Discrete Mathematics Midterm Exam (Spring 2014)

No :
Name: Edu-Type : 1 / 2

1. LOGIC (15*P*) Prove the following logical inference problem by using natural deduction for propositional logic.

$$\begin{array}{r} p \rightarrow q \\ s \rightarrow r \\ p \\ \therefore q \rightarrow \neg r \\ \hline \neg s \end{array}$$

(1)	p	*Premise*
(2)	$p \rightarrow q$	*Premise*
(3)	q	(1), (2), *Modus Ponens*
(4)	$q \rightarrow \neg r$	*Premise*
(5)	$\neg r$	(3), (4), *Modus Ponens*
(6)	$s \rightarrow r$	*Premise*
(7)	$\neg s$	(5), (6), *Modus Tollens*

2. RELATION (20*P*) Design a Hasse diagram so that is corresponds to this set:
$S = \{(x, y) \mid x \in N, y \in N, \; 1<x<y<10, \; y\%x=0 \}$

To draw a Hasse diagram for a set, that set need to be a partial order set. We have 3 rules to check whether a set is partial order or not: (1. Reflexive, 2. Antisymmetric, 3. Transitive)
But set of S cannot be reflexive because of the rule of 1<x<y<10. Thus for all $x \in N$, we cannot write the relation of $(x, x) \in S$.

3. COMPLEXITY (15*P*) Find the complexity of the pseudo code below for the worst case time.

```
procedure f(n)
z = 1
    for i=1 to $n^3$
        z = z * i
    next
    if $n \leq 1$ then
        return (z)
    else
        return (n * f(n-2))
end f
```

Without regarding the recursion, count of transactions depends on (n^3). Without regarding "for" loop, count of transactions depends on ($n/2$). If we combine them roughly, the total number of transactions depends on ($n^4/2$). But in detail time function is almost $2^3(1^3+2^3+\ldots+n^3)$, and based on Gauss's formula, it can be written as $2^3 \, (n \, (n+1)/2)^2$. So for the worst case, the complexity of the procedure is *$O(n^4)$.*

4. MODULAR ARITHMETIC (20*P*) Using RSA algorithm, we want to send our message. First, we transform our message into a numeric form, and we found integer 4. The public key pair is (5, 91) and the private key pair (29, 91). Compute the sent message and show the reacquiring of the original message.

where e = 5, d = 29, n = 91, m = 4. And by using these variables we can compute sent message by

$m` = m^e \pmod{n} = 4^5 \pmod{91} = 23$

Then the receiver side can obtain the original message again by

$m`` = m = (m`)^d \pmod{n} = 23^{29} \pmod{91} = 4^{(5*29) \bmod \phi(91)} \pmod{91}$

$= 4^{(5*29) \bmod 72} \pmod{91} = 4^1 \pmod{91} = 4$

5. COMBINATORICS (15*P*) Suppose a class has T tables and S students. The tables are double (two students can sit) or triple (three students can sit). What should be the relation between T and S so that at least 3 students sit in the triple tables?

To sit in the triple tables at least 3 students, only one triple table is enough. So the relation between T and S must be:

$2*T+1 \leq S$

6. PROBABILITY (15*P*) In Orange County, 51% of the adults is male. One adult is randomly selected for a survey involving credit card usage. The selected survey subject is smoking a cigarette. Also, 9.5% of males smoke, whereas 1.7% of females smoke. Find the probability that the selected subject is a male.

$P(M) = 0.51 \qquad P(\neg M)=0.49 \qquad P(S|M)=0.095 \qquad P(S|\neg M)=0.017$

$$P(M|S) = \frac{P(S|M)*P(M)}{P(S)} = \frac{0.095*0.51}{0.095*0.51+0.017*0.49} \cong 0.85$$