**A Basic Course in Number Theory**
**Professor Shripad Garge**
**Department of Mathematics**
**Indian Institute of Technology, Bombay**
**Lecture 04**
**Division Algorithm and the GCD**

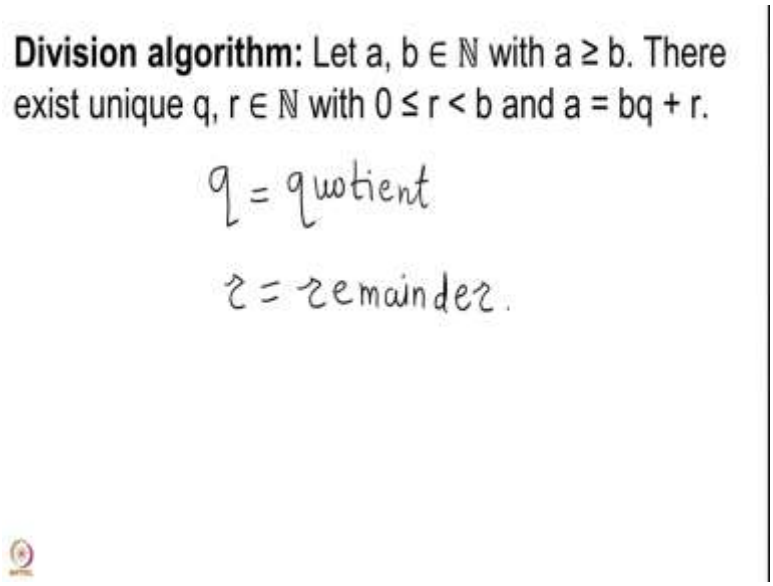
Welcome back, in our last lecture we proved that there are infinitely many primes. So, if we really want to study numbers we have infinitely many prime elements at our disposal. That is a good result to have primes are some of the very interesting numbers and it is a good thing that there are infinitely many primes.

Because actually it turns out that primes one could perhaps even say that if there is a property that an infinite set should satisfy then prime numbers will satisfy that. Any reasonable property ofcourse, for instance, there is this twin prime conjecture which says that there are infinitely many primes p such that p plus 2 is also a prime.

On the other hand, one can write down any set of consecutive n integers such that there is not a single prime in this set and you should be able to construct this set for yourself. You have seen all the required concepts for do producing such a counter example in the last lecture itself. So, I am not going to tell you that example. I am not going to tell you how to produce this set. But I will leave it to you.

At the end of the last lecture I promised that we will see the fundamental theorem of arithmetic. What does that this theorem say? It says that if you take any natural number n bigger than 1 then this n is uniquely a product of prime integers. This is a non-trivial theorem and a very basic theorem that is why this is called the fundamental theorem of arithmetic. So, before going to prove this result, we will need to develop 2 or 3 important concepts.

(Refer Slide Time: 02:25)



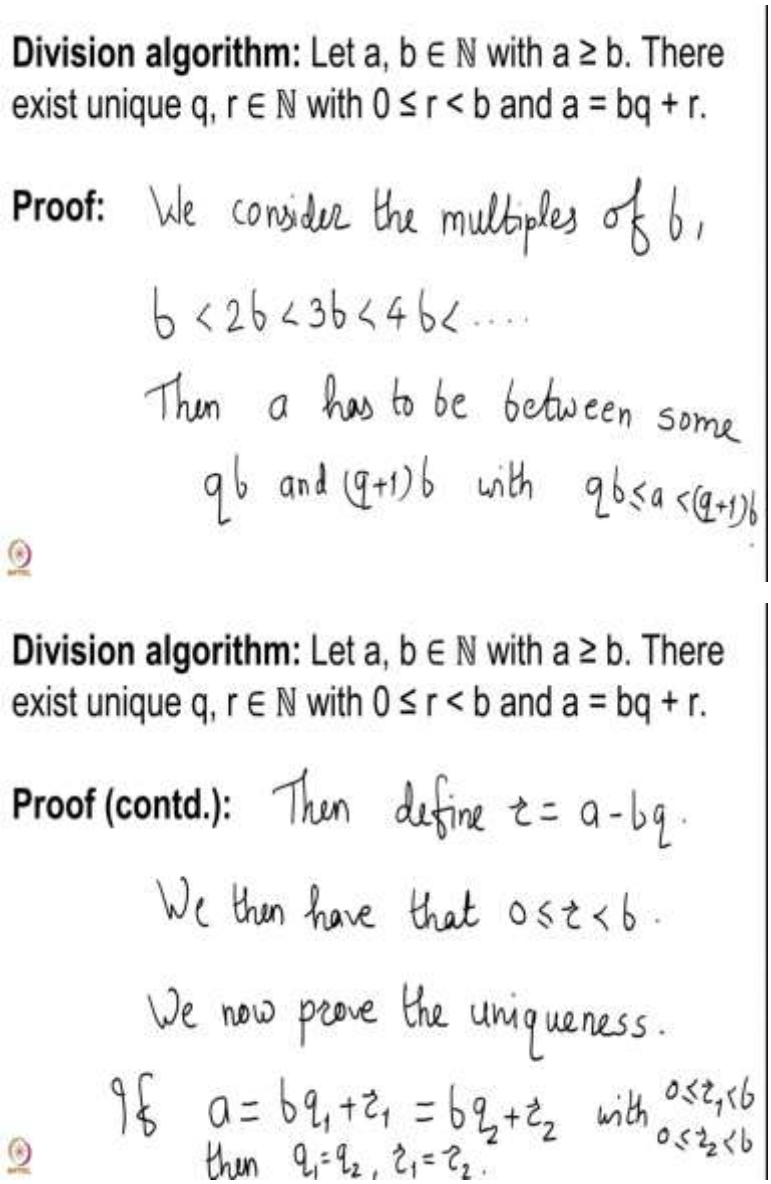

So, let us go to the first one, this is the division algorithm. What we do in this is the following thing. Suppose we have two natural numbers a and b and let us assume that a is bigger than or equal to b. Then there exists unique integers q and r with 0 less equal or less than b and a equal to bq plus r. So, what do these q and r represent?

If you have done long division in your school, then you would realize that this q is nothing but the quotient and r is nothing but the remainder. Here q stands for quotient and r stands for remainder. So, it says that when you have a and b and we are assuming that a is bigger equal b. Remember we had this property that whenever b divided a, b should be less than or equal to a, you have a number dividing some another number then that another number has to be bigger.

So here we are also allowing the possibility that r b equal to 0 because then that would give us that b divides a, it would give us that a is b into q. So, we are starting with a bigger equal b. Then there exists q and r with the property that a is bq plus r. Moreover, we have that this remainder r is between 0 and b, but it is allowed to be equal to b. We allow r to go only up to b minus 1.

Another important thing to prove here is that these numbers are unique. This is something that you would think should be quite natural to have meaning some of you may even wonder why we need a proof for such a statement. But the uniqueness is the thing which requires a proof and the uniqueness is going to be proved using the condition that we have that 0 is less than or equal to r less than b, okay. So, we go about proving this statement. What we do is the following thing.

(Refer Slide Time: 05:06)




We consider the multiples of b. So you have b, 2b because your b is a natural number. We will have b to be less than 2b, less than 3b, less than 4b and so on. So, we have this set of multiples of b, which goes this set goes all the way up to infinity. Now a is a natural number, it will have to belong to some such subset.

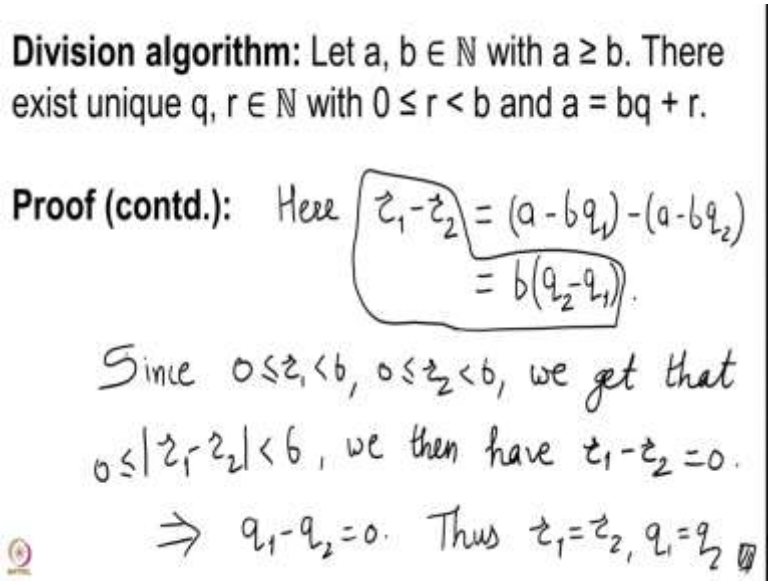
So a has to be between some qb and q plus 1 b. What did we do? We are looking at all multiples of b, which go all the way up to infinity and a is a natural number so there has to be a multiple of b, which is beyond a. Among all those multiples which are multiples of b, which are beyond a, we look at the smallest one.

And we then have that a is between some qb and q plus 1 b with the property that qb is less than or equal to b, which is strictly less than q plus 1 into b. It may happen that a itself is a multiple of b. If that happens then we take q to be that particular multiple. We do not take it to be q plus 1. What did we do? We have now obtained q which has given us that a is bigger than or equal to qb and strictly less than q plus 1 into b.

Let us continue our proof then define r to be a minus b into q by our very construction of q, we see 0 is less than or equal to r strictly less than b. This is because a was strictly between, a was bigger than or equal to bq but strictly less than q plus 1 into b. So, we have constructed r, we have constructed q.

Now, we need to show the uniqueness. What do we have to do to show uniqueness? We start with assuming that there are two such pairs of q and r and we have to prove that the corresponding q's are same and the corresponding r's are same. So, if a is bq1 plus r1 and bq2 plus r2 with 0 less than or equal to r1 less than b, 0 less than or equal to r2 less than b, then q1 is q2, r1 is r2. This is the statement that we should prove. So, let us go on proving this.

(Refer Slide Time: 09:40)




Here r1 minus r2 is a, what is r1? r1 is a minus bq1, r2 is a minus bq2. So this is b into q2 minus q1. So r1 minus r2 is b into q2 minus q1 in particular r1 minus r2 is a multiple of b. But, what is r1? r1 is something from 0 to b, but it does not equal b, r2 is something from 0 to b, but does not equal b.

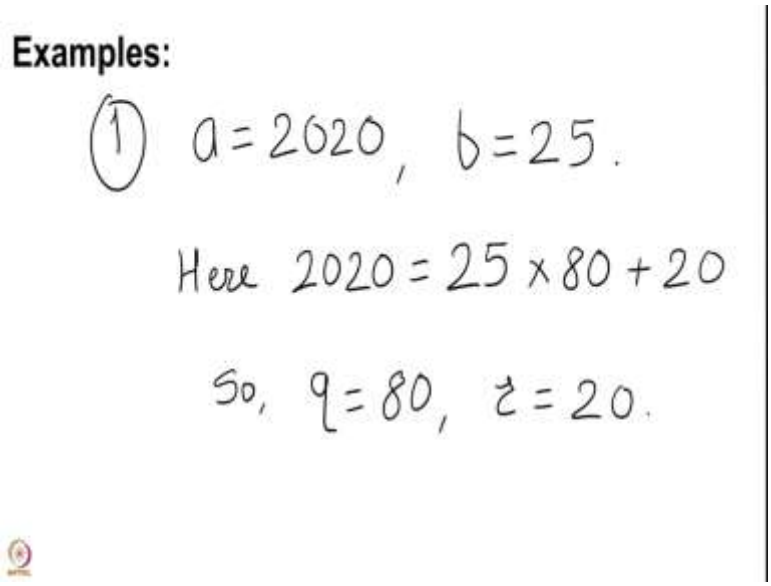
So, we have these possibly b distinct elements 0, 1, 2, 3 all the way up to b minus 1. So we have b distinct elements, r1 and r2 are among these b distinct elements. Their difference will always be between minus b and b. Because it can happen that r1 is smaller than r2. But their modulus of the difference is going to be always less than b.

So, if b divides it, then the difference r1 minus r2 has to be 0. So since 0 less than r1 less than b, 0 less than r2 less than b, we get that modulus of r1 minus r2. This is allowed to be 0 but it is strictly less than b but since this is a multiple of b we then have r1 minus r2 to be 0, there is no other possibility. So this implies also that q1 minus q2 is 0.

Because from here, we see that r1 minus r2 is b into (q1 min) q2 minus q1. So if the difference r1 minus r2 is 0, b into q2 minus q1 is 0 but b is a natural number it is not 0 and if q2 minus q1 was a non-zero number either positive or negative that into b would give you another (natural) non-zero number.

If the product is 0 then q2 minus q1 has to be 0, which says that q1 is q2. This way we have completed the proof. So this proves that when we have the division algorithm then the quotient q and the remainder r, that we get here r unique, a is b into q plus r for unique integers q and r and now we are going to see some examples of this phenomenon. So, we will start with some a and some b and we will try to find these quotients q and the remainders r something very simple.

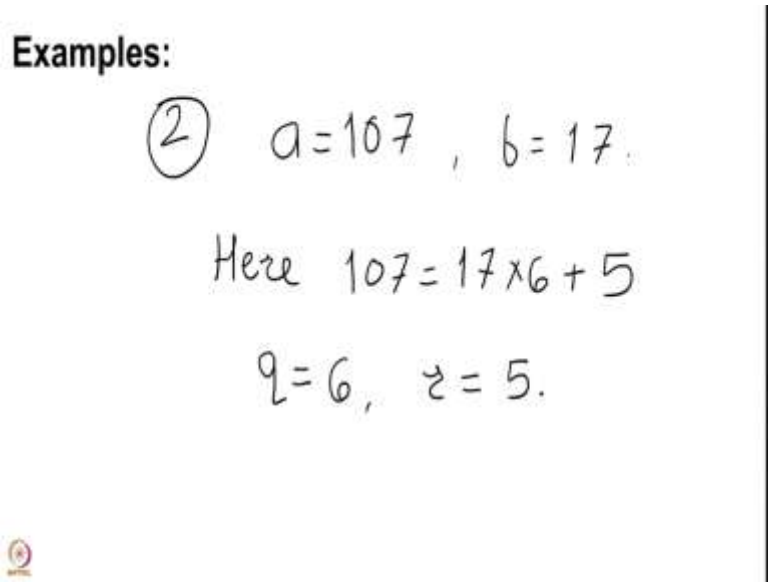
(Refer Slide Time: 13:43)




So, start with the first example where I take a to be 2020 since this is our Gregorian here, let us work with 2020 and let me take b to be 25. I want to have an easy division. So what is the multiple of b 25 which goes all the way up to 2020 but does not cross it? So what is the quotient q of b with the property that b into q is less than or equal to 2020 but b into q plus 1 goes beyond 2020.

So for this division, you know (())(14:29) we see that 2000 should that multiple because 2000 is a multiple of 100. 2000 is 20 into 100 and therefore it is going to be 80 into 25. So here 2020 is 25 into 80 plus 20. So, q the quotient is not 25, sorry, this is 80 and the remainder r is 20, 2020 is 25 into 80 plus 20. Let us take another example a simpler example.

(Refer Slide Time: 15:26)




Suppose I take a to be 107 (())(15:32) and I take b to be the prime 17, I do not know if 107 is a prime when we some year lectures back listed all the primes we listed them only up to 100 not beyond that so we do not know whether 107 is a prime but b 17 is a prime.

Now, I want to find the quotient q such that when I multiply 17 by q we go up to a and 17 into q plus 1 goes beyond a goes beyond 107. So this is the time to remember your multiplication table of 17. So if you remember that you will notice that 17 into 6 is 102 and 17 into 7 becomes 119 where you go past a, past 107. So, here 107 is 17 into 6 which is 102 plus 5. So q is 6 the remainder r is 5.

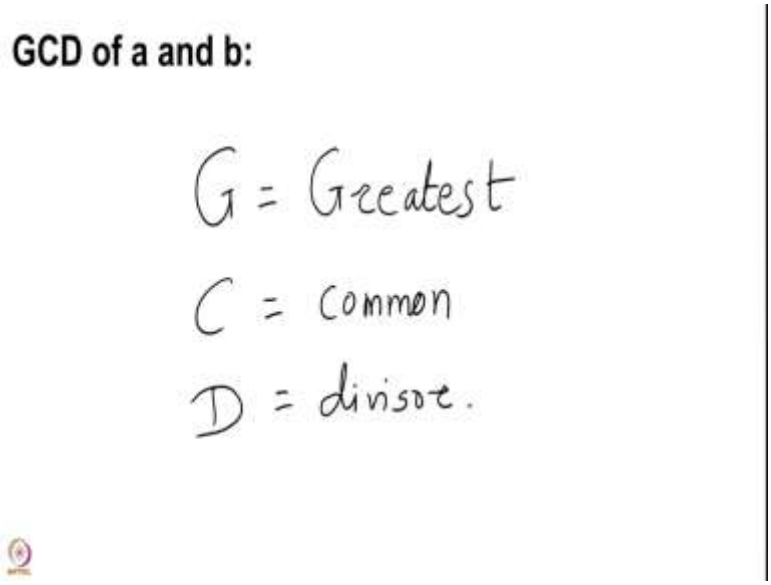
These are some of the very basic examples in the quiz that we will have this week we will see some more examples, but these are not by any means impossible example meaning these are some problems where you will have to sit down with your pen and paper and do the writing. You can also use calculator for that, if you wish, you know what you have to do is compute a upon b make sure that a is bigger than b.

I will not give you problem where a is equal to b. Make sure that a is bigger than b compute the division a by b on your calculator. It will be some integer dot something else after the dot ignore the dot that integer that you get is going to be your q. So, that is your q you already know what are a and b you will then be able to compute r which is going to be a minus bq.

So that way you will have a equal to bq plus r that way you are going to have the quotient q and the remainder r. Now this algorithm which is called division algorithm, which is due to Euclid is something which is very fundamental to the computation of what is known as the greatest common divisor of any two natural numbers. So you may ask given any two natural numbers a and b whether there are any common divisors.

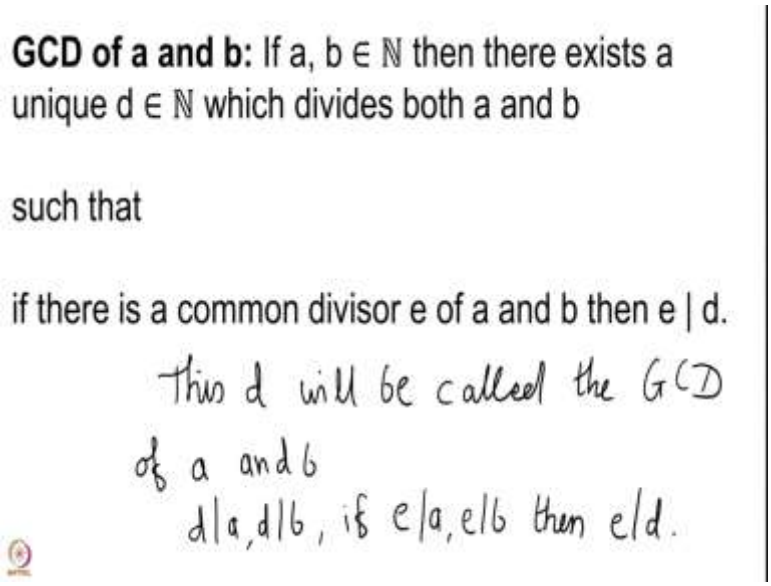
So, ofcourse, we know that 1 divides every a therefore 1 is going to divide both a and b. So, the question turned out to be very simple question that we wanted to know whether there are common divisors and here is a common divisor 1. Then we modify the question. We asked whether there is anything beyond 1 which divides both a and b and our question is even more precise. We want to get the largest such integer which divides both a and b.

(Refer Slide Time: 19:05)




This is called the GCD the greatest common divisor of a and b. So, GCD here G stands for greatest common divisor. This is what we want to find. So, there is a statement that needs to be understood and then proved which is as follows.

(Refer Slide Time: 19:40)

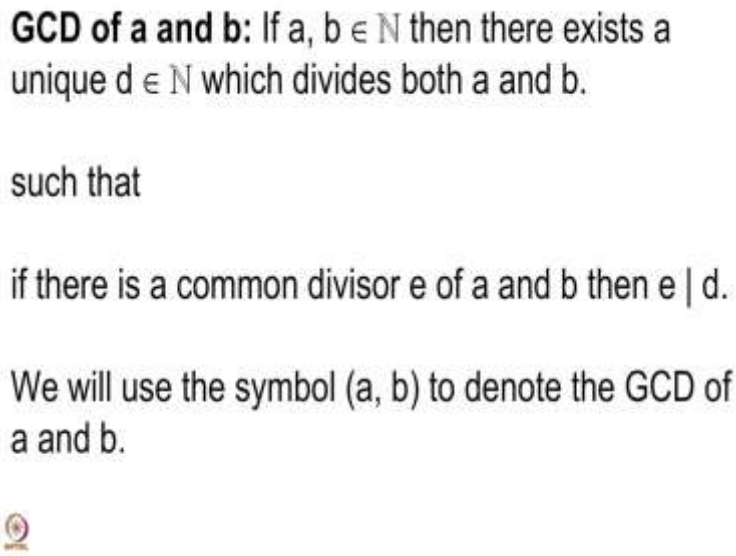



Suppose we have two natural numbers a and b. Then the statement says that there exists a unique d which divides both a and b mind you that there is no full stop here. So, our statement is not yet complete. So, what does the statement say? The statement says that there is a unique d which divides both a and b. If you are saying something is unique clearly the dividing of a and b cannot be unique because one divides it and possibly there are some more devisors.

So, there is one more property of this d, which is that such that, so the uniqueness is with respect to this condition, which is now going to follow after that such that. If there is a common divisor e of a and b then e divides d. So what does it say? It says that there are two conditions. The GCD, so this d will be called the GCD of a and b. What property does it have? It says that d divides a d divides b. If e divides a, e divides b then e divides d.

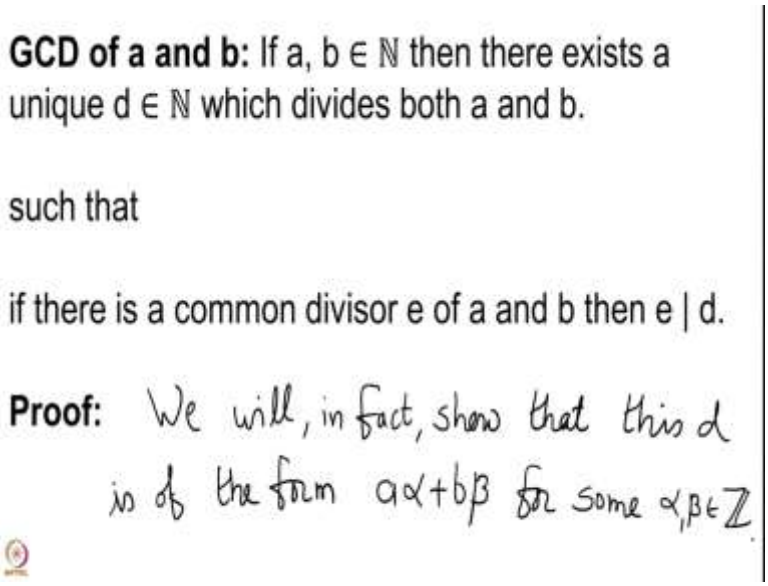
In this sense, it is the greatest common divisor. So it is among the common divisors. It is the greatest of them.

(Refer Slide Time: 21:23)




What we are now going to do is to prove that such a greatest common divisor actually exists. Given any two integers a and b it would not be very difficult to find this GCD. This is something that we have been doing in school, but to prove abstractly that this holds for any two natural numbers is not that trivial it will require some trick. So, let us see the proof. We will in fact.

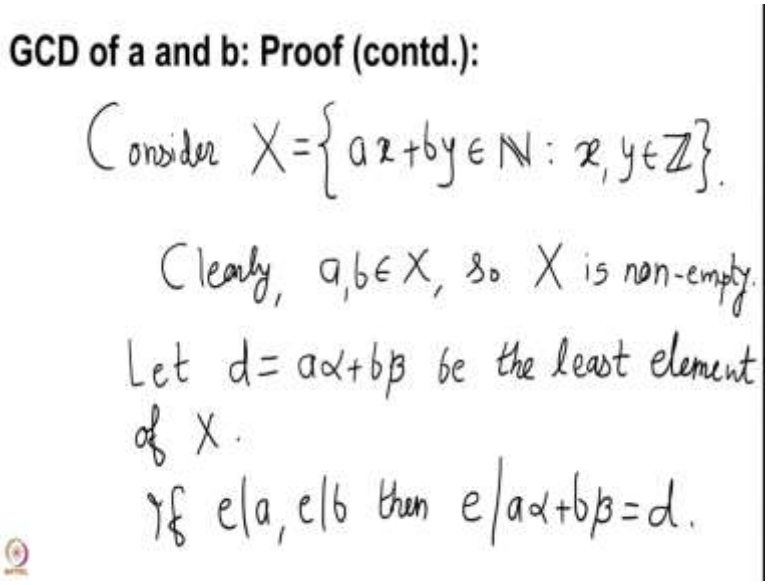
(Refer Slide Time: 22:11)




We will in fact show that this d is of the form a alpha plus b beta for some alpha beta in Z. I hope you all remember that Z denotes the set of integers you take negative numbers, positive numbers

and 0. This is the set of integers. We will take alpha beta from this and we will actually show that our d belongs to this set, d is of these form, okay. So, that is what we want to prove.

(Refer Slide Time: 23:14)




Consider the set X of the form of elements ax plus by, x and y belong to z. We considered, we are considering the set of the form of natural numbers of the form ax plus by where x and y comes from the set of integers. So we are allowing x and y to take positive as well as negative values or even 0, but what we demand is that the number you obtain ax plus by that should be a natural number.

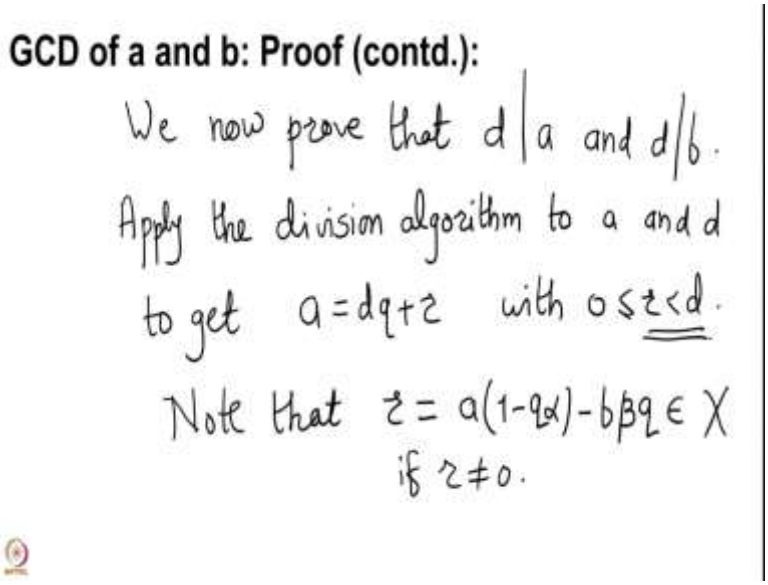
Okay so this is our set capital X. Is this set empty? Does it have some elements? So we are allowing the sets to, we are allowing the elements x y to also have the value 0 or positive or negative or any such value. So, clearly a and b belong to X. So X is non-empty, a is there because x is 1 and y is 0 will give you that ax plus by is a.

Similarly x is 0 and y is equal to 1 will give you that b is there. So, a and b these are natural numbers. Both are there in X. So X is non-empty. Then principle of mathematical induction will tell you that there has to be the a least element of this set. So let d which is of the form a alpha plus b beta be the least element of X. We are almost done. We have found the candidate d. We also found it to be of the form a alpha plus b beta.

Now, we have to prove that it is over GCD. So, clearly if e divides a, e divides b, then e is going to divide a alpha plus b beta which is equal to d. So, e will divide d. So, if you prove that it is a

common divisor that is something that we have not yet proved. We have not proved that d divides a or d divides b. We have only proved that if you have any divisor of a and b, then such a divisor should divide d. Now, the only thing left to prove now is to prove that d is a divisor of a and b.

(Refer Slide Time: 26:40)

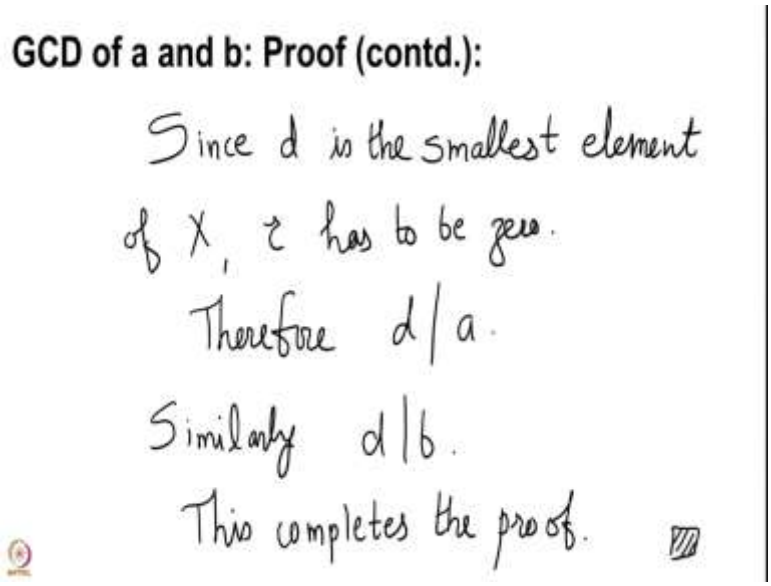



We now prove that d divides a and d divides b. How do we do it? We start with apply the division algorithm to a and d. What will it give? Division algorithm will tell you that you can divide a by d to get a equal to dq plus r with 0 less than or equal to r less than d. This is our quotient and remainder. So we get this r.

Note that r is of the form. Remember that a d was a alpha plus b beta. So, r is of the form a times 1 minus q alpha minus b beta, r is a minus dq, d is a alpha so there is an q that we should add here. So, d is a alpha plus b beta therefore dq is a alpha q plus b beta q you subtract them from a and you get that r is also an element in X, if r is non-zero.

But this is a contradiction you started with d being the least element in X. If your r is non-zero you get a number which is strictly smaller than d. We have that r is less than d.

(Refer Slide Time: 29:06)




This contradiction says, since d is the smallest element of X, r has to be zero. Which means that a which means that a is divisible by d. Similarly d divides b, so this completes the proof. Let us recall quickly what we have done.

We have looked at the division algorithm which gave us that a and b can have the form that a is dq plus r, where q and r are natural numbers, r is strictly bit less than b but bigger than or equal to 0 and using this we proved that there is a GCD, the greatest common divisor of any two natural numbers more over this GCD is of the form a alpha plus b beta where alpha and beta are integers. We stop here for the moment. See you in the next lecture. Thank you.