MATH 240; EXAM # 1, 100 points, October 14, 2004 (R.A.Brualdi)

TOTAL SCORE (13 problems; 100 points possible):

Name: These R. Solutions

TA: Darren Neubauer (circle time) Mon 12:05 Mon 1:20 Wed 12:05 Wed. 1:20

1. [6 points] Let $P(x)$, $Q(x)$ and $R(x)$ be predicates where the universe of discourse for x is some set U. Let $A = \{x : P(x) \text{ is true}\}$, $B = \{x : Q(x) \text{ is true}\}$, and $C = \{x : R(x) \text{ is true}\}$ be the truth sets of $P(x)$, $Q(x)$, and $R(x)$, respectively.

(a) What predicate has truth set equal to $(A \cap \overline{B}) \cup C$?

$(P(x) \wedge \neg Q(x)) \vee R(x)$

(b) In terms of A, B, and C, what is the truth set of the predicate $Q(x) \rightarrow (P(x) \vee R(x))$?

$\overline{B} \cup (A \cup C)$

(2) [6 points] Circle the statement below which is **not** logically equivalent to the others:

(a) $p \rightarrow q$

(b) $\neg p \vee q$

(c) *** $p \wedge \neg q$

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

(e) $\neg q \rightarrow \neg p$

(3) [6 points] Circle the statement below which is logically equivalent to $\neg \forall x \exists y P(x, y)$:

(a) $\forall x \exists y \neg P(x, y)$

(b) $\exists x \exists y P(x, y)$

(c) *** $\exists x \forall y \neg P(x, y)$

(d) $\exists x \forall y P(x, y)$

(e) $\forall x \forall y P(x, y)$

4. [6 points] Let $f : A \rightarrow B$ be a function. Identify the **incorrect** statement below, or circle (e).

(a) If f is injective, then $|A| \leq |B|$.

(b) *** If $|A| \geq |B|$, then f is surjective.

(c) If f is injective and $|A| = |B|$, then f is surjective.

(d) If f is surjective and $|A| = |B|$, then f is bijective.

(e) All are correct.

5. [6 points] CIRCLE **all** the **incorrect** statements below, or circle (e):

(a) *** $\lceil -3.8 \rceil = -4$.

(b) $\lfloor x \rfloor = -\lceil -x \rceil$

(c) *** $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$

(d) $\lceil x - 0.5 \rceil$ is the closest integer to x, rounding down in the case of ties.

(e) All are correct.

6. [6 points] The number of Boolean functions of n Boolean variables equals:

(a) $2n$

(b) n^2

(c) *** 2^{2^n}

(d) 2^n

(e) None of the above

7. [6 points] For each of the functions $f(n)$ below, give the **simplest** function $g(n)$ such that $f(n) = \Theta(g(n))$.

(a) $x^2 \ln(\frac{x^2+5}{x+2})$.

$\Theta(x^2 \ln x)$

(b) $\frac{x^5 - x^4 + 2x^2 - 5}{100x^5 + 3x^3 - 5x}$

$\Theta(1)$

8. [5 points] Compute the Boolean product:

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}$$

9. [9 points] Compute a simple closed form expression for the sum

$$\sum_{i=0}^{m} \sum_{j=1}^{n} j3^i.$$

$= \frac{3^{m+1}-1}{2} \frac{n(n+1)}{2}$

(10) [14 points]

1. If it exists, **use the Euclidean Algorithm** to find the multiplicative inverse of 25 modulo 152 (**trial and error not acceptable**):

   $152 = 6 \cdot 25 + 2$

   $25 = 12 \cdot 2 + 1$

   $2 = 2 \cdot 1 + 0.$

   Using these equations in the reverse order, we get

   $1 = 73 \cdot 25 - 12 \cdot 152.$

   Thus the inverse of 25 modulo 152 is 73.

2. **Use your answer above — calculator answer not acceptable —** to find a solution to $25x \equiv 9 \bmod 152$ **where x is between 0 and 151**.

   We get that $x = 25^{-1} \cdot 9 \bmod 25 = 657 \bmod 125 = 49$.

11. [10 points] Use Fermat's Little Theorem (no other method acceptable) to compute 55^{55} mod13. **(You must show your work; a calculator answer is unacceptable).**

First we note that 55 mod 13 is 3, so we can use 3 instead of 55. i.e 3^{55} mod 13. By FLT, we have, since 13 is a prime, $3^{12} = 1$ mod 13. So using this 4 times we are down to 3^7 mod 13, which now we easily see is 3.

12. [10 points] Bob wants to allow anyone to send him secure messages via the RSA cryptosystem. So he determines two large primes p and q and computes their product $n = p \cdot q$. He also determines an encryption exponent e and a decryption exponent d.

(a) What does Bob put on his public web page? n and e

(b) What defining property must e have?

GCD$(e, (p-1)(q-1)) = 1$

(c) What defining property must d have?

d is the inverse of e mod $(p-1)(q-1)$

13. [10 points] Prove by mathematical induction that for all $n \geq 0$, $2^{2n} \equiv 1 \bmod 3$.
Briefly:

Basis step: $2^{2 \cdot 0} = 1$ so OK.

Inductive Step: If $2^{2n} \equiv 1 \bmod 3$, then $2^{2(n+1)} \equiv 1 \bmod 3$,
So Assume $2^{2n} \equiv 1 \bmod 3$ is True. Then

$$\begin{aligned} 2^{2(n+1)} &= 2^{2n+2} \\ &= 2^{2n} \cdot 2^2 \\ &\equiv 1 \cdot 4 \bmod 3 \\ &\equiv 1 \bmod 3. \end{aligned}$$

So $2^{2(n+1)} \equiv 1 \bmod 3 is True$, and the result hold by mathematical induction