CMSC 250 Quiz #7 ANSWERS Wednesday, Oct. 13, 2004

Write all answers legibly in the space provided. The number of points possible for each question is indicated in square brackets – the total number of points on the quiz is 30, and you will have exactly 20 minutes to complete this quiz. You may not use calculators, textbooks or any other aids during this quiz.

1. [18 pnts.] Disprove by counter example or Give a complete proof for each of the following:

   a. If $a \equiv_m b$ and $m|a$, then $b \equiv_m 0$.
   ANSWER: TRUE - Proof by generalizing from the generic particular and conditional world.

   Proof:
   Let p, q be arbitrary in Z, and let x be arbitrary in Z^+.
   Assume $p \equiv_x q \wedge x|p$

   $p \equiv_x q$ by conjunctive simplification.
   $x|(p-q)$ by definition of equiv in a mod.
   $\exists k \in Z, p - q = kx$ by definition of devides.

   $x|p$ by conjunctive simplification.
   $\exists d \in Z, p = xd$ by definition of divides.

   Since $p - q = kx$, by substitution we know $xd - q = kx$
   $q = xd - kx = x(d-k)$ and $q - 0 = x(d-k)$ by algebra.
   $d - k \in Z$ by closure of the integers during subtraction.
   $x|q - 0$ by definition of divides.
   $q \equiv_x 0$ by definition of equiv in a mod.
   $p \equiv_x q \wedge x|p \rightarrow q \equiv_x 0$

   $\forall a, b \in Z, \forall m \in Z^+, a \equiv_m b \wedge m|a \rightarrow b \equiv_m 0$ by generalizing from the generic particular.

   b. For any odd integer n, $\lfloor \frac{n^2}{4} \rfloor = (\frac{n-1}{2})(\frac{n+1}{2})$
   ANSWER: true - proof by generalizing from the generic particular.

   $\forall n \in Z^{odd}, \lfloor \frac{n^2}{4} \rfloor = (\frac{n-1}{2})(\frac{n+1}{2})$
   Proof:
   Let n be arbitrary in Z^{odd}.
   $\exists k \in Z, n = 2k+1$ by definition of odd.
   $n^2 = (2k+1)^2 = (2k+1)(2k+1) = 4k^2 + 4k + 1$.
   $\frac{n^2}{4} = \frac{4k^2+4k+1}{4}$ by substitution.
   $= k^2 + k + \frac{1}{4}$ by algebra.
   $\lfloor \frac{n^2}{4} \rfloor = \lfloor k^2 + k + \frac{1}{4} \rfloor$ by substitution.
   $= k^2 + k$ by the definition of floor.
   Since $n = 2k+1$, we know by algebra that $k = \frac{n-1}{2}$
   $k^2 + k = \frac{n-1}{2}^2 + \frac{n-1}{2}$
   $= \frac{(n-1)^2}{4} + \frac{n-1}{2}$
   $= \frac{(n-1)^2+2(n-1)}{4}$
   $= \frac{(n^2-2n+1)+(2n-2)}{4}$
   $= \frac{n^2-1}{4}$
   $= \frac{(n-1)(n+1)}{4}$
   $= \frac{n-1}{2}\frac{n+1}{2}$ by algebra.

2. [12 pnts.] Use the Unique Prime Factorization Theorem to prove that

$$\forall p \in Z^{prime}, \forall n \in Z^{>1}, p > 10 \wedge p|7n \rightarrow p|2n$$

PROOF:
Let $p \in Z^{prime}$ and $n \in Z^{>1}$ be arbitrary.

Assume $p > 10 \wedge p|7n$

Assume $p = 7$
This is a contradiction to the fact that $p > 10$ since $7 \not> 10$
Therefore we know that $p \neq 7$ by closing the conditional world with a contradiction.

Since 7n is greater than 1 (since both 7 and n are greater than 1), and
Since 7n is an integer by the closure of integers in multiplication, it can be prime factorized.

$$\exists k \in Z^{+}, \exists p_1, p_2, ..., p_k \in Z^{prime}, \exists e_1, e_2, ..., e_k \in Z^{+}, 7n = p_1^{e_1} * p_2^{e_2} * ... * p_k^{e_k}$$

Since 7 is prime, 7 must be one of the p_i in this list.
Since p divides 7n, p must be one of the p_j in this list.

Since $p \neq 7$ from above, we know that $p_i \neq p_j$

we can factor them both out and substitute to get:

$$7n = 7^{e_i} * p^{e_j} * b$$

where b is an integer because it is the product of the remaining primes. Since b is the product of the remaining primes, $b \in Z$ by closure of Z in multiplication.

If we divide both sides of the equation by 7, one of the p_j must still be equal to p.

$$n = 7^{e_i - 1} * p^{e_j} * b$$

Then by commutativity and associativity of multiplication we get:

$$n = p * [7^{e_i - 1} * p^{e_j - 1} * b]$$

Since the smallest value for both $e_i - 1$ and $e_j - 1$ is 0, the contents of the square brackets is an integer by closure of integers in multiplication.

We can multiply both sides by 2 to get:

$$2n = 2p * [7^{e_i - 1} * p^{e_j - 1} * b]$$

and do commutativity and associativity to get:

$$2n = p * [2 * 7^{e_i - 1} * p^{e_j - 1} * b]$$

The contents in the square brackets is still an integer by closure of Z in multiplication. Therefore $p|2n$ by definition of divides.

Since p and n were both arbitrary as defined above, we can generalize from thegeneric particulars to get:

$$\forall p \in Z^{prime}, \forall n \in Z^{>1}, p > 10 \wedge p|7n \rightarrow p|2n$$