CS 113: Mathematical Structures for Computer Science

Dr. Francis Parisi

Pace University

Fall 2018

Integers

Chapter 7

Integers

- Divisibility Properties
- Primes
- The Division Algorithm
- Congruence
- Greatest Common Divisors
- Integer Representations

Integers – Divisibility Properties

- An integer n is even if $n = 2k$ for some integer k
- An integer n is odd if $n = 2k + 1$ for some integer k

Definition

For integers a and b, with $a \neq b$, we say a **divides** b if $b = ac$ for some integer c. We indicate this by $a \mid b$. If a does not divide b we write $a \nmid b$

- a is a factor (or divisor) of b and b is a multiple of a
- $a|b$ can either be true or false, hence $a|b$ is a statement
- $12|52$ is false and $12|72$ is true *but* $12|72$ has no numerical value

Integers – Divisibility Properties

Exercise

For each pair $a, b \in \mathbb{Z}$ determine whether $a|b$. If yes, find c such that $b = ac$.

(a) $a = 7,\ b = -70$

(b) $a = 16,\ b = -40$

(c) $a = 1,\ b = 10$

(d) $a = 8,\ b = -8$

(e) $a = 14,\ b = 0$

(f) $a = 0,\ b = 14$

Integers – Divisibility Properties

Exercise

Let $a, b \in \mathbb{Z},\ a \neq 0$. Prove that if $a|b$ then $a|(-b)$ and $(-a)|b$.

Integers – Divisibility Properties

Exercise

Disprove the following: Let a and b be integers with $a \neq 0$ and $b \neq 0$. If $a|b$ and $b|a$ then $a = b$.

Integers – Divisibility Properties

Exercise

Prove the following: For every non-negative integer n

$$4 | 5^n - 1.$$

Hint: Use Induction.

Integers – Divisibility Properties

Exercise

Let a, b and c be integers with $a \neq 0$. Prove that if $a|b$ and $a|c$ then

$$a|(bx + cy)$$

for every two integers x and y.

Integers – Divisibility Properties

Exercise

Let a, b and c be integers with $a \neq 0$ and $b \neq 0$. Prove that if $a|b$ and $b|c$ then $a|c$.

Integers – Primes

Definition

A prime is an integer $p \geq 2$ whose only positive integer divisors are 1 and p.

The Fundamental Theorem of Algebra

Theorem

Every integer $n \geq 2$ is either prime or can be expressed as a product of primes, that is

$$n = p_1 p_2 \cdots p_k$$

where $p_1, p_2, \ldots, p_k$ are primes.

Integers – Primes

Tips for determining whether a certain prime p divides an integer n

- $2 \mid n$ if the last digit of n is even
- $4 = 2^2 \mid n$ if 4 divides the last two digits of n
- $8 = 2^3 \mid n$ if 8 divides the last three digits of n
- $2^k \mid n$ if 2^k divides the last k digits of n

- $3 \mid n$ if three divides the sum of the digits of n
- $5 \mid n$ if the last digit is 5 or 0
- $11 \mid n$ if $11 \mid (a - b)$ where a is the sum of alternating digits, and b is the sum of the rest

Integers – Primes

Exercise

Express each of the following as a product of primes.

(a) 30

(b) 12

(c) 100

(d) 605

Integers – Primes

Definition

An integer $n \geq 2$ that is not prime is called a composite number (or just composite).

Theorem

An integer n is composite if and only if there exist integers a and b with $1 < a < n$ and $1 < b < n$ such that $n = ab$

Theorem

There are infinitely many primes

Theorem

Let $\pi(n)$ be the number of primes less than n. Then $\pi(n) \approx n \ln n$.

$$\lim_{n \to \infty} \frac{\pi(n)}{n \ln n} = 1$$

Integers – Primes

Exercise

Prove the following Theorem: There are infinitely many primes.
Hint: Use proof by contradiction.

Integers – Primes

Exercise

Express each of the following as primes.

(a) 250

(b) 297

(c) 2662

(d) 1225

(e) 891

Integers – The Division Algorithm

- When one integer is divided by another we have a quotient and a remainder
- For example, if we divide 18 by 7 we get a quotient of 2 and a remainder of 4

Theorem

For every two integers m and $n > 0$, there exist unique integers q and r such that

$$m = nq + r \text{ where } 0 \leq r < n.$$

- When m is not positive the results may be surprising
- Recall from above that $0 \leq r < n$
- Thus when m is not positive q will be the next multiple up

Integers – The Division Algorithm

Example

Suppose $m = -58$ and $n = 7$

$$m = nq + r \Rightarrow -58 = 7q + r$$

We get $q = -9$ and $r = 5$
$-58 = 7 \cdot (-9) + 5$

Integers – The Division Algorithm

Exercise

For each of the following pairs of integers m, n find q and r when m is divided by n.

(a) $m = 58,\ n = 7$

(b) $m = 0,\ n = 7$

(c) $m = -58,\ n = 7$

(d) $m = 21,\ n = 7$

Integers – The Division Algorithm

Exercise

Determine $\lfloor m/n \rfloor$ and $m - n\lfloor m/n \rfloor$ for each of the following pairs m, n of integers.

(a) $m = 18,\ n = 7$

(b) $m = 0,\ n = 7$

(c) $m = -18,\ n = 7$

Integers – Congruence

- Our interest shifts to integers that have the same remainder when divided by some integer $n \geq 2$
- This is the concept of congruence

Definition

For integers a, b and $n \geq 2$, the integer a is **congruent to** b **modulo** n if $n \mid (a - b)$

- If a is congruent to b modulo n we write $a \equiv b \pmod{n}$
- If not we write $a \not\equiv b \pmod{n}$

Integers – Congruence

There is a convenient way to tell if a is congruent to b modulo n

Theorem

Let a, b and $n \geq 2$ be integers. Then $a \equiv b \pmod{n}$ if and only if $a = b + kn$ for some integer k

Another useful theorem is as follows

Theorem

Let a, b and $n \geq 2$ be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n

Integers – Greatest Common Divisors

Definition

Let a, b and d be integers, where a and b are not both 0 and $d \neq 0$. The integer d is a **common divisor** of a and b if $d \mid a$ and $d \mid b$.

Definition

For integers a and b not both 0 the **greatest common divisor** of a and b is the greatest positive integer that is a common divisor of a and b. This is denoted by $\gcd(a, b)$.

Integers – Greatest Common Divisors

- Finding $\gcd(a, b)$ when the numbers are relatively small is easy
- For larger numbers we make use of the Euclidean algorithm

Theorem

Let a and b be two positive integers. If $b = aq + r$ for some integers q and r, then

$$\gcd(a, b) = \gcd(r, a).$$

Integers – Greatest Common Divisors

- This recursive application leads to the following result

$$\begin{aligned}\gcd(a,b) &= \gcd(r,a) = \gcd(r_1,r) = \gcd(r_2,r_1)\\ &= \cdots = \gcd(r_k,r_{k-1}) = \gcd(0,r_k) = r_k\end{aligned}$$

- The greatest common divisor of a and b is the last non-zero remainder
- The repeated application of the theorem is the Euclidian Algorithm

Integers – Greatest Common Divisors

Example

Suppose we wish to find $\gcd(384, 477)$

$$\begin{aligned}
477 \bmod 384 &= 93 \quad [\gcd(a, b)] \\
384 \bmod 93 &= 12 \quad [\gcd(r, a)] \\
93 \bmod 12 &= 9 \quad [\gcd(r_1, r)] \\
12 \bmod 9 &= 3 \quad [\gcd(r_2, r_1)] \\
9 \bmod 3 &= 0 \quad [\gcd(r_3, r_2)]
\end{aligned}$$

... so the $\gcd(384, 477) = 3$.

Integers – Greatest Common Divisors

- Recall we can express integers as the product of primes
- Suppose we express a and b in terms of the same primes
- We have

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \text{ and } b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \tag{6.1}$$

- Then

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)} \tag{6.2}$$

Integers – Greatest Common Divisors

- We have seen that the $\gcd(a, b)$ is the divisor that divides both a and b
- We now consider those integers that are divisible by both a and b
- These are the Least Common Multiples

Definition

For two positive integers a and b, an integer n is a common multiple of a and b if n is a multiple of a and b. The smallest positive integer that is a common multiple of a and b is the least common multiple of a and b. This number is denoted by $\text{lcm}(a, b)$.

Integers – Greatest Common Divisors

Properties of the $\operatorname{lcm}(a,b)$

1. $b \leq \operatorname{lcm}(a,b) \leq ab$
2. If $a \mid b$, then $\operatorname{lcm}(a,b) = b$
3. If a and b are represented as in (6.1) then

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_k^{\max(a_k,b_k)} \tag{6.3}$$

Finally from equations (6.2) and (6.3)

$$ab = \gcd(a,b)\operatorname{lcm}(a,b)$$

Moreover, with $1 \leq a \leq b$

$$1 \leq \gcd(a,b) \leq a \leq b \leq \operatorname{lcm}(a,b) \leq ab$$

Integers – Greatest Common Divisors

Relatively Prime Integers

- Recall $\gcd(a, b) = a$ if and only if $a \mid b$
- If $\gcd(a, b) = 1$ then no prime divides both a and b

Definition

Two integers a and b, not both 0, are **relatively prime** if $\gcd(a, b) = 1$

Linear Combinations of Integers

Definition

Let a and b be two integers. An integer of the form $ax + by$ where x and y are integers, is a **linear combination** of a and b

Integers – Integer Representations

Consider the integer 5492 and the meaning of each digit in the number. In base 10 we have

$$5492 = 5 \cdot 10^3 + 4 \cdot 10^2 + 9 \cdot 10^1 + 2 \cdot 10^0$$

Theorem

Let $b \geq 2$ be an integer. Then every positive integer n has a unique representation in base b as

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0 b^0,$$

where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b and $a_k \neq 0$

What is the decimal expansion of the following:
$(100101)_2$, $(171)_8$, and $(2A1)_{16}$

Integers – Key Results

- Let a, b and c be integers with $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for every two integers x and y.
- Let a, b and c be integers with $a \neq 0$. If $a \mid b$ and $b \mid c$, then $a \mid c$.
- **The Fundamental Theorem of Algebra:** Every integer $n \geq 2$ is either prime or can be expressed as $n = p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are primes. This factorization is unique except possibly for the order in which the primes appear.
- An integer $n \geq 2$ is composite if and only if there exist integers a and b with $1 < a < n$ and $1 < b < n$ such that $n = ab$.
- If n is a composite number, then n has a prime factor p such that $p \leq \sqrt{n}$.
- There are infinitely many primes.
- **The Prime Number Theorem:** The number $\pi(n)$ is approximately equal to $n / \ln n$. More precisely $\lim_{n \to \infty} \frac{\pi(n)}{n / \ln n} = 1$.

Integers – Key Results

- **The Division Algorithm:** For every two integers m and $n > 0$, there exist unique integers q and r such that $m = nq + r$, where $0 \leq r < n$.
- Let a, b and $n \geq 2$ be integers. Then $a \equiv b \pmod{n}$ if and only if $a = b + kn$ for some integer k.
- Let a, b and $n \geq 2$ be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n.
- Let a, b and $n \geq 2$ be integers. Then $a \equiv b \pmod{n}$ if and only if $a \textbf{ mod } n = b \textbf{ mod } n$.
- Let a and b be two positive integers. If $b = aq + r$ for some integers q and r, then $\gcd(a, b) = gcd(r, a)$.
- **Euclidean Algorithm:** An algorithm to determine $\gcd(a, b)$.
- For every two positive integers a and $b, ab = \gcd(a, b) \times \operatorname{lcm}(a, b)$.
- For every two consecutive integers are relatively prime.

Integers – Key Results

- Let a and b be integers that are not both 0. Then $gcd(a, b)$ is the smallest positive integer that is a linear combination of a and b.
- Two integers a and b are relatively prime if and only if 1 is a linear combination of a and b.
- Let a, b and c be integers with $a \neq 0$. If $a \mid bc$ and $\gcd = 1$ then $a \mid c$.
- Let b and c be integers and p a prime. If $p \mid bc$ then either $p \mid b$ or $p \mid c$.
- Let $a_1, a_2, \ldots, a_n$ be $n \geq 2$ integers and let p be prime. If $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some integer i with $1 \leq i \leq n$
- Let $b \geq 2$ be an integer. Then every positive integer n has a unique repreentation in base b as $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0 b^0$, where k is a non-negative integer, the digits $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b and $a_k \neq 0$.