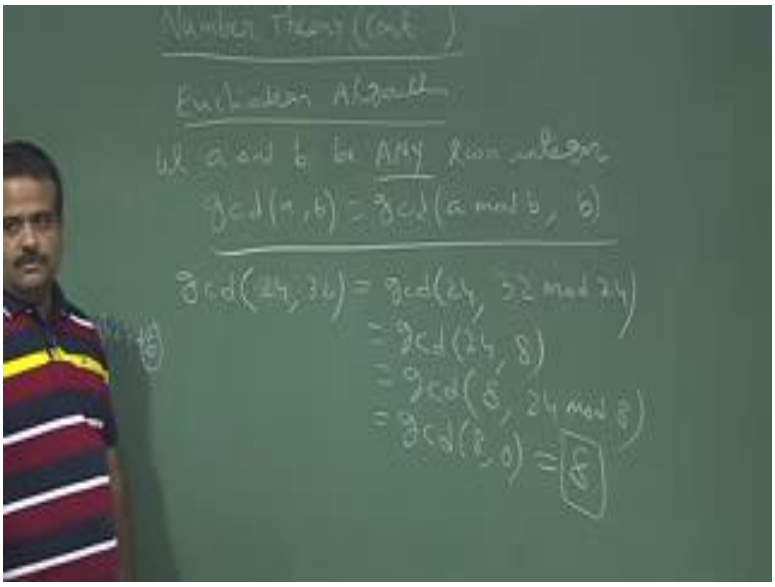
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 15
Number Theory (Contd.)

So, we talk about Eucliadean algorithm or Euclid algorithm which is basically the method to find the gcd.

(Refer Slide Time: 00:33)

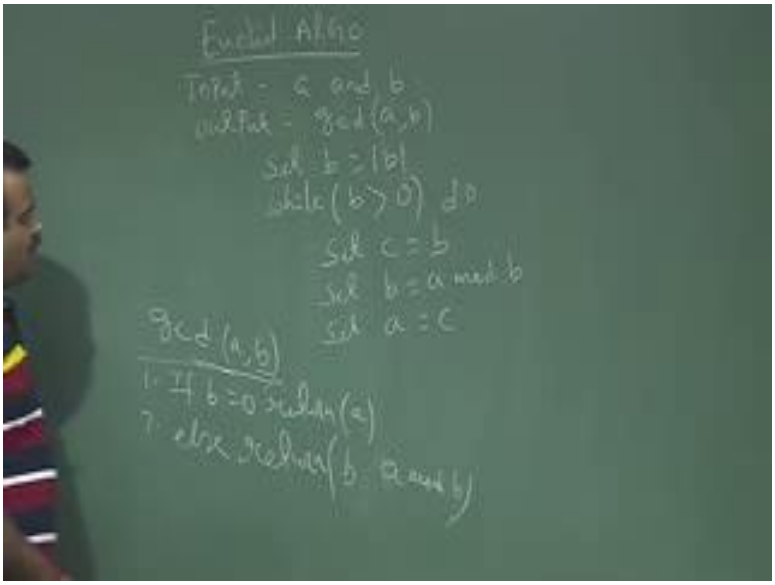


So, in the previous lecture we have seen this theorem or this result if you have two integer a, b. Let a and b be any two integer, then we have seen this result gcd of a b is equal to gcd of a mod b comma b. So, this is basically gives us the; what is called a Euclid algorithm to find the gcd. So, we will use this theorem or this result to have algorithm.

So let us take an example, suppose you have to find the gcd of say 24, 32. So, this is basically gcd of 24 then 32 mod 24 from this theorem. Now 32 mod 24 means if we divide 32 by 24, then the remainder is basically 32 mod 24. So, this is basically how much this is 8, so because 24 is basically 32 is basically 24 plus 8, so 1 into 24 plus 8, so this is q this is r; the remainder, so this is basically gcd of 24 comma 8. So, again this we can just gcd of a b is basically gcd of b a; you can just take it there and then just we can say this 8; 24 mod 8.

Now 24 mod 8 means basically 0 because 8 divides 24, so this is basically gcd of 8 comma 0, so gcd of a comma 0 is basically 8; so this is basically 8. So, 8 is the gcd of 24 and 32, so this is basically what is called Euclid algorithm. So, we will write in a formula way, so basically we will keep on calculating the remainder and until its converts to 0 then the previous one will give us the gcd of a b.

(Refer Slide Time: 03:43)



So, let us write this in a algorithm form, so this is Euclid algo. So, it has two input which is basically two integer a and b and the output will be their gcd; gcd of a b which we can store in some number. So, this is the input output and what is the code? We set this we take b to be positive. So, if b is negative we set this to be positive then while b is greater than 0, we keep on doing this set c is equal to b and we set b is equal to a mod b and we set a is equal to c, so this is the code for finding the gcd. So, basically this is the while loop and this will execute until the b is not becoming 0.

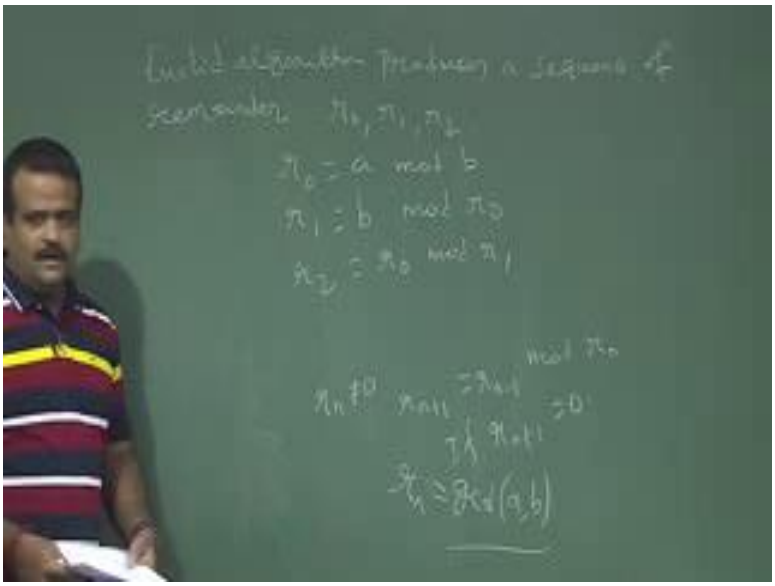
So we can think for some recursive version of this; recursive version is basically that formula a Euclid. So, Euclid a b is basically this is the recursive call of this; if b is equal to 0 then return a as a gcd, basically gcd of a b we are going to find out instead of Euclid we can just write that as gcd; the name of the algorithm, but algorithm is Euclid, else if b is greater than 0, what we do? We return this the recursive call, we return a comma or a mod b comma b; sorry a comma a mod b. So, basically we will just sorry; b comma a

mod b; this is the b part. So, this is the recursive call; anyway this is the code, so it is coming from that theorem that gcd of a b is equal to gcd of a comma a mod b comma b.

(Refer Slide Time: 06:56)

So before going to extended equity algorithm; which is basically give us this theorem, theorem means that is theorem is, so gcd of a b can be written as ax plus by; where x and y are some integer and this theorem will prove, but this theorem is basically give use what is called extended Euclidean algorithm, finding the inverse mode something modulus inverse. So what do you mean by module inverse? Further we need to know the modulus yield metric, so before that let us; so this is basically will prove this theorem, this is basically coming from the Euclid algorithm what we are doing the remainder.

(Refer Slide Time: 07:59)



So, basically in the Euclid algorithm, we produces a sequence of remainder; remainder r 0, r 1, r 2 and so on, where r 0 is equal to a mod b, r 1 is equal to b mod r 0, r 2 is equal to r 0 mod r 1 like this. So, basically we continue this until we get r n is not equal to 0, so r n plus 1 is basically r n minus 1, mod r n. Now if r n plus 1 is 0 then r n is basically gcd of a comma b. So, this is the way we find the gcd using the Euclid algorithm based on the theorem.

(Refer Slide Time: 09:46)

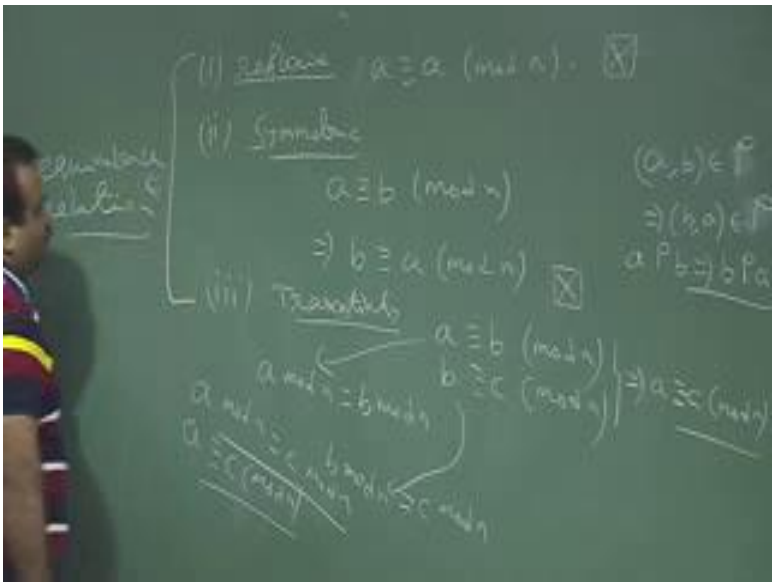
So, now we will talk about modular arithmetic or the congruence relations between two integer a, b. So, let us take an integer n; let n be an integer, it could be positive, it could be negative and let us take this, let I be the set of all possible integer, this is the integer set; set of integer, this we denote by capital I. Now if you take any integer a; now we try to divide this a by n, then we get a remainder. Now if you take another integer b, we try to divide b by; so this is basically remainder is a mod n and if you take another integer b and if you try to divide b by this integer n so that will give us the b mod n.

So, if these two are same; if a mod b is equal to b mod n then we say that a b are related, this is the relation you are defining and this relation is congruent relation and this relation is been denoted by this symbol, then we say a b are related. Now this a b belongs to r, we say a is congruent to b mod n, so that means, this is the relation basically so that means, a is related with b if you try to divide b by n the remainder will get is same.

So for example, if n is equal to say 7 or say n is equal to 8. Now if you take a is equal to 2 say a is equal to 10 and if you take b is equal to say 18 then what is a mod 8? It is basically 2; which is same as 18 mod 8. So that means, these two are related, this 10 is congruent to 18 mod 8, so that means, these 10 and 18 are related under this relation, so this relation is defined as a is congruent to b mod n.

So, now we will show that this is an equivalence relation, this relation is having some property; it is reflexive symmetric transitivity. So, what is reflexive property of a relation?

(Refer Slide Time: 13:43)



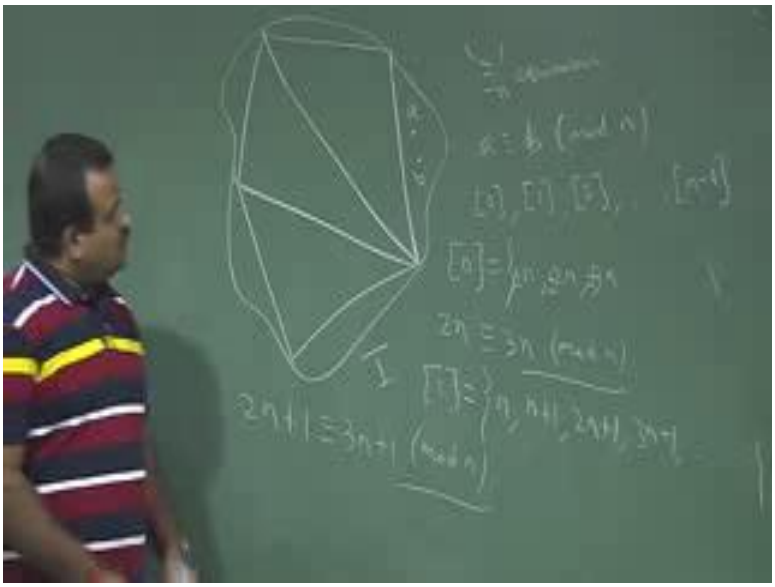
So this congruence relation is equivalence relation, so for that you need to show the 3 result, it must be reflexive; reflexive means; so a must be related with a. So a must be congruent to a mod n, this is quite obvious because if we divide a by n, the remainder is same as if we divide c by n, so this is quite obvious nothing to prove here.

Now second property is symmetric; symmetric means a relation r is called symmetric, if a b belongs to r this is a relation r, r is the real number set also. So, we denote by row relation then if this imply b a, this row; row is the relation; that means, a row b if this imply b row a; anyway r a here row is basically this symbol. So, this means symmetric means if a is congruent to b mod n then this imply b is also congruent to; this is also quite obvious nothing to prove here because basically a mod n, the remainder is same as b mod n; the both way, so this is also done.

Now the third property is transitivity; transitivity, so this relation is transitive relation; that means, if a is congruent to b mod n and b is congruent c mod n, then you have to show that a is congruent to c mod n. So, this should imply a is congruent to c mod n. If this is true for all a b c then we call this relation is transitive relation; so is this true? Yes this is true because from here we can say a mod n is basically equal to b mod n and from here we can say b mod n is equal to c mod n, so from these two, we can say a mod n is equal to c mod n; that means, a is congruent to c mod n, so this is the transivity property. So since these 3 results tell us this is an equivalence relation, you got the set of integer.

So now we know I mean this is the result from algebra, if we have equivalence relations then it will partition the sets into the equivalence classes, so that in each class, the elements are related with each other.

(Refer Slide Time: 17:43)



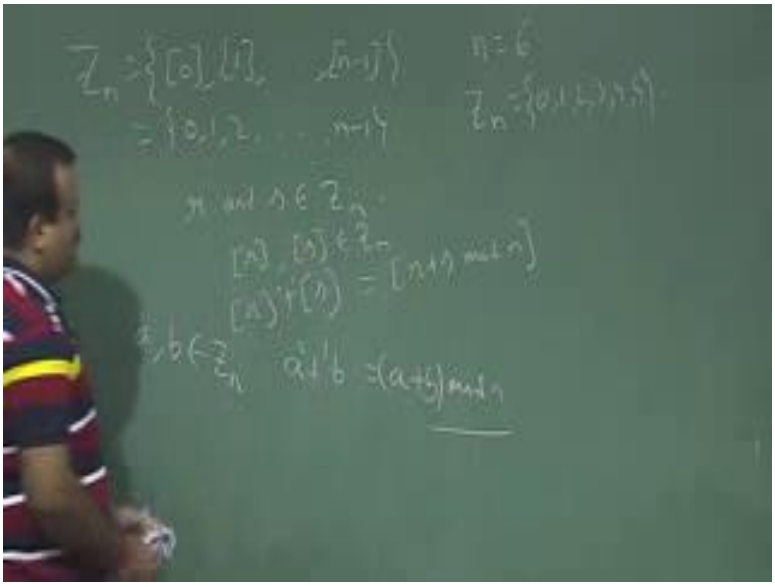
So, basically this will partition the set or set is the set of integer, so this is the integer set I and this is an equivalence relation; just now we have seen, this is an equivalence relation mod p mod n. So, this n we can just write anyway; so this is mod n, so this will partition the integer set into the equivalence classes, this joint partition dot, dot, dot this joint partition and this partition says in each of this partition, in each of this class these are called equivalence class; if a b are related under this relation, mod n then they are in the same class.

So, this class are basically denoted by 0, 1, 2 upto n minus 1, so 0 class means all the integers if it divides by n its remainder gives us 0 that means, all the integers (Refer Time: 19:09) so 0 class means this set n, 2 n, 3 n plus minus like this, so that means, 2 n is congruent to 3 n mod n, that means, they are related; so that means, 2 n is related with 3 n because 2 n; if we divide 2 n by n then the remainder is 0 and if you divide 3 n by n then also the remainder is 0. So, there in the same class and that class we denote by 0 because remainder same; remainder is 0.

So, similarly this one class the remainder is 1; so n, n plus 1, 2 n plus 1, 3 n plus 1 like this. So, these are the all integers which belongs to one class; that means, remainder is 1.

So, if you take any integer, so they are related. So, they are basically so 2 n plus 1 is congruent to 3 n plus 1 mod n because their remainder is same. So, 2 n plus 1 mod n is 1 3 n plus n mod n is 1, so remainder is 1, so that is why this class is denoted by class 1 in the remainder sense. So, that is the reason, so if we divide any integer by n; the remainder will be either 0, 1, 2 upto n minus 1. So, that is the reason we define this set upto n minus 1, so any integer will be fall one of this class, so this set is basically denoted by Z n.

(Refer Slide Time: 21:11)

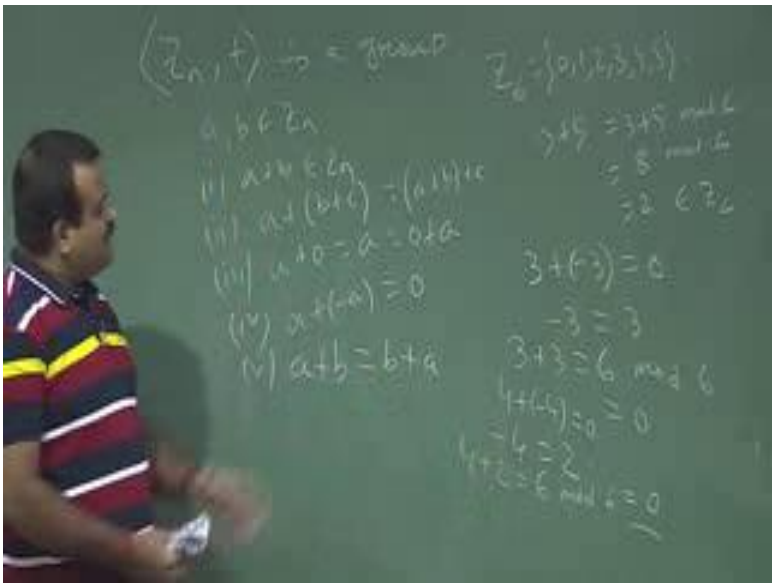


So, we denote Z n by this set 0, 1 up to this classes; equivalence classes for the simplicity we just write this 1, 2 upto n minus 1. This is denoted by Z n, so this is basically set of all equivalence classes; that means, any integer will belongs to one of this class. So, if you take any integer a; now if you take mod n it will belongs to Z n, so remainder will be either one of this 0 to n minus 1.

Now let us take an example, suppose we take say n is equal to 6 then what is Z n; Z n is basically 0 plus 1 plus 2 plus 3 plus 4 plus 5 plus so; that means, any integer if you take if you divide by 6; it will be remainder will be either one of this integer. So, it will be any one of this class. Now we will define a addition on this set this Z n, so how we can define addition on Z n, suppose we take two element from Z n; r and s let r and s from z n. So, basically we can write this by this sense for simplicity we are just writing this 0 1, 2. So, then we define class as, so we just take the r plus s mod n box. So, if you take r

plus s mod n, so it will be again in Z n, it will be from 0 to n minus 1. So, this is the class operation we defined over Z n. So, basically for simplicity, so if a b coming from Z n then we define a plus b is basically a plus b mod n so; that means, it will be one of this.

(Refer Slide Time: 23:55)



So then we can show that this will form a group, this z n along with this plus will form a group; Z n comma this is a group not only group it is a cyclic group and this is number of elements are finites, so this is an example of finite group. So, how to prove this is a group. So, for group we need to have few properties like closure property, which can be easily solved, so a plus. So, if you take two element from this; if you take two element a b from Z n then the closure property is a plus b is also Z n, the plus the way plus we have defined.

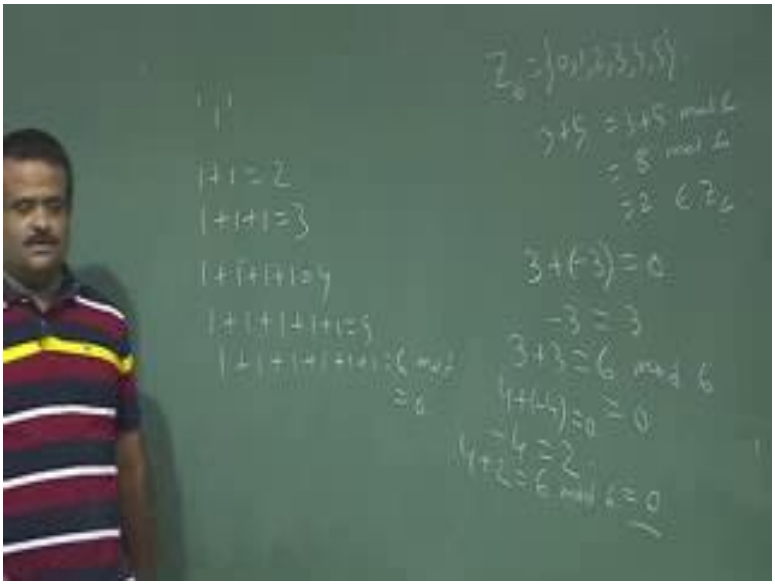
Then associativity is also true a plus b plus c is equal to a plus b plus c, we can easily check that and the existence of identity elements, so identity element is basically 0. So, a plus 0 is basically a is equal to 0 plus a, so this is the identity element existence of inverse. So, for each for a we have minus a, so minus a again is; so minus a mod n. So, a plus or minus a is equal to 0, so then this will form a group not only group it is a Abelian group; that means, a plus b is equal to b plus a, it is a Abelian group.

So, now we just take an example; suppose we take this Z 6; Z 6 is basically 1, 3, 4, 5, so the closure property is satisfied to take any two element. So, basically say 3 plus 5 how we define? This is basically 3 plus 5 mod 6, so this is 8. So, this is basically 8 mod 6; this

is basically 2 which is belongs to Z 6. So, closure property satisfied similarly we can show that associativity is also satisfy then 0 is there, so if you take any element so 3 plus 0 is 3; any element plus 0 is 0 now the inverse.

So, what is the inverse of minus 3, so minus 3 is basically so 3 plus or minus 2 should give us 0, so it is in mod 6 operation. So, minus 3 is basically plus 3 because if we take 3 plus 3 this is 6, so 6 mod 6 is basically 0. So, 3 minus is basically 6 now what is the minus 4, so 4 plus or minus 4 should give us 0. Now so basically minus 4 is 2 because so 4 plus 2 is basically 6, now 6 mod 6 is basically 0 it is giving the; so operation is the as if our real number addition, but under mod 6 operation. So, this will form a; so this 2 is (Refer Time: 27:30) as the minus 4; 2 is the additive inverse of 4. So, like this, so this is every elements has a inverse and this is a Abelian group and so this is a finite group because there are all the 6 element and this is a cyclic group, so who is the generator for this?

(Refer Slide Time: 27:54)



So, we can check that 1 is the generator because 1; if we 1 plus 1 will give us 2; 1 plus 1 plus 1 will give us 3 like this. So, 1 plus 1 plus 1 plus 1 - 4, 1 plus 1 plus 1 plus 1 plus 1 - 5 then 1 plus 1 plus - 6; then mod 6 is basically 0. So, 1 is generating all the elements, so 1 is the primitive element. So, we will check whether this is the additive sets; we will define the addition of this set. Now we will talk about the multiplicative sets whether it is

a group under multiplicative sets or not. So, that we will talk about and we will see in general in the multiplicative set Z n is not a group, so we will see that.

Thank you.