MTH150

Midterm Exam 2

November 7, 2006

NAME (please print legibly): _____

Your University ID Number: _____

- **On each of the four sections A, B, C, D, complete all but one problem. Circle the numbers of the problems (on this page) from each section that you want counted toward your score.**
- **Show your work and justify your answers. You may not receive full credit for a correct answer if insufficient work is shown or insufficient justification is given.**
- **No calculators are allowed on this exam.**

Part A		
QUESTION	VALUE	SCORE
1	10	
2	10	
3	10	
TOTAL	20	

Part B		
QUESTION	VALUE	SCORE
1	10	
2	10	
3	10	
TOTAL	20	

Part C		
QUESTION	VALUE	SCORE
1	10	
2	10	
3	10	
4	10	
5	10	
TOTAL	40	

Part D		
QUESTION	VALUE	SCORE
1	10	
2	10	
3	10	
TOTAL	20	

Part A

1. (10 points)

Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{0, 3, 6\}$. Find

(a) $A \cup B$

(b) $A \cap B$

(c) $A - B$

(d) $B - A$

2. (10 points)

Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ that is

(a) one-to-one but not onto.

(b) onto but not one-to-one.

(c) both onto and one-to-one (but different from the identity function).

(d) neither one-to-one nor onto.

3. (10 points)

(a) For each of these lists of integers, provide a simple formula that generates the terms of an integer sequence that begins with the given list.

(i) $3, 6, 12, 24, 48, 96, 192, \ldots$

(ii) $3, 6, 9, 12, 15, 18, 21, \ldots$

(b) Compute each of these double sums.

(i) $\displaystyle\sum_{i=1}^{2}\sum_{j=1}^{3}(i+j)$

(ii) $\displaystyle\sum_{i=1}^{2}\sum_{j=1}^{3}ij$

Part B

1. (10 points)

Use bubble sort to sort 3, 1, 5, 7, 4, showing the lists obtained at each step.

procedure *bubble sort*($a_1, a_2, \ldots, a_n$: real numbers with $n \geq 2$)
for $i := 1$ **to** $n - 1$
    for $j := 1$ **to** $n - i$
        if $a_j > a_{j+1}$ **then** interchange a_j and a_{j+1}
{$a_1, \ldots, a_n$ is in increasing order}

2. (10 points)

(a) Show that $2n^2 + 6$ is $O(n^2)$. [Hint: Just find C and k that work.]

(b) Show that n^3 is not $O(n^2)$. [Hint: Show that no such C and k can exist.]

3. (10 points)

Determine the most number of comparisons, or worst-case performance, required to sort a list of n elements using bubble sort. [Hint: $1 + 2 + \cdots + m = m(m+1)/2$.]

procedure *bubble sort*($a_1, a_2, \ldots, a_n$: real numbers with $n \geq 2$)
for $i := 1$ **to** $n - 1$
    for $j := 1$ **to** $n - i$
        if $a_j > a_{j+1}$ **then** interchange a_j and a_{j+1}
{$a_1, \ldots, a_n$ is in increasing order}

Part C

1. (10 points)

(a) Evaluate these quantities.

(i) $13 \bmod 3$

(ii) $-97 \bmod 11$

(b) Find the prime factorization of each of these integers.

(i) 193 [Hint: $\sqrt{193} \approx 13.8$.]

(ii) 1001 [Hint: $\sqrt{1001} \approx 31.6$.]

2. (10 points)

(a) Convert these integers from decimal notation to binary notation.

(i) 94

(ii) 231

(b) Use the Euclidean algorithm to find

(i) $\gcd(111, 201)$.

(ii) $\gcd(1001, 1331)$.

3. (10 points)

(a) Use the extended Euclidean algorithm to express $\gcd(35, 78)$ as a linear combination of 35 and 78.

(b) Solve the congruence $35x \equiv 6 \pmod{78}$ if possible. If there is a solution, give one satisfying $0 \leq x < 78$. If there is no solution, state so and explain.

4. (10 points)

(a) Use the modular exponentiation algorithm to compute 7^{26} **mod** 20 showing the values of x and *power* an each step. [Hint: $(26)_{10} = (11010)_2$.]

procedure *modular exponentiation* (b: integer, $n = (a_{k-1}a_{k-2}\dots a_1a_0)_2$, m: positive integers)
$x := 1$
$power := b$ **mod** m
for $i := 0$ **to** $k - 1$
    if $a_i = 1$ **then** $x := (x \cdot power)$ **mod** m
    $power := (power \cdot power)$ **mod** m
$\{x = b^n$ **mod** $m\}$

(b) Use Fermat's Little Theorem to compute 5^{601} **mod** 7.

5. (10 points)

Consider the RSA encryption system with $n = 10403$ and $e = 1001$.

(a) What is the encryption function?

(b) What would you first have to know in order to find the decryption function?

(c) Given your answer to part (b), explain how to find d.

(d) Given d, what is the decryption function?

Part D

1. (10 points)

(a) Conjecture a formula for

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)}$$

by examining the values of this expression for small values of n.

(b) Prove the formula you conjectured in part (a) using induction.

2. (10 points)

(a) Conjecture which amounts of postage can be formed using just 3-cent and 5-cent stamps.

(b) Prove the answer you conjectured in part (a) using strong induction.

3. (10 points)

(a) Find $f(4)$ if $f(n)$ is defined recursively by $f(0) = 0$ and $f(n+1) = f(n)^2 + f(n) + 1$ for each $n \in \mathbb{N}$.

(b) Give a recursive definition of the sequence $\{a_n\}$ defined by $a_n = 6n$ for each $n \in \mathbb{N}$.

(c) Give a simple description of the set S defined recursively by $7 \in S$ and $x - y \in S$ whenever $x \in S$ and $y \in S$.