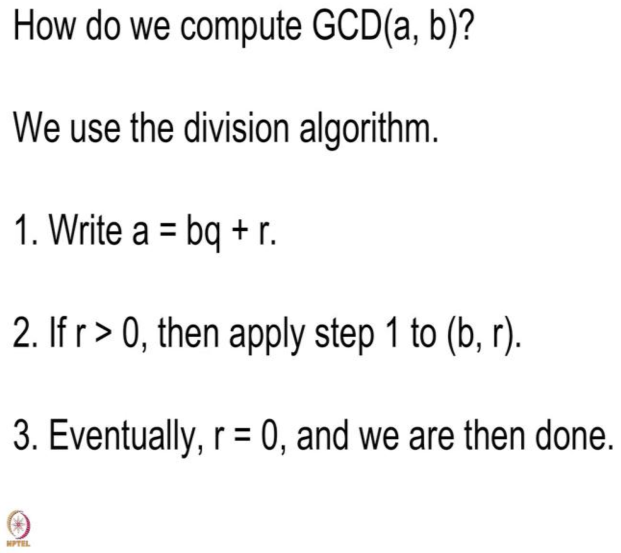
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology Bombay
Lecture 05
Computing the GCD and Euclid’s lemma

Welcome back. We saw in the last lecture that whenever there are two natural numbers a and b, then we have the GCD of a and b. This is yet another natural number, possibly it could be one of them, but it is a natural number d, which has two properties, property number one says that d should divide both a and b, this is the first property.

So, GCD stands for greatest common divisor, so that the property one which says that d should divide both a and b says that it is a common divisor. And now, we have to say that it is the greatest among all the common divisors. So, you could say that among all the common divisors this number is the biggest that is one way to say, but since we are talking about divisibility, we encode it in the second property in the following way, that whenever there is a natural number e, which divides both a and b, then e should divide d.

Two properties, d divides a, d divides b, second property, e divides a, e divides b, then e divides d, this is the greatest common divisor. And if you saw the proof carefully, we actually wrote this greatest common divisor as a linear combination of a and b itself. We wrote it as a alpha plus b beta, where alpha beta could be from integers, they could be positive or negative or sometimes they could even be 0, that is indeed possible you may have a dividing b, in that case a will be the GCD, and then we will have that the GCD which is a, is a into 1 plus b into 0. So now, once we define any such thing, the question is how do you compute it? It is not so easy at all.

(Refer Slide Time: 2:33)



How do we compute GCD(a, b)?

We use the division algorithm.

1. Write a = bq + r.

2. If r > 0, then apply step 1 to (b, r).

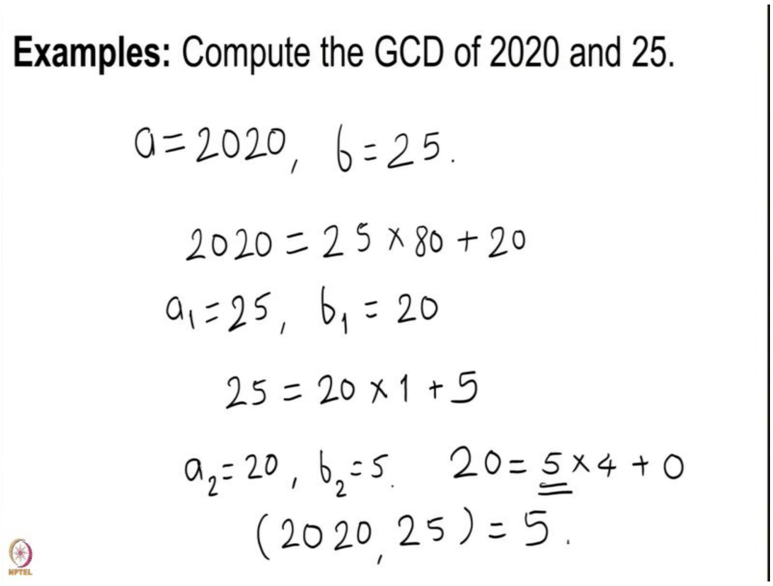
3. Eventually, r = 0, and we are then done.

How do you compute GCD of any two given numbers? This is the question that we must answer, and we are going to use Euclid's division algorithm, I hope you remember the division algorithm. Division algorithm says that whenever you have a and b, two natural numbers, then you can write a as b into q plus r, where q was the quotient and r was the remainder, apply the division algorithm that is our first step of computing GCD a b, so we have a equal to bq plus r. And remember, r is between 0 to b, but it is not equal to b, it is only up to b minus 1, so if r is not equal to 0 then you consider.

Now, r is less than b, so you can divide b by r, you can call b as the new a1 and r will be the new b1. And you will then have a1 equal to b1 q1 plus r1, where r1 will be further smaller, and we proceed this way. So the step number 2, if r is bigger than 0, then apply step 1 to b comma r, ultimately r will be 0, and we are then done. So, what we have to do is the following thing. We start with a and b, assume that a is bigger than or equal to b and apply the division algorithm for the pair a and b to get a as bq plus r.

So, r now starts from 0, r can be 0 or can be 1, r can be 2 all the way up to r can be b minus 1, if it is not equal to 0. If r is 0, then we have got our GCD which is b because b divides a, so if r is not 0, then we have not yet got our GCD. Therefore, we apply the division algorithm to new a1 which is b and new b1 which is r, then we get a new q1, new r1 where this new r1 will be again from 0 all the way up to b1 minus 1, but b1 was our r, so it will go up to r minus 1. And since, you had earlier b r was a natural number which was strictly less than b, now you have a new natural number r1, which is strictly less than r, and so on at each step, you are coming down at least by 1 and therefore, this process will eventually end in 0, so eventually r is going to be 0, and then we are done, so let us apply this and try to compute the GCD.

(Refer Slide Time: 5:45)



Examples: Compute the GCD of 2020 and 25.

$a=2020, \quad b=25.$

$2020 = 25 \times 80 + 20$

$a_1 = 25, \quad b_1 = 20$

$25 = 20 \times 1 + 5$

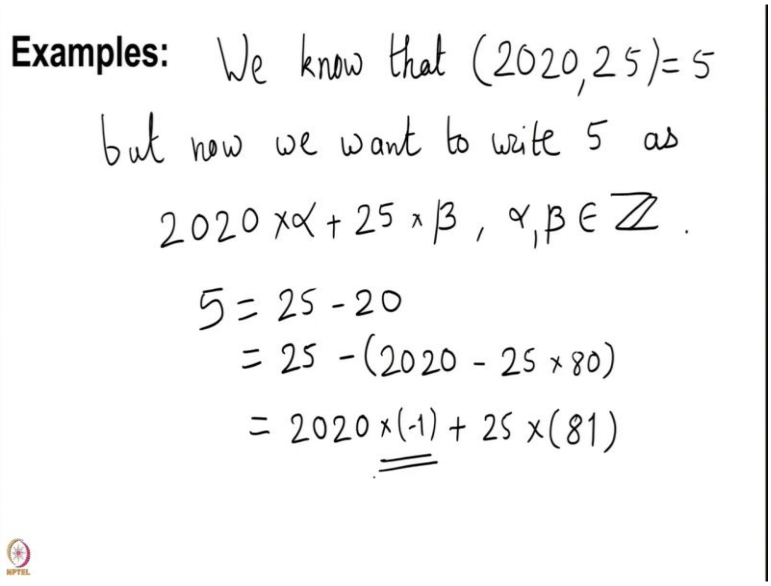
$a_2 = 20, \quad b_2 = 5. \qquad 20 = \underline{\underline{5}} \times 4 + 0$

$(2020, 25) = 5.$

So if you remember, we had applied our division algorithm to the pair 2020 and 25. So, we want to compute the GCD of these two numbers. So, our a is 2020, b is 25, if you remember the calculation that we have done, we noticed that 2020 is 25 into 80 plus 20. So here the r is 20 it is less than b but it is not 0, so this our new a1 is 25, new b1 is 20, again apply division algorithm to get 25 to be 20 into 1 plus 5, once again our new r1, remember a1 was 25, b1 is 20, q1 is 1, and r1 is 5, r1 is still not 0, so we let a2 to be 20, b2 to be 5, but then we get 20 equal to 5 into 4 plus 0, so we are done 5 is our GCD. So, the GCD of 2020 comma 25 is 5. You may say that, you know you could tell this GCD just by looking at the numbers, which is true, many of you would be able to tell this GCD, just by looking at these two numbers.

In fact, if some of you are not able to tell it at the first step, certainly by the time you reach the second step, where you have 20 and 25, I am sure that almost everybody of you would tell the GCD to be 5. But still a process is important, and this process can be applied to any pair of natural numbers not just to some simple numbers like 2020, 25 or 2520 you can apply to any such thing. But wait, there is one more thing remaining. We now, want to write 5 as a linear combination of these two numbers 2020 and 25. So, how do you want to write this? You can use division algorithm to go back, we have been able to write 5 as a linear combination of 25 and 20.

(Refer Slide Time: 8:33)



Examples: We know that $(2020,25)=5$ but now we want to write 5 as $2020\times\alpha+25\times\beta$, $\alpha,\beta\in\mathbb{Z}$.

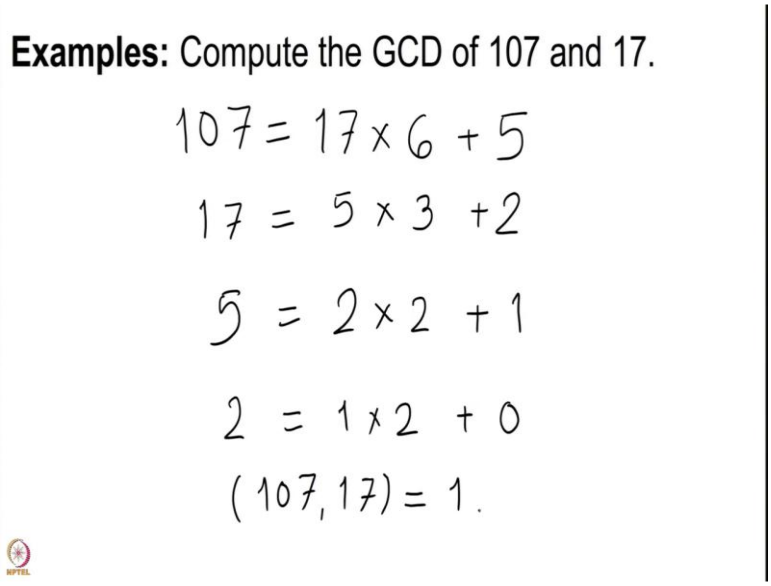
$$\begin{aligned}5&=25-20\\&=25-(2020-25\times 80)\\&=2020\times\underline{\underline{(-1)}}+25\times(81)\end{aligned}$$

We know that the GCD of 2020 and 25 is 5, but now we want to write 5 as 2020 into alpha plus 25 into beta, where alpha, beta are coming from integers, of course they cannot be natural numbers because if you have any non zero multiple of 2020 from natural numbers you would be at least 2020 or beyond, and then you cannot write 5 or if you put 0 for 2020 and any non zero multiple of 25, again coming from natural numbers it will go beyond 25. So, it will not be possible to write the GCD as a linear combination of natural numbers a b, again over natural numbers we have to go outside the set of natural numbers, but that is okay.

So here, we want to write this and if you remember, we had obtained 5 as 25 minus 20 and how did we get 20 it was a difference of 2020 and a multiple of 25, so we just apply that, we write 5 as 25 minus 20. How did we get 25 20? We got it as 2020 minus 25 into 80, that is it. So, we ultimately get this as 2020 into minus 1 plus 25 into 79 because here you have 80 comes with two negative signs, so that gives you 80 and then of course you have to add 1 you are not going to subtract 1.

So it will be 81, as you will see this easily that the difference of 25 into 81, which is going to be 2025, 2025, and when you subtract 2020 once from that, note that here we have minus one multiplied to 2020, so that will indeed give you 5. So we have computed the GCD of 2020 and 25. And then we also wrote it as a linear combination of these two numbers over integers.

(Refer Slide Time: 11:52)



Examples: Compute the GCD of 107 and 17.

$$107 = 17 \times 6 + 5$$

$$17 = 5 \times 3 + 2$$

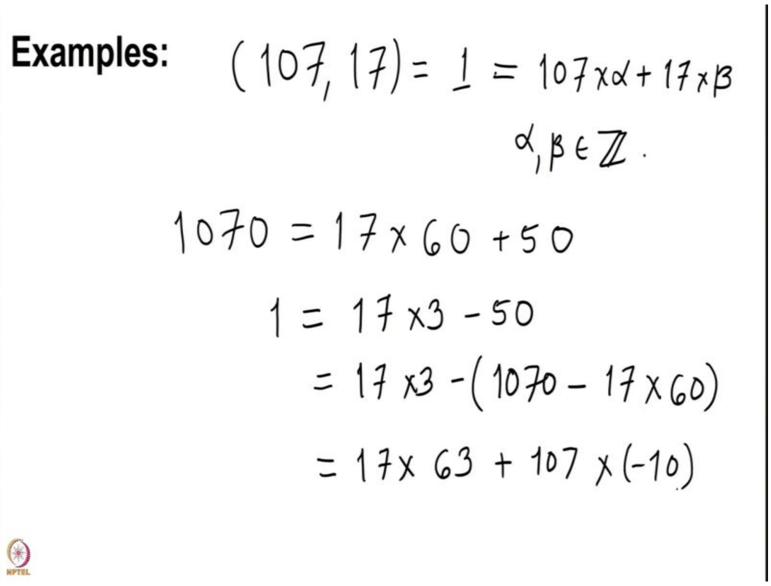
$$5 = 2 \times 2 + 1$$

$$2 = 1 \times 2 + 0$$

$$(107, 17) = 1.$$

Let us do one more problem to have a better practice. What is the GCD of 107 and 17? So, we are going to apply division algorithm once again, we write 107 if you remember, your multiplication tables 17 into 6 is 102 and the remainder is 5. Now, we have to work with 17 and 5, so we write 17 as 5 into 3 plus 2. Next we work with 5 and 2, we have still not got our remainder to be 0, so we need to continue, but now this is very easy. So, the GCD of 117 and 17 is 1, and you can just go back this way and write 1 as a linear combination of 107 and 17. But you should know that there are more than one ways to do that. I am going to tell you one way to write 1 as a linear combination of 107 and 17 not by tracing the steps back, but by just observing what the products are.

(Refer Slide Time: 13:33)



Examples: $(107, 17) = \underline{1} = 107 \times \alpha + 17 \times \beta$

$$\alpha, \beta \in \mathbb{Z}.$$

$$1070 = 17 \times 60 + 50$$

$$1 = 17 \times 3 - 50$$

$$= 17 \times 3 - (1070 - 17 \times 60)$$

$$= 17 \times 63 + 107 \times (-10)$$

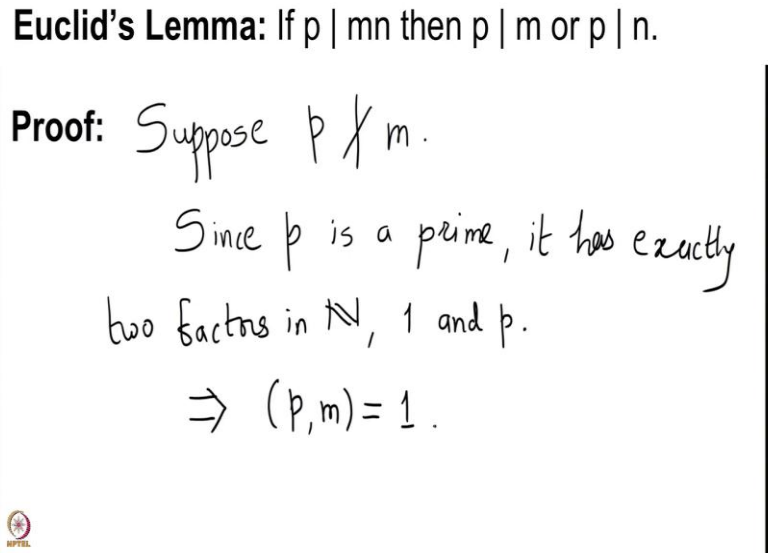
107, 17 the GCD is 1 and we want to write this 1 as 107 into alpha plus 17 into beta, where we want alpha beta to be integers. When we multiplied 17 by 6 and subtract it from 107, we were left with 5, 17 into 6 is 102, 107 minus 102 gives you 5. So, if I multiply all the equation, the whole equation 107 equal to 17 into 6 plus 5 by 10 then we would get 107 into 10, so we will get 1070 equal to 17 into 60 which is 1020 plus 50. And you of course know that 17 into 3 is 51.

So, the 50 that here we have obtained will help us in that, so 17 into 3 which is 51 minus 50, which is 17 into 3 minus 50 is 1070 minus 17 into 60 to give us ultimately, 17 into 63 plus 1070 into minus 1, so we have obtained 1 as a linear combination of 17 and 107, I should indeed make that correction here to write this as 107 into minus 10 that will do. So this is one way by which we can write the GCD.

What we have done here, in a nutshell is using the theory of congruence. So we observed something, which is that when you divide 107 by 17, you take all multiples of 17 away from it, as long as you are left with a number which is less than 17, then you were left with 5. So if we did this for 107 into 10, what you will be left with is going to be 5 into 10, 50. And then you can of course remove some more multiples of 17, but that is okay. We have observed that if you remove multiples of 17, from 107, you are left with 5.

So there is a way to remove multiples of 17 from 107 into 10, which is 1070 and we left with 50. And now, 50 is very close to a multiple of 17, in fact the difference is just 1. This is another way to write GCD as a linear combination of the two numbers a and b with integer coefficients. So, what did we do? We have, since we began this lecture course, we defined the prime number, using primes, we want to now write every integer as a product of primes. And this is indeed true, which we call the fundamental theorem of arithmetic, there is just one more step to go before we go to this theorem. This is called a lemma.

(Refer Slide Time: 17:41)



Euclid's Lemma: If p | mn then p | m or p | n.

Proof: Suppose $p \nmid m$.

Since p is a prime, it has exactly two factors in $\mathbb{N}$, 1 and p.

$\Rightarrow (p,m) = \underline{1}$.

So, you will see that mathematical statements have many names, you will have a theorem, you will have a proposition, you will have a lemma, you will have a corollary. Typically, lemma is something which is used in proving a big theorem, so a theorem should really be a statement which is a grand statement, which is an important statement. And lemma should be the one, which is actually a step of proving the theorem.

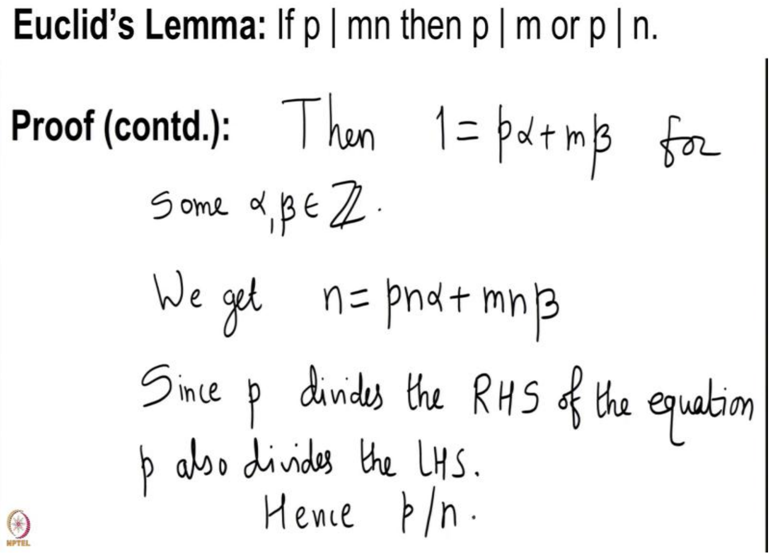
Just that taking this step out would make the theorem more accessible. So this is the statement that if you have a prime p, which divides product of two natural numbers, you take any two natural numbers m and n and assume that p divides the product mn, then p should divide m or p should divide n, the prime p will help to divide one of them. It cannot happen that p is a prime it divides mn and yet it does not divide any of the m and n.

So, let us see a proof of this, proof is actually quite simple. Suppose p does not divide m, we started with a prime p dividing the product mn. And now, we assume that p does not divide m. If this statement of the lemma has to be true, then p should now divide n, because our statement says that when you have p dividing mn and p does not divide m, it should divide n, it should divide one of the two m or n.

We have assumed that p does not divide m, then we should prove that p divides n. So, how do we go about that? We use the notion of GCD, the GCD of p and m should be 1, since p is a prime it has exactly two factors in N, 1 and p. Now, if we want to compute the GCD of p and m it should first of all be a divisor of both p and m, the factors of p are 1 and p.

So, the GCD has to be among these two, can it be p, GCD cannot be p because p does not divide m GCD has to divide both p and m. So, GCD, this is the symbol, which we mathematicians use to say that the earlier statement implies the next statement. It says that the GCD of p and m is 1. But if 1 is the GCD of p and m, we should be able to write 1 as a linear combination of p and m.

(Refer Slide Time: 21:20)



Euclid's Lemma: If p | mn then p | m or p | n.

Proof (contd.): Then $1 = p\alpha + m\beta$ for some $\alpha, \beta \in \mathbb{Z}$.

We get $n = pn\alpha + mn\beta$

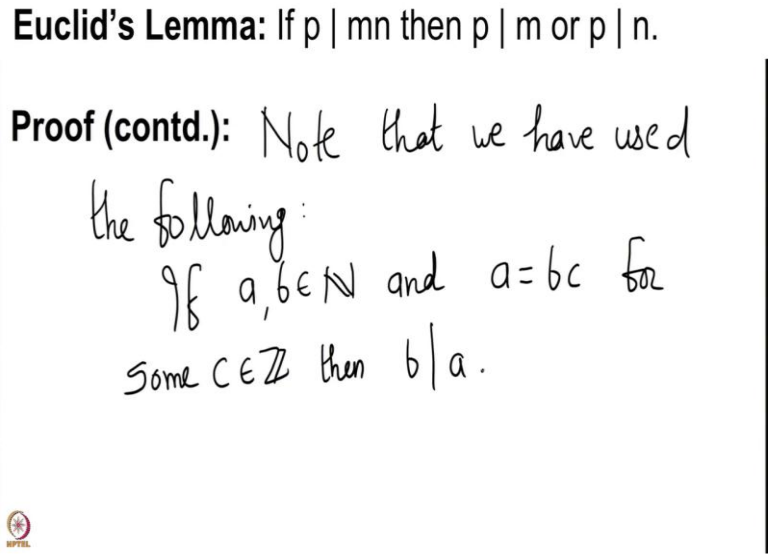
Since p divides the RHS of the equation p also divides the LHS.

Hence p/n.

So, then 1 is p alpha plus m beta for some alpha beta in Z. Now, what do we do? We will multiply both sides of this equation by n, n equal to pn alpha plus mn beta, we multiplied both sides of the equation 1 equal to p alpha plus m beta by n and we obtained n equal to pn alpha plus mn beta. Now, p divides the right hand side because p divides pn alpha and p divides mn beta p divided by mn, so it should divide mn beta and therefore, p divides n.

Since p divides the RHS which stands for the right hand side of the equation, p also divides the LHS. Hence, p divides n, mind you that we have not used the fundamental theorem of arithmetic here, what we have done is the following, we had n equal to pn alpha plus mn beta, which can be written as p into some natural number and therefore, we conclude that n has to be a multiple of p. So, we have now proved that p divides mn and p does not divide m, then p should divide n, there is one more small thing which we have used here.

(Refer Slide Time: 24:03)



Euclid's Lemma: If p | mn then p | m or p | n.

Proof (contd.): Note that we have used the following:

If $a, b \in \mathbb{N}$ and $a = bc$ for some $c \in \mathbb{Z}$ then $b | a$.

Note that we have used the following. If a comma b are natural numbers and a equal to bc for some c in integers then b divides a. Our definition of division was that this c has to be among the natural numbers. But if you see the previous proof carefully we had alpha and beta which were coming from integers. There was no guarantee that those alpha beta are positive. In fact, if you have the GCD to be 1, and you have these numbers, which are m n and p, which are bigger than 1, then one of the alpha beta has to be negative. Otherwise, you do not get 1 as a linear combination of p and m.

Even then, we would then have n as a product of prime into a natural number. So, how do we do it? We use this statement. If you have a, b, both are natural numbers, but a is b into c for some integer c, then b divides a, so this c has to be a natural number. And that is very easy to see, because we have a trichotomy, remember, whenever we have any two, the natural numbers, we have the trichotomy that a is b, or a is less than b or a is bigger than b. And this trichotomy holds actually for the whole set of integers. So we use this trichotomy for the pair 0 and c.

So now, c can be 0, if c is 0, then you have that a itself is 0, which is a contradiction because 0 is not an element in (()) (26:09), so, c cannot be 0, can c be negative can c be less than 0, you have b which is positive being a natural number, and if you multiply to that by a negative number, the product has to be negative, which will mean that a cannot be natural. In fact, a is a negative of a natural number.

So, we conclude that the third case, third possibility of the trichotomy must hold, which is that c has to be bigger than 0 and therefore c has to be a natural number. Thus, we have that b divides a. Alright, so we will stop for the moment here and in the next lecture, we will really begin with the proof of the fundamental theorem of arithmetic. See you then.