Direct Proof – Divisibility

Lecture 15
Section 4.3

Robb T. Koether

Hampden-Sydney College

Fri, Feb 7, 2014

Outline

Divisibility

Definition (Rational Number)

Let $a, b \in \mathbb{Z}$. Then a **divides** b, denoted $a \mid b$, if $a \neq 0$ and there exists $c \in \mathbb{Z}$ such that $b = ac$.

- In other words, a divides b if b is a multiple of a.
- Note the following:
  - Every integer divides 0, but 0 divides no integer.
  - 1 divides every integer, but only 1 and -1 divide 1.
  - Every integer except 0 divides itself.

Example

Theorem

Let $a, b, c, \in \mathbb{Z}$. *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

Example

Proof.

- Let $a, b, c, \in \mathbb{Z}$ and suppose that $a \mid b$ and $b \mid c$.
- Then there exist integers s and t such that $b = as$ and $c = bt$.
- So

$$\begin{aligned} c &= bt \\ &= (as)t \\ &= a(st). \end{aligned}$$

- $st \in \mathbb{Z}$, so it follows that $a \mid c$.

$\square$

Example

Theorem

Let $a, b, c \in \mathbb{Z}$. *If* $a \mid b$ *and* $b \mid a + c$, *then* $a \mid c$.

Example

Proof.

- Let $a, b, c \in \mathbb{Z}$ and suppose that $a \mid b$ and $b \mid a + c$.
- Then there exist integers s and t such that $b = as$ and $a + c = bt$.
- Then

$$\begin{aligned} c &= bt - a \\ &= (as)t - a \\ &= a(st - 1). \end{aligned}$$

- Therefore, $a \mid c$.

□

Outline

Prime Integers

Definition

An integer $p \in \mathbb{N}$ is prime if $p \geq 2$ and the only divisors of p are 1 and p.

- The last condition is equivalent to saying

$$\forall a \in \mathbb{N}, a \mid p \to (a = 1 \vee a = p).$$

- List the first 15 prime numbers.
- What is the negation of the property of being a prime?

Composite Integers

Definition

An integer $n \in \mathbb{N}$ is composite if there exist integers a and b such that $a > 1$, $b > 1$, and $n = ab$.

- List the first 15 composite numbers.
- Are there any numbers that are neither prime nor composite?
- Is 1 prime? Is 1 composite?
- Is 0 prime? Is 0 composite?

Negative Primes and Composites

- There is no problem with extending the definitions of prime and composite to negative integers.
- An integer $p \in \mathbb{Z}$ is prime if $|p| \geq 2$ and if $a \mid p$, then $|a| = 1$ or $|a| = p$.
- An integer $n \in \mathbb{Z}$ is composite if there exist integers a and b such that $|a| > 1$ and $|b| > 1$ and $n = ab$.

Other Integers

Definition

An integer $u \in \mathbb{Z}$ is a unit if $u \mid 1$.

- The only units in $\mathbb{Z}$ are 1 and -1.

Example

Theorem

Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \mid a$, then either $a = b$ or $a = -b$.

Example

Proof.

- Let $a, b \in \mathbb{Z}$ and suppose that $a \mid b$ and $b \mid a$.
- Then there exist integers s and t such that $b = as$ and $a = bt$.
- Then

$$\begin{aligned} a &= bt \\ &= (as)t \\ &= a(st). \end{aligned}$$

$\square$

Example

Proof.

- Then $1 = st$, so $s \mid 1$ and $t \mid 1$.
- So s and t are units and must equal 1 or -1.
- It follows that either $a = b$ or $a = -b$.

$\square$

Outline

The Fundamental Theorem of Arithmetic

Theorem (The Fundamental Theorem of Arithmetic)

Let n be a positive integer. Then there exists a set of primes $p_1, p_2, \ldots, p_k$, for some integer $k \geq 0$, and positive integers $e_1, e_2, \ldots, e_k$ such that

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

- Write the prime factorizations of 1024, 768, 324, 500, and 997.
- Describe an algorithm for factoring integers.
- Use your algorithm to factor 969969.

Greatest Common Divisors

Definition

Let $a, b \in \mathbb{Z}$, not both 0. The greatest common divisor of a and b, denoted $\gcd(a, b)$, is the largest integer d such that $d \mid a$ and $d \mid b$.

- If $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, then

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}.$$

Prime Numbers

Theorem (True or false?)

For any integers a, b, c,

$$\gcd(a, bc) = \gcd(a, b) \cdot \gcd(a, c).$$

Theorem (True or false?)

For any integers a, b, c,

$$\gcd(a, bc) = \gcd(\gcd(a, b), \gcd(a, c)).$$

Definition (Prime Number)

An integer p is prime if p is not a unit and for any integers a and b, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

- Can we prove that this is equivalent to the original definition?

Outline

Assignment

Assignment

- Read Section 4.3, pages 170 - 177.
- Exercises 5, 12, 13, 15, 18, 23, 28, 29, 30, 36, 37, 40, page 177.