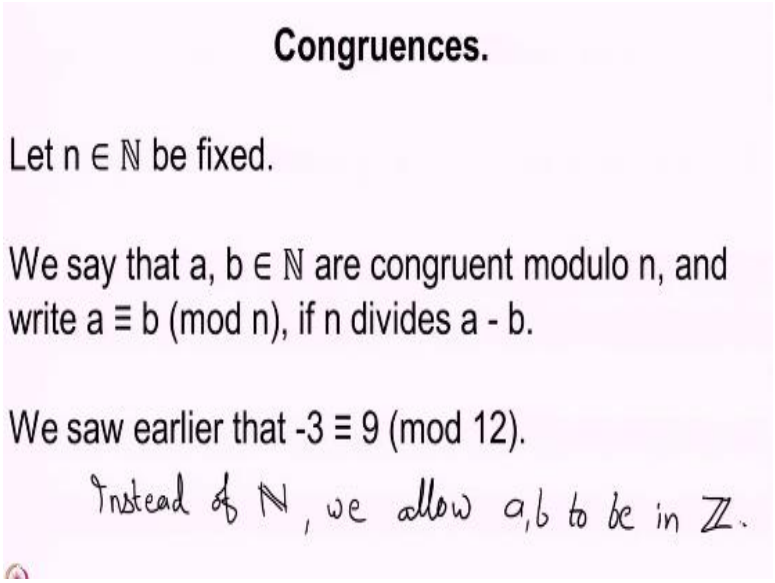
A Basic Course in Number Theory
Professor. Shripad Garge
Department of Mathematics
Indian Institute of Technology – Bombay
Lecture – 09
Basic Results in Congruences

Welcome back. We almost began our new theme in the last lecture which is on Congruences. We gave the very basic definition which is of two natural numbers being congruent to each other module a third given and fixed natural number N. The definition was as follows.

(Refer Slide Time: 00:41)



Whenever we fix this N so we assume that this N is fixed now then any two natural numbers a and b are said to be congruent to each other modulo n if n divides the difference a minus b. So, we have that n divides a minus b then we say that a is congruent to b mod n and we write it as a three horizontal lines b bracket mod n bracket complete. So, this is only for natural numbers.

But we also saw earlier in the previous lecture that minus 3 is congruent to 9 modulo 12. Now, this is easy to check because 9 minus, minus 3 which is going to give you 9 plus 3 is 12 which is divisible by 12 so 9 is indeed congruent to minus 3 modulo 12, but some of you may question here that the definition of congruence that we gave was only for pairs a, b coming from natural numbers how do you allow minus 3 then.

This is a very valid question and this can be resolved in two ways. Number 1 is that instead of N we allow a, b to be in Z. This is one way to resolve the difficulty. We say that we have a definition for pairs a, b coming from natural number we extend this definition to pairs a, b coming from integers. Indeed, infact we remark also earlier that the difference a minus b can be negative.

So, when we say that n divides a minus b the division may actually happen in Z not necessarily always in n. Infact, we saw the symmetry relation that whenever a is congruent to b mod n you also have that b is congruent to a mod n. So, that means whenever n divides a minus b we will use that n divides b minus a. Now, one of the a minus b and b minus a has to be a negative number unless of course both are equal and then they are equal to 0.

So, we are anyway talking about division taking place in Z so it is not a big deal, it is not a harmful thing to consider a, b to come from Z that will then take care of this minus 3. There is another way what way is that so we have to just think about what we mean by negative of 3, what is really negative of 3 what is minus 3. It is after all a symbol and in mathematics every symbol has a story to tell.

Sometimes the story is very long, sometimes the story is very short minus 3 tells a story. It says that minus 3 is that particular quantity which when added to 3 gives you 0. This is what minus 3 is the minus that we put next to 3 it is just to indicate that it is the particular number which when added to 3 gives you 0. This is a symbol which is universally accepted and so work with that. I will give you one more example of such a symbolism.

Whenever we take any two natural numbers say P and Q then we know that P by Q which we write as P slash Q that is a rational number, but that symbol P by Q also has a story. What does the symbol P by Q tell us? It tells us that P by Q is that entity which when multiplied by Q gives you P. So, this now tells you very easily that 2 slash 1 is same as 4 slash 2, 2 slash 1 is that entity which when multiplied by 1 gives you 2 that is 2.

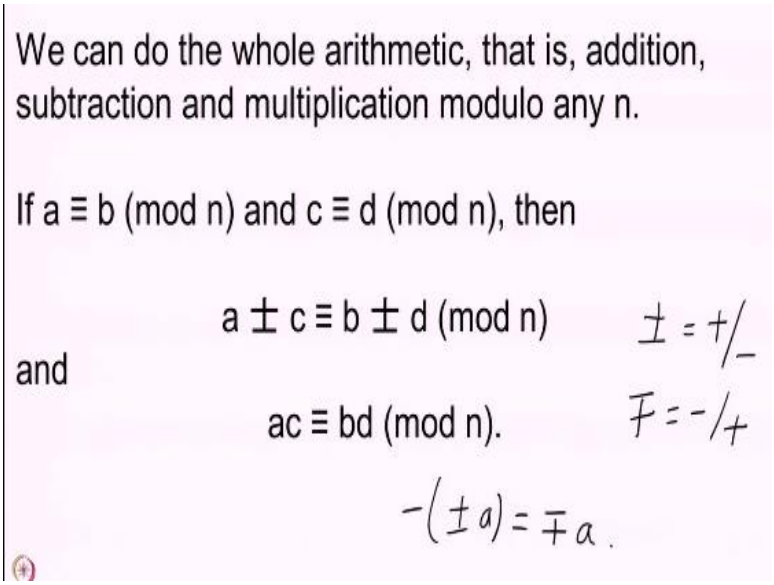
So, 2 by 1 is actually equal to 2 and similarly 4 by 2 is that entity which when multiplied by 2 gives you 4 and so again you get it equal to 2. If you have done any advanced classes in algebra you would have seen that given an integral domain, we construct the field of fractions and the field of fractions is constructed in the same way as we construct rational numbers from natural numbers or from integers.

And then you have various symbol of the type P by Q and you have to tell when P1 by Q1 is equal to P2 by Q2 there is some equivalence relation that you put by saying that the cross products agree or if you are looking at a general such construction which is called localization then you have to have some more conditions there, but this is all because you are writing it by means of a symbol and then there could be more than one way to write it.

So, coming back to our story when we are talking about minus 3 you could simply also say that 9 here is that particular natural number which when added to 3 gives you 0 modulo 12. This is really rushing ahead we are going to see the addition, subtraction modulo are given integer, but I told you this so that we can also make sense of minus 3 while remaining within the realm of natural numbers.

But if you are not convinced with this you can also assume that we are now going to define the congruence relation for a, b coming from integers we will get the same results, same examples so there is no problem even in that assumption. So, let us go ahead.

(Refer Slide Time: 07:35)



So, this is what we have that we can do the whole arithmetic that is addition, subtraction and multiplication modulo any n and what does it really mean? It means that if you have two pairs of natural numbers or if you were not happy with minus 3 and if you are not convinced by my explanation of minus 3 as 9 and you would rather have all equivalence relation given by congruence to be defined for pairs of integer then you can consider a, b and c, d to come from integers.

So, here we have two pairs a congruent to b mod n and c congruent to d mod n. Now, I can add a and c or I can also add b and d and the very first result says that whether you add or subtract it does not matter if you take a and c or if you take b and e. So, the first result says that a plus minus c this symbol is plus or minus. So, it says that if you are taking a plus c we will get b plus d mod n or if you take a minus c then you get it to be congruent to b minus d mod n.

We are using a short form mathematical symbols or mathematical sentences are they tend to be very long because we want to have them precise and therefore we use symbols to write them in short form just like I told you that P by Q is that particular number which were multiplied by Q gives you P. By the way when we are talking about P by Q it will also tell you 1 upon 0 is not defined.

Because 1 upon 0 has to be that particular number which when multiplied by 0 gives you 1 and if you are looking within a set of say real numbers, complex numbers, rational or integers then we know that 0 into any such numbers gives you 0. So, you are not going to get 1 upon 0 to be any element of b sets and therefore you have to construct a new symbol called infinity for that.

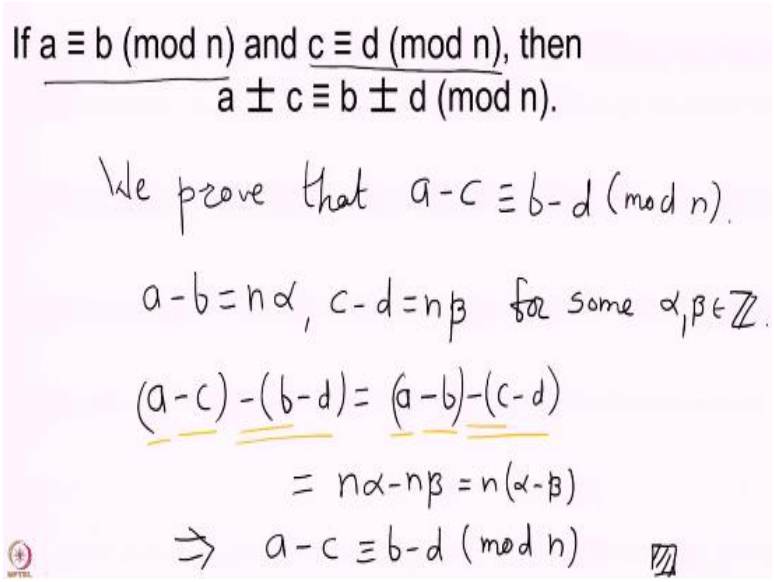
So, coming back to our story a plus minus c is congruent to b plus minus d this is about addition and subtraction and if you were to think about multiplication we will also have that ac is congruent to bd mod n. Since, we have gone to the next slide let me put it here again for your convenience that this symbol means either of the two, but you have to be careful if you are taking the first one then you will take the first one on the other side of the equation.

If you take the second one then you will take the second one. There is a similar symbol called negative and positive which says negative or positive. So, this order is very important, for instance, negative of plus minus a is negative or positive a. The order is very important. So, we are beginning a new theme of congruence relations I have given you the very basic definition.

And here is a very basic statement that a is congruent to b mod n, c is congruent to d mod n then a plus minus c is congruent to b plus or minus d modulo n. I am going to write this statement in the next slide you may choose any of the plus or negative and think about a proof for a minute. I will give you one minute, I will tell my proof, my proof meaning the proof that I am going to present after having prepared it from some books. I will present that

proof and if your proof happens to be different as always do write to me and let know your ideas.

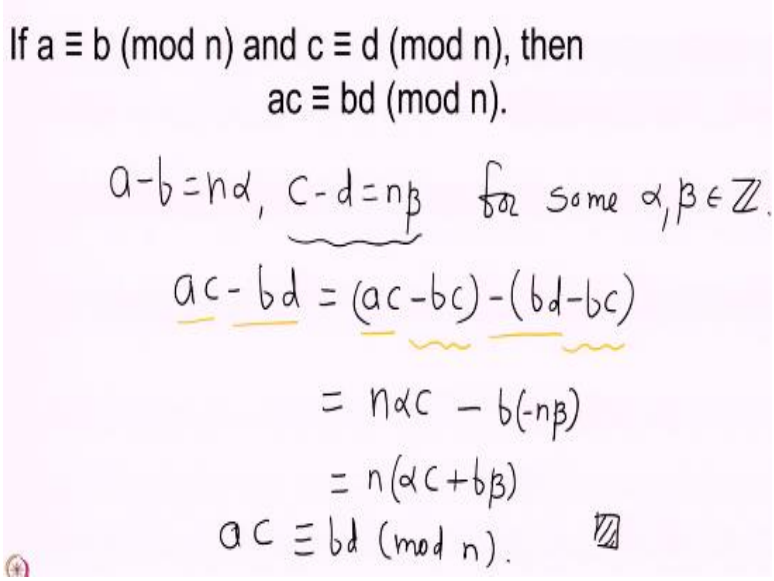
(Refer Slide Time: 12:07)



So, this is the statement which I invite you to think about for a minute. If you want to think about it for more than a minute you can of course pause this video and continue to think about this problem, but do un-pause it later and see the complete solution. So, here your minute starts now. So, now that the minute is over let me give you one proof. We will start with a minus c congruent to b minus d mod n that is what we will prove.

Since we have that a is congruent to b mod n we get that a minus b is n alpha and c congruent to d mod n gives us that c minus d is n beta. So, I need to just consider a minus c minus b minus d which is going to be a minus b minus c minus d. Check that the signs are all same b comes with negative sign, c comes with negative sign and d comes with double negative sign which is actually a positive sign and we have that a comes with positive sign. So, this is then equal to n alpha minus n beta which is n alpha minus beta which implies that a minus c is indeed congruent to b minus d mod n that is all. So, this proof was indeed quite simple.

(Refer Slide Time: 15:52)



Let us turnover to the second statement which says that whenever a is congruent to b mod n and c is congruent is d mod n then you take product on one side which is a into c this is same as taking the product on the other side which is b into d. So, we get that ac is congruent to bd mod n. Once again, I will give you a minute to think about it and sometimes a minute may not be enough so please feel free to pause the video, think about it for yourself.

The more you think about these problems for yourself the more clear these things will be to you, so your minute starts now. So, now that the minute is over or if you have taken anymore time then that time is also over. Let me now try to give you one way to prove this statement. So, we again have a minus b is n alpha c minus d is n beta for some alpha beta in integers. This is the thing which is given to us.

We want to think about ac minus bd we want to show that ac minus bd is a multiple of n. So, if you were to think about this one very natural thing would be to write it as ac minus bc minus bc minus bd. Check once again that this sign are all coming correct ac is coming with positive sign bd is coming with indeed we made a mistake here. So, bd is coming with negative sign and the signs for bc get cancelled because here it is coming with negative sign and then you have negative coming twice which is positive.

So, bc minus bc just gets cancelled. So, now our equation is okay and let us untangle what we have on the other side. This is really a minus b into c which is n alpha c because ac minus bc is a minus b into c that gives you n alpha c minus this is b into d minus c so this is b into d

minus c is minus n beta because c minus d was our n beta. So, d minus c is going to be minus n beta and so ultimately, we get it to be n alpha c plus b beta.

And then that completes our solution because we then get that ac is congruent to bd mod n. So, here we needed to have one small trick someone may say that this addition and subtraction of bc is a trick sometimes the solutions are very natural, natural in the sense that any person with some small background in mathematics will think about only that solution that is what is called a natural solution of course it is not a very precise word.

But this is what one means by natural solutions and sometimes there is a trick involved you may think that it is not really fair for a teacher to ask a question which involves a trick because the trick may occur to some students and it may not occur to some other students, but this is where practice or problems is important because there are things in mathematics in the theorem proving in the proofs of the theorem and so on which are called methods.

You know I told you about the methods of proving a result by contradiction. After all contradiction or using that method is a trick, but if you have seen this method n number of times then this trick becomes a method for you. Method of induction that is a trick who would have thought about it that if you think about proving the result for one particular integer and then you prove this weird looking statement that whenever the statement holds for an integer it holds for the very next integer.

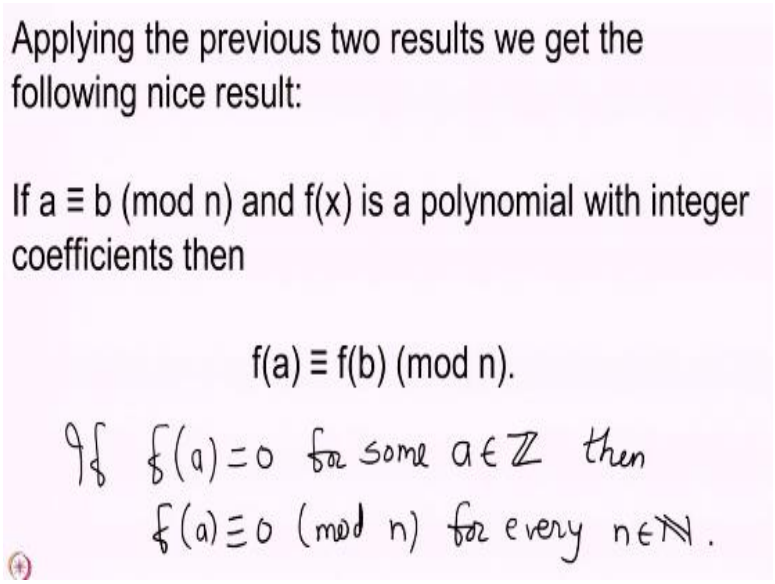
Then the statement holds for all the integers from the first integer for which I have proved it, it is a trick after all, but if you have used it so many times it becomes a method and so this addition and subtraction of bc is also going to be a method very soon for you. So, these are the things I always tell my students that you should have several bags with you. The first bag is about definitions.

Whenever you are learning mathematics you should keep all the definition secure in a bag, you should keep them there and the moment they are required you should be able to pull it out from your bag and tell definitions are very important. Second bag should be of examples whenever you have a definition there should be several examples that you should be able to do.

You should be able to give at least five examples for each definition. You should also try to have these examples of different flavor. Third bag perhaps a small bag will be the bag of counterexamples which is where if you have a definition which may have several conditions and then whenever one part of the definition is not applied you do not have the corresponding term that is when the counterexample helps you.

So, you should have counterexamples again also in a bag and finally you should have a bag of tricks which is actually a bag of methods with you. Once you have these four bags no one will be able to stop you from doing mathematics. So, we have now proved that you can add two elements modulo n the structure modulo n, the congruence modulo n does not get disturbed when you add or subtract. Similarly, the structure does not get disturbed when you multiply modulo n.

(Refer Slide Time: 24:12)



So, what it says is that you can do more things with these two. In fact you can apply these two results repeatedly to get this very nice result which is one of my favorite results. It says that if you have a polynomial fx whose coefficients are all integers so something like 5x square plus 2x minus 200 or it could be a polynomial in higher degree or it could just be a linear polynomial.

So, you take a polynomial whose all coefficients are integers and if you have two numbers a and b which are congruent modulo n then applying the polynomial to any of these two will give you the same result modulo n. So, applying previous two results repeatedly the addition, subtraction or multiplication and then finally adding it all taking powers again add them and

so on will give you that the polynomial evaluated at a is congruent to the polynomial evaluated at b mod n.

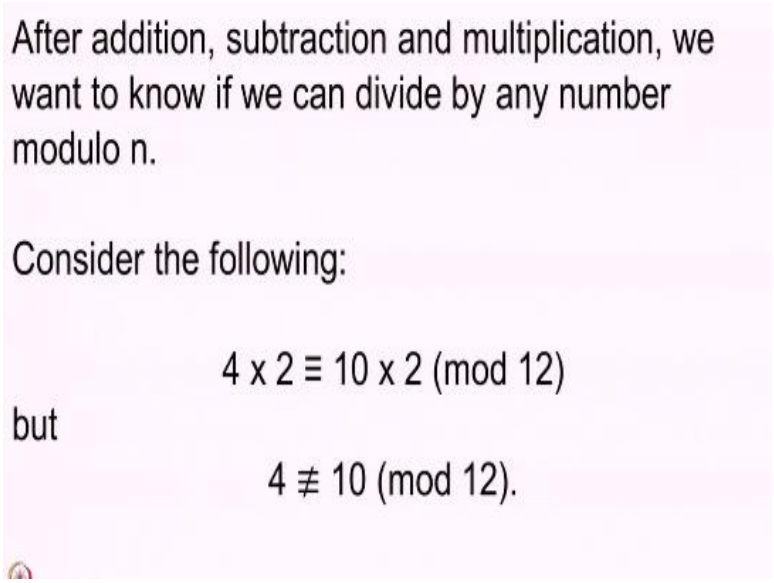
This is where we see the power of congruence if you were wondering why we are studying congruence at all, why do we have to have this slightly unnatural concept. You may say that already it is not easy to deal with the clock which works modulo 12. Why do I have to introduce all these different clocks modulo n for any given integer n, any given natural number n.

The reason is that ultimately we would like to solve equations polynomial equations in integers, you would want to solve a given polynomial, you would want to see whether there is a route for a given polynomial in integers. If there is a route then there is a route for every n. This is a very beautiful statement so let me write it first. If fa is 0 for some a in N or you know we can also take it to be a in Z.

Then fa is congruent to 0 modulo n for every n because 0 is after all congruent to 0 mod n. What we have observed here is that fa is one particular number and this number is equal to 0 and whenever there are two numbers which are equal they are of course congruent modulo n this was the first property of the congruence relation that we have seen it was called reflexivity.

So, if fa is 0 then fa is 0 mod n and turning the statement in the other way we will tell you that if you can find an n such that there is no 0 modulo that n which means that if you could find an n such that for no a you get fa congruent to 0 mod n then you cannot get fa equal to 0 for any integer n. We will be seeing one particular explicit example of this phenomenon very soon.

(Refer Slide Time: 28:06)



But let me now move towards one small observation. So, after addition, subtraction and multiplication we would like to know if you can divide by any number modulo n. We have done addition, we have done subtraction, we have also seen multiplication. Can you have a division? Modulo n already the division property in the natural numbers or in the integers was very interesting it gave us very nice concept of prime number.

Can you think about primes here also or maybe we can divide or sometimes it is not possible to divide what would happen? When we try to divide by a number modulo n. So, let us see an example. So, I am going to give you this congruence equation which says that 4 into 2 it is congruent to 10 into 2 modulo 12 because 4 into 2 is 8 and 10 into 2 is 20 and the difference of 8 and 20 is exactly 12.

So, we have that 4 into 2 which is 8 is congruent to 10 into 2 which is 20 so that means that if you were thinking of dividing 8 by 2 which answer will you consider? Will you consider 4 or will you consider 10? So, you will not be able to tell the division of 8 by 2. If you were thinking about it modulo 12 of course if you had some more information then you will be able to answer this very quickly.

So, there are now once again two ways to deal with this problem either you reduce the number of elements by which you can divide or you accept that there are multiple solutions when you divide by some number modulo and n. So, just to complete this discussion we observe that 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 modulo 12 because the difference of 4 and 10 is 6 or minus 6

depending on which we subtract and 6 is not divisible by 12 within integers in Z. So, this is something that we need to keep in mind, we will come back to this in our next lecture, but we take a break here. Thank you.