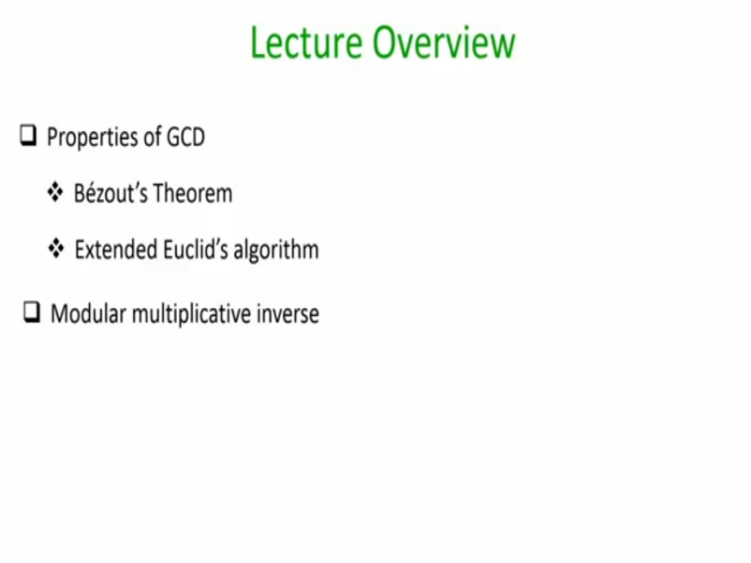
Discrete Mathematics
Prof. Ashish Choudhury
International Institute of Information Technology, Bangalore

Lecture – 57
Properties of GCD and Bezout's Theorem

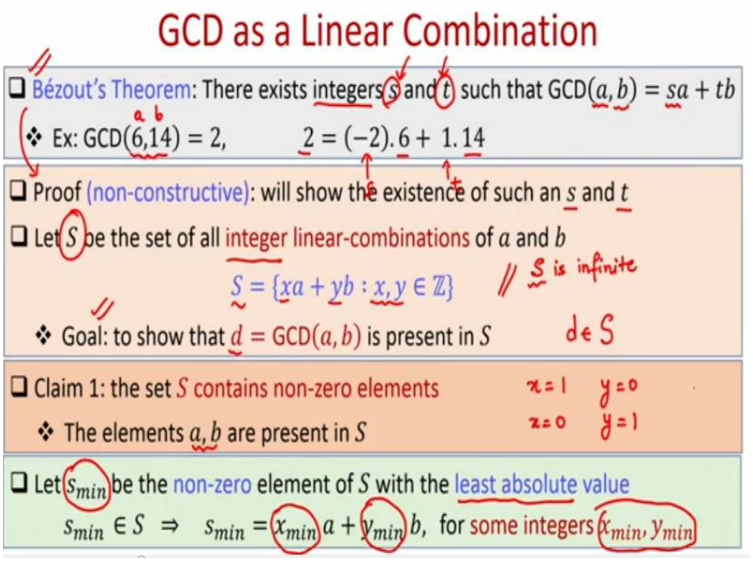
Hello, everyone, welcome to this lecture, in this lecture we will discuss about the properties of GCD and we will also discuss about Bezout's theorem.

(Refer Slide Time: 00:29)



So, the plan is as follows, we will discuss Bezout's theorem, we will discuss about extended Euclid's algorithm and then we will discuss about modular multiplicative inverse.

(Refer Slide Time: 00:42)



So, let us start with Bezout's theorem, which is a very interesting theorem. And what it says is the following. It says that you can always express the GCD of 2 numbers as a linear combination of the 2 numbers itself. So, more specifically, if you are given 2 values a and b and if you have found their GCD, then what the theorem says is that you can always find integer linear combiners that is important, you can always find integer linear combiners s and t, such that if you linearly combine a and b using this combiners s and t respectively, then that will give you the GCD. And when I say integer combiners s and t, your s and t may not be positive they can be can be negative as well, the only condition is that they should be they are integers. So, for instance, if you take a and b to be 6 and 14, respectively then the GCD is 2.

And it is easy to see that I can write 2 as a linear combination of my a and b, namely 6 and 14, where my linear combiners s and t are -2 and 1 respectively. So, that is the Bezout's theorem. And we will prove this theorem and the proof is slightly involved. So, please pay attention here and proof will be non-constructive. Namely, I would not show you the exact linear combiners s and t for a given a and b. But I will argue that indeed, there exist linear combiners s and t satisfying the conditions of Bezout's theorem.

Later, we will see a constructive proof as well when we are given a and b, I can show you how to construct your linear combiners s and t. So, as I said the proof is non-constructive. And the goal will be to show the existence or I will logically argue about the existence of s and t. So, to begin

with, let me first define a set S, which is a set of all integer linear combinations of your inputs a and b.

Remember throughout the proof, we will be focusing only on integer linear combinations, because the theorem says that we can find integer linear combiners s and t. So, let S be the set of all integer linear combinations of a and b. So, S is the form x times a + y times b where my linear combiners x and y can be arbitrary integers, $S = \{xa + by : x, y \in \mathbb{Z}\}$. So, it is easy to see that S is infinite because my linear combiners x and y can be any arbitrary integers and there are infinite number of integers.

Now, it is an exercise for you to find out whether the set S is whether it is countably infinite or uncountable, whether its cardinality is ℵ or not. Now, my goal is to show the following if I want to prove the Bezout's theorem, I have to show that the GCD of a, b is also an element of the set S. So, let d denote the GCD of a and b, my goal is to show that this element d is also a member of the set S, namely it can be expressed as some integer linear combination of a and b.

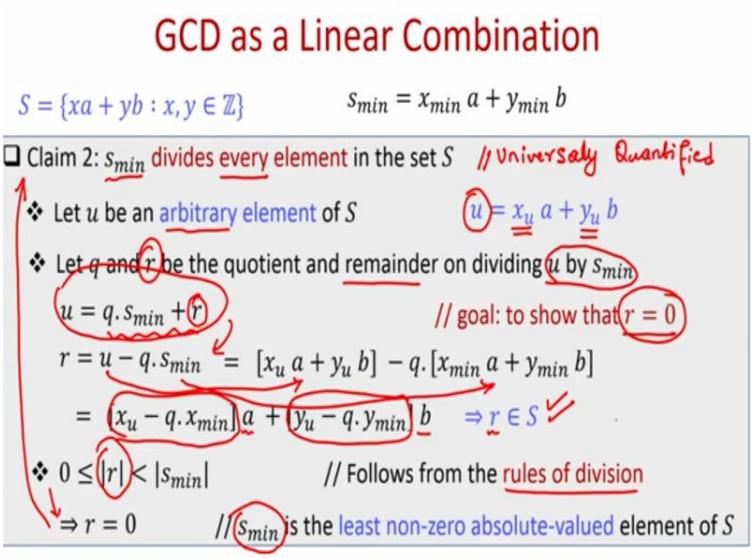
So, I will prove or I will achieve my goal using a series of claims. So, the first claim is very simple. It says that the set definitely contains non-zero elements. Of course, it will contain 0 element as well because if I set my linear combiners x and y to be 0, then 0 times a + 0 times b will be 0. So, 0 is of course, an element of S. But other than 0, set S also have non-zero elements. And two trivial examples of non-zero elements which are present in the set S are a and b.

So, if I set x = 1 and y = 0, if these are my linear combiners then I obtain a belonging to S and if I set x = 0 and y = 1 then I get b belonging to the set S. So, claim 1 is trivial to prove. Now there are infinite number of non-zero elements in the set S. Among all those nonzero elements I denote by s_{min} the element which has the least absolute value, that is important I am not focusing whether s_{min} is positive or negative, s_{min} could be negative as well, but it has the least absolute value.

So, you have the element 0 present in S and you have the non-zero elements present in S the non-zero elements are positive as well as negative among them s_{min} denotes the element which has

the least absolute value. So, since s_{min} is a member of the set S that means, there exists some linear combiners x_{min} and y_{min} such that s_{min} is x_{min} times a + y_{min} times b. And again this linear combiners x_{min} and y_{min}, they can be positive negative, they are some arbitrary integer combiners.

(Refer Slide Time: 06:18)



Now, my claim 2 is the following. I claim that this element s_{min}; it divides every element of the set S. That is very interesting. And since this is a universally quantified statement, because I am claiming that s_{min} has a property with respect to all the elements of the set S, so the statement is universally quantified. The proof strategy for proving this claim is that I take some arbitrary element u from the set S and show that s_{min} indeed divides that arbitrary u.

And then using universal generalization, I can conclude that indeed my claim is correct. So, let u be some arbitrary element of the set S. So, corresponding to u let the linear combiners are x_u and y_u. Now, my goal is to show that this u is completely divisible by s_{min}. So, imagine that u is some q times s_{min} + r. I do not know what exactly is the remainder r my goal is to show that indeed, u is completely divisible by s_{min}.

So, my goal is to show that r is 0. But in general, I can write u in this form, I can say u is some quotient times s_{min} + r. And from this, I get that r is equal to the difference of u and q times s_{min}. And remember, my goal is to show r is 0 then only I can conclude that u is completely divisible by s_{min}. Now, what I can do is the following, I substitute the value of u in terms of linear

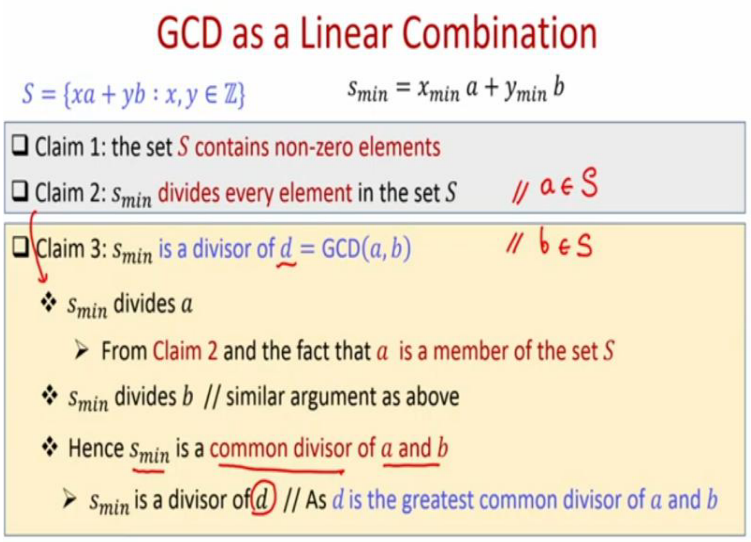
combinations of a and b and I substitute the value of s_{min} in terms of linear combinations of a and b.

And this overall thing I can write again as a linear combination of a and b where this will be my linear combiner for with respect to a and this will be the linear combiner with respect to b. So that means I get that the element r is also a member of the set S. Now, what can I say about the range of the absolute value of r. So, since r is the remainder, obtained by dividing u by s_{min}, the remainder can be 0. And it can be at most $s_{min} - 1$, that is a fact that I have that follows from the rules of the division.

So, I can say that the absolute value of r could be either 0 or it is strictly less than the absolute value of s_{min}. But this implies that r has to be 0. And this is because of my assumption that s_{min} is the is least non-zero absolute valued element of S. Remember, s_{min} is also an element of the set S and it is a special element of the set S in the sense that among all the non- zero elements of the set S, s_{min} has the least absolute value.

So, how can it be possible that you have another element r which is also an element of the set S and its absolute value is strictly less than s_{min}. That is not possible. That is possible only if $r = 0$ that means r is not a non-zero element. And that is precisely what I wanted to prove I wanted to prove that indeed u is some q times s_{min}. So that proves my claim number 2.

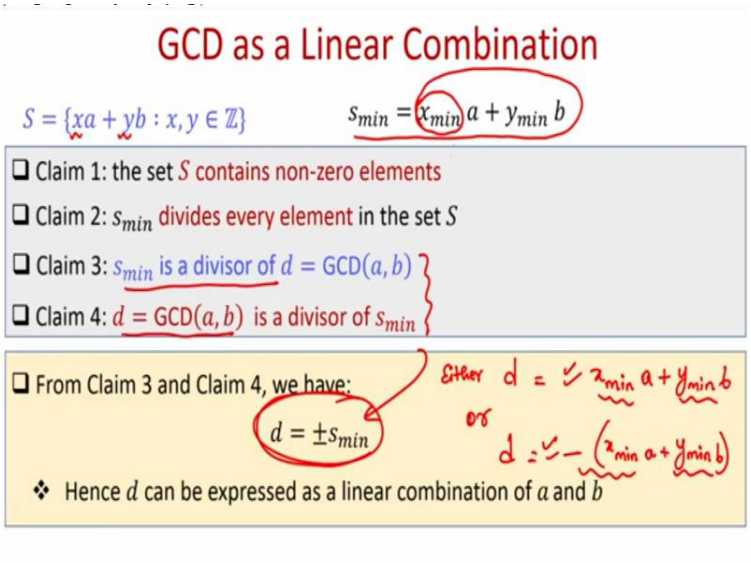
(Refer Slide Time: 10:17)



Now, my third claim is the following. I claim that the value s_{min} is a divisor of your GCD of a and b. So, remember, d is the GCD of a and b. And let us prove this claim number 3. So, from claim number 2, I know that s_{min} divides every element in the set S and remember that the element a belongs to the set S as well. So that means s_{min} divides a as well. So that is a proof for this fact. And due to the same reason, I know that b is a member of the set S and from claim 2 s_{min} divides every element of the set S so that means s_{min} divides b as well. That means what I can say is the following s_{min} is a common divisor of a and b. And if s_{min} is a common divisor of a and b that means s_{min}, of course is a divisor of the common divisor of a and b which is the greatest in the sense it is the largest common divisor of a and b.

So that proves your claim number 3, because if s_{min} is a common divisor of a and b, but s_{min} may not be the greatest common divisor there might be another divisor which is bigger than s_{min} and which divides a and b both in that case I can say that s_{min} divides that common divisor d as well. So that proves my claim number 3.

(Refer Slide Time: 11:52)



Now, I will show that the common greatest common divisor of a and b is also a divisor of s_{min}. And then finally using claim 3 and 4 I will conclude that Bezout's theorem is true. So, let us prove claim number 4. So, since d is a common divisor of both a as well as b that means d has to divide a and that means d divides any multiple of a as well. Similarly d is a divisor of b as well because d is a common divisor of both a and b. So, if it is a common divisor of a and b both it will be dividing b and hence d will divide any multiple of b as well.

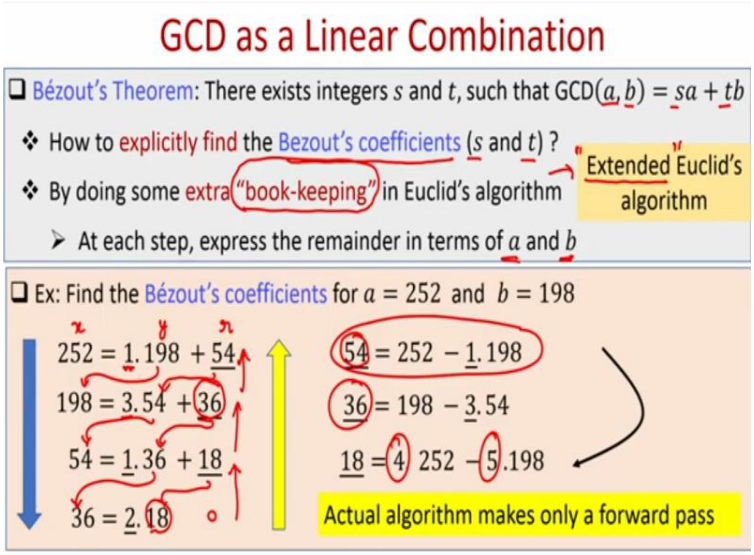
Now, if d divides x times a, for every integer x, and if d divides every integer multiple of b, then I can say that d divides x times a + y times b for every integer x and y and hence, I can conclude that d is a divisor of s_{min}. Because s_{min} is also some linear combination of a and b. So, what I have shown here is that d is a divisor of every x times a + y times b that means you take any integer linear combination of a and b, d divides that integer linear combination.

And s_{min} is also one of the integer linear combination of a and b. So, hence d divides s_{min} as well. So, these are the 4 claims that I have established. Now what I can do is the following. From claim 3 and 4, I can conclude that the value of d is either the same as s_{min} or it is same $-s_{min}$ because claim 3 says s_{min} is a divisor of d and claim 4 says that d is a divisor of s_{min} that is possible only if this condition holds, $d = \pm s_{min}$.

That means; and what is s_{min}? s_{min} is a linear combination of a and b; that means either d is equal to positive x_{min} times a + y_{min} times b or d is equal to minus of (x_{min} times a + y_{min} times b). So, if this is the case, then my linear combiners are x_{min} and y_{min} whereas if this is the case, then my linear combiners are $-x_{min}$ and $-y_{min}$. Irrespective of the case I know that d is expressible as an integer linear combination of a and b

So, Bezout's theorem has been proved. Specifically we have shown this. But why this is a non-constructive proof is the following. We do not know the exact value of x_{min} and y_{min}, which will give me s_{min}, because the set S is an infinite set. And I cannot iterate over all possible integer combiners, x and y and come with the minimum value x_{min} and y_{min}, because my set is infinite. So that is why it is a non-constructive proof, but logically I have argued that the greatest common divisor of a and b can be expressed as some linear integer combination of a and b itself.

(Refer Slide Time: 15:42)



So now, the next interesting question will be that how exactly I find those integer linear combiners. So, if you are given a and b, by running the Euclid's algorithm, you can find their GCD but if I also want to find out the integer linear combiners as which are guaranteed to exist as per the Bezout's theorem, how exactly I can find them. And you might be wondering that why at the first place, I will be interested to find out the Bezout's coefficient. So, these integer linear combiners, they are called as Bezout's coefficient.

So, you might be wondering why at the first place I am interested to find them; later on when we will discuss about modular multiplicative inverse, this Bezout's coefficients will come very handy, so that is why we want to find them. So, it turns out that by doing some extra book-keeping, that means by maintaining some additional values and data structure in my Euclid algorithm, which are used for finding out the GCD of a and b, I can find out the Bezout's coefficient as well.

And running time will remain more or less the same, I would not have to do significant amount of extra work. And extra book-keeping that we have to do leads to what we call as extended Euclid's algorithm. So, this was not the algorithm Euclid proposed, Euclid gave only the algorithm to compute the GCD of 2 numbers. But the reason we call it extended Euclid's algorithm is we do some extension. Namely, we do some extra bookkeeping. And that extra book-keeping helps us to find out the exact values of Bezout's coefficient.

And extra book-keeping that we have to do is that each step, we have to express the remainders that we keep on getting in terms of our original a and b. And that is always possible to do that. So, I would not be giving you the exact pseudocode for extended Euclid's algorithm, but I will demonstrate it and then I will leave it as an exercise for you to express it as an algorithm. So, suppose my a is 252, and b is 198. And I want to find out the Bezout's coefficient s and t for this value of a and b.

So, now let us see how exactly the various remainders are computed during the execution of the Euclid's GCD algorithm. So, in my first step, this will be my x (252) and this will be my y (198). And this will be my r (54). In the next iteration, this will become my x (198), my current r will become next y (54) and this will be the next r (36). So, the underlined things are the remainders that I am obtaining. And these underlined things are the quotients. So, then this becomes my x, this becomes my y, and this will be my new r.

And then this becomes my x, this becomes my y. And finally, I obtain 0 as the remainder and I stop. And I stop and say that 18 will be my GCD. Now, my 18 is a GCD of 252 and 198. And now my goal is to find out the integer linear combiners s and t such that, that s times 252 + t

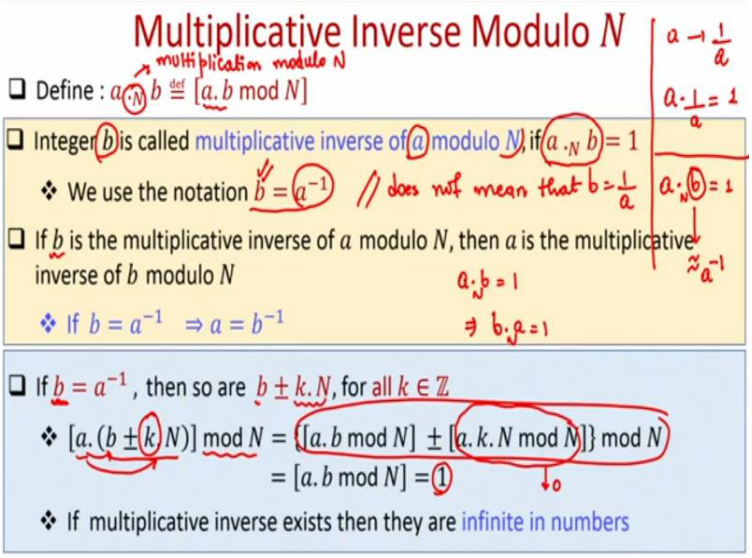
times 198 gives me the value 80. So, for that as I said that each step at each step, you express the remainders in terms of a and b. So, let us start with the final remainder, which is 18.

And if I go back, then 18 is the difference of 54 and 1 times 36. But as I said, that everything has to be expressed in terms of a and b, so I will go 1 step back. And then I can see that 36 is expressible in terms of 198 and 54. So, I can substitute the value of 36 in this equation, and then I get that 18 is represented in terms of 198 and 54. But I want to represent 54 also in terms of 198 and 252. And for that I have to go 1 step back further and 54 satisfies this equation and then I can substitute this value of 54 in this equation.

And then I get my Bezout's coefficients as 4 and -5. So, basically what we have to do is at each step, we have to keep track of my quotients, and the remainder and quotients and the remainder, that is why I have underlined them. So, in this demonstration, I have actually done a backward pass, because we went all the way back and stopped where 54 was expressed in terms of 252 and 198. And then I substituted that value in this final equation.

But in the actual pseudo code of extended Euclidean algorithm, you do not need to make a backward pass, everything is a forward pass. It is just a small modification. And that is all. So, that means, anyhow, you will be performing the computation x modulo y to find out the remainders in each iteration of the Euclid's algorithm, what I am saying is you can also keep track of the various quotients and that will help you to find out the exact values of Bezout's coefficients s and t.

(Refer Slide Time: 21:07)



So, now using notion of GCD and Bezout's coefficient, we will define what we call as multiplicative inverse modulo N. And let us first see the definition and then we will see how exactly we can find out the multiplicative inverse using extended Euclid's algorithm. So, I define operation multiplication modulo N that is denoted by this notation ($\cdot_N$) . So, this notation is for multiplication modulo N, that means you multiply a and b and then take the remainder. That is our definition.

Now, I say an integer b to be the multiplicative inverse of another integer a modulo N if a times b modulo N gives me 1, that means, if you multiply a with b and then take the modulo N and if the value is 1, then I will say that value b is the inverse of a (multiplicative inverse), why it is inverse because typically in the regular arithmetic, when I say inverse of a is 1 / a, the interpretation there is that if I multiply a with 1 / a, then I get 1.

In the same way in the modular world, I am interested to find out a number b, which when multiplied with a and then taken modulo N and gives me 1, if that is the case, then this b can be treated as if it is a^{-1}. That is the interpretation here. So, it is like more or less same as your regular inverse, but we call it modular multiplicative inverse because everything happens modulo N. So, we use this notation $b = a^{-1}$; this does not mean that b is 1/a remember very often student gets confused.

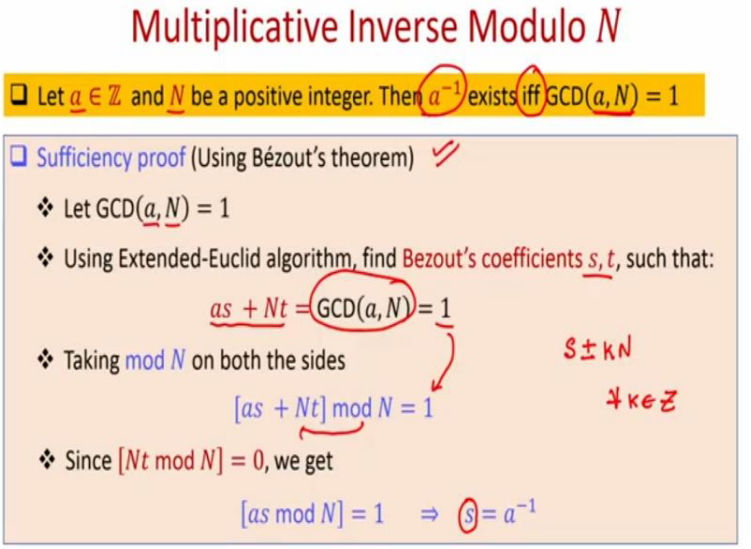
This is just a notation when I say a inverse (a^{-1}) that does not mean 1 / a, a^{-1} is another integer b which when multiplied with a and then taken; and then if you do modulo N we get answer 1. Now, it is easy to see that if b is the multiplicative inverse of a modulo N, then a is the multiplicative inverse of b modulo N, because when you multiplied a with b modulo N and you get 1 that means when you multiplied a with b and then take modulo N you get 1.

So, in that sense, b is the inverse of a ; multiplicative modular inverse of a. Now, another interesting fact here is the following if b is the multiplicative inverse of a then any number of the form b plus minus any multiple of your modulus N, $b \pm k \cdot N$ for all $k \in \mathbb{Z}$, will also be an inverse of a and you can verify that so what will be the result of multiplying a with this number b plus minus kN and then taking modulo N? Well this will be the same as this.

So, remember, I can take this dot inside because as per the rules of modular arithmetic, I can first reduce my operands and then perform the operation and this . (dot) is distributive over the plus here as well as minus. So, now, when I do akN modulo N this will give me 0, because this number is completely divisible by N then whatever is the remainder obtained by dividing ab / N that will be the overall answer and ab modulo N is nothing but 1 because that is the definition of b.

This shows that if at all you have multiplicative inverse, then they are infinite in numbers that means, once you find 1 multiplicative inverse for a you are guaranteed to have infinite number of multiplicative inverse because your k; you extend it in the positive direction or negative direction you substitute k = 1, 2, 3, 4 up to infinity and you substitute k = -1, -2, -3, infinity and k = 0 you get infinite number of inverses.

(Refer Slide Time: 25:57)



But now, the interesting question is when can we say that the multiplicative inverse modulo N for a number a exists - is it the case that for every a for every modulus N I can say that the multiplicative inverse modular and exist? Unfortunately the answer is no, there is only under certain conditions I can say that multiplicative inverse modular and exist. So, the theorem statement is the following.

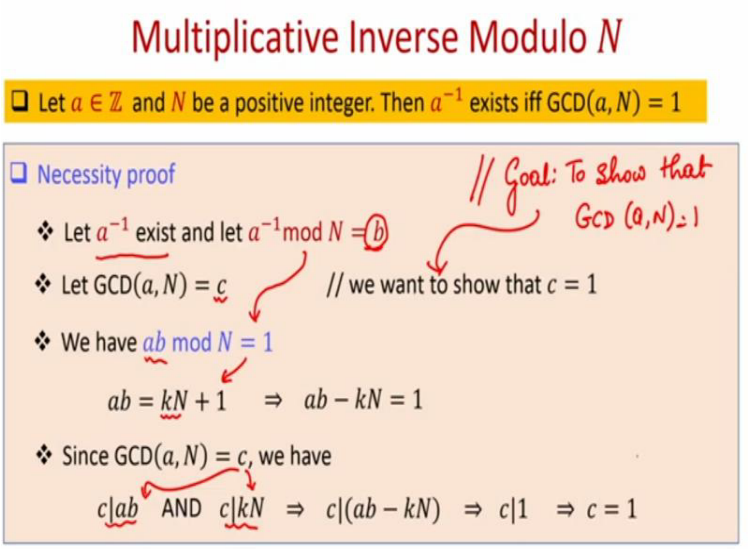
If you are given some number integer a and a modulus N then the claim is that the multiplicative inverse of a exists if and only if a is co-prime to N namely the GCD of a and N is 1. So, this is an if and only if statement that means, this condition is both necessary as well as sufficient. So, let us first prove the sufficiency condition using Bezout's theorem. That means, assume that you have a number a and a modulus N such that they are co-prime.

If that is the case then I have to show that I can find out the multiplicative inverse of a using Bezout's theorem and using extended Euclid algorithm. So, using extended Euclid's algorithm I can find out the exact Bezout's coefficients s and t such that the integer linear combination of a and N as per the combiners s and t is same as the GCD of a and N and remember the GCD of a and N is 1. Now, if I take mod N on both the sides that means, this is your LHS I take mod N and this is your RHS.

I take mod N. Now 1 modulo N will give you 1 because you divide 1 by any modulus N the remainder will be N whereas, left hand side will be as + Nt mod N So, I can take mod inside. Now, N times t mod N will 0 because this is a multiple of N and hence it is completely divisible by N that means, my LHS becomes as times modulo N and anyhow in my RHS, I have 1, that means I can say that the Bezout's coefficient s is nothing but your multiplicative inverse of a.

And as I said earlier, if you know to find 1 multiplicative inverse, you can find the others as well, just take s plus minus equal to k times N for all k belonging to Z ($s \pm kN \; \forall \; k \in \mathbb{Z}$). That will give you all multiplicative inverses. So, that is a sufficiency proof. If you give me a number, which is co-prime to your modulus I know how to find out its multiplicative inverse.

(Refer Slide Time: 28:38)



Now, I want to prove the necessity condition. Namely, I want to show that if at all the multiplicative inverse of a exist then it implies that the number a is co-prime to your modulus. So, assume you have an a for which you can find out the multiplicative inverse how you find out I do not care, but it exists. And suppose the multiplicative inverse of a is b, I have to show; my goal is to show that a is co-prime to N, that is my goal. So, imagine the GCD of a and N is c.

And as I said earlier, my goal is to show that c = 1. Now, as per the definition of multiplicative inverse, I know that ab modulo N is 1 because b is the multiplicative inverse of a. That means when I divide ab / N, I get a remainder 1. That means I can say that a times b is some multiple of

N + 1 that comes from the rules of division. That means I can rewrite 1 as the difference of ab and kN.

Now since I know that the GCD of a and N is c, that means c is the greatest, it is a common divisor of a and N, and it is the greatest common divisor. Then I know that c divides any multiple of a, namely, it divides b times a and c divides any multiple of N. Namely, it can it will divide k times N, if c divides a times b, and c also divides k times N, then remember in our earlier lecture, we showed that c divides the summation of those two numbers as well.

That summation could be positive, negative anything. So, I can say that c divides ab - kN as well, that means I can say that c divides 1. And that is possible only when c = 1. And that is what precisely we wanted to show.

(Refer Slide Time: 31:06)

So, we showed that indeed if multiplicative inverse for a modulo N exist, then your number a has to be co-prime to N otherwise the multiplicative inverse does not exist. So, this is a very powerful condition, it says that multiplicative inverse modulo N exists only if some condition is satisfied and the condition is that your number should be co-prime to your modulus.

So, that brings me to the end of this lecture, just to summarize : in this lecture, we saw few other nice properties of the GCD is namely, we saw that the GCD of any 2 numbers a and b can be

expressed as a linear combination of the numbers itself. And we know how to find those integer linear combiners using extended Euclid's algorithm. And we discussed the definition of multiplicative inverse modulo N and the condition under which multiplicative inverse modulo N exists. Thank you.