Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 32
Chinese Remainder Theorem

We will talk about Rabin key cryptosystem which is based on the, what is called Chinese remainder theorem and the quadratic residue. So, before going to the Chinese remainder theorem, we want to see what is the, how to solve the system of linear equation modulo p.

(Refer Slide Time: 00:41)

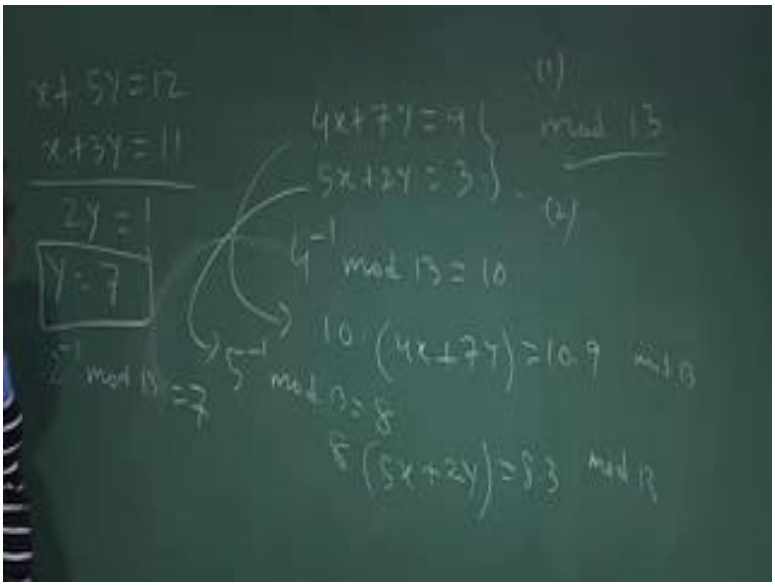
System of linear equation modulo some p or n, so, basically we have some system of linear equation say a 11 x 1 plus a 12 x 2, x 3, a 1a x n equal to b 1. This is first equation and the second equation is this a 22 x 2 plus dot, dot, dot, a 2n x n equal to b n dot, dot, dot, suppose there are n equations. So, am 1 x 1 plus into x 2 a mn x n equal to so, this is b 2 b m.

This is a system of equation; there is an equation in unknowns. So, this we can write in the matrix form as you know a 11, a 12, a 1n; a 21, a 22, a 2n; a m1, a m2, a mn and then this is the etcetera and corresponding we have b vector, the m equations and this is modulo n means we have taking each is each of a ij is coming from Z n, so and also b ij

is coming from Z n. So, we have to find the solution for this. So, we have to find x ij such that which is coming from Z n, we satisfy this system of equations.

That is the problem. So, to solve this, we know we have to check the rank of the augmented matrix is same as rank of the matrix. So, those are the concept there. So, let us take a simple example, how we can solve this type of system of linear equations modulo some prime. So, we will take an example.

(Refer Slide Time: 03:21)



Suppose we have this system 4x plus 7y equal to 9 and 5x plus 2y equal to 3 and we have to solve the system of equations modulo 13. So, our n is equal to let us see modulo 13.

How we can solve this system? So, we can multiply this by 4 inverse mod 13 and then so, this is equation number 1, equation number 2. So, basically 4 inverse mod 13 is basically how much? 10 because if you multiply 10 with 4 it is 40 then if you take the mod 13, it is 1. So, that is basically 10. So, we multiply this with this 10. So, this will be so 1 becomes x plus then this is 10 into 7. So, this is basically 10 into say so we multiply this equation by 10; that means 4 inverse mod 13. So, 10 into 4x plus 7y is equal to 10 into 9 and every operation is under mod 13 and similarly we know that 5 inverse mod 13 is how much? 5 inverse mod 13 is basically 8. So, what we do? So, then we multiply this equation by 8. So, 8 into 5x plus 2y is equal to 8 into 3 mod 13, every operation is under mod 13.

So, if we just multiply, this will be getting 2 equations x plus 5y equal to 12, this is coming from this equation and from here we are getting x plus 3y equal to 11, now if we subtract, we are getting 2y equal to 1, now y is equal to 2 inverse mod 13. So, this is the secret inverse basically 7 because 2 inverse mod 13 is basically 7. So, we got y as 7.

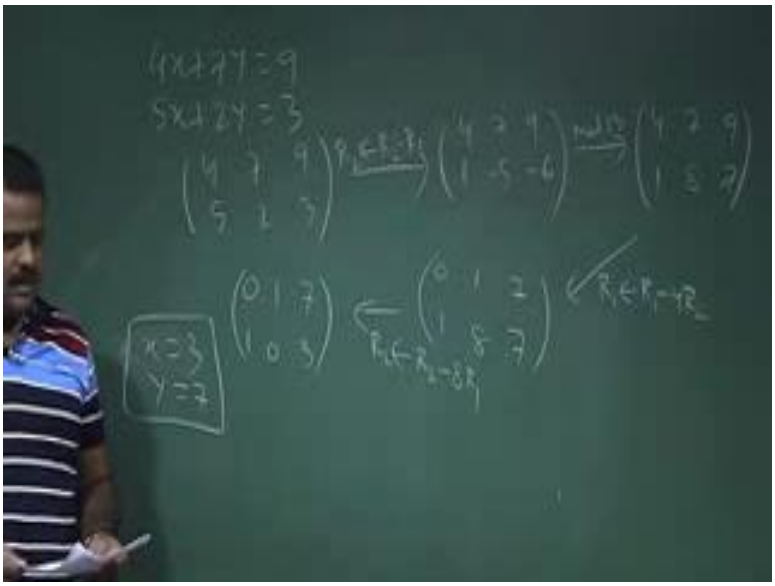
Now once we have the y then we can put this value into one of this equation either this or this and we should able to get x.

(Refer Slide Time: 06:22)

Then x is basically so, from here x is basically 12 minus 5y, so, 12 minus 5 into 7 so, under mod 13. So, this will give us 3. So, basically you will get x equal to 3. So, this 2; this is the solution of this system of equation modulo 13.

Now if we want to; if you try to solve this in matrix form so and you have to perform the matrix operation like row operation column operation. So, we can try that also.

(Refer Slide Time: 07:08)



Our equation is basically what? If our equation is 4x plus 7y equal to 9 and 5x plus 2y equal to 3. So, this we can write as 4 7 5 2 and if we take the augmented matrix, this is the so we have to perform the operation on this matrix and we have to row operation and you have to make this 1 0 0 1 then that will give us the solution. So, to do that what we do? We will perform the row operation.

Basically we perform R2 is going to R2 minus R1 and if we do that we will be getting this R1 is remain same R2. So, 1 minus 5 minus 6, now this has to be under mod 13. So, if you take the mod 13. So, this will be basically 4 7 9, this is 1, this 15 is basically 8 and this 6 is basically 7 under mod 30. So, now, this is the current position of that augmented matrix, now we have to make it. So, now, we have to perform R1 is going to R1 minus 4 R2. R1 is going to R1 minus 4 R2 if you do so, we will be getting 0 1 7, 1 8 7. So, now, we are, we want to make it 0. So, for that we have to perform this operation and every time we are doing mod 13. So, we are doing R2 minus. So, this we multiply by 8 and then R2 is going to R2 minus 8 R1 if you do so, then we are getting 0 1 1 0 7 3. So, from here also you can say x equal to 7, sorry, x equal to 3 and y is equal to 7. So, these are also we can solve this, but every time our operation should be modulo operation under that here it is 13 in general, it is a mod P under that P.

Now, the Chinese remainder theorem: so, basically you want to have a system of modular equation and we want to we have more than one equation and we want to solve that.

(Refer Slide Time: 10:12)

For example, suppose we have this is one equation, a mod n and x is congruent to b mod n. So, these 2 is the modular equation we have and here we are assuming gcd of m n are 1 so; that means, m is relatively prime, this symbol we can use as relatively prime to n, both are relatively prime to each other, suppose we have this type of system then what is the solution. So, Chinese remainder theorem will give us the solution not only 1 system, we have we may have many system so, but let us start with 1 system. So, how we can solve it?

Let us take an example like say we have x is congruent to 3 mod 5 and x is congruent to say 5 mod 7. So, now, we want to have a, this is equation 1, equation 2. So, we want to have a solution for this system. So, we want to find the value x which satisfy both the equation. So, the x which satisfy equation ones are basically all the integers from this 3 8, all the integer which we try to divided by 5 reminder should be 3 so, 3, 8, 13, 18, 23, 28, 33, 38, so on so, this is all x which satisfying equation 1.

Now, similarly so, this is say a set a 1. So, this is the all x satisfying equation 1, similarly we can find the whole x, we satisfying this equation 2. So, those are basically all the integer if we divided by 7, it should give us 5 so, 5, 12, 19, 26, 33, 40, like this A 2. So,

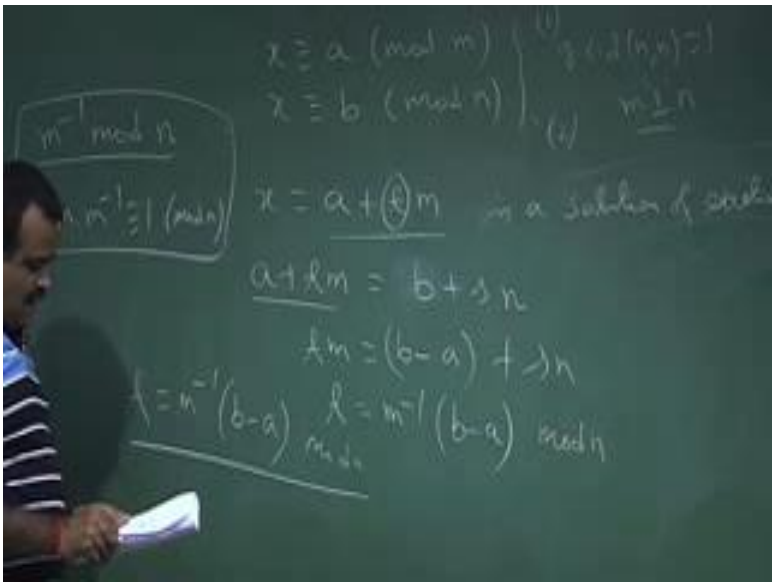
A 2 is the set where all the values; all the values satisfy equation 2, now we want the solution, we satisfying both the equations. So, that is basically the intersection A 1 intersection A 2.

(Refer Slide Time: 13:02)

This one is the x which satisfying both the equation. So, this is basically 33. So, this is basically any 2 number, any 2 element in this intersection differ by a multiple of 35. So, any 2, any 2 element; element in A 1 intersection, A 2 differ by a multiple of 37 which is basically is 5 into 7 that we can easily verify putting any 2 point then they should differ by a, they will be differ by a this. So, this is the 37 is the solution for this 33, 33 is the solution for this system mod 35. So, this x is equal to x is congruent to 33 mod 35. So, this is the solution for this system of equation.

Now, you can easily verify this is because this is satisfy these equation, this is also satisfied this equation. So, this is the name way, but we need to know how we can in general how we can get the solution. So, suppose we have the equation like this the general form a ax is congruent to a mod n and also x is congruent to b mod n. So, now, we want to find out, we want to find out the solution for this.

(Refer Slide Time: 14:58)



Say we are taking this as equation 1; we are taking this as equation 2.

Now, the x satisfying equation 1 will be of this form x equal to a plus some t into m by t is a positive integer t, it t is an integer. So, any x of this form is a solution of is a solution of solution, sorry, solution of equation 1, now we want this to be also solution for equation 2 then only it is that x will satisfy both. So, we need to find t such that this a plus t m will satisfy this equation also second equations. So, if you have to do that so, a plus t m we need to find t such that so, if it is satisfying this equation then it should be written as this should be written as b plus b plus some s into n.

Now the question is how we can get n? So, we can take this that side. So, t m is equal to b minus a plus s n. So, now, basically if we just so, t is basically m inverse b minus a mod n. So, basically we need to find m inverse mod n m inverse mod n, yes and then m inverse mod n means. So, that inverse with this m will give us is congruent to 1 mod n. So, that is the definition of inverse. So, if m inverse, but. So, m inverse modulo will exist because this is the guarantee because gcd of m and n are one. So, that is that is that is guarantee that inverse will exist. So, this inverse we can calculate by external Euclidean algorithm. So, once we got m inverse, so, then we choose t s which is t s like this m inverse b minus a; obviously, mod n and if we choose t as this then it will also satisfy equation 2. So, then this is satisfying both equation 1 and equation 2.

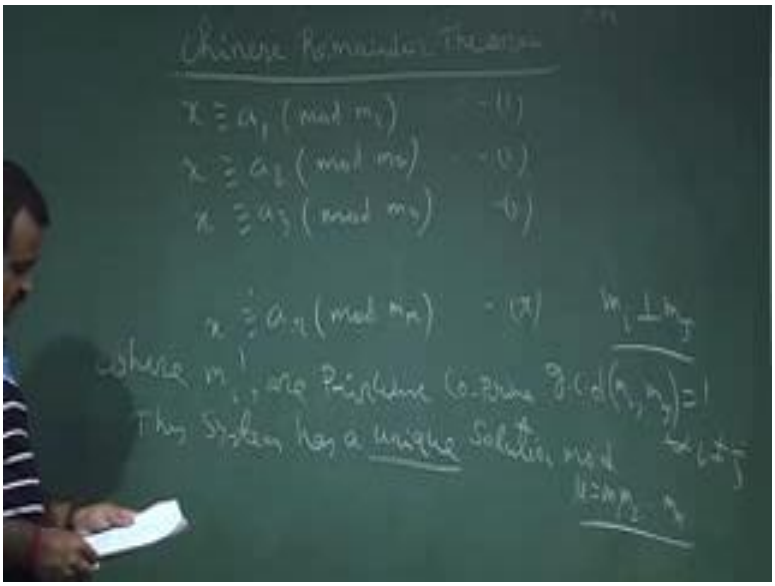
(Refer Slide Time: 18:15)

Now, we just calculate this by if the previous example. So, our equation was x is congruent to 3 mod 5 and x is congruent to 5 mod 7. So, so basically this is our a, this is our m, this is our b and this is our n. So, now, the question is how we can get the solution? So, what is the m inverse mod n? So, m inverse mod n is basically m is basically 5, so, 5 inverse mod 7, so, 5 inverse mod 7 is basically 3 mod 3 into 5 is basically for 15. So, 15 mod 7 is basically 1.

So, now t is basically m inverse so, 3, if this m inverse b minus a mod n, so, m inverse is 3, what is b? B is 5. So, 5 minus 3 mod 7, so, this is this will basically give us 6. So, the x is basically a plus t into m. So, 3 plus 5 into 6, 33 mod m into n, so, that is 35. So, this is the solution coming from this. So, this is the Chinese remainder theorem for 2 equations.

Now, suppose we have general case I mean we have many equations; more than 2 equations then the question is how we can solve it. So, that is the Chinese remainder theorem.

(Refer Slide Time: 20:29)

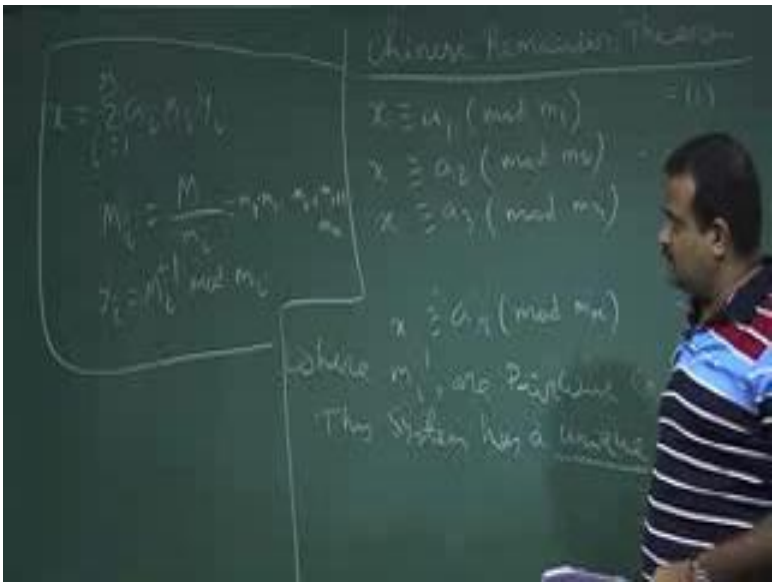


Chinese remainder theorem I mean this is a general form of the Chinese remainder theorem, suppose you have R equations x equal to a 1 mod m 1, x is congruent to a 2 mod m 2, x is congruent to a 3 mod m 3 dot, dot, dot, x is congruent to a R mod m R. So, suppose there are R equation in the system where the system of modular equations and there are R equations and here we have some conditions from the same. So, this set m i s are mutually co prime.

This m i's where m i's are the pairwise co prime so; that means, g c d of m i m j is 1 for all i not equal to j; that means, m i's co prime with m j for i not equal to j. So, that condition must be there for this system to have the solution not only solution it will have unique solution under mod of this product. So, we have seen for 2, now it is a general case and after that we will take a particular case for 3 and we try to solve that.

So, suppose we have this system and then it is Chinese remainder theorem is telling the system has a where this then the system has a unique solution earlier solution was 33 because if you take any other solution that will differ by the 35. If you take mod of that product 5 into so, this will again give us 33. So, that is why it is unique because every time to take any 2 solution, they will be differing by that product I mean 7 into 5 35 so; that means, if you take that solution mod 35, it will give us 33 anyway. So, this system has a unique solution mod, under mod m which is basically this product m 1 into m 2 into m r. So, this system of equations has a unique solution under this.

(Refer Slide Time: 24:01)



Now the question is what is the form of that solution, we will just write the form of the solution, the form that unique solution is basically x equal to summation of a i m i y i, i is equal to 1 to R. So, a i we know and what is m i? M i is basically this capital M by small m i basically in this product the m i is missing. So, this is basically all the elements other than all the primes not primes all these numbers. So, m i minus 1 m i plus 1 dot, dot, dot, m R, so, m i is missing here and y i basically this m i inverse mod m i. So, this is the solution of this system of equations, the system of equation has the unique solution this is the solution.

Now the question is how we can execute this? So, we will take an example, we will take 3 equation, as 2 equation we have seen how we can taken, now we take 3 equations and then we will try to get the unique solutions by Chinese remainder theorem.

(Refer Slide Time: 25:22)

Let us take 3 equations suppose x is congruent to 4 mod 29 x is congruent to 7 mod 30, x is congruent to 8 mod 31. So, this is 3 equations R is equal to 3 here.

Now the question is how we can solve these equations? So, we will use the Chinese remainder theorem. So, we know the solution for general case, but we will derive this. So, how to solve? So, this is equation 1, equation 2, equation 3. So, we have seen the example or we can handle 2 equations at a time. So, what we do? We take 2 equation at a time then we get the solution which satisfy that these 2 equation then we will take that solution along with this equation, this is also this is also 2 equation. So, we will take 2 equations at a time. So, you first take these 2 equations, equation 2 and equation 3 and we apply that technique a plus t m t; a plus t m and t is equal to that form. So, if you use that. So, this is a, this is b, this is m, this is n. So, the solution will be basically so, for that we need to find out this is m. So, for t we need to find out m inverse m inverse mod n m is 31 here, so, if you calculate this, this is basically 30, you can verify this.

Now, so t is basically if you remember that form m inverse, this is m, this is n, this is a, this is b. So, m inverse b minus a mod n, so, if you just put this value m inverse is 30, b is basically 8, so, 8 minus 7 mod n, mod n basically mod 31. So, this will give us basically again 30. So, x is basically then a plus t m. So, t we got m we know. So, x is this mod m into n. So, this is basically 7, this is 7 plus 30 into 30 mod. So, these 2 if you multiply, these 2 will be getting 9 3 0. This is basically coming out to be 9 0 7 mod 9 3 0.

So, we have the solution for these 2 equations. So, these 2 equation will give us a solution x equal to 7 mod 3. So, now, we have a equation with this 4 and we have equation 1. So, now, again there are 2 equations and we can easily verify because these are all mutually co prime.

Now this is also will be co prime through this. So, now, this is m, this is n, this is a, this is b. So, now, we need to solve these 2 equations by the similar fashion and that should give us the solution. So, let us try that so, now, our equation is, now we have this is one equation.

(Refer Slide Time: 29:31)

And another equation we have - the first one x equal to 4 mod 29, so this is now a, this is m this is now b, this is n. So, to get the solution, we have to find out m inverse. So, 29 inverse mod, so, this again by Euclidean algorithm and we know these 2 are relatively prime. So, inverse will exist and using external Euclidean algorithm, 1 can get this, this is the inverse, now t you can calculate t is basically m inverse into b minus a so, 4 4 9 into b minus a, b minus a mod n mod. These will give us basically if we calculate 8 9 7.

So, now, x equals to what x equal to a plus t m mod m into n these 2. So, basically it will be 4 plus a is 4, now t we got this and m is this. So, 97 into 29, so, this if we calculate this, will give us 2 6 0 1 7 mod this product. So, this is the unique solution, we are getting 29 into 30 into 31. So, this is our x. So, this is the way we solve this system of equation, if you have 3 equations of this the; so, we take it to then we solve it and with

that solution, we again solve with this equation. So, this way we will continue, if you have more equation, we will continue this process if you have another equation, we will just take that one with this and we will get the solution. So, that will give us the solution for the Chinese remainder theorem.

Thank you.