CMSC 250 Fall 2004 — Homework 6 Answer

Due Wed., Oct. 13 at the beginning of your discussion section.

You must write the solutions to the problems single-sided on your own lined paper, with all sheets stapled together, and with all answers written in sequential order or you will lose points.

1. Prove each of the following. Either give a complete formal proof that the statement is true or a specific counter example with justification to prove that it is false.

   (a) For any integer n,
   $$\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right).$$

   ANSWER: False - disproof by counter example:
   Let n = 2.
   $n^2 = 4$
   $\frac{n^2}{4} = 1$
   $\lfloor \frac{n^2}{4} \rfloor = 1.$

   $\frac{n-1}{2} = \frac{1}{2}$
   $\frac{n+1}{2} = \frac{3}{2}$
   $\frac{1}{2} \cdot \frac{3}{2} = \frac{3}{4}.$

   Since, $1 \neq \frac{3}{4}$, this is a valid counter example.

   (b) For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.
   ANSWER: False: disproof by counter example:
   Let $x = 1.5$
   $\lfloor 1.5^2 \rfloor = 2$
   $\lfloor 1.5 \rfloor^2 = 1.$
   Since $1 \neq 2$, This is a valid counter example.

   (c) For all real numbers x and y, if x is irrational and y is rational then $x - y$ is irrational.
   ANSWER: True- proof by contrapositive.
   Original Statement: $\forall x, y \in R, (x \in Q \wedge y \notin Q) \rightarrow x - y \notin Q$
   Contrapositive: $\forall x, y \in R, x - y \in Q \rightarrow \sim (x \in Q \wedge y \notin Q)$
   by DeMorgan's and def of Impl: $\forall x, y \in R, (x - y) \in Q \rightarrow ((x \in Q) \rightarrow (y \in Q))$
   PROOF: Let x and y be arbitrary in R.
   Assume $x - y$ is rational.
   There exists $a, b \in Z$ such that $x - y = \frac{a}{b}$ and $b \neq 0$ by the definition of rational.
   Assume x is rational.
   There exists integers c, d such that $y = \frac{c}{d}$ and $d \neq 0$ by the definition of rational.

   y

$= (x - x) + y$ by algebra
$= x - (x - y)$ by associativity and commutativity
$= \frac{c}{d} - \frac{a}{b}$ by substitution
$= \frac{(bc-ad)}{bd}$ by algebra

Since $(bc - ad)$ and bd are integers by closure of integers in subtraction and multiplication, and since $bd \neq 0$ because both b and d are not 0, this implies y is also rational by the definition of rational.

Closing the conditional worlds in the reverse order of which they were opened gives us: $x - y \in Q \rightarrow (x \in Q \rightarrow y \in Q)$
Then by generalizing from the Generic Particular we get: $\forall x, y \in R, ((x - y) \in Q) \rightarrow ((x \in Q) \rightarrow (y \in Q))$
QED

(d) For all integers a, b and c, if $a|b$ and $a \nmid c$ then $a \nmid (b + c)$.
ANSWER: True - proof by generic particular
Rewrite: $\forall a, b, c \in Z, a|b \wedge a \nmid c \rightarrow a \nmid (b + c)$
PROOF:
Assume a, b, and c are all arbitrary in Z.

Assume $a|b \wedge a \nmid c$.
Since $a|b$, we know $\exists k \in Z, b = ka$ by definition of devides.
Since $a \nmid c$, we know $\exists q, r \in Z, c = qa + r$, where $0 < r < a$ by the quotient remainder theorem.
Then
$(b + c) = (ka + (qa + r))$ by substitution.
$(b + c) = a(k + q) + r$ where $0 < r < a$ by algebra
Since $k + q \in Z$ by closure of Z in addition, $a \nmid (b + c)$.
Closing the Conditional World we get: $a|b \wedge a \nmid c \rightarrow a \nmid (b + c)$.
And Generalizing from the Generic Particular we get: $\forall a, b, c \in Z, a|b \wedge a \nmid c \rightarrow a \nmid (b+c)$.
OR (Another Method)
Rewrite: $\forall a, b, c \in Z, a|b \wedge a \nmid c \rightarrow a \nmid (b + c)$
CONTRAPOSITIVE: $\forall a, b, c \in Z, a|(b + c) \rightarrow \sim (a|b \wedge a \nmid c)$
Using DeMorgan's: $foralla, b, c \in Z, a|(b + c) \rightarrow ((\sim a|b) \vee (a|c))$
Using the Def of Implication: $\forall a, b, c \in Z, a|(b + c) \rightarrow (a|b \rightarrow a|c))$
PROOF:
Let a,b, and c be arbitrary integers.
Assume $a|(b + c)$
Since $a|(b + c)$, $\exists k \in Z, b + c = ak$ by definition of divides.

Assume $a|b$.
Since $a|b$, $\exists m \in Z, b = am$ by definition of divides.
Since $b = am \wedge b + c = ak$, we know $am + c = ak$ by substitution of equals.

$c = ak - am$ by algebra.

$c = a(k - m)$ by distribution.

Since $k - m \in Z$ by closure of Z in subtraction.

$a|c$ by definition of divides.

Closing the first conditional world we get $a|b \rightarrow a|c$.

Closing the second conditional world we get $a|(b + c) \rightarrow ((a|b) \rightarrow (a|c))$

And, Generalizing from the Generic Particulars we get: $\forall a, b, c \in Z, a|(b + c) \rightarrow (a|b \rightarrow a|c)$.

(e) $\log_5 2$ is irrational.

ANSWER: True - Use the method of proof by contradiction.
Suppose $\log_5 2$ is rational.
Then there exists integers a, b with $b \neq 0$ such that $\log_5 2 = \frac{a}{b}$ by the definition of rational.
Since $\log_5 2$ is positive by rules of algebra. Both a and b would have to both be positive or both negative. If they are both negative, multiply the fraction by $\frac{-1}{-1}$ so that both a and b are positive integers.

	$5^{\log_5 2} = 2$	by algebra
Then	$5^{\frac{a}{b}} = 2$	by substitution
	$5^a = 2^b$	by raising both sides to the b power.

Since a, b are positive integers, 5^a and 2^b can both be prime factorized (in fact this is their prime factorization).
By the Unique Prime Factorization Theorem, they must be the same prime factorization.
This is a Contradiction because one factors to a set of 5's and the other to a set of 2's so they can not be the same prime factorization.

(f) For all integers n, if $n > 2$ then there is a prime number p such that $n < p < n!$ (hint: consider $n! - 1$).

ANSWER: True - Proof by constructive proof of existance.
PROOF:
Let n be arbitrary in Z.
Consider $n! - 1$.
First notice that if $n > 2$, then $n! - 1 \geq 2n - 1 > n$ by substitution of unequals on both sides.
It is either the case that $n! - 1$ is prime or it is not.
If $n! - 1$ is prime then we are done.
If $n! - 1$ is not prime, then it must have some prime factors. But for any primes $p \leq n$, $(n! - 1) \bmod p \neq 0$ since $n!$ has prime factor p. Therefore $n! - 1$ must have some prime factors that are greater than n (and these prime factors are certainly less than $(n!)$).

And generalizing from the Generic Particular we get:
$\forall n \in Z, n > 2 \rightarrow \exists p \in Z^{prime}, n < p < n!$.