MATH 240; EXAM # 1, 100 points, October 17, 2005 (R.A.Brualdi)

TOTAL SCORE (10 problems; 100 points possible):

Name: These R. Solutions

TA: Luanlei Zhao (circle time) Mon 9:55 — Mon 11:00 — Wed 9:55 — Wed. 11:00

1. [10 points] Using the method of **proof by contradiction**, give a proof of the following proposition:

If n is a positive integer, then not both n and $n+2$ are perfect squares.

Suppose n is a positive integer, and that both n and $n+2$ are perfect squares. Then $n = k^2$ and $n+2 = l^2$ where $l > k$. Since $n+2$ is 2 more than n, we have $k^2 + 2 = l^2$ and so

$$2 = l^2 - k^2 = (l+k)(l-k).$$

Since 2 is a prime, $l + k = 2$ and $l - k = 1$. Adding these two equations we get $2l = 3$ or $l = 3/2$, contradicting that l is an in integer. This contradiction shows that not both n and $n+2$ are perfect squares.

2. [8 points] Let $P(x)$ and $Q(x)$ be predicates where the universe of discourse for x is some set U. Let $A = \{x : P(x) \text{ is true}\}$ and let $B = \{x : Q(x) \text{ is true}\}$ be the truth sets of $P(x)$ and $Q(x)$, respectively.

Circle all the predicates below that have truth set equal to $\overline{A} \cup \overline{B}$?

(a) $P(x) \rightarrow \neg Q(x)$ ****

(b) $\neg(P(x) \wedge Q(x))$ ****

(c) $\neg(\neg P(x) \vee Q(x))$

(d) $P(x) \vee \neg Q(x)$

3. [10 points] When you say "$p \rightarrow q$" you've also said (**Circle all right answers below**):

(a) p is a necessary condition for q

(b) p is a sufficient condition for q ****

(c) p only if q ****

(d) q is a necessary condition for p ****

(e) q is a sufficient condition for p

4. [10 points] Let $f : A \to B$ and $g : B \to C$ be functions. **Circle all the correct statements below**:

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

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

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

(d) If g is injective, then $g \circ f$ is injective.

(e) If $g \circ f$ is surjective, then g is surjective. ****

5. [8 points] For each of the functions $f(n)$ below, give the **simplest** function $g(n)$ such that

$$f(n) = \Theta(g(n)).$$

(a) $f(n) = \lfloor 10^{10} n \rfloor$: $= \Theta(n)$

(b) $f(n) = \log(n^8 + n^2 + 2)$: $= \Theta(\log n)$

(c) $f(n) = 2^n + n^{20} \log n$: $= \Theta(2^n)$

(d) $f(n) = 1,000 \sin n := \Theta(\sin n)$

(Note: when I originally made up this question I was think of Big-Oh, not Big-Theta. But note that while $f(n) = O(1)$, that is, is bounded by a constant, $f(n) \neq \Theta(1)$. This is because $\sin n$ takes on the value 0 infinitely often as n goes to infinity and so $1 \neq O(\sin n)$ (which would have to happen if $\sin(n) = \Theta(n)$. Unless someone wrote something foolish, I didn't take off for this problem.

6. [12 points] **Fill in the strongest conclusion possible**:

(i) The composite integer n has for sure a prime factor less than or equal to: $\sqrt{n}$

(ii) If the GCD of m and n is 72 and the LCM is 5544, then mn equals: $72 \cdot 5544$

(iii) If a is a divisor of bc and $\text{GCD}(a, c) = 1$, then: a is a divisor of b

(iv) If a is an integer and $\left\lfloor \frac{a}{11} \right\rfloor = -6$ and $a \bmod 11 = 6$, then $a =$: $(-6) \cdot 11 + 6 = -60$

7. [10 points]

(i) What is the **disjunctive normal form** (that is, **sum of products**) of the Boolean function $f(x, y, z)$ of three Boolean variables x, y, z that equals 1 if and only if $x = 1, y = 0, z = 0$, or $x = 0, y = 0, z = 1$, or $x = 1, y = 1, z = 1$.

$$x\bar{y}\bar{z} + \bar{x}\bar{y}z + xyz.$$

(ii) Let f be the Boolean function $f(x, y) = x^3y + \overline{\overline{x} + \overline{y}}$. Give **as simple as possible** expression for $f(x, y)$ without any *bars* and then compute all the values of f.

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

$$f(1, 1) = 1, f(1, 0) = 0, f(0, 1) = 0, f(0.0) = 0.$$

8. [10 points] Compute a **simple closed form expression** for the sum

$$\sum_{i=0}^{m}\sum_{j=0}^{n} 5i3^j.$$

$$\sum_{i=0}^{m}\sum_{j=0}^{n} 5i3^j = 5\sum_{i=0}^{m} i \cdot \sum_{j=0}^{n} 3^j = 5m(m+1)/2 \cdot (3^{n+1} - 1)/2 = 5/4(m(m+1)(3^{n+1} - 1)).$$

9. [10 points] Use modular exponentiation **no other method acceptable** to compute 55^{55} mod13. **(You must show your work; a calculator answer is unacceptable).**

First 55mod13 = 3 so we can compute 3^{55}. Then

$$55 = 2^5 + 2^4 + 2^2 + 2 + 1.$$

Repeated squaring gives

$$3^2 = 9, 3^4 = 3, 3^8 = 9, 3^{16} = 3, 3^{32} = 3 \text{ all mod } 13.$$

Hence

$$3^{55} = (9)(3)(3)(9)(3) = 3 \mod 13.$$

10. [12 points]

(a) If it exists, **use the Euclidean Algorithm** to find the multiplicative inverse of 25 modulo 82 (**trial and error not acceptable**). Answer should be an integer between 1 and 81.

Repeated division gives:

$$\begin{aligned} 82 &= 3 \cdot 25 + 7 \\ 25 &= 3 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot +0. \end{aligned}$$

Thus the GCD of 25 and 82 equals 1 and 25 has a multiplicative inverse mod 82. Using these equations in the reverse order we get:

$$1 = 23 \cdot 25 - 7 \cdot 82.$$

Thus $1 = 23 \cdot 25 \bmod 82$ and 23 is the inverse of 25 mod 82.

(b) Use your answer above — **calculator answer not acceptable** — to find a solution to $25x - 10 \equiv 0 \bmod 82$ **where x is between 0 and 81**.

From $25x = 10 \bmod 82$ we get using above, that $x = 23 \cdot 10 \bmod 82$ and this is 66.