EXAM 2 solutions (COT3100, Sitharam, Spring 2017)

NAME:last_____first:_____

UF-ID _____

Section _____

NOTE: You have 2 hours, please plan your time. Problems are not ordered by difficulty.

(1) Are the following functions one-to-one (injective)? Onto (surjective)? **Fill in the table with T/F and give a 1 line argument below for each "F" answer:**
$\mathbb{R}$ – the set of all real numbers
$\mathbb{R}^+$ – the set of all positive real numbers
$\mathbb{N}$ – the set of natural numbers $\{1, 2, 3, ...\}$
$\mathbb{Z}$ – the set of all integers $\{... - 3, -2, -1, 0, 1, 2, 3...\}$

Domain	CoDomain	function	0ne-to-one	onto
$f : \mathbb{R}$	$\to \mathbb{R}$	$f(x) = 3$	$--$	$--$
$f : \mathbb{Z}$	$\to \mathbb{Z}$	$f(x) = x + 1$	$--$	$--$
$f : \mathbb{N}$	$\to \mathbb{N}$	$f(x) = x + 1$	$--$	$--$
$f : \mathbb{R}^+$	$\to \mathbb{R}^+$	$f(x) = x^2$	$--$	$--$
$f : \mathbb{N}$	$\to \mathbb{N}$	$f(x) = x^2$	$--$	$--$
$f : \mathbb{N}$	$\to \mathbb{R}$	$f(x) = \log x$	$--$	$--$

Solution.

One-to-one	Onto	Reason
F	F	Not one-to-one because $f(1) = f(2)$. Not onto because no x maps to 1
T	T	
T	F	Not onto because there is no $x \in \mathbb{N}$ such that $f(x) = 1$
T	T	
T	F	Not onto because there is no $x \in \mathbb{N}$ such that $f(x) = 2$
T	F	No negative numbers are in the codomain

(2) Let f and g be functions such that $f : A \to B$ and $g : B \to A$, where A and B are finite sets. **Show that the composition $g \circ f : A \to A$ has a nice property: it is onto(surjective) if and only if it is one-to-one(injective).**

Solution.

Notice that $g \circ f$ has A as both its domain and codomain.

If $g \circ f$ is not one-to-one, since A and B are finite sets, the size of the image of $g \circ f$ will be less than the size of the domain A, that is, the image of $g \circ f$ cannot be the entire codomain A. So $g \circ c$ cannot be onto.

If $g \circ f$ is one-to-one, since A and B are finite sets, the size of the image of $g \circ f$ will equal to the size of the domain A, that is, the image of $g \circ f$ is the entire codomain A. So $g \circ f$ is onto.

(3) **Prove that the set of pairs** (a, b) **where** a **and** b **are rational is a countable set**.

Solution:
We know that $\mathbb{N} \times \mathbb{N}$ is countable. (Proved in the class with a picture – linearly order or walk through the lattice of pairs (p, q)). We know the set of rational numbers $\mathbb{Q}$ has at most the cardinality of $\mathbb{N} \times \mathbb{N}$, and hence countable, because there is a surjective function mapping a rational number p/q to $(p, q) \in \mathbb{N} \times \mathbb{N}$.

Since $\mathbb{Q}$ is countable, define bijection $f : \mathbb{N} \to \mathbb{Q}$, and from it the bijection $F : \mathbb{N} \times \mathbb{N} \to \mathbb{Q} \times \mathbb{Q}$ by $F(n, m) = (f(n), f(m))$. Therefore $\mathbb{Q} \times \mathbb{Q}$ is also countable since $\mathbb{N} \times \mathbb{N}$ is.

(4) **Prove the following using the definition of decimal representation of a number.** For any 3 numbers $a, b, c \in \{0, 1, \ldots, 9\}$, the decimal numbers $abcabc$ and abc – constructed from the digits a, b, c – satisfy:

$$\frac{abcabc}{1001} = abc.$$

Solution.
$abcabc \div 1001 = (abc * 1000 + abc) \div 1001$
$= ((1000 + 1) * abc) \div 1001$
$= abc$

(5) You are given 9 coins that look alike and you are told that one of them is fake and that it is very slightly lighter than the others. You are given a precision balance, using which you can weigh sets of coins against each other: i.e., you can tell if the left side is heavier or lighter than the right side but you are not given any standard weights or scales. **What is the minimum number of weighings with which you can find the fake coin. Prove your answer.** *Hint:* what is the maximum fraction of coins can be eliminated in the worst case, after each weighing?

Solution.
This was explained in class.

The minimum number of weighings required is 2. First, pick any 6 coins and weigh them on the balance, 3 on each side. If one side is lighter, the fake is among the 3 coins on that side; if two sides balance, the fake is among the remaining 3 coins; either way we eliminate 6 coins. Now weigh any 2 coins

from the remaining 3 on the balance, 1 on each side. If one of them is lighter, that one is fake; if they balance, the remaining one is fake.

Proof of minimality: notice that in a weighing, we divide all coins under consideration into three sets: the left side, the right side, and the remaining. After the weighing we can possibly eliminate two of these sets. Since our division is arbitrary, the fake coin can be in the set with the largest cardinality which is at least 1/3. I.e., at least 1/3 of the coins will remain. In the end one of the sets must have size 1 (the fake coin). In the first weighing, this largest set cannot have size 1 as we have 9 coins to consider, therefore we cannot guarantee to find the fake using only 1 weighing.

(6) Show that if coin denominations are $k^0, k^1, k^2, .., k^m$, where k, m are positive integers, then the *greedy* algorithm for making change (finding a set of coins of equal total value) for any input positive integer x guarantees the smallest number of coins in the change. *Hint:* Start with $k = 2$ and $m = 3$, prove it, then extend the proof to arbitrary k and m.

Solution:

This problem is directly from the assigned homework. One way to see this problem is finding the base k representation of the input amount. Each digit gives the number of coins needed of value k^m, where m is the place of the digit. Clearly you can get this representation by using a greedy algorithm. The algorithm begins by using as many coins of value k^m as it can. This leaves a value $n_1 < k^m$. Hence, we can use at most $k - 1$ coins of value k^{m-1} leading to a value $n_2 < k^{m-1}$. Here the sum of the digits is the number of coins needed. So the question is whether a nongreedy algorithm can get fewer coins than the sum of the digits in base k representation. Suppose to the contrary, and that it helps to take j fewer k^i coin than the greedy algorithm would. Now the difference jk^i has to be covered by fewer than j coins of denominations k^{i-1} or less, which is impossible.

(4) Write an algorithm that merges two input sorted lists of size n into a single sorted list of size $2n$. The number of steps your algorithm executes should be $O(n)$. Prove that your algorithm is correct.

Solution:

This was explained in class.

For convenience pad the given sorted lists $l1$ and $l2$ into arrays of size $2n$ putting n copies of $\max(l1(n), l2(n)) + 1$ into the last n entries of both arrays. The padding takes no more than $O(n)$ steps. From the pseudocode below, you can see that those last n entries will never make their way into $l3$. The pseudocode has a single for loop that uses n iterations of $O(1)$ steps, so the algorithm takes no more than $O(n)$ steps.

```
Merge (l1, l2)
// Input:  l1 and l2 are two sorted lists of size 2n
// Output: A sorted list l3 of elements in l1 and l2
```

```
top1 :=1; top2 := 1;
For i from 1 to 2n
if l1(top1) <= l2(top2)
then l3(i) := l1(top1)
top1 = top1+1
else
then l3(i) := l2(top2)
top2 = top2+1
return l3
```

(8) (8a) Show the following for n, m positive integers, with $m \geq n$. $\gcd(m, n) =$

1. m if $m = n$
2. 2*gcd$(m/2, n/2)$ if m, n, both even
3. gcd$(m/2, n)$, if m is even and n is odd
4. gcd$(m - n, n)$ if m and n are odd.

(8b) Use (8a) to design a gcd algorithm for two input positive integers, using only comparisons, subtractions, and shifts of binary numbers (i.e, division by 2), without using any other divisions.
(8c) Give a complexity analysis of your algorithm in terms of m and n.

Solution.
(8a)

1. If $m = n$, $\gcd(m, m) = m$, as $m \mid m$, and m is the maximum integer that divides m.
2. If m, n are both even, $2 \mid \gcd(m, n)$. Let $m = 2s, n = 2t, \gcd(c, d) = 2u$ for positive integers s, t and u. Now $2u$ is the maximum integer dividing $2s$ and $2t$, so u is the maximum integer dividing s and t, that is, $u = \gcd(s, t)$, i.e. $\frac{\gcd(c,d)}{2} = \gcd(\frac{m}{2}, \frac{n}{2})$.
3. If m is even and n is odd, 2 cannot be a factor of $\gcd(m, n)$. Therefore, we can divide m by 2 without affecting the value of gcd.
4. $\gcd(m - n, n) = \gcd(m, n)$ directly comes from Euclid's algorithm.

(8b)

```
gcd (m, n)
// Input:  m and n are two positive integers
// Output: gcd(m,n)
if m = n
  return m
// &: bitwise and; >>: shift right; <<: shift left
if m & 1 = 0 and n & 1 = 0  // both m and n are even
  t = gcd(m>>1, n>>1)
  return t<<1
if m & 1 = 0  // only m is even
  return gcd(m>>1, n)
if n & 1 = 0  // only n is even
  return gcd(m, n>>!)
// both m and n are odd
if m < n
  temp = m; m = n; n = temp
return gcd(m-n, n)
```

(8c) The time complexity of the algorithm is $O(\log m)$ assuming $m \geq n$. In each recursive calling of the procedure gcd, if at least one parameter is even, at least one parameter is halved; if both parameters are odd, $m-n$ will be even and in the next recursive calling at least one parameter is halved. So the time complexity is at most $2(\log m + \log n)$ which is $O(\log m)$.

(9) Show that
(9a) $x^2 = 1 \bmod p$ for p prime implies $x = 1 \bmod p$ or $x = -1 \bmod p$.*Hint*: recall that $-1 = p - 1 \bmod p$; factor a polynomial and use contrapositive.
(9b) Show that for $p > 2$ the set of numbers from 2 to $p-2$ can be split into a $(p-3)/2$ pairs that are inverses of each other mod$p$, i.e, pairs (a, b) such that $a.b = 1 \bmod p$
(9c) Use (9a) and (9b) to show that the product $(p-1)(p-2)\ldots 1 = -1 \bmod p$.
(9d) Where did you use the fact that p is prime?

Solution.

(9a) $x^2 \equiv 1 \pmod p \implies p \mid (x^2-1) \implies p \mid (x+1)(x-1)$. Since p is a prime, $p \mid (x+1)$ or $p \mid (x-1)$, that is, $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$.

(9b) Since p is prime, any integer $1 \leq k \leq p-1$ has a unique inverse $\bar{k}$ modulo p. For $k = 1$ and $k = p-1$, $\bar{k} = k$. Furthermore, we have $\bar{k} \neq k$ for any other k, since $k^2 \equiv 1 \pmod p$ implies $k \equiv 1 \pmod p$ i.e. $k = 1$ or $k \equiv -1 \pmod p$ i.e. $k = p-1$. Now there are $p-3$ integers greater than 1 and less than $p-1$, that is $(p-3)/2$ pairs.

(9c) $((p-1)! \bmod p) = (1 \cdot 2 \cdot \cdots \cdot (p-1)) \bmod p$. By (9b), we group the integers between 2 and $p-2$ into $(p-3)/2$ pairs with each pair $(a \cdot b \bmod p) = 1$. So $((p-1)! \bmod p) = (1 \bmod p) \cdot ((p-1) \bmod p) = -1$.

(9d) The fact that p is prime is used in (9a): $p \mid mn \implies p \mid m$ or $p \mid n$, and (9b): existence of unique inverse for $1 \leq k \leq p-1$.

(10) Show by induction that $n^3 - n \bmod 6 = 0$ whenever n is a non-negative integer.

Solution. The statement is true for the base case $n = 0$, since $0 mod 6 = 0$.
Now assume $P(K)$ is true. which means $(k^3 - k) mod 6 = 0$
we must show that $((k+1)^3 - (k+1)) mod 6 = 0$
By expanding we obtain $k^3 + 3k^2 + 3k + 1 - k - 1 = (k^3 - k) + 3(k+1)k$.
By inductive hypotheses 6 divides $(k^3 - k)$. Since one of k and $k+1$ is even 6 divides $3(k+1)k$ as well. This completes the proof.

Bonus 1: Given a countably infinite sequence of countable subsets $S_1, S_2, \ldots$ of the natural numbers, show that there is a subset S^* of the natural numbers that is different from all of them. Give a construction/description of such an S^*.

Solution:

We can use Cantor's diagonalization proof to construct such an S^*.

	1	2	3	4	5	...
S_1	**0**	1	1	0	1	...
S_2	1	**1**	1	0	1	...
S_3	1	1	**0**	0	1	...
S_4	0	1	0	**1**	1	...
S_5	0	1	0	0	**1**	...
$\vdots$						

Each subset S_i of natural numbers can be represented using an infinite 0-1 string, where the jth digit is 0 if $j \notin S_i$, 1 if $j \in S_i$.

Since the sequence is countable, we can list the sets $S_1, S_2, \ldots$ as in the above table. By inverting the diagonal (change 0 to 1 and 1 to 0), we obtain a set S^* which is different from every set S_i in the sequence with respect to at least one natural number.

Bonus 2: Show by induction on n that the set of elements that belong to an odd number of sets $A_1 \ldots A_n$ is exactly $\bigoplus_{i=1}^{n} A_i$, where $A \oplus B := (A \cap \bar{B}) \cup (\bar{A} \cap B)$.

Solution. Basis step : when $n = 1$, $x \in \bigoplus_{i=1}^{1} A_i$ is true if and only if $x \in A_1$.

IH : set of elements that belongs to an odd number of sets $A_1 ... A_n$ is given by $\bigoplus_{i=1}^{n} A_i$, where $A \bigoplus B = (A \cap \bar{B}) \cup (\bar{A} \cap B)$

Induction step:

$\bigoplus_{i=1}^{n+1} A_i = (\bigoplus_{i=1}^{n} A_i \cap \bar{A}_{n+1}) \cup (\bigoplus_{i=1}^{n^-} A_i \cap A_{n+1})$

$x \in (\bigoplus_{i=1}^{n} A_i \cap \bar{A}_{n+1}) \cup (\bigoplus_{i=1}^{n^-} A_i \cap A_{n+1})$ is true if x belongs to odd number of sets from $A_1...A_n$ and does not belong to A_{n+1} or belongs to even number of sets from $A_1...A_n$ and belongs to A_{n+1}. Both cases mean x belongs to odd number of sets from $A_1...A_{n+1}$.

$x \in \bigoplus_{i=1}^{n} A_i \cap \bar{A}_{n+1}) \cup (\bigoplus_{i=1}^{n^-} A_i \cap A_{n+1})$ is false if x belongs to even number of sets from $A_1...A_n$ and does not belong to A_{n+1} or belongs to odd number of sets from $A_1...A_n$ and belongs to A_{n+1}. Both cases mean x belongs to even number of sets from $A_1...A_{n+1}$.