Number Theory. Class 1

Victor H. Moll
Tulane University

January 15, 2008

Divisibility

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.

Divisibility

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.

Divisibility

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.

Divisibility

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.

Divisibility

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.

Divisibility

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.

Divisibility

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.

Divisibility

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.

Divisibility

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.

Divisibility (continuation)

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.

Divisibility (continuation)

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.

Divisibility (continuation)

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.

Divisibility (continuation)

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*.*

Prime numbers

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 φ is unbounded.

Prime numbers

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 φ is unbounded.

Prime numbers

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 φ is unbounded.

Prime numbers

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 φ is unbounded.

Prime numbers

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 φ is unbounded.

Prime numbers

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 φ is unbounded.

Prime numbers (continuation)

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. □

Prime numbers (continuation)

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. $\square$

Prime numbers (continuation)

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. □

Prime numbers (continuation)

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. □

Prime numbers (continuation)

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. □

Prime numbers (continuation)

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. □

Prime numbers (continuation)

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.

□

Prime numbers (continuation)

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. □

Prime numbers (continuation)

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.

□

Prime numbers (continuation)

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.

$\square$

Prime numbers (continuation)

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.

□

Prime numbers (continuation)

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.

$\square$

Prime gaps

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

Prime gaps

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

Prime gaps

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

Prime gaps

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

Prime gaps

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

Prime gaps

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

Prime gaps

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

Prime gaps

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