

A Basic Course in Number Theory
Professor. Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture No. 02
Divisibility and Primes

Welcome back. In the last lecture, we ended with the Divisibility relation. So, let us quickly go through that, let us just repeat. If you have two natural numbers, a and b and if you are able to write a as b into c , for yet another natural number, then we say that b divides a . And we will write it in the short form, as b vertical bar a . However, while reading that short form, we will still read it as b divides a . And in the last lecture, we actually saw a quick proof, that 1 divides a for every natural number.

(Refer Slide Time: 1:07)

Now, we turn to the reverse operation of multiplication.

For $a, b \in \mathbb{N}$ if $a = bc$ for some $c \in \mathbb{N}$ then we say that b divides a and write it as $b \mid a$.

It is clear that $1 \mid a$ for every $a \in \mathbb{N}$.

It is also clear that $a \mid a$ for every $a \in \mathbb{N}$.



As well as a divides a for every natural number. So, every natural number comes equipped with two God given divisors. There is 1 and there is the natural number itself. So, let us just go to the next slide.

(Refer Slide Time: 1:30)

Just like the subtraction, this also gives an order relation, called the relation of *divisibility*.

However, we do not have the trichotomy here.

We again have some basic properties of the divisibility.



Where we see that like the subtraction, divisibility also gives you an order. You may wonder that I have been talking about order relation. So, is there a definition of the order relation? Indeed, there is a definition, of in fact not just of an order relation, there is a definition of a relation. What do you mean by two elements in a set being related? Once you see that definition, then the order relation should come with some more properties. It should be a relation with some more properties.

So, I will just invite you to go and read somewhere, may be in some basic book or you may want to search on the internet. Or may be Wikipedia will help you in that. But those definitions are not important for us, at the moment. What we are going to do is concentrate on this very specific order relation; the relation of divisibility.

And as we observed in the last lecture also, we do not have a Trichotomy here. You can have two natural numbers, say 2 and 7. Now, 2 does not divide 7, 7 does not divide 2. And off-course 2 and 7 are not the same. So, given any two natural numbers, we cannot say that $a = b$ or a divides b or b divides a . However, when the situation is not normal, that is when things get interesting.

So, this is what will give us our basic definition, the most fundamental definition that offer prime integer. And then, primes come equipped with many fantastic properties. That we, as we will see later. So, before going to do that, let us again warm up ourselves with some very basic properties of divisibility. I am going to list them on the next page and just like the last lecture, we will try to prove them one-by-one.

(Refer Slide Time: 3:47)

If $a \mid b$ and $b \mid c$ then $a \mid c$.

If $a \mid b$ and $c \in \mathbb{N}$ then $ac \mid bc$.

If $a \mid b$ then $a \leq b$.

These are the 3 properties. What does the first property say? It says that, if you have a dividing b and b dividing c , then a divides c . This is encoded by saying that the order relation is transitive. If a divides b and b divides some another natural number c , then a should divide c . What does the next property say? It says that, if a divides b and I multiply both sides by a natural number c , then the division relation is preserved. The multiplication will preserve the division relation.

You may ask what will happen if I add a number. If a divides b and you add an integer, is it true that $a + c$ divides $b + c$. If I have not written that property, may be there is a possibility that this property does not hold. Why do not you think about this, for a while? After this lecture is complete, you may think about this. Does it hold, that a divides b and I add any integer c , any natural number c to a and b and yet, we have that $a + c$ divides $b + c$. Think about this.

What is the third property? Third property tries to combine the divisibility relation with the earlier relation. This is a thing which is omnipresent in mathematics. You will see that everywhere. Whenever we are developing a theory, we will introduce some concepts. And each time, we introduce a new concept, we will try to relate it with the earlier concepts. That is what makes mathematics more interesting. You will not see us, introducing one concept after another and not seeing the properties of what happens with respect to one concept and the other concept. This is very nice about mathematics.

So, the third property says that whenever I have a dividing a b, remember we are within the set of natural numbers. Whenever you have a natural number a dividing a natural number b, then it should happen, that a is less than or equal to b. So, it tells you, when you turn this statement around, it will tell you that if you have a number a which is bigger than some number b, then this bigger number can never divide the smaller number.

The statement I have just said is equivalent to the statement we have seen here. So, there are these 3 properties. We will try to go over them one-by-one and prove them one-by-one. So, here comes the very first property.

(Refer Slide Time: 7:05)

If $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof: We have $b = ad_1$ and $c = bd_2$ for some $d_1, d_2 \in \mathbb{N}$.

Then $c = bd_2 = (ad_1)d_2 = a(d_1d_2)$ where $d_1d_2 \in \mathbb{N}$.

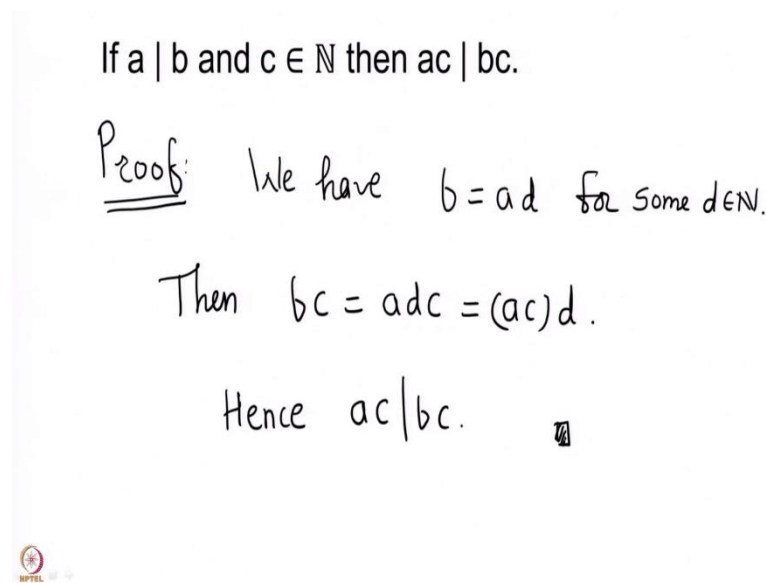
Hence $a \mid c$. \square

If a divides b and b divides c, then a divides c. Like our last lecture, I am going to give you a minute to think about this proof. And then after that I will give my own proof. Well, my meaning the one that is there in most of the books. If you have any other proof, than the one that I am giving, please write to me and let me know your proof. So, I have given you your minute and now let me give you my proof. So, here goes. We want to prove that the divisibility relation is transitive.

Proof. We have b equal to a d1. It is given that a divides b. So, b has to be of the form, a into some natural number d1 and c equal to b into d2, for some d1 d2 in N. This is what we must have. If you have a divides b and b divides c, then we should have that b is a into a natural number, c is b into possibly another natural number. We do not care. So, we have b is a d1 and c is b d2.

Then, in this equation, I will take the value of the b that we have got here. This is a into d_1 into d_2 , which is same as a into $d_1 d_2$. And note that $d_1 d_2$ being product of two natural numbers, is a natural number itself. So, we have written c as a into a natural number. And hence, a divides c . So, we have proved that when a divides b and b divides c , then a must divide c . Let us go to the next property.

(Refer Slide Time: 11:16)



If $a \mid b$ and $c \in \mathbb{N}$ then $ac \mid bc$.

Proof: We have $b = ad$ for some $d \in \mathbb{N}$.

Then $bc = adc = (ac)d$.

Hence $ac \mid bc$. \square

If a divides b and c is the natural number, then ac divides bc . So, multiplication by a natural number respects the divisibility relation. Once again, as we have our deal, I will give you a minute to think about this proof. Quite likely, you will get the proof that I have in mind, which is a very good thing. That will tell us that we are thinking in the same direction. Or even more interestingly, you may have a different proof. And I would like to know that different proof. So, your minute starts now.

So, your minute is up. And let me now attempt to give you a proof. We are given that a divides b . So, we have b equal to a into d , for some d in \mathbb{N} . a divides b . So, b is a into a natural number. Now, to this equation, we can multiply by c . So, we have bc equal to ad into c , which is same as ac into d . So, therefore we have written bc which is a natural number, as ac into a third natural number, which clearly says that ac divides bc .

Whenever a natural number a divides another natural number b and to both sides, you be fair to both the natural numbers which are there on either side of the vertical bar. You multiply by a natural number to both these natural numbers. Then the divisibility relation is respected. We

now go to the third property, which is a very important property and we will use it quite often.

(Refer Slide Time: 14:43)

If $a \mid b$ then $a \leq b$.

Proof: Since $a \mid b$, we have $b = ad$
for some $d \in \mathbb{N}$.

If $d = 1$ then $b = a \cdot 1 = a$.

If $d > 1$ then $b = \underbrace{a + a + a + \dots + a}_{d\text{-times}}$.

If $a \mid b$ then $a \leq b$.

$b = ad$. If $d = 1$ then $a = b$.

If $d > 1$, observe that $a + a > a$.

Then $a + a + a > a + a > a$

This way $da > a$ if $d > 1$.

Hence $b > a$. \square

This says that, if you have a natural number a dividing a natural number b , then with respect to the earlier order that we have defined less than, it should be less than or equal to b . This strange symbol that you may see here, means that either a is less than b or a is equal to b . Once again, I will give you a minute to think about this proof. And after your minute is done, I will state my proof.

Very well, your minute is up. So, let us see the proof. This proof is quite interesting. How would we prove this? So, let us see. So, since a divides b , we have b equal to ad , for some natural number d . So, we have b as a product of a and a natural number d . Now this natural

number d that you have got, could either be equal to the number 1. Or it could be bigger than 1. So, if d is 1, then b is a into 1, which is a . This is one case, that b is equal to a .

Now, if I take d bigger than 1, then b is a plus a plus a plus a . How many times do we get this? This is d times. We have that b is a into d . So, b is a plus a plus a , d times. What we want to prove is that, if you have a dividing b , then a is less than or equal to b . This is what we want to prove. And we have already seen, that when d so, b is a into d , if d is 1, then a equal to b . If d is bigger than 1, observe that first of all, a plus a is bigger than a . I 20:47f I have a natural number a and I add the natural number to itself, I get something which is bigger than that.

And then, inductively I get a , I am adding a to both the sides. And we know that the addition respects the bigger than sign or the less than sign. But what is also true, is that it preserves the transitivity is preserved. That means if you have a natural number, which is bigger than second natural number, which is bigger than the third natural number, then we see that the difference of the first one and the third one is a natural number. And therefore, we have transitivity.

This way, d into a , I will just write it as d into a , which is a plus a plus a , d times, is going to be bigger than a . And remember our b was d into a , or a into d . This completes our proof. Once again, there were 2 possibilities. Either you could write b as a into 1, in which case you get equality. Or you could write b as a into d , which is bigger than 1. And then we get that b is strictly bigger than a . It is not equal to a , but it is strictly bigger than a .

(Refer Slide Time: 21:17)

We have thus proved:

If $a \mid b$ and $b \mid c$ then $a \mid c$.

If $a \mid b$ and $c \in \mathbb{N}$ then $ac \mid bc$.

If $a \mid b$ then $a \leq b$.




So, let us just repeat what we have proved until now. We have proved that, when a divides b and b divides c , then a divides c . This says that the divisibility relation is transitive. Further, if you have a dividing b and you multiply both sides by a natural number c , then we will have that ac divides bc . And finally, the most important property is, when a divides b , then a has to be less than or equal to b . These 3 are very important. There might be some extensions of these properties for the set of integer, for the set z .

In fact, you could go all the way up to the set of real numbers, complex numbers or if you know some advanced mathematics, the number of the quaternions, what are also known as Hamiltonians, all the way up to wherever you can go. But, at the moment what we have is the following. If you have two natural numbers, then we say that one natural number divides the another natural number. If there is a third natural number, such that the first one can be, the second one can be written as the first into the third.

Now brace yourself. We are coming to the most important definition, in the basic theory of numbers, which is as follows.

(Refer Slide Time: 22:47)

A prime is a $p \in \mathbb{N}$ which has exactly two divisors.	
Is 1 a prime?	No!
Is 2 a prime?	Yes!
Is 3 a prime?	Yes!



This is the definition of a prime. Really, the English word prime has very good meaning. It is you know something which is in the best of its situations. And prime number is really the best thing, that you can have in the number theory. So, what is a prime? We have observed that whenever you take any natural number a , there are two God given divisors. 1 divides it and the number a divides it.

If your natural number happens to be just the number 1, then there is only one God given divisor, because both these divisors happen to be the same. In any case, any number bigger than 1 is going to have two divisors, which are given to us always. And we say that a natural number is a prime, if there are no further divisors. So, we say that our natural number p is a prime, if there are exactly 2 divisors, not 1, not 3 and not further, no 4, 5, 6, 7. So, once we have made a definition, a natural thing would be to see some properties, maybe prove some results. But before that, we should see examples.

Let us go over our numbers. We are working with natural numbers. So, we will start from 1 and go onwards. Let us start from 1, go onwards and see if we get a prime. Is 1 a prime? What would you think? How many divisors are there for 1? We saw just now, that for 1 there are no two divisors. Because for any integer, for any natural number a , there are two divisors, 1 and a . But 1 unfortunately has the property, that both these divisors become the same. So, the number of divisors of 1 in \mathbb{N} is 1.

1 is the only unfortunate number in this way. So, 1 cannot be a prime. 1 is not a prime. What about the next number? Is 2 a prime? How many divisors are there for 2? 1 is a divisor of 2, 2 is a divisor of 2. Is 3 a divisor of 2? What did we learn in the last property of divisibility? If 3 divided 2, then 3 would have to be less than or equal to 2. But 3 minus 2, which is a natural number 1, tells us that 3 is bigger than 2. Similarly, 4, 5, 6, 7, all numbers are bigger than 2. So, if you are looking for divisors of 2, you should go no further. This is something you should take a note of.

If you are looking for divisors of a number a , you need to go only up to a . You do not have to consider the natural numbers from a plus on onwards. So, it has become a finite problem. To find the divisors of a , you have to go no further than a . In fact, you can make this problem simpler. You need to go only up to the square root of a . But that will come when we deal with really large numbers. So, is 2 a prime? We have counted the number of divisors of 2. 1 is a divisor and 2 is a divisor. And there are no further. So, 2 is in deed a prime. What about 3? Is 3 a prime?

1 divides 3, 3 divides 3. We need to look no further. So, 4 onwards are the natural numbers that we will ignore. There is another number sitting between 1 and 3, which is 2. Does 2 divide 3? How do the multiples of 2 look like? 2 into 1 is 2, 2 into 2 is 4, 2 into 3 is 6. So, the higher natural number, you multiply it by 2, you get bigger and bigger numbers. So, 2 into a

natural number is not equal to 3. Therefore, 2 does not divide 3. So, the divisors of 3 are 1 and 3, nothing further. So, 3 is also a prime.

What about 4? Can you think about 4 being a prime? We will need to look at the divisors of 4. 1 is a divisor, 4 is a divisor. But we have counted the divisors of, the multiples of 2 just now. And we saw that 2 into 2 is 4. So, 4 has 3 divisors, 1, 2 and 4 itself. So, 4 is not a prime. So, we got 1 is not a prime, 2 is a prime, 3 is a prime, 4 is not a prime. You may continue this way.

(Refer Slide Time: 28:52)

Can we list all primes up to 100?

Yes, there are 25 of them.

2, 3, 5, 7, 11,
13, 17, 19, 23, 29,
31, 37, 41, 43, 47,
53, 59, 61, 67, 71,
73, 79, 83, 89, 97.

Can we list all primes up to 100? Well, the way we have done so far, this should be a work, which is possible. So, yes. There are 25 of them. Can we list them all? 2, 3, 5, 7, 11. This is the next bunch, this is the next bunch, this is the next and this is the last bunch. So, these are exactly the primes up to 100. You know you would see a teacher in your class, giving you a problem. And if you solve it very easily, the teacher will give you a slightly harder problem. I am going to do the same.

(Refer Slide Time: 29:41)

Can we list all primes up to 1000?

Yes, there are 168 of them.

Can we list all primes up to 10000?

Yes, there are 1229 of them.

Can we just go on and on?
can!

Yes, we



Can we list all primes up to 1000? The answer is yes. There are 168 of them. The number of primes up to 100 was 25. The number of primes up to 1000, we have multiplied 100 by 10. So, we got 1000. The number 25 did not get multiplied by 10. It got multiplied to somewhere between 6 and 7. So, we got 168. I am not going to write all those primes here. I will give that to you as an interesting homework. Do not send that list to me. Keep it with you.

Can we list all primes up to 10000? Yes, we can. I can tell you the number. There are 1229 of them. Once again, we went from 1000 to 10000, by multiplying by 10. And the number 168 did not get multiplied by 10. It got multiplied by a number, which is slightly smaller than 8. So, after 10000, you may ask what about 100000, what about 1 lakh, or can we just go on and on.

Can we just go on and on? And the answer is yes, we can. What this means to say is that, there are infinitely many primes out there. There are plenty of primes. The set of primes is not finite. With this punch line, we will stop here in this lecture. And we will state the result of the infinitude of primes in the next lecture and also see a proof. Thank you.