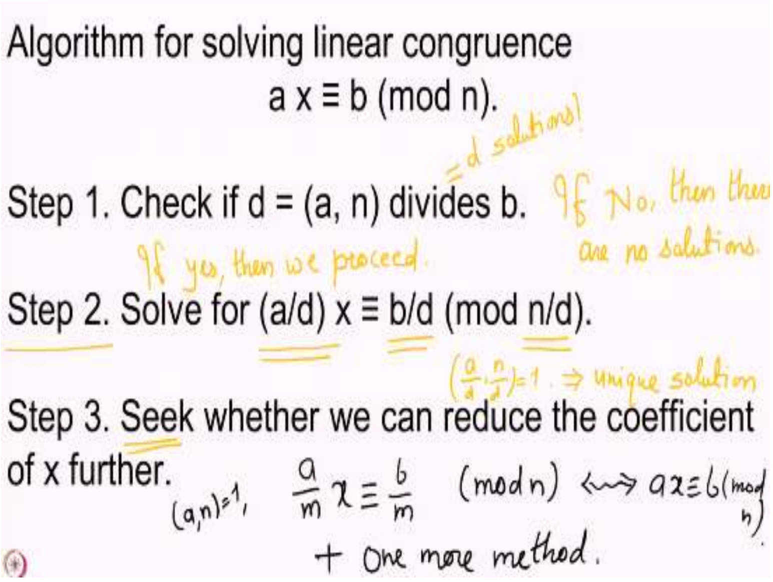
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 16
Solving Linear Polynomials Modulo n - IV

Welcome back so we are considering the solutions to linear congruences modulo n and we saw that there is an algorithm.

(Refer Slide Time: 00:28)



Algorithm for solving linear congruence

$a\,x \equiv b \pmod{n}$.

Step 1. Check if d = (a, n) divides b. $\equiv$ d solutions! If No, then there are no solutions.

If yes, then we proceed.

Step 2. Solve for (a/d) x ≡ b/d (mod n/d).

$(\frac{a}{d}, \frac{n}{d}) = 1 \Rightarrow$ unique solution

Step 3. Seek whether we can reduce the coefficient of x further.

$(a,n)=1, \quad \frac{a}{m}x \equiv \frac{b}{m} \pmod{n} \leftrightsquigarrow ax \equiv b \pmod{n}$

+ One more method.

So algorithm had two lemmas which we have proved but let me put the algorithm here for your reference. So what we have done is in the first step that we have been able to reduce the coefficient of x the constant term as well as the congruence by having divided by the GCD. So, ofcourse if the answer is no then there are no solutions. If yes then we proceed this is what we do.

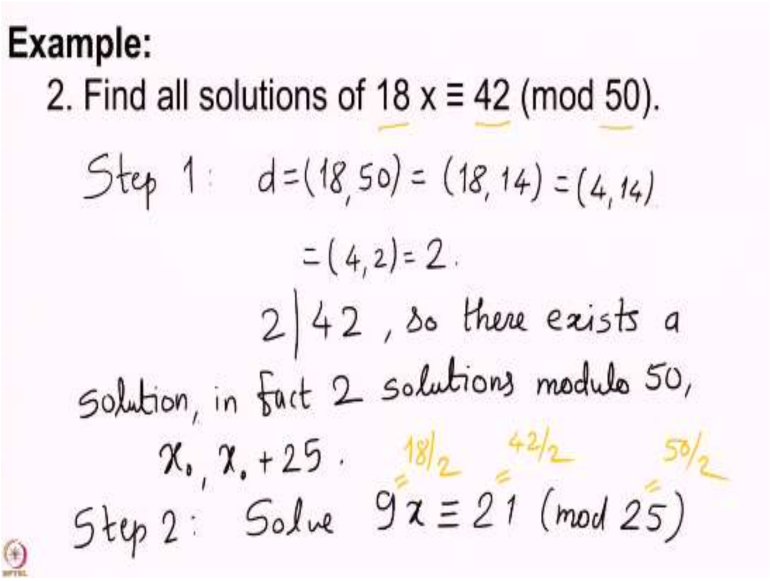
And then we come to step 2 which is to solve for a by d x congruent to b by d modulo the smaller congruence now n by d and having done this the number of solutions has changed because earlier we had d solutions and now because the GCD of a by d and n by d is 1. Here we are now going to get a unique solution so this implies unique solution whereas in the earlier case here we will have d solutions.

So that is one small thing that we need to take care. Now we want to know how to reduce the coefficient of x further and I told you that this can be done by cancelling out anything which is there in the coefficient of a so you can look at am x congruent to b by m x mod n, solutions to this are related to solutions to ax congruent to b mod n. This is our second step we proved this was the second lemma which we proved in the last lecture.

That even if you have the GCD of a and bn to be 1 so that you cannot reduce the modulus further the modulus of the congruence which is then that cannot be reduced because now the GCD of a and n is 1 you cannot divide by the GCD, the GCD is not more than 1.

So the modulus does not reduce, but you can still reduce the coefficient of x and the congruence so that is something that we can do, but there is one more method plus 1 more method which we will hopefully see in the next equation.

(Refer Slide Time: 03:48)



Example:

2. Find all solutions of $\underline{18}\,x \equiv \underline{42} \pmod{\underline{50}}$.

Step 1: $d=(18,50)=(18,14)=(4,14)$

$=(4,2)=2.$

$2 \mid 42$, so there exists a solution, in fact 2 solutions modulo 50,

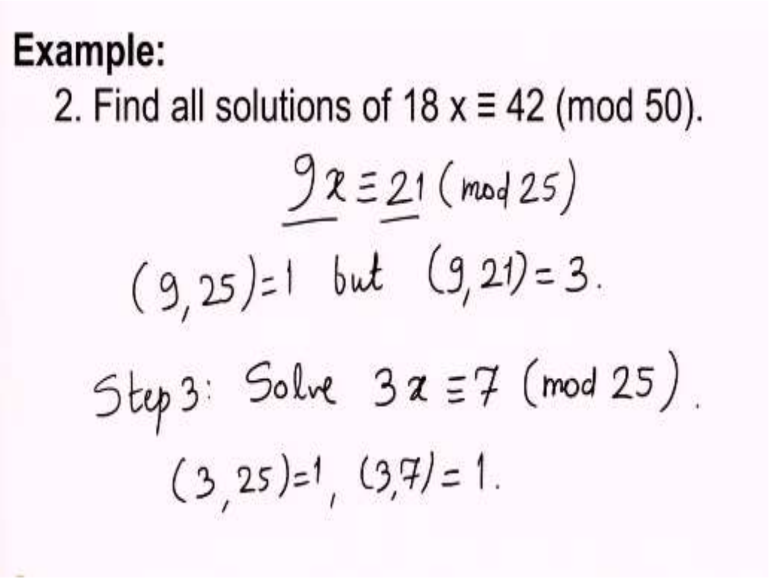
$x_0,\ x_0+25.$

Step 2: Solve $\overset{18/2}{9}x \equiv \overset{42/2}{21} \pmod{\overset{50/2}{25}}$

So let us go towards solving this. We want to solve 18 x congruent to 42 modulo 50. So the GCD here is 2 as we can see so step 1 tells us that the GCD of 18 and 50 you can cancel out the multiples of 18 from 50. So that will give you 18 and 14 because 18 into 2 is 36 once you remove 36 from 50 you are left with 14. This is same as 4, 14 which is same as 4, 2 and therefore the GCD is 2.

Here, 2 divides 42 so there exist a solution in fact 2 solutions modulo 50 this will be x0 and x0 plus 25 and now we apply step 2 to cancel thus this GCD which is 2. So we will solve 9x congruent to 21 modulo 25. We have divided by 2 to all the coefficients remember 9 is 18 upon 2 this was 18. 21 is 42 divided by 2 here we have 42 and 25 is 50 by 2 here we have 50. So we want to now solve for 9x congruent to 21 modulo 25.

(Refer Slide Time: 06:13)



Example:

2. Find all solutions of $18 x \equiv 42 \pmod{50}$.

$$\underline{9}x \equiv \underline{21} \pmod{25}$$

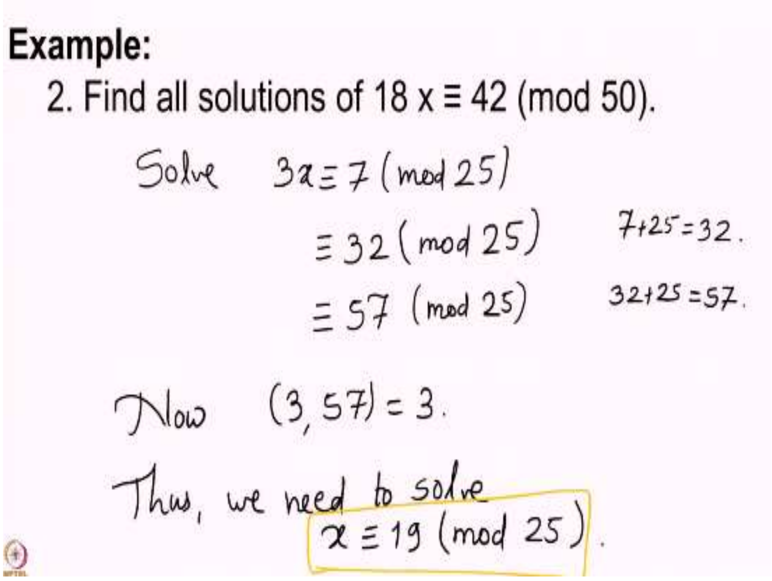
$(9,25)=1$ but $(9,21)=3$.

Step 3: Solve $3x \equiv 7 \pmod{25}$.

$(3,25)=1$, $(3,7)=1$.

The GCD of 9 and 25 now is 1, but 9 and 21 have a non-trivial GCD which is 3. So this can be still cancelled out from the coefficients of x and the constant term and thus we get 3x congruent to 7 modulo 25 so we have reached up to this level. Here now the GCD of 3, 25 is 1, the GCD of 3,7 is also 1 so no further numbers can be cancelled and therefore what we do is apply a small trick. So this is how that small trick goes.

(Refer Slide Time: 07:26)



Example:

2. Find all solutions of $18 x \equiv 42 \pmod{50}$.

Solve $3x \equiv 7 \pmod{25}$

$\equiv 32 \pmod{25}$ $7+25=32$.

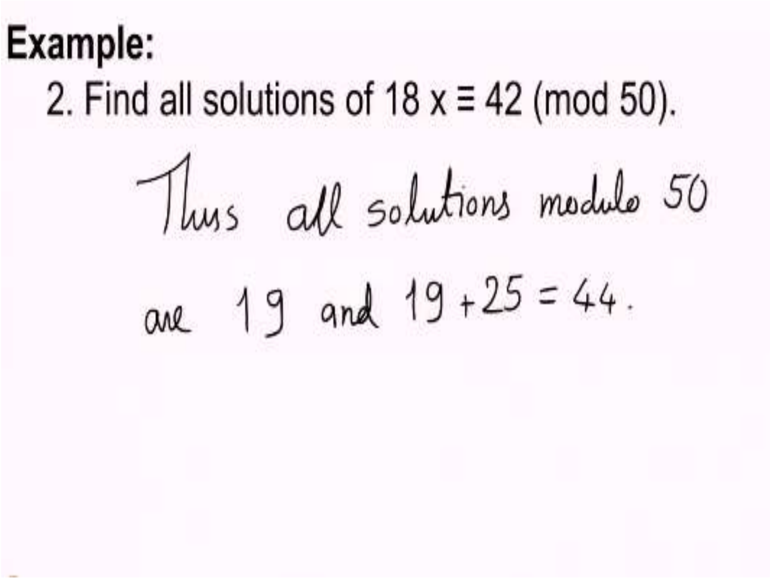
$\equiv 57 \pmod{25}$ $32+25=57$.

Now $(3,57)=3$.

Thus, we need to solve $\boxed{x \equiv 19 \pmod{25}}$.

Solve 3x congruent to 7 mod 25, but 7 is small thing as 32 mod 25 because 7 plus 25 is 32. We still do not have the GCD of 3 and 32 to be bigger than 1. So I will add 25 to this further to obtain 57 because we have 32 plus 25 is 57. Now the GCD of 3 and 57 is 3 we can cancel this and thus we need to solve x congruent to 19 mod 25, but there is nothing to solve here this is itself our solution. So, we obtain the solution x congruent to 19 mod 25. And as I pointed out to you when we proved those lemmas that this solution is not going to change.

(Refer Slide Time: 08:55)



Example:

2. Find all solutions of $18x \equiv 42 \pmod{50}$.

Thus all solutions modulo 50 are 19 and $19 + 25 = 44$.

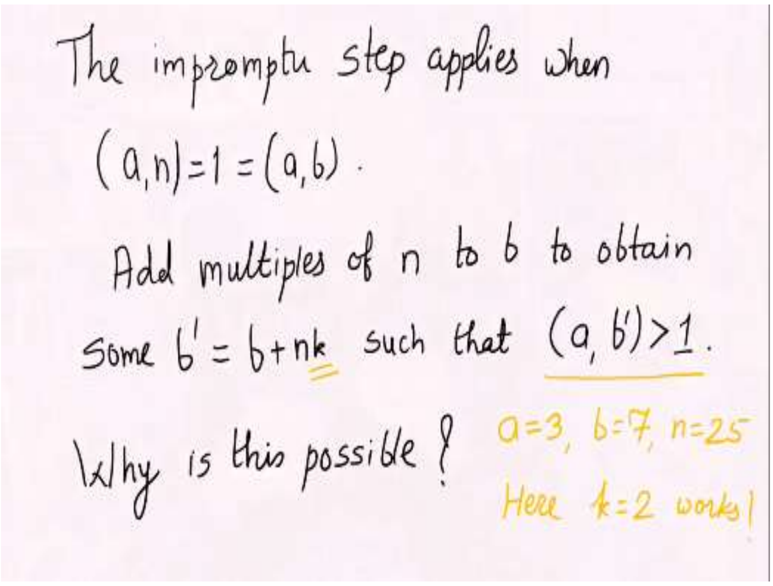
So, all solutions modulo 50 are 19 and 19 plus 25 which is 44. So we had in our algorithm 3 steps. The first step was to check whether the GCD divided the constant term which is b the second step was then to cancel out the GCD so you would be left with a prime x congruent to b prime modulo n prime. The third step was to see and try to cancel out common terms from a prime and b prime.

So you have now that the coefficient of x which we call a prime and n prime they have GCD is equal to 1 because the earlier GCD of a and n has now been cancelled. So there is no further GCD and therefore you cannot cancel terms from all the three. However you can cancel still try to cancel terms from the constant term and the coefficient of x.

And the next step would be where all the GCDs are 1 you have the GCD of a and n is equal to 1, you have the GCD of a and b equal to 1 and still so then ofcourse there are 2 options you can try to invert a. Once you have the possibility of inverting a then you can simply multiply by the inverse of a to b and that will give you a solution or another way is to keep adding n to b so that the GCD of a and some b plus n times alpha becomes more than 1.

Reduce that GCD again by cancelling out the GCD from the coefficient of x and the constant term and proceed. So we will just note down this extra step.

(Refer Slide Time: 11:23)



The impromptu step applies when

$(a,n)=1=(a,b)$.

Add multiples of n to b to obtain

some $b'=b+n\underline{\underline{k}}$ such that $\underline{(a,b')>1}$.

Why is this possible? $a=3$, $b=7$, $n=25$

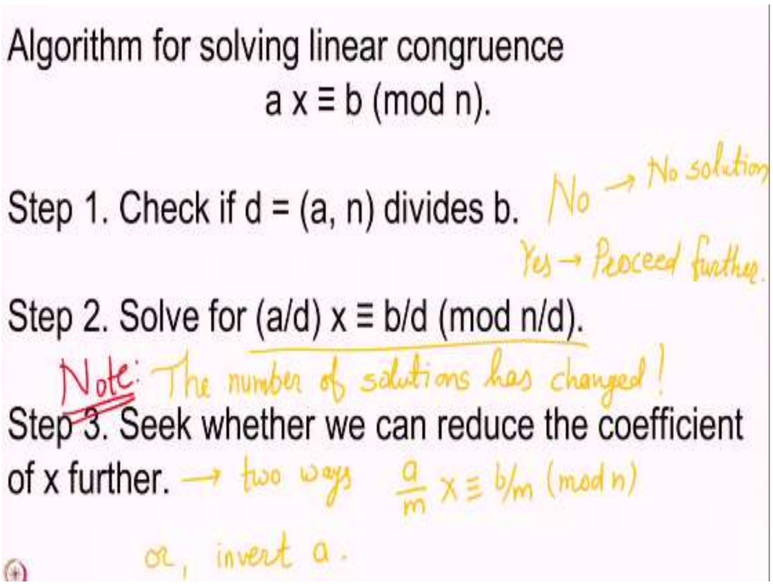
Here $k=2$ works!

So the impromptu step applies when you have that GCD of a, n is 1 and the GCD of a, b is 1 and the step is that add multiples of n to b to obtain some b prime which is b plus n into k such that the GCD of a and b prime is now bigger than 1, but whenever we apply any such step we should be able to prove that this is possible. So the question is why is this possible that means why should you be able to find this k.

Such that you get the corresponding b prime and the GCD of a and b prime is bigger than 1. We saw it in the last example where we had 3 and 7 modulo 25 we added 25 into 2 which was 50 to 7 to obtain 57 and that give us the answer. So a is 3, b is 7 and n is 25 here k equal to 2 works, but why should such a k exist in general? This is going to be part of the exercise sheets that I am going to circulate.

So I will not explain this to you at this moment, but this is not a very difficult thing this is simply playing around with the earlier theme on primes that we have developed quite a lot and that will help you in solving this.

(Refer Slide Time: 13:57)



Algorithm for solving linear congruence

$a\,x \equiv b \pmod{n}$.

Step 1. Check if d = (a, n) divides b. No → No solution

Yes → Proceed further.

Step 2. Solve for $(a/d)\,x \equiv b/d \pmod{n/d}$.

Note: The number of solutions has changed!

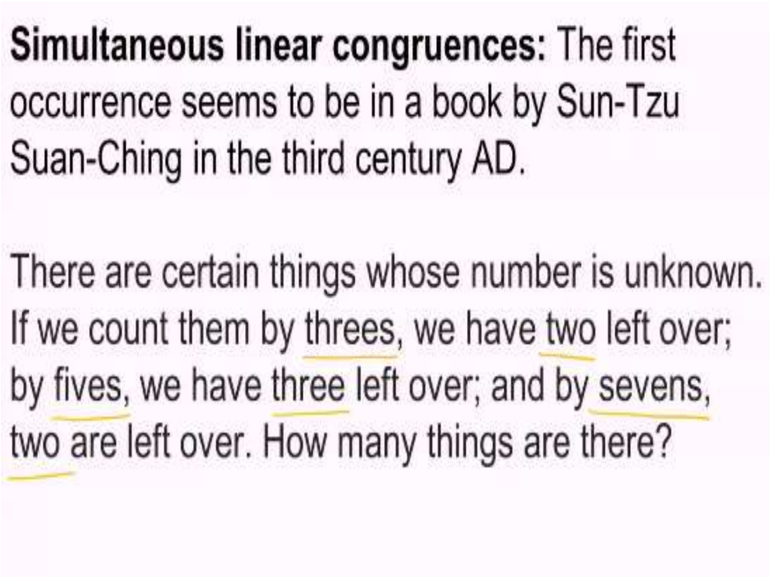
Step 3. Seek whether we can reduce the coefficient of x further. → two ways $\frac{a}{m} x \equiv b/m \pmod{n}$

or, invert a.

So we have this algorithm once again for your reference check if the d which is the GCD of a and n divides b no means no solutions yes then proceed further then you solve for a prime x congruent to b prime mod n prime and this can be done in two ways a by m x congruent to b by m mod n or invert a and these are the steps of the algorithm which will definitely help you solving any linear congruence provided of course that there is a solution.

You should always check that after applying for this the number of solutions has changed this is something that you should always note, this is something that you should note and so we put it in the red ink.

(Refer Slide Time: 15:46)



Simultaneous linear congruences: The first occurrence seems to be in a book by Sun-Tzu Suan-Ching in the third century AD.

There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?

Alright, so now next thing that we want to do after having obtained a condition for solving linear congruence is the following thing that we would like to solve for simultaneous linear congruences. We are looking for solutions to simultaneous linear congruences, but with a small thing that to begin with we are going to keep the coefficient of x to be equal to 1. So it will solve two things it will tell us that the GCD is 1 and therefore there are always solutions.

And it will also tell you the second thing that because the GCD is 1 there is a unique solution. So we will not have to worry about the non-existence of solutions and we will also not have to worry about multiple solutions. So as the mathematics keeps developing the subject of history of mathematics also keeps developing and one wonders what was the time when a particular thing was studied first or who was the person where the particular thing was studied first.

Often there is some tradition to hold a particular time to be the first time when something is studied and then people realize that this was studied much before that and then one has to correct the history and perhaps go on correcting history for some time. So for this the theorem that we are going to talk about is called the Chinese remainder theorem and this is called the Chinese remainder theorem because it was studied for the first time as the history tells us now in China during the third century AD.

So, the first occurrence of this seems to be in a book by this Chinese mathematician Sun-Tzu Suan-Ching in the third century AD. It was a very nice delightful book there are lots of parallels that we should see here. So in India we know that Bhaskaracharya had written Lilavati which was basically a collection of problems.

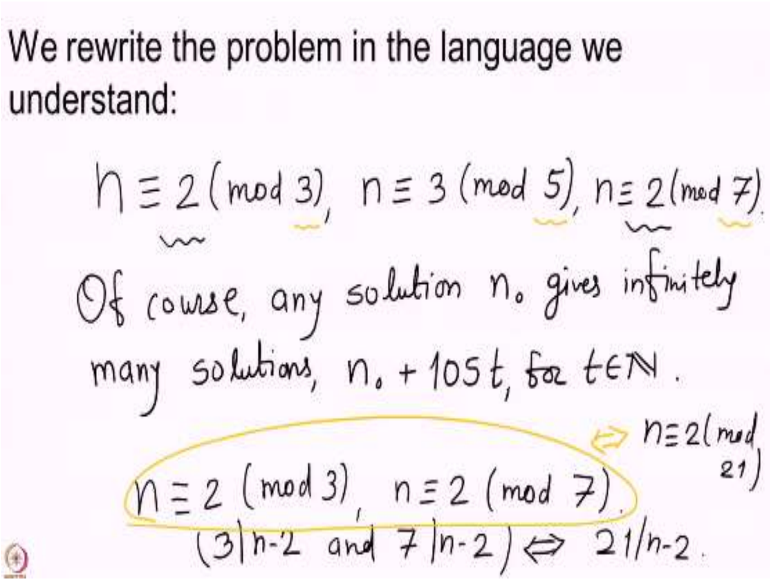
And the solutions to these problems led to various theories on how to solve this problems. So, there were problems of similar types, there were methods describe to solve this problems and so we learnt new methods. Similarly, this book by Sun-Tzu Suan-Ching had a problem which reads as follows. So, the problem says that there are certain things whose number is unknown so you have n things.

If we count them by threes we have two left over. So when you partition the number n in groups of threes there will be two which are left over. So n is a multiple of 3 plus 2 or n is congruent to 2 mod 3 this is what we would say in our current language. If you group them by 5 then there are three left over so that means n when partitioned in the groups of 5 three things are left over.

Which means that n is a multiple of 5 plus 3 or n is congruent to 3 modulo 5 and when you do it by 7s then two are left over that means when you try to partition n in the groups of 7 after having done after having separated some groups of 7 two things will be left over. So n is a multiple of 7 plus 2 or that n is congruent to 2 mod 7 then Sun-Tzu asked how many things are there?

So this is the problem that is pretty well defined. What we need to do is to convert this problem in the language that we understand better. So we read the problem again and try to take out the information that is of importance to us. When you count it by 3, 2 are left over so it is 2 mod 3 when you count it by 5, 3 are left over so this is 3 mod 5 and when you do it by 7 again 2 are left over.

(Refer Slide Time: 20:29)



We rewrite the problem in the language we understand:

$n \equiv 2 \pmod{3}$, $n \equiv 3 \pmod{5}$, $n \equiv 2 \pmod{7}$.

Of course, any solution n_0 gives infinitely many solutions, $n_0 + 105t$, for $t \in \mathbb{N}$.

$n \equiv 2 \pmod{3}$, $n \equiv 2 \pmod{7}$ $\Leftrightarrow$ $n \equiv 2 \pmod{21}$

$(3 | n-2$ and $7 | n-2) \Leftrightarrow 21 | n-2$.

And we use this to write the problem in the language that we understand. So, we have n is congruent to 2 mod 3 n is congruent to 3 mod 5 and n is congruent to 2 mod 7 and then Sun-Tzu asked what is the number n. So of course any solution n0 gives infinitely many solutions, how? We just take the product of 3 and 5 which is 15 and multiplied by 7 to get 105. So the moment you have a solution n0 adding any multiple of 105 will give you a solution.

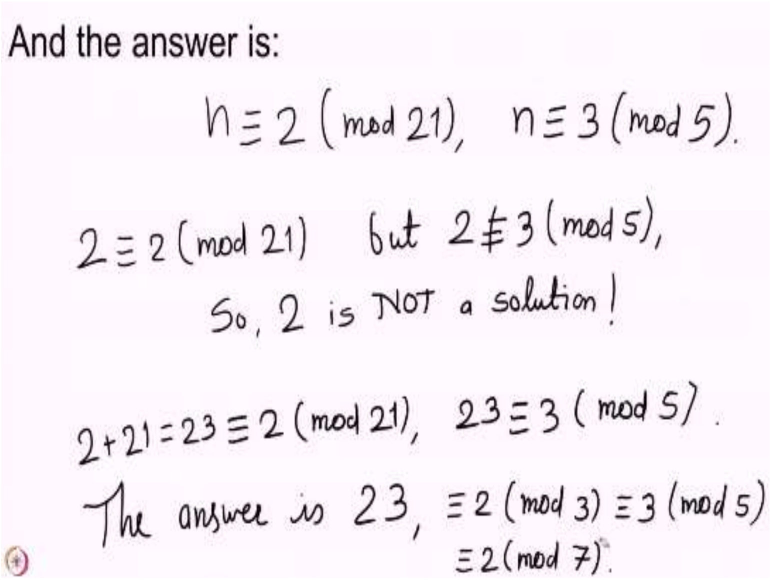
Because n0 and any multiple of 105 are going to be congruent modulo 105, but if you have two numbers a and b then a and b are congruent modulo n if and only if a and b are congruent modulo pi power ni where you have the prime factorization of 100 n as product of pi power ni this was the result which we have proved some lectures back. So the numbers n0 and n0 plus 105 p are going to be congruent to each other mod 105.

And therefore they are congruent to each other modulo 3, modulo 5 and modulo 7 that means you have one more solution to the problem which was proposed by Sun-Tzu. Now we want to solve this. So solving such a problem actually requires a method, but in some very special cases one may still be able to solve this problem in the following way. So here we observe that there is a same congruence modulo 2 moduli.

So n is 2 mod 3 and n is 2 mod 7 what does it give us? So because n is congruent to 2 mod 3 and n is congruent to 2 mod 7 it tells us that 3 divides n minus 2 and 7 divides n minus 2. So we have 3 divides n minus 2 and 7 divides n minus 2. Now this will occur if and only if we have 21 divides n minus 2. So what we have done is to replace these two congruences by one single congruence which is that n is congruent to 2 mod 21.

So the three congruences that we had first are now reduced to two congruences n is congruent to 3 mod 5 and n is congruent to 2 mod 21. We will now solve this.

(Refer Slide Time: 24:40)



And the answer is:

$$n \equiv 2 \pmod{21}, \quad n \equiv 3 \pmod{5}.$$

$2 \equiv 2 \pmod{21}$ but $2 \not\equiv 3 \pmod{5}$,

So, 2 is NOT a solution!

$$2+21=23 \equiv 2 \pmod{21}, \quad 23 \equiv 3 \pmod{5}.$$

The answer is 23, $\equiv 2 \pmod{3} \equiv 3 \pmod{5}$

$\equiv 2 \pmod{7}$.

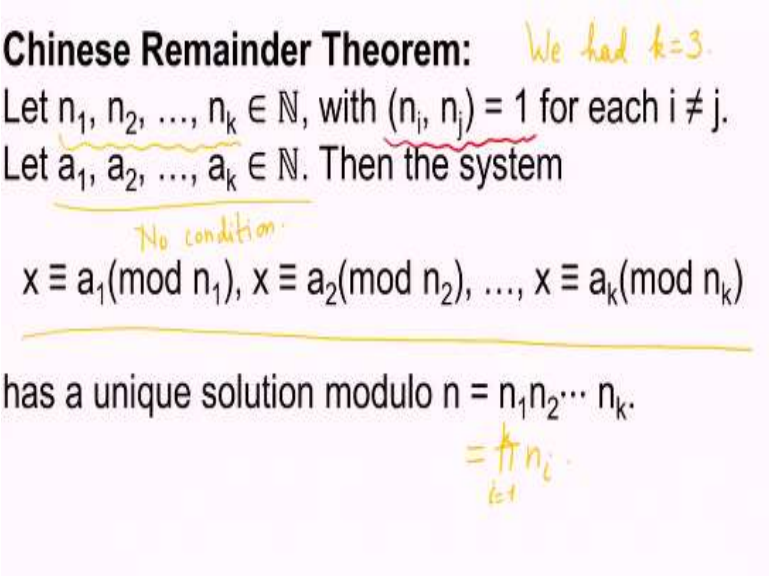
So let us just go over the things which are 2 mod 21 so 2 is 2 mod 21, but 2 is not congruent to 3 mod 5 so 2 is not a solution. Let us add 21 to 2 so 2 plus 21 which is 23. This is congruent to 2 modulo 21 and as luck would have it we have that 23 is also congruent to 3 modulo 5. So all our congruences are satisfied so the answer is 23 check that this is 2 modulo 3.

This is congruent to 3 modulo 5 and that this is congruent to 2 modulo 7 23 is 21 plus 2 therefore it is 2 mod 3 it is 20 plus 3 therefore this is 3 mod 5 and it is 21 plus 2 once again so it is 2 mod 7. This was an impromptu method to solve this very special equation, but we need a result which will guarantee that whenever we have these things there is always a solution. So what was one special thing here?

We had 2 mod 3 and 2 mod 7 and immediately we jumped to 2 mod 21. The reason for that was that 3 and 7 were co-prime there was no common prime factor for 3 and 7. Similarly, the third modulus was 5 and so all these three 5 and 7 these are all relatively prime to each other what are known as pairwise relatively prime. If you took 2 and 3 if you took 3 and 5 the GCD is 1, 5 and 7 GCD is 1 and finally 3 and 7 the GCD is 1.

So whenever we have such pairwise relatively co-prime numbers there is a guarantee that there will be solution and this solution will be unique modulo the number n which is product of all this moduli. So let us see the statement of this result.

(Refer Slide Time: 28:10)



Chinese Remainder Theorem: We had $k=3$.

Let $n_1, n_2, \ldots, n_k \in \mathbb{N}$, with $(n_i, n_j) = 1$ for each $i \neq j$.

Let $a_1, a_2, \ldots, a_k \in \mathbb{N}$. Then the system

No condition.

$$x \equiv a_1 (\text{mod } n_1),\ x \equiv a_2 (\text{mod } n_2),\ \ldots,\ x \equiv a_k (\text{mod } n_k)$$

has a unique solution modulo $n = n_1 n_2 \cdots n_k$.

$= \prod_{i=1} n_i$.

So this is called the Chinese remainder theorem. The statement says that we start with any k natural numbers n1, n2 up to nk and so there is no restriction on what k can be, in our problem we had k equal to 3. The only condition and that is a very important condition is that the ni and nj be coprime whenever you have i not equal to j.

So whenever i is not equal to j the numbers ni and nj are relatively prime. So n1, n2, n1, n3, n1, n4 all the way up to n1 nk then n2, n3, n2, n4 again all the way up to n2 nk and so on up to nk minus 1 nk. So all these pairs should give you pairs of relatively prime integers which means that there is no common factor between any two of these chosen ni. Once you have this take any natural numbers a1, a2, ak there is no condition on these.

Then this system x congruent to a1 mod n1 x congruent to a2 mod n2 so on up to x congruent to ak mod nk has a unique solution modulo the number n which is product of all these ni. So we will need to prove that there is a solution in the natural numbers and we will further prove that this solution is unique modulo this n. We will see this proof in the next lecture so I hope to see you, bye until then.