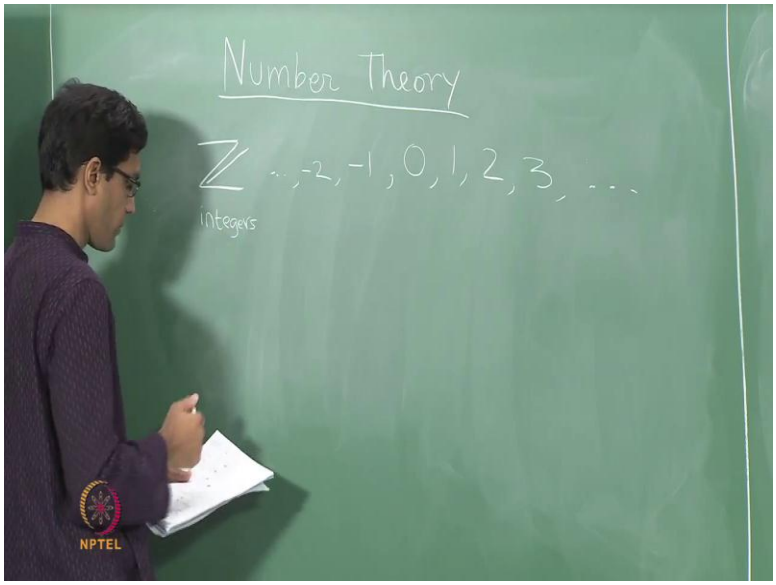
An Invitation to Mathematics
Prof. Sankaran Viswanath
Institute of Mathematical Sciences, Chennai

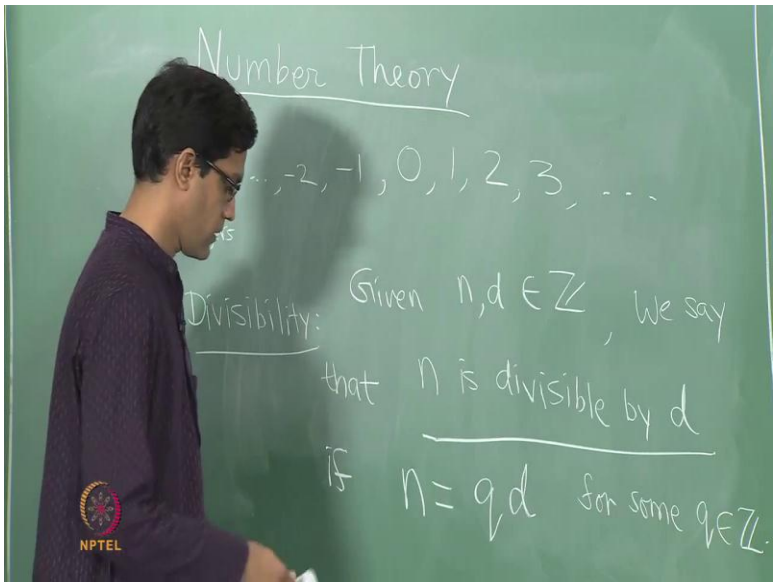
Unit
Number Theory
Lecture - 33
Divisibility, Prime numbers

(Refer Slide Time: 00:23)



Today we will talk about some elementary Number Theory. So, number theory really concerns properties of the set of integers. So, let us denote that set by a Z, so this is the set of integers. So, recall this just all numbers 0, 1, 2, 3, and so on, also the negative integers and so sometimes we will just restrict all size to the positive integers, it is not too important.

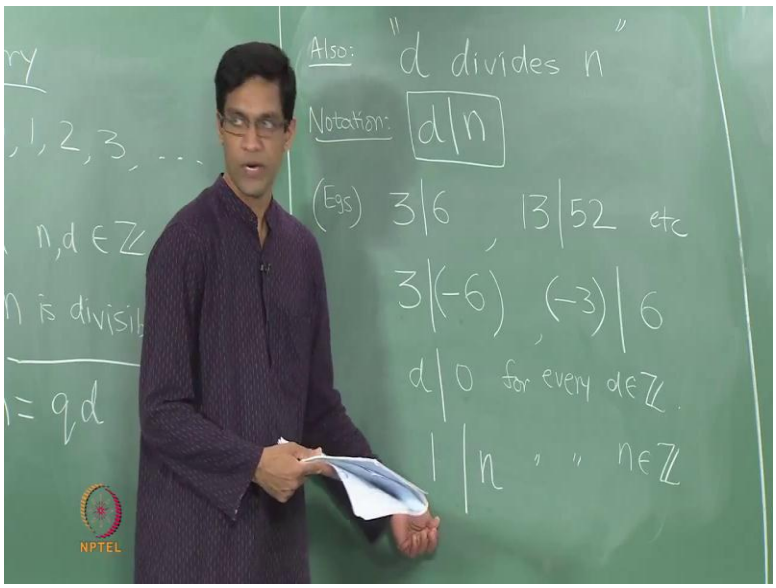
(Refer Slide Time: 00:51)



So, the key property of integers that one studies of the very first property is the notion of divisibility. So, let says define this formally, so given two integers n and d. So, given it is called n and d integers, we say that d divides n. So, we say that, there are several different equivalent ways of seen this. So, we say that, let us call it n is divisible by d, if n is sum multiple of d, if n can be written as q d for some integer q.

So, there are other ways in which we express this, we also say that, if this happens, we often say d divides n or the n is the multiple of d. So, there are all just other ways of expressing the same thing.

(Refer Slide Time: 02:05)

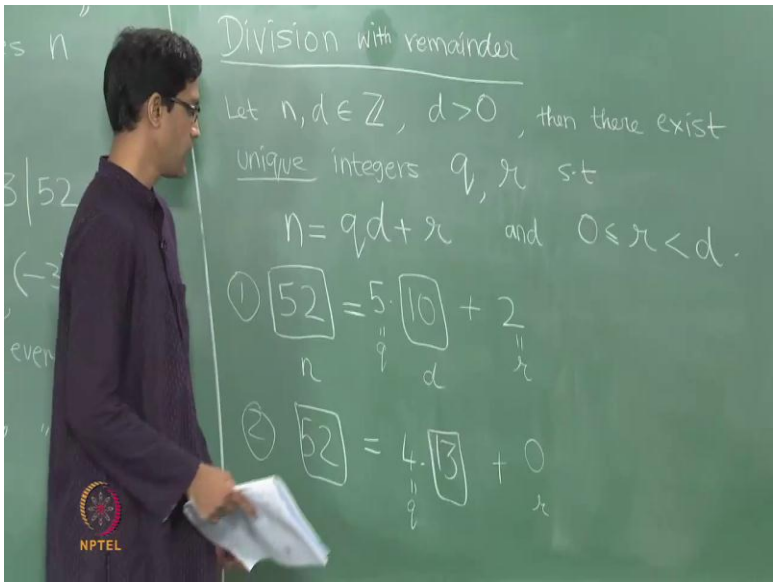


So, let me just say also another common thing, commonly used expression is the d divides n and this of course, has a notation which has very convenient in many situations. So, this is the notation, we write d divides n, divides just being this vertical line here. So, that is the notation for divisibility. So, what are examples of course, this is very familiar and easy.

So, for instance 3 divide 6, because 6 can be written as 3 times 2, 13 divides 52, because 52 is 13 times 4 and so on, etcetera, you can think of large number of such examples. It is also interesting to keep in mind on that you know these numbers could be negative here. For instance, we would say that 3 divides minus 6, similarly minus 3 also divides 6 for instance, because minus 6 can be written as 3 times minus 2. And similarly, 6 here can be written as minus 3 times a minus 2. So, these are also perfectly valid ways of they also, you know they also fit the definition of divisibility.

Now, here are some border cases which we need to keep in mind d, no matter what d you pick always divides 0. So, d divides 0 for every d in set, because 0 can always can be written as d times 0. So, 0 is a multiple of every number, similarly 1 divides every number n, so 1 divides n for every n set. So, every number is a multiple of n, similarly because n can be written as 1 times n. So, these are some sort of the as I said the border line cases to keep in mind.

(Refer Slide Time: 04:19)



Now, of course, we do not always have divisibility meaning every number does not divide every other number. So, a useful think to keep in mind is the notion of division

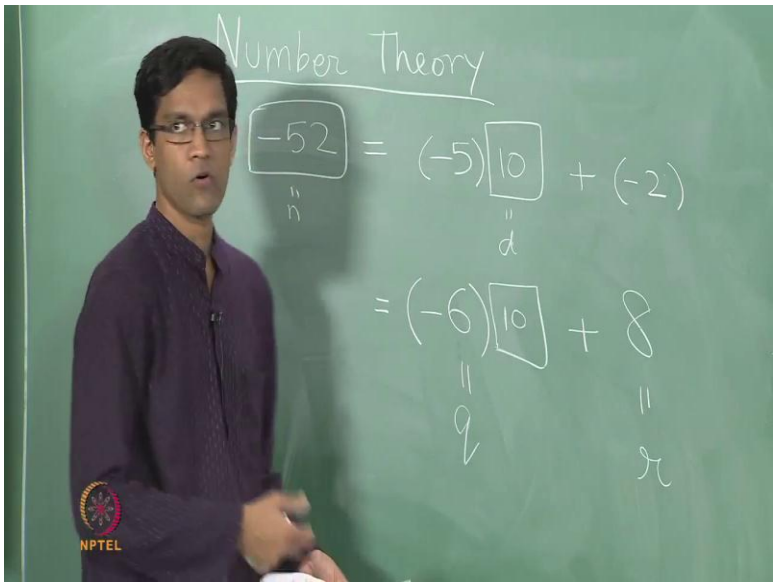
with remainder, so also called division with remainder. So, what is this mean, where let us write it out formally first, and then we will write out examples, let n and d, the integers and let us assume that, d is positive, it just a assumption for convenience. So, d is positive, then there exist unique integers is call them q and r, the quotient and the remainder.

Such that n can be written as q times d plus r and the constraint on r, the remainder is that, it is a number between 0 and d minus 1. So, r is greater than equal to 0 and less than d. So, that is the condition and recall this of course, very much resembles the notion of long division of polynomials that, we talked about of the variant. In fact, these are really one can think of them as been two instances of the same principle.

So, this again is the formal statement, but I am sure the various examples are, I am sure you have seen this in examples. So, here are a few of them. So, if I take the number 52 for instance; that is n and we try to divide it by 10; that is the d. So, here is n and here is d. So, of course, it is not exactly divisible, but you can think of the quotient as been 5. So, that accounts for a 50 and the remainder of 2. So, that is the remainder here; that is r and the quotient is a 5.

Similarly, if I take it is 252 divided by let say 13. So, I have the number 52, I try to divide it by the number 13 and in this case, it divides exactly. So, it is 4 times 13 plus no remainder. So, think of remainder now has been 0, so here the remainder is r is 0, quotient is 4. So, an alternate equivalent way of defining divisibility, so you would say the d divides n, if and only if the remainder is 0. So, that is an equivalent way of stating the same thing and here, again negative numbers need to be treated a little more carefully.

(Refer Slide Time: 07:35)



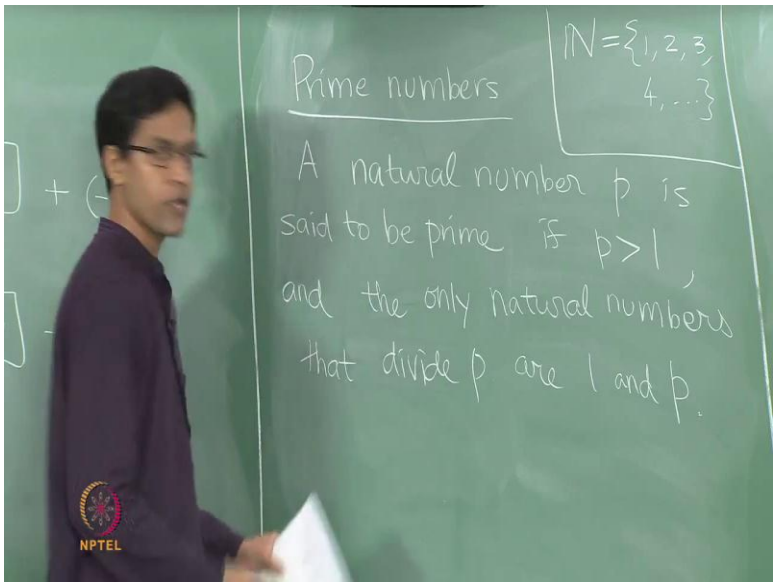
So, if for instance you try to divide the number minus 52, so if that is your number n. So, now, for convenience way we have already assume that d is positive. So, let me say, I try to divide it by the number is 10; that is my d. So, of course, you could still think of it as a sort of being like forgetting the minus sign for now, it is like dividing 52 by 10. So, if you think of say the quotient as being minus 5 in this case.

So, there is a minus 5 and if you see, what is left, there is a minus 2 left. So, minus 52 is minus 5 times 10 plus a minus 2. So, you could be tempted to think of the quotient as minus 5 and the remainder as minus 2. But, that is not okay, because we have at least in the way we stated it, we have required the remainder to be a number between 0 and d minus 1. So, the remainder has to be a number between 0 and 9, minus 2 is not allowed as impossibility.

So, this is not quiet going to serve our purpose, instead what we need to do is the following, we need to do something to get the remainder to be a positive number. So, we increase all well rather decrease the quotient, you change the quotient by 1, so as to obtain a positive remainder. So, here is an alternate way of writing the same thing, you can think of it as minus 6 times 10, so it is minus 60 plus an 8.

That still a minus 52 and now, this is really the expression you want. So, you should think of the quotient as been minus 6 and the remainder as being 8. So, the remainder now of course, satisfies the constraint that we wanted to satisfy. So, that is about divisibility and division with remainder.

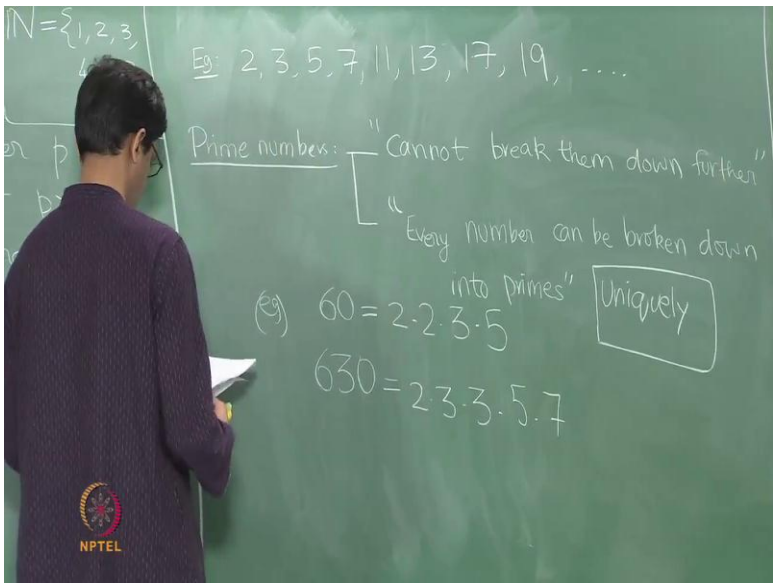
(Refer Slide Time: 09:26)



So, very important classes of numbers are what are called the prime numbers. So, what are the prime numbers well an integer greater than 1, so this is what you call a natural number. So, before we talk about prime numbers let us recall the set of natural numbers n is just well all the positive integers. So, this just 1, 2, 3, 4 and so on is what is called the set of natural numbers. So, a prime number is a natural number.

So, if the natural number p is said to be prime is the following, if firstly, p has to be at least 2. So, p is strictly greater than 1 and further, the only natural numbers that divide p are 1 and p and the only natural numbers. So, it has no other divisors other than 1 and itself, so again I assume this must be familiar.

(Refer Slide Time: 10:57)



So, what are the list of prime numbers? Well, at least we can write out the first few. So, we have 2, 3, 5, 7, 11, 13, 17, 19; that is a full list of prime numbers until 20, but then the list really goes on. So, it is well there are in fact, infinitely many prime numbers, we will come back to that in a minute. So, here have sort of two different ways of thinking about prime numbers and the one hand, they do not really have devisors other than 1 and itself.

In other words, you cannot a really break them down; you cannot break them down into smaller numbers. So, if you think of. So, here is picture of prime numbers; that it is useful to keep in mind, if they did have factors. So, any number which has a devisor can be written as in our product of smaller numbers, but since prime numbers do not have devisor rather than 1 and itself, you cannot really break them down any further write them as a product of smaller numbers.

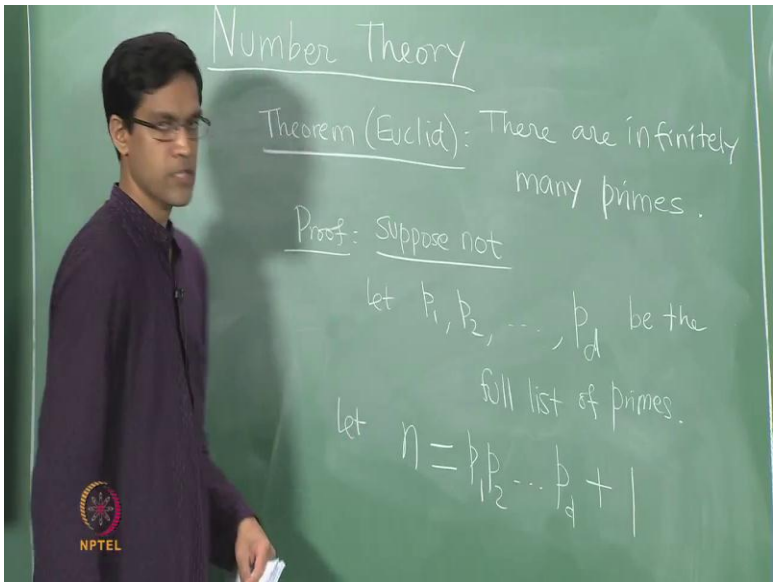
Search one aspect of prime numbers, but the sort of also a complementary aspect which is that every number can always be written as a product of primes. So, this is an other property if you wish previous of times that every number can be broken down into primes, every natural number can be broken down into product of primes. So, examples of the latter principle, if you have the number 60, so this is 2 into 2 into 3 into 5 is nearly 630 for instance would be 2 times 3 times 3, 5 times 7 and so on.

So, this is often, what we can call the prime factorization at an arbitrary number can all way is be written as a product of primes and further this expression really is unique. So, that is an other important property of prime factorization. So, every number can be broken down into primes, but in an essentially unique fashion. So, further uniquely is another important and interesting feature of this.

So, for instance the number 630, if you wanted to write it down as a product of primes, the only sort of different looking expressions, you can produce or things in which the primes are written in different in orders. So, you could probably 1 to write 630 as may be 7 times 5 times 3 times 3 times 2, may be in the descending order of primes or in some other arbitrary order.

But, other than that, there is a much you can do you cannot find then other expression for 630, which say does not involve these prime say for it is an something which contains 13 as one of it is factors. So, such things are not possible, it is essentially unique, these expressions. So, up to reordering, so let us come back to this property that I just mention that it is an infinite list.

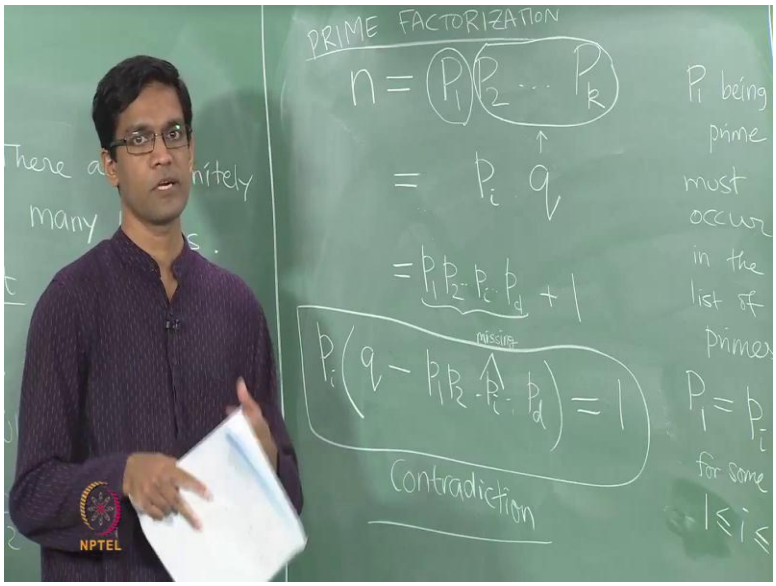
(Refer Slide Time: 14:45)



So, the list of prime numbers is infinite is very famous statement, which goes back all the way to Euclid. So, theorem due to Euclid says that, there are infinitely many primes and the proof itself is rather interesting in and uniting proceeds through. So, let me just quickly sketch the proof, Euclid's first proof of this fact that there are infinitely many primes. So, it says a fine suppose not, suppose not in other words, there are only finitely many points. So, let us give the name. So, let p 1, p 2, p d, let say, be the full list of primes.

So, you imagine for the moment that the list is finite and that is the full list and now, what you do is the following, you create number. So, you form the following number, let n denote the product of all these primes p 1, p 2, p d, but it one added to it. So, you look at the number p 1, p 2, p d plus 1. So, that some natural number which is well bigger than all the primes, because it is in fact, there it is bigger even than the product.

(Refer Slide Time: 16:38)



And now, we do the following, n of course, is some natural number and sort of by using the principle that every natural number has a prime factorization. So, let us write n, so you was there let us break n down into prime. So, it was the prime factorization of n. So, we write n as let say capital P 1, capital P 2, P let us call it capital P k, where all the Pi's are all primes.

So, they could of course, be you know there could be reputations, when you write down prime factorizations as we just saw, then we talk about 630 and 60 and so on, some of these could be could be repeated. So, the does not quit matter for us. So, let us write n in the fashion and let us do the following, let us think of this as well two parts the first p 1, let us isolate P 1 and let us think of remaining as being another number P 2, P 3 to P k, let us call that as q.

So, this part as q, the second number and P 1, remember is the very first factor in this expression is a prime. So, P 1 after all is a prime, it occurs in the prime factorization. So, P 1 being prime must occur in the list of primes, must occur in the full list of primes that we wrote out, must occur in the list of primes. In other words, it is some P i, in other words P 1 has to be somewhere in the list let us call it P i for some i between 1 and d, because some i d. So, let us call P 1 as the prime P i.

So, here is what we conclude that this number n is in fact of the form p I times q, in other words is a multiple of that prime P i. now, the other hand n, we move what n was, it is P, 1, P 2, P d. So, remember in this list P i also appears. So, this is P i will occurs

somewhere in the middle plus of 1. So, here are two different expressions for the same number n, but there mutually contradictive. So, these two expressions cannot both the true at the same time and why is that, well to see it, what will do is, we will move this all these terms over the left hand side right.

So, this equality provides us the following equivalent reformulation P i times. So, I keep the q as it is and I will subtract, I will move this term over to the left. So, I am a pulling out a P i common. So, this is now p 1, p 2, p d, but in which p i is missing. So, P i has out, so this P i term here and put on the hat on top to say that you should think of that term as been missing from this expression. So, it is p i times q minus the product of the other pi's is the number 1.

So, that is the conclusion we might form, but observe that is clearly not possible, because the left hand side is a multiple of the prime P i it is P i times some other, where is a right hand side is a number 1 and a prime of course, is a number which is 2 or more. So, there is no way that a number that is bigger than two can multiply something out to give you the number 1.

So, this finite expression here is a contradiction and that in fact cruse that our initial assumption most on that the list of primes is finite. So, that is really Euclid's rather ingenious proof that the number of primes is in fact, fine is infinite and since, then of course, that have been several different proofs using several different. So, next time will talk about little bit more that one can do with division with remainder and primes and so on.