Math 325K - Lecture 8
Section 4.2 & 4.3

Bo Lin

September 25th, 2018

Outline

- Rational numbers.
- Divisibility.
- Unique Factorization Theorem.

Definition

Definition

A real number r *is* **rational** *if and only if it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is* **irrational**. *Formally, if* r *is a real number, then*

$$r \text{ is rational } \Leftrightarrow \exists a, b \in \mathbb{Z} \text{ such that } \left(r = \frac{a}{b}\right) \wedge (b \neq 0).$$

The set of rational number is denoted by $\mathbb{Q}$.

Definition

Definition

A real number r is **rational** *if and only if it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is* **irrational***. Formally, if r is a real number, then*

$$r \text{ is rational } \Leftrightarrow \exists a, b \in \mathbb{Z} \text{ such that } \left(r = \frac{a}{b}\right) \wedge (b \neq 0)\,.$$

The set of rational number is denoted by $\mathbb{Q}$.

Remark

Since it is an existential statement, in general it's easier to show that a real number is rational than showing that a real number is irrational.

Examples: rational and irrational numbers

Example

Are the following numbers rational or irrational?

(a) $10/3$;
(b) 0.365;
(c) $4/0$;
(d) $0.12121212\ldots$.

Examples: rational and irrational numbers

Example

Are the following numbers rational or irrational?

(a) $10/3$;
(b) 0.365;
(c) $4/0$;
(d) $0.12121212\ldots$.

Solution

(a) Yes.

Examples: rational and irrational numbers

Example

Are the following numbers rational or irrational?

(a) $10/3$;

(b) 0.365;

(c) $4/0$;

(d) $0.12121212\ldots$.

Solution

(a) Yes. (b) Yes, because $0.365 = 365/1000$.

Examples: rational and irrational numbers

Example

Are the following numbers rational or irrational?

(a) $10/3$;
(b) 0.365;
(c) $4/0$;
(d) $0.12121212\ldots$.

Solution

(a) Yes. (b) Yes, because $0.365 = 365/1000$. *(c) No,* $4/0$ *is not a number at all.*

Examples: rational and irrational numbers

Example

Are the following numbers rational or irrational?

(a) $10/3$;
(b) 0.365;
(c) $4/0$;
(d) $0.12121212\ldots$.

Solution

(a) Yes. (b) Yes, because $0.365 = 365/1000$. *(c) No,* $4/0$ *is not a number at all.*
(d) Yes. Let $x = 0.12121212\ldots$, *then* $100x = 12.12121212\ldots$. *So* $12 = 100x - x = 99x$, $x = 12/99$. *In general, all repeating decimal numbers are rational.*

Sum of rational numbers

Theorem

The sum of any two rational numbers is rational.

Sum of rational numbers

Theorem

The sum of any two rational numbers is rational.

We first rewrite the statement formally:

Theorem

$\forall r \in \mathbb{Q}, \forall s \in \mathbb{Q}, r + s \in \mathbb{Q}.$

Sum of rational numbers

Proof.

Let r, s be arbitrary rational numbers. Then there exist integers a, b with $b \neq 0$ such that $r = \frac{a}{b}$, and there exist integers c, d with $d \neq 0$ such that $s = \frac{c}{d}$. So

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad + bc}{bd}.$$

Sum of rational numbers

Proof.

Let r, s be arbitrary rational numbers. Then there exist integers a, b with $b \neq 0$ such that $r = \frac{a}{b}$, and there exist integers c, d with $d \neq 0$ such that $s = \frac{c}{d}$. So

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad + bc}{bd}.$$

Since a, b, c, d are integers, so are $ad + bc$ and bd. In addition, since both b and d are nonzero, so is bd. (This is the **zero product property**). By definition, $\frac{ad+bc}{bd}$ is rational, in other words $r + s$ is rational. □

Sum of rational numbers

Proof.

Let r, s be arbitrary rational numbers. Then there exist integers a, b with $b \neq 0$ such that $r = \frac{a}{b}$, and there exist integers c, d with $d \neq 0$ such that $s = \frac{c}{d}$. So

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad + bc}{bd}.$$

Since a, b, c, d are integers, so are $ad + bc$ and bd. In addition, since both b and d are nonzero, so is bd. (This is the **zero product property**). By definition, $\frac{ad+bc}{bd}$ is rational, in other words $r + s$ is rational. □

Product of rational numbers

Theorem

The product of two rational numbers is rational.

Product of rational numbers

Theorem

The product of two rational numbers is rational.

Proof.

Let r, s be arbitrary rational numbers. Then there exist integers a, b with $b \neq 0$ such that $r = \frac{a}{b}$, and there exist integers c, d with $d \neq 0$ such that $s = \frac{c}{d}$. So

$$r \cdot s = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Since a, b, c, d are integers, so are ac and bd. In addition, since both b and d are nonzero, so is bd. By definition, $r \cdot s$ is rational. □

Quotient of rational numbers

Theorem

If $r, s \in \mathbb{Q}$ *and* $s \neq 0$, *then* $\frac{r}{s} \in \mathbb{Q}$.

Quotient of rational numbers

Theorem

If $r, s \in \mathbb{Q}$ *and* $s \neq 0$, *then* $\frac{r}{s} \in \mathbb{Q}$.

Proof.

Let r, s be arbitrary rational numbers with $s \neq 0$. Then there exist integers a, b with $b \neq 0$ such that $r = \frac{a}{b}$, and there exist integers c, d with $d \neq 0$ such that $s = \frac{c}{d}$. So

$$\frac{r}{s} = \frac{a}{b} / \frac{c}{d} = \frac{ad}{bc}.$$

Quotient of rational numbers

Theorem

If $r, s \in \mathbb{Q}$ *and* $s \neq 0$, *then* $\frac{r}{s} \in \mathbb{Q}$.

Proof.

Let r, s be arbitrary rational numbers with $s \neq 0$. Then there exist integers a, b with $b \neq 0$ such that $r = \frac{a}{b}$, and there exist integers c, d with $d \neq 0$ such that $s = \frac{c}{d}$. So

$$\frac{r}{s} = \frac{a}{b} / \frac{c}{d} = \frac{ad}{bc}.$$

Since a, b, c, d are integers, so are ad and bc. Since $s \neq 0$, we have that $c \neq 0$. Since both b and c are nonzero, so is bc. By definition, $\frac{r}{s}$ is rational. □

Definition

Definition

If n and d are integers and $d \neq 0$ then n is **divisible** *by d if and only if n equals d times some integer. Instead of n is divisible by d, we can also say that*

- *n is a* **multiple** *of d;*
- *d is a* **factor** *of n;*
- *d is a* **divisor** *of n;*
- *d* **divides** *n.*

The notation $d|n$ is read d divides n. Symbolically, if n and d are integers and $d \neq 0$

$$d|n \Leftrightarrow \exists k \in \mathbb{Z} \text{ such that } n = dk.$$

Examples: checking divisibility

Example

(a) *Is* 21 *divisible by* 3*?*

(b) *Does* 4 *divide* 22*?*

(c) *Is* 28 *a multiple of* -7*?*

Examples: checking divisibility

Example

(a) *Is* 21 *divisible by* 3*?*

(b) *Does* 4 *divide* 22*?*

(c) *Is* 28 *a multiple of* -7*?*

Solution

(a) Since $21 = 3 \cdot 7$*, yes.*

Examples: checking divisibility

Example

(a) *Is* 21 *divisible by* 3*?*

(b) *Does* 4 *divide* 22*?*

(c) *Is* 28 *a multiple of* -7*?*

Solution

(a) Since $21 = 3 \cdot 7$*, yes.*
(b) Since $22/4 = 5.5 \notin \mathbb{Z}$*, no.*

Examples: checking divisibility

Example

(a) *Is* 21 *divisible by* 3*?*

(b) *Does* 4 *divide* 22*?*

(c) *Is* 28 *a multiple of* -7*?*

Solution

(a) Since $21 = 3 \cdot 7$*, yes.*
(b) Since $22/4 = 5.5 \notin \mathbb{Z}$*, no.*
(c) Since $28 = (-7) \cdot (-4)$*, yes.*

Divisors of special integers

Proposition

Any nonzero integer k divides 0.

Divisors of special integers

Proposition

Any nonzero integer k divides 0.

Proof.

Because $0 = k \cdot 0$. □

Divisors of special integers

Proposition

If a and b are positive integers and $a|b$, then $a \leq b$.

Divisors of special integers

Proposition

If a and b are positive integers and $a|b$, then $a \leq b$.

Proof.

Let a and b be such a pair of integers. Since $a|b$, there is an integer k such that $b = ak$. Since both a, b are positive, so is k. Then $k \geq 1$ and

$$a = a \cdot 1 \leq a \cdot k = b.$$

□

Divisors of special integers

Proposition

If a and b are positive integers and $a|b$, then $a \leq b$.

Proof.

Let a and b be such a pair of integers. Since $a|b$, there is an integer k such that $b = ak$. Since both a, b are positive, so is k. Then $k \geq 1$ and

$$a = a \cdot 1 \leq a \cdot k = b.$$

□

Corollary

The only divisors of 1 are 1 and -1.

Examples: divisibility of algebraic expressions

Example

Let a and b be integers. Is $6a + 9b$ always divisible by 3?

Examples: divisibility of algebraic expressions

Example

Let a and b be integers. Is $6a + 9b$ always divisible by 3?

Solution

Note that $6a + 9b = 3 \cdot (2a + 3b)$. Since a and b are both integers, so is $2a + 3b$. By definition, $6a + 9b$ is divisible by 3.

Connection to prime numbers

Proposition

A positive integer $n > 1$ is prime if and only if all of its positive divisors are 1 and n.

Connection to prime numbers

Proposition

A positive integer $n > 1$ is prime if and only if all of its positive divisors are 1 and n.

Proof.

We prove its contrapositive. Suppose n has a positive divisor k other than 1 and n. Then $\frac{n}{k}$ is also a positive integer and $n = k \cdot \frac{n}{k}$ is another way to write n as the product of two positive integers. By definition, n is not prime.

Connection to prime numbers

Proposition

A positive integer $n > 1$ is prime if and only if all of its positive divisors are 1 and n.

Proof.

We prove its contrapositive. Suppose n has a positive divisor k other than 1 and n. Then $\frac{n}{k}$ is also a positive integer and $n = k \cdot \frac{n}{k}$ is another way to write n as the product of two positive integers. By definition, n is not prime.
Conversely, suppose n is not prime, then there is another way to write n as the product of two positive integers, say $n = a \cdot b$. Then $a|n$ and $1 < a < n$, so n has a positive divisor a other than 1 and n. □

Transitivity of divisibility

Theorem

For integers a, b, c, if $a|b$ and $b|c$, then $a|c$.

Transitivity of divisibility

Theorem

For integers a, b, c, if $a|b$ and $b|c$, then $a|c$.

Proof.

First, since $a|b$, by definition $a \neq 0$ and there is an integer r such that $b = ar$. Next, since $b|c$, there is an integer s such that $c = bs$. So

$$c = bs = ars = a \cdot (rs).$$

Since both r and s are integers, so is rs. By definition, $a|c$. □

Prime divisors

Theorem

Every integer $n > 1$ has at least a prime divisor.

Prime divisors

Theorem

Every integer $n > 1$ has at least a prime divisor.

Proof.

If n itself is prime, we are done. Otherwise it must be composite, by definition there are integers $1 < a\&b < n$ such that $n = ab$. Now we repeat the procedure for a. a is either prime or composite, if a is prime, then it is a prime divisor of n; if a is composite, we can further decompose a as the product of two positive integers strictly between 1 and a. Since there are only finitely many positive integers upto n, the process must terminate after finitely many steps, and we are done. □

The theorem

Theorem (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist a positive integer k and distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

And any other expression for n as a product of prime numbers is identical to this one, up to a change of order of the factors $p_i^{e_i}$.

The theorem

Theorem (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist a positive integer k and distinct prime numbers $p_1, p_2, \dots, p_k$, and positive integers $e_1, e_2, \dots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

And any other expression for n as a product of prime numbers is identical to this one, up to a change of order of the factors $p_i^{e_i}$.

Remark

We postpone the proof to future sections.

Standard factored form

Definition

Given any integer $n > 1$, the **standard factored form** *of n is an expression of the form*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \ldots < p_k$.

Standard factored form

Definition

Given any integer $n > 1$, the **standard factored form** *of n is an expression of the form*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \ldots < p_k$.

Remark

In the standard factored form, since the order of prime numbers is fixed, the form is unique.

Examples: standard factored form

Example

Find the standard factored form of the following positive integers:

(a) 16;
(b) 30;
(c) 35^3.

Examples: standard factored form

Example

Find the standard factored form of the following positive integers:

- (a) 16;
- (b) 30;
- (c) 35^3.

Solution

(a) $16 = 2^4$. *Since* 2 *is prime,* 2^4 *is the answer.*

Examples: standard factored form

Example

Find the standard factored form of the following positive integers:

- (a) 16;
- (b) 30;
- (c) 35^3.

Solution

(a) $16 = 2^4$. *Since* 2 *is prime,* 2^4 *is the answer.*
(b) $30 = 2 \cdot 3 \cdot 5$. *Since* $2, 3, 5$ *are all prime,* $2 \cdot 3 \cdot 5$ *is the answer.*

Examples: standard factored form

Example

Find the standard factored form of the following positive integers:

(a) 16;

(b) 30;

(c) 35^3.

Solution

(a) $16 = 2^4$. *Since* 2 *is prime,* 2^4 *is the answer.*
(b) $30 = 2 \cdot 3 \cdot 5$. *Since* $2, 3, 5$ *are all prime,* $2 \cdot 3 \cdot 5$ *is the answer.*
(c) First $35 = 5 \cdot 7$ *and both* 5 *and* 7 *are prime numbers. So*

$$35^3 = (5 \cdot 7)^3 = 5^3 \cdot 7^3$$

is the answer.

HW# 4of these sections

Section 4.2 Exercise 5, 14, 25, 30.
Section 4.3 Exercise 5, 13, 28, 29, 39, 45.