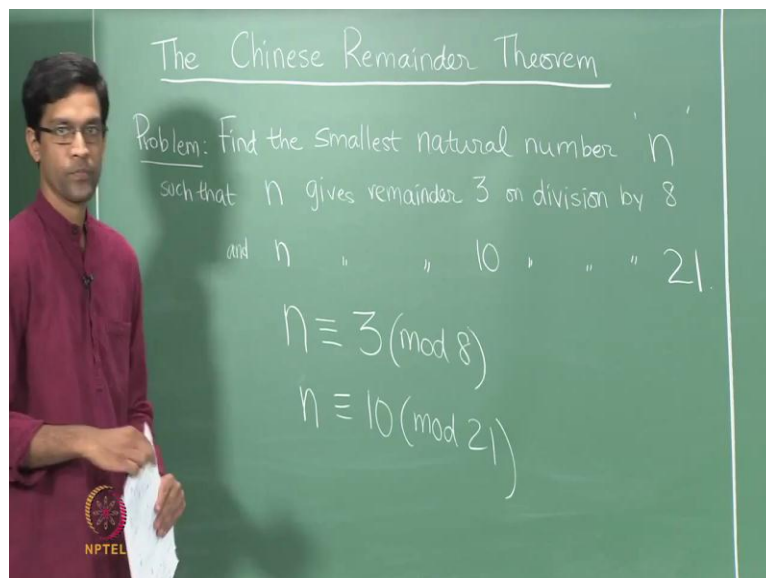


**An Invitation to Mathematics**  
**Prof. Sankaran Viswanath**  
**Institute of Mathematical Sciences, Chennai**

**Unit**  
**Number theory**  
**Lecture - 35**  
**The Chinese Remainder Theorem**

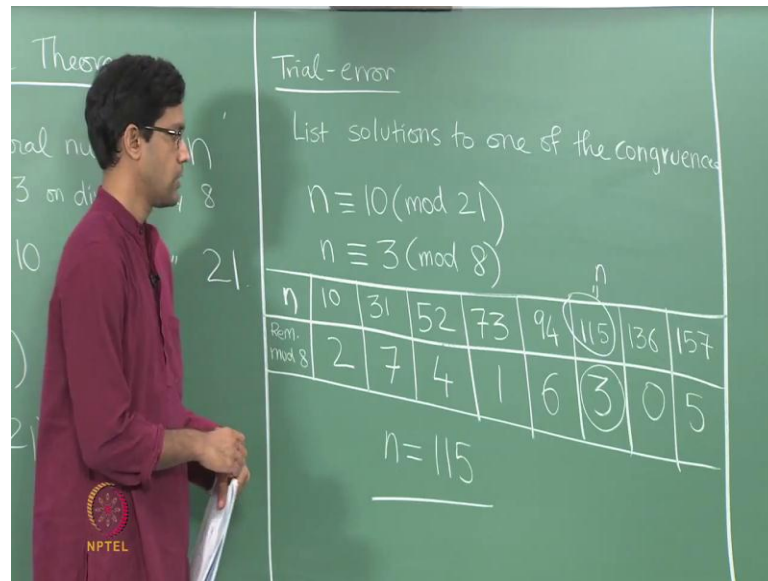
Today, we will talk about, what is called the Chinese Remainder Theorem, so the typical problem is the following. Find the smallest natural number  $n$ , such that  $n$  gives a remainder of 3, when divided by 8 and gives a remainder of 10 on division by 21. So, let us try and see what we would do to solve a problem like this.

(Refer Slide Time: 00:41)



So, firstly, let us rewrite this using our notation of congruence's. So, recall the first condition, just becomes  $n$  is congruent to 3 modulo 8 and the second condition is, that  $n$  is congruent to 10 modulo 21. And so, this is really a system of simultaneous congruence's. We are trying to solve two congruence's, which need to be simultaneously true.

(Refer Slide Time: 01:14)



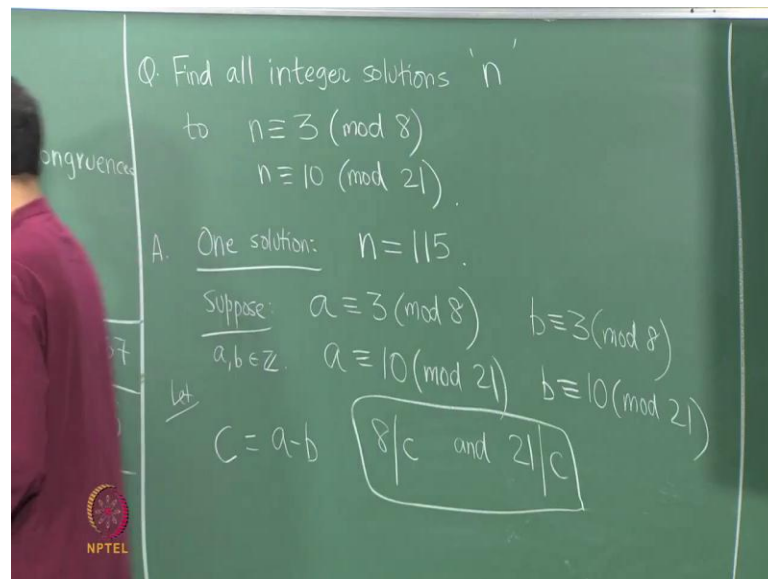
So, let us try and go about this in one way, which is a sort of a Brute Force approach. So, here is a trial and error or a Brute Force method is the following, you write out all possible solutions to one of the congruence's. So, list all solutions to one of the two congruence's, for instance here, let me pick  $n$  is congruent to 10 modulo 21 and let us write out all the values of  $n$ . So, recall from last time, this just means the following that, so let me write down some values of  $n$  here.

So, I am only looking for natural numbers. So,  $n$  equals 10 is one possibility, and then since it needs to be congruent 10 or 21, all we need to do get the rest of the solution is to keep adding multiples of 21. So, I have 10, I add 21 to it, I get 31, I add 21 to this, I get 52, then I get 73 and so on, write out a few more 94, 115, 136, 157 and so on. The list keeps going on, but for now I will stop there.

And now, what do we do well we remember need to also solve the second congruence. So, this list of numbers of course, solves the first congruence. So, let us figure out what remainders these numbers give us when divided by 8. So, here we will write down the remainders, when divided by 8, so let me call it remainders modulo 8. So, I will divide 10 by 8 and get a remainder of 2, if you divide 31 by 8, 31 is let see 24 is nearest multiple of 8. So, this gives a remainder of 7, 52, 8 6's are 48 and you are left with the remainder of 4 and so on.

So, let me write out the next few remainders it is a 1, it is a 6, this is the 3, this is the 0 and the 5. So, now, you scan through this list and you find that the number 115 also satisfies the second condition that we want. So, we also want  $n$  to satisfy  $n$  congruent to 3 mod 8 and of course, that is exactly what we want. So, the solution that we are interested in is the number  $n$  equals 115. So, we have solved the problem here  $n$  equals 115 is the smallest natural number which is congruent to 10 mod 21 and 3 modulo 8. So, that is sort of a Brute Force approach here.

(Refer Slide Time: 04:09)



Now, let us also ask the following modification of this question, what are all solutions? So, suppose I want to know, so here is the modified problem, find all, let me say integer solutions. So, I mean even allowing negative integers now; find all integer solutions  $n$  to the following congruence's. So,  $n$  must be an integer, satisfying the very same to congruence's,  $n$  congruent to 3 modulo 8.

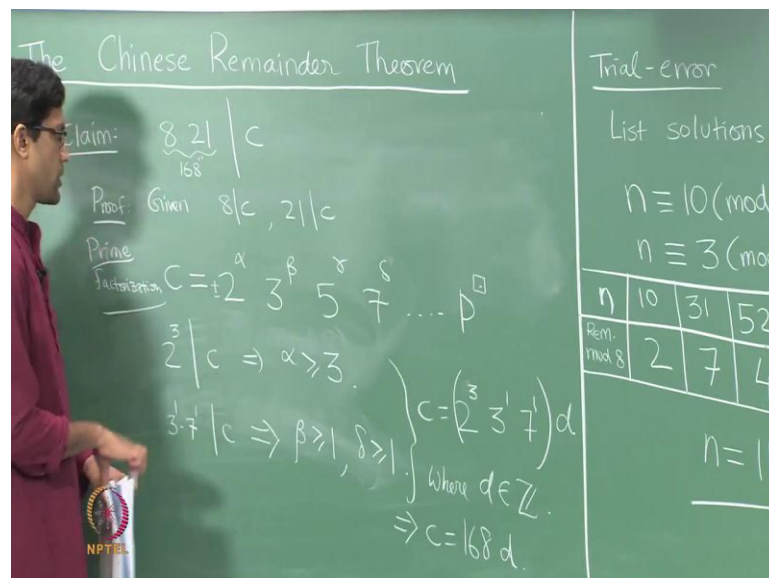
So, we have found one solution, we have found the smallest natural numbers solution to be 115, but now this question says, can you also find out all solutions, so all integer values which satisfied these very same congruence's. So, here is the key observation here, so here is the answer to this question. Suppose, I have another solution, so I know one solution now, one solution has been found by our trial and error procedure to be 115.

Now, here is the key point, suppose I have two solutions to these congruence's, so suppose  $a$  and  $b$  are solutions. So, suppose I have two solutions  $a$  and  $b$ , so  $a$  is congruent

to 3 mod 8 and what are a b. Let me say a b are integers, satisfying a congruent in 3 mod 8 and 10 mod 21, b satisfies the same relation, b is congruent to 3 mod 8, 10 mod 21. What can one say about a and b? So, let us do the following, observe that if you subtract a minus b, so let me call the difference to be c, let c be a minus b.

Now, what do these properties imply in terms of c, since a and b leave the same remainder modulo 8, a minus b as we observed last time, must be a multiple of 8. So, observe that c is in fact a multiple of 8. So, 8 divides c, similarly a and b give you the same remainder on division by 21, implies a minus b must be a multiple of 21. So, there are two properties that c satisfies, that c is divisible by 8 and by 21, so now let see, what this implies about c.

(Refer Slide Time: 06:48)



So, we claim that the fact that it is divisible by both 8 and 21, implies that in fact, c is divisible by the product of 8 and 21. So, the claim is that 8 into 21, so that is 168. In fact, divides c, c is a multiple of 168 and let us proves this. So, proof what do we know, we know that we are given that c is a multiple of 8 and that c is a multiple of 21. So, 8 divide c, 21 divide c and we want to conclude that c is a multiple of the product of these two numbers, it is just 168.

So, how do we prove this, where we sort out by thinking of the prime factorization of t of c? So, recall we said last time that every integer has a unique prime factorization. So, here is the prime factorization of c. So, what is prime factorization mean, it can be

written as the product of various prime numbers and alternate way of expressing the same thing is to write  $c$  as a product of powers of those various distinct primes.

So, this is probably more familiar, you can write  $c$  as, so what are the various primes involved, so 2, 3, 5, 7, 11 and so on are the initial primes. So, you can write  $c$  as some power of 2, so let say  $2^\alpha$  times some power of 3 times some power of 5, 7 and so on. So, imagine you write it as products of powers of all the prime numbers, well there can only be finitely many prime numbers involved. So, there is some  $p$  power something.

So, I do not really care, so this is what  $c$  looks like and what we know is that this expression is unique, you cannot have two different ways of writing  $c$  in terms of powers of primes. Now, what do we know about  $c$ , we know that 8 divides  $c$ , 8 divides  $c$  means that, well 8 is just  $2^3$ , so observe 8 is  $2^3$ . So,  $c$  must be a multiple of  $2^3$ ; that is the thing that is given.

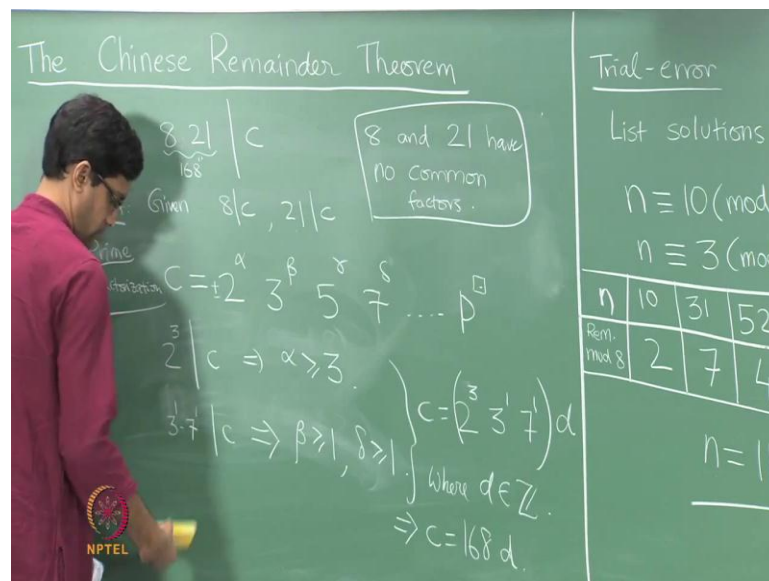
So, what is that mean? The prime factorization of  $c$ , here is the power of 2 that appears; the power of 2 had better be at least 3. This means that the power of 2 which appears must be at least a 3, only then can 8 occur as a factor of  $c$ . Similarly, 21 is 3 times 7, so it is  $3^1$  times  $7^1$ ,  $c$  is a multiple of that, implies that there must be at least 1 power of 3 and there must be at least 1 power of 7, let us call it.

And the rest of the things I cannot say anything about, but at least I have conclude that the prime factorization of  $p$  must have, you know at least a  $2^3$  appearing, a  $3^1$  appearing and a  $7^1$  appearing. So, the final expression for  $c$  therefore, looks like  $2^\alpha$ , it is 3 plus something, so this power here is at least a 3. So, let me think of it as, there is surely a  $2^3$  plus in addition there may be you know more powers of 2 involved.

Similarly, there is at least a  $3^1$ , there is at least a  $7^1$ , these factors are guaranteed to be there, in addition, there could be other things. Let me say  $c$  therefore, looks like this times  $d$ , where  $d$  is some natural number, where are some integer. So, observe, I did not quit assume that  $c$  is a positive integer. So, it could be that, it is a negative number, but that does not affect any of the arguments here.

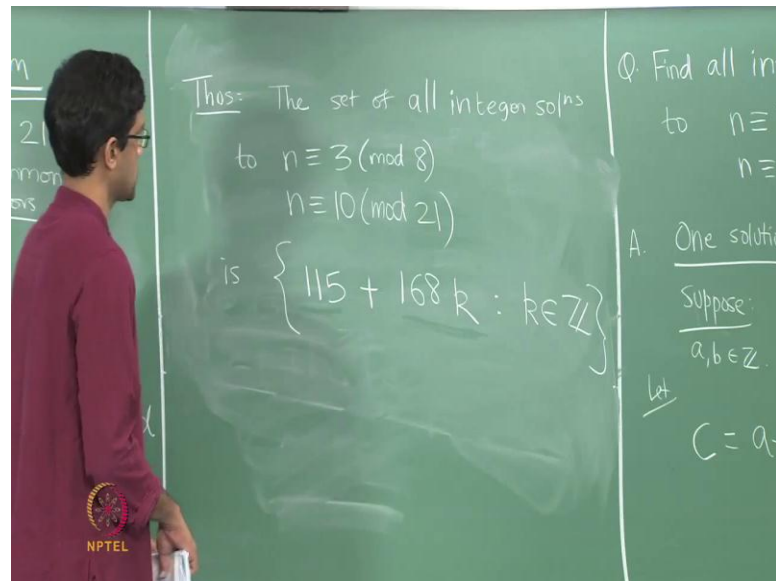
So, if  $c$  is negative I just put a negative sign and find it, but the final thing is true, if  $c$  is negative, I will think of  $d$  as being negative. So, anyway, so the point here been that this is 2 cubed, whereas that involves 3 and 7. So, there is a special property of these numbers that we have used. So, so by the way, we have finally proved what we want,  $c$  therefore is written as 8 into 3 into 7; that is exactly 8 into 21 or 168. So, we are finally written  $c$  as a multiple of 168, which we what wanted to prove, so our claim is proved. Now, observe there is one important fact that we have used, which really makes this whole thing work, which is that 8 and 21, do not have any common factors.

(Refer Slide Time: 11:18)



So, what makes this proof really take is the following fact that 8 and 21 have no common factors and we will see this point again. So, what we are manage to do is two things, one we are found one solution by a Brute Force approach, and then we have set the following that any two solutions have the following relation that their difference must be a multiple of 168. So, let us complete the solution to the problem we asked, so we said find all integer solutions.

(Refer Slide Time: 12:05)



Thus, here is the conclusion, how do you find all integer solutions to the original set of congruence's, all you do is you take one solution and you add any multiple of 168 to it; that is the only way you can get another solution. Thus, here is the conclusion, the set of all integer solutions to the two congruence's is... Well, the set is exactly the following, you take one solution which is 115 plus any multiple of 168, where k can be any integer.

Here, is the full set of solutions and why is this true, why does this follow from what we just proved, remember 115 is one solution and suppose you have any other solution, then the thing we just did as you take the difference between those 2's two guys. Then the difference is a multiple of 168, so you take 115 and any solution, take their difference. The result is a multiple of 168, which automatically means that the other solution had better have this form, it should look like 158 plus a multiple of 168, 115 plus a multiple of 168.

So, this is an important observation to make that somehow the fact that these two numbers do not have a common factor is what place a role here. So, suppose we did not want to actually find the solution, but maybe only wanted to show or be convince that a solution always exists.

(Refer Slide Time: 13:50)

integer sol<sup>ns</sup>


Alternate approach:  $8 \cdot 21 = 168$

n	1	2	3	4	5	6	7	8	9	10	11	...	27	...	168
n mod 8	1	2	3	4	5	6	7	0	1	2	3		3		0
n mod 21	1	2	3	4	5	6	7	8	9	10	11		6		0

$R: k \in \mathbb{Z}$

$T = \{(x, y) \mid 0 \leq x \leq 7, 0 \leq y \leq 20\}$

$S = \{1, 2, \dots, 168\}$



So, here is an alternate approach and let us do the following, let us write out, so I will sort of frame the problem at the end, but for now let us consider the following. Let us take the same two numbers 8 and 21, observe 8 times 21 is of course, 168 as we just said and let us do the following, let us make a list. So, let us write down all the numbers. So, of course, I am not going to be able to do this, but imagine that we write out a list of all numbers from 1 through 168 and now I am going to make a table.

So, I am going to write out all the numbers let say write out 1, 2, 3; just let us go little further, 8 may be until 11. So, imagine then that you keep going like this. So, let just pick some random thing in the middle, let me say 27 and then keep going all the way to 168. So, 27 just some random entry somewhere pick So, here is the short of table that I make, write down all numbers from one through 168 and there are two more rows here, where I will tabulate the following, I will look at the remainder, when n is divider by 8 and by 21.

So, I am going to extract two pieces of information. So, I am going to say n mod 8 by which I mean, the remainder on division by 8 and n mod 21 is just the remainder on division by 21. So, let us tabulate these values. So, for instance the number 1, when you divided by 8 or 21, we will just give you remainder 1. Similarly, the number 2 is just going to be a 2. So, nothing interesting happens at first, these numbers just give you back the same thing, so as remainders 7, 7.



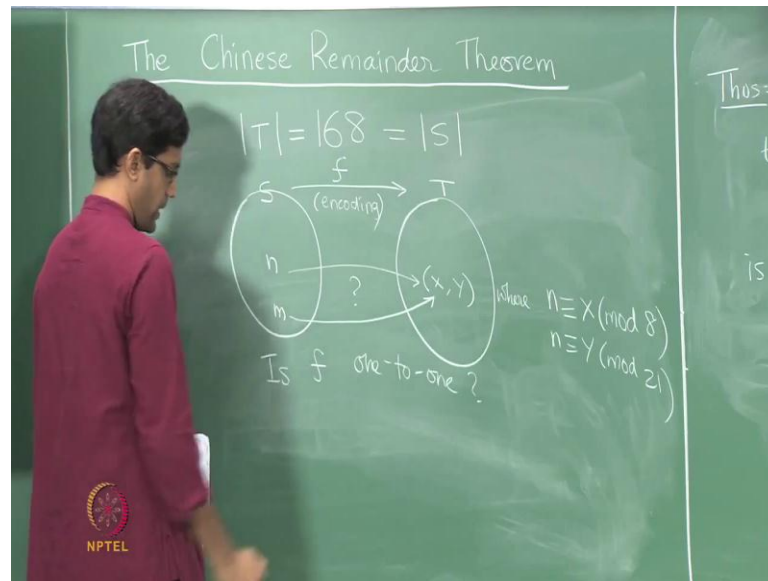
Now, comes the first time in something interesting happens, the number 8 on division by 8 will give, you remainder of 0. Whereas, on division by 21 of course, just gives you remember 8, so 9 is remainder 1, 10 is a 2 on division by 8 and just 10 on division by 21, 11 and let us look at so and so on. Let us look at 27 on division by 8 is 3 plus 24 plus 3 is 27 and on division by a 21 gives you a remainder of 6 and you keep going till the very last fellow is a multiple of both 8 and 21.

So, when you divide by both 8 and 21, it gives you 0. So, what you now have is the following, you have in our table of numbers from 1 through 168 and a tabulation of the remainders modulo 8 and modulo 21. Now, think of this as a pairs of numbers. So, the number 1 is sort of encoded by the pair 112 corresponds to 2 2 and so on. So, 27 for instance corresponds to the pair 3 comma 6, 168 is the pair 0 0, so I am sort of encoding each number by the pair of remainders that I get on division by these two place.

So, think of it as some kind of code, now here is the thing, let us set up. So, let us call these pair is the set of these pair is a something, I will call the set as T, let it be the set of all pairs of numbers  $x$  comma  $y$ , where remember what can  $x$  d it is a number between 1, well 0 and 7,  $y$  is a number between 0 and 20. Those are the possible remainders on division by 21.

So, the pairs  $x$  comma  $y$  are these fellows, so that is the set  $p$  consisting of all such pairs and the set S, let it just denote the set of all numbers from 1 through 168. So, I construct these two sets. Now, the first observation make is that, the set  $t$  also has 168 elements, just like the set S, which obviously has 168 elements. The set T also has the same number of elements.

(Refer Slide Time: 18:22)



And why, it is clear, because the elements of  $T$ , so the elements of  $T$  are just pairs of numbers  $x$  and  $y$  and for the first entry  $x$ , you have 8 choices, numbers from 0 to 7 and for the second entry,  $y$  you have 21 choices. So, the total number of choices, number of ways in which you can form pair is exactly 8 times 21. So, it is clear cardinality of  $T$  is 8 times 21; cardinality of  $S$  is of course, the same.

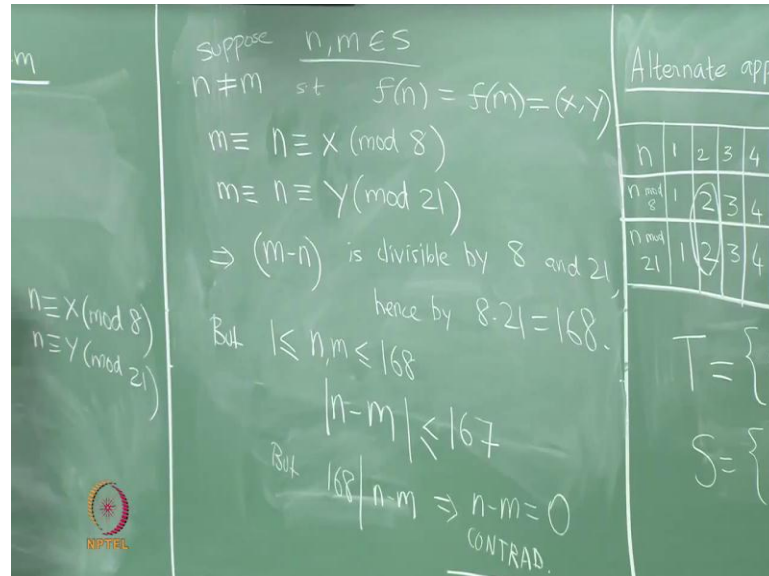
And now, what we are doing here by means of this table are, this encoding that I am just talking about is defining a map. So, here is the encoding map if you wish, which is doing the following, it is taking any number between 1 and 168 and sort of encoding it by a pair of numbers  $x$  and  $y$ , where what is  $x$ , it is a remainder that you get on division by 8,  $y$  is the remainder that you get on division by 21.

So, where what is  $x$ ,  $n$  is congruent to  $x \pmod{8}$  and  $y \pmod{21}$ ,  $x$  is between 0 and 7,  $y$  is between 0 and 20, only then will it be an element of  $T$ . So, here is the encoding map if you wish, so let us give the encoding map, let us just call it  $f$ , think of this as the encoding, and now here is the natural question, you can ask, what sort of property is just this map.

For instance is this encoding a faithful encoding, in other words can two different numbers lead to the same code. So, I would ideally like codes to sort of be faithful in the sense that I would want different numbers to be encoded as different things. So, let us ask that question is  $f$  one to one function is  $f$  one to one, in other words, can it happen

that I have different numbers  $n$  and  $m$ , which lead to the same answer here to the same code can such a thing happen.

(Refer Slide Time: 20:29)



So, let us consider this, so let us call suppose there are two numbers  $n$  and  $m$ , suppose  $n$  is not equal to  $m$ . So, what are  $n$  and  $m$   $n$  and  $m$  are elements of the set  $S$ , which are not equal and suppose it happens, such that there codes are the same  $f$  of  $n$  turns out to be the same as  $f$  of  $m$ , then let see, what we can obtain from this. So, what is the mean to say,  $f$  of  $n$  is equal to  $f$  of  $m$ , it means well that  $n$  is congruent to 3 mod 8, but then  $m$  is also congruent to 3 mod 8.

So,  $n$  satisfies these two properties not 3, but rather, if this is  $x$  comma  $y$ , then it means that  $n$  is congruent to  $x$  and  $y$  mod 21 and the same property is true for  $m$ ; that  $m$  is also congruent to  $x$ . So, recall are congruence can also be return like this,  $m$  congruent to  $n$  just means that, you know they both give the same remainder on division by 8; that was I have definition. So, they both give remainder  $x$  and division by 8, they both give remainder  $y$  on division by 21 and we have just done this argument.

So, this of course, implies at the difference  $m$  minus  $n$  is divisible by both 8 and 21 and hence by 168, we just said this, so this is divisible by 8 and 21, hence by their product which is 168. So, we conclude that  $m$  and  $n$  must in fact, differ by a multiple of 168, but observe that cannot happen, because  $n$  and  $m$  to start with, where elements of  $S$ , elements

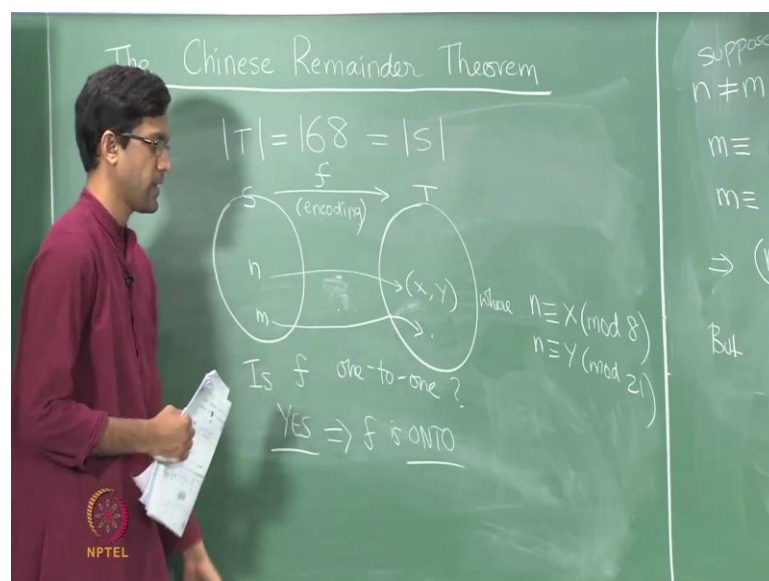
of  $S$  just means that they are numbers between 1 and 168. So,  $n$  is a number between 1 and 168,  $m$  is a number between 1 and 168.

So, if you take the difference, well what are the possibilities that and they are not equal to each other. So, the difference cannot be 0. So, the point is that the difference could never be a multiple of 168. So, the only possibilities are  $n$  minus  $m$ . So, may be in other way of saying in this is, if I have two numbers between 1 and 168, what can I say about the difference or the absolute value of the difference if you wish. So, what is the for thus they can be, one of them can be a 1 and the other can be 168; that is the only way in which you will get a very large difference. So, and that is just a 167 difference.

So, modulus of  $n$  minus  $m$  can be at most 167. So, what is this mean,  $n$  minus  $m$  is therefore, a number between plus 167 and minus 167, but it is also suppose to be a multiple of 168. So, you know this the only way that can happen is if it is 0, but we also know that 168 divides  $n$  minus  $m$ . So, the only multiple of 168 that lies in this range between minus 167 and plus 167 is the multiple 0.

So, this just means  $n$  minus  $m$  had better be the multiple 0, but that is a contradiction, because we assume that  $n$  is not equal to. So, what this implies is that  $f$  is in fact, a one to one function or in other words this code is a faithful code and what does it imply, let us come back to this function here.

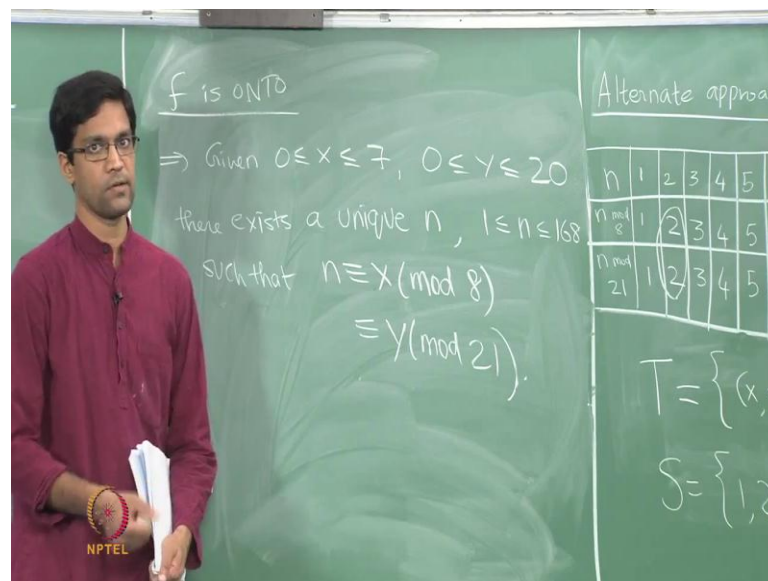
(Refer Slide Time: 24:09)



So, we have just concluded that yes  $f$  is one to one, so this can happen. So, this fellow had better go to a different point, but now recall that both these sets have the same numbers of elements both have 168 elements,  $f$  is a one to one function, automatically implies that  $f$  is an on to function, because what is the image of  $S$  under this function, well every fellow here maps to a different point. So, the total number of different points that you get in the image is exactly a 168.

So, the image has size 168, but the set  $T$  also only has size 168. So, the image had better equal the entire set  $T$ . So, yes and further this implies that  $f$  is a also on to. So, what is that mean it means that, this encoding function has the following property no matter which  $x$  comma  $y$ , you pick in  $T$ , which means you pick any number between 0 and 7 any number  $y$  between 0 and 20, you will always be able to find a number  $n$  between 1 and 168, such that  $n$  is congruent to  $x \pmod{8}$  and  $n$  is congruent to  $y \pmod{21}$ . So, let me just write the final conclusion here of this argument.

(Refer Slide Time: 25:35)



So, conclusion  $f$  is on to implies the following, given any  $x$  and any  $y$ , if in 7 and 20 respectively, there exist the unique, a unique number  $n$  between 1 and 168, such that,  $n$  is congruent to  $x \pmod{8}$  and  $y \pmod{21}$ . So, the original problem, we asked of finding the case, where  $x$  is 3 and this is 10, this only a special case and there we explicitly found the value of  $n$  to be 115. More generally, no matter which pair, you pick you can just pick

anything you want and you will always be able to find sum number  $n$ , which has that particular encoding.

So, it is a somewhat surprising fact at first, but here is the proof, non constructive proof an existence proof, it is tells you can always be done. So, what we look at next time is a way of actually doing this constructively in a somewhat more systematic fashion, then just doing Brute Force.