Discrete Mathematics

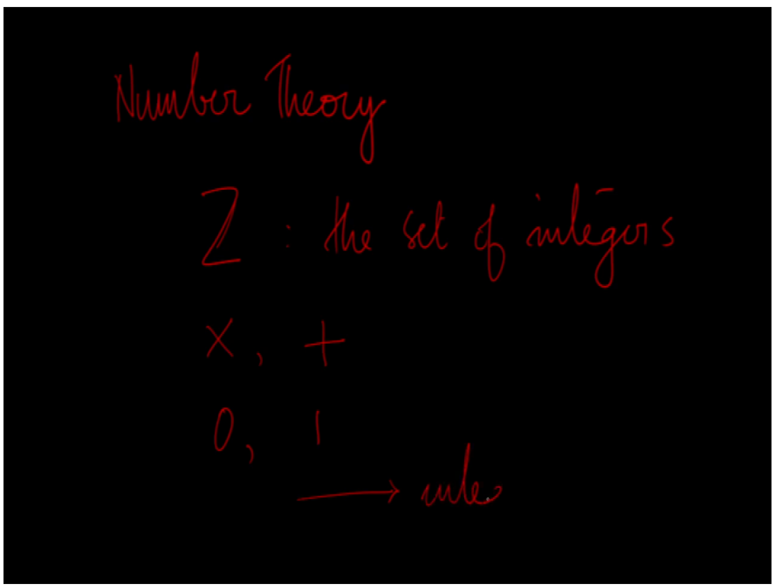
Professor Sajith Gopalan
Department of Computer Science and Engineering,
Indian Institute of Technology, Guwahati.

Lecture 22~~:~~

Natural Number, D~~d~~ivisor

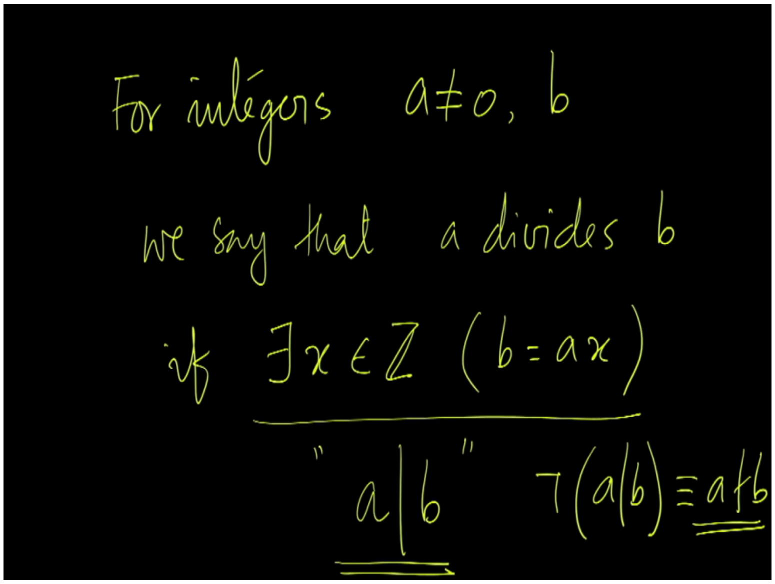
Welcome to the NPTEL MOOC on discrete mathematics. This is the first lecture on number theory. In number theory we study the theory on integers. Integers along with the two operators multiplication and addition and the two constant 0 and 1~~one~~ you would see in the module on algebraic structures that form what is called an integral domain? So number theory is the study of this integral domain.

(Refer Slide Time: 1:04)



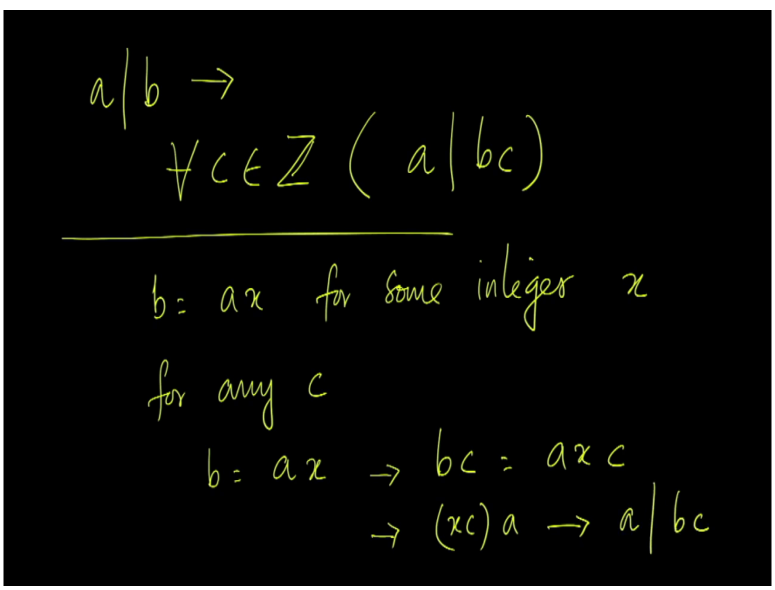
So in number theory, we deal with a set of integers and operators multiplication in addition along with 0 and 1~~one~~ together this form an integral domain.

(Refer Slide Time: 1:37)



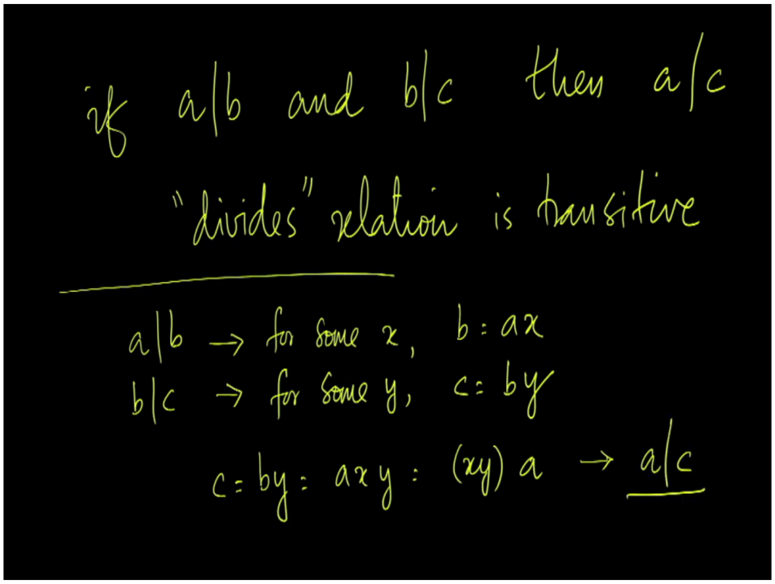
For two integers a and b where is a not equal to 0. We say that a divides b, if there exists an integer x, so that b equals ax, that is a board multiplying a with some integer x, we would get b that is when we said that a divides band this is denoted in this fashion~~slash~~ using a vertical bar. This notation asserts that a divides b. The negation of this, that is the negation of a divides b this often written like this across the vertical bar to indicate that a does not divide b.

(Refer Slide Time: 2:43)



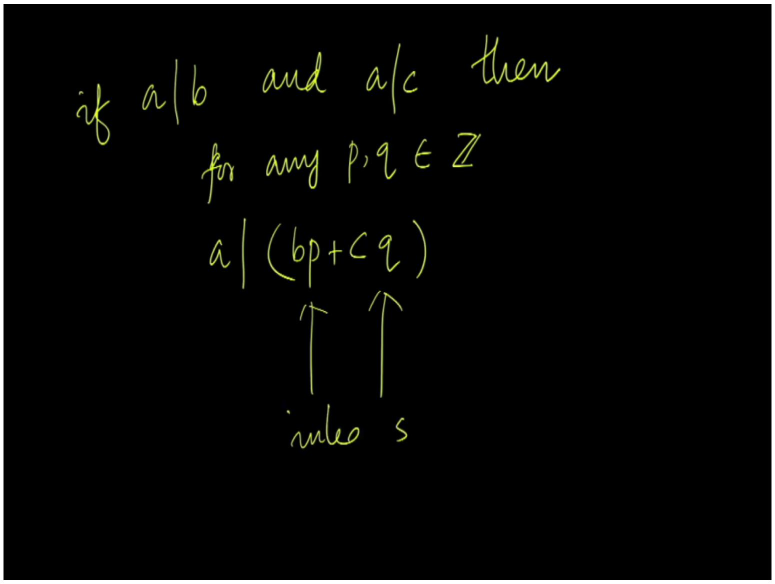
So let us see some results related to division if a divides b then for every c which is an integer it is the case that a divides bc. ~~See~~ T~~t~~his is easy to show if a divides b then b equal to ax for some integer x then for any c we have b equal to ax. Therefore bc equal to ax into c which by associativity of multiplication can be written as xc times a this implies that a divides bc. So that was easy to show.

(Refer Slide Time: 3:42)



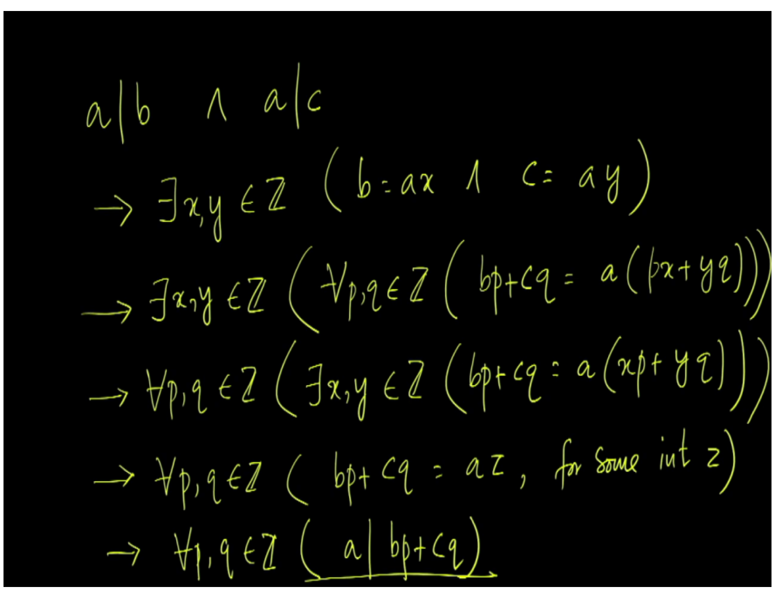
Another result is ~~tussle does~~ this if a divides band b divides c, then a divides c. In other words, the divides relation is transitive. This is also easy to show, a divides b implies that for some integer x, b equal to ax. Similarly, b divides c implies that for some integer y, c equal to by, therefore c can be written as the product of xy and a which means there is an integer so that a into that integer is c. So that implies that a divides c.

(Refer Slide Time: 4:56)



The third result is this if a divides band a divides c then for any p, q be that are integers, a divides bp plus cq. That is if a divides band a divides -c, then a will be divide any linear combination of band c, where the linear combination has integer coefficients p. ~~p~~ and q are the coefficients of the linear combination, these are integers. So any such linear combination of band c will be divided by a.

(Refer Slide Time: 5:48)

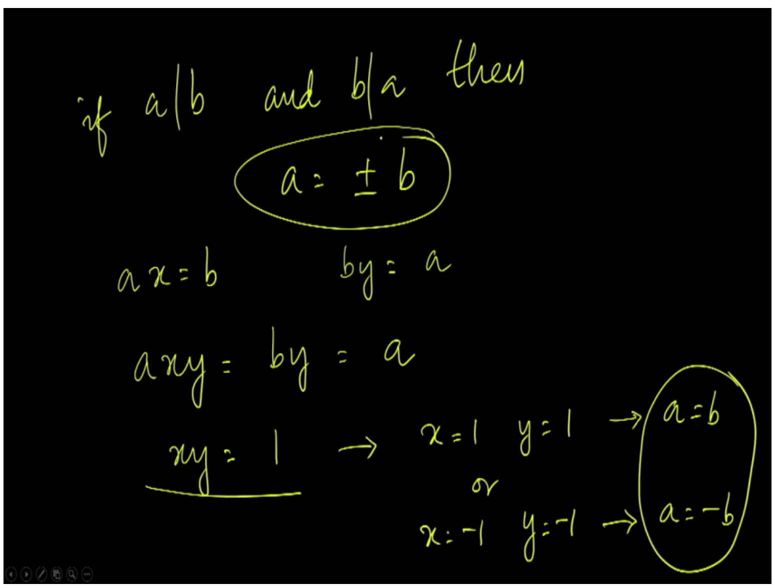


How do we show this, what is given as this a divides band a divides c. If this is the case, then by the definition we know that there are integers x and y. So that b equal to ax and c equal to ay. B is a multiple of a and c is also a multiple of a. In that case for any xy we can say for every p,q which are also integers bp plus cq this a into px plus yq.

For any pair of integers p and q we can write bp plus q as a ~~into~~ px plus ayq because b is ax and c is ay which implies that for all integers p and q their exist x and y such that bp plus cq equals a into xb plus yq. That is because this statement is a weakest treatment in comparison to the one above or in other words for every pair of integers p and q, bp plus cq is az for some integer set.

In other words for all p,q which are integers the bp plus cq is a multiple of a or a divides b plus cq and that is precisely what we wanted to show. For any pair of integers p and q the linear combination of b and c is a multiple of a.

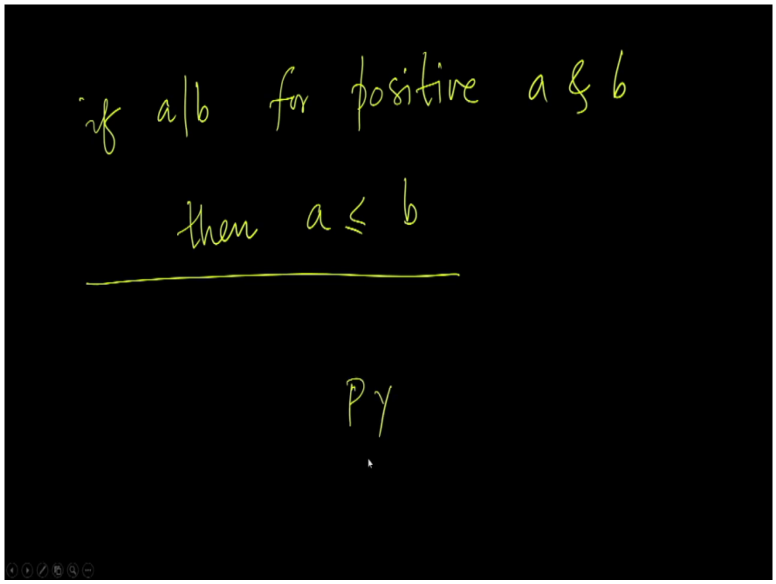
(Refer Slide Time: 8:19)



Our fourth statement is this if a divides b and b divides a then a equals plus or minus b. If a divides b, then a into x is equal to b which is an integer and if b divides a then by is a for some integer y then a xy is by which is a, where both x and y are integers. So there exist integers x and y so that a xy equal to a, or in other words xy equals one.

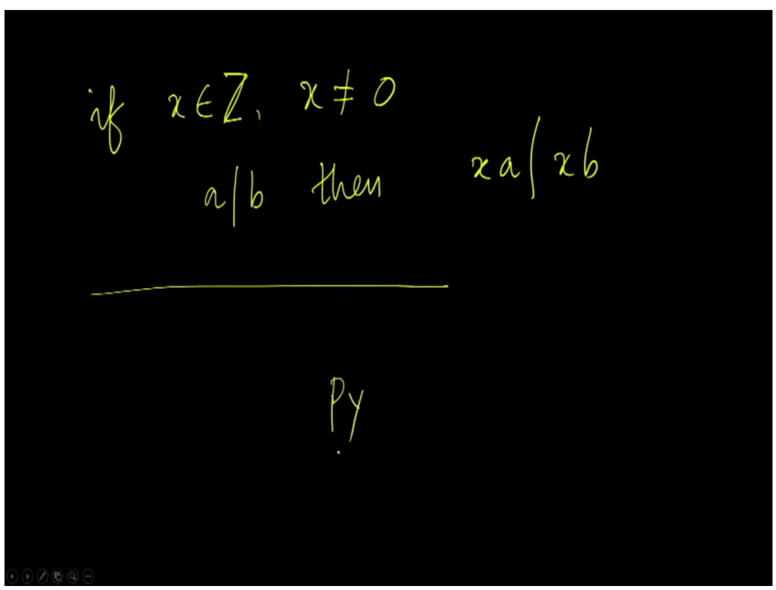
If for integers x and y, x into y happens to be 1 then we have only two possibilities either x equal to 1 and y equal to 1 or x equal to minus 1 and y equal to minus 1. In the first case we have a equal to b in the second case we have a equal to minus b. So combining these two we can assert that is a plus or minus b.

(Refer Slide Time: 9:35)



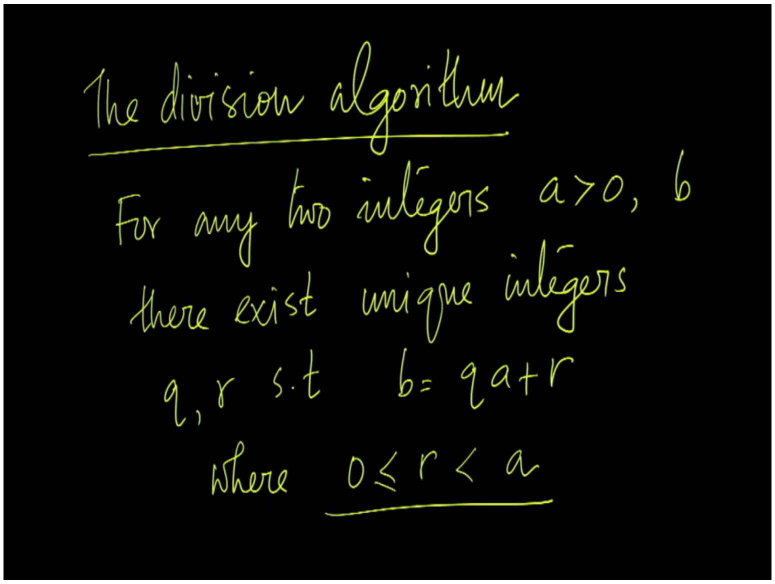
If a divides b for positive a and b then a less than or equal to b prove this yourself.

(Refer Slide Time: 9:59)



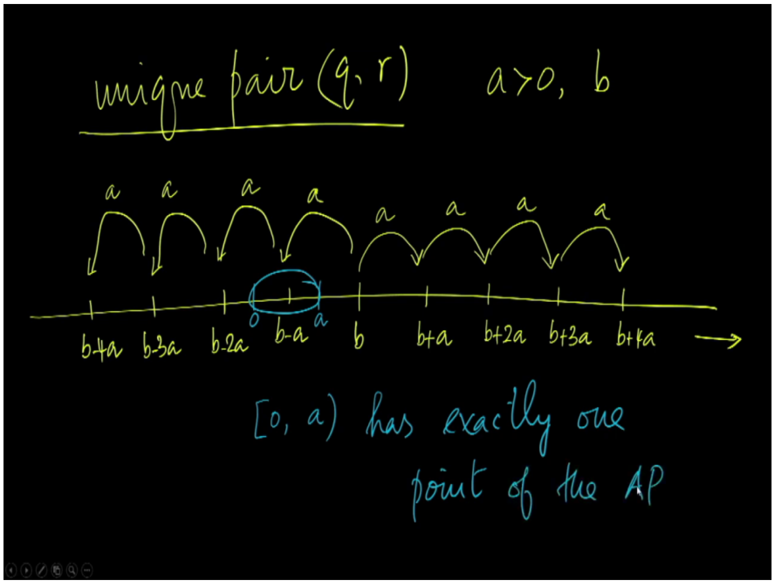
And another property of the divides relation is this if an integer x that is non 0 is given and a divides b then xa divides xb. This also you can try out, so those were some results about their divisibility relation.

(Refer Slide Time: 10:36)



Now let us see what is called the division algorithm. At the heart of this algorithm we have this theorem. For any two integers a and b, where a is greater than 0, b need not be greater than 0 there exist unique integers given r such that b is qa plus r, where 0 is less than or equal to r which is less than a. So when you find such a unique ordered pair q,r q is called the quotient and r is called the remainder.

(Refer Slide Time: 11:50)

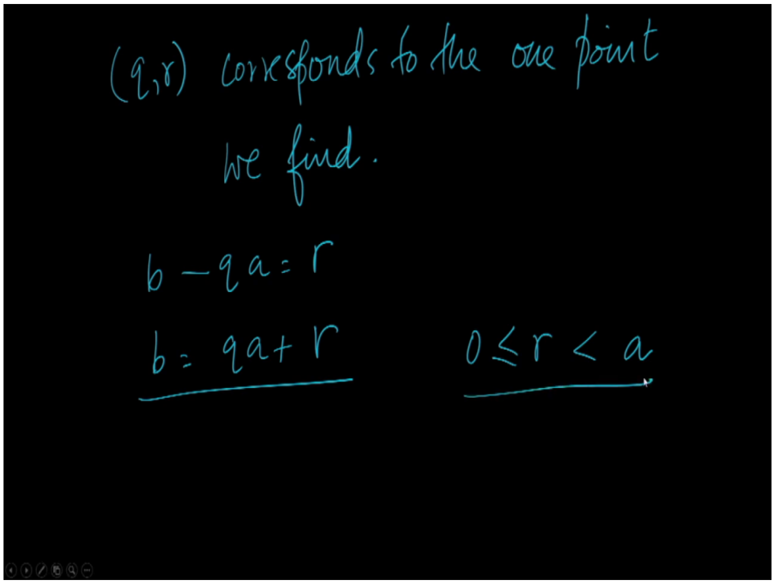


So how do we prove that there exits such a unique pair qr? That is what we want. We consider the real line on this real line consider point b. b is an integer it may be positive or negative and we have a which is greater than 0. From b let us start marking points that are at distance a. So we get an arithmetic progression b plus a is the next point, b plus 2a is the one after that~~,~~ b plus 3a is one after that and so on.

That is going to ~~Let us go into~~ the right side. If you go to the left side we have b minus a, b minus 2a, b minus 3a and so on. So starting from b we are going to the right jumping at a distance of a every time. Similarly, we can also move to the left jumping at a distance of a every time. Now on this real line 0 is somewhere let us say this is where 0 is.

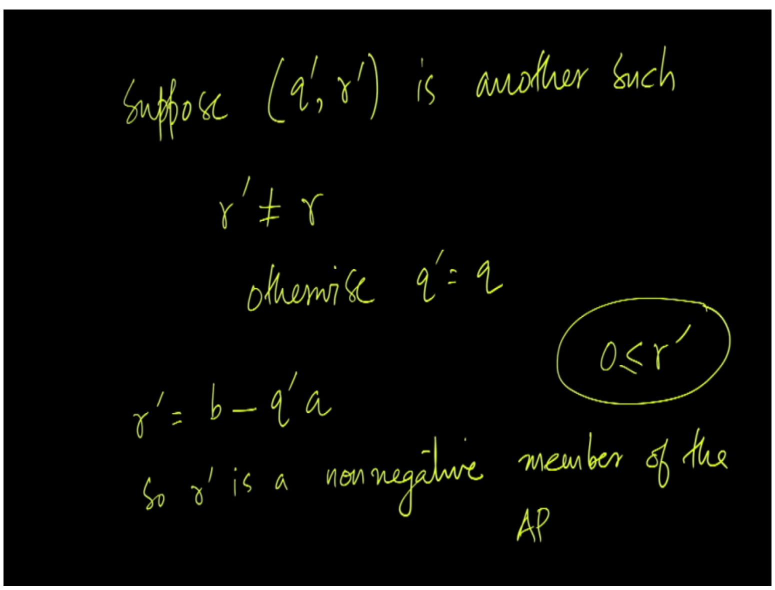
In that case a will be here at a distance of a from 0 to the right. So let us consider this interval, the interval from 0 to a. You start from b and start jumping at a distance of a either to left or to the right. In one of the directions you would jump into this interval exactly once. That is there will be exactly one point falling in this interval which is within this arithmetic progression. This interval has exactly one point of the, in particular what we need to know is that there is one point.

(Refer Slide Time: 14:26)



Suppose that one point corresponds to q,r, ordered pair q,r corresponds to the one point that we find. Then at this point we have b minus qa equal to r or b equals qa plus r and here 0 less than or equal to r less than a. Now we have to argue that this ordered pair is unique.

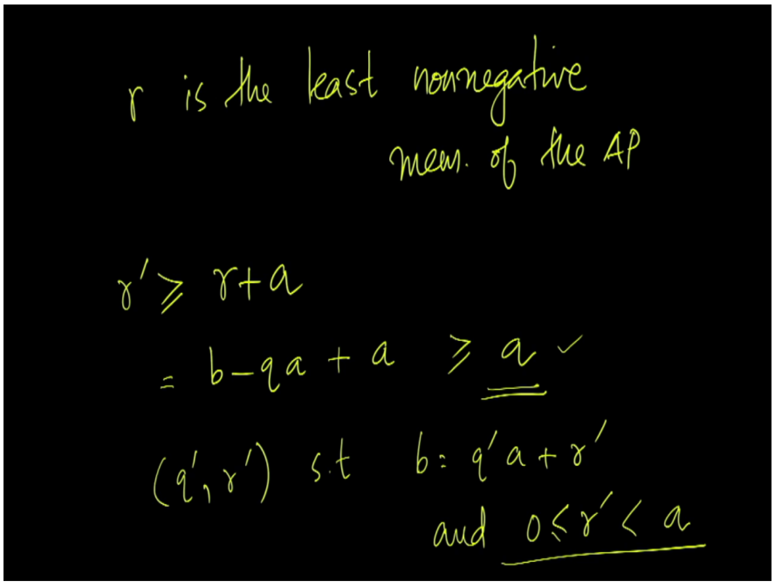
(Refer Slide Time: 15:16)



Suppose otherwise. Suppose q prime r prime is another such ordered pair. ~~cl~~Clearly r prime is not equal to r because otherwise q prime is the same as q and therefore this ordered pair would not be distinct from the earlier one. So r prime is not equal to r and r prime is b minus q prime a that is because q prime r prime is an ordered pair which satisfies our requirement.

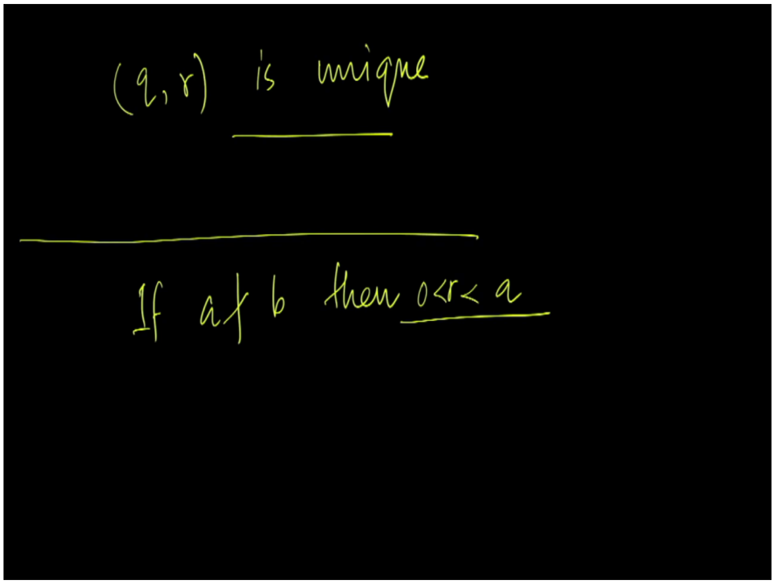
So r prime is a ~~non negative~~non-negative member of the a prime that is because we assume that 0 less than or equal to r prime. q prime r prime is another ordered pair where r prime is greater than or equal to 0.

(Refer Slide Time: 16:29)



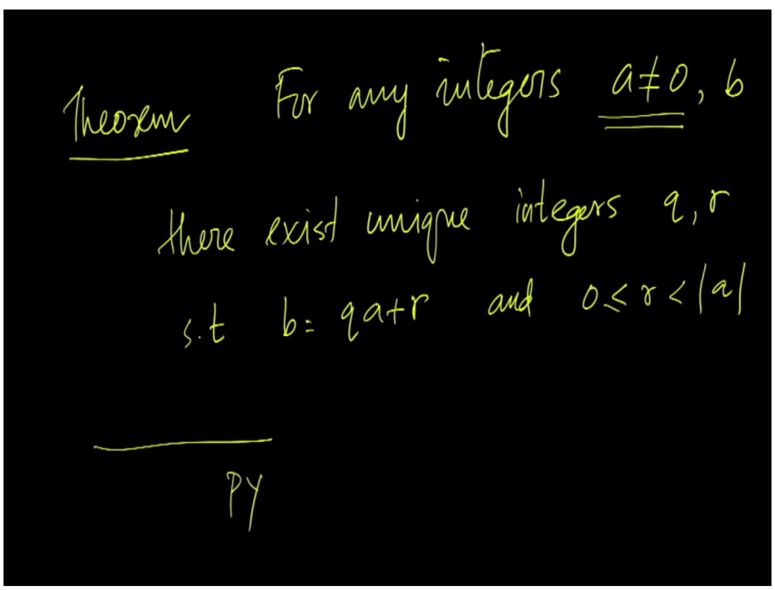
But then r is the least non-negative member of the a ~~prime~~. So r prime is greater than or equal to r plus a. But what is r plus a this is b minus qa plus a. But this is then greater than or equal to a. And therefore our prime will not qualify, because we want like q prime r prime such that b is q prime a plus r prime and 0 less than or equal to r prime less than a. This is violated here. Therefore, there cannot be another ordered pair q prime, r prime.

(Refer Slide Time: 17:30)



So q,r is unique hence our claim. If a does not divide b then 0 less than r less than a. In that case none of the points in the arithmetic progression will be devisor~~ice~~s of a. Therefore, r will be strictly greater than 0.

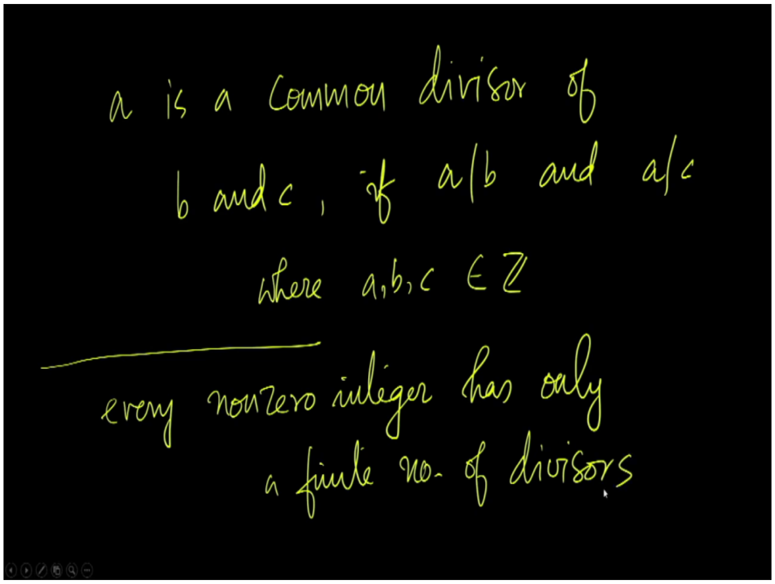
(Refer Slide Time: 18:09)



Now it is easy to show this theorem. For any two integers a and b where is not equal to 0, there exist unique integers q and r such that b is qa plus r and 0 less than or equal to r less than mode a.

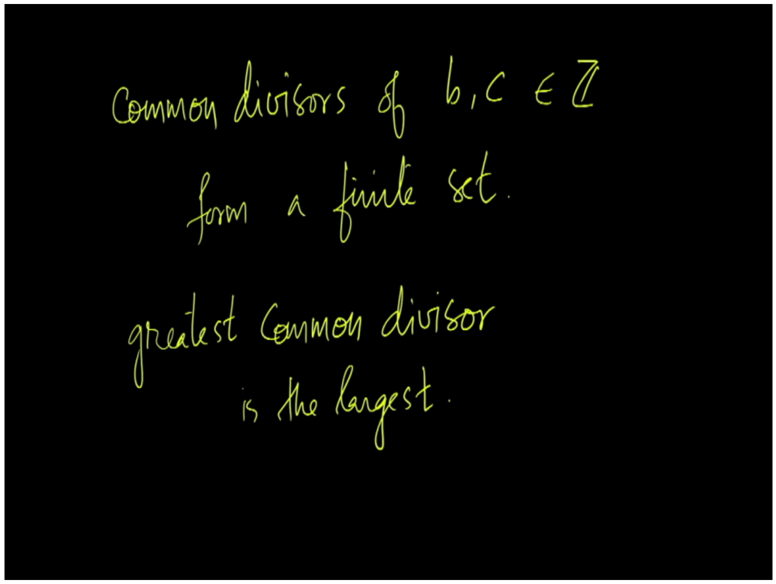
See here we only say that a is not equal to 0 we do not assume that a is greater than or equal to 0. So you can prove this theorem yourself.

(Refer Slide Time: 19:01)



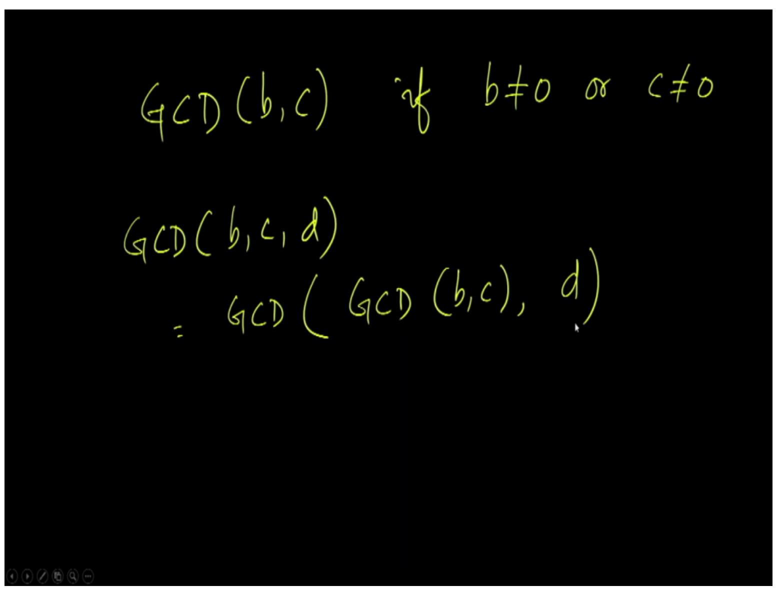
We say that a is a common divisor of b and c if a divides b and a divides c where a, b, c are all integers. So a pair of numbers b and c can have multiple common devisoers every nonzero integer has only a finite number of divisor.

(Refer Slide Time: 19:56)



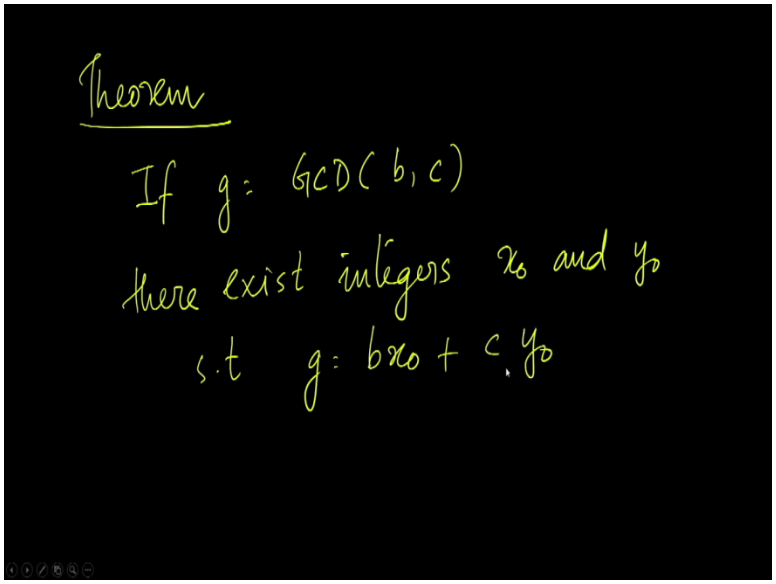
Therefore, the common divisors of two numbers b and c which are integers form a finite set. Therefore, we can talk about the greatest of them. The greatest common divisor happens to be the largest of this finite set.

(Refer Slide Time: 20:41)



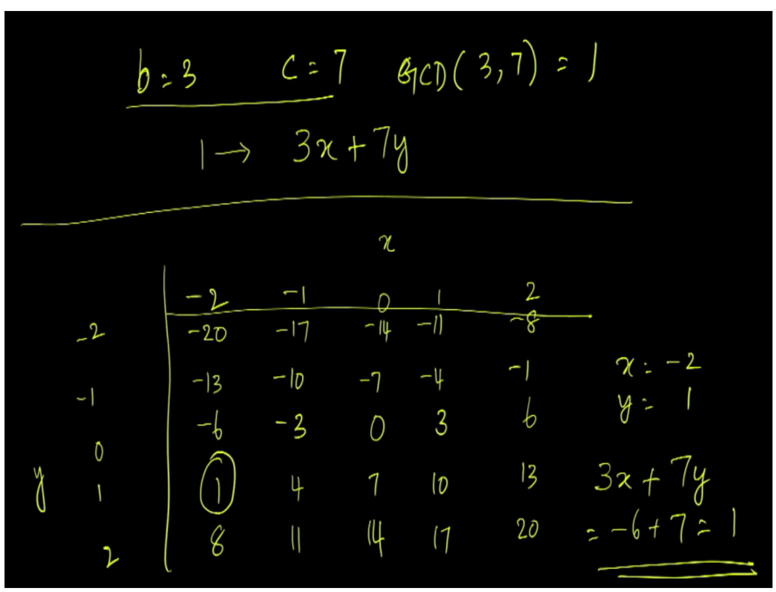
So we will denote this by GCD of b and c if b not equal to 0 or c not equal to 0. We can extend this notion to multiple integers we can talk about GCD of b, c, d which is the GCD of GCD of b and c and d.

(Refer Slide Time: 21:16)



Now we shall study an interesting theorem which says that, If G is the GCD of two numbers b and c then there exist integers x naught ~~θ~~ and y naught~~θ~~ such that j is bx naught~~θ~~ plus cy naught~~θ~~. In other words, if g is the GCD of b and c then g can be expressed as a linear combination of b and c with integer coefficients.

(Refer Slide Time: 22:03)

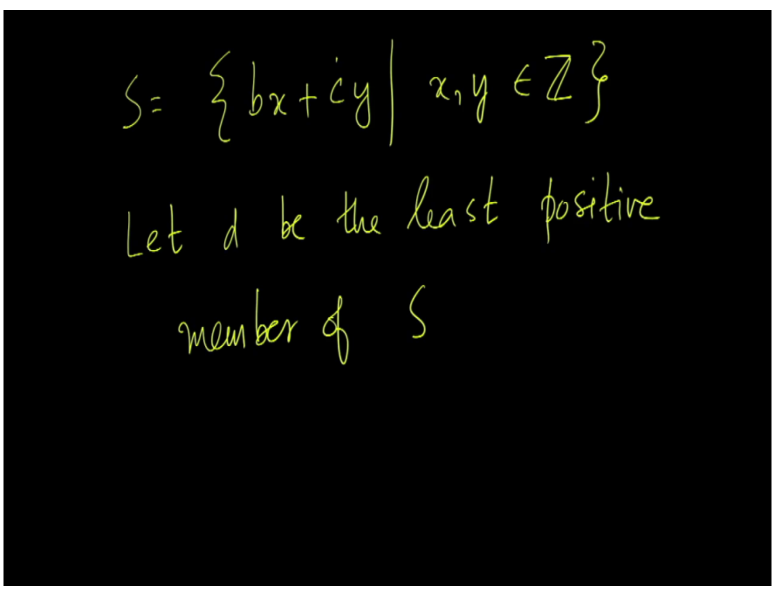


So let us see how to do this. In particular consider two numbers let us say b equal to 3 and c equal to 7. Then we want to express the GCD of these two which we know is 1. GCD of 3 and 7 is 1. We want to express 1 as a linear combination of -3 and 7. So we could write this as 3x plus 7y we have to find x and y so that 1 is equal to 3x plus 7y that is precisely what the theorem says, The GCD of two numbers can be expressed as a linear combination of those two numbers with integer coefficients x and y.

So let us consider the various possible values of x and various possible values of y. When x equal to 0, y equal to 0, we have the linear combination evaluating to 0. When x is 1 and y is 0 we have 3. When x is 2 y is 0 we have 6. On the negative side we have minus 3, minus 6. When y is 0 and x is 1 when x is 0 and y is 1 we have 7. when x is 0, y is 2 we have 14.

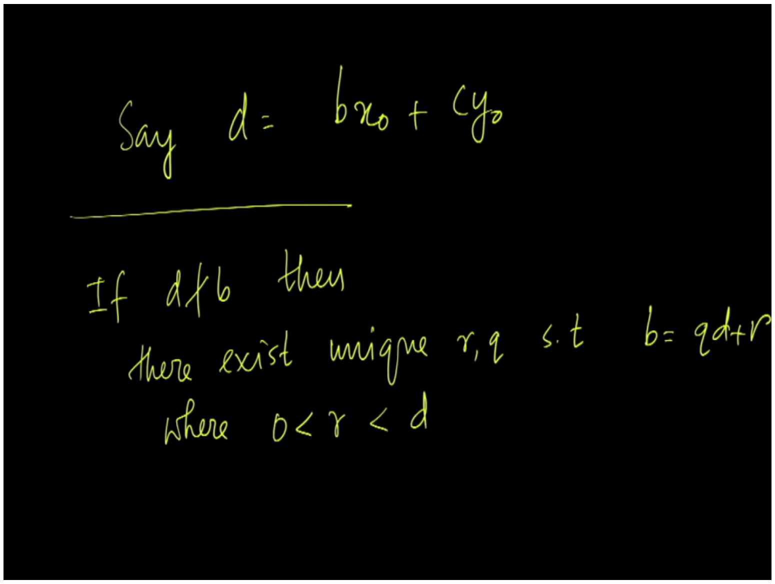
On the other direction we have minus 7 and minus 14. Here we have 10 and 17. This is how the values would look like. For various integral values of x and y, the linear combination 3x plus 7y would have these values. So you find that indeed there is one particular choice of x and y for which the linear combination of value is to 1. When x equal to minus 2 and y equal to 1 we have 3x plus 7y evaluating 2 minus 6 plus 7 which is 1. So there is a choice of x and y for which the linear combination evaluates to 1. S~~s~~o how do we generalize this? We want to bring the assertion for every pair of integers b and c.

(Refer Slide Time: 25:01)



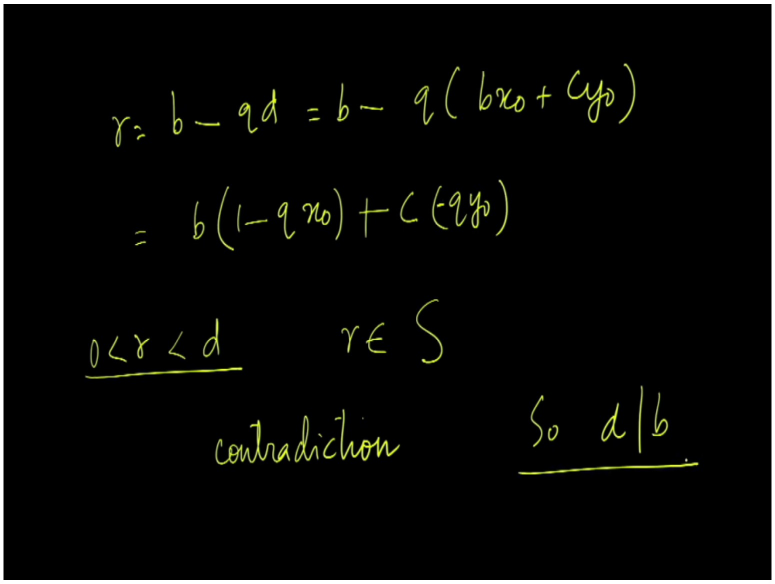
So we have this pair of integers b and c. Let us define the set s as the set of all integers bx plus cy where x and y are integers. So it is precisely this set that we depicted here for integers 3 & 7. So this is clearly an infinite set. Let d be the least positive member of s. Depending on the various choices for x and y we have different values in s we are picking out the least positive member of s we call it d.

(Refer Slide Time: 25:57)



Say d is bx naught~~θ~~ plus cy naught~~θ~~. Every member of s is a linear combination of b and c for some choice of x and y. So d is also the same. So there is a choice of x and y namely x naught ~~θ~~ and y naught~~θ~~ for which d is bx naught ~~θ~~ plus cy naught~~θ~~. If d does not divide b, then there exist unique r and q such that b is qd plus r, where r- is strictly between 0 and d.

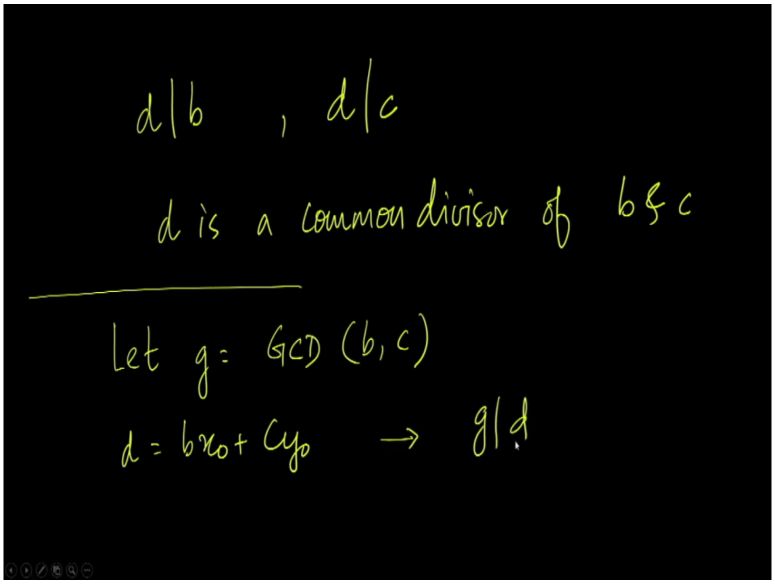
(Refer Slide Time: 26:58)



So we have r is b minus qd which is b minus q into dx naught~~θ~~ plus cy naught~~θ~~. Rearranging we get that, this is b into 1 minus qx naught~~θ~~ minus c into qy naught~~θ~~ or I can put plus here and move the negative sign here. So we have two integers 1 minus qx nauhgt~~θ~~ and minus into qy naught~~θ~~ so that our is a linear combination of b and c with these as the coefficients.

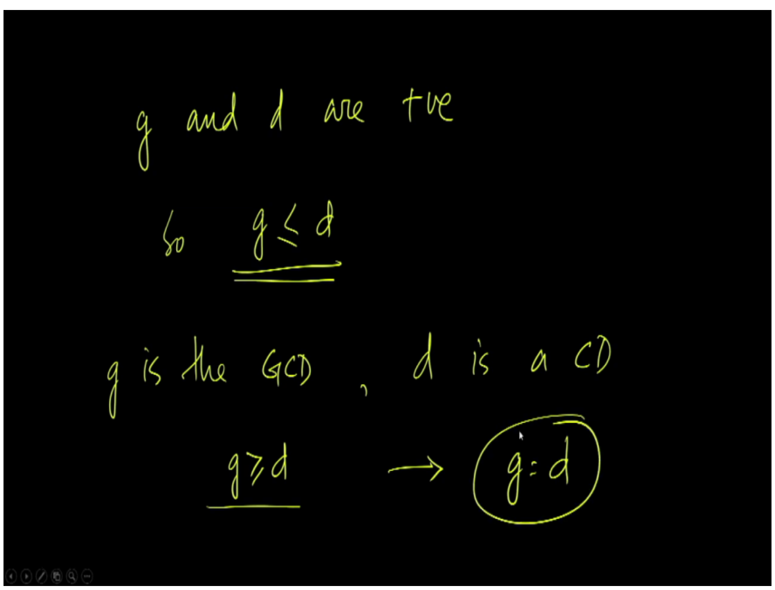
But we know that r is strictly between 0 and d therefore what we have found is that r belongs to s and r is positive. But we had picked d as the least positive member of s and here we find r which is a positive is a member of s but is less than d. Therefore, we have a contradiction and from what we derived this contradiction we assume that d does not divide b and then got this contradiction therefore it must be that d divides b.

(Refer Slide Time: 28:28)



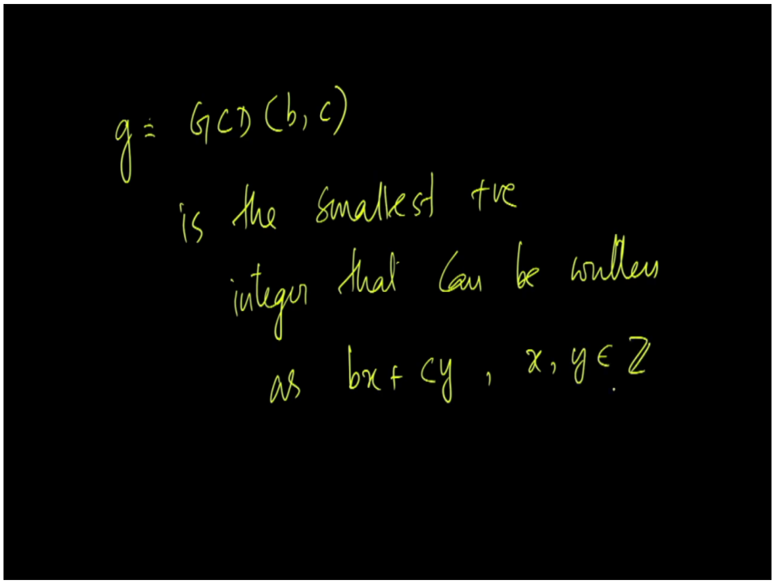
Similarly, we can also argue that d divides c. So if d divides b and d divides c then d is a common divisor of b and c. Now consider the GCD of b and c. Let g be the GCD of b and c. Since d is bx naught~~θ~~ n plus cy naught~~θ~~, we have that g divides d. g divides b and g divides c, so g divides bx naught~~θ~~ plus cy naught~~θ~~ as per the theorem we saw earlier so g divides d.

(Refer Slide Time: 29:18)



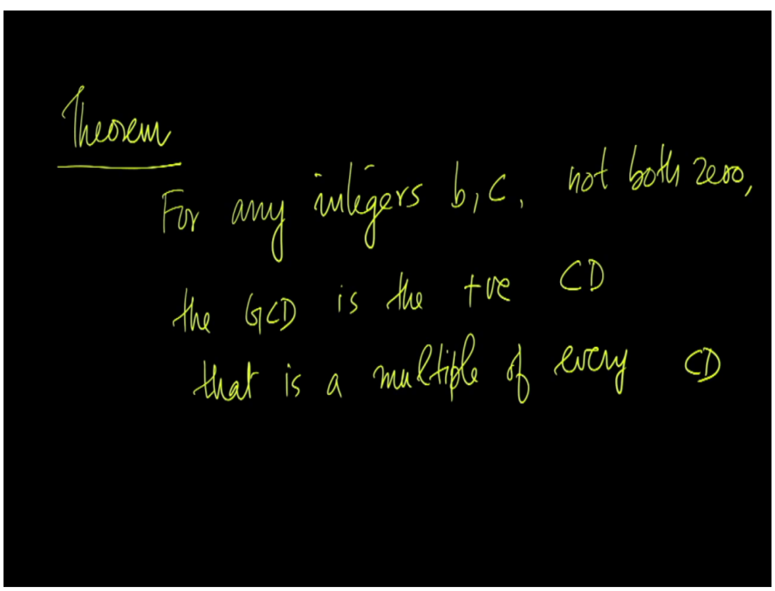
g and d are both positive. So since g divides d, g is less than or equal to d. But then g is the GCD of b and c and d is a CD a common device. g is the greatest common divisor therefore clearly g is greater than or equal to d in other words g is equal to d.

(Refer Slide Time: 30:01)



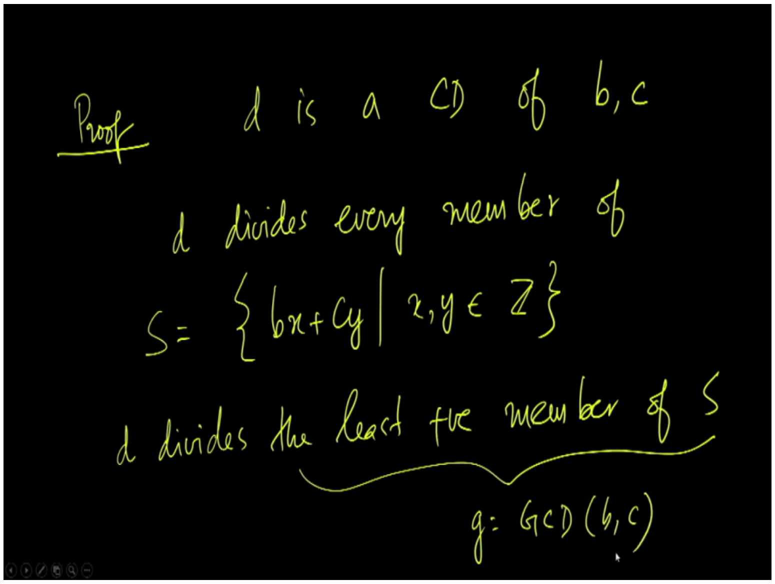
In other words, the GCD of b and c, this is the smallest positive integer that can be written as a linear combination of b and c with integer coefficients.

(Refer Slide Time: 30:37)



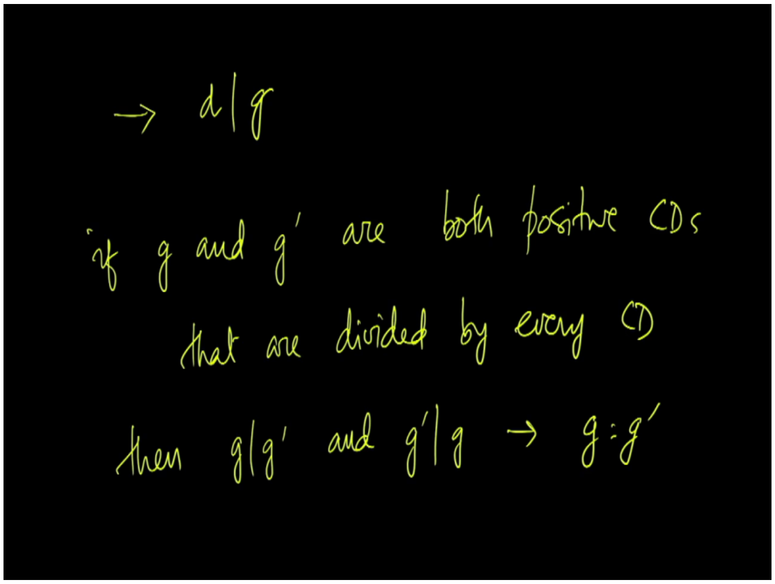
Now another theorem, For any two integers b and c not both 0. The GCD is the positive common divisor that is a multiple of every common devisor. For any pair of integers b and c, not both 0, the greatest common divisor happens to be the positive common devisor~~ee~~s that is a multiple of every common divisor.

(Refer Slide Time: 31:33)



To prove this, suppose d is a common divisor of b and c, then d divides every linear combination of b and c. If d divides b and d divides c then d divides bx plus cy for any pair of integers x and y. So d divides every member of the set. In particular d divides the least positive member of the set. This is what we call s. ~~b~~B~~u~~ut then what is the least positive member of s. That happens to be the GCD b and c so if d is a common divisor of b and c then d divides g.

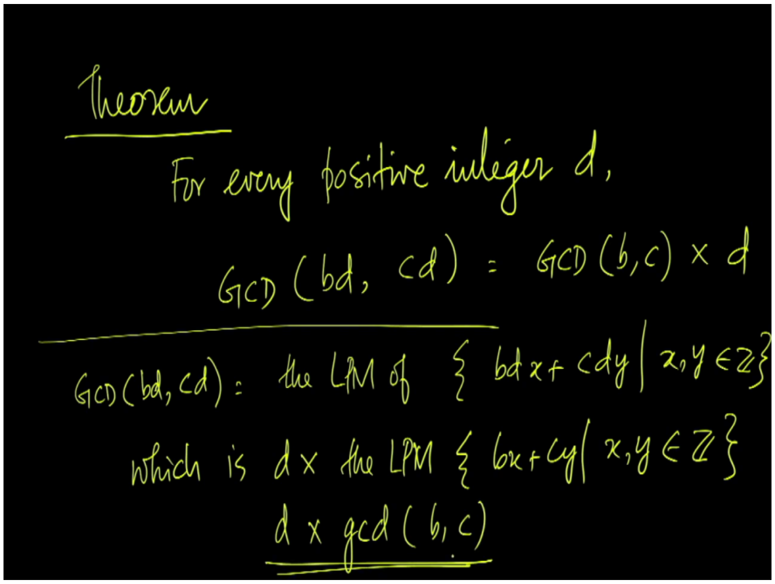
(Refer Slide Time: 32:45)



So every common divisor of b and c divides g. If g and g prime are both positive common divisors, that are divided by every common divisor, then g and g prime of themselves common divisors then we have g divides g prime and g prime divides g, which implies the g equal to g prime.

But in other words g is the only common divisor with this property the only common divisor that is divided by every common divisor of b and C. In other words, the only common divisor of b and c which is divided by every common divisor of b and c is the GCD of b and c.

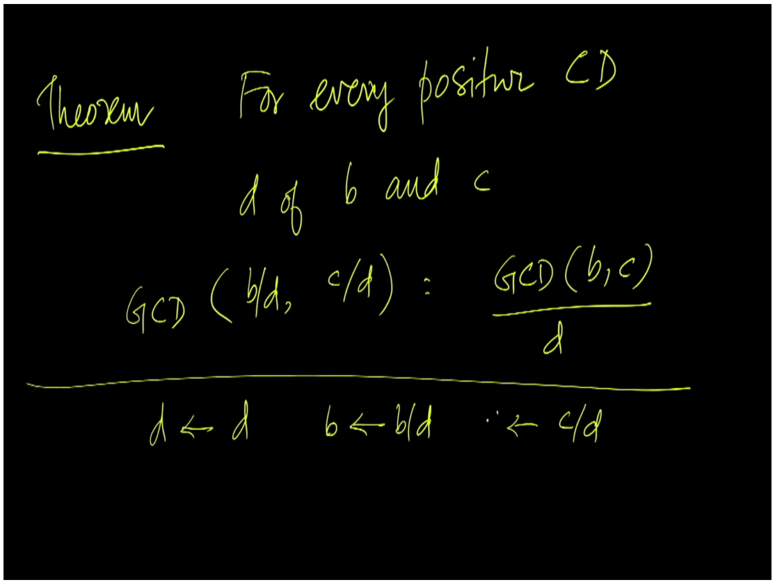
(Refer Slide Time: 33:58)



Another theorem regarding GCD’s for every positive integer d we have that GCD of bd, cd equals GCD of bc multiplied by d. What is the GCD of bd and cd. This happens to be the least positive member of the set bd x plus cd y where x and y are integers. Which is d times the least positive member of bx plus cy, where x and y are integers.

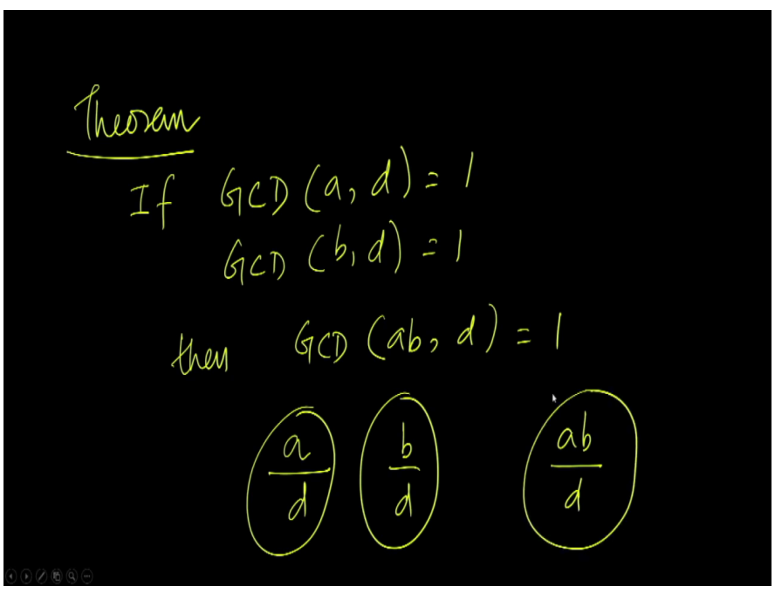
This is the case when d is a positive integer which is indeed the case here. But this is the GCD of b and c that is precisely what we wanted to show. So you can remove common factors from bd and cd, d is a common factor of bd and cd and then find the common GCD of the remnants.

(Refer Slide Time: 35:48)



Now~~The~~ related theorem is this, f~~F~~or every positive common divisor d of b and c GCD of b by d, c by d is GCD of b and c divided by d. How do we prove this? In the previous theorem you put dsd, b by dsb and c by dc. If you substitute thus in this theorem we get the new theorem as a corollary.

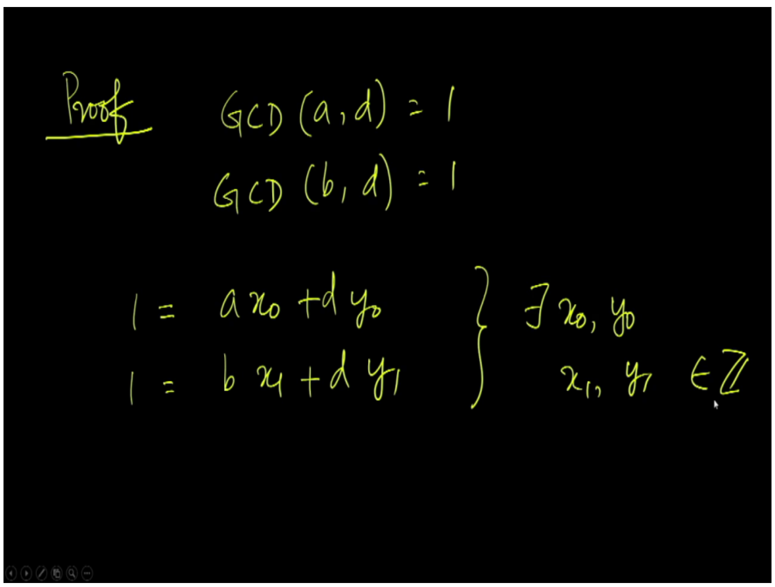
(Refer Slide Time: 36:48)



Yet another theorem if GCD of a and d is 1 and GCD of b and d is 1 then GCD of ab and d is 1. In other words, look at the fraction a by d you cannot reduce this fraction anymore a and d do not cancel. Similarly, b and d also do not cancel. B and d do not have common factors other than 1 therefore if you consider ab by d then d cannot cancel against ab.

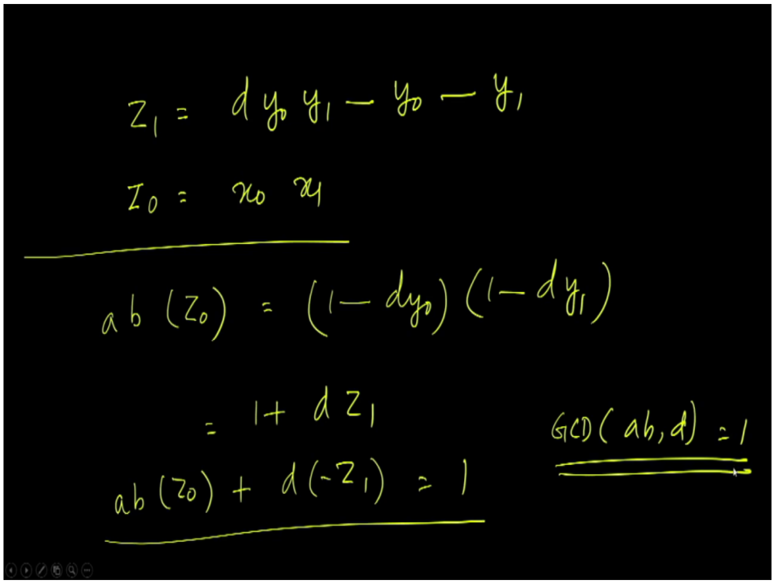
d and a~~e~~ do not have common factors d and b do not have common factors other than 1 therefore d and ab also will not have common factors other than 1. Of course intuitively clear to you but how do you prove it?

(Refer Slide Time: 37:57)



We know that GCD of a, d equal to 1 GCD of b and d is also equal to 1. Therefore we have integers x_naught~~θ~~, y_naught~~θ~~, x_1, y_1 so that 1is ax_naught~~θ~~ plus by_naught~~θ~~ and one is bx_1 plus dy_1. So there exists x_naught ~~θ~~, y_naught ~~θ~~, x_1, y_1 all integers. So that this is satisfied.

(Refer Slide Time: 38:52)



Let us define z1 as dy naught ~~θ~~ y1 minus y naught ~~θ~~ minus y 1 and z naught~~θ~~ as x naught ~~θ~~ x1. If this is the case, then we readily find that ab into z naught ~~θ~~ is 1 minus dy naught~~into~~ 1 minus dy1. Replacing x naught~~θ~~ and x1 with 1 minus dy naught~~θ~~ and 1 minus dy 1 we find that ab into z naught ~~θ~~ is this. Which is 1 plus dz 1. That is ab into z naught~~θ~~ plus d into minus z 1 equal to 1.

T~~T~~herefore if you consider the linear combinations of ab and d with integer~~-~~, the least positive member of that set is going to be 1. If 1 is present in that set, certainly 1 has to be the least among them. In other words, GCD of ab and d will have to be 1. That is it from this lecture. We will see more properties of GCD in the next class hope to see you in the next. Thank you.