CSE 20

Lecture 5: Number Theory

Some Number Theory Notations

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

It is denoted as $b \mid a$.

Some Number Theory Notations

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

It is denoted as $b \mid a$.

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

Number Theory Observations: 1

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

- p divides a implies $a = pr$, for some posetive integer r.

Number Theory Observations: 1

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

- p divides a implies $a = pr$, for some posetive integer r.
- Similarly p divides b implies $b = ps$, for some posetive integer s.

Number Theory Observations: 1

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

- p divides a implies $a = pr$, for some posetive integer r.
- Similarly p divides b implies $b = ps$, for some posetive integer s.
- So $a + b = pr + ps$

Number Theory Observations: 1

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

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

Number Theory Observations: 1

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

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

What is a remainder?

Let a, d be two posetive integers.

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

What is a remainder?

Let a, d be two posetive integers.

If a can be written as $dq + r$ where q and r are posetive 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 divisble 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 posetive integers then b divides a if $a = bq$ for some posetive integer q.

b divides a?

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

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

Number Theory Observations: 2

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

- p divides a implies $a = pr$, for some posetive integer r.

Number Theory Observations: 2

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

- p divides a implies $a = pr$, for some posetive integer r.
- Similarly p does not divide b implies $b = ps + t$, for some posetive integer s, t and $1 \leq t < p$.

Number Theory Observations: 2

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

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

Number Theory Observations: 2

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

- p divides a implies $a = pr$, for some posetive integer r.
- Similarly p does not divide b implies $b = ps + t$, for some posetive 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 posetive integers such that a is divisible by p and b is not divisible by p then prove that p does not divide $a + b$.

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

Number Theory Observatons: 3

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

Number Theory Observatons: 3

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

- p divides a implies $a = pr$, for some posetive integer r.

Number Theory Observatons: 3

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

- p divides a implies $a = pr$, for some posetive integer r.
- Similarly q divides b implies $b = qs$, for some posetive integer s.

Number Theory Observatons: 3

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

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

Number Theory Observatons: 3

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

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

Problem 1

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

Problem 1

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

Thus we have to prove that for any posetive integer a

$$a^2 \not\equiv 2 (\text{mod } 4)$$

Proof

If a posetive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

Proof

If a posetive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

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

Proof

If a posetive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

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

We will solve in in case by case basis.

Proof

If a posetive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

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

We will solve in in case by case basis.
We split the problem into 4 case depending on the remainder when a is divided by 4.

Proof

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

Case 1 The remainder when a is divided by 4 is 0

Case 2 The remainder when a is divided by 4 is 1

Case 3 The remainder when a is divided by 4 is 2

Case 4 The remainder when a is divided by 4 is 3

Proof: Case 1

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

Case 1 The remainder when a is divided by 4 is 0

Proof: Case 1

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

Case 1 The remainder when a is divided by 4 is 0

- $a = 4r$ for some posetive integer r.

Proof: Case 1

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

Case 1 The remainder when a is divided by 4 is 0

- $a = 4r$ for some posetive integer r.
- So $a^2 = 16r^2$.

Proof: Case 1

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

Case 1 The remainder when a is divided by 4 is 0

- $a = 4r$ for some posetive integer r.
- So $a^2 = 16r^2$.
- Thus $a^2 - 4b = 16r^2 - 4b = 4(4r^2 - b)$

Proof: Case 1

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

Case 1 The remainder when a is divided by 4 is 0

- $a = 4r$ for some posetive integer r.
- So $a^2 = 16r^2$.
- Thus $a^2 - 4b = 16r^2 - 4b = 4(4r^2 - b)$
- Since $4r^2 - b$ is an integer and 4 time an integer can never be 2 so $a^2 - 4b$ cannot be equal to 2.

Proof: Case 2

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

Case 2 The remainder when a is divided by 4 is 1

Proof: Case 2

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

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some posetive integer r.

Proof: Case 2

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

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some posetive integer r.
- So $a^2 = 16r^2 + 8r + 1$.

Proof: Case 2

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

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some posetive integer r.
- So $a^2 = 16r^2 + 8r + 1$.
- Thus $a^2 - 4b = 16r^2 + 8r + 1 - 4b = 4(4r^2 + 2r - b) + 1$

Proof: Case 2

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

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some posetive integer r.
- So $a^2 = 16r^2 + 8r + 1$.
- Thus $a^2 - 4b = 16r^2 + 8r + 1 - 4b = 4(4r^2 + 2r - b) + 1$
- Since $4r^2 + 2r - b$ is an integer and 4 time an integer can never be 1

Proof: Case 2

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

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some posetive integer r.
- So $a^2 = 16r^2 + 8r + 1$.
- Thus $a^2 - 4b = 16r^2 + 8r + 1 - 4b = 4(4r^2 + 2r - b) + 1$
- Since $4r^2 + 2r - b$ is an integer and 4 time an integer can never be 1
- so $4(4r^2 + 2r - b) + 1$ cannot be equal to 2

Proof: Case 2

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

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some posetive integer r.
- So $a^2 = 16r^2 + 8r + 1$.
- Thus $a^2 - 4b = 16r^2 + 8r + 1 - 4b = 4(4r^2 + 2r - b) + 1$
- Since $4r^2 + 2r - b$ is an integer and 4 time an integer can never be 1
- so $4(4r^2 + 2r - b) + 1$ cannot be equal to 2
- and so $a^2 - 4b$ cannot be equal to 2.

Proof: Case 3

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

Case 3 The remainder when a is divided by 4 is 2

Proof: Case 3

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

Case 3 The remainder when a is divided by 4 is 2

- $a = 4r + 2$ for some posetive integer r.

Proof: Case 3

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

Case 3 The remainder when a is divided by 4 is 2

- $a = 4r + 2$ for some posetive integer r.
- So $a^2 = 16r^2 + 16r + 4$.

Proof: Case 3

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

Case 3 The remainder when a is divided by 4 is 2

- $a = 4r + 2$ for some posetive integer r.
- So $a^2 = 16r^2 + 16r + 4$.
- Thus $a^2 - 4b = 16r^2 + 16r + 4 - 4b = 4(4r^2 + 4r + 1 - b)$

Proof: Case 3

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

Case 3 The remainder when a is divided by 4 is 2

- $a = 4r + 2$ for some posetive integer r.
- So $a^2 = 16r^2 + 16r + 4$.
- Thus $a^2 - 4b = 16r^2 + 16r + 4 - 4b = 4(4r^2 + 4r + 1 - b)$
- Since $4r^2 + 4r + 1 - b$ is an integer and 4 time an integer can never be 2 so $a^2 - 4b$ cannot be equal to 2.

Proof: Case 4

If a and b are two posetive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

Proof: Case 4

If a and b are two posetive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

- $a = 4r + 3$ for some posetive integer r.

Proof: Case 4

If a and b are two posetive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

- $a = 4r + 3$ for some posetive integer r.
- So $a^2 = 16r^2 + 24r + 9$.

Proof: Case 4

If a and b are two posetive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

- $a = 4r + 3$ for some posetive integer r.
- So $a^2 = 16r^2 + 24r + 9$.
- Thus
  $a^2 - 4b = 16r^2 + 24r + 9 - 4b = 4(4r^2 + 6r + 2 - b) + 1$

Proof: Case 4

If a and b are two posetive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

- $a = 4r + 3$ for some posetive integer r.
- So $a^2 = 16r^2 + 24r + 9$.
- Thus
  $a^2 - 4b = 16r^2 + 24r + 9 - 4b = 4(4r^2 + 6r + 2 - b) + 1$
- Since $4r^2 + 6r + 2 - b$ is an integer and 4 time an integer can never be 2 so $a^2 - 4b$ cannot be equal to 1.
- so $4(4r^2 + 6r + 2 - b) + 1$ cannot be equal to 2

Proof: Case 4

If a and b are two posetive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

- $a = 4r + 3$ for some posetive integer r.
- So $a^2 = 16r^2 + 24r + 9$.
- Thus
  $a^2 - 4b = 16r^2 + 24r + 9 - 4b = 4(4r^2 + 6r + 2 - b) + 1$
- Since $4r^2 + 6r + 2 - b$ is an integer and 4 time an integer can never be 2 so $a^2 - 4b$ cannot be equal to 1.
- so $4(4r^2 + 6r + 2 - b) + 1$ cannot be equal to 2
- and so $a^2 - 4b$ cannot be equal to 2.

Complete Proof

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

Complete Proof

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

If a posetive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

Complete Proof

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

If a posetive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

We will solve in in case by case basis.

Complete Proof

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

If a posetive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

We will solve in in case by case basis.

We split the problem into 4 case depending on the remainder when a is divided by 4 and show that for every case $a^2 - 4b$ cannot be equal to 2.

Prime Numbers

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

Prime Numbers

A posetive 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 posetive 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 dive $(a + b)$.

Problem for next class

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.