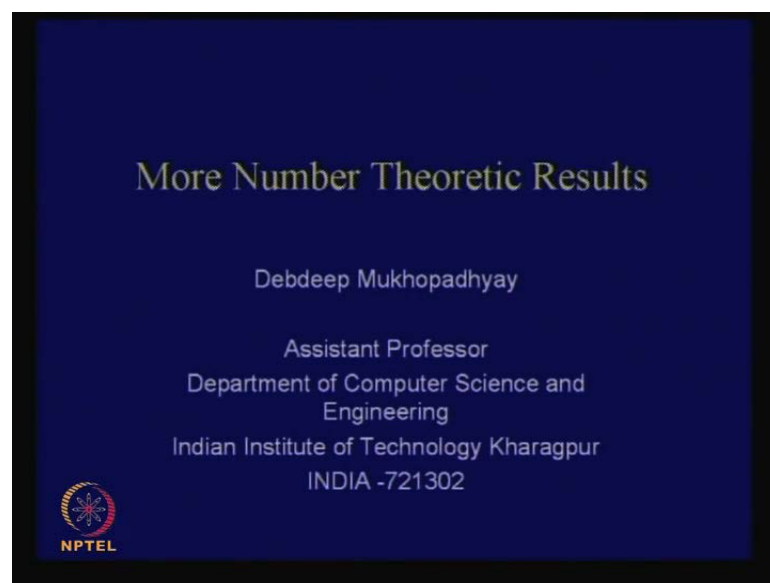


Cryptography and Network Security
Prof. D. Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

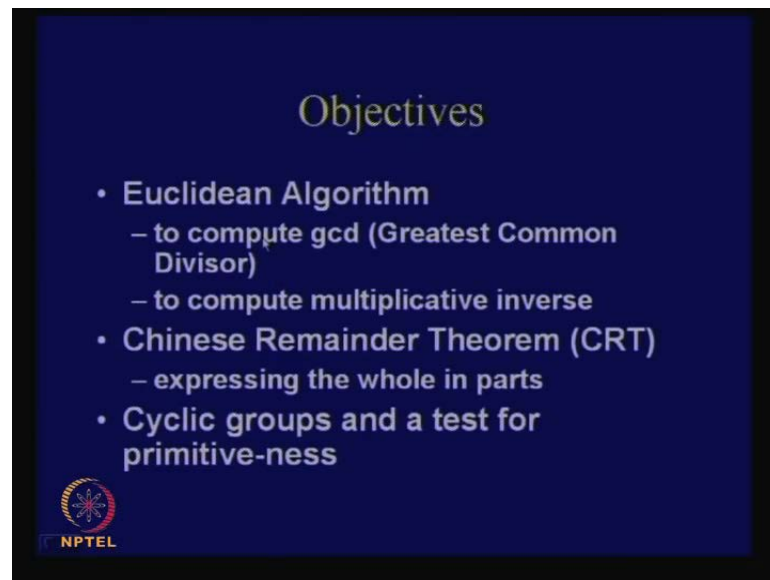
Lecture No. # 27
More Number Theoretic Results

(Refer Slide Time: 00:21)



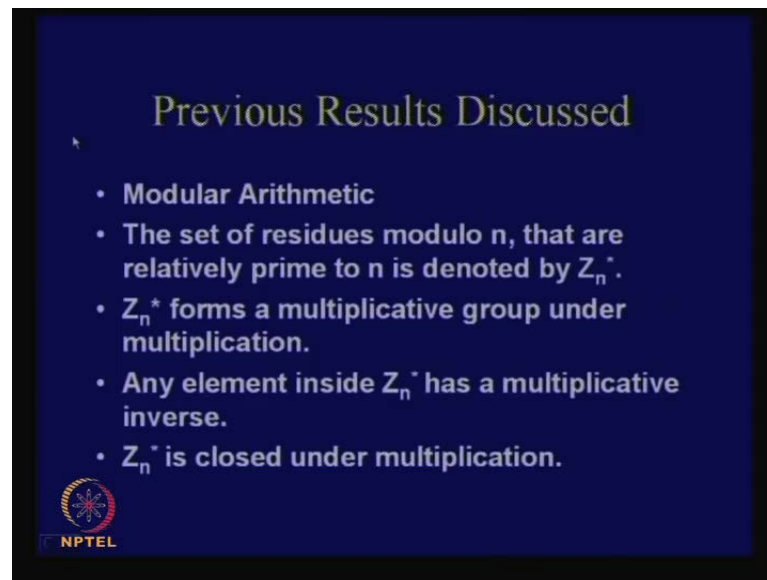
So, today, we will study more number theoretic results, so, which will be useful in our future studies or asymmetric cryptography.

(Refer Slide Time: 00:28)




So, today, we will discuss about two interesting and important algorithms - one is called Euclidean algorithm which is used to compute the GCD or the greatest common divisor of two integers. There are also which is useful to compute the multiplicative inverse. So, we have defined what a multiplicative inverse. So, we will see how the Euclidean algorithm can be extended to compute the multiplicative inverse, and then, we will discuss about another very interesting algorithm, it is called Chinese remainder theorem. The theme is to express whole in parts. So, we will see what is that, and then, also conclude with some important results on cyclic groups and also discuss about a test of primitiveness of an element.

(Refer Slide Time: 01:08)



Previous Results Discussed

- Modular Arithmetic
- The set of residues modulo n , that are relatively prime to n is denoted by Z_n^* .
- Z_n^* forms a multiplicative group under multiplication.
- Any element inside Z_n^* has a multiplicative inverse.
- Z_n^* is closed under multiplication.

 NPTEL

So, previous results, if you remember that what we did in the last time when we studied about number theory, we studied modular arithmetic. So, we have a more or less seen what is meant by modular arithmetic and the idea was of, the, so, Z_n^* was used to denote the set of residues modulo n that are relatively prime to n . So, I hope you will remember this notation.


So, Z_n^* means that, if n is any number given, so, n is not necessarily a prime number. So, Z_n^* means all those elements when I am reducing the element modular n . So, which those elements has to, I mean the residues has to be relatively prime; so, they have to be co-prime to n . So, therefore, they should not have any factor with n except 1. So, therefore, they are co-prime to n and Z_n^* is used to denote that particular set. So, we have seen that Z_n^* forms a multiplicative group under multiplication; that means, that Z_n^* essentially what we saw is the every element has a multiplicative inverse. So, any element inside Z_n^* has a multiplicative inverse and Z_n^* is also closed under multiplication.

(Refer Slide Time: 02:36)

The Euclidean Algorithm

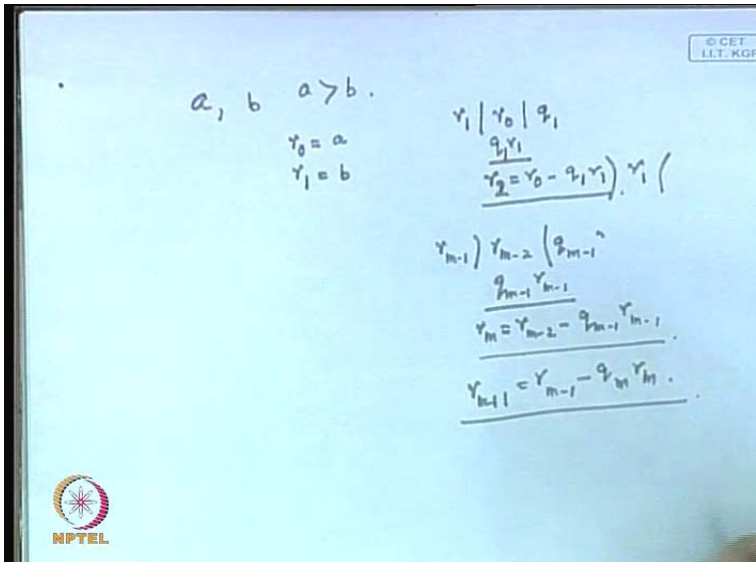
EUCLIDEAN ALGORITHM(a, b)

```
r0 ← a
r1 ← b
m ← 1
while rm ≠ 0
do {
  qm ← ⌊ rm-1 / rm ⌋
  rm+1 ← rm-1 - qmrm}
  m ← m + 1
m ← m - 1
return (q1, ..., qm; rm)
comment: rm = gcd(a, b)
```



So, if you take two elements which is lies in Z_n star and multiply them and also take a modulo n , then a result is also inside Z_n star. So, that is the closure property. So, today we will take up an algorithm is called the Euclidean algorithm. So, I think all of us know this algorithm meaning actually. So, therefore, this is actually the same algorithm which we have used in our school days to compute GCD of two numbers.

(Refer Slide Time: 02:57)




$a, b \quad a > b.$

$r_0 = a$
 $r_1 = b$

$r_1 \mid r_0 \mid q_1$
 $\frac{q_1 r_1}{r_2 = r_0 - q_1 r_1} \cdot r_1$

$r_{m-1} \mid r_{m-2} \mid q_{m-1}$
 $\frac{q_{m-1} r_{m-1}}{r_m = r_{m-2} - q_{m-1} r_{m-1}}$

$r_{m+1} = r_{m-1} - q_m r_m$



So, the thing is that we will just study that little bit more carefully. So, let us see that suppose two numbers are provided to us - a and b , and we have suppose a greater than b . So, what do you do? Typically what you do is like this, that is, you take a and you store a in a variable called r_0 and you take b and store that in a variable call r_1 . Then, what you do is that, you start dividing r_0 by r_1 . You obtain a quotient called q_1 , and here, you get $r_0 = q_1 r_1 + r_2$. Therefore, r_2 . So, the remainder which you get is called r_2 ; I denote by r_2 and $r_2 = r_0 - q_1 r_1$. So, this is the remainder. So, you get r_0 here and it subtract $q_1 r_1$ and you obtain r_2 . So, that is actually r_2 .

So, that is, therefore, if you see that this, I can actually continue. Therefore, what I do is that next I take r_1 here and I divide r_1 and I continue with this process. So, therefore, at any stage, that is, at any m th stage, I have got this particular thing. I have got r_{m-2} and I divide that by r_{m-1} and I get here q_{m-1} and I get here $q_{m-1} r_{m-1}$ into r_{m-2} and this remainder is r_m . So, $r_m = r_{m-2} - q_{m-1} r_{m-1}$. So, this is the corresponding result at the m th stage of this algorithm.

So, therefore, now, we know that we continue this kind of division, and when we get the remainder value to be equal to 0, then we look at the previous divisor value and report that as the GCD of these two numbers r_0 and r_1 . So, that is the fundamental working of the algorithm.

(Refer Slide Time: 05:12)


The Euclidean Algorithm

EUCLIDEAN ALGORITHM(a, b)

```

 $r_0 \leftarrow a$ 
 $r_1 \leftarrow b$ 
 $m \leftarrow 1$ 
while  $r_m \neq 0$ 
  do  $\begin{cases} q_m \leftarrow \lfloor \frac{r_{m-1}}{r_m} \rfloor \\ r_{m+1} \leftarrow r_{m-1} - q_m r_m \\ m \leftarrow m + 1 \end{cases}$ 
 $m \leftarrow m - 1$ 
return  $(q_1, \dots, q_m; r_m)$ 
comment:  $r_m = \text{gcd}(a, b)$ 

```



So, I think all of us know this algorithm. So, why does this algorithm work? Therefore, this is the pseudo code of the algorithm. You see that r naught has been stored; I mean a has been stored in r naught; b has been stored in r 1 and you start with m equal to 1; you compute the quotient. So, you are quotient is the floor of when you divide r m minus 1 by r m . **So, that is the...** So, this is the r m minus 1 divided by r m and you get q m and then you get r m plus 1.

(Refer Slide Time: 05:43)

Handwritten mathematical derivation on a whiteboard:

$$a, b \quad a > b.$$

$$r_0 = a$$

$$r_1 = b$$

$$r_1 \mid r_0 \mid q_1$$

$$\frac{q_1 r_1}{r_2 = r_0 - q_1 r_1} \cdot r_1 \left($$

$$r_{m-1} \mid r_{m-2} \mid q_{m-1}$$

$$\frac{q_{m-1} r_{m-1}}{r_m = r_{m-2} - q_{m-1} r_{m-1}}$$

$$\frac{r_{m-1}}{r_{m+1} = r_{m-1} - q_m r_m}$$

NPTEL logo is visible in the bottom left corner.

(Refer Slide Time: 05:55)

The Euclidean Algorithm

```

    EUCLIDEAN ALGORITHM( $a, b$ )
     $r_0 \leftarrow a$ 
     $r_1 \leftarrow b$ 
     $m \leftarrow 1$ 
    while  $r_m \neq 0$ 
    do
         $q_m \leftarrow \lfloor \frac{r_{m-1}}{r_m} \rfloor$ 
         $r_{m+1} \leftarrow r_{m-1} - q_m r_m$ 
         $m \leftarrow m + 1$ 
     $m \leftarrow m - 1$ 
    return  $(q_1, \dots, q_m; r_m)$ 
    comment:  $r_m = \text{gcd}(a, b)$ 
    
```


NPTEL logo is visible in the bottom left corner.

So, r_{m+1} is $r_{m-1} - q_m r_m$. So, same thing, I mean in the particular equation that we wrote, you can also write $r_{m+1} = r_{m-1} - q_m r_m$. So, therefore, this particular state is written out here. So, $r_{m+1} = r_{m-1} - q_m r_m$ and m equal to you increment m each times, and when you get the value of remainder equal to 0, you see m equal to $m-1$. That is a previous stage and it report the corresponding r_m of the previous; I mean which is the previous divisor as the corresponding GCD.

(Refer Slide Time: 06:18)

Proof of Correctness

- $\gcd(a,b) = \gcd(r_0, r_1) = \gcd(q_1 r_1 + r_2, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \dots = \gcd(r_{m-1}, r_m) = r_m$
- Thus, the EA algorithm can be used to compute the gcd of two positive integers
 - Also to check whether an integer modulo n has a multiplicative inverse.
- But how can we compute the inverse?



 NPTEL

So, now, what is the reason why this is correct? I mean the correctness of this algorithm can be seen by these particular equations such as what I have interested in computing is GCD of a, b . So, what is a ? a is r_0 and b is r_1 . So, r_0 is actually equal to $q_1 r_1 + r_2$ and r_1 is r_1 . So, therefore, if I take a GCD of these two numbers because r_1 is here and r_1 is also here, this reduces to GCD of r_1, r_2 .

Therefore, continue in this fashion I get GCD of r_1, r_2 equal to GCD of r_2, r_3 , and similarly and then, finally, since r_m is dividing r_{m-1} . Therefore, the GCD is r_m . Therefore, this actually terminates this, I mean this algorithm gives you also correctly that corresponding GCD of a and b . So, therefore, the Euclidean algorithm can be used to compute the GCD of 2 positive integers and it is also can be used to check whether an integer and modular n has a multiplicative inverse.

How can you do that? How can you check? So, what is the check? Whether a particular element whether particular integer modular n has a multiplicative inverse. We have started this property.

What is the property?


G c d a, n.

Yes, GCD of a, n is equal 1. Therefore, what I have to do is that, I have to compute the GCD and the GCD has to be 1. If the GCD is 1, then the element has an integer, I mean has a multiplicative inverse, but the question is how can I compute the inverse? That is the next question. Therefore, I can check the whether an element or whether a integer modulo n has a multiplicative inverse very easily, but the thing is that I am also interested to compute the corresponding inverse value.

(Refer Slide Time: 08:04)

Example

- Compute the $28^{-1} \text{ mod } 75$
 $75=2 \times 28+19$
 $28=1 \times 19+9$
 $19=2 \times 9+1$
 $9=9 \times 1$
- So, $\text{gcd}(28,75)=1$. So, what is the inverse?
- Can you express the gcd as a linear combination of 28 and 75?



NPTEL

(Refer Slide Time: 08:20)

Handwritten work on a whiteboard showing the extended Euclidean algorithm for finding the inverse of 28 modulo 75.

Top left: $28^{-1} \pmod{75}$

Below it: $1? = \gcd(28, 75)$

Euclidean algorithm steps:

$$75 = 2 \times 28 + 19$$

$$28 = 1 \times 19 + 9$$

$$19 = 2 \times 9 + 1$$

$$9 = 1 \times 9$$

Extended Euclidean algorithm steps:

$$19 = 75 - 2 \times 28$$

$$9 = 28 - 1 \times 19 = 28 - 1 \times (75 - 2 \times 28) = 3 \times 28 - 1 \times 75$$

$$1 = 19 - 2 \times 9 = (75 - 2 \times 28) - 2(3 \times 28 - 1 \times 75) = 3 \times 75 - 8 \times 28$$

Top right: Division steps for the Euclidean algorithm:

$$28 \overline{) 75} \begin{array}{r} 2 \\ \underline{56} \\ 19 \end{array} \begin{array}{r} 2 \\ \underline{38} \\ 19 \end{array} \begin{array}{r} 1 \\ \underline{19} \\ 0 \end{array}$$

Bottom left: NPTEL logo

Bottom right: IIT KGP logo

So, this particular algorithm is called the extended Euclidean algorithm. So, therefore, let us study or let us try to compute the inverse of 28 modulo 75. So, therefore, if I am, I mean what I can start doing is that, so, what I am trying to compute is 28 inverse modulo 75. So, suppose, first of all, I should know that whether 28 inverse really exists or not. So, therefore, what I will do is that I will find out the GCD of 28 and 75.

So, therefore, what is the corresponding GCD of 28 and 75? Therefore, ideally this should be 1 and I have to check this thing. So, 28 if I divide 75 by 28, I get here 56, and therefore, this is equal to 19 1 19; I get here 9 19 2 18 and I get here 1 divide; I get here 0 So, therefore, 1 is my corresponding GCD. So, the multiplicative inverse really exists. So, therefore, now, you can actually start expressing these things in this fashion. You can write like 75. So, this 75 is equal to 2 into 28 plus...

Plus 19

19

So, 2 into 28 plus 19. So then, what you can do is that, you can see 28. 28 is 1 into 19 plus...

9

9. Then you have got 19; 19 is equal to 2 into 9 Plus 1, and finally, you have got 9 equal to 1 into 9. So, now, the interesting thing is that, you will see that each of this remainders, that is, whatever you are getting the as a remainder can be expressed as a linear combination of the elements 28 and 75.

See, for example, 19 is equal to 75 minus 2 into 28. So, what about 9? 9 is actually 28 minus 1 into 19, but I know how to express 19. So, I know that 19 is nothing but 1 into 75 minus 2 into 28. So, therefore, these I can collect and I can write like these as 3 into 28 minus 1 into 75. So, what about the next element? The next remainder is 1. So, 1 is 19 minus 2 into 9. So, 19 I know as 3 into 28 minus 1 into 75. So, this is not point. So, 1 into, so, minus 2 into 9.

So, therefore, what is 9?

(C)

I think I wrote the wrong thing. Therefore, 19 is actually 75 minus 2 into 28 minus 2 into 9. So, 9 is 3 into 28 minus 1 into 75. So, therefore, this is actually 75. Therefore, this is actually 3 into 75 minus 8 into 28.

(Refer Slide Time: 11:59)

The image shows a whiteboard with the following handwritten text:

$$1 = 3 \times 75 - 8 \times 28.$$

$$\Rightarrow \underline{1} = \boxed{-8} \times 28 \pmod{75}$$

Multiplicative Inverse of $28 \pmod{75} = -8$
 $= 67.$

There is a small logo in the bottom left corner that says "NPTEL" and a small copyright notice in the top right corner that says "©CET IIT, RGP".

So, now, you see that, if you take this final equation and I will write properly. So, this is what? This is 1 equal to 3 into 75 minus 8 into 28. Now, suppose I take a modulo 75 on both sides. So, what do I get? I get 1 equal to minus 8 into 28 mod 75 because this term

goes to 0 in that case. So, now what is the multiplicative inverse of 28? It is minus 8 because if I multiply with minus 8 I get back 1. So, therefore, minus 8 mod 75 means?

67


67

So, therefore, the multiplicative inverse of 28 mod 75 is equal to minus 8 and that is equal to 67. So, therefore, what was the main objective? The main objective was that, at each stage, the Euclidean algorithm whatever remainder we were getting from Euclidean algorithm; we are expressing that remainder as a linear combination of the starting two elements. That is the mod value that, I mean what you are doing modulo with and the element for which you are interested in computing the multiplicative inverse.

(Refer Slide Time: 13:23)

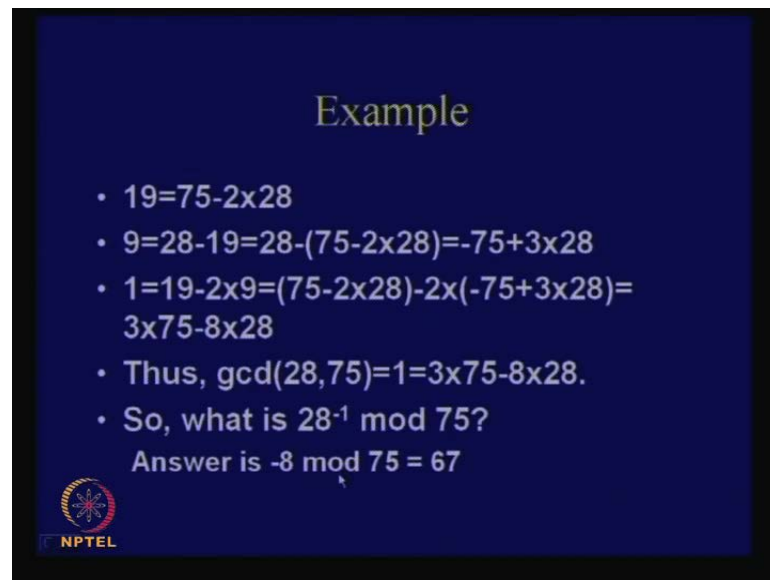
Example

- Compute the $28^{-1} \text{ mod } 75$
 $75 = 2 \times 28 + 19$
 $28 = 1 \times 19 + 9$
 $19 = 2 \times 9 + 1$
 $9 = 9 \times 1$
- So, $\text{gcd}(28, 75) = 1$. So, what is the inverse?
- Can you express the gcd as a linear combination of 28 and 75?

 NPTEL

And that is the main working principle. So, therefore, the main question is that can you express the GCD as a linear combination of 28 and 75. So, after that, it is quite easy, because we know that GCD has to be 1. So, if I take a modulo with this corresponding 75, then whatever element I get on the right hand side, I mean the remain which I multiplying 28 to get back 1 is the multiplicative inverse of 28.


(Refer Slide Time: 13:48)



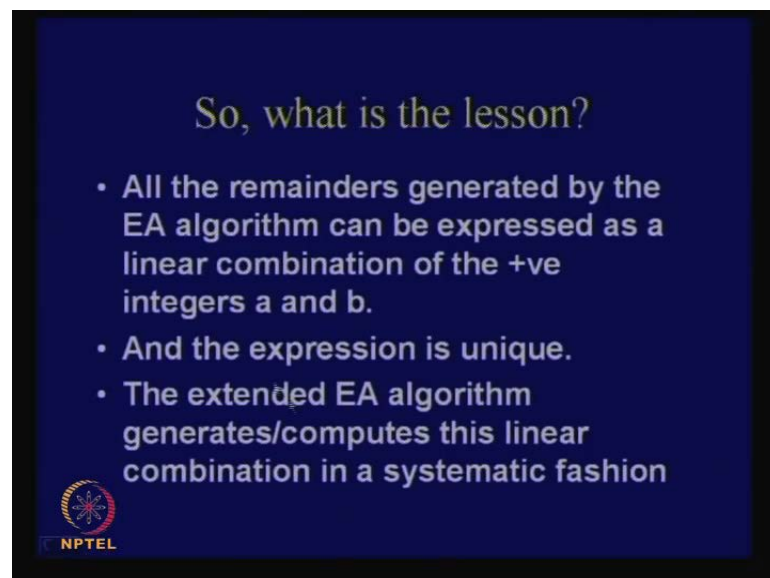
Example

- $19 = 75 - 2 \times 28$
- $9 = 28 - 19 = 28 - (75 - 2 \times 28) = -75 + 3 \times 28$
- $1 = 19 - 2 \times 9 = (75 - 2 \times 28) - 2 \times (-75 + 3 \times 28) = 3 \times 75 - 8 \times 28$
- Thus, $\gcd(28, 75) = 1 = 3 \times 75 - 8 \times 28$.
- So, what is $28^{-1} \pmod{75}$?

Answer is $-8 \pmod{75} = 67$




(Refer Slide Time: 13:55)



So, what is the lesson?

- All the remainders generated by the EA algorithm can be expressed as a linear combination of the +ve integers a and b.
- And the expression is unique.
- The extended EA algorithm generates/computes this linear combination in a systematic fashion



So, this is what I did. So, therefore, answer is actually minus 8 mod 75 equal to 67. So, therefore, now we will generalize this, but... So, what is the lesson that we learn? That all the remainders which are generated by the Euclidean algorithm can be expressed as a linear combination of the positive integers a and b, and although I am not proving, but it is quite easy to prove that the expression is actually unique. Therefore, you cannot find two search linear combinations which will actually satisfy this.


So, this extended Euclidean algorithm actually generates or computes a linear combination in a very systematic fashion. So, that is the main objective. So, therefore, we will see that the extended algorithm, it just generates or computes this linear combination values in a quite systematic fashion.

(Refer Slide Time: 14:34)

• Define (t_0, t_1, \dots, t_m) and (s_0, s_1, \dots, s_m)

$$t_j = \begin{cases} 0 & \text{if } j = 0 \\ 1 & \text{if } j = 1 \\ t_{j-2} - q_{j-1}t_{j-1} & \text{if } j \geq 2 \end{cases} \quad s_j = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{if } j = 1 \\ s_{j-2} - q_{j-1}s_{j-1} & \text{if } j \geq 2 \end{cases}$$

For $0 \leq j \leq m$, we have that $r_j = s_j r_0 + t_j r_1$, where the r_j 's are as defined in the Euclidean Algorithm, and the s_j 's and the t_j 's are as defined in the recurrence.



So, how do we do this? So, therefore, this is how it is done. So, you define a series of t terms. So, t_0 to t_m , and similarly, from s_0 to s_m and this is how you define t_j and you define s_j . So, basically you have a recursive construction. So, you see that j equal to 0 t_j has been initialized to 0, and if j equal to 1, then t_j is equal to 1. What about s_j ? s_j is just the other way round. So, if j equal to 0, and then, s_j is equal to 1; if j equal to 1, then s_j equal to 0.

So, this is just the opposite of this definition 0 1 and 1 0, why? Because this t_j and s_j is actually used to, is the corresponding, what am I interesting to do? I am interested to express the remainder as a linear combination of r_0 and r_1 . So, now, this, I mean the corresponding coefficient in that linear combination is being generated by the series t_j and the series s_j .

So, here, the first remainder is, if I start with r_0 . So, therefore, if I say that the j equal to 0 or 0 , so, r_0 will be equal to 1 into r_0 plus 0 into r_1 . So, therefore, the starting point of this should be 1 and. So, when this is 1 , this is actually 0 . So, therefore, you see that when this is 1 , this is 0 . So, when you are expressing r_1 , then similarly this t_j has to be 1 and s_j has to be 0 . Therefore, s_j is 0 when j equal to 1 ; then s_j equal to 0 and t_j is equal to 1 .

But for the rest of the j values, that is been j is greater than 1 , that is, j is greater than equal to 2 . So, in that case, in those scenarios, t_j is defined like this and s_j is also defined like this. So, t_j is what? t_j minus 2 minus q_j minus 1 t_j minus 1 . So, q_j minus 1 is a same as that we got in the Euclidean algorithm and s_j is equal to s_j minus 2 minus q_j minus 1 into s_j minus 1 .

So, what we can actually prove is that r_j which is the corresponding remainder value of the j th stage can be expressed as a linear combination of r_0 and r_1 with coefficient s_j and t_j . So, there r_j 's are as defined in the Euclidean algorithm and s_j 's and t_j 's are as defined in the above recurrence. So, why does it work? So, we can see why we work. So, for base cases like for j equal to 0 and j equal to 1 , this is trivial. That is what we argue.

(Refer Slide Time: 17:20)

Handwritten mathematical derivation on a whiteboard:

$$j = i-2, j = i-1.$$

$$j = i-1.$$

Assume, $\left\{ \begin{array}{l} r_{i-2} = s_{i-2}r_0 + t_{i-2}r_1 \\ r_{i-1} = s_{i-1}r_0 + t_{i-1}r_1 \end{array} \right\}$

$$r_{i-1} \mid r_{i-2} \quad q_{i-1} \quad r_i = r_{i-2} - q_{i-1}r_{i-1}$$

$$r_i = r_{i-2} - q_{i-1}r_{i-1}$$

$$= (s_{i-2}r_0 + t_{i-2}r_1) - q_{i-1}(s_{i-1}r_0 + t_{i-1}r_1)$$

$$= (s_{i-2} - q_{i-1}s_{i-1})r_0 + (t_{i-2} - q_{i-1}t_{i-1})r_1$$

$$= s_i r_0 + t_i r_1$$

Watermark: © CET I.I.T. KGP

So, let us assume that it is true for j equal to i minus 1 and j equal to i minus 2 and j equal to i minus 1 . So, what we will prove is that it is also true for j equal to i minus 1 , I mean j

equal to i . So, this is basically mathematical induction. So, we are applying mathematical induction to prove this result.

So, what type of induction is this weak or strong?

Weak

This is weak induction.

So, we apply j equal to i , and so, we know we expect the results for j equal to $i - 2$ and j equal to $i - 1$ and we are proving the result for j equal to i . So, when we are assuming for j equal to $i - 2$, therefore, that means that, I can assume that r_{i-2} equal to $s_{i-2}r_0$ plus $t_{i-2}r_1$ and also r_{i-1} equal to $s_{i-1}r_0$ plus $t_{i-1}r_1$. So, these are two given results.

So, what about, so, when I am computing r_i , that is, r_i is the corresponding remainder. Then that means that, what I have done in that particular step in the Euclidean algorithm is that I have taken r_{i-2} and I have divided that with r_{i-1} . And what was my remainder here? It was q_{i-1} and I have got $q_{i-1}r_{i-1}$ and my remainder was r_i . So, what was r_i ? r_i was $r_{i-2} - q_{i-1}r_{i-1}$.

So, therefore, r_i is equal to $r_{i-2} - q_{i-1}r_{i-1}$. So, therefore, I can take this previous two given or assumed results and I can plug in them. So, therefore, I get r_{i-2} as equal to $s_{i-2}r_0$ plus $t_{i-2}r_1$ minus q_{i-1} and $s_{i-1}r_0$ plus $t_{i-1}r_1$. So, that is equal to, if I take $s_{i-1}r_0$ out from this, therefore, if collect r_0 , I get $s_{i-2} - q_{i-1}s_{i-1}$ into r_0 plus $t_{i-2} - q_{i-1}t_{i-1}$ into r_1 .

So, therefore, you see at this particular these two terms are nothing, but what is S_i and t_i . Therefore, I can write this as $s_i r_0$ plus $t_i r_1$ and that proves the case for j equal to i . So that means that the remainder can be expressed as a linear combination of r_0 and r_1 where the corresponding coefficients are s_i and t_i , and s_i and t_i are defined by these particular recurrence. So, therefore, I can repeatedly I can keep on continuing this values, this coefficient values, and then, I should be able express that remainder at each stage as a linear combination of r_0 and r_1 . So, any doubts about this?

(Refer Slide Time: 21:09)

```
EXTENDED EUCLIDEAN ALGORITHM(a, b)
a0 ← a
b0 ← b
t0 ← 0
t ← 1
s0 ← 1
s ← 0
q ← ⌊a/b⌋
r ← a0 - qb0
while r > 0
  temp ← t0 - qt
  t0 ← t
  t ← temp
  temp ← s0 - qs
  s0 ← s
  s ← temp
  a0 ← b0
  b0 ← r
  q ← ⌊a/b⌋
  r ← a0 - qb0
r ← b0
return (r, s, t)
comment: r = gcd(a, b) and sa + tb = r
```

The
Extended
EA
algorithm

NPTEL

So, therefore, this is now the pseudo code of the algorithm. So, it is quite simple actually. If you just observe it minutely, it is nothing; I mean there are just its some temporary variables we have been used. It is just to save some variables, but it is same thing, you see that $t_0 - qt$ and $s_0 - qs$ are the main things. So, therefore, you are basically computing the t series and the s series. So, I am here using that to compute the corresponding coefficient values.

So, therefore, finally, what you are giving back by the extended Euclidean algorithm, when you have given two numbers, two positive numbers - a and b , you are actually giving back the corresponding GCD of a and b and you are also expressing the remainder as the linear combination of a and b . So, you are giving by the coefficients s and t . So, therefore, how can I use this, to compute the multiplicative inverse is quite clear. So, therefore, I have to just take a modulo on both sides, and therefore, I should get the remainder; I mean I should get the multiplicative inverse if it exists.

(Refer Slide Time: 22:13)


Example

i	r_i	q_i	s_i	t_i
0	75		1	0
1	28	2	0	1
2	19	1	1	-2
3	9	2	-1	3
4	1	9	3	-8

$$t_j = \begin{cases} 0 & \text{if } j = 0 \\ 1 & \text{if } j = 1 \\ t_{j-2} - q_{j-1}t_{j-1} & \text{if } j \geq 2 \end{cases}$$

$$s_j = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{if } j = 1 \\ s_{j-2} - q_{j-1}s_{j-1} & \text{if } j \geq 2. \end{cases}$$

$1 = 3 \times 75 + (-8) \times 28$
 Thus, taking modulo 75, $28^{-1} \bmod 75 = -8 = 67$



So, this is an example, same example. So, therefore, previously we were trying to compute. We are taking 2 numbers 75 and 28. You plug in this to the extended Euclidean algorithm. You get the q_i series and the, I mean you get the, these are the corresponding quotients and this is the s series and these are t series. So, therefore, you can use this particular recurrence to compute these values. So, you start with 1 0 and 0 1 and, the, subsequently you can take these q values and you can take this previous t values, because at this stage, you know already the previous two stages.

So, you can employ this recurrence to compute the values for s_2 and also for t_2 , because you know the value of s_0 and you know the value of s_1 and you also know the corresponding coefficient, I mean the quotient value. So, therefore, you can check this that this works as follows. Finally, what you obtain is this thing, that is, you obtain that 1 which is the GCD is actually equal to 3 into 75 minus 8 into 28. So, therefore, taking modulo 75 $28^{-1} \bmod 75$ is equal to minus 8. Therefore, you remember that this s_i was actually getting multiplied with 75.

So, therefore, if I take mod 75 on both sides, then actually this series, I mean we could have, if we are really interested in computing only the inverse, then computing this s_i series is a actually of no use, because I am actually taking modulo 75 on both sides. So, therefore, actually I can make this algorithm mod $(())$ for the multiplicative inverse

computation by actually removing this exercises, because I do not require to compute this. You all of you understand this that this is not require to compute this? Yes.

(Refer Slide Time: 24:07)

Improvement


Note that we do not require the s_i 's and can take a modulo 75 each time while computing the t_i 's. This will make the algorithm efficient.

i	r_i	q_i	t_i
0	75		0
1	28	2	1
2	19	1	-2
3	9	2	3
4	1	9	-8

$$t_j = \begin{cases} 0 & \text{if } j = 0 \\ 1 & \text{if } j = 1 \\ t_{j-2} - q_{j-1}t_{j-1} & \text{if } j \geq 2 \end{cases}$$

take a modulo operation with $a=75$.

The answer is $-8 \bmod 75 = 67..$



So, this is an improvement. So, note that we do not require the s_i 's and can take a modulo 75 each time while computing the t_i 's. So, this will make the algorithm mod efficient. So, therefore, I can actually do without computing this column and the answer that I will still get this minus 8. So, therefore, minus 8 mod 75 means 67.


(Refer Slide Time: 24:29)

The Chinese Remainder Theorem (CRT)

- It solves a system of congruences.
- Suppose m_1, m_2, \dots, m_r are pairwise relatively prime positive integers.
- System of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}. \end{aligned}$$

CRT asserts that there is a unique solution to this system



So, therefore, this concludes our discussion on the Euclidean algorithm, and then, we will take another interesting algorithm, it is called the Chinese remainder theorem. So, basically it is a systematic algorithm which solves the system of congruences. So, originally people say that it was employed by the Chinese people. So, therefore, as idea was that suppose, they wanted to find out how many people were there in their army.

So, therefore, they use to say that you stand in groups of 5, stand in groups of 3. So, in co-prime models, and whatever is the remainder which is a small number in inside 5 and 3, they use to compute that, and from there, they use to find out how many people are there in the army without counting that was the objective. So, therefore, the idea was that it solves a system of congruences, and suppose m_1, m_2 and so on as m_r are pairwise relatively prime positive integers.

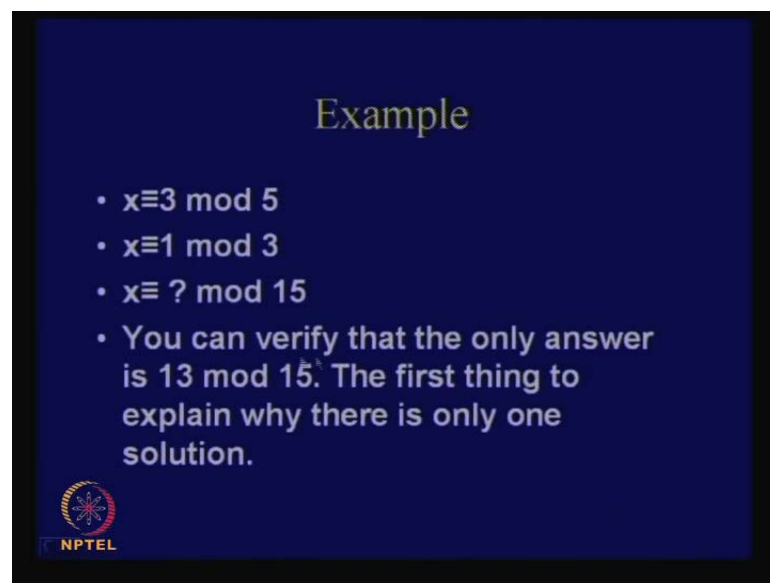
So, the system of congruences is as follows. You take x and you report only a a_1 which is when you take mod of m_1 . Similarly, you take mod of m_2 , you report a a_2 ; you take mod of m_r , you report a a_r . So, this a_1, a_2 and so on till a_r are actually just the, I mean the values when you take modulo of x with m_1 . So, therefore, this number is definitely smaller than m_1 . Similarly this number is smaller than m_2 and similarly this number is smaller than m_r .

So, computing these values is actually easy in that case, because this is a quite small numbers. So, therefore, what you are saying is that, this, I mean when you are solving this x value from this system of equations. So, what you are essentially trying to say is that you are expressing the whole as in parts. So, therefore, the theme is that to express the whole in parts. So, you see that this algorithm has got lot of applications in cryptography and may be many other places. So, therefore, I mean for cryptography, actually we will see that this algorithm is naturally a secret sharing algorithm.

So, what you are doing is that, suppose there is a file, and instead of giving disclosing the file and suppose there are r users. So, I am not giving everyone, I mean I am not giving each one the entire file content. So, what I am doing is that, I am dividing it amongst the r value r people. So, not, I mean suppose I divide it among r people in this class, the entire file content becomes evident only if this r people join, but not when $r - 1$ people join.

So, therefore, I can write this information theoretically also; that means that, if r people are joining, then the information is totaled, but if r minus 1 people join, then the information is actually 0. So, you do not have any information of the file, but there is something which is called as a threshold scheme. This is not a threshold scheme which I have told you, but this is definitely a secret sharing scheme. So, Chinese remainder theorem has got so many applications actually. So, let us try to understand how it works.

(Refer Slide Time: 27:28)



Example

- $x \equiv 3 \pmod{5}$
- $x \equiv 1 \pmod{3}$
- $x \equiv ? \pmod{15}$
- You can verify that the only answer is $13 \pmod{15}$. The first thing to explain why there is only one solution.

NPTEL

So, first, let us start with a small example. So, therefore, suppose that x is actually $3 \pmod{5}$ and x is $1 \pmod{3}$. So, what is the value of x when you take $\pmod{15}$? So, you can verify and the only answer is actually $13 \pmod{15}$. So, therefore, the only answer to this is 13. So, the first thing to explain is why there is only one solution. That is why is there only one unique solution. See, in order to understand that, let us do one thing.

(Refer Slide Time: 28:00)

Uniqueness

• $X(x) = (x \bmod 5, x \bmod 3)$

$\chi(0) = (0, 0)$	$\chi(1) = (1, 1)$	$\chi(2) = (2, 2)$
$\chi(3) = (3, 0)$	$\chi(4) = (4, 1)$	$\chi(5) = (0, 2)$
$\chi(6) = (1, 0)$	$\chi(7) = (2, 1)$	$\chi(8) = (3, 2)$
$\chi(9) = (4, 0)$	$\chi(10) = (0, 1)$	$\chi(11) = (1, 2)$
$\chi(12) = (2, 0)$	$\chi(13) = (3, 1)$	$\chi(14) = (4, 2)$

Note that the mapping is bijective...

NPTEL

So, let us define one function which is like this you take x , which is the actual thing which we need to compute and you express this as tuples like this like $x \bmod 5, x \bmod 3$. So, you note that what are the possible values of x since you are considering x from mod 15, there are actually 15 values from 0 to 14. So, for each of them, what I am doing is that, I am storing $x \bmod 5, x \bmod 3$. For this case, for example, when the x value is 0, then I am storing $0 \bmod 5$ and $0 \bmod 3$; when x is 1, I am storing $1 \bmod 5$ and $1 \bmod 3$. See, for example, when x is 10, I am storing $10 \bmod 5$ which is 0 and $10 \bmod 3$ which is 1.

So, similarly, I can populate this table, and the thing or the interesting thing to be noted is that, this is actually a bijective mapping, which means that you will never get two 0, 0's in this on the right hand side. So, you see that the domain is actually that there are 15 values; I mean the ranges also there are 15 values and there is actually a 1 to 1 connections. So, therefore, it is definitely a bijective mapping. So, first, we will try to prove this, but it will actually give you a constructive proof; so that means, it will give you a solution and also prove that are this unique.

(C)

Why are

(C)


(Refer Slide Time: 29:36)

The Chinese Remainder Theorem (CRT)

- It solves a system of congruences.
- Suppose m_1, m_2, \dots, m_r are pairwise relatively prime positive integers.
- System of congruences:

$$\begin{aligned}x &\equiv a_1 \pmod{m_1} \\x &\equiv a_2 \pmod{m_2} \\&\vdots \\x &\equiv a_r \pmod{m_r}.\end{aligned}$$

CRT asserts that there is a unique solution to this system



So, another interesting thing I probably missed it, or so, you see that the m values are actually relatively prime. So, this will work with any m values which are relatively prime. So, it could have worked with, but therefore, you understand that it has to be odds, because otherwise they are not relatively prime. If you take 2 even numbers, then 2 is a common factor.


(Refer Slide Time: 30:00)

Uniqueness

- $\chi(x) = (x \bmod 5, x \bmod 3)$

$\chi(0) = (0, 0)$	$\chi(1) = (1, 1)$	$\chi(2) = (2, 2)$
$\chi(3) = (3, 0)$	$\chi(4) = (4, 1)$	$\chi(5) = (0, 2)$
$\chi(6) = (1, 0)$	$\chi(7) = (2, 1)$	$\chi(8) = (3, 2)$
$\chi(9) = (4, 0)$	$\chi(10) = (0, 1)$	$\chi(11) = (1, 2)$
$\chi(12) = (2, 0)$	$\chi(13) = (3, 1)$	$\chi(14) = (4, 2)$

Note that the mapping is bijective...



So, therefore, this will work if you take 2 mutually

Mutually prime number


Mutually prime numbers. Therefore, you can take this as an even numbers and this as an odd number, but you cannot take two even numbers.

(Refer Slide Time: 30:20)

Example

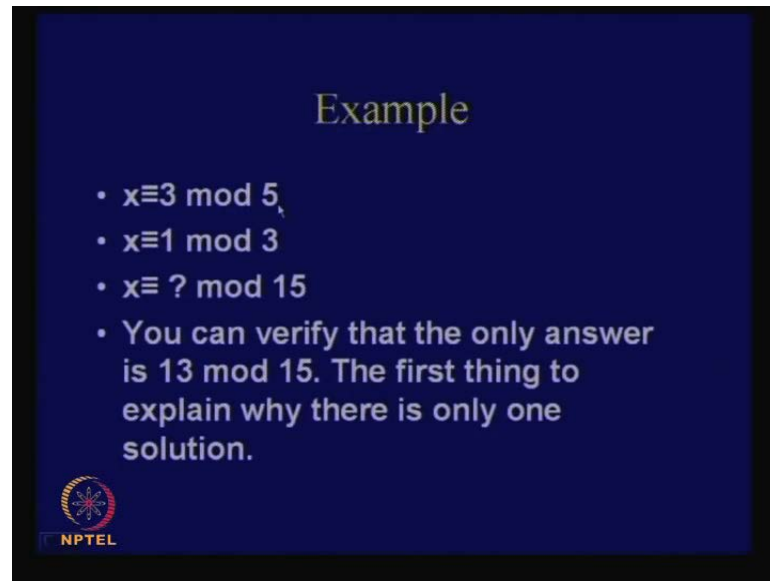
- $M=5 \times 3=15$
- $M_1=15/5=3, 3^{-1} \bmod 5=2$
- $M_2=15/3=5, 5^{-1} \bmod 3=2$
- $x=(3 \times 3 \times 2+1 \times 5 \times 2) \bmod 15$
 $=28 \bmod 15=13$

What is the principle?




So, we will try to prove this. So, therefore, you see that we can do like this, that is, you take m . So, therefore, you take 5 and 3 and you multiply these two things. So, therefore, this is the modulo value 5 and this is the modulo value 3. You multiply them and obtain M_1 by dividing 15 by 5. So, when you take 15, you divide by the first modulo value which is 5 and you get 3, and now, you see that 3, since you have taken 3 or rather factor out 3, 3 and 5 are mutually co-prime. So, therefore, you can actually compute 3 inverse mod 5, and 3 inverse mod 5 is actually equal to 2. Similarly, M_2 also you can compute by dividing 15 by 3 and you get 5 and you can compute 5 inverse mod 3 which is also equal to 2.

(Refer Slide Time: 31:15)



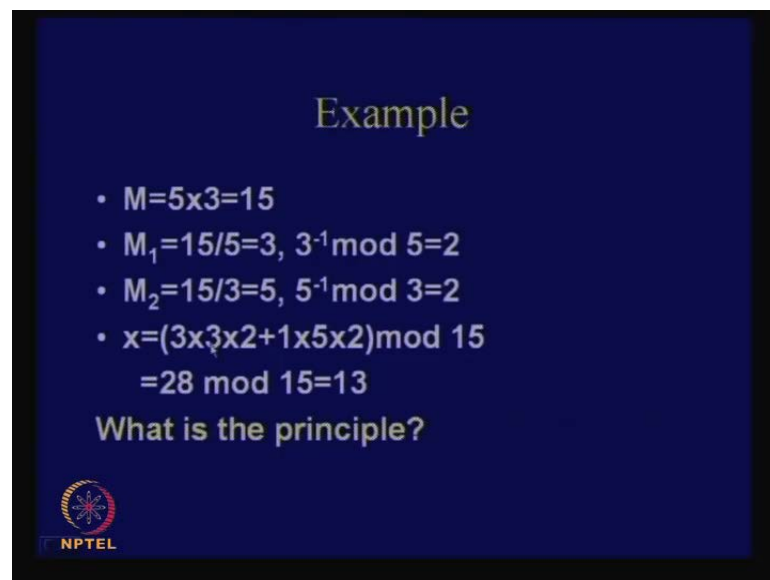
Example

- $x \equiv 3 \pmod{5}$
- $x \equiv 1 \pmod{3}$
- $x \equiv ? \pmod{15}$
- You can verify that the only answer is $13 \pmod{15}$. The first thing to explain why there is only one solution.



So, you see that X which is that actual thing, which you are interested to compute will be equal to 3. So, 3 is this value, that is, 3 is this value, and you take 3 and multiply it with 5 and multiply with the inverse value.


(Refer Slide Time: 31:25)



Example

- $M = 5 \times 3 = 15$
- $M_1 = 15/5 = 3, 3^{-1} \pmod{5} = 2$
- $M_2 = 15/3 = 5, 5^{-1} \pmod{3} = 2$
- $x = (3 \times 3 \times 2 + 1 \times 5 \times 2) \pmod{15}$
 $= 28 \pmod{15} = 13$

What is the principle?



So, therefore, you take 3, you multiply with 3 and you multiply with 2. Similarly, you take 1, you multiply with 5 and multiply with 2, and if you take this, this works out to 28 and $28 \pmod{15}$ is actually equal to 13. So, what is the underlying principle? We will try to understand that first.

Sir


Yes



(Refer Slide Time: 31:58)

Generalization

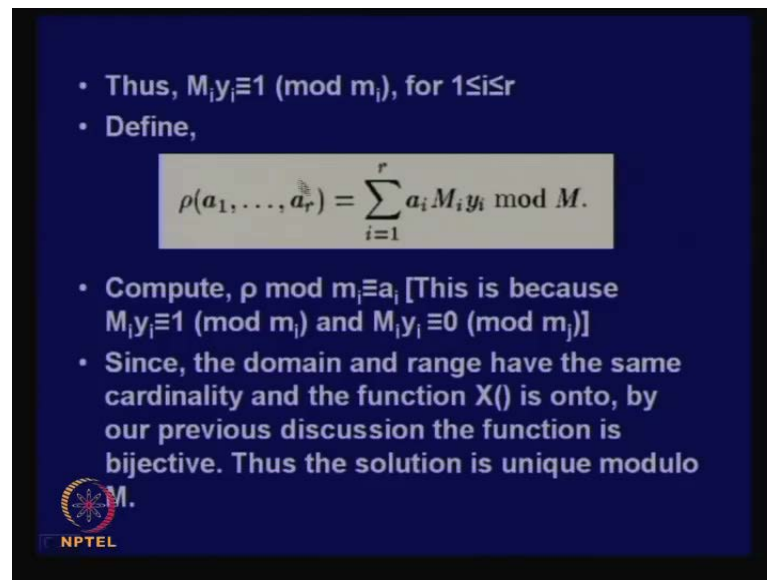
- We shall present a constructive proof
- In fact, CRT gives an explicit formula for $X^{-1} \pmod M$, where $M=m_1m_2\dots m_r$
- Compute, $M_i=M/m_i$ for $1 \leq i \leq r$
 - Thus, $\gcd(m_i, M_i)=1$
- Compute $y_i=M_i^{-1} \pmod m_i$

 NPTEL

So, let us do one thing. So, let us go ahead and read the solution and let us try to understand the principle, and then, we will go back to this example. So, maybe I could have placed this afterwards. So, let us present the constructive proof, that is, in fact, this Chinese remainder theorem gives an explicit formula for computing X inverse mod M - so, where m is actually equal to the product of m_1 to m_r , and what I do is that, for each step, I compute m_i where I divide M by small m_i .

So, what is the GCD of m_i and big m_i ? It is of course equal to 1, because you see that all these numbers are mutually co-prime. So, if you divide M by m_i , so, your factor out m_i . So, therefore, this m_i 's or capital m_i has to be co-prime with small m_i . So, now, therefore, I can take m_i inverse mod smaller m_i because m_i and small m_i are mutually co-prime. So, therefore, I can compute y_i in this fashion. So, therefore, now you see that y_i is equal to m_i inverse mod of small m_i .

(Refer Slide Time: 33:09)




• Thus, $M_i y_i \equiv 1 \pmod{m_i}$, for $1 \leq i \leq r$

• Define,

$$\rho(a_1, \dots, a_r) = \sum_{i=1}^r a_i M_i y_i \pmod{M}.$$

• Compute, $\rho \pmod{m_i} \equiv a_i$ [This is because $M_i y_i \equiv 1 \pmod{m_i}$ and $M_i y_i \equiv 0 \pmod{m_j}$]

• Since, the domain and range have the same cardinality and the function $X()$ is onto, by our previous discussion the function is bijective. Thus the solution is unique modulo M .



So, what I say is that, so, therefore, $M_i y_i$ will be equal to 1 if I take mod of m_i , but if you take mod of m_j where j is not equal to i , then what is this corresponding value, is actually equal to 0 because m_j will divide m_i . Do you understand this? That is, if I take $M_i y_i$ and I take mod of m_j where j is not equal to i , then this value will be equal to 0 because m_j will divide M_i .

So, what I say is that this is a . So, as I told you is a constructive proof. So, therefore, what I am saying is that this solution will be equal to $\sum a_i M_i y_i$. So, therefore, now you see that, what I am multiplying is that I am multiplying with a_i and I am multiplying with big M_i and I am multiplying with y_i . So, therefore, now you see that, if you go back to the example, this was the corresponding congruence value. M_i was the corresponding thing when you divided M by small m_i .

So, in that case, M was 15 and you are divided that with 5. So, you got 3, and what was the value of y_i ? It was 2; it was inverse. So, similarly you can get the second term also. So, the next thing to be understood is that why it is 2. So, this you can actually easily check because, so, therefore, first thing is that we will see that this really satisfies the original system of equation. So, you take this row and you take mod of some M_i values. See if you take mod of M_i , then obviously you understand that only for i , this value $M_i y_i$ will go to 1. So, you have only a_i .

But for the other things, that is, for the other j values, this will actually go to 0. So, only this will result in.

A_i

A_i . Therefore, if you take mod of m_i , then the of right hand side will be only reduced to a_i . So, therefore, what you can do is that, you compute this row mod m_i . So, row mod m_i will be equal to a_i , why? Now, because $M_i y_i$ is equal to $1 \pmod{m_i}$ and $M_i y_i$ equal to $0 \pmod{m_j}$ when j is not equal to i . So, therefore, the right hand side will only result in a_i . So, therefore, similarly, you can see that the all the system or equation will get satisfied.

So, therefore, what you observe here is this that, this mapping or which I called as a ψ_x or ψ_x is actually an onto mapping, which means that given any result, that is, given any corresponding congruence value, I am always able to find out an X value mod m which will satisfy this. So, which means that nothing is left out on the...

Right hand side

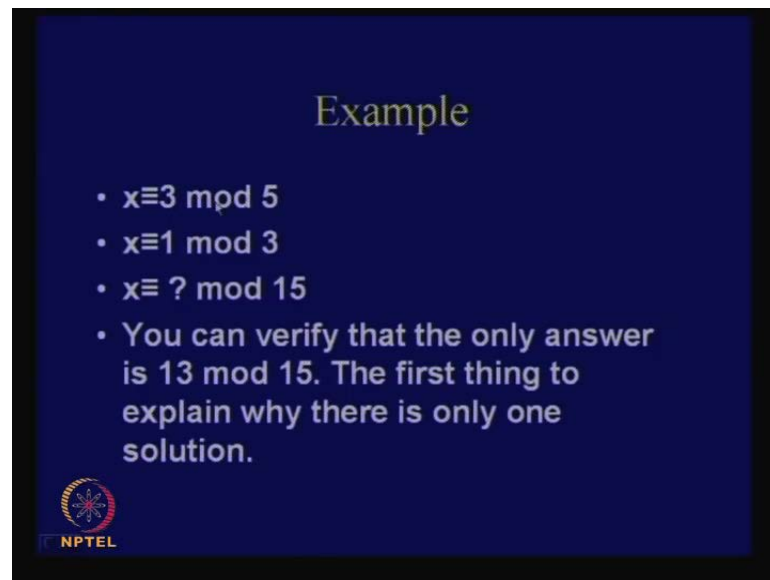
On the right hand side on the range part.

So, therefore, the next thing to be argued is that this function is actually a bijective function. Therefore, we have actually trying to show is that this is a unique mapping. So, since the domain and range have got the same cardinality, this becomes quite clear because we showed that the domain and range has got the same cardinality, and on the right hand side, these are also onto mapping. So, therefore, if you combine these two things, it becomes a bijective mapping; so that means, that the solution is actually unique modulo M . So that means that you not only get a solution, but this solution is actually only one and only one. This is clear?

(C)


Example, I gave you an example just now.

(Refer Slide Time: 36:59)

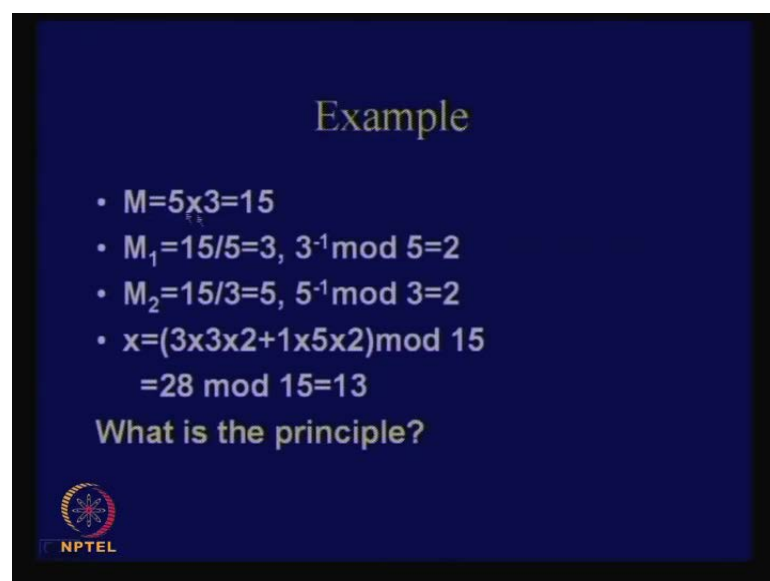


Example

- $x \equiv 3 \pmod{5}$
- $x \equiv 1 \pmod{3}$
- $x \equiv ? \pmod{15}$
- You can verify that the only answer is $13 \pmod{15}$. The first thing to explain why there is only one solution.




(Refer Slide Time: 37:11)



Example

- $M = 5 \times 3 = 15$
- $M_1 = 15/5 = 3, 3^{-1} \pmod{5} = 2$
- $M_2 = 15/3 = 5, 5^{-1} \pmod{3} = 2$
- $x = (3 \times 3 \times 2 + 1 \times 5 \times 2) \pmod{15}$
 $= 28 \pmod{15} = 13$

What is the principle?




I gave you just now, this is example this. So, what I am interested into compute is this - X equal to $3 \pmod{5}$ and X equal to $1 \pmod{3}$. So, I am interested in computing this mod 15. So, what I do is that I take M . So, if I take 5 when I take 3 and I multiply them, I get 15. So then, what I do is that, I take 15 and I divide with the first M_i value. So, that is 3, and then, I take 3 inverse mod of 5. So, 3 inverse mod of 5 will be 2. So, similarly I take 15 divided by 3, I get 5 and I take the inverse of 5 it is 2.

So, therefore, X you can actually write in this fashion. So, this is that sigma thing which you saw. So, this is if you open up the sigma, you get this that 3 into 3 into 2 plus 1 into 5 into 2; it works out to 28 and mod 15 equal to 13. You can check this.

(Refer Slide Time: 37:50)

Example

- $x \equiv 3 \pmod{5}$
- $x \equiv 1 \pmod{3}$
- $x \equiv ? \pmod{15}$
- You can verify that the only answer is $13 \pmod{15}$. The first thing to explain why there is only one solution.

 NPTEL

So, therefore, this 13 you can see will satisfy this system of equation, because if you take mod 5, it is 3; if you take mod 3, it is 1. Therefore, 13 satisfies this simultaneous equations congruences actually.

(())


(Refer Slide Time: 38:05)

Uniqueness

- $X(x) = (x \pmod{5}, x \pmod{3})$

$\chi(0) = (0, 0)$	$\chi(1) = (1, 1)$	$\chi(2) = (2, 2)$
$\chi(3) = (3, 0)$	$\chi(4) = (4, 1)$	$\chi(5) = (0, 2)$
$\chi(6) = (1, 0)$	$\chi(7) = (2, 1)$	$\chi(8) = (3, 2)$
$\chi(9) = (4, 0)$	$\chi(10) = (0, 1)$	$\chi(11) = (1, 2)$
$\chi(12) = (2, 0)$	$\chi(13) = (3, 1)$	$\chi(14) = (4, 2)$

Note that the mapping is bijective...

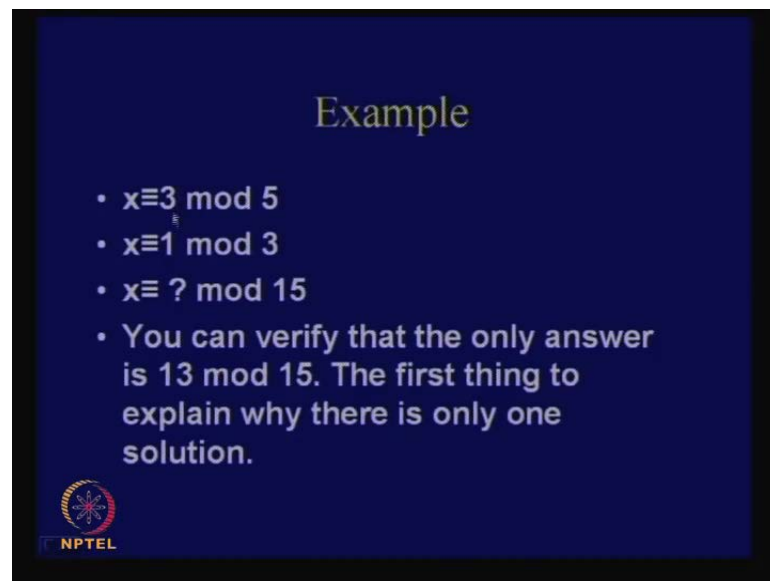
 NPTEL

Cardinality becomes equal from here because you see that your input size is actually equal to what? You have been, there are 15 values in this case in the domain part. In the range part also you are storing them as these numbers can vary from what? From mod 5 and mod 3.

So, the first ordinate will actually vary from 0 to 4. There are 5 values. In the second case also there are 3 values. So, how many possibilities are there? There are also 15 values. So, in the domain and in the range there are, I mean both of them have got the same cardinality, and at the same time you also showed that it is onto. Therefore, it is a bijective mapping.

(C)

(Refer Slide Time: 38:53)



Example

- $x \equiv 3 \pmod{5}$
- $x \equiv 1 \pmod{3}$
- $x \equiv ? \pmod{15}$
- You can verify that the only answer is $13 \pmod{15}$. The first thing to explain why there is only one solution.

NPTEL

So, what I am saying is like this, that is, suppose I am giving you some solution here like this where these are co-prime and all this things. So, there are actually from their, you can at least find out one X value for which this is getting satisfied.

(Refer Slide Time: 39:07)

Uniqueness

- $X(x) = (x \bmod 5, x \bmod 3)$

$\chi(0) = (0, 0)$	$\chi(1) = (1, 1)$	$\chi(2) = (2, 2)$
$\chi(3) = (3, 0)$	$\chi(4) = (4, 1)$	$\chi(5) = (0, 2)$
$\chi(6) = (1, 0)$	$\chi(7) = (2, 1)$	$\chi(8) = (3, 2)$
$\chi(9) = (4, 0)$	$\chi(10) = (0, 1)$	$\chi(11) = (1, 2)$
$\chi(12) = (2, 0)$	$\chi(13) = (3, 1)$	$\chi(14) = (4, 2)$

Note that the mapping is bijective...

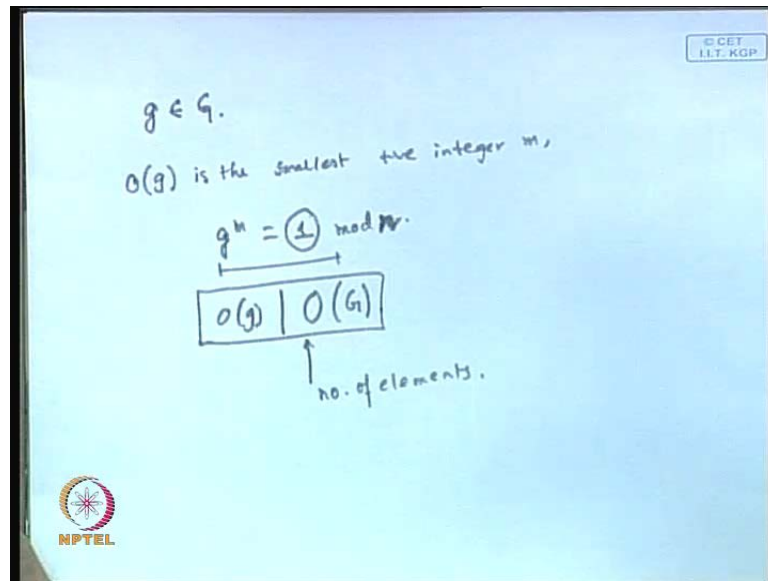
So; that means, in the right hand side, I mean you can note that this is like a function. Therefore, you see that if I give you some value in the right hand side, in the left hand side you always getting 1 value; it is not that you are not getting some value. From this function, you will definitely get at least one value. And since the number is same in both the cases, there has to be a it is a bijective mapping. You can also actually formally prove this by fusional principle also, but I am not going to do that. So, but this is quite straight forward actually. I hope you understand this.

(Refer Slide Time: 39:41)

Other Useful Facts

- Suppose G is a multiplicative group of order n , and $g \in G$. Then the order of g divides n .
- Corollary 1: If $b \in \mathbb{Z}_n^*$, then $b^{\phi(n)} \equiv 1 \pmod{n}$
- Corollary 2: Suppose p is prime and $b \in \mathbb{Z}_p$. Then $b^p \equiv b \pmod{p}$

(Refer Slide Time: 40:14)



So, therefore, you will now conclude with some more useful facts say which will be useful for our understanding actually. So, suppose G is a multiplicative group of order n and G is belonging to G . So, assume that G is a multiplicative group and has got order n . So, order n means that number of elements are actually n .

So then, the order of G will actually divide n . So, what is small g 's order? So, suppose there is a multiplicative group and say there is a g element which belongs to capital G , then the order of g , I call this as order of g is actually equal is the smallest number or smallest positive integer m for which g power m is equal to 1. And of course, this is the corresponding unity element so that identity element. Therefore, g to the power m is equal to 1 or 1.

1 mod

And yes, mod of m of course. So, what I am saying essentially is that, the order of g will divide actually n . So, therefore, the order of g will actually divide the number of elements in the group G . So, this is actually O means this is, are the number of elements in G . So, this I am not proving, this is called Lagrange's theorem. So, we will just assume this.

(C)

Mod m

()

(Refer Slide Time: 41:45)

The slide has a dark blue background with yellow text. The title 'Other Useful Facts' is centered at the top. Below it are three bullet points. The first bullet point states: 'Suppose G is a multiplicative group of order n, and $g \in G$. Then the order of g divides n.' The second bullet point is 'Corollary 1: If $b \in \mathbb{Z}_n^*$, then $b^{\phi(n)} \equiv 1 \pmod{n}$ '. The third bullet point is 'Corollary 2: Suppose p is prime and $b \in \mathbb{Z}_p$. Then $b^p \equiv b \pmod{p}$ '. In the bottom left corner, there is a circular logo with a star and the text 'NPTEL' below it.

1 mod n. So, therefore, there are two natural interesting corollary that as follows. If you take b which belongs to \mathbb{Z}_n^* , so, \mathbb{Z}_n^* is a multiplicative group that we k. Now, therefore, suppose the order of b is say d. So, therefore, b to the power of d should be equal to 1, and what is the order of the group \mathbb{Z}_n^* ? It is $\phi(n)$. $\phi(n)$ we have seen. What is a $\phi(n)$? Therefore, b to the power of $\phi(n)$ has to be equal to 1 mod n because b will divide $\phi(n)$, and therefore, b to the power of $\phi(n)$ is also equal to 1.

Yes

Similarly, from this, it follows that, if n is a prime number, then $\phi(p)$ will actually be equal to p minus 1. So, b to the power of p minus 1 will be equal to b. Therefore...

()

Yes

So, therefore, b to the power p will be equal to b mod p. And this is written in this form, and I mean because suppose there can be two cases. So, here, we have written b belongs to \mathbb{Z}_p . So, first of all, assume that b belongs to \mathbb{Z}_p^* . So, what does it mean? Whom does it exclude?

()

No, whom does it p is a prime number.

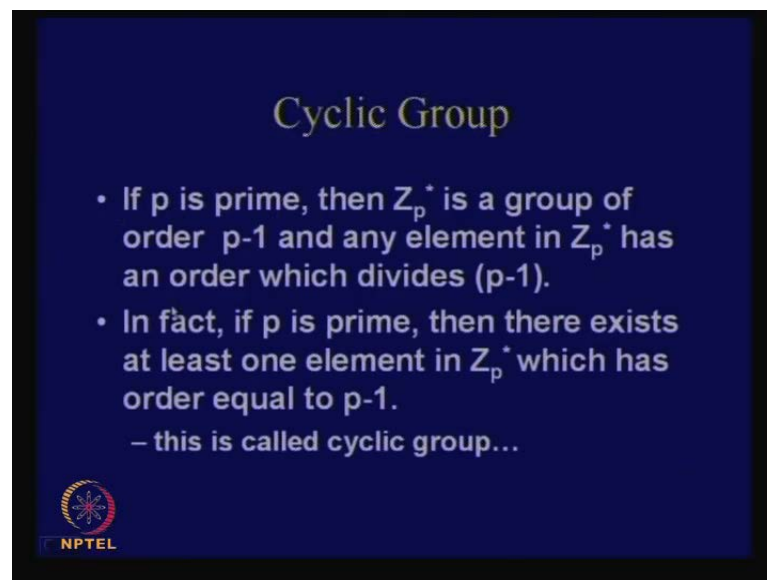
So, all elements are co-prime, but if I say b belongs to Z_p^* and then; that means that from b belongs to Z_p which element am I excluding?

(())

0


I am excluding 0. In Z_p , actually 0 is there, but in Z_p^* 0 is not there. So, here, you see that 0 will satisfy this equation trivially. So, therefore, what we need to show is only the when b belongs to Z_p^* . And if b belongs to Z_p^* , then the previous result holds. So, b to the power of p . So, b to the power of p means what? b to the power p minus 1. See, in that case also this holds. So, therefore, this holds for b belongs to Z_p . That is why it is written like this b to the power p is actually equal to $b \pmod p$. But if I written b to the power of p minus 1 equal to 1, then b would have belong to Z_p^* ; I could have now written b belongs to Z_p .

(Refer Slide Time: 43:56)



Cyclic Group

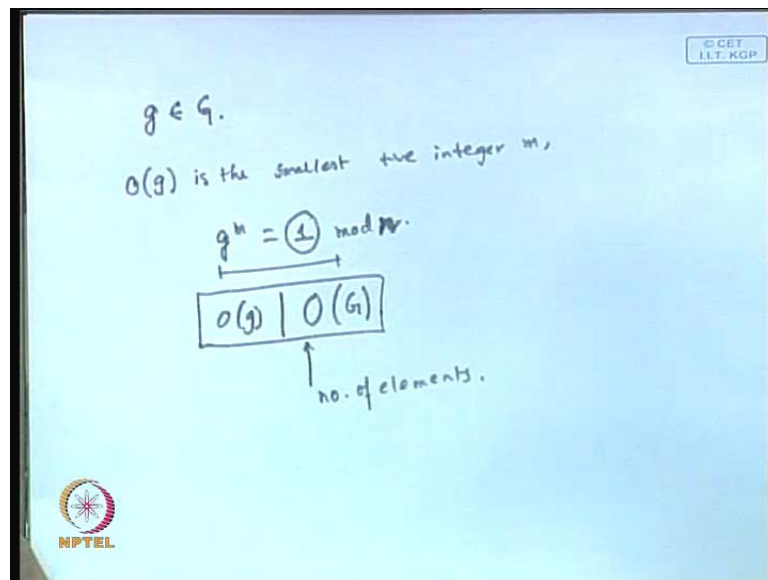
- If p is prime, then Z_p^* is a group of order $p-1$ and any element in Z_p^* has an order which divides $(p-1)$.
- In fact, if p is prime, then there exists at least one element in Z_p^* which has order equal to $p-1$.
 - this is called cyclic group...

 NPTEL

So, therefore, so, therefore, so, we have seen that what is the cyclic group. So, you see that if p is a prime, then Z_p^* is the group of order p minus 1 and any element in Z_p^* which as an order which will divide p minus 1. So, in fact, if p is prime, then there exists at least 1 element in Z_p^* which has got an order equal to p minus 1.

So, what does it mean that, if you take that particular element and if you keep on multiplying, then the smallest number for which it will repeat or it will give you 1 is actually $p - 1$. So, that is, at least 1 element whose order is actually equal to $p - 1$, and therefore, it is called as a cyclic group, because if you take this element, then it will generate all the elements in that field, and finally, it will come back to itself. So, therefore, it is called as cyclic group and this element is sometimes called the primitive element. So, here, if you remember that cycle that we draw in context to AES, you take an element if you keep on multiplying like α , α^2 , α^3 , α^4 and so on. Then finally, you get α^{p-1} , it will be equal to 1.

(Refer Slide Time: 45:10)




And $p - 1$ is the smallest number for which that happens; so that means, this α if you multiply, it will generate all the elements in that field, and therefore, the name called cyclic group.

(Refer Slide Time: 45:30)

Primitive Element

- If p is prime, then \mathbb{Z}_p^* is a cyclic group.
- Any element α having order $p-1 \pmod p$ is called a primitive element. Thus α is a primitive element iff:

$$\{\alpha^i : 0 \leq i \leq p-2\} = \mathbb{Z}_p^*$$




So, therefore, primitive element is defined like this. If p is prime, then \mathbb{Z}_p^* is a cyclic group, and any element α having order $p-1 \pmod p$ is called a primitive element. So, thus α is a primitive element if and only if. If you take α to the power of i and from 0 to $p-2$, you get actually the entire \mathbb{Z}_p^* . So, therefore, you can use α and compute the corresponding powers, and finally, you get the entire \mathbb{Z}_p^* . So, therefore, α generates the entire group. So, α is called the primitive element.

(Refer Slide Time: 46:02)

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	α^{15}	α^{16}	α^{17}	α^{18}	
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1	1	1	1
3	6	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1	1	1	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1	1	1	1
5	6	11	17	9	7	16	4	1	3	6	11	17	9	7	16	4	1	1	1	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1	1	1	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	1	1	1
8	7	18	11	12	1	6	7	18	11	12	1	6	7	18	11	12	1	1	1	1
9	3	7	6	16	11	4	17	1	9	3	7	6	16	11	4	17	1	1	1	1
10	5	12	6	3	11	15	17	16	9	14	7	13	16	6	4	2	1	1	1	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	1	1	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1	1	1	1
13	17	12	4	14	11	10	16	18	6	2	7	15	3	8	9	1	1	1	1	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1	1	1	1
15	16	12	9	2	11	13	5	18	4	1	10	17	8	6	14	1	1	1	1	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1	1	1	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1	1	1	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	1	1	1

- $n=19$, There are 6 primitive elements.
- Note the order of each element in \mathbb{Z}_{19}^* .

Is there a relation?



So, you see that this is an example to a clear that. So, you take alpha here and alpha is equal to 2 and you keep on computing the powers. So, therefore, here your n value is 19. So, I am taking mod 19; so, that means, I am computing alpha, alpha square, alpha power 3 alpha power 4 and so on till alpha power 18. So, you see the alpha power 18 is equal to 1; so, that means, now you see that all the elements which are there in Z_n^* is actually generated here. So, that means what? This alpha is a primitive element because it is generating in the entire group.

So, you see that there are some elements for which the order is not actually equal to p minus 1, but smaller than p minus 1, but in this case, you will find that there are exactly 6 primitive elements, why, because this is one primitive element; this is one primitive element; this is one primitive element; this is another primitive element; this is another primitive element; this is another primitive element. So, how many primitive elements you have? There are six primitive elements.

So, can I justify why there are exactly 6 when n is equal to 19? So, we will try to see all these things. So, therefore, note that the order of each element. So, you can note that the order of each element in Z_{19}^* and you will find that. It will divide the, I mean each order which you take here will actually divide, divide what?

(())

19 or 19 minus 1?

19 minus 1

19 minus 1

So, therefore, each order will actually divide 19 minus 1 and primitive element will have the largest order. So, the order of primitive element is actually equal to 18. So, therefore, you see that, do you understand why it is a cyclic group, because you take this, it will go back to 1 means after that, if you multiply, it will come back to this. So, it will continue like this. Actually all the elements are cyclic groups. So, if you take these, therefore, you take 4 16 7 9 17 11 16 5 1; again it come backs to 4. So, you see that all of them are forming cyclic groups, but only the largest if you take a primitive element, then it forms the entire multiplicative group.


(Refer Slide Time: 48:19)

Order of any element

- Any element β in Z_p^* (where p is prime) can be written uniquely in the form $\beta = \alpha^i$, where α is a primitive element and $0 \leq i \leq p-2$.
- The order of β is:

$$\frac{p-1}{\gcd(p-1, i)}$$

- β is itself primitive iff $\gcd(p-1, i) = 1$. Hence, what is the number of primitive elements modulo p ?

 NPTEL

So, actually you can show that any element b in Z_p^* where p is a prime can be written uniquely in the form of $\beta = \alpha^i$. So, this follows straight from the definition of primitive element. Where α is a primitive element and lies between 0 and $p-2$ the order of β . So, where $\beta = \alpha^i$ the order of β is actually equal to $p-1$ divided by $\gcd(p-1, i)$, and β is itself primitive if and only if $\gcd(p-1, i) = 1$.

So, now, can you say how many primitive elements will be there?

Yes

(())

What?

You said something.

5 of $p-1$

So, if you take in this case 19 , therefore, number of primitive elements will be 5 of 18 .

So, what is 5 of 18 ?

(Refer Slide Time: 49:15)

$18 = 3^2 \times 2.$
 $\phi(18) = \underline{\underline{6}}.$
 $\text{order}(\beta) = \frac{p-1}{\gcd(p-1, i)}.$
 $\beta = \alpha^i \rightarrow k.$
 $\beta^k \equiv 1 \pmod{p}$
 $\alpha^{ik} \equiv \alpha^{t(p-1)} \pmod{p} \Rightarrow ik = t(p-1).$
 $\therefore k = \frac{p-1}{\gcd(p-1, i)}.$
 $\frac{i}{t} | p-1. \quad \frac{i}{t} | i$

So, what is 18? 18 I can write as 3 square into..

2

2. So, what is phi 18?

(C)

Phi of 18 is 6. I hope you remember that 18 into 1 minus 1 by 3, and similarly, you can write that. So, this will compute to 6. So, therefore, that is the reason why you had exactly six primitive elements. So, now, why is the order of beta equal to p minus 1 also we can justify I think. Let it be like this, that is, order of beta is equal to p minus 1 divided by GCD of p minus 1, i. So, I will be try to give you a simple proof for this, that is, if you take say beta equal to alpha to the power of I and let the order of this element be it is a K - where K is some positive integer; so that means what? That beta to the power of K should be equal to 1 mod of p.

So, this one I could have written as some alpha to the power of some t into p minus 1 mod p, where alpha is the corresponding primitive element because alpha to the power of p minus 1 is what? 1. So, therefore, this is 1. So, what about the left hand side? It is beta to the power of k. So, therefore, that is alpha to the power of ik is equal to alpha to the power of t p minus 1.

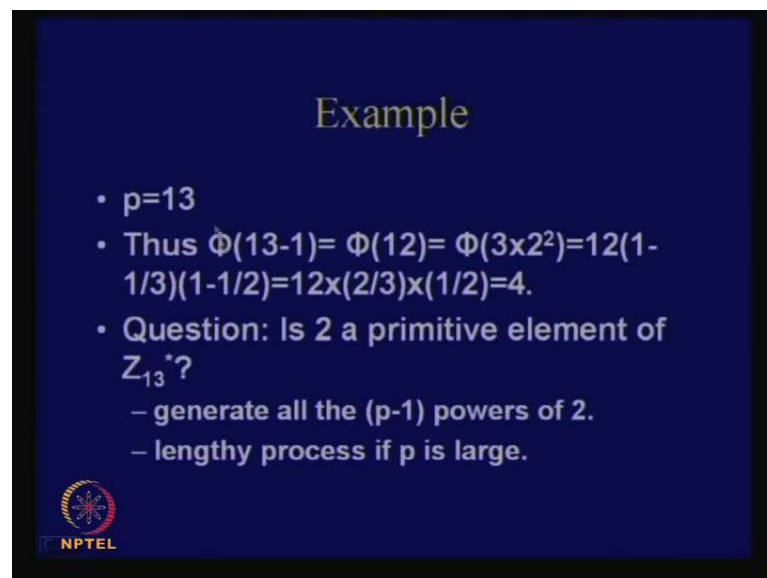
So, from here, I can actually write that i of k equal to t of p minus 1, and therefore, k is equal to p minus 1 divided by i by k . So, now, certain things becomes important, I mean observable from here. That first of all, i of k has to divide p minus 1 because otherwise k is not integer.

Sir, i by t .

Sorry, i by t , yes.

So, i by t . So, i by t has to divide p minus 1. So, i by t has to divide p minus 1, and what is the other thing that you observe from here that i by t has to be a factor of i also. So, i by t is also a factor of i . So, therefore, now if i since the order is actually the least such number, therefore, it has to be corresponding to this denominator has to correspond to the greatest common divisor of p minus 1 and i , because the order is the least such number. So, therefore, it actually equal to p minus 1 divided by greatest common divisor of p minus 1 and i .

(Refer Slide Time: 52:09)



Example

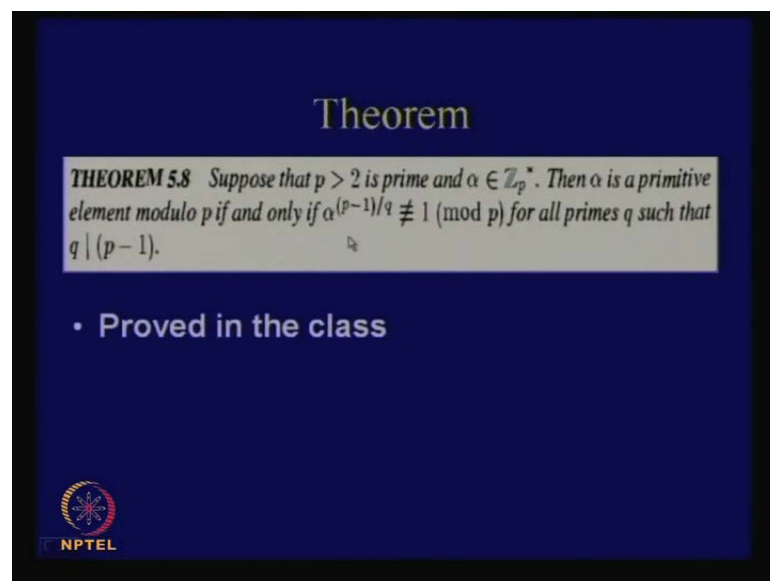
- $p=13$
- Thus $\Phi(13-1) = \Phi(12) = \Phi(3 \times 2^2) = 12(1 - 1/3)(1 - 1/2) = 12 \times (2/3) \times (1/2) = 4$.
- Question: Is 2 a primitive element of Z_{13}^* ?
 - generate all the $(p-1)$ powers of 2.
 - lengthy process if p is large.

NPTEL

So, this you can prove in a other ways also. This is just one sample. So, you see that p equal to 13 ϕ of 13 minus 1 equal to ϕ of 12 and that is actually equal to 4 or 6?

Now, this is this is a different example I think. So, p equal to 13 ϕ of 13 minus 1 equal to ϕ of 12, this works out to 4. So, what does it show? It shows that if you take p equal to 13, then there are 4 primitive elements. So, the question now which I will ask you is that is 2 a primitive element for \mathbb{Z}_{13}^* . So, what it will do? The first thing that we can do is that we will generate all the p minus 1 powers of 2 and check that whether it is equal to 1. So, this is quite a lengthy process.

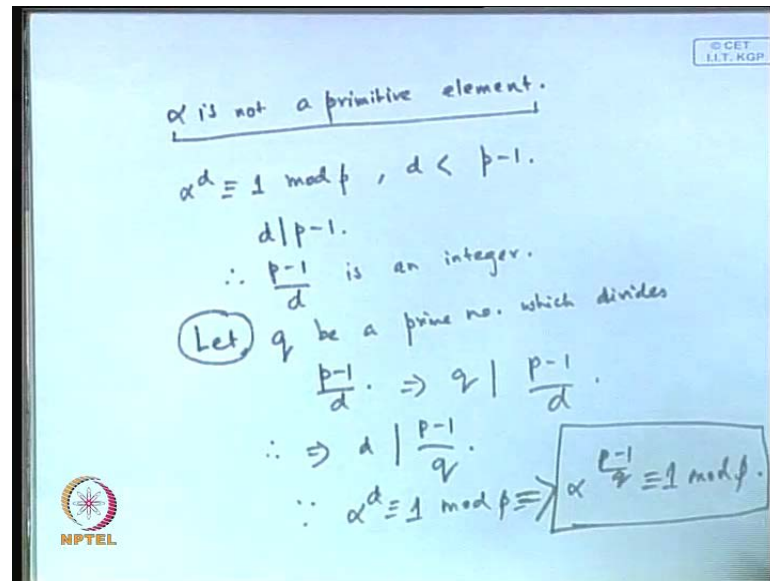
(Refer Slide Time: 52:48)



So, actually, luckily we have this theorem which gives you easy check for the **primarity**, so, for the primitiveness. It says that suppose that p is greater than 2 is prime and α it belongs to \mathbb{Z}_p^* . Then α is a primitive element modulo p if and only if α to the power of p minus 1 divided by q is actually not equal to 1 mod p for all primes such that q divides p minus 1. So, how can I proof this result? So, you see that one part is quite clear, because if α is actually a primitive element, then obviously p minus 1 by q being smaller than p minus 1. This can never be equal to 1, because in that case, α is not a primitive element.

The other thing that we needs to be proved is that, if α to the power of p minus 1 by q is not equal to 1 for all such primes, then α is a primitive element. So, therefore, the contrapositive of this would be what? That if α is not a primitive element, then there exists a q which divides p minus 1 such that α to the power of p minus 1 by q is equal to 1. That is the contrapositive. So, we will prove this.

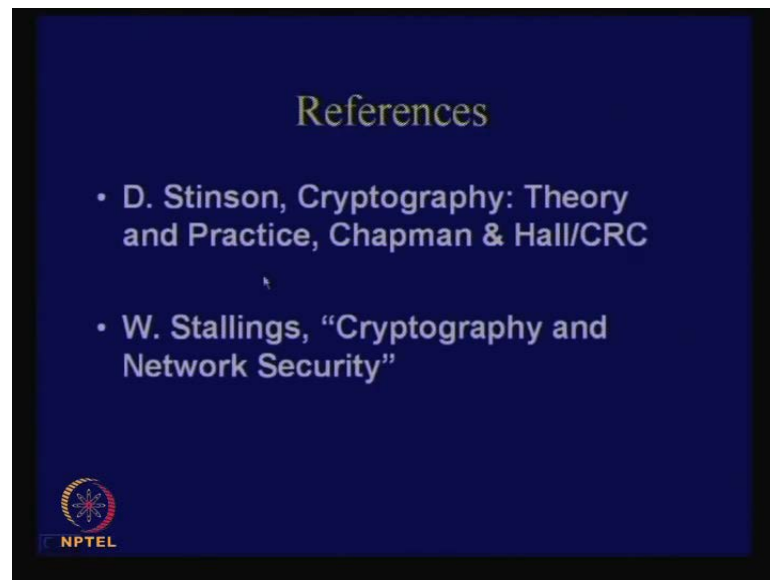
(Refer Slide Time: 54:02)



So, therefore, we will say that alpha is actually a not, I mean alpha is not a primitive element. So, which means that there exists an alpha power d, which is equal to 1 mod p, and what d is actually? Smaller than p minus 1. So, we know that d divides p minus 1. Therefore, p minus 1 by d is actually an integer value. So, therefore, let q be a prime number which divides p minus 1 by d. So, you see that the moment I am saying that, let q be a prime number. So that means that, basically what I am saying is that there exists a q for which this is true.

So, therefore, q divides p minus 1 by d. So, therefore, this implies that d also divides p minus 1 by q. So, now, since alpha to the power of d is equal to 1 mod p, this implies that alpha to the power of p minus 1 by q is also equal to 1 mod. So, therefore, this proves the result. Did you follow the proof?

(Refer Slide Time: 55:46)



(Refer Slide Time: 55:51)



So, that concludes this particular lesson. So, we are followed from Stinson and also portions from William Stallings cryptography and network security, and next day, we will continue with the RSA cryptosystem.