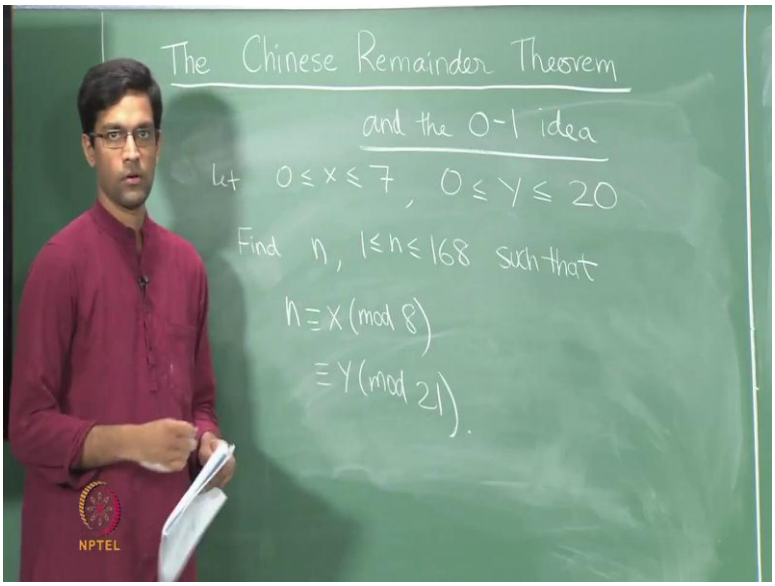
An Invitation to Mathematics
Prof. Sankaran Viswanath
Institute of Mathematical Sciences, Chennai

Unit
Number theory
Lecture - 36
The Euclidean algorithm, the 0-1 idea and
The Chinese Remainder Theorem

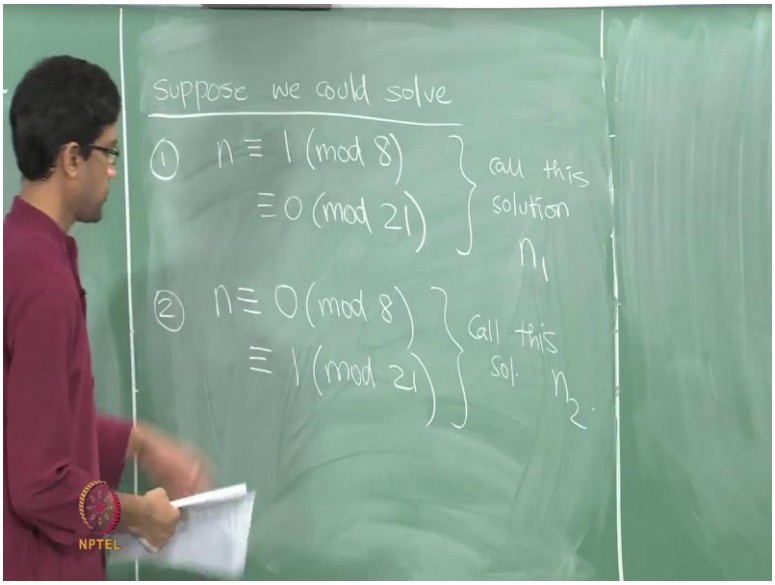
Now, this time we will talk about the Chinese Remainder Theorem again, but somewhat more constructive approach, which allows us to systematically find the solution. So, now, title did the Chinese Remainder Theorem and the 0-1 idea. So, we will see in a minute that the 0-1 idea that we have looked at in various different contacts also has a nice application in this particular problem.

(Refer Slide Time: 00:44)



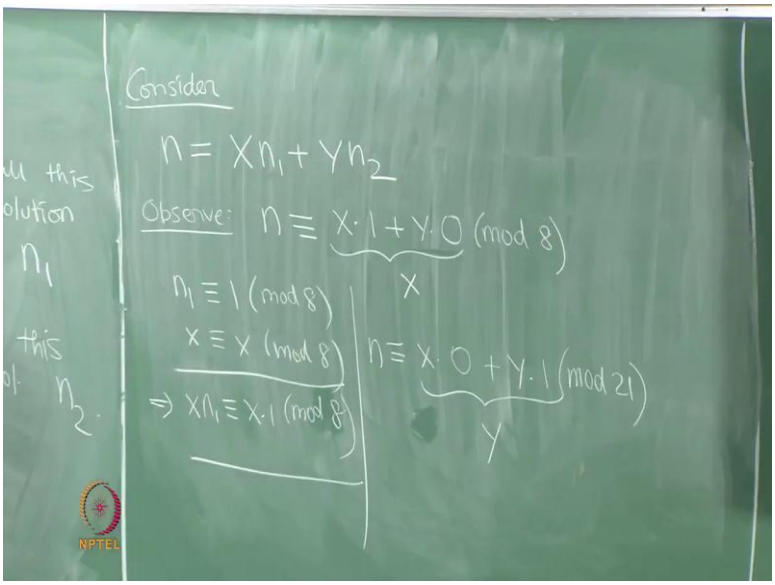
So, here is the same question asked last time, we said, so except I am going to do little more generally. So, let x be any number between 0 and 7 and y be any number between 0 and 20, a question is find a number n between 1 and 168, such that n satisfies those two congruence's, n is congruent to x mod 8 and congruent to y mod 21. So, now, let us bring in our 0-1 idea again, so this is the general problem we are trying to solve.

(Refer Slide Time: 01:40)



But, suppose we could do the following, so let us try instead to solve two problems. So, suppose we could solve, well problem 1, which is I can find a n, which is congruent to 1 mod 8 and 0 mod 21 and so let me say, suppose I knew how to solve this and let me call that solution as n 1, so call this solution as n 1. So, similarly let say, we can solve a second problem as well, which is the congruence n congruent to 0 mod 8 and 1 mod 21 and let us call, again as I am saying, let me assume I can solve this, so let me call this solution as n 2. So, suppose we could do these two problems, then the general problem is very easy to solve, so let see why.

(Refer Slide Time: 02:57)



Then consider, how do you solve the general problem. Consider the following choice of n, x times n 1 plus y times n 2. It is define n to be this and observe that, you know what you get when you look at the remainder of n, what is n congruent to modulo 8; that is the really the question. So, observe n 1 and n 2, so what are they congruent to mod 8, n 1 is congruent to 1 mod 8 by construction, n 2 is congruent to 0 mod 8. So, n will turn out to be congruent to x times 1 plus y times 0 mod 8, here I use the fact that n 1 is congruent to 1 and n 2 is congruent to 0.

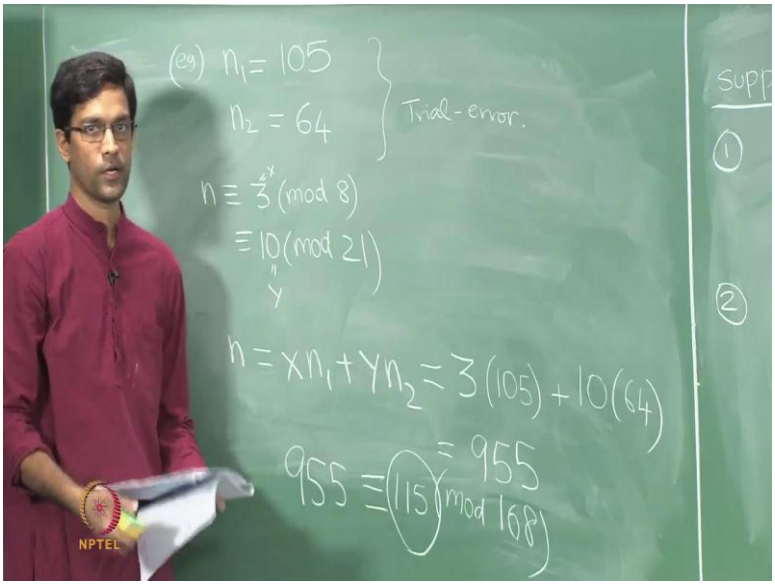
So, why is this? This is by the properties of congruence's that we talked about. So, recall congruence's have these nice properties with respect to addition and multiplication. So, how do I prove this for instance, so let me just catch a proof of this, n 1 is known to be congruent to 1 mod 8. So, what I will do an x is congruent to x mod 8, so this is the trivial statement, I am not saying anything here. This just says that x and x leave the same remainder when divided by 8; that is more or less tautology.

So, here are two congruence's mod 8 and last time, we had this property which said that, when you have things like this, you can multiply x and 1 will therefore, be congruent to x times 1. So, x and 1 will be congruent to x times 1 mod 8, this is the property of multiplication of congruence's. So, that is why I have concluded that the first term x and

1 is congruent to x mod 8. Similarly, the same logic apply to n 2 will show you that, why n 2 is congruent to y time 0 mod 8.

So, now, what is this, this is just x, x into 1 plus y into 0 is just x. So, for x n is indeed congruent to x mod 8 and by the same logic, if you look at congruence as modulo 21, now you will get n 1 is congruent to 0 and n 2 is congruent to 1, so it is again y, this is indeed. So, n terms out to be congruent to y mod 21. So, the key point is this, of this is to solve the general problem, it is actually enough if you can solve two simple problems. One for where you have a 1 0 for 8 and 21 and the other where you have a 0 1 for 8 and 21. This is the classic 0-1 idea that we have been using in many contacts before.

(Refer Slide Time: 05:53)



And in this case, let me just say, if you could solve these two, so let us actually do it in this example. So, the value of n 1, so let me tell you the value of n 1. So, this can be found by Brute Force, the value of n 1 is 105. So, if you look back at the table that we wrote out in the very beginning last time, where we try to do this by Brute Force, you will find that n 1 equals 105 has the property that it is congruent to 1 mod 8, but 0 mod 21.

Similarly, n 2 which is congruent to 0 mod 21, n 2 should be congruent to 0 mod 8, but 1

mod 21, so that is 64. So, n 1 and n 2 in this case turn out to be 105 and 64 and how do I obtain this for now, well if you think of it, it is just by trial and error, just by Brute Force. But, having gotten this, let us try and solve the problem from last time. So, now suppose I want to say, I want to find n which is congruent to 3 mod 8 and 10 mod 21, which is what we try to do, in other words x is 3 and y is 10.

So, what is a solution give us here, it says well since you know the solutions n 1 and n 2, the general answer is just given by x n 1 plus y n 2, which in this case is let see x is 3 into 105 plus 10 into 64, which turns out to be 955. So, doing it this way, produces the answer 955 and this may vary you for a minute, because remember the earlier answer we got was 115, when we did by Brute Force, but observe what we are getting by this method is just one solution.

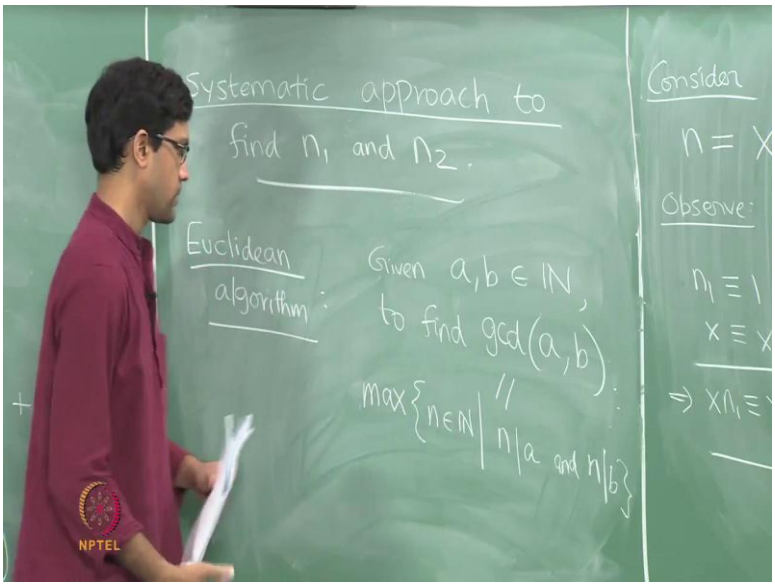
So, we are not necessarily getting the smallest natural number which solves this problem, all you are getting is some natural number or could even be an integer, if you know, if you take negatives here. All you are getting is some integer which satisfies this system of simultaneous congruence's. But, that is not you know too bad, because we know how to get all solutions starting from any one solution, all you do is just add or subtract multiples of168.

So, if instead of any one solution you wanted maybe the smallest natural number which satisfies these guys, these two congruence's. All you do is you just take 955 subtract out the appropriate multiples of 168 and see, what you get. So, in other words, you find the remainder that you get, when you divide 955 by 168, can you find that, when you divide 955 by 168, so 840 is a 168 times 5 and so this is exactly 115 more than that. So, 955 is in fact the same thing as 115 modulo 168.

So, here is the other, here is the smallest natural number solution, just 115. So, here is a second approach, which allows us to solve the same problem. But, still this requires one Brute Force step, how do you find n 1 and n 2. You now have two problems to solve and if you are finally going to solve both of them by trial and error, this seems like it is actually more work than just trying to do Brute Force directly on the original set of congruence's.

So, this approach is useful only if you can have a more systematic way of solving for n 1 and n 2, without using a trial and error theorem. So, that is the approach, I will describe next.

(Refer Slide Time: 09:45)



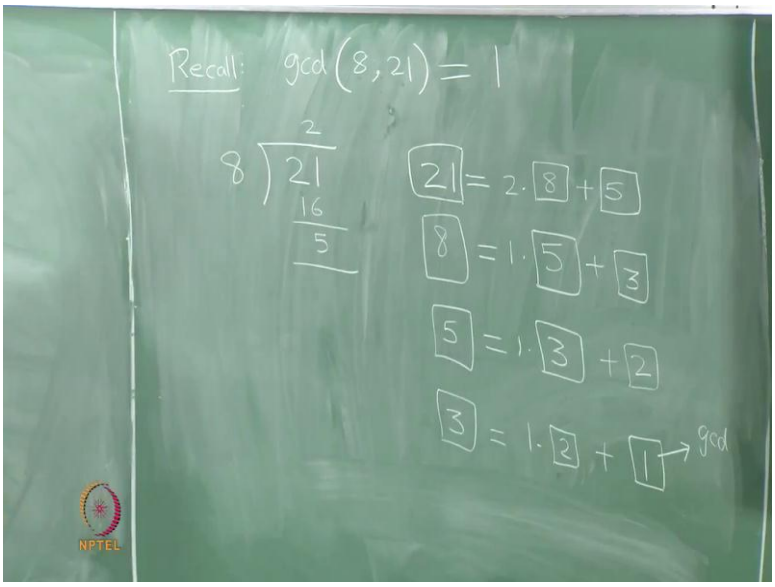
So, what we want is the following thing, we need a systematic or more algorithmic approach, systematic approach to find n 1 and n 2. So, in order to this, so let me just talk briefly about, something called the Euclidean algorithm, which may be familiar to you. So, what is a Euclidean algorithm do? So, let just do it by an example. So, given two numbers, it finds their greatest common divisor. So, that is the point of the Euclidean algorithm.

So, given two natural numbers, you wish a and b, it is an algorithm which finds the greatest common divisor the GCD of a and b. So, what is a greatest common divisor mean? It just means, well you do the following, you take all natural numbers n, which divide a and which divide b. So, such a thing would be called a common divisor, numbers which are factors are both a and b and amongst the numbers in the set, you find the maximum.

So, it is a maximum number in the set of n, such that, n divides a and n divides b that

maximum element is what is called the greatest common divisor of these two numbers a and b. So, now, the Euclidean algorithm, so let us apply it to the two numbers 8 and 21 that we started out with.

(Refer Slide Time: 11:38)



So, recall 8 and 21 have no common factors. So, we already said that before, in other words, there are no common divisors, so 8 and 21, if you look at what the common divisors are, well you only get 1, the number 1, of course divides everything. So, 1 will divide 8, 1 divides 21, but other than that there are in to any other numbers n. So, the GCD of 8 and 21 is 1, so sometimes we express this by saying they are relatively prime.

So, now, what is a Euclidean algorithm do? Given the numbers 21 and 8 and suppose you did not know to start with that they were relatively prime, you want to find that GCD in general given two numbers, how do you find that GCD. So, here is what the algorithm says, you perform a set of successive divisions. So, look at 21 and you divide 21 by 8 and find the remainder. So, 21, I divide 21 by 8, let see, whatever I get 8 2's are 16 and I get a remainder of 5.

So, in other words, this is nothing that we have been doing, you have been writing 21, you write it as some, so let me just do this, 21 can be written as 2 times 8. So, I divide 21

by 8 and I get a remainder of 5. So, here is the remainder 5. So, now, what you do beyond this well. So, what is the algorithm say, it is says the following. Now, instead of 21 and 8 as being the two players in the picture, you now replace 21 by 8 and think of 8 and 5 as being the two players in the picture.

So, may be a will just box this as well, because that is going to be something that enters the algorithm now. So, I write 21 as some quotient times 8 plus remainder and instead of thinking of 21 and 8 as been the two important entities, I replace them by 8 and 5. What is it mean, I divide 8 by 5, so next step the algorithms are following divide 8 by 5 and again find the quotient and remainder. So, 8 divided by 5, quotient is 1, remainder is 3.

Now, the same thing, so whatever the two numbers on the right hand side 8 and 5, you divide the larger by the smaller. Similarly, we have a 5 and 3, I divide 5 by 3. So, I write 5 as I divide 5 by 3, find quotient to be 1, remainder to be 2, do it again 3 and 2. So, I finally, get 3 is 1 times 2 plus 1. And if I do it once more, if I write 2 and 1, if write 2 as some multiplies of 1, so I could do this once more, I write 2 as some quotient times 1 plus a remainder, but now the remainders going to be 0.

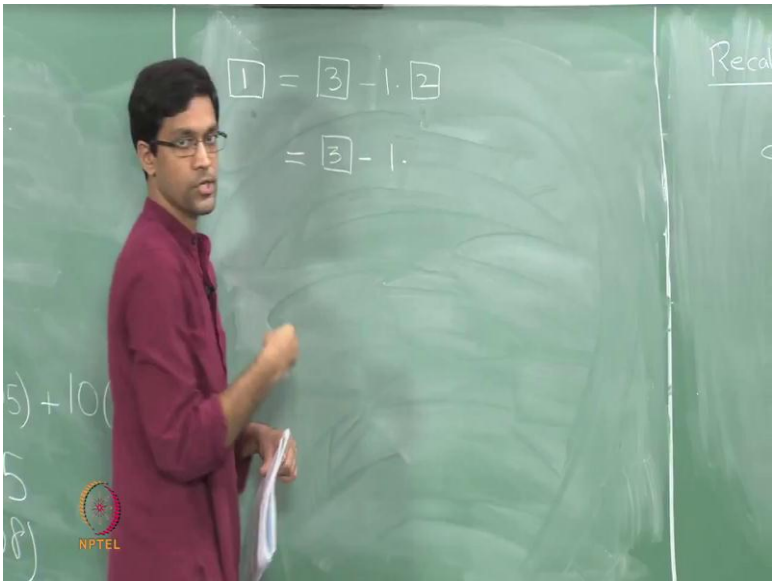
So, you keep doing this algorithm, so this is the Euclidean algorithm, you keep performing success to finds success of remainders. Now, finally, when the remainder becomes a 0, at some point, it will become a 0. So, what you do at that step is, well you forget that step, you just look at what you got one step preceding that. So, I forget the last step, the preceding step, there would have been a remainder that remainder is the GCD; that is what Euclid's algorithms says.

So, in this case, the final non-zero remainder, this fellow here is in fact the GCD of the two numbers of you know 8 and 21 in this case are more generally, if you had any a and b and kept doing this algorithm again and again. The final non-zero that you are obtain is the GCD of two numbers. So, let Euclidean algorithm, but you know, what is the GCD got to do with trying to solve for this congruence's and how do you find n 1 and n 2 from this congruence's.

Look at something more that you get the Euclidean algorithm. So, you should think of

the Euclidean algorithm as being a set of four such equations in this for this particular example, there are four equations. Now, the final equation which says that the GCD is a 1, so let me short of read these four equations from bottom to top. So, I turn the sequence around, I start from the end.

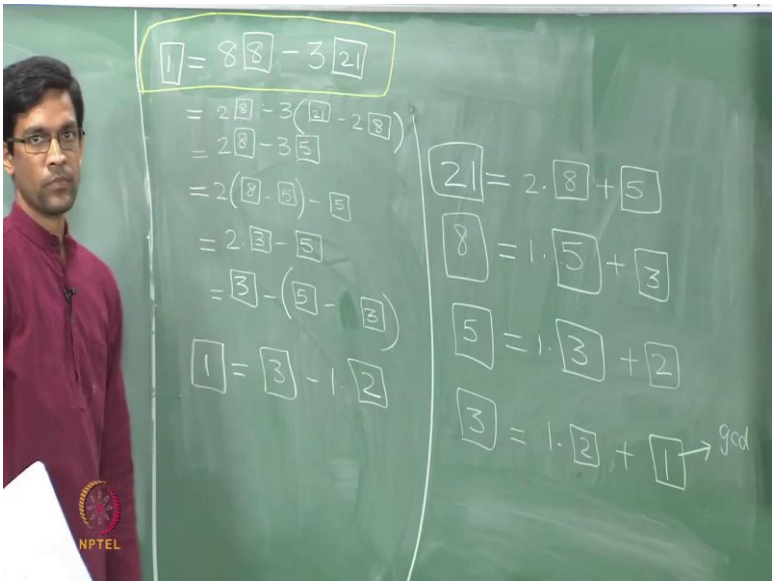
(Refer Slide Time: 16:07)



So, I will write 1 that was the last remainder as, well what is it get 3 minus 1 times 2. So, I am going to write the remainder alone on the right. So, now, I am written 1 in terms of 3 and 2. So, again now I mean recall I am trying to do this in reverse. So, 2, I will now replace with, so instead of having 3 and 2, I will try and write things in terms of 5 and 3. So, those who were the two players in the one preceding step and in going further, I will replace 5 and 3 by 8 and 5.

So, I want to keep replacing the two active numbers by what was active one step preceding to that. So, what will I do, I will write this as 3 minus 1 times. So, I will read my equation, you know the one preceding equation said that 2, maybe I will do it on this board, where see at all the original sets of equations.

(Refer Slide Time: 17:13)



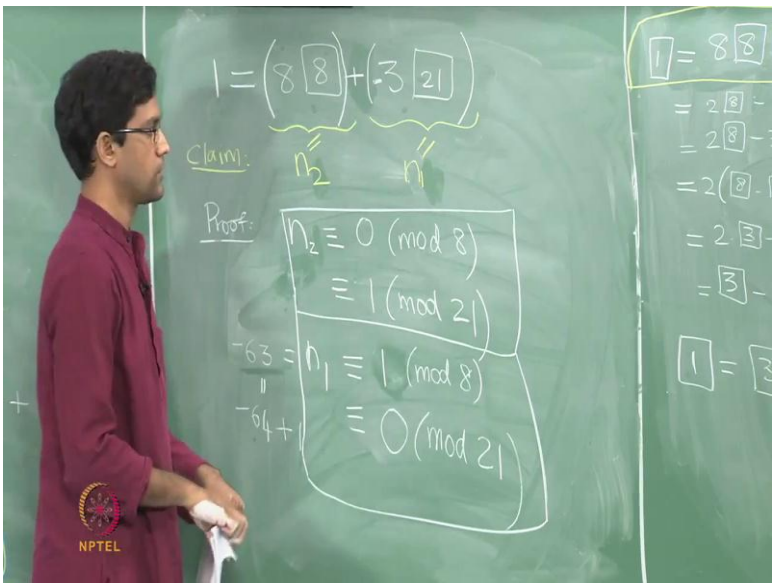
So, I start from the last equation, I write this as 1 equals 3 minus 1 times 2 and so going one step further, the 2, I will write as 5 minus 1 times 3. So, this would be return going to equal to here, the 3, I will leave as it is minus this 2, I will write as 5 minus 1 times 3 or 5 minus 3. So, this expression let me simplify little bit, what is this, this is a 3 plus 3, so it 2 times 3 minus 5.

So, now, I have written the 1, the final GCD in terms of 3 and 5. So, now, again I will go further in terms of whatever I get one step before do it. So, the 3 for instants here is 8 minus 5. So, I replace 3 like that and writhed as 2 times 8 minus 5. So, let simplify, it is 2 into 8 minus 2 into 3 into 5. So, it is 2 times 8 minus 3 times 5. So, last step, I will replace the 8 and the 5 by the 8 and the 21, now other words I will write the 5 is 21 minus 2 times 8, let us do that, it is 2 times 8 minus 3 times 5 becomes 21 minus 2.

So, this is the just Euclidean algorithm in reverse, where the idea finally, is to write the GCD back in terms of the original two numbers. So, what is this? So, let simplify this a little bit, this is a 2 into 8 plus 6 into 8. So, this is 8 times 8 minus 3 times 21. So, finally, what do I get, I get the following equation, when I finish this Euclidean algorithm in reverse. It just says that the GCD 1 is actually the following combination; it is 8 times 8 minus 3 times 21.

Observe, I done this completely systematically, I did not need to know, what these numbers a and b where, this procedure can be program on a computer for instance. So, all it saying is just keep going back words one step at a tim, substituting you know variable that you do not want are the number you want in terms of the numbers that you do on. So, finally, so observe this is of course, now 64 minus 63; that is indeed 1. So, the manage write in this way.

(Refer Slide Time: 20:08)



So, now, what so great about being able to write one in this fashion, the reason why did all this finally, what we here is obtain, it is 8 times number 8 minus 3 times 21. So, let me think of this plus 3 times minus 21, 3 times or plus minus 3 times 21. So, I am writing one some of these two numbers 8 times 8 plus minus 3 times 21. Now, here is what will do, define n 1 to be this number. So, remember we are trying to find n 1 and n 2, the solutions to those two congruence's, the claim is you can take n 1 to be just this number and n 2 to be this number, so that is a claim for now.

So, let us try and proof this. So, why is this in fact true, proof, so let us see what property did n 1 have to satisfy, so let just do it in this example. But, you will see it actually more generally true, n 1 was suppose to be divisible by such see which way was which, n 1 was suppose to be divisible by 8 and n 2 was divisible by this. So, let me call this as n 1

and this assign to n 2. So, let see, what properties plus and look at n 2 first.

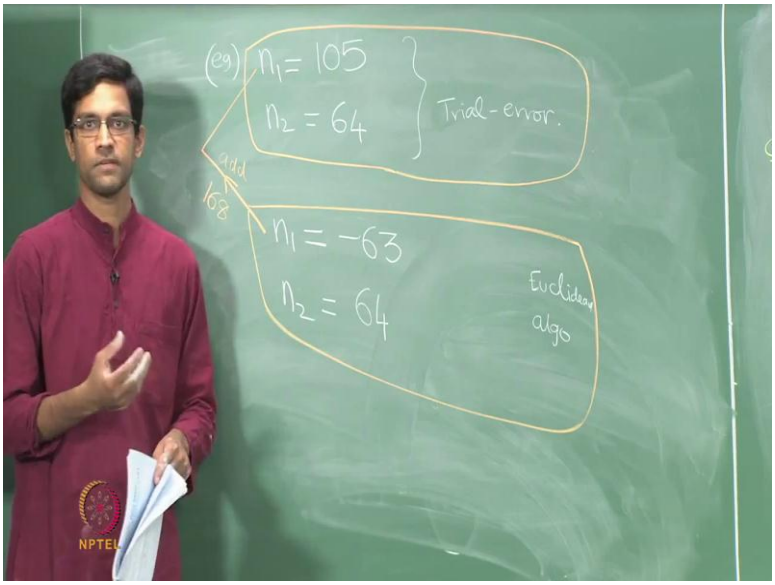
So, what properties does n 2 have, n 2 is just 64 in this case, it is congruent to 0 mod 8 and 1 mod 21, why said 0 mod 8, because it is multiple of 8; that is module as clear. Why, is said congruent 1 mod 21, well you divide 64 by 21 you get 63 as the quotient and thus a one left over and that is exactly, what is happening here, because there is a 63 you know that is the part divisible by 21 and then that is the one that is 1 the other side.

So, when you divide this number n 1 by 21, because this is a multiple of 21, what is left will always be a 1. So, it is kind of by design. So, n 2 satisfy these two congruence's, similar let us could n 1, n 1 in this case is a minus 63. So, observe, it is not a positive number, it is a negative number, but nevertheless, it is a solution to the set of congruence's.

So, this is a multiple of 21 0 mod 21, because after all it is minus 63, it is minus 3 times 21, but here is the interesting part in surely the 1 mod 8, why is that because minus 63 think of it as minus 64 plus 1. So, this is here is a multiple of 8, which is minus 64 and your adding 1 to that. So, the remainder on division minus by 8 is in fact a plus 1, if you take this first fellow as n 2. And the second fellow is n 1, the automatically satisfy the two congruences that you require of them, n 2 satisfy this 0 1 congruence and n 1 satisfy is the 1 0 congruence.

And this is the general fact, no matter which a and b you start with provided you know instead of 8 and 21. You start with any two relatively prime numbers things which do not have a factor, perform the Euclidean algorithm on them, you finally, obtain the GCD, you run the Euclidean algorithm in reverse to obtain and expression, where the GCD 1 is return as some multiple of the number a plus some multiple number of the b. Then, this you know pick one of the factor is n 1, the other factor is n 2, they will always satisfy they will be these 0 1 solutions, these solutions to the 1 0 and 0-1 congruence's. This is at completely general fact and completely systematic way of finding the solutions n 1 and n 2. So, now, in this case, you know what are the two solutions, one them n 1 is minus 63 on the other is 64. So, those are the two solutions in this particular example.

(Refer Slide Time: 24:23)



Now, the solutions from before, so we know these two things, where things we found by trial and error. Now, here is the solution which we are going to find by out systematic procedure, the Euclidean algorithm approach. So, here is the Euclidean algorithm provided solutions the Euclidean algorithm says as n 1 is the minus 63 and n 2 is a number 64. This is what Euclidean algorithm gives.

Now, comparing with what we had before, observe we had return out two solutions by trial and error, but again you know, so what is a difference n 2 is a same, but n 1 change different, the trial and error method said that 105, but this said this minus 63. But, again note that, this is only one solution and to get any other solution, all you need to do is, you know going from here to here, you can add any multiple of 168 to get a new solution.

So, minus 63, you add 168 to 8; that is exactly going to give you plus 105. So, how do you go from this Euclidean solution to the trial and error solution, well you just add 168 and that is of course, something we know you can always do. So, this is just this short of concludes this idea. So, we have done two things one really, one is we are introduce the 0-1 idea in this context and seen that, it actually has a very nice application to this problem.

Secondly, we have use the Euclidean algorithm to give a systematic solution of the 0 and problem. Often, it is not the fact that the 0-1 problem gives a solution that matters that there many contacts, it is being able to write easy solutions to 0-1 problems that is being something we have of used again and again. In the Lagrange interpolation method for instants the 0-1 problems has a very easy solution, because of those special forms of Lagrange polynomials, product of the x minus x 1, x minus 2, whatever divided by something. That something we could get by using properties of polynomials.

In the example, when we talked about three dimensional vectors and the 0-1 idea, we were able to solve the 0 1 and problem more or less by using the cross product of vectors. So, the cross came and handy there, allowed as to give quick solution of in the 0-1 problem. Here, the solution of the 0-1 problem comes through the Euclidean algorithm and you need to do whatever we said, run it in reverse to do this and then you are done in one step you get the 0-1 problem. So, all of this for instants can be programmed on a computer in a completely systematic fashion and own require any guessing or trial and error.