Math 55: Sample Midterm 1, 9 December 2009

Write your name, your student ID number, your section time and number, and a three-problem grading grid, on the cover of your blue book. Remain in your seat and hand in your exam book at 3:30 pm. Books, notes, calculators, scratch paper and/or collaboration are not allowed. Justify your computations: correct answers with inadequate explanation may receive partial credit.

1: Define a sequence a_n recursively by $a_0 = 1$ and $a_{n+1} = \sum_{j=0}^{n} a_j$ for $n \geq 0$.
(a) Compute a_0, a_1, …, a_5.
(b) State a closed formula for the sum S of a geometric series $S = \sum_{j=0}^{n-1} r^j$ with ratio $r \neq 1$.
(c) Use strong induction to prove that $a_n = 2^{n-1}$ for $n \geq 1$.

2: Consider the following pseudocode:

```
$G(n \in \mathbf{N}, m \in \mathbf{N}, \textbf{function } f : \{0,1,2,\ldots,n-1\} \to \{0,1,2,\ldots,m-1\})$
    for $i := 0$ to $m-1$
        $h_i := 0$
    end
    for $j := 0$ to $n-1$
        $i := f(j)$
        $h_i := h_i + 1$
    end
    for $i := 0$ to $m-1$
        if $(h_i \neq 1)$ then return F
    end
    return T
end
```

(a) What function of f, n and m does G return?
(b) What is its worst-case complexity in terms of m and n in big-O notation? Justify your answer.
(c) Let $n = m > 2$. For what values of $a \in \mathbf{Z}$ does G return T for the function f defined by $f(j) = aj \bmod n$?

3: **(a)** Compute $(7 \times 11 \times 711 \times 777) \bmod 13$ by modular arithmetic.
(b) Compute $666^{77} \bmod 11$.

4: **(a)** Define what it means for a compound proposition to be a tautology.
(b) Use a truth table to determine whether $((p \vee q) \wedge (p \rightarrow r)) \rightarrow (q \vee r)$ is a tautology by the definition of (a). Explain why your answer is intuitively reasonable.
(c) Verify the result of (b) by applying logical equivalences. State which equivalence you are using at each step.

5: (20 points)
(a) How many integers x between 0 and $7 \cdot 8 \cdot 9 - 1$ inclusive satisfy the system of congruences

$$\begin{aligned} x &\equiv 0 \pmod 7 \\ x &\equiv 1 \pmod 8 \\ x &\equiv 2 \pmod 9 ? \end{aligned}$$

Justify your answer.
(b) Find integers x_1, x_2 and x_3 such that $x = x_1 \cdot 8 \cdot 9 + x_2 \cdot 7 \cdot 9 + x_3 \cdot 7 \cdot 8$ solves the congruences in (a).

6: (20 points) Define a sequence a_n by $a_0 = 7$, $a_1 = 14$ and $a_n = 2a_{n-1} + a_{n-2}$ for $n \geq 2$. Use strong induction to prove that $7 | a_n$ for $n \geq 0$.

7:

(a) Use a truth table to show $p \rightarrow q \Leftrightarrow \neg p \vee q$.

(b) Show by applying logical equivalences that $p \wedge (p \rightarrow q) \rightarrow q$ is a tautology. State which logical equivalence is used at each step.

8: Define $\mathbf{Z}^+ = \{1, 2, 3, \ldots\}$ and

$$\mathbf{Q}^+ = \{p/q \mid p \in \mathbf{Z}^+ \wedge q \in \mathbf{Z}^+ \wedge \gcd(p, q) = 1\}.$$

Define $f : \mathbf{Q}^+ \rightarrow \mathbf{Z}^+$ by $f(p/q) = p + q - 1$. Justify your answers to the following questions.

(a) Is f onto?

(b) Do $\mathbf{Z}^+$ and $\mathbf{Q}^+$ have the same cardinality?

9:

(a) Run the Euclidean algorithm to compute $\gcd(32, 7)$.

(b) Find an inverse d of $7 \pmod{32}$ with $0 \leq d < 32$. Verify your result.

(c) Use the procedure of the Chinese Remainder Theorem to find an integer x such that $0 \leq x < 51$ and

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 9 \pmod{17} \end{aligned}$$

Verify your result.

10: (20 points) Let $\mathbf{Z}$ be the set of integers and define $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ by $f(s, t) = 13s + 8t$.
(a) Is f 1-1? Why or why not?
(b) Is f onto? Why or why not?
(c) Find integers s and t such that $4 = 13s + 8t$.
(d) Find an integer solution t of the congruence $8t \equiv 4 \pmod{13}$ satisfying $0 \leq t < 13$.

11: (20 points) Consider the following pseudocode:

```
function $G$(set $A = \{a_1, a_2, \ldots, a_n\}$, set $B = \{b_1, b_2, \ldots, b_m\}$, function $f : A \to B$)
    for $i := 1$ to $m$
    begin
        $h := 0$
        for $j := 1$ to $n$
        begin
            if $(f(a_j) = b_i)$ then $h := h + 1$
        end
        if $(h \neq 1)$ then return F
    end
    return T
```

(a) What function of f, A and B does G return?
(b) What is its worst-case complexity in terms of m and n in big-O notation?

12: (10 points) Assume that every subset of a countable set is countable. Let A be an uncountable set and B be another set such that $A \subset B$. Prove B is uncountable.

13: (10 points) Prove that $(p \wedge q) \to (p \vee q)$ is a tautology without using a truth table. Justify each step.

14: Consider the following pseudocode:

```
function $G$(set $A = \{a_1, a_2, \ldots, a_n\}$, set $B = \{b_1, b_2, \ldots, b_m\}$, function $f : A \to B$)
    for $i := 1$ to $m$
        $h := 0$
        for $j := 1$ to $n$
            if $(f(a_j) = b_i)$ then $h := h + 1$
        end
        if $(h \neq 1)$ then return F
    end
    return T
```

(a) What function of f, A and B does G return?
(b) What is its worst-case complexity in terms of m and n in big-O notation? Give constants C and k and justify your answer.
(c) Modify the pseudocode to reduce the worst-case complexity to $O(m+n)$.
(d) Let $p > 2$ be a positive integer and $A = B = \{0, 1, 2, \ldots, p-1\}$. For what values of $a \in \mathbf{Z}$ does G return T for the function $f : A \to B$ defined by $f(n) = an \bmod p$?

15: **(a)** State Fermat's little Theorem.
(b) Use Fermat's little Theorem and modular arithmetic to compute $555^{555} \bmod 17$.
(c) Run the Euclidean algorithm forward and backward to find an inverse of $15 \pmod{17}$.

(d) State the Chinese Remainder Theorem for the case when there are three moduli m_1, m_2 and m_3.
(e) Use the Chinese Remainder Theorem and modular arithmetic to compute $555^{555} \bmod 255$.

16: **(a)** Build a truth table with columns for $p \to q$, $p \wedge (p \to q)$, and so forth to determine whether $(p \wedge (p \to q)) \to q$ is a tautology. Explain why your answer is intuitively reasonable.
(b) Verify the result of (a) by applying logical equivalences. State which equivalence you are using at each step.
(c) Prove that for any sets A, B and C we always have

$$A \cap (\bar{A} \cup B) \subset B.$$

17: Define the Fibonacci numbers by

$$f_0 = 0, \quad f_1 = 1, \quad f_{n+1} = f_n + f_{n-1} \text{ for } n \geq 1.$$

The first few are

$$f_0 = 0, f_1 = 1, f_2 = 1, \ f_3 = 2, \ f_4 = 3, \ f_5 = 5, \ f_6 = 8, \ f_7 = 13, \ \ldots$$

(a) Write each positive integer $n \leq 12$ as a sum of one or more *distinct* Fibonacci numbers. The first few are

$$1 = f_2, \ 2 = f_3, \ 3 = f_4, \ 4 = f_4 + f_2, \ 5 = f_4 + f_3 = f_5, \ldots$$

(b) Given a positive integer n, how is the sequence $(b_2, b_3, \ldots, b_m)$ produced by the following procedure related to n? Justify your answer with a step-by-step analysis.

```
procedure $B$( $n$ : positive integer )

$m := 1$
while $f_{m+1} \leq n$
begin
        $m := m + 1$
```

```
        $b_m := 0$
end

while $m \geq 2$
begin
        if $f_m \leq n$ then
        begin
                $n := n - f_m$
                $b_m := 1$
        end
        $m := m - 1$
end
```

(c) What is the worst-case complexity of $B(n)$ in terms of n in big-O notation? You may use the following formula, which we proved in class:

$$f_m = \frac{1}{\sqrt{5}} \left(\varphi^m - (1 - \varphi)^m \right)$$

where

$$\varphi = \frac{1}{2} \left(1 + \sqrt{5} \right) = 1.618 \ldots.$$

Justify your answer with a detailed analysis.

(d) Prove by induction that *every* positive integer n can be written as a sum of one or more *distinct* Fibonacci numbers. (Hint: Choose m so that $f_m \leq n < f_{m+1}$ and let $k = n - f_m$.)

(e) The representation of some integers n as a sum of distinct Fibonacci numbers is not unique. What additional requirement do you think will make the representation unique? (Hint: $f_{n+1} = f_n + f_{n-1}$.)