Discrete Mathematics

Lecture 5: Elementary Number Theory

Instructor: Sourav Chakraborty

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 $b \mid a$.

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 $a \nmid b$.

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.

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 $a + b$.

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.

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.

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 $a + b = pr + ps$

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 $a + b = pr + ps = p(r + s)$.

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 $a + b$.

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.

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

Modulus

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

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

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

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

b divides a?

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

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 $1 \leq r < b$

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 $a + b$.

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.

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 $1 \leq t < p$.

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 $a + b = pr + ps + t$

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 $a + b = pr + ps + t = p(r + s) + t$.

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 $(a + b)$

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.

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.

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.

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 $ab = pr.qs = pq(rs)$

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

Prime Numbers

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

Prime Numbers

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

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

Prime Numbers

A positive number p is a prime is 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 $(a + b)$.

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.

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

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

Problem for next week: Problem 2

Prove that the square of a prime number is always $1 (mod\ 6)$, when the prime number if ≥ 5.

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