

CS 2336: Discrete Mathematics

Chapter 4

Properties of the Integers: Mathematical Induction

Instructor: Cheng-Hsin Hsu

Outline

4.1 The Well-ordering Principle: Mathematical Induction

4.2 Recursive Definitions

4.3 The Division Algorithm: Prime Numbers

4.4 The Greatest Common Divisor: The Euclidean Algorithm

4.5 The Fundamental Theorem of Arithmetic

Well-Ordering Principle

- What makes \mathbf{Z} different from \mathbf{Q} and \mathbf{R} ?
- Observation: $\mathbf{Z}^+ = \{x \in \mathbf{Z} \mid x > 0\} = \{x \in \mathbf{Z} \mid x \geq 1\}$
 - but: $\mathbf{Q}^+ = \{x \in \mathbf{Q} \mid x > 0\}$, $\mathbf{R}^+ = \{x \in \mathbf{R} \mid x > 0\}$
- Every nonempty subset X of \mathbf{Z}^+ contains a **least (smallest)** element
 - Why it's not true for \mathbf{Q}^+ and \mathbf{R}^+ ?
- This is called the **Well-Ordering Principle**
 - We say \mathbf{Z}^+ is well-ordered

Principle of Mathematical Induction

- Let $S(n)$ denote an open statement that involves the positive integer variable n
 - $S(1)$ is true and \leftarrow **basis step**
 - When $S(k)$ is true then $S(k+1)$ is true \leftarrow **inductive step**

Then $S(n)$ is true for all n in \mathbf{Z}^+

- Extension:
 - May use $S(k_0)$ instead of $S(1)$ as the basis step
 - Can expand \mathbf{Z}^+ into $\{x \mid x \in \mathbb{Z}, x > n_0\}$, where $n_0 < 0$ is a finite number

Examples

- Ex 4.1: Prove $\sum_{i=1}^n i = \frac{n(n+1)}{2}, \forall n \in \mathbb{Z}^+$
- Ex 4.4: Prove $\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}, \forall n \in \mathbb{Z}^+$
- Ex 4.6: Check if the inductive step of the following (**invalid**) theorem works?

$$S(n) : \sum_{i=1}^n i = \frac{n^2 + n + 2}{2} \quad \forall n \in \mathbb{Z}^+$$

- Ex 4.13: Prove that any integer larger than or equal to 14 can be written as a sum of only 3's and 8's.

Alternative Form

- Let $S(n)$ denote an open statement that involves the positive integer variable n , let $n_0 \leq n_1$ be two positive integers
 - $S(n_0), S(n_0+1), \dots, S(n_1-1), S(n_1)$ are true and
 - When $S(n_0) \dots S(k)$ are true, where $k \geq n_1$ then $S(k+1)$ is true

Then $S(n)$ is true for all $n \geq n_0$

Example

- Ex 4.14 (alternative proof): It is possible to write $14, 15, 16$ using only 3's and 8's:
 - $14=3+3+8$
 - $15=3+3+3+3+3$
 - $16=8+8$

Prove

$S(n)$: n can be written as a sum of 3's and 8's
is true for all positive integer $n \geq 14$

Outline

4.1 The Well-ordering Principle: Mathematical Induction

4.2 Recursive Definitions

4.3 The Division Algorithm: Prime Numbers

4.4 The Greatest Common Divisor: The Euclidean Algorithm

4.5 The Fundamental Theorem of Arithmetic

Explicit Formula

- A sequence of integers may or may not be written in explicit formula (depending on if you can observe a pattern!)
 - 0, 2, 4, 8, 12, 20, ...
 - 1, 2, 3, 6, 11, 20, 37, ...
- For those sequences that do not have explicit formulas, we may define it **recursively**:
 - E.g., $a_0=1$, $a_1=2$, $a_2=3$, and $a_n = a_{n-1} + a_{n-2} + a_{n-3}$
- Not necessary for sequence, but also for general mathematical concepts
 - e.g., conjunction of multiple statements

Recursive Definition

- Ex: 4.17 Considers sets $A_1, A_2, \dots, A_n, A_{n+1}$, where $A_i \subseteq \mathcal{U}$ we define their union **recursively** as

- The union of A_1, A_2 is $A_1 \cup A_2$ ← **base definition**

- The union of A_1, A_2, \dots, A_{n+1} for $n \geq 2$, is given by

$$A_1 \cup A_2 \cup \dots \cup A_n \cup A_{n+1} = (A_1 \cup A_2 \cup \dots \cup A_n) \cup A_{n+1}$$

← **recursive process**

- **Then we have**

$$(A_1 \cup A_2 \cup \dots \cup A_r) \cup (A_{r+1} \cup \dots \cup A_n) = \\ A_1 \cup A_2 \cup \dots \cup A_r \cup A_{r+1} \cup \dots \cup A_n$$

if $n, r \in \mathbb{Z}^+$ where $n \geq 3, 1 \leq r < n$

← **prove this using induction**

Harmonic Numbers

- Define Harmonic numbers H as
 - $H_1 = 1$
 - $H_{n+1} = H_n + 1/(n+1)$ for $n \geq 1$
- Prove $\sum_{j=1}^n H_j = (n+1)H_n - n, \forall n \in \mathbb{Z}^+$
- Another example of recursive definition: factorial
 - $0! = 1$
 - $(n+1)! = (n+1)n!,$ for all $n \geq 0$
- Define even number as a sequence b_0, b_1, b_2, \dots using recursive definition

Fibonacci Numbers

- Define Fibonacci numbers F as

- $F_0=0, F_1=1$

- $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$

- Ex 4.19: Prove $\sum_{i=0}^k F_i^2 = F_k \times F_{k+1}, \forall n \in \mathbb{Z}^+$

Lucas Numbers

- Define Lucas numbers L as
 - $L_0=2, L_1=1$
 - $L_n=L_{n-1}+L_{n-2}$, for $n \geq 2$
- Ex 4.20: Prove: $L_n = F_{n-1} + F_{n+1}$, $\forall n \in \mathbb{Z}^+$

Table 4.2

n	0	1	2	3	4	5	6	7
L_n	2	1	3	4	7	11	18	29

Recursively Defined Set

- Start from an initial set of element with one/multiple rules to create new elements based on the known element
 - All the elements in the recursively defined set either belong to the initial set, or were created by the rules
- Example 4.22: Define the set X recursively by: (i) 1 is in X , and (ii) for each a in X , $a+2$ is also in X .

Outline

4.1 The Well-ordering Principle: Mathematical Induction

4.2 Recursive Definitions

4.3 The Division Algorithm: Prime Numbers

4.4 The Greatest Common Divisor: The Euclidean Algorithm

4.5 The Fundamental Theorem of Arithmetic

Definition 4.1

- For $a, b \in \mathbb{Z}$ and $b \neq 0$, we say that b **divides** a , or $b|a$, if there is an integer n such that $a=bn$. In this case, b is a **divisor** of a and a is a **multiple** of b .
- Properties for $a, b, c \in \mathbb{Z}$
 - $1|a$ and $a|0$
 - $[(a|b) \wedge (b|a)] \Rightarrow a = \pm b$
 - $[(a|b) \wedge (b|c)] \Rightarrow a|c$
 - $a|b \Rightarrow a|bx \ \forall x \in \mathbb{Z}$
 - If $x=y+z$ and a divides two out of three integers, it divides the last one as well
 - $[(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$
 - $a|(x_1x_1 + \cdots + c_nx_n)$ if $a|c_i, \forall 1 \leq i \leq n$

Examples

- Ex 4.23: Do there exist integers x , y , and z , so that $6x+9y+15z=107$?
- Ex 4.24: a , b are two integers and $2a+3b$ is a multiple of 17 . Show that 17 divides $9a+5b$.

Primes and Composite

- **Primes** are integers ($n > 1$) with exactly two positive divisors
- All other integers ($n > 1$) are called **composite**
- Lemma: If $n \in \mathbb{Z}^+$ is composite, then there is a prime p such that $p|n$ ← Well-Ordering Principle
- Theorem: There are infinitely many primes. How to prove it? ← By contradiction

The Division Algorithm

- For any $a, b \in \mathbb{Z}, b > 0$, there exist unique $q, r \in \mathbb{Z}$ with $a = qb + r, 0 \leq r < b$
 - q is called **quotient**
 - r is called **remainder**
 - a is called **dividend**
 - b is called **divisor**
- Ex 4.25: Find the q and r for the following a and b
 - $a = 170, b = 11$
 - $a = -45, b = 8$

Integers in Bases Other than 10

- Ex 4.27: Write 6137 in the octal system (base 8). In other words, find r_0, r_1, \dots, r_k so that $(6137)_{10} = (r_k \dots r_2 r_1 r_0)_8$.
- Ex 4.28: write 3387 into binary (base 2) and hexadecimal (base 16).

		Remainders
8	$\overline{6137}$	
8	$\overline{767}$	$1(r_0)$
8	$\overline{95}$	$7(r_1)$
8	$\overline{11}$	$7(r_2)$
8	$\overline{1}$	$3(r_3)$
	0	$1(r_4)$

		Remainders	
16	$\overline{13,874,945}$		
16	$\overline{867,184}$	1	(r_0)
16	$\overline{54,199}$	0	(r_1)
16	$\overline{3,387}$	7	(r_2)
16	$\overline{211}$	11 (= B)	(r_3)
16	$\overline{13}$	3	(r_4)
	0	13 (= D)	(r_5)

Negative Integers

- Question: How to represent negative integers x in binary?
 - One's complement: write $|x|$ in binary, and replace each 0 (1) with 1(0)
 - Two's complement: add 1 to one's complement
- Ex 4.29: Write -5 as two's complement in 4- and 8-bit integers
- Ex 4.30: Perform the subtraction $33-5$ in base 2 8-bit integers ← observe the overflow, in this case we discard the left-most bit

Outline

4.1 The Well-ordering Principle: Mathematical Induction

4.2 Recursive Definitions

4.3 The Division Algorithm: Prime Numbers

4.4 The Greatest Common Divisor: The Euclidean Algorithm

4.5 The Fundamental Theorem of Arithmetic

Common Divisor

- For $a, b \in \mathbb{Z}$, $c > 0$ is a common divisor of a and b if $c|a$ and $c|b$
- Let $a, b \in \mathbb{Z}$, where $a \neq 0$ or $b \neq 0$. Then $c \in \mathbb{Z}^+$ is a **greatest common divisor** of a and b if
 - $c|a, c|b$
 - For any common divisor d of a and b , we know $d|c$
- Theorem 4.6 For all $a, b \in \mathbb{Z}^+$ there exists a unique greatest common divisor of a and b , written as $\gcd(a, b)$ ← Well-Ordering Principle, $\gcd(a, b)$ is actually the smallest positive integer that can be a linear combination of a and b

A Few Facts on GCD

- $\gcd(a,b) = \gcd(b,a)$
- $\gcd(a,0) = |a|$, for any nonzero a
- $\gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b) = \gcd(a,b)$
- $\gcd(0,0)$ is undefined.

- Integer a and b are relatively prime if $\gcd(a,b) = 1$
 - If there exist integers x and y , so that $ax + by = 1$

Euclidean Algorithm

$$\begin{array}{r}
 22 \quad 250 \\
 \underline{242} \\
 8 \\
 \underline{6} \\
 2 \\
 \underline{2} \\
 0
 \end{array}
 \quad
 \begin{array}{r}
 11 \\
 \underline{8} \\
 3 \\
 \underline{2} \\
 1
 \end{array}
 \quad
 \begin{array}{l}
 1 \\
 1
 \end{array}$$

	Quotient	Remainder
	↓	↓
$250 =$	$22 \times$	$11 + 8$
$11 =$	$1 \times$	$8 + 3$
$8 =$	$2 \times$	$3 + 2$
$3 =$	$1 \times$	$2 + 1$
$2 =$	$2 \times$	$1 + 0$

- Then, r_n , the last nonzero remainder, equals $\gcd(a,b)$
- Ex 4.34: Find the $\gcd(250,11)$?

Examples

- Ex 4.35: Prove that $8n+3$ and $5n+2$ are relative prime
- Ex 4.36: Realize the Euclidean algorithm

```
$ cat GCD.java
```

```
public class GCD{  
    public static void main(String[] args) {  
        // a, b are positive integers  
        int a = 120, b = 32;  
        int r = a % b;  
        int d = b;  
        while (r > 0) {  
            int c = d;  
            d = r;  
            r = c % d;  
        }  
        // gcd(a,b) is d the last nonzero remainder  
        System.out.println("gcd(" + a + ", " + b + ") = " + d);  
    }  
}
```

```
$ java GCD
```

```
gcd(120, 32) = 8
```

Diophantine Equation

- For positive integers a, b, c , the Diophantine equation $ax+by=c$ has an integer solution $x=x_0, y=y_0$ if $\gcd(a,b)$ divides c
- Ex 4.38: Brian can debug a Java program in 6 mins and a C++ program in 10 mins. If he continuously works for 104 mins and doesn't waste any time, how many programs can he debug in each languages?
 - Basically find integers x and y so that $6x+10y=104$

Common Multiple

- Let $a, b \in \mathbb{Z}^+$. c is a **common multiple** of a and b . c is the **least common multiple** if it is the smallest positive common multiple of a, b , we write $c = \text{lcm}(a, b)$
- If $a, b \in \mathbb{Z}^+$ and $c = \text{lcm}(a, b)$. For any d that is a common multiple of a and b , we know $c \mid d$
- Thm 4.40: For all $a, b \in \mathbb{Z}^+$, $ab = \text{lcm}(a, b)\text{gcd}(a, b)$

Outline

4.1 The Well-ordering Principle: Mathematical Induction

4.2 Recursive Definitions

4.3 The Division Algorithm: Prime Numbers

4.4 The Greatest Common Divisor: The Euclidean Algorithm

4.5 The Fundamental Theorem of Arithmetic

Fundamental Theorem of Arithmetic

- Lem 4.2: If $a, b \in \mathbb{Z}^+$ and p is a prime, then $p|ab \Rightarrow p|a$ or $p|b$
- Lem 4.3: Generalize Lem 4.2 to n positive integers
- Thm 4.11: Integer $n > 1$ can be written as a (unique) product of primes

- Ex 4.42: What is the prime factorization of 980,220?

- Ex 4.43: Prove that $17|n$ given

$$10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot n = 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14$$

Examples

- Ex 4.44: Count the number of positive divisors of 360.

- Ex 4.45: Let $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, $n = p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$, with $e_i, f_i \geq 0, \forall e_i, f_i$ we have

$$\gcd(m, n) = \prod_{i=1}^t p_i^{a_i}, \text{ and } \text{lcm}(m, n) = \prod_{i=1}^t p_i^{b_i},$$

where $a_i = \min(e_i, f_i)$, $b_i = \max(e_i, f_i)$

- Find the gcd and lcm of $491891400 = 2^3 3^3 5^2 7^2 11^1 13^2$
and $1138845708 = 2^2 3^2 7^1 11^2 13^3 17^1$

Take-home Exercises

- Exercise 4.1: 2, 8, 16, 19, 26
- Exercise 4.2: 1, 8, 10, 12, 16
- Exercise 4.3: 7, 15, 20, 22, 28
- Exercise 4.4: 1, 2, 7, 14, 19
- Exercise 4.5: 1, 2, 8, 24, 25