CS182 Spring 2016: Homework 7

Due date: Friday, April 15, 2016 (before class).

1. Number Theory and Cryptography

   (a) Let n be a positive integer such that $n = d_k d_{k-1} \dots d_1$ where $d_i \in \{0, 1, \dots, 9\}$ (each d_i is a digit of n). Prove that $n \mod 3 = 0$ if and only if $\left(\sum_{i=1}^{k} d_i\right) \mod 3 = 0$.

   (b) Given an 11-digit number $x = x_{11}x_{10}\dots x_1$, this number is a USPS valid money order number if and only if $x_{11} = x_1 + x_2 + \cdots + x_{10} \mod 9$. In the following questions, let Q denote a digit that has been lost. Recover the smudged digit if possible. (Note: any answer without justification/work shown will receive minimal credit)

      i. $Q1223139784$

      ii. $6702120Q988$

      iii. $213279032Q1$

   (c) Find all solutions, if any, to the system of congruences:

$$\begin{aligned} x &\equiv 5 \pmod{6} \\ x &\equiv 3 \pmod{10} \\ x &\equiv 8 \pmod{15} \end{aligned}$$

2. Basic Induction Proofs

   (a) Let $a_n = \sum_{i=0}^{n} 2(-7)^i$. Prove that for all $n \geq 0, n \in \mathbb{Z}$, $a_n = (1 - (-7)^{n+1})/4$ using induction.

   (b) Suppose $a, b \in \mathbb{R}$ such that $0 < b < a$. Prove using induction that for any $n \in \mathbb{Z}^+$, we have $a^n - b^n \leq na^{n-1}(a - b)$.

3. Strong Induction Proofs

   (a) Show that for all $n \in \mathbb{Z}^+$, n can be written as the sum of distinct powers of 2. (Consider two cases for your inductive step: one where $k+1$ is odd and one where $k+1$ is even. Remember, when $k+1$ is even, then $(k+1)/2$ is an integer).

   (b) Prove that if $n \in \mathbb{Z}^+$ such that $n \geq 18$, then n can be expressed as $n = 4x + 7y$, where $x, y \in \mathbb{Z}^+ \cup \{0\}$ (Note: you will need $n = 18, 19, 20, 21$ for your base cases).

4. Recursive Definitions

   (a) Let $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ be the Fibonacci numbers, where F_n is the n^{th} Fibonacci number defined when $n \geq 2$. Prove that for any $n \in \mathbb{Z}^+$, $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

(b) Suppose you are given n real numbers $a_1, \ldots, a_n$ and you want to find the maximum of those numbers. Give a recursive definition for the function $f(a_1, \ldots, a_n) = \max\{a_1, \ldots, a_n\}$ and prove that this function indeed returns the maximum of these n real numbers.

(c) Let $S = \{(a, b) \colon (a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \text{ and } a + b \text{ is odd}\}$. Give a recursive definition for this set.

5. Recursive Algorithms

(a) Given $x, n, m \in \mathbb{Z}^+$, write a recursive algorithm to compute $x^n \mod m$ given the fact that $x^n \mod m = (x^{n-1} \mod m \cdot x \mod m) \mod m$. Prove that your algorithm is correct.

(b) Give an $\mathcal{O}(n)$-time recursive algorithm to compute the n^{th} Fibonacci number.

6. Program Correctness

(a) Verify that the program segment

`if` $x < 0$ `then` $x := 0$

is correct with respect to the initial assertion **True** and the final assertion $x \geq 0$.

(b) Develop rules of inference for the verification of partial correctness of the following program:

`if` $x < 0$ `then`
  $y := -2|x|/x$
`else if` $x > 0$ `then`
  $y := 2|x|/x$
`else if` $x = 0$ `then`
  $y := 2$

then verify that the program is correct with respect to the initial assertion **True** and the final assertion $y = 2$.

7. Counting

(a) Let $S = \{1, 2, \ldots, 100\}$. How many subsets of S have exactly 2 elements?

(b) How many bit strings of length 10 contain either 5 consecutive 0s or 5 consecutive 1s?

(c) How many functions are there from the set $\{1, 2, \ldots, n\}$ $(n \geq 4)$ to the set $\{0, 1, 2\}$ that are

i. one-to-one?

ii. assign exactly 3 numbers less than n to 0?