CSE 321 Autumn 2008 Midterm Solutions

1. (20 points) Circle T or F to indicate whether each of the following statements is true or false. *Briefly* explain why. You do not need to list the reasons for intermediate steps as long as they are obvious. Assume positive integers for all numbers.

   (a) If $a|bc$, then $a|b$ or $a|c$. . . . . F

   Let $a = 6, b = 2, c = 3$. $6|(2 \cdot 3)$, but 6 does not divide either 2 or 3.

   (b) If $a|b$ and $c|\frac{b}{a}$, then $c|b$. . . . . T

   Since $a|b$, then $\frac{b}{a}$ is an integer. Because $c|\frac{b}{a}$, then $c|\frac{b}{a}a$ ("If $a|b$, then $a|bc$"). Thus $c|b$.

   (c) If $a|b + c$ and $a|b$, then $a|c$. . . . . T

   From $a|b$, we also know $a| - b$. Since $a|b + c$ and $a| - b$, then $a|(b + c) + (-b)$ or $a|c$. For some reason, quite a few people misread it as saying "If $a|b + c$, then $a|b$ or $a|c$."

   (d) $\neg p \rightarrow F$ is a tautology. . . . . F

   This simplifies to $\neg(\neg p) \vee F \iff \neg(\neg p) \iff p$.

   (e) $p \rightarrow (q \rightarrow p)$ is a tautology. . . . . T

   This simplifies to $\neg p \vee (\neg q \vee p) \iff (\neg p \vee p) \vee \neg q \iff (T \vee \neg q) \iff T$.

   (f) If p and q are integers and p is prime, then gcd(p, q) = 1. . . . . F

   Let $p = 3$ and $q = 6$. gcd(3, 6) = 3.

   (g) gcd(a,a mod b) = gcd(b,b mod a). . . . . F

   Let $a = 3$ and $b = 7$.
   $\gcd(3, 3 \bmod 7) = \gcd(3, 3) = 3 \neq 1 = \gcd(7, 1) = \gcd(7, 7 \bmod 3)$

2. (15 points) Prove that n is odd if and only if $5n^2 + 4$ is odd.

   To prove an “if and only if”, you have to prove in both directions.

   $\rightarrow$: “If $5n^2 + 4$ is odd, then n is odd.”

   We will prove this using a proof by contraposition. Assume n is even. Then $n = 2k$ for some k.

$$\begin{array}{rcl} 5n^2 + 4 & = & 5(2k)^2 + 4 \\ & = & 20k^2 + 4 \\ & = & 2(10k^2 + 2) \end{array}$$

   Thus, $5n^2 + 4$ is even.

   $\leftarrow$: “If n is odd, then $5n^2 + 4$ is odd.”

   We will prove this directly. Assume n is odd. Then $n = 2k + 1$ for some k.

$$\begin{array}{rcl} 5n^2 + 4 & = & 5(2k + 1)^2 + 4 \\ & = & 5(4k^2 + 4k + 1) + 4 \\ & = & 20k^2 + 20k + 5 + 4 \\ & = & 20k^2 + 20k + 8 + 1 \\ & = & 2(10k^2 + 10k + 4) + 1 \end{array}$$

   Thus $5n^2 + 4$ is odd.

   A very common error was doing the proof in only one direction.

3. (15 points)

(a) Use the extended Euclidean algorithm to solve $8x \equiv 9 \pmod{27}$ for x.

We will need to find an inverse of 8 modulo 27. We first use Euclid's algorithm to find the gcd of 8 and 27, then we will use the computation history of this algorithm to find the inverse. This process in full is the extended Euclidean algorithm.

gcd(27,8) = gcd(8,3) = gcd(3,2) = gcd(2,1) = gcd(1,0) = 1.

If we expand out the computations used in the execution of this algorithm, we will be able to find our inverse.

(a) $27 = 3 \cdot 8 + 3$
(b) $8 = 2 \cdot 3 + 2$
(c) $3 = 1 \cdot 2 + 1$
(d) $2 = 2 \cdot 1$

To find an inverse of 8 modulo 27, we are looking for an s and t such that $1 = s \cdot 27 + t \cdot 8$. Such an inverse is guaranteed to exist, because 27 and 8 are relatively prime, as we showed above. We combine each of the four equations above to express 1 in this way.

Equation (c) gives us $1 = 3 - 1 \cdot 2$.

We then replace the 2 with larger terms, by using equation (b).

$1 = 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8$.

Finally, we replace the second 3 with larger terms by using equation (a).

$1 = 3 \cdot 3 - 8 = 3 \cdot (27 - 3 \cdot 8) - 8 = 3 \cdot 27 - 10 \cdot 8$.

We now see that $1 = s \cdot 27 + t \cdot 8$, where $s = 3$, and $t = -10$. -10 is the inverse of 8 modulo 27.

Moving back to the linear congruence we were trying to solve, $8x \equiv 9 \pmod{27}$.

$-10 \cdot 8 \equiv 1 \pmod{27}$, so $-10 \cdot 8x \equiv -10 \cdot 9 \pmod{27} \iff x \equiv -90 \pmod{27}$.

There were two common mistakes. (1) Some people took -10 to be x instead of the inverse and just stopped there. (2) Others read $1 = 27 \cdot 3 - 8 \cdot 10$ to mean that the inverse of 8 modulo 27 was 10 (not -10).

If you made a mistake in your math somewhere that caused a chain reaction of wrong answers, you were usually given most of the credit as long as we could follow the rest of your logic.

(b) If your answer to (a) was not in the range of [0, 26], find a correct value in this range.

-90 mod 27 = 18

(c) Find an inverse of 27 modulo 8.

This is not the same as finding an inverse of 8 modulo 27. However, you already did most of the work in (a). It is s or 3.

4. (20 points) Define the following predicates.

- $F(x, y)$: "x considers y as a friend"
- $E(x, y)$: "x considers y as an enemy"

Let the universe for all variables be the set of all people. Do *not* use the uniqueness quantifier, $\exists!$. Express the following:

(a) Everyone considers Tom as a friend.
$\forall x F(x,\text{Tom})$

(b) Mr. Rogers has no enemies (i.e., he does not consider anyone as an enemy).
$\neg\exists x E(\text{Mr. Rogers}, x)$

(c) Everyone knows at least one other person that they consider as a friend.
$\forall x \exists y (F(x, y) \wedge x \neq y)$
Many people did not state that $x \neq y$.

(d) People do not consider any of their enemies as friends.
$\forall x \forall y (E(x, y) \rightarrow \neg F(x, y))$
or
$\forall x \forall y (F(x, y) \rightarrow \neg E(x, y))$

(e) "The enemy of my enemy is my friend." (i.e., people consider the enemies of their enemies as friends)
$\forall x \forall y \forall z ((E(x, y) \wedge E(y, z)) \rightarrow F(x, z))$

5. (20 points) Prove that for every positive integer $n \geq 2$, $(n+2)! > 3^n + 3$.

Let $P(n)$ be the statement "$(n+2)! > 3^n + 3$".

Base case: $P(2)$

$(2+2)! = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$

$3^2 + 3 = 9 + 3 = 12$

$(2+2)! > 3^2 + 3$

Inductive hypothesis: Assume $P(k)$, that is $(k+2)! > 3^k + 3$.

Inductive step: Prove $P(k+1)$

$$\begin{aligned}
(k+1+2)! &= (k+3)! && (1)\\
&= (k+3) \cdot (k+2)! && (2)\\
&> (k+3) \cdot (3^k + 3) && (3)\\
&> 3 \cdot (3^k + 3) && (4)\\
&= 3 \cdot 3^k + 9 && (5)\\
&= 3^{k+1} + 9 && (6)\\
&> 3^{k+1} + 3 && (7)
\end{aligned}$$

Step (3) above results from the inductive hypothesis.

6. (10 points) Let a be an integer greater than 1. Prove that $a^n + a - 2$ is divisible by $a - 1$ for $n \geq 0$. There are multiple ways to solve this problem; if you get stuck, try a different approach.

Modular arithmetic:

If $a = 2$, then this is trivially true, because $a - 1 = 1$ and 1 divides anything. In the general case, showing that $a - 1$ divides $a^n + a - 2$ is the same as showing that $a^n + a - 2 \bmod (a-1)$ is 0. Recall that $a + b \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$ and $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$.

$$\begin{aligned} a^n + a - 2 \bmod (a-1) &= ((a^n \bmod (a-1)) + (a \bmod (a-1)) - (2 \bmod (a-1))) \bmod (a-1) \\ &= ((a \bmod (a-1))^n + (a \bmod (a-1)) - (2 \bmod (a-1))) \bmod (a-1) \\ &= (1^n + 1 - 2) \bmod (a-1) \\ &= (1 + 1 - 2) \bmod (a-1) \\ &= 0 \end{aligned}$$

Mathematical induction:

Let $P(n)$ be "$a^n + a - 2$ is divisible by $a - 1$ for $a > 1$".

Base case: $P(0)$

$a^0 + a - 2 = 1 + a - 2 = a - 1$ which is clearly divisible by $a - 1$.

Inductive hypothesis: Assume $P(k)$, that is "$a^k + a - 2$ is divisible by $a - 1$ for $a > 1$"

Inductive step: Prove $P(k+1)$

$a^{k+1} + a - 2 = a \cdot a^k + a - 2 = (a-1) \cdot a^k + a^k + a - 2 = (a-1) \cdot a^k + (a^k + a - 2)$

By the inductive hypothesis, we know that $(a^k + a - 2)$ is divisible by $(a-1)$. The first term is a multiple of $(a-1)$ so clearly divisible by $(a-1)$, so $a^{k+1} + a - 2$ is divisible by $(a-1)$.

Factoring:

Some people knew that $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + a^{n-3} + ... + 1)$.

$a^n + a - 2 = a^n - 1 + (a-1) = (a-1)(a^{n-1} + a^{n-2} + a^{n-3} + ... + 1) + (a-1)$

Both terms are multiples of $(a-1)$ and thus $a^{k+1} + a - 2$ is divisible by $(a-1)$.