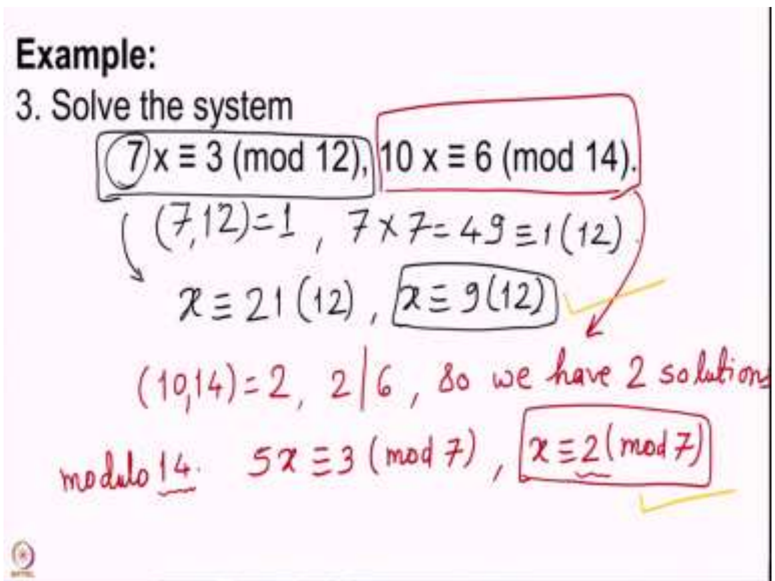
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 19
Chinese Remainder Theorem, more examples

Welcome back. In our last lecture we proved the Chinese Remainder Theorem and then did two very basic examples where we solved the systems of simultaneous linear congruences using the Chinese remainder theorem. Ofcourse now we are going to do some problems where we have the systems are slightly different, we cannot readily apply the Chinese remainder theorem, but we can modify the systems slightly so that we can then apply the CRT.

(Refer Slide Time: 00:53)



So the very first system that we would have is the next one, since we have done problems 1 and 2 in the previous lecture, to have continuity we will name this as problem number 3. So this problem is 7x congruent to 3 mod 12 and 10x congruent to 6 mod 14. If you have attended all my lectures up to now and if you remember the examples which we have done, after seeing how we can solve one linear congruence, then you will realize that these two are the ones which we have already solved there.

And you may also perhaps remember the answers to these two. So remember or note here that the moduli are not co-prime to each other. We have one modulus is 12 and another modulus is 14, so we cannot on the nose apply the Chinese remainder theorem, we will have to modify the systems and see whether the modified systems have the possibility of applying the Chinese remainder theorem. So how do we go about it? Let us work each of these two linear congruences separately and see what we get.

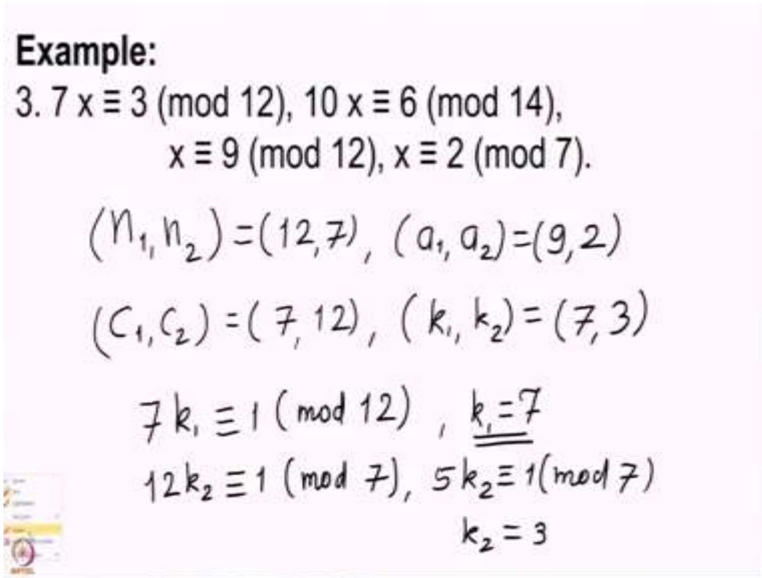
So in the very first we see that 7 and 12 are co-prime, so here we have that 7 and 12 are co-prime and therefore this system does have a unique solution modulo 12. And thus unique solution is obtained by simply multiplying by the inverse of 7 to the left hand side. So when I apply the inverse of 7, what is the inverse of 7 modulo 12? Again this is something that we have done, the inverse of 7 is 7 itself. So you have 7 into 7 which is 47 and this is 1 modulo 12.

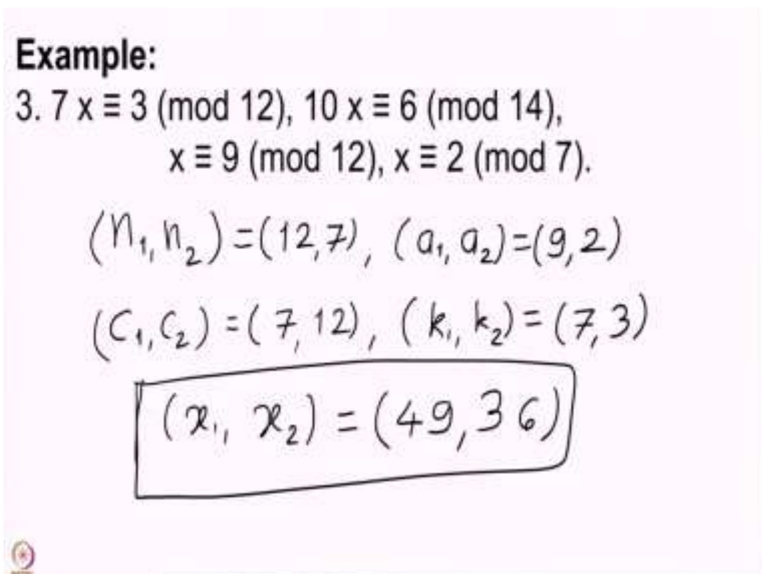
So the first equation will convert to x congruent to I multiply by 7 to 3 because 7 is the inverse of 7. So I get 21 modulo 12 or it is actually 9 modulo 12. This is the solution to the first system. Now we look at the second one and perhaps it would be better if I use a different (chalk), different ink for this so to solve the second one, we note that the GCD of 10 and 14 is 2 and 2 does divide 6, so we have two solutions, modulo 14.

And those two solutions if you, so the next thing would be to cancel 2 from all these three numbers, so we are left with 5x congruent to 3 mod 7 and then we see that x congruent to 2 mod 7 is the answer to this. So the, there are 2 solutions indeed but they are modulo 14 and therefore modulo 7 there is only one solution which is 2 mod 7, modulo 14 the solutions would be 2 and 9, but modulo 7 there is only one solution.

So this is the system which is equivalent to the system that we have here and this is the linear congruence, which is equivalent to the linear congruence which we have here. So the two linear congruences that we should now solve are 9 mod 12 and 2 mod 7, these are the things which we should solve.

(Refer Slide Time: 04:58)

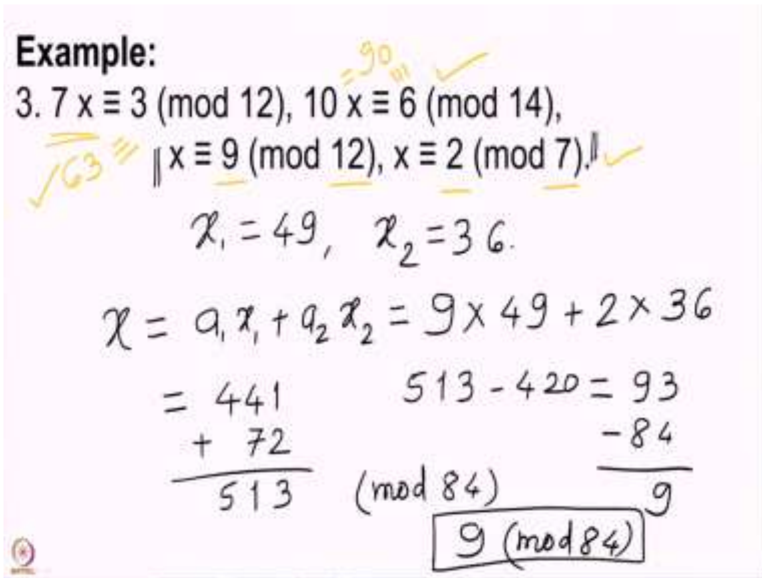




Indeed, that is what we have here in the next slide, we should solve 9 modulo 12 and 2 modulo 7 and this actually is quite easy we should just write what is our n1, n2 these are 12 and 7, our a1, a2 are 9 and 2; c1, c2 are nothing n2, n1 and now I want to compute k1, k2. What would be k1? K1 should have the property that when I multiply by 7 to k1, I get 1 modulo 12. But, so I want to compute the inverse of 7 modulo 12 and this is something that we have already done in the last slide, k1 is 7 itself.

There would be a unique such and k2 will have the property that we should have 12 k2 congruent to 1 mod 7 or which is the same thing as saying 5k2 congruent to 1 mod 7. And so we have to compute the inverse of 5 modulo 7 and that is simply 3, so k2 is 3. Once we have computed these, let me erase these computations that we done here so that we can use the same slide to do further computations namely x1 and x2. And if you remember x1 is c1k1, x2 is c2k2; so x1, x2 are c1k1 so that is 49 and x2 is c2k2 which is 36. These are the most important numbers which we need to solve the equation 49 and 36.

(Refer Slide Time: 07:16)



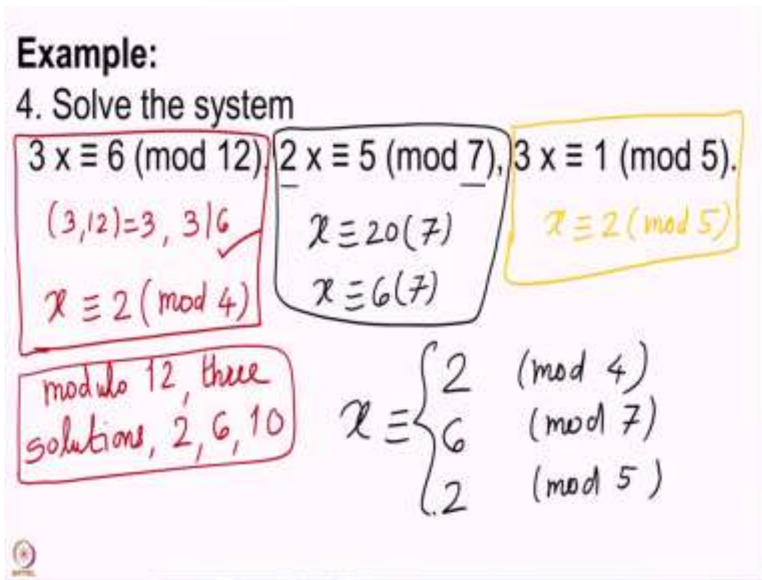
And then to solve the general equation we should take a1x1 plus a2x2, so a1 is 9 we should look at 9 into 49 plus 2 into 36. So 9 into 49 is 490 minus 49, so 490 minus 50 is 440 add 1, we get 441 and then we add 72, which is 36 into 2. So we get 3, 1 and 5, so our answer is 513 but we need to go modulo 84 which is the LCM of 12 and 7.

So when we need to go modulo 84 you can readily subtract 520 from 413, so that will give us 93 and then you subtract 84 from here to get 9. So our answer should be 9 modulo 84, is that really the answer? Let us check it. So when we go modulo we do get 9, after all 9 is 9 modulo 12. And when you go modulo 7, you do get 2 because 9 is also 2 mod 7.

But this is about this congruence, what about this congruence? When I multiply 9 by 7 we get 63 which is indeed 3 mod 12, so this is alright. And when you multiply 9 by 10 you get 90 which is also 6 modulo 14, so this is also okay. So thus we have been able to solve this different looking system by first modifying it to a system where we can apply the Chinese remainder theorem. And then we applied Chinese remainder theorem to obtain the solution.

Once again what are the systems where we can apply Chinese remainder theorem? The systems should have that they moduli be all pair wise co-prime and furthermore an important thing in case if you have not noticed it until now is that the coefficients of x is always 1. You are not allowed to have any different coefficient, if there is a different coefficient, try to cancel out the GCD or try to multiply by the inverse of that coefficient modulo your number so that you have the coefficient to be 1. This is an important thing.

(Refer Slide Time: 10:44)



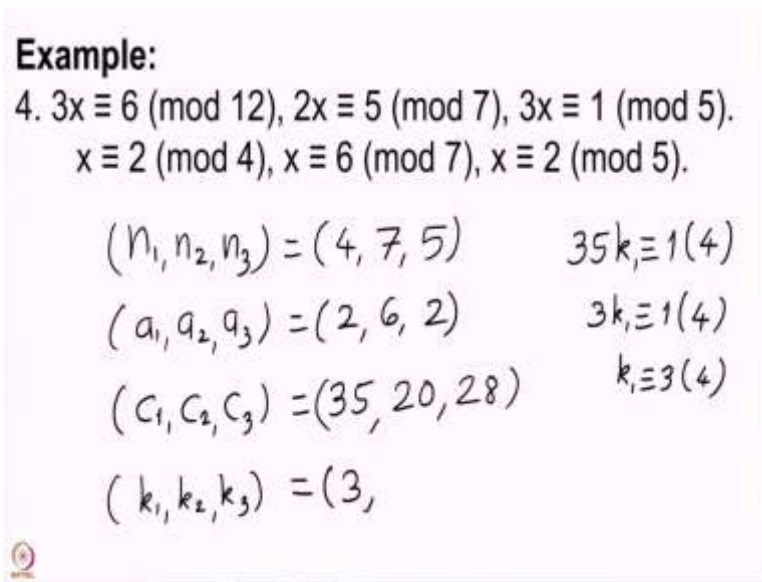
So having solved this third problem, let us go to the next problem which is slightly more complicated, because here all the three systems are with coefficients of x not equal to 1. So we need to convert this into systems where the coefficients of x are 1 and for that we have to simply compute either the inverses which we can do here, the inverse of 2 modulo 7 is 4, 2 into 4 is 8, so I multiply by 4 to get x congruent to 20 mod 7 and 20 is nothing but 6 modulo 7.

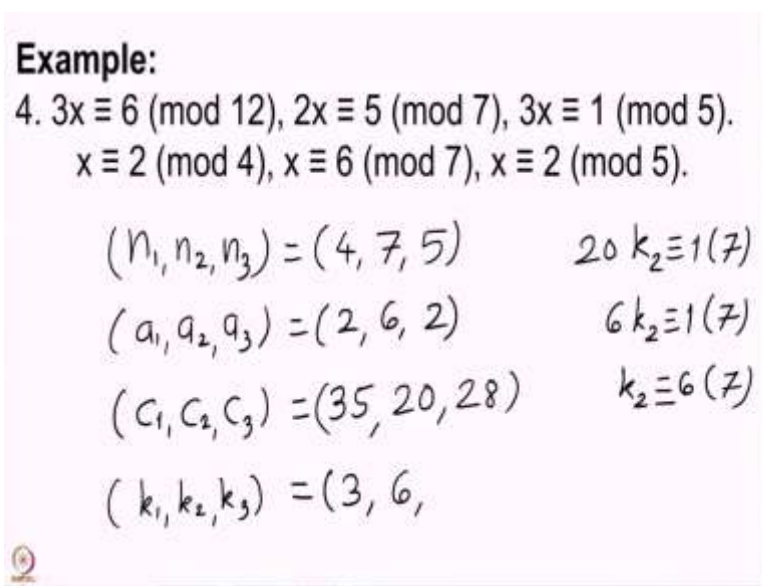
So this system is same as this system, we have these three are equivalent, then I change my color of the ink and go to the next one. I am not coming here because here we do not have quite that the inverse of 3 modulo 12, we will have to cancel out the GCDs. So I will come to this again, but for the moment I can cancel the GCD here, I can cancel 3 modulo 5 by multiplying by 2 on both sides. So here we get x is congruent to 2 mod 5 which is consistent with this system.

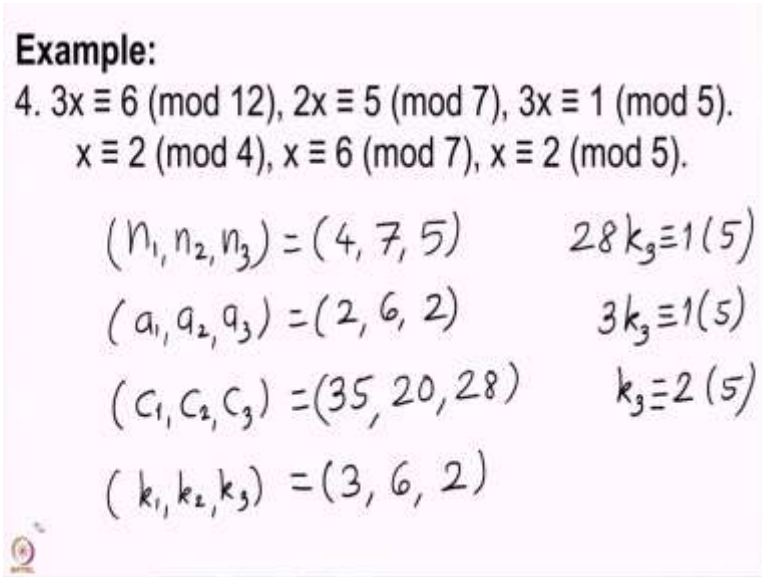
And now we come finally to the system that we have here, so by cancelling out GCD, the GCD of 3 and 12 is 3 and 3 divides 6, so we are okay. We cancel GCD to get x congruent to 2 mod 4, this is the system that is consistent with this system. So modulo 12, we are going to get three solutions, namely 2, 6 and 10. You can quickly check that when you multiply 2 by 3, we do get 6. Next you can check that when you multiply to 6 by 3 you get 18, which is also 6 modulo 12 and finally you check that when you multiply 10 by 3, you get 30, which is also 6 modulo 12.

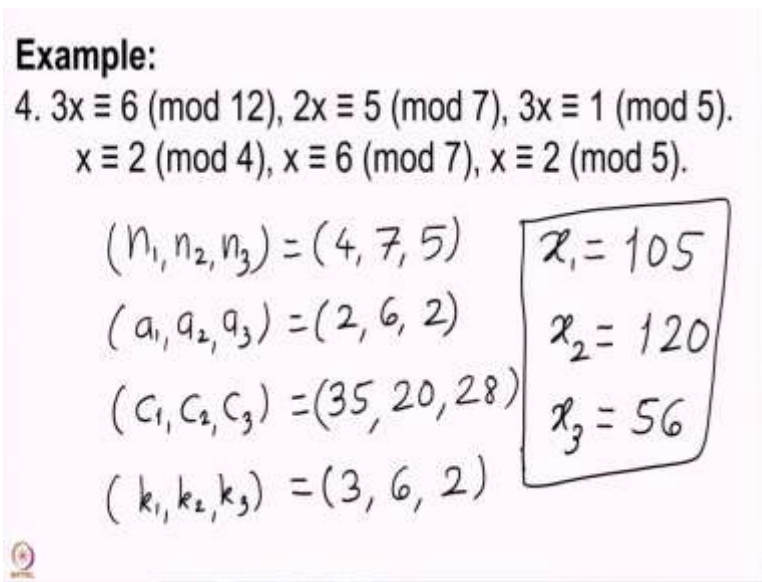
So nevertheless, what is important for us is that we have converted these three systems into these other three systems and those are the ones that we need to remember, so they are 2 mod 4, 6 mod 7 and 2 mod 5. And these are the three systems that we now we have to solve, so 2 mod 4, 6 mod 7 and 2 mod 5.

(Refer Slide Time: 14:01)









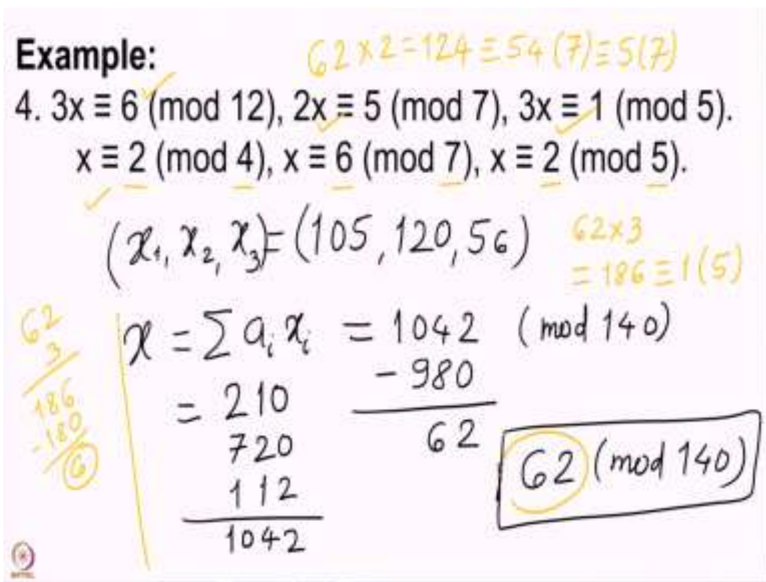
That is what we have here 2 mod 4, 6 mod 7 and 2 mod 5, so by now we are quite expert in solving systems like this. Let us compute n1, n2, n3 here quickly, these are given 4, 7 and 5. A1, a2, a3 are 2, 6 and 2 and then we compute c1, c2, c3; c1 is the product of n2n3 so this is 35, c2 is the product of n1n3 so this is 20 and c3 is the product of n1n2 so we get 28.

Now from here I want to compute k1, k2, k3; k1 should have the property that 35k1 should be 1 modulo 4. But modulo 4 35 is already 3, so we get the equation to be 3 k1 congruent to 1 mod 4 and so k1 is 3 modulo 4.

We next go and compute k2. k2 should have the property that 20 k2 should be congruent to 1 mod 7, 20 is 6, 6k2 should be congruent to 1 mod 7 and that then says that k2 is 6 modulo 7, because 6 into 6 is 36, which is 1 mod 7, so k2 is 6. And finally we need to compute k3, which should have the property that c3k3 be 1 modulo n3. c3 is 28, so 28 k3 should be 1 modulo 5, which means 3k3 has to be 1 modulo 5, which says that k3 should be equal to 2 mod 5. So we get that k3 is indeed equal to 2.

Now once we have computed the k3; k1, k2, k3 we need to compute x1, x2, x3. So k1, k2, k3 are nothing but 3, 6, 2 and x1 is the product of c1 and k1, therefore x1 is 35 into 3 so it is 105; x2 is 20 into 6 that is 120; x3 is 28 into 2 so that is 56. These are the three most important numbers that we need to remember for solving this system 105, 120 and 56.

(Refer Slide Time: 17:20)



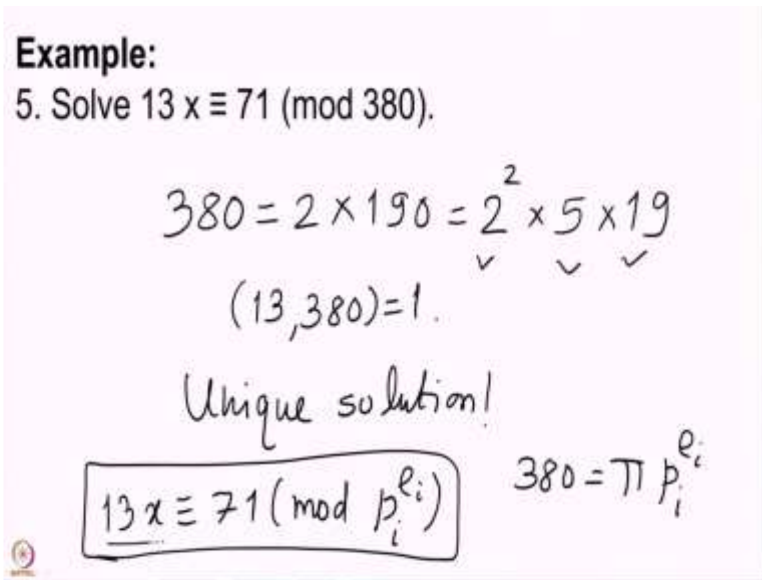
So the numbers are 105, 120 and 56, this is our x1, x2, x3 and to compute x finally which is summation ai xi. So 105 into 2 gives us 210, 120 into 6 that gives 720, 56 into 2 that gives 112. So the answer is 2, 4 and 10, so this is equal to 1042. But we need to go modulo 5 into 7 which is 35 into 4, 35 into 4 is 140. So if you once again remember your table of 14, 14 into 7 is 980.

So I can 14 into 7 is 98, so I can simply remove 980 from here to get 2 and here we get 6. So 62 modulo 140, this is the final answer that we get, so the answer, the smallest answer to the system is 62. Shall we quickly check whether this is indeed our solution? When we go mod 4 to 62, you remove 60 and indeed what you get is 2, when you go modulo 7, 62 is 56 plus 6, therefore modulo 7 62 is 6 and 62 modulo 5 is indeed 2, you will remove the 60 from 62 and what you are left with is 2.

Shall we also quickly check what happens when we do these computations? So if you have 62, you want to multiply to it by 3. So let me do it on one side here, 62 into 3 gives you 186 and you want to remove 12, multiples of 12 from that and indeed you can remove 180 itself to get 6 as the remainder modulo 12. We multiply 62 by 2, so 62 into 2 is 124 and when you want to remove multiples of 7, so modulo 7 124 is 54 which is indeed 5 modulo 7.

And finally we multiply to 62 by 3 to obtain that you have 186 and clearly this is 1 modulo 5. So all our congruences are satisfied, so our answer is indeed equal to 62. Time permitting, we will have one more problem and then we will go and see some of the more complicated problems. So the next problem I want you to think about is this problem.

(Refer Slide Time: 20:46)

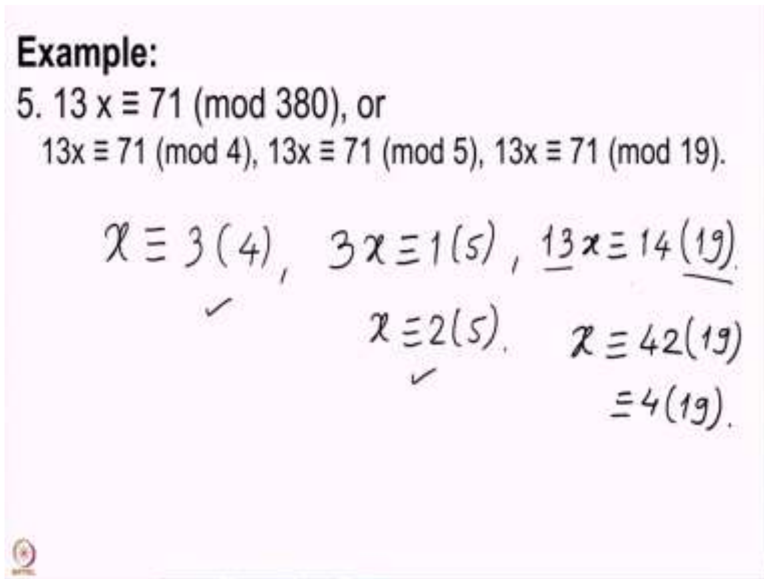


Here we have a single congruence, we do not have a system of simultaneous congruences but a single linear congruence, 13x congruent to 71 modulo 380. To be able to apply the Chinese remainder theorem, meaning you know of course you can try to invert, you know what we observe here readily is that 380 is 2 into 190 and therefore 2 square into 95 which is nothing but 5 into 19.

So 13 and 380, they are co-prime, so we should have a unique solution modulo 380. But to compute this unique solution, we need to invert 13 modulo 380, which is a very difficult problem. So what we observe is that 13x congruent to 71 modulo 380 holds if and only if 13x congruent to 71 mod pi power ei holds where you have that 380 is product of pi power ei. So we need to solve this system of linear congruence modulo each of these three.

So we will have a single looking congruence but the modulus is going to change. And that is how we are going to get a system of simultaneous linear congruences.

(Refer Slide Time: 22:34)

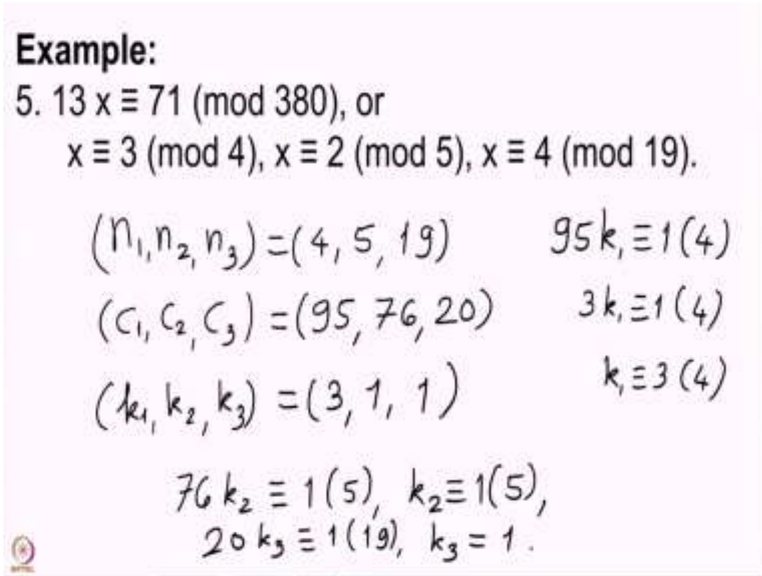


So this is what we have, we have 13x congruent to 71 modulo 4, modulo 5 and modulo 19. And this is the system that we will try to solve but we again observe that modulo 4 for instance your 13 is nothing but 1, 13 modulo 4 is 1. So here you have x congruent to 71 is 3, so 3 mod 4, modulo 5 we write this as 3x congruent to 1 mod 5 and modulo 19 unfortunately 13 cannot be reduced, but you can reduce 71.

So observe that 19 into 4 is 76, therefore 71 is either minus 5 or is equal to 14. So 3 mod 4, 3x congruent to 1 mod 5, so 3x congruent to 1 mod 5 can also be immediately written as x congruent to 2 mod 5. So 3 mod 4, 2 mod 5 and 13x congruent to 14 mod 19, this we should try to invert 13 now modulo 19.

So observe that 13 into 3 is 39 which is 1 mod 19, so we multiply both sides by 3 to get that x is congruent to 42 mod 19 which is 4 modulo 19. So our ultimate equation now becomes x congruent to 3 mod 4, x congruent to 2 mod 5 and x congruent to 4 mod 19. This is the system of simultaneous linear congruences that we would like to solve.

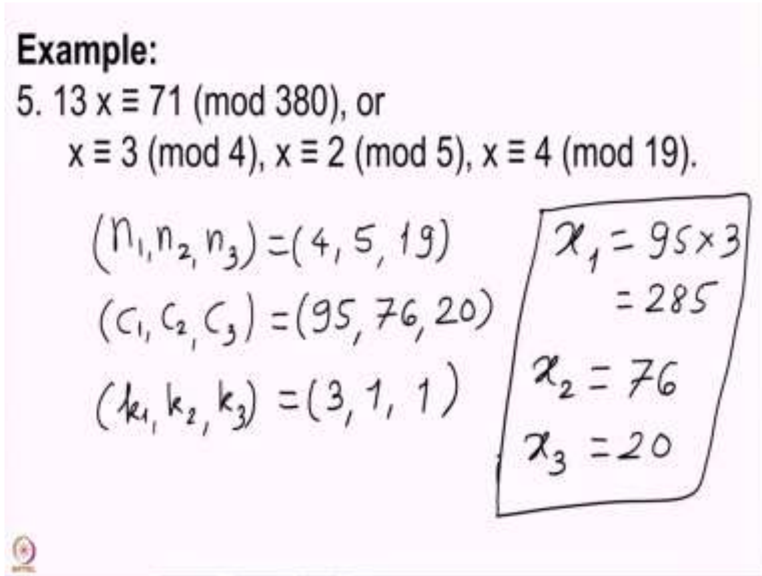
(Refer Slide Time: 24:23)



And the method is the same method. We compute n1, n2, n3; a1, a2, a3; c1, c2, c3; k1, k2, k3 which allow us to compute x1, x2, x3 and then we take summation ai xi to obtain the solution. So let us get going. We have n1, n2, n3 are 4, 5 and 19. We can perhaps immediately compute c1, c2, c3 because a1, a2, a3 will be required only towards the last step, c1 is the product of n2n3 so we get it to be 95, c2 is 19 into 4 that is 76 and c3 is 4 into 5 that is 20.

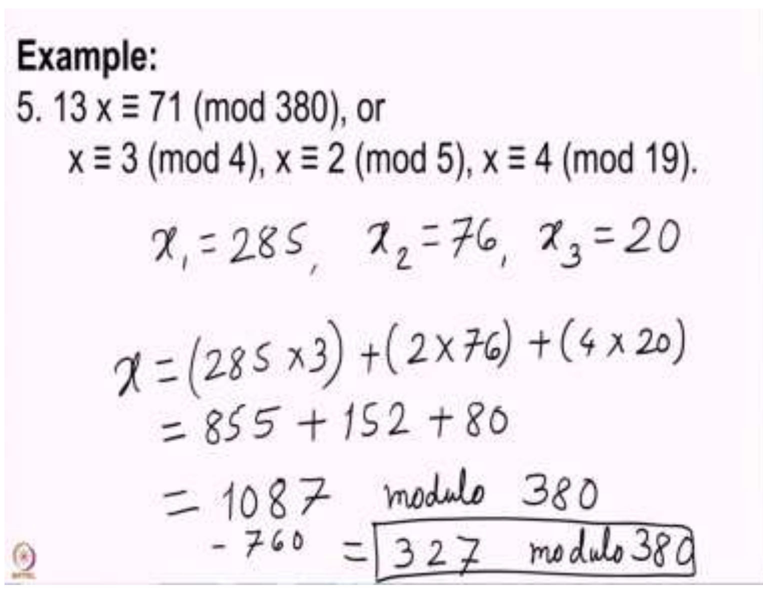
So now we have k1, k2, k3 with the property that c1k1 should be 1 mod n1 so 95 k1 needs to be 1 modulo 4, 95 is 3 so we have that 3k1 is 1 modulo 4 and therefore k1 is 3 modulo 4, so we get 3 here. Next we want to compute k2, so k2 should have the property that 76 k2 is congruent to 1 modulo 5, 76 itself is 1 modulo 5 so we get this to be k2 congruent to 1 modulo 5 and so what we get is k2 is 1 and for k3 we have that 20 k3 has to be 1 modulo 19 which tells us that k3 has to be equal to 1. So our c1k1, the products will give you what the xi are and let us write those products.

(Refer Slide Time: 26:50)



So we have x1 which is c1k1 95 into 3 which is nothing but 285, x2 is 76 into 1 that is simply 76 and x3 is simply 20. So these are the important things that we need to remember 285, 76 and 20.

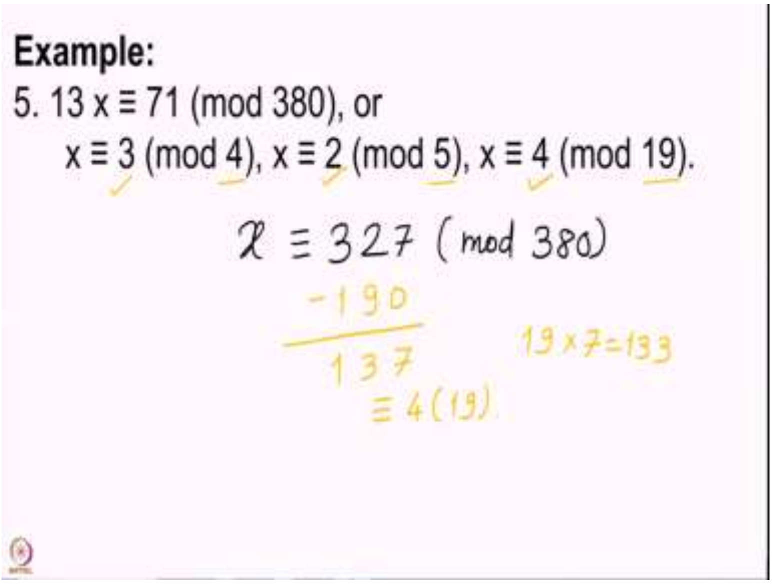
(Refer Slide Time: 27:24)



And our final solution is going to be a1xi, so I need to multiply to 285 by 3, then I need to multiply to 76 by 2 and in the end I multiply to 4 by 20. So here we have 5 into are 15 and 28 into 3 is 84, so we get 855 plus 76 into this is just 152 and here we get it to be 80. So the answer is going to be 5 plus 2 is 7, 5 plus 5 is 10 plus 8 is 18, so we write 8 and take 1 out, 8 plus 1 and then that 1 gives us 1087.

This is the ultimate answer but we have to go modulo 380 and so we observe here that 380 into 2 is 760. So I remove 760 from this to obtain 7, 2 and 3, so 327 modulo 380. This is the answer that we are getting 327 modulo 380.

(Refer Slide Time: 29:07)



Let us write the answer here and verify. So when we go modulo 4, we do verification with a different ink, when we go modulo 4, 327 is indeed 324 plus 3, therefore this is okay. When you go mod 5, you will remove 325 and what is left is 2, this is okay. Now we want to go modulo 19, so let us remove 190 first from here to get 137 and then we observe that 19 into 7 is 133. Therefore, this is congruent to 4 modulo 19. So indeed this is also okay.

Since we have the correct moduli, module, since we have the correct congruences, modulo each of the prime power factors of 380, we should have the correct answer for this thing also. I will leave it to you to check, what you need to do is take 327 multiply that by that 13, remove 71 and check whether the number that you get is a multiple of 380. Once we are done with this, we are more or less done with some routine problems to do with Chinese remainder theorem.

In the next lecture we will do one or two more problems which will lead to a theory for the part that we are going to develop later. So see you in the next lecture. Thank you.