CMSC 250 Fall 2004 — Homework #5

Due Friday, Oct. 8 at the beginning of your LECTURE 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.

Prove each of the following statements true or false. Remember, a counterexample may only be used to prove that a "for all" statement is false, and all counterexamples must include specific values and enough algebra/justification to show that they are truly counterexamples.
Your proofs must be complete as discussed in class -including things like a sequence of statements that are known to be true and the reason you know that the statement you wrote is true.

1. There is an integer n such that $2n^2 - 5n + 2$ is prime.
   Answer: True.
   Constructive Proof of Existence:
   when $n = 3$, $2 \cdot 3^2 - 5 \cdot 3 + 2 = 5$ which is prime.

2. For all integers n, if n is prime then $(-1)^n = -1$.
   Answer: False.
   Disproof by Counterexample:
   when $n = 2$, n is prime but $(-1)^2 = 1 \neq -1$.

3. For all integers $n \geq 1$, $n(n+1)(n+2)(n+3)$ is one less than a perfect square.
   Answer: True.
   Proof:
   Let n be an arbitrary integer.
   $n(n+1)(n+2)(n+3) + 1 = n^4 + 6n^3 + 11n^2 + 6n + 1$ by algebra.
   $= (n^2 + 3n + 1)^2$ by factoring the polynomial.
   Since $n^2 + 3n + 1 \in Z$ by closure of Z in multiplication and addition,
   $(n^2 + 3n + 1)^2$ must be a perfect square by definition of perfect square.
   Since $n(n+1)(n+2)(n+3) + 1 = (n^2 + 3n + 1)^2$, then
   $n(n+1)(n+2)(n+3) = (n^2 + 3n + 1)^2 - 1$ by subtracting 1 from both sides.
   This means, $n(n+1)(n+2)(n+3)$ is one less than a perfect square.
   Since n was defined as arbitrary above we can generalize from the generic particular,
   $\forall n \in Z, \exists x \in Z^{ps}$ where $n(n+1)(n+2)(n+3)$ is one less than x.
   note: Z^{ps} means the subset of Z that are perfect squares.

4. Given any two rational numbers r and s with $r < s$, there is another rational number between r and s. (Hint: consider $\frac{r+s}{2}$.)
   Answer: Translated to Formal Notation: $\forall r, s \in Q, (r < s) \rightarrow \exists m \in Q$ where $r < m < s$.
   True.
   Let r and s be arbitrary rational numbers in Q such that $r < s$.
   We then want to consider the value $\frac{r+s}{2}$.
   (a) We need to first prove that $\frac{r+s}{2}$ is indeed rational:
   Since r and s are rational by their definition above, $\exists a, b, c, d \in Z$ where $b \neq 0 \wedge d \neq 0$

such that $r = a/b$ and $s = c/d$ by the definition of rational.
$\frac{r+s}{2} = (\frac{a}{b} + \frac{c}{d})/2 = \frac{ad+bc}{2bd}$ by substitution of equalities and by algebra of finding a common denominator.
Since $(ad + bc)$ and $2bd$ are integers by the closure of integers in addition and multiplication
and since $2bd \neq 0$ because the only way to get a 0 as the product if to have one of the multipliers equal to 0,
$\frac{r+s}{2}$ is rational by the definition of rational.
Let's call this rational value m.

(b) Then we also need to prove that $r < \frac{r+s}{2} < s$:
$r = \frac{r+r}{2}$ by multiplying r by $\frac{2}{2}$
$\frac{r+r}{2} < \frac{r+s}{2}$ by substitution of unequals.
$r < m$ by substitution.
$s = \frac{s+s}{2}$ by multiplying s by $\frac{2}{2}$
$\frac{s+s}{2} > \frac{r+s}{2}$ by substitution of unequals.
$m < s$ by substitution.
$r < m < s$ by conjuctive addition of the two equalities above.

Therefore, $(\frac{r+s}{2})$ is both rational and between r and s by conjunctive addition of these two parts.
So $\frac{r+s}{2}$ is the value we needed to prove the statement true, and this is the value previously named m.
Therefore, $\forall r, s \in Q, r < s \rightarrow \exists m \in Q$ where $r < m < s$ by generalizing from the generic particulars r and s.

5. The sum of any two even numbers is a multiple of 4.
Answer: False.
Disproof by Counterexample: $2 + 4 = 6$ but $4 \nmid 6$.

6. For all integers a and b, if $a|b$ then $a^2|b^2$.
Answer: True.
Translation of the statement to formal notation:
$\forall a, b \in Z, a|b \rightarrow a^2|b^2$
Proof:
Let a and b be arbitrary members of Z.

Assume $a|b$.
Since $a|b$, $ak = b$ for some $k \in Z$ by definition of divides.
$(ak)^2 = b^2$ by squaring both sides, which means
$a^2k^2 = b^2$ by multiplying out the square.
Since k^2 is an integer by the closure of integers in multiplication, $a^2|b^2$ by definition of divisible. Therefore $a|b \rightarrow a^2|b^2$ by closing the conditional world.

$\forall a, b \in Z, a|b \rightarrow a^2|b^2$ by generalizing from the generic particular.

7. If n is an odd integer, then $n^4 \equiv_4 1$.
Answer: True.
Translation to formal notation:

$\forall n \in Z, n \in Z^{odd} \to n^4 \equiv_4 1$
Proof:
Let n by arbitrary in the integers.

Assume $n \in Z^{odd}$.
Since n is odd, $\exists k \in Z, n = 2k + 1$ by the definition of "odd".
$n^4 = (2k+1)^4 = 16k^4 + 32k^3 + 24k^2 + 8k + 1$ by substitution and algebra.
Then $n^4 = 4(4k^4 + 8k^3 + 6k^2 + 2k) + 1$ by distribution,
and $n^4 - 1 = 4(4k^4 + 8k^3 + 6k^2 + 2k)$ by subtracting 1 from both sides.
Since $4k^4 + 8k^3 + 6k^2 + 2k \in Z$ by closure of Z in addition and multiplication,
$4 | n^4 - 1$ by definition of divides.
This means that $n^4 \equiv_4 1$ by definition of equivalence in a mod.
In closing the conditional world, we get the implication that $n \in Z^{odd} \to n^4 \equiv_4 1$

Since n was defined above as arbitrary, we can generalize from the Generic Particular to get $\forall n \in Z, n \in Z^{odd} \to n^4 \equiv_4 1$.