what do I mean by this?

What one means is that you may take one class corresponding to a , take another, take some class which might be the same class or may be a different class corresponding to b , we can define addition of these two. And this addition is going to be defined to be the class of a plus b . Similarly, if you take the class of a and take class of b the product of these two is defined to be the class of product ab .

Okay these statements need a proof. To say that these are well-defined operations should be, that needs to be proved but I will leave it to you or you may go back and check some of the basic books on this theory that these operations are well-defined. Let me just tell you now what it means to say that these are well-defined. You see here we are adding two classes, the class of a and class of b and we say that this addition is equal to the class of a plus b . When you write it as class of a plus b you are really using the elements a and b .

Now, it may happen that the class of a is also equal to class of c . Somebody else may see it as a class of c . And somebody else may see the class of b as class of d . So, when you are adding two classes you have the addition of class a class b which is the same as class c class d . You are adding the class of c and class of d .

But if you are giving the definition of the addition as look at the element which is giving you the class, take the sum of these two elements and take the corresponding class then there are several ways. I can either take a plus b, take its class. I can take c plus b, take that class. I can take a plus d, take that class or c plus d, take the corresponding class. So, we will need to prove that all these four classes are actually the same.

(Refer Slide Time: 26:55)

Since +, - and \times preserve congruence modulo n , the set of residue classes modulo n admits addition, subtraction and multiplication. $\text{If } [a]=[c], [b]=[d]$

$$[a] + [b] = [a + b], \text{ then } [a+b] = [c+b]$$

$$= [c+d] = [a+d].$$

$[a] \times [b] = [ab].$ Similarly about the product.

So, the confusion here or the thing which needs to be proved is that if class a is class c, class b is class d then the class a plus b is the same as the class c plus b which is same as the class c plus d which is also same as the class b plus d. So, here we are replacing a by c, here we are replacing b by d and here we are again replacing, so this should be a plus d. So, the four ways by which you can add should give you the same set. That is what it means. Similarly, about the product, so similarly about the product but these are the things which can be checked quite easily and these are things which we have actually checked.

(Refer Slide Time: 28:14)

Since +, - and \times 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, $0, 1, \dots, n-1$.



So, I will not go over these but I will make one final remark before we stop this lecture which is that the arithmetic modulo n , this is what we are going to do, the arithmetic modulo n is an arithmetic with these n numbers. So, we are going to add $0, 1, 2, 3$ all the way up to n minus 1 with each other or we will subtract one from another or we will multiply these but the addition, subtraction and multiplication is to be taken with respect to the congruence relation modulo n . That is the only thing that we will be doing in this theme of our course which is the congruence and we will explore this further. So, I hope to see you again in the next lecture, thank you.