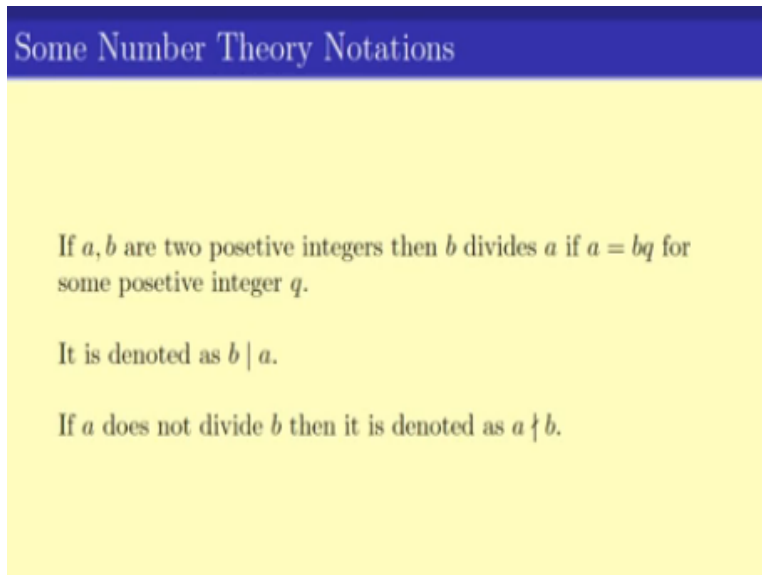


**Discrete Mathematics**  
**Prof. Sourav Chakraborty**  
**Department of Mathematics**  
**Indian Institute of Technology- Madras**

**Lecture - 05**  
**Elementary Number Theory**

Welcome to the fifth video lecture in discrete mathematics, this will be the last video in the introductory week. So in this video, we will be introducing you to the notion of elementary number theory and its notations will be using number theory for various problems in the following lectures and that is the reason, this introduction to number theory is very essential. Now, number theory is something that all of us have used or seen in our high school or colleges.

**(Refer Slide Time: 00:41)**



Some Number Theory Notations

If  $a, b$  are two positive integers then  $b$  divides  $a$  if  $a = bq$  for some positive integer  $q$ .

It is denoted as  $b \mid a$ .

If  $a$  does not divide  $b$  then it is denoted as  $a \nmid b$ .

We have seen integers and we have seen divisions. So let us start with this simplest operation that we have learned namely if you are given 2 positive integers A and B then we say B divides A if A can be written as B times Q where Q is some positive integer. The notation that we used to denote it is this notation which means B divides A. Now, if A does not divide B, it is denoted using this notation A with a vertical line and strikeout B. So it reads as A does not divide B.

**(Refer Slide Time: 01:34)**

## Exercise

Prove that the relation " $a$  divides  $b$ " is a reflexive and Transitive relation in the set of positive integers.

Also show that the relation is no symmetric.

Now here is a small exercise namely this relation A divides B prove that it is reflexive and transitive, also show that this relation is not symmetric. This will also help you understand the notion of relations that we have described in previous video bit.

**(Refer Slide Time: 02:17)**

## Number Theory Observations: 1

If  $a, b, p$  are three positive integers such that  $a$  and  $b$  are divisible by  $p$  then prove that  $p$  divides  $a + b$ .

Now in this video, I have made some few observations, these are pretty standard observations in number theory. Thus, for completeness, I have written down explicitly and we will be going over it one by one. Here is the first one, if A, B and P are 3 positive integers such that P divides both A and B that is P divides A and P divides B, then we can show that P divides  $A + B$ , so let us see why is this true?

**(Refer Slide Time: 03:13)**

## Number Theory Observations: 1

If  $a, b, p$  are three positive integers such that  $a$  and  $b$  are divisible by  $p$  then prove that  $p$  divides  $a + b$ .

**Proof of the observation:**

- $p$  divides  $a$  implies  $a = pr$ , for some positive integer  $r$ .
- Similarly  $p$  divides  $b$  implies  $b = ps$ , for some positive integer  $s$ .
- So  $a + b = pr + ps = p(r + s)$ .
- Since  $r + s$  is a positive integer so  $p$  divides  $a + b$ .

Note that all these things should follow from the basic definition of division. So this to start since  $P$  divides  $A$  this implies that  $A$  can be written as  $P$  times  $R$  for some positive integer  $R$ , similarly since  $P$  divides  $B$ ,  $B$  is equals to  $P$  times  $S$  for some positive integer  $S$ . So what is  $A + B$  so  $A + B$  is  $P$  times  $R + P$  times  $S$  which is of course  $P$  times  $R + S$ . Now, since  $R$  is an positive integer and  $S$  is a positive integer this means that  $R + S$  is also an positive integer.

In other words,  $P$  divides  $A + S$  sorry  $P$  divides  $A + B$ , because  $A + B$  is written as  $P$  times  $R + S$  where  $R + S$  is a positive integer, it is a very easy observation that follows from the basic definition of division.

**(Refer Slide Time: 04:26)**

## What is a remainder?

Let  $a, d$  be two positive integers.

If  $a$  can be written as  $dq + r$  where  $q$  and  $r$  are positive integers and  $r < d$  then  $r$  is the remainder when  $a$  is divided by  $d$ .

In other words, if  $d$  divided  $a - r$  when  $r < d$  then  $r$  is the remainder when  $a$  is divisible by  $d$

Now, let us move on to the next thing, this is again something that we must have seen in our elementary school or middle school that is the notion of remainder. So if  $A$  and  $D$  are 2 positive integers then  $A$  can be written as  $D$  times  $Q + R$  where  $Q$  is an integer, positive integer and  $D$  is also positive integer, but  $R$  is strictly less than  $D$ . Note that there is a unique way of writing  $A$  as  $DQ + R$  where  $R$  is strictly less than  $T$  and  $R$  is a positive integer.

When we can write it this way we say,  $R$  is the remainder when  $A$  is divisible is divided by  $P$ , just a quick comment if  $R$  is equals to 0 that means if the remainder is 0 in that case what happens? In that case  $A$  is equals to  $D$  times  $Q$  where  $Q$  is a positive integer or in other words,  $A$  is divisible by  $D$ . Thus, if  $D$  divides  $A$  then the remainder is 0. Else we get a remainder that is less than  $D$ .

Also one more observation to do is that since  $A$  can be written as  $DQ + R$  that means  $A - R$  is  $DQ$  which also means that  $D$  divides  $A - R$ . Here is another way of writing, the remainder so if  $D$  divides  $A - R$  where  $R$  is a positive number, positive integer less than  $D$  then,  $D$  is the remainder when  $A$  is divided by  $D$ .

**(Refer Slide Time: 07:00)**

Modulus

If  $r$  is the remainder when  $a$  is divided by  $d$  it is represented as

$$a \equiv r(\text{mod } d)$$

In other words  $a \equiv r(\text{mod } d)$  should be read as

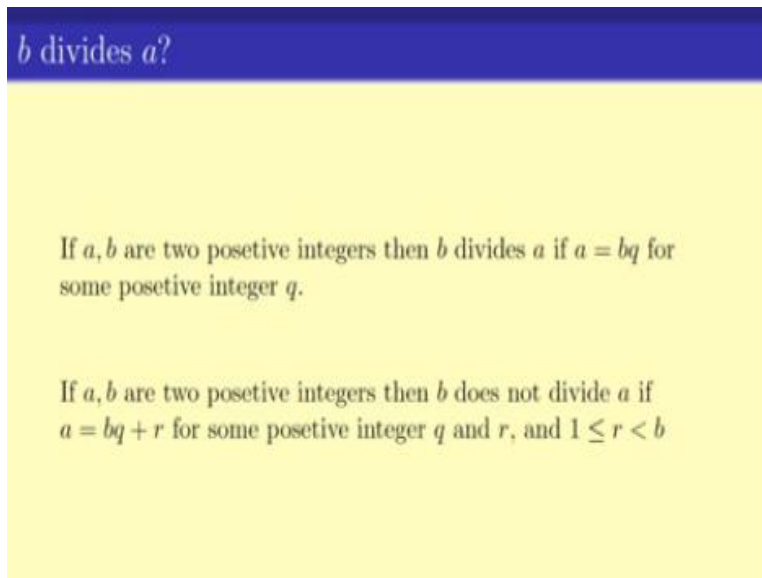
$$d \text{ divides } a - r.$$

Now, to represent this notion that when  $A$  is divided by  $D$  the remainder is  $R$ . We use this following notation  $A$  is congruent to  $R \text{ mod } D$ . The way to read it is  $A$  is congruent to  $R \text{ mod } D$  and it means  $A - R$  is divisible by  $D$  or  $A$  or  $R$  is the remainder when  $A$  is divided by  $D$ . Okay?

So it reads as D divides A - R, just a comment, this notion of modulus, the mod does not necessarily need R to be strictly less than D.

In fact, if D divides A - R then we can write it as A is congruent to R mod D. We will be using this notation quite often in the course.

**(Refer Slide Time: 08:07)**



*b divides a?*

If  $a, b$  are two positive integers then  $b$  divides  $a$  if  $a = bq$  for some positive integer  $q$ .

If  $a, b$  are two positive integers then  $b$  does not divide  $a$  if  $a = bq + r$  for some positive integer  $q$  and  $r$ , and  $1 \leq r < b$

Now this is something I just now spoke about, if A and B are 2 positive integers then, B divides A, if A is equals to B times P for some integer P, for some integer Q and if B does not divide A that means A will when divided by B purely has an integer that is not equal to 0 or I get an R which Is greater than equal to 1 and strictly less than B. So whether - so if we get a remainder which is not 0 and between 1 and b then, it means that B does not divide A.

**(Refer Slide Time: 09:12)**

## Number Theory Observations: 2

If  $a, b, p$  are three positive integers such that  $a$  is divisible by  $p$  and  $b$  is not divisible by  $p$  then prove that  $p$  does not divide  $a + b$ .

**Proof of the observation:**

- $p$  divides  $a$  implies  $a = pr$ , for some positive integer  $r$ .
- Similarly  $p$  does not divide  $b$  implies  $b = ps + t$ , for some positive integer  $s, t$  and  $1 \leq t < p$ .
- So  $a + b = pr + ps + t = p(r + s) + t$ .
- Since  $r + s$  is a positive integer so  $p$  divides  $(a + b) - t$ .
- Since  $1 \leq t < p$  so  $p$  does not divide  $(a + b)$

So this brings us to the second observation, namely, If  $A, B$  and  $P$  are 3 positive integers, such that  $A$  is divisible by  $P$  and  $B$  is not divisible by  $P$  then,  $P$  does not divide  $A + B$ . So let us see the proof of this, it is again and follows from the standard definition of remainder and divisibility. So  $P$  divides  $A$  implies  $A$  is equals to  $P$  times  $R$  for some integer  $R$ . Now  $P$  does not divide  $B$  that means  $B$  can be written as  $P$  times  $S + T$  for some  $T$  which is greater than equals to 1 and strictly less than  $P$ .

So what is  $A + B$ ?  $A + B$  equals to  $PR + PS + T$  which is  $P$  times  $R + S + T$ . Again, here it is so we can see that  $A + B = P$  times  $R + S$  which is a positive integer + number  $T$  which is a number which is by the definition of  $T$  greater than or equals to 1 and less than  $P$  or in other words it is not 0, so by the definition, it shows that  $P$  does not divide  $A + B$ .

**(Refer Slide Time: 11:04)**

## Number Theory Observations: 3

If  $a, b, p, q$  are three positive integers such that  $a$  is divisible by  $p$  and  $b$  is divisible by  $q$  then prove that  $pq$  divides  $ab$ .

**Proof of the observation:**

- $p$  divides  $a$  implies  $a = pr$ , for some positive integer  $r$ .
- Similarly  $q$  divides  $b$  implies  $b = qs$ , for some positive integer  $s$ .
- So  $ab = pr.qs = pq(rs)$
- So  $pq$  divides  $ab$

Now let us see the third observation. So if  $A, B, P$  and  $Q$  are 4 positive numbers (There is a mistake here) it is not 3, 4 positive integers such that  $A$  is divisible by  $P$  and  $B$  is divisible by  $Q$  then, we would like to show that  $PQ$  divides  $AB$ . again it follows from the first principle. So here is the proof. So  $P$  divides  $A$  that means  $A$  is equal to  $P$  times  $R$  for some positive integer  $R$ . Similarly,  $Q$  divides  $B$  that means  $B$  is equal to  $Q$  times  $S$  for some positive integer  $S$ .

So  $A$  times  $B$  equals to  $PR$  times  $QS$  which is  $PQ$  times  $RS$ . Now, since  $R$  and  $S$  are both positive integers,  $R$  times  $S$  is also a positive integer which means that  $AB$  is divisible by  $PQ$ , so this gives us 3 observations in number theory.

**(Refer Slide Time: 13:31)**

## Prime Numbers

A positive number  $p$  is a prime if for all  $1 < x < p$ ,  $x$  does not divide  $p$ .

A number that is not a prime is divisible by a prime.

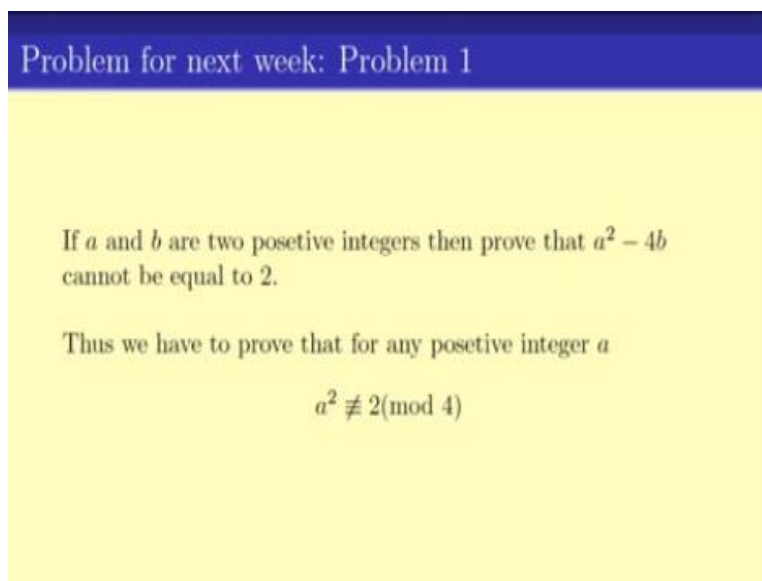
If  $a, b$  are two integers such that  $p$  divides  $a$  but does not divide  $b$  then  $p$  does not divide  $(a + b)$ .

Moving on, let us see one of the most crucial and beautiful concepts in number theory or the beauty in numbers namely prime numbers. So we say that a positive number  $P$  is a prime if no number or no integer lesser than  $P$  divides  $P$ . So for, any  $X$  which is bigger than 1 and less than  $P$ , it is not that does not divide. So in other words, you can check or proof for yourself that a number that is not prime is divisible by some other prime.

So what are the examples of prime? So 2 is a prime and it is in fact, the only even prime that we have, the other primes are 3, 5, 7, 11, 13, 17, 23, 29, 31 and so on. Here is another observation that is there, we have not proved it here but I leave it to you guys to check it or verify it. If  $A$  and  $B$  are two integers such that  $P$  divides  $A$  but does not divide  $B$  then,  $P$  does not divide  $A + B$ . So this brings us the short video of introducing you to the subject of number theory.

I encourage you guys to quickly revise your high school or elementary notes on number theory, numbers prime numbers, divisibility and so on. We will be spending some time on number theory in the next two weeks.

**(Refer Slide Time: 14:41)**



Problem for next week: Problem 1

If  $a$  and  $b$  are two positive integers then prove that  $a^2 - 4b$  cannot be equal to 2.

Thus we have to prove that for any positive integer  $a$

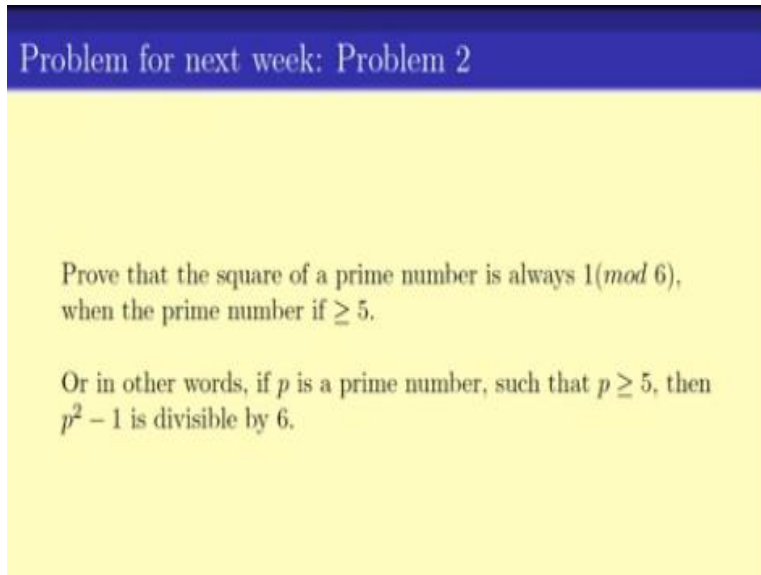
$$a^2 \not\equiv 2 \pmod{4}$$

I end this video with two problems, problem 1 is that if  $A$  and  $B$  are two positive integers then prove that  $A^2 - 4B$  cannot be equal to 2. So irrespective of what  $A$  and  $B$  are as long as they are positive integers  $A^2 - 4B$  cannot be equal to 2. So in other words, in the notation of module, we would like to say that  $S$  square or any square of any integer  $A$  cannot be



congruent to 2 mod 4. Again this should be read as A square - 2 is not divisible by 4. We will be solving this problem in the next week.

**(Refer Slide Time: 15:49)**



Problem for next week: Problem 2

Prove that the square of a prime number is always  $1 \pmod{6}$ , when the prime number is  $\geq 5$ .

Or in other words, if  $p$  is a prime number, such that  $p \geq 5$ , then  $p^2 - 1$  is divisible by 6.

The second problem that we have is, if  $P$  the prime number proves that the square of the prime number is always congruent to 1 mod 6, when the prime is bigger than or equal to 5 or in other words, if  $P$  is the prime number bigger than or equal to 5, then  $P$  square -1 is divisible by 6. These are two very beautiful and easy problems; the first problem says that the square of any integer -1 cannot be divisible by 4.

And the second one says that for any prime bigger than or equals to 5 the square of the prime -1 is divisible by 6. So this tells us some beautiful facts about integers, since this was the first week of this course, I have given only introductory live lecture videos on various topics. From next week, we will start on solving problems using various techniques and so on. Thank you.