**MATH 240; EXAM # 1, 100 points, October 13, 2003 (R.A.Brualdi)**

**TOTAL SCORE (11 problems; 100 points possible):**

**Name: SOLUTIONS**

**TA: Josh Davis, (circle) TUES 1:20 TUES 2:25 THURS. 1:20 THUR 2:25**

**TA: Neil Ramsamooj, (circle)TUES 8:50 TUES 12:05 THUR 8:50 THUR 12:05**

1. [6 points] First state the converse and contrapositive in English of: **If I am a CS major, then I get an A in this course.**

**Converse:** If I get an A in this course, then I am a CS major.

**Contrapositive:** If I do not get an A in this course, then I am not a CS major.

2. [8 points] Determine all values of $x$ with $1 \leq x \leq 2$ for which $\lfloor x + \frac{1}{2} \rfloor \neq \lceil x - \frac{1}{2} \rceil$?

Just $x = 3/2$.

3. [8 points] What is the **disjunctive normal form** (sum of products) of the Boolean function $f(x, y, z)$ which equals 1 if and only if $x, y, z$ has an even number of 1's.

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

Note that 0 is an even number.

4. [8 points] Let $P(x)$ and $Q(x)$ be predicates where the universe of discourse for $x$ is some set $U$. Let

$$A = \{x : P(x) \text{ is true}\} \text{ and } B = \{x : Q(x) \text{ is true}\}$$

be the **truth sets** of $P(x)$ and $Q(x)$, respectively. In terms of $A$ and $B$ and set operations, give:

(a) the truth set of the predicate $Q(x) \to P(x)$:

$\overline{B} \cup A$ since this predicate is logically equivalent to $\neg Q(x) \vee P(x)$.

(b) Then give a predicate, obtained using only $\neg$ (negation) and $\vee$ (disjunction) from $P(x)$ and $Q(x)$, whose truth set is

$$\overline{A} \cap B.$$

$\overline{A} \cap B = \overline{A \cup \overline{B}}$ by DeMorgan's law; hence $\neg(Q(x) \to P(x))$

5. [6 points] Determine the truth value (TRUE or FALSE) of each of the following statements where the universe of discourse for all variables is the set $Z^+$ of positive integers.

(a) $\exists m, \forall n, (mn = 0)$: F

(b) $\exists m, \neg\forall n, (mn = 1)$: T

(c) $\neg\forall m, (\exists n, m|n)$: F

6. [6 points] Which of the following propositions doesn't belong in this group?

(a) $\neg(\neg p \wedge q)$

(b) $p \vee \neg q$

(c) $q \rightarrow p$

(d) $\neg q$ is a sufficient condition for $p$

(e) $p$ is a necessary condition for $q$

(d) doesn't belong; all the others are logically equivalent.

7. [8 points] Arrange the following functions in order of **increasing order of magnitude** (**no proof necessary**):

(a) $f(x) = 10x^2 \log x + 100x^2 + 200$

(b) $g(x) = \frac{x^4}{3x^2 - 20x + 5}$

(c) $h(x) = x \sin x$

(d) $l(x) = (1.001)^x$

**Smallest order of magnitude to largest order of magnitude:**

(c), then (b), then (a), then (d). (Note that $|\sin x| \leq 1$.)

8. [20 points] Alice wants to communicate with Bob using the secure RSA system and Bob's public key. She finds $n = 437$ and $e = 35$ on Bob's public page. Unlike Alice or anyone else, Bob knows that $437 = 19 \cdot 23$. **(You must show your work; a calculator example is unacceptable.)**

(a) What is Bob's decryption key (a positive integer)?

Using the Euclidean algoritm with $a = 396 = 18 \cdot 22$ and $b = 35$, and then working backwards we get that $1 = 16 \cdot 396 - 181 \cdot 35$. Hence the inverse of $e = 35$ is $-181$ which mod 396 is 215. So $d = 215$.

(b) Check that your decryption key is correct:

We check that $35 \cdot 215 = 19 \cdot 396 + 1$.

(c) Suppose that Bob receives the integer 3 from Alice. What integer did Alice send Bob?

Alice sent $3^{215}$ mod 437 which using modular exponentiation equals 108.

9. [10 points] Give an **indirect proof** of: *If $n$ is an integer and $n^2 + 8$ is odd, then $n$ is odd.*

Assume that $n$ is not odd, then $n$ is even and so $n = 2k$ for some integer $k$. Then

$$n^2 + 8 = (2k)^2 + 8 = 4k^2 + 8 = 2(2k^2 + 4),$$

and $n^2 + 8$ is also even.

10. [10 points] Give a **direct proof** of the following cancellation law: *Let $n$ be a positive integer. Let $a, b, c$ be positive integers with $c$ and $n$ relatively prime. If $ac \equiv bc($ mod $n)$, then $a \equiv b$ (mod $n$).*

Assume that $ac \equiv bc \pmod{n}$. Then $n \mid (ac - bc)$ and so $n \mid c(a - b)$. Since $n$ and $c$ are **relatively prime**, $n$ and $c$ have no common factor other than 1. Thus all the prime factorization of $n$ is in $a - b$. So $n \mid (a - b)$ and hence $a \equiv b \pmod{n}$.

Or one could use that fact that $c$ has an inverse $d$ modulo $n$, since $c$ and $n$ are relatively prime, and then multiply $ac \equiv bc \pmod{n}$ by $d$, etc.

11. [10 points] Given a sequence of numbers $a_1, a_2, \ldots, a_n$, describe an algorithm **(using the pseudocode as practiced in class)** which locates the last occurrence of the largest element on the list and the value of the largest element.

$x := a_1$
loc:= 1
For $i = 2, \ldots, n$, if $a_i \geq x$, then
  $x := a_i$
  loc:= $i$.
($x$ is the largest element and loc is the location of its last occurrence.)