## Number Theory. Class 1

Victor H. Moll Tulane University

January 15, 2008

Notation:

- $\mathbb{N}:=\{1,\,2,\,3,\cdots\}$  the natural numbers
- $\mathbb{N}_0 := \{0, 1, 2, \cdots \}$  the cardinal numbers
- $\mathbb{Z} := \{-2, -1, 0, 1, 2, \cdots \}$  the integers

#### Definition

- Given  $a, b \in \mathbb{Z}$ , we say that a divides b
- if there is  $c \in \mathbb{Z}$  such that b = ac. We write a b.

Equivalent terminology:

- b is a multiple of a
- a is a divisor of b

#### Notation:

- $\mathbb{N}:=\{1,\,2,\,3,\cdots\}$  the natural numbers
- $\mathbb{N}_0 := \{0, 1, 2, \cdots \}$  the cardinal numbers
- $\mathbb{Z} := \{-2, -1, 0, 1, 2, \cdots \}$  the integers

#### Definition

- Given  $a, b \in \mathbb{Z}$ , we say that a divides b
- if there is  $c \in \mathbb{Z}$  such that b = ac. We write a b.
- Equivalent terminology:
- b is a multiple of a
- a is a divisor of b.

## Notation:

 $\mathbb{N}:=\{1,\,2,\,3,\cdots\}$  the natural numbers

 $\mathbb{N}_0 := \{0, 1, 2, \cdots \}$  the cardinal numbers

 $\mathbb{Z}:=\{-2,\,-1,\,0,\,1,\,2,\cdots\}$  the integers

#### Definition

Given  $a, b \in \mathbb{Z}$ , we say that a divides b

if there is  $c \in \mathbb{Z}$  such that b = ac. We write a b.

Equivalent terminology:

b is a multiple of a

a is a divisor of b.

## $$\label{eq:Notation:} \begin{split} &\mathbb{N}:=\{1,\,2,\,3,\cdots\} \text{ the natural numbers} \\ &\mathbb{N}_0:=\{0,\,1,\,2,\,\cdots\} \text{ the cardinal numbers} \end{split}$$

 $\mathbb{Z} := \{-2, -1, 0, 1, 2, \cdots \}$  the integers

#### Definition

Given  $a, b \in \mathbb{Z}$ , we say that a divides b

if there is  $c \in \mathbb{Z}$  such that b = ac. We write a | b.

Equivalent terminology:

b is a multiple of a

a is a divisor of b.

#### Notation:

$$\begin{split} \mathbb{N} &:= \{1, 2, 3, \cdots\} \text{ the natural numbers} \\ \mathbb{N}_0 &:= \{0, 1, 2, \cdots\} \text{ the cardinal numbers} \\ \mathbb{Z} &:= \{-2, -1, 0, 1, 2, \cdots\} \text{ the integers} \end{split}$$

#### Definition

Given a, b ∈ ℤ, we say that a divides b if there is c ∈ ℤ such that b = ac. We write a

Equivalent terminology:

b is a multiple of a

a is a divisor of b.

#### Notation:

$$\begin{split} \mathbb{N} &:= \{1, 2, 3, \cdots\} \text{ the natural numbers} \\ \mathbb{N}_0 &:= \{0, 1, 2, \cdots\} \text{ the cardinal numbers} \\ \mathbb{Z} &:= \{-2, -1, 0, 1, 2, \cdots\} \text{ the integers} \end{split}$$

#### Definition

Given  $a, b \in \mathbb{Z}$ , we say that a divides bif there is  $c \in \mathbb{Z}$  such that b = ac. We write a|b.

Equivalent terminology

b is a multiple of a

a is a divisor of b.

#### Notation:

$$\begin{split} \mathbb{N} &:= \{1, 2, 3, \cdots\} \text{ the natural numbers} \\ \mathbb{N}_0 &:= \{0, 1, 2, \cdots\} \text{ the cardinal numbers} \\ \mathbb{Z} &:= \{-2, -1, 0, 1, 2, \cdots\} \text{ the integers} \end{split}$$

#### Definition

Given  $a, b \in \mathbb{Z}$ , we say that a divides bif there is  $c \in \mathbb{Z}$  such that b = ac. We write a|b.

#### Equivalent terminology:

*b* is a multiple of *a*. *a* is a divisor of *b*.

#### Notation:

$$\begin{split} \mathbb{N} &:= \{1, 2, 3, \cdots\} \text{ the natural numbers} \\ \mathbb{N}_0 &:= \{0, 1, 2, \cdots\} \text{ the cardinal numbers} \\ \mathbb{Z} &:= \{-2, -1, 0, 1, 2, \cdots\} \text{ the integers} \end{split}$$

#### Definition

Given  $a, b \in \mathbb{Z}$ , we say that a divides bif there is  $c \in \mathbb{Z}$  such that b = ac. We write a|b.

Equivalent terminology: *b* is a multiple of *a*.

#### Notation:

$$\begin{split} \mathbb{N} &:= \{1, 2, 3, \cdots\} \text{ the natural numbers} \\ \mathbb{N}_0 &:= \{0, 1, 2, \cdots\} \text{ the cardinal numbers} \\ \mathbb{Z} &:= \{-2, -1, 0, 1, 2, \cdots\} \text{ the integers} \end{split}$$

#### Definition

Given  $a, b \in \mathbb{Z}$ , we say that a divides bif there is  $c \in \mathbb{Z}$  such that b = ac. We write a|b.

Equivalent terminology: b is a multiple of a. a is a divisor of b.

#### Question

Given a,  $b \in \mathbb{Z}$ , how do we decide if a divides b

#### Question

Given  $a \in \mathbb{Z}$ , how do we find all divisors of a.

#### Question

Given  $a \in \mathbb{Z}$ , how do we find some divisors of a.

#### Question

Given  $a, b \in \mathbb{Z}$ , how do we decide if a divides b.

#### Question

Given  $a \in \mathbb{Z}$ , how do we find all divisors of a.

#### Question

Given a  $\in \mathbb{Z}$ , how do we find some divisors of a.

#### Question

Given  $a, b \in \mathbb{Z}$ , how do we decide if a divides b.

#### Question

Given  $a \in \mathbb{Z}$ , how do we find all divisors of a.

#### Question

Given a  $\in \mathbb{Z}$ , how do we find some divisors of a.

#### Question

Given a,  $b \in \mathbb{Z}$ , how do we decide if a divides b.

#### Question

Given  $a \in \mathbb{Z}$ , how do we find all divisors of a.

#### Question

Given  $a \in \mathbb{Z}$ , how do we find some divisors of a.

#### Definition

The integer  $p \in \mathbb{N}$  is called prime if its only divisors are 1 and p.

#### Definition

The number of divisors of  $n\in\mathbb{N}$  is denoted by arphi(n).

This is the Euler phi-function or totient function

#### Proposition

n>1 is prime if and only if arphi(n)=2

#### Exercise

Prove that the function arphi is unbounded

#### Definition

The integer  $p \in \mathbb{N}$  is called prime if its only divisors are 1 and p.

#### Definition

The number of divisors of  $n\in\mathbb{N}$  is denoted by arphi(n)

This is the Euler phi-function or totient function

#### Proposition

n>1 is prime if and only if arphi(n)=2

#### Exercise

Prove that the function arphi is unbounded

#### Definition

The integer  $p \in \mathbb{N}$  is called prime if its only divisors are 1 and p.

### Definition

The number of divisors of  $n \in \mathbb{N}$  is denoted by  $\varphi(n)$ .

#### This is the Euler phi-function or totient function

#### Proposition

n>1 is prime if and only if arphi(n)=2

#### Exercise

Prove that the function arphi is unbounded

<ロ> < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

#### Definition

The integer  $p \in \mathbb{N}$  is called prime if its only divisors are 1 and p.

#### Definition

The number of divisors of  $n \in \mathbb{N}$  is denoted by  $\varphi(n)$ .

#### This is the Euler phi-function or totient function.

## n > 1 is prime if and only if $\varphi(n)$ .

#### Exercise

Prove that the function arphi is unbounded

#### Definition

The integer  $p \in \mathbb{N}$  is called prime if its only divisors are 1 and p.

#### Definition

The number of divisors of  $n \in \mathbb{N}$  is denoted by  $\varphi(n)$ .

This is the Euler phi-function or totient function.

#### Proposition

n > 1 is prime if and only if  $\varphi(n) = 2$ .

#### xercise

Prove that the function arphi is unbounded

#### Definition

The integer  $p \in \mathbb{N}$  is called prime if its only divisors are 1 and p.

#### Definition

The number of divisors of  $n \in \mathbb{N}$  is denoted by  $\varphi(n)$ .

This is the Euler phi-function or totient function.

#### Proposition

n > 1 is prime if and only if  $\varphi(n) = 2$ .

#### Exercise

Prove that the function  $\varphi$  is unbounded.

#### l heoren

Every integer  $n \in \mathbb{N}$  is divisible by a prime.

#### Proof.

nduction on n.

lf *n* is prime, done

If not, let b < n be one of its divisors.

Every prime divisor of *b*, also divides *n*. Done

#### Theorem

Every integer  $n \in \mathbb{N}$  is divisible by a prime.

#### Proof.

Induction on *n*.

lf *n* is prime, done

f not, let b < n be one of its divisors.

Every prime divisor of *b*, also divides *n*. Done.

#### Theorem

Every integer  $n \in \mathbb{N}$  is divisible by a prime.

#### Proof.

Induction on n.

lf *n* is prime, done

If not, let b < n be one of its divisors.

Every prime divisor of *b*, also divides *n*. Done.

#### Theorem

Every integer  $n \in \mathbb{N}$  is divisible by a prime.

#### Proof.

Induction on n.

#### If *n* is prime, done.

If not, let b < n be one of its divisors.

very prime divisor of *b*, also divides *n*. Done.

#### Theorem

Every integer  $n \in \mathbb{N}$  is divisible by a prime.

#### Proof.

Induction on *n*. If *n* is prime, done. If not, let b < n be one of its divisors.

Every prime divisor of *b*, also divides *n*. Done

#### Theorem

Every integer  $n \in \mathbb{N}$  is divisible by a prime.

#### Proof.

Induction on *n*. If *n* is prime, done. If not, let b < n be one of its divisors. Every prime divisor of *b*, also divides *n*. Done.

#### I heorem

There are infinitely many primes.

#### Proof.

Assume  $\{p_1, p_2, \cdots, p_N\}$  are all the primes.

Form  $I_N := p_1 p_2 \cdots p_N + \dots$ 

If  $p_j$  divides  $T_N$ , then it divides  $1 = T_N - p_1 p_2 \cdots p_N$ .

Therefore T<sub>N</sub> has no primes divisors. Contradiction

#### Theorem

There are infinitely many primes.

#### Proof.

Assume  $\{p_1, p_2, \cdots, p_N\}$  are all the primes.

Form  $T_N := p_1 p_2 \cdots p_N + \dots$ 

f  $p_j$  divides  $T_N$ , then it divides  $1 = T_N - p_1 p_2 \cdots p_N$ .

Therefore *T<sub>N</sub>* has no primes divisors. Contradiction

<ロ> < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

#### Theorem

There are infinitely many primes.

#### Proof.

Assume  $\{p_1, p_2, \cdots, p_N\}$  are all the primes.

 $-\text{orm } T_N := p_1 p_2 \cdots p_N + \dots$ 

f  $p_j$  divides  $T_N$ , then it divides  $1 = T_N - p_1 p_2 \cdots p_N$ .

Therefore *T<sub>N</sub>* has no primes divisors. Contradiction

#### Theorem

There are infinitely many primes.

#### Proof.

Assume  $\{p_1, p_2, \cdots, p_N\}$  are all the primes.

Form  $T_N := p_1 p_2 \cdots p_N + 1$ .

If  $p_j$  divides  $T_N$ , then it divides  $1 = T_N - p_1 p_2 \cdots p_N$ .

Therefore *T<sub>N</sub>* has no primes divisors. Contradiction

#### Theorem

There are infinitely many primes.

#### Proof.

Assume  $\{p_1, p_2, \cdots, p_N\}$  are all the primes.

Form  $T_N := p_1 p_2 \cdots p_N + 1$ .

If  $p_i$  divides  $T_N$ , then it divides  $1 = T_N - p_1 p_2 \cdots p_N$ .

Therefore T<sub>M</sub> has no primes divisors. Contradiction

#### Theorem

There are infinitely many primes.

#### Proof.

Assume  $\{p_1, p_2, \cdots, p_N\}$  are all the primes.

Form  $T_N := p_1 p_2 \cdots p_N + 1$ .

If  $p_j$  divides  $T_N$ , then it divides  $1 = T_N - p_1 p_2 \cdots p_N$ .

Therefore  $T_N$  has no primes divisors. Contradiction.

#### I heorem

The difference between consecutive primes can be as large as you want.

#### Proof.

The numbers

#### $n! + 2, n! + 3, n! + 4, \cdots, n! + n$

are all composite = not prime.

Open question

There are infinitely many primes p such that p + 2 is also prime.

These are called twin primes

# Theorem The difference between consecutive primes can be as large as you want.

#### Theorem

The difference between consecutive primes can be as large as you want.

#### Proof.

The numbers

#### $n! + 2, n! + 3, n! + 4, \cdots, n! + n$

are all composite = not prime.

Open question

There are infinitely many primes p such that p + 2 is also prime.

These are called twin primes

#### Theorem

The difference between consecutive primes can be as large as you want.

#### Proof.

The numbers

$$n! + 2, n! + 3, n! + 4, \cdots, n! + n$$

are all composite = not prime.

Open question.

There are infinitely many primes  $\rho$  such that  $\rho + 2$  is also prime.

These are called twin primes

#### Theorem

The difference between consecutive primes can be as large as you want.

#### Proof.

The numbers

$$n! + 2, n! + 3, n! + 4, \cdots, n! + n$$

are all composite = not prime.

Open question.

There are infinitely many primes p such that p + 2 is also prime.

These are called <del>twin primes</del>

#### Theorem

The difference between consecutive primes can be as large as you want.

#### Proof.

The numbers

$$n! + 2, n! + 3, n! + 4, \cdots, n! + n$$

<ロ> < 回> < 三> < 三> < 三> < 三> < 三</p>

are all composite = not prime.

Open question.

There are infinitely many primes p such that p + 2 is also prime.

These are called to

#### Theorem

The difference between consecutive primes can be as large as you want.

#### Proof.

The numbers

$$n! + 2, n! + 3, n! + 4, \cdots, n! + n$$

<ロ> < 回> < 三> < 三> < 三> < 三> < 三</p>

are all composite = not prime.

Open question.

There are infinitely many primes p such that p + 2 is also prime.

These are called to

#### Theorem

The difference between consecutive primes can be as large as you want.

#### Proof.

The numbers

$$n! + 2, n! + 3, n! + 4, \cdots, n! + n$$

are all composite = not prime.

Open question.

There are infinitely many primes p such that p + 2 is also prime.

These are called twin primes