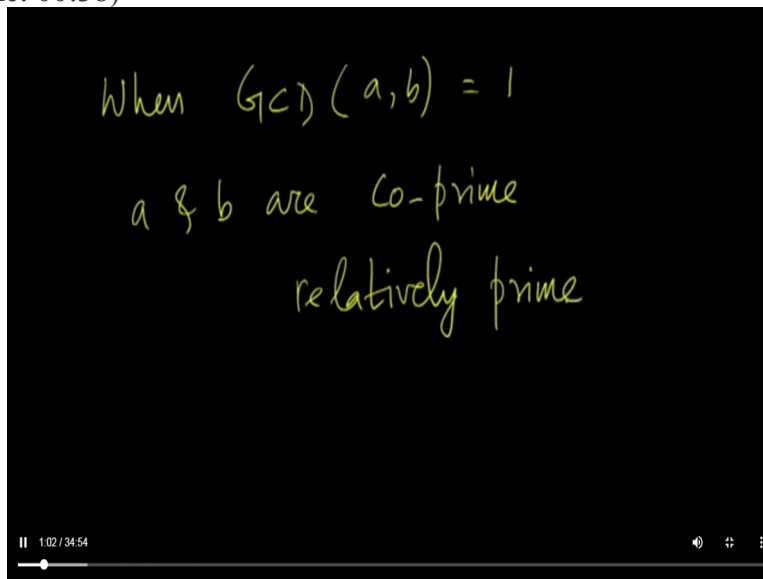


Discrete Mathematics
Professor Sajith Gopalan
Professor Benny George
Department of Computer Science and Engineering
Indian Institute of Technology Guwahati
Lecture 24 – GCD, Euclid's Algorithm

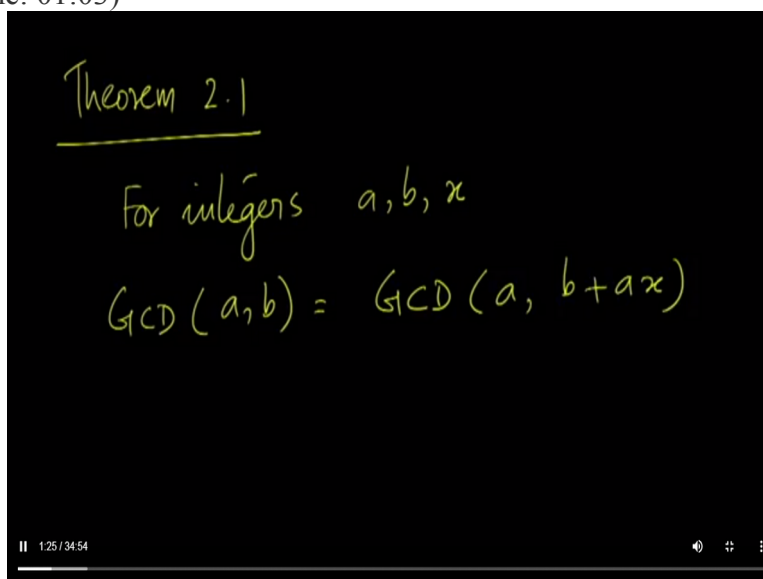
Welcome to the NPTEL MOOC on Discrete Mathematics. This is the second lecture on number theory.

(Refer Slide Time: 00:38)



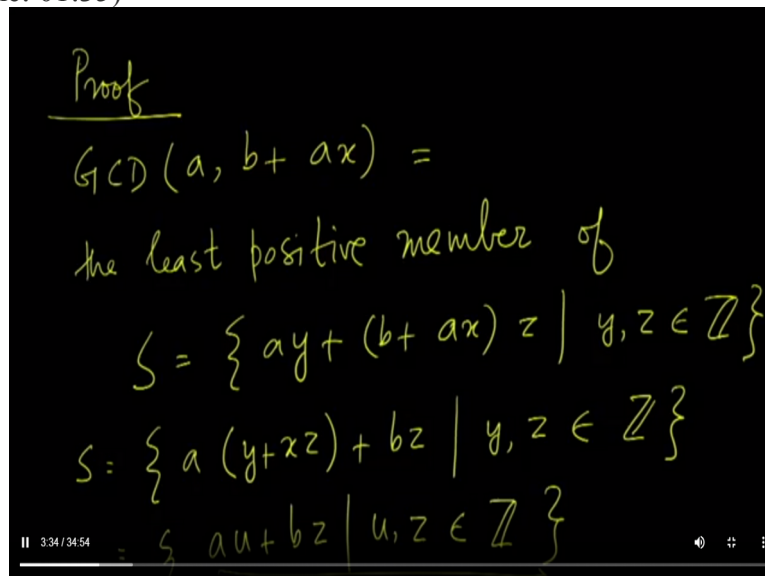
When the GCD of two numbers, two integers a and b is 1, we say that a and b are co-prime or that they are relatively prime.

(Refer Slide Time: 01:03)



Let us see a theorem which we call theorem 2.1. For integers a , b and x , GCD of a and b is the same as the GCD of a and b plus ax , that is an integer multiple of a added to b . Along with a will have the same GCD as a and b .

(Refer Slide Time: 01:35)



Proof

$$\text{GCD}(a, b+ax) =$$

the least positive member of

$$S = \{ ay + (b+ax)z \mid y, z \in \mathbb{Z} \}$$

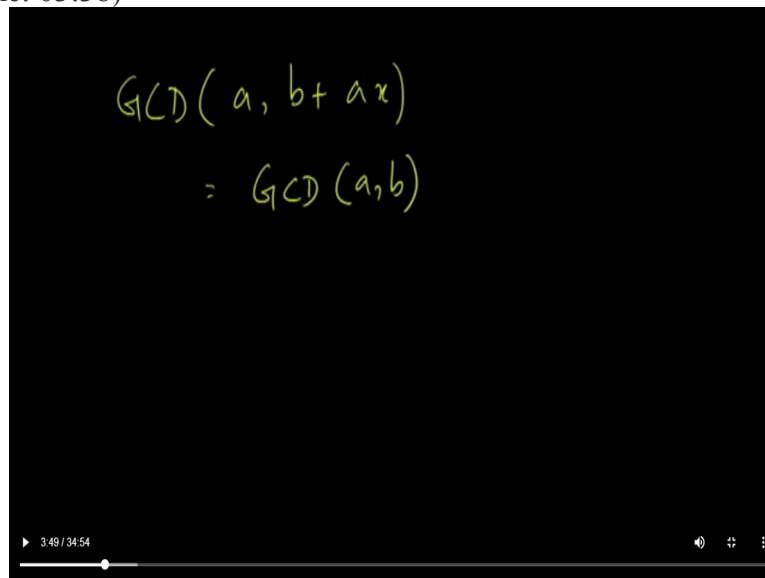
$$S = \{ a(y+xz) + bz \mid y, z \in \mathbb{Z} \}$$

$$= \{ au + bz \mid u, z \in \mathbb{Z} \}$$

The proof goes like this: GCD of a and b plus ax according to what we saw in the last class, is the least positive member of set S , where the set S is the set of all linear combinations of a and b plus ax using integer coefficients. So GCD of a and b plus ax is the least positive member of this set. But then this set is identical to that is this definition can be re-written as a into y plus xz plus bz where y and z are in the set of integers.

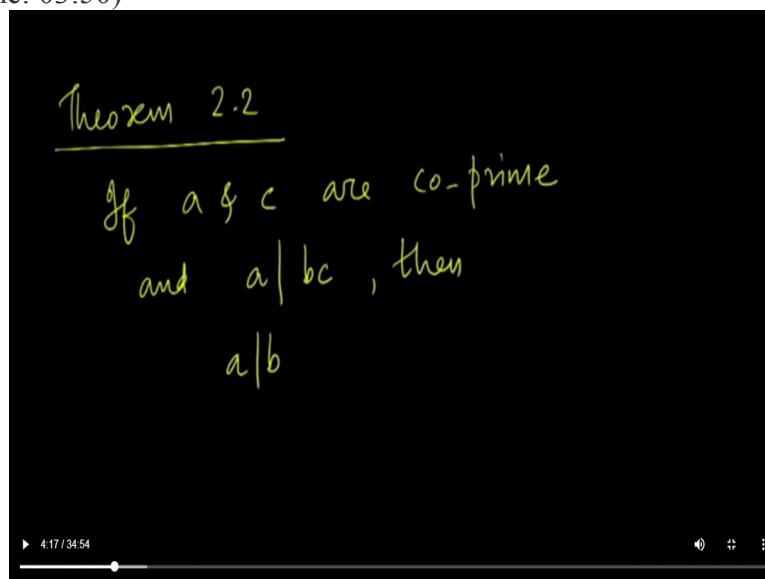
This can be written as that is because given u and z . Any number a into u plus bz can be written as a into y plus xz plus bz for integers y and z . That is for every such u we can find such a y . u will be y plus xz , therefore y will be u minus xz . But the least positive member of this set in the final form we know is nothing but GCD of a and b .

(Refer Slide Time: 03:38)


$$\begin{aligned} \text{GCD}(a, b+ax) \\ = \text{GCD}(a, b) \end{aligned}$$

Therefore GCD of a and b plus ax is nothing but GCD of a, b. Hence, the theorem.

(Refer Slide Time: 03:50)



Theorem 2.2
If a & c are co-prime
and $a|bc$, then
 $a|b$

Another theorem, which we number 2.2, states this, if a and c are co-prime or relatively prime which means their GCD is 1 or they do not have a common factor and it divides bc, then a divides b.

(Refer Slide Time: 04:18)

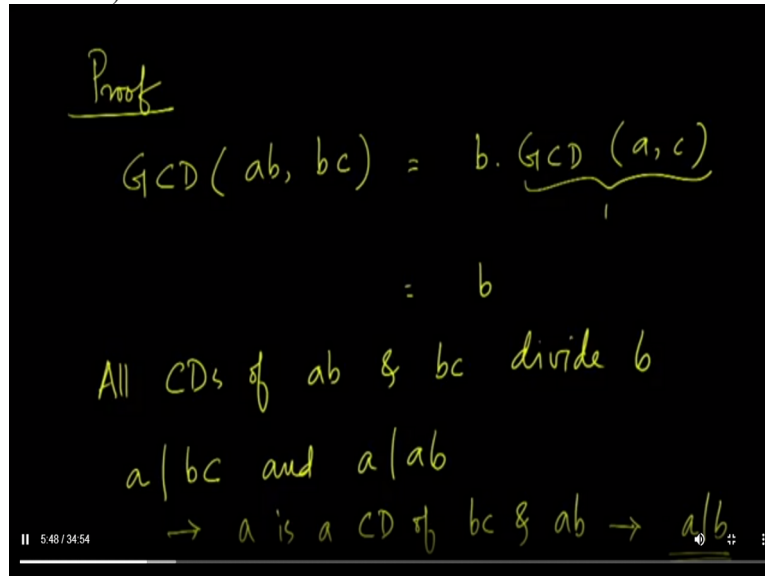
Proof

$$\begin{aligned} \text{GCD}(ab, bc) &= b \cdot \underbrace{\text{GCD}(a, c)}_1 \\ &= b \end{aligned}$$

All CD's of ab & bc divide b

$a|bc$ and $a|ab$

$\rightarrow a$ is a CD of bc & $ab \rightarrow a|b$

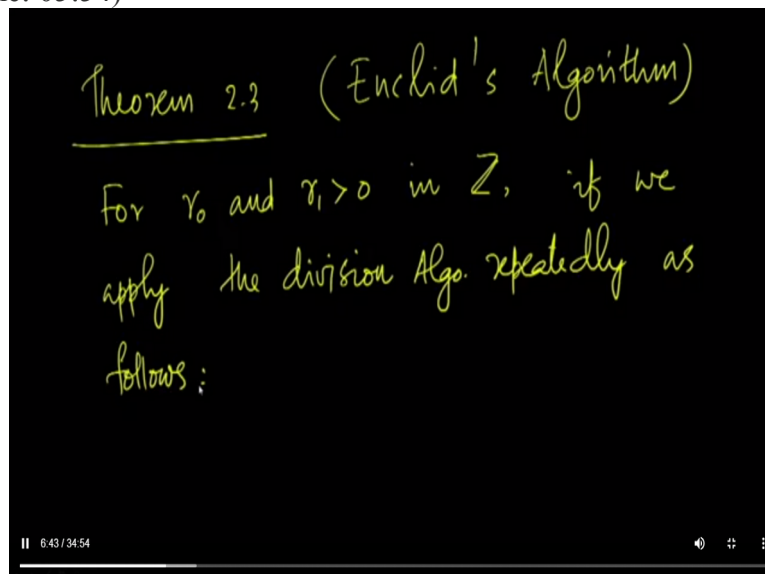


To prove this, we consider GCD of ab and bc . This we know from the theorem proved in the last class as b times GCD of a and c . But a and c are co-prime therefore GCD of a and c is 1 , therefore this is b . So GCD of ab and bc is b , which means all common divisors of ab and bc divide b . Now a divides bc and a divides ab . Therefore, a is a common divisor of bc and ab . a divides bc is given, ab is a product of a and b therefore a divides ab . Therefore we know that a is a common divisor of bc and ab which means a divides b which is indeed the conclusion that we have been seeking. Hence, the theorem.

(Refer Slide Time: 05:54)

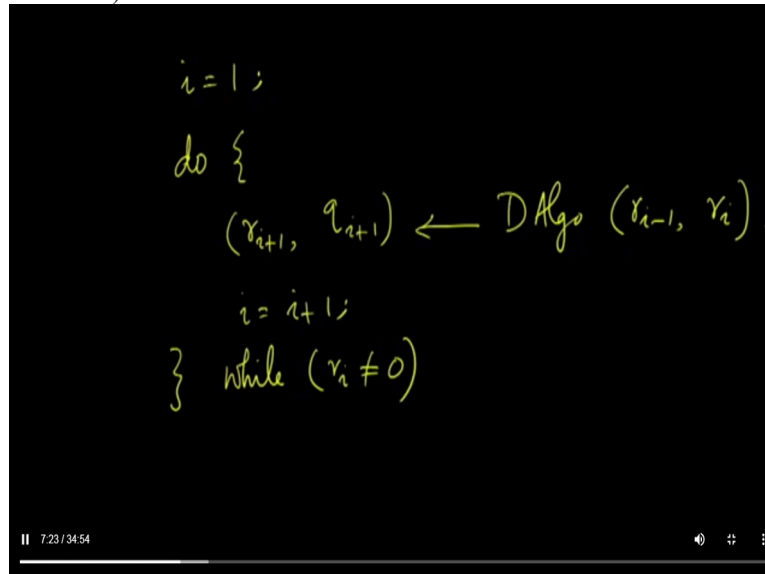
Theorem 2.3 (Euclid's Algorithm)

For r_0 and $r_1 > 0$ in \mathbb{Z} , if we apply the division Algo. repeatedly as follows:



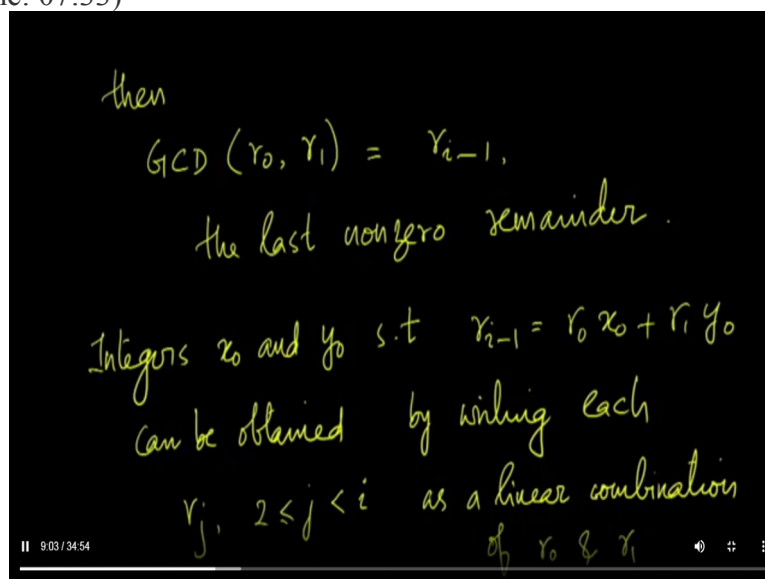
The next theorem which we number theorem 2.3 is the one which talks about Euclid's Algorithm. What this theorem says is this: for r_0 and $r_1 > 0$, both of which are integers if we apply the division algorithm repeatedly, if you apply the division algorithm repeatedly as follows:

(Refer Slide Time: 06:48)



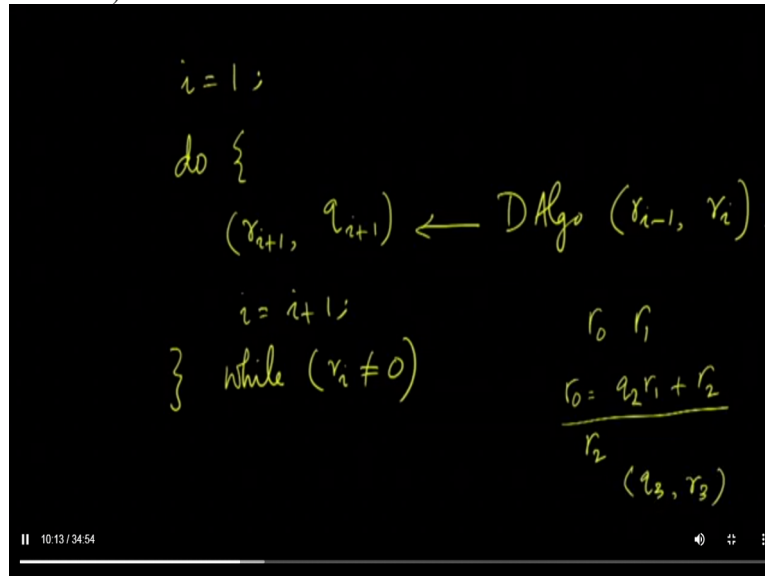
The division algorithm is applied like this. We said variable i to 1 and then we have a do loop in which what we do is this. We form ordered pair r_{i+1}, q_{i+1} using division algorithm applied on r_{i-1} and r_i and then we increment i . We do this while r_i is not equal to 0. So we apply division algorithm in this sense.

(Refer Slide Time: 07:33)



First let me complete the statement of the theorem, after that we will revisit the division algorithm. Then what the theorem says is this GCD of r_0 and r_1 is r_{i-1} which is the last nonzero remainder of the process and in particular integers x_0 and y_0 such that the GCD that we find namely r_{i-1} is a linear combination of r_0 and r_1 with x_0 and y_0 as the coefficients can be obtained by writing each r_j where j varies from 2 to $i-1$ as a linear combination of r_0 and r_1 .

(Refer Slide Time: 09:06)



Now let us take a look at the division algorithm. The algorithm begins with r_0 and r_1 and then we find r_2 in the sense, we write r_0 as $q_1 r_1$ plus r_2 , $q_2 r_1$ plus r_2 . That is we find a unique ordered pair r_2, q_2 so that when the division algorithm is applied on r_0 and r_1 , this ordered pair is what we get. Then r_0 would be expressible in this form. So we have now r_2 . So r_2 is the remainder of the division of r_0 not with r_1 .

So now we have r_1 and r_2 . Then what we do is to recurse with r_1 and r_2 . The division algorithm is next invoked on r_1 and r_2 . Then we would get an ordered pair q_3 and r_3 . r_3 would be the new remainder then we would recurse with r_2 and r_3 . So when you continue like this, the remainders would keep decreasing in value as we go along in absolute value. Finally when we come to a stage where r_i equal to 0 we come out of the loop. At this point the last non-zero remainder that we had, namely r_{i-1} , that would be the GCD of the two given numbers r_0 and r_1 .

(Refer Slide Time: 10:51)

Example 512, 432

$$\text{GCD}(512, 432)$$
$$512 \bmod 432 = 80$$
$$\text{GCD}(432, 80)$$
$$432 \bmod 80 = 32$$
$$\text{GCD}(80, 32)$$
$$80 \bmod 32 = 16$$

12:35 / 34:54

$\text{GCD}(32, 16)$

$$32 = 2 \times \underline{16} + 0$$

$\text{GCD}(16, 0) = 16$

$$\text{GCD}(512, 432) = 16$$

12:49 / 34:54

Let us work out an example first and then we will prove the theorem. In the example, we took a, consider two numbers 512 and 432. Let us say we want to find the GCD of 512 and 432. What we do is this, we find the remainder of 512 on division with 432. Remainder is 80. Then we discard the largest number which is 512 and then recurse with 432 and 80. So now we want to find GCD of 432 and 80. That is to find the GCD of 512 and 432. It is enough to find the GCD of 432 and 80. $432 \bmod 80$ is 32.

Therefore, it is enough to find the GCD of 80 and 32. $80 \bmod 32$ is 16, 64 plus 16 is 80. To find the GCD of 512 and 432, it is enough to find the remainder of the division of 512 with 432 which is 80. So now we should recurse with the smaller of the two original numbers namely 432 and the new remainder which is 80. So 512, the ordered pair 512, 432 reduces to the ordered pair 432, 80 which then reduces to the ordered pair 80, 32 which then reduces to

32, 16 and which reduces to 16 and 0. The GCD of 16 and 0 is 16 and this would be the GCD of the original pair of numbers.

(Refer Slide Time: 12:57)

16 as a linear combin of 512 & 432
with int. coeffs.

$$512 = 1 \times 432 + 80$$

$$80 = 1 \times 512 - 1 \times 432 \quad \text{--- (1)}$$

The theorem also says how the GCD 16 can be expressed as a linear combination of 512 and 432 with integer coefficients. If you go through the steps, you find that in the first step, we take the modulus of the division of 512 with 432. Therefore we have 512 is 1 into 432 plus 80 or 80 is 1 into 512 minus 1 into 432. Let us call this equation 1.

(Refer Slide Time: 13:59)

$$432 = 5 \times 80 + 32$$

$$32 = 1 \times 432 - 5 \times 80 \quad \text{--- (2)}$$

$$80 = 2 \times 32 + 16$$

$$16 = 1 \times 80 - 2 \times 32 \quad \text{--- (3)}$$

And then in the next step we have a division of 432 with 80. We find that 432 is 5 into 80 plus 32 which means 32 is 1 into 432 minus 5 into 80. Let us call this equation 2. The next step is on the ordered pair 80 and 32. 80 is 2 into 32 plus 16. Or in other words 16 is 1 into 80 minus 2 into 32. Let us say this is equation 3. So 16 can be expressed as a linear combination

of 80 and 32 with coefficients 1 and minus 2 respectively. But, then 32 can be expressed as a linear combination of 432 and 80 with 1 and minus 5 as the coefficients.

(Refer Slide Time: 15:13)

$$\begin{aligned} 16 &= 1 \times 80 - 2 \times 32 \\ &= 1 \times 80 - 2 (1 \times 432 - 5 \times 80) \\ &= 11 \times 80 - 2 \times 432 \\ &= 11 (1 \times 512 - 1 \times 432) - 2 \times 432 \\ &= \underline{11 \times 512 - 13 \times 432} \end{aligned}$$

So 16 is 1 into 80 minus 2 into 32. But 32 in turn we find this expressible in this form which upon simplification gives us 11 into 80, this is 1 into 80 and then minus 2 into minus 5 is 10. So 10 plus 1, 11 minus 2 into 432. So 16 is expressible as a linear combination of 80 and 432 with 11 and minus 2 as the respective coefficients. And then 80 we know is 1 into 512 minus 1 into 432 from the first equation. So substituting that here we find that 16 is 11 into 512 minus 13 into 432.

So, now 16 has been expressed as a linear combination of 512 and 432 with 11 and minus 13 as the coefficients. So this is what the theorem talks about.

(Refer Slide Time: 16:42)

Proof

By Thm 2.1,

$$\begin{aligned} \text{GCD}(r_0, r_1) &= \text{GCD}(r_1, \underbrace{r_0 - r_1 q_2}_{r_2}) \\ &= \text{GCD}(r_1, r_2) \\ &= \text{GCD}(r_2, r_3) \\ &= \text{GCD}(r_3, r_4) \\ &\vdots \\ &= \text{GCD}(r_{i-1}, 0) = \underline{r_{i-1}} \end{aligned}$$

18:03 / 34:54

To prove the theorem, what we do is this: we know that by theorem 2.1, GCD of r_0 and r_1 is the same as GCD of r_1 and $r_0 - r_1 q_2$. We use integer q_2 here which is GCD of r_1 and r_2 , that is because the second term is nothing but r_2 . $r_0 - r_1 q_2$ is the same as r_2 . So GCD of r_0 and r_1 is indeed GCD of r_1 and r_2 . So if you continue like this, you can show that this is the same as GCD of r_2 and r_3 which is the same as GCD of r_3 , r_4 and so on, until we come to GCD of r_{i-1} and 0 where r_{i-1} is 0.

But GCD of r_{i-1} and 0 for nonzero r_{i-1} is nothing but r_{i-1} . So GCD of r_0 and r_1 is r_{i-1} as the theorem claims.

(Refer Slide Time: 18:14)

Show by induction

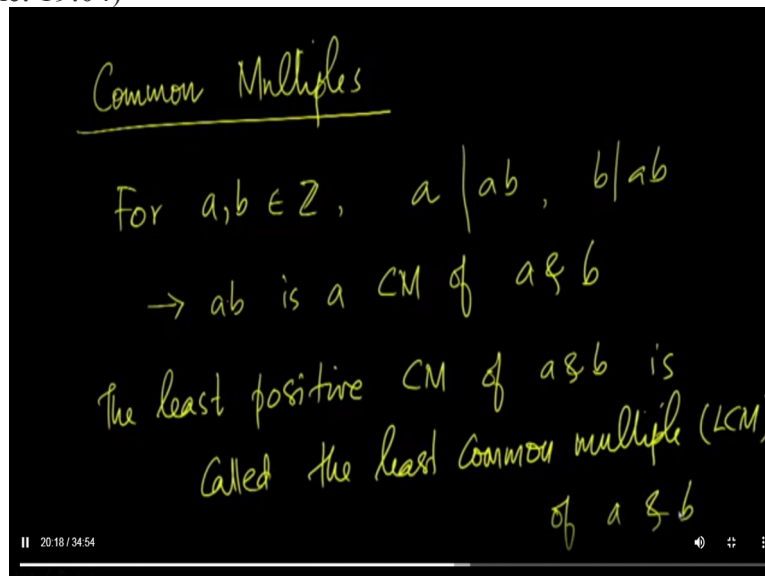
r_j is a linear combination
of r_0 & r_1 , $\forall j$ $2 \leq j \leq i-1$

18:53 / 34:54

Now do as an exercise. The rest of the proof that is by induction show that r_j is a linear combination of r_0 and r_1 for all j varying from 2 to $i-1$. So in particular r_{i-1}

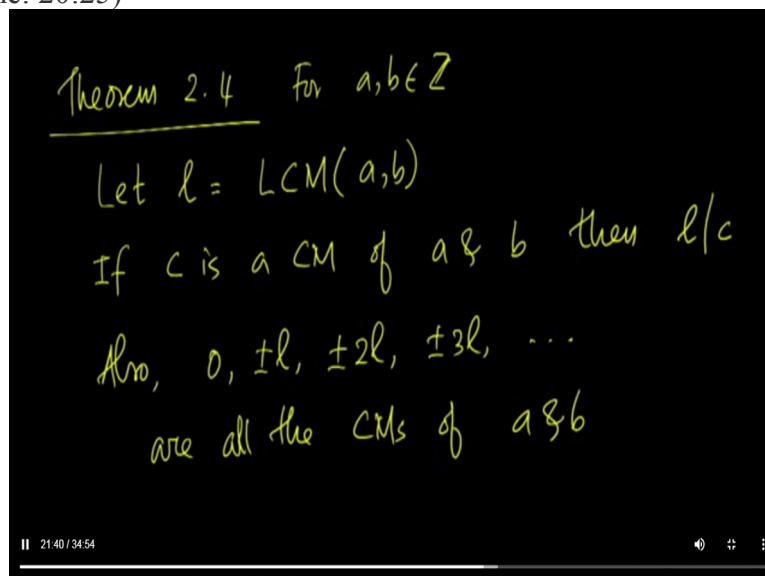
which is the result of the algorithm, which is the GCD of r not and r_1 is also a linear combination of r not and r_1 . So I leave this to you as an exercise. So we have been talking about common divisors and greatest common divisors.

(Refer Slide Time: 19:04)



Now let us talk about common multiples. For integers a and b , we know that a divides ab and b divides ab . So ab is a multiple of a and ab is a multiple of b which means ab is a common multiple of a and b . So a and b do have common multiples. The least positive of the common multiples of a and b is called the least common multiple or LCM of a and b . So for any pair of integers a and b , we can define the least common multiple of a and b .

(Refer Slide Time: 20:25)

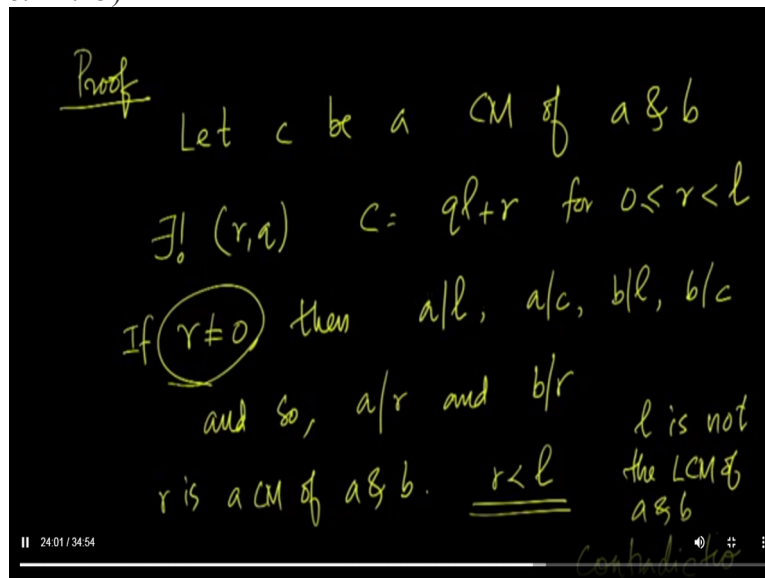


So we have a theorem for this notion, which we number 2.4. Let l denote LCM of a, b for integers a and b . If c is a common multiple of a and b , then l divides c . Also 0 plus or

minus l , plus or minus $2l$, plus or minus $3l$, et cetera. That is the integer multiples of l are all the common multiples of a and b . So these are the only common multiples of a and b and all of these are common multiples of a and b .

So what we assert here is this, if l is the LCM of a and b and c is a common multiple of a and b then l divides c . In other words the LCM divides every other common multiple. So common multiples are all multiples of LCM.

(Refer Slide Time: 21:45)



So we prove as follows: Let c be a common multiple of a and b , an arbitrary common multiple of a and b , then by the division algorithm, we know that there is a unique pair r, q such that c equals $q l$ plus r for 0 less than or equal to r less than l . Suppose, this r is nonzero. Then a divides l , a divides c , a divides l because l is LCM of a and b . So l in particular is a common multiple of a and b . So l divides l , l divides c because by definition c is a common multiple of a and b .

Similarly, b divides l and b divides c . If a divides l and a divides c then a must divide r as well because then r is c minus $q l$, then a divides r and similarly b divides r . Or in other words r is a common multiple of both a and b . r is between 0 and l minus 1 inclusive of both the limits. Therefore, r is less than l or in other words, l is not the LCM of a and b as we assumed. So this is a contradiction. We started with the assumption that l is the LCM of a and b . So we get a contradiction. Therefore, it must be that the assumption we made namely that r is not equal to 0 must be false.

(Refer Slide Time: 24:04)

$$\begin{aligned} \underline{r=0} \\ c = ql + r = ql \quad \rightarrow \quad l|c \end{aligned}$$

So every CM of a & b
is among $0, \pm l, \pm 2l, \pm 3l \dots$

So we conclude that r equal to 0. But c is $q l$ plus r which is now $q l$ since r equal to 0. In other words, l divides c . So c is a multiple of the LCM. So every common multiple of a and b is among these as the theorem claims.

(Refer Slide Time: 24:47)

Theorem 2.5
For every positive integer d ,
 $\text{LCM}(bd, cd) = \text{LCM}(b, c) \cdot d$

Another theorem about LCM: For every positive integer d LCM of bd, cd is LCM of b and c multiplied by d .

(Refer Slide Time: 25:25)

$$\begin{aligned} \text{Let } l &= \text{LCM}(b, c) \\ L &= \text{LCM}(bd, cd) \\ \text{Then } bd &| ld, \quad cd | ld \\ \text{So } ld &\text{ is a CM of } bd \text{ \& } cd. \\ \text{So } L &| ld \end{aligned}$$

So to prove this, let us define small l as the LCM of b and c and capital l as the LCM of bd and cd . So we have these two numbers small l and capital l . Then bd divides ld and cd divides ld . l is LCM of b and c . So in particular l is a multiple of b . Therefore ld is a multiple of bd . Similarly ld is multiple of cd as well. So ld is a common multiple of bd and cd . So, L divides ld because we have just shown that the LCM divides every common multiple. So capital L is the LCM of bd and cd . Therefore capital L divides small ld .

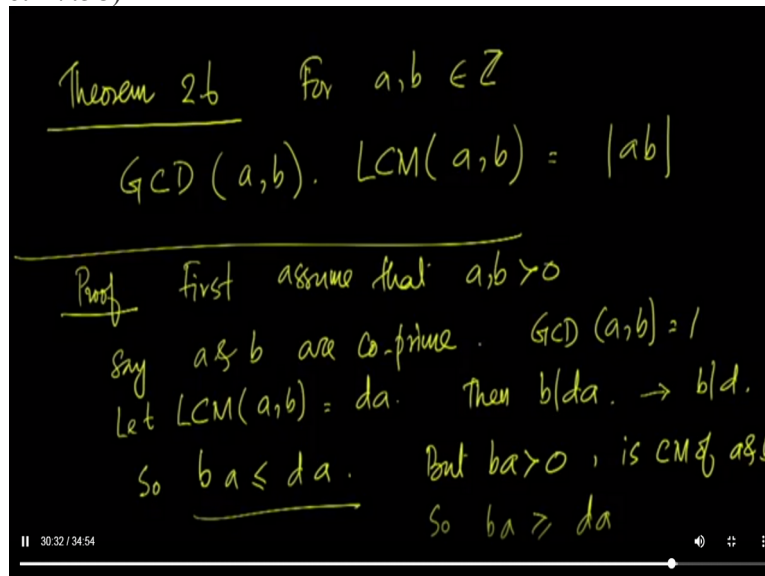
(Refer Slide Time: 26:38)

$$\begin{aligned} \text{Also, } b &| \frac{L}{d} \quad \text{and} \quad c | \frac{L}{d} \\ \frac{L}{d} &\text{ is a CM of } b \text{ \& } c \\ l &| \frac{L}{d} \rightarrow ld | L \\ &\rightarrow L = ld \end{aligned}$$

Also b divides the number L by d . And c divides L by d . That is because the capital L is a multiple of bd and capital L is a multiple of cd . Therefore b divides the number L by d , L by d is an integer. So L by d is a common multiple of b and c . In other words the LCM of b and c namely small l divides L by d which implies that small ld divides capital L .

So we have just shown that capital L divides small l and small l divides capital L. Therefore, it must be that capital L is the same as small l which is precisely what we want to show. We wanted to claim that LCM of b and c which is capital L is the same as d times LCM of b and c which is d times small l. Hence the theorem.

(Refer Slide Time: 27:58)



Another theorem dealing with GCD and LCM, which we name theorem 2.6, this asserts that, for any pair of integers a and b , the GCD of a and b multiplied by the LCM of a and b is the absolute value of ab , the product of a and b . To prove this, first we assume that both a and b are positive. So first, let us assume a and b are co-prime. We consider the case of a and b being co-prime first.

Then GCD of a and b must be 1. They are relatively prime so they do not have a common factor other than 1. Let the LCM of a and b be d times a for some d , some integer d . Then b divides da , da is the least common multiple of a and b . So in particular da is multiple of b or in other words b divides da . But then b does not divide a ; b and a are co-prime. So GCD of b and a is 1, therefore b does not divide a .

This therefore implies that b divides d . So ba is less than or equal to da . But ba is greater than 0, that is because both a and b are positive. So b is greater than 0. This is a common multiple of a and b , b is greater than 0 and is also a common multiple of a and b . So ba is greater than or equal to da . da is the LCM of a and b as we assumed. Therefore ba must be greater than or equal to da . So we have these two inequalities here, ba is less than or equal to da . Similarly ba is greater than or equal to da .

(Refer Slide Time: 30:41)

Handwritten notes on a blackboard:

$$da = ba$$
$$\underline{LCM(a, b) = a \cdot b = |ab|}$$

At the bottom left of the slide, there is a timestamp: 31:00 / 34:54. At the bottom right, there are icons for volume, full screen, and a list.

Combining these two we have da equal to ba which means the LCM of a and b is a into b , which is the same as the magnitude of a, b since a and b are both positive. So this is the case where a and b are co-prime.

(Refer Slide Time: 31:10)

Handwritten notes on a blackboard:

a & b are not co-prime

$$GCD(a, b) = g > 1$$
$$GCD\left(\frac{a}{g}, \frac{b}{g}\right) = 1$$
$$g \cdot GCD\left(\frac{a}{g}, \frac{b}{g}\right) \cdot g \cdot LCM\left(\frac{a}{g}, \frac{b}{g}\right) = a \cdot b$$
$$\underline{GCD(a, b) \cdot LCM(a, b) = ab = |ab|}$$

At the bottom left of the slide, there is a timestamp: 32:50 / 34:54. At the bottom right, there are icons for volume, full screen, and a list.

So now let us assume that a and b are not co-prime which means they do have a common divisor which is greater than 1. Let, g be the GCD of a and b . So g is greater than 1. Therefore, from the theorem that we saw in the last class, we have the GCD of a by g and the GCD of b by g is 1. But we know that the GCD of a by g , b by g multiplied by the LCM of a by g , b by g is a by g into b by g . Multiplying both sides by g squared we can write the equation in this manner, g into GCD of a by g , b by g multiplied by g into LCM of a by g , b by g is a into b . But this is nothing but GCD of a, b and this is nothing but LCM of a, b .

Therefore, the product of the two GCD of a, b multiplied by LCM of a, b is a into b. Once again, we assume that a and b are positive, therefore this is the same as the magnitude of ab.

(Refer Slide Time: 32:54)

When a or b is negative,

$$\text{GCD}(a, b) = \text{GCD}(|a|, |b|)$$
$$\text{LCM}(a, b) = \text{LCM}(|a|, |b|)$$
$$\text{GCD}(|a|, |b|) \cdot \text{LCM}(|a|, |b|) = |a||b| = |ab|$$

So the only remaining case is when a or b is negative. When one of a or b is negative, then GCD of a, b is GCD of mod a mod b. And LCM of a, b is LCM of mod a mod b. Now mod a and mod b are both positive integers. Therefore the product of GCD of mod a mod b and LCM of mod a mod b would be mod of a into mod of b, which is the same as the magnitude of ab.

Now the left hand side here is GCD of a, b multiplied by LCM of a, b. GCD and LCM of any pair of integers are positive. Therefore the left hand side is GCD of a, b multiplied by LCM of a, b and the right hand side is mod ab, exactly what we wanted to prove. So that is it from this lecture. Hope to see you in the next. Thank you.