MATH 240; EXAM # 1, 100 points, Oct. 7, 2002 (R.A.Bruualdi)

TOTAL SCORE (10 problems):

Name: SOLUTIONS

TA (circle): Matthew Petro    Dilip Raghavan

Disc. (circle) TUES.    THURS.    TIME:

1. [8 points] Calculate the sum $\sum_{i=0}^{n} 10 \cdot 8^i$:

$$10 \cdot \frac{8^{n+1} - 1}{7}$$

2. [8 points] Give the disjunctive normal form (sum of products) of the Boolean function $f(x, y, z, u)$ where $f(x, y, z, u) = 1$ if and only if exactly one of $x, y, z, u$ is 1.

$$f(x, y, z, u) = \bar{x}y\bar{z}u + \bar{x}\bar{y}z\bar{u} + \bar{x}y\bar{z}\bar{u} + xy\bar{z}\bar{u}$$

3. [8 points] Let $Q(x, y)$ be the predicate: Team $x$ in Conference $y$ has a winning record. Express using quantifiers and the predicate $Q(x, y)$:

Every conference has at least one team with a winning record:

$$\forall y \exists x Q(x, y)$$

There is a conference in which no team has a winning record.

$$\exists y \forall x \neg Q(x, y)$$

4. [8 points] Express the set $\overline{A - B}$ in a simple way that does not use the complement:

Using DeMorgan’s Law we have,

$$\overline{A - B} = \overline{A \cap B} = A \cup B.$$ 

5. [12 points] Let $f : A \to B$ be defined as follows:

$A = B = \{x : x$ a real number and $0 \leq x \leq 10\}$ and $f(x) = [x] - \lfloor x \rfloor$.

Answer the following questions:

(i) Is $f$ an injection? Why or why not?
NO, since e.g. $f(0) = f(1) = 0$.

(ii) Is $f$ a surjection? Why or why not?
NO, since e.g. there is no $x$ such that $f(x) = 2$. (or see (iii) below) 

(iii) What is the range of $f$?

Range $= \{0, 1\}$.

6. [8 points] Let $f(x) = \frac{3x^2-4x+1}{x+5}$. Find a very simple function $g(x)$ such that $f(x) = O(g(x))$.

Taking limits we see that $f(x) = O(x)$.

7. [10 points] Recall the identification:

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

In the Caesar Cipher defined by $f(p) = p + 5 \mod 26$, **decrypt** the word DFP.

The inverse function of $f$ is $f(p) = p - 5 \mod 26$, that is, $f(p) = p + 21 \mod 26$. So DFP is decrypted as YAK

8. [12 points] Use the **Euclidean algorithm and only the Euclidean Algorithm** to find the GCD(330,124):

Using the Euclidean algorithm in a straightforward way we get that the GCD is 2.

9. [12 points] Use the **technique of the Chinese Remainder Theorem** to calculate the smallest positive solution of the system of congruences:

$x \equiv 1 \mod 4$
$x \equiv 2 \mod 5$
$x \equiv 3 \mod 7$.

See pages 142-3 of the text. We have $M = 4 \cdot 5 \cdot 7 = 140$, $M_1 = 5 \cdot 7 = 35$, $M_2 = 4 \cdot 7 = 28$, and $M_3 = 4 \cdot 5 = 20$. We find the inverse of $M_1 = 35 \mod 4$ to be 3, the inverse of $M_2 = 28 \mod 5$ to be 2, and the inverse of $M_3 = 20 \mod 7$ to be 6. The solution is $x \equiv 1(35)(3) + 2(28)(2) + 3(20) \mod 140$, and this gives mod 140 the smallest number 17.

10. [14 points] Let $a, b, m$ be positive integers with $m \geq 2$. Suppose that $a \equiv b \mod m$.

Prove that $\text{GCD}(a, m) = \text{GCD}(b, m)$.

We have $a = b + qm$ for some integer $q$. From this we see that any integer that divides both $a$ and $m$ also divides $b$ (so divides both $b$ and $m$), and any integer that divides both $b$ and $m$ also divides $a$ (so divides both $a$ and $m$). So $\{a, m\}$ and $\{b, m\}$ have the same divisors and so the same GCD.