CMSC 250 Homework 6 Spring 2006

Due Wed Mar 8 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.

For each of the following statements, prove that the statement is true, or give a counterexample to show that it is false.

1. There is an even prime number larger than two.

   FALSE.

   Proof (by contradiction).

   Let n be an even prime number larger than two.
   Then $\exists k \in Z, n = 2k$, by definition of even.
   Since $n > 2$, $2k > 2$, by substitution.
   $k > 1$, by algebra.
   Since $k > 0$, $2k > k$, by algebra (adding k to both sides).
   So $n > k$, by substitution.
   Thus, $1 < k < n$, by combining inequalities.
   Since, $1 < 2 < n$ by the hypothesis, there esits two integers,
   each strictly between 1 and n whose product is n.
   Therefore, n is not prime.
   QED

2. There are an infinite number of composite numbers that are not perfect squares.

   TRUE.

   Proof (by construction).

   There are an infinite number of odd primes $\{r_i\}_{i \in Z^+}$,
   since there an infinite number of primes and 2 is the only even one (by problem 1).
   Consider the set $\{s_i\}_{i \in Z^+} = \{2r_i\}_{i \in Z^+}$.
   Each element s_i is composite since $1 < 2 < s_i \wedge 1 < r_i < s_i \wedge 2r_i = s_i$, by the definition of composite.
   The set is infinite, since $\{r_i\}$ is infinite and no two elements are equal.
   (If $s_i = s_j$ for $i \neq j$, then $2r_i = 2r_j$ and $r_i = r_j$, by substitiion and algebra.)
   No number s_i is a perfect square, since its prime factors $(2, r_i)$ both have degree 1 in its prime factorization.
   QED

3. $\forall n \in \mathbf{Z}^{odd}$, $n^2 \equiv_8 1$.

   TRUE.

Proof (by dilemma).

Let n be arbitrary in Z, by universal instantiation.
$n \equiv_4 0 \ \vee \ n \equiv_4 1 \ \vee \ n \equiv_4 2 \ \vee \ n \equiv_4 3$, by the definition of mod and quotient remainder theorem.
Cases 0, 2: $n \equiv_0 0$, $n \equiv_4 2$.
n is even, so the antecedent is false.
So the statement is true.
Case 1: $n \equiv_4 1$.
$\exists k \in Z,\ n = 4k + 1$, by the definition of mod.
$n^2 = (4k+1)^2 = 16k^2 + 8k + 1 = 8(2k^2 + k) + 1$, by substitution and algebra.
$2k^2 + k$ is an integer, since the integers are closed under addition and multiplication.
$n^2 \equiv_8 1$, by the definition of mod.
QED
Case 3: $n \equiv_4 3$.
$\exists k \in Z,\ n = 4k + 3$, by the definition of mod.
$n^2 = (4k+3)^2 = 16k^2 + 24k + 9 = 8(2k^2 + k + 1) + 1$, by substitution and algebra.
$2k^2 + k + 1$ is an integer, since the integers are closed under addition and multiplication.
$n^2 \equiv_8 1$, by the definition of mod.
So, $n \in \mathbf{Z}^{odd} \rightarrow n^2 \equiv_8 1$, by dilemma.
$\forall n \in \mathbf{Z}^{odd}$, $n^2 \equiv_8 1$, by universal generalization.
QED

4. $\exists n \in \mathbf{Z}, n^2 \equiv_8 5$.

   FALSE.

   We will show $\sim \exists n \in \mathbf{Z}, n^2 \equiv_8 5$ is TRUE, which is equivalent to
   $\forall n \in \mathbf{Z}, n^2 \not\equiv_8 5$.

   Proof (by dilemma).

Let n be arbitrary in Z, by universal instantiation.
$n \equiv_8 0 \;\vee\; n \equiv_8 1 \;\vee\; n \equiv_8 2 \;\vee\; n \equiv_8 3 \;\vee\; n \equiv_8 4 \;\vee\; n \equiv_8 5 \;\vee\; n \equiv_8 6 \;\vee\; n \equiv_8 7$
by the Quotient Remainder Theorem

Case 0: $n \equiv_8 0$
$n^2 \equiv_8 0$, therefore $n^2 \not\equiv_8 5$, by algebra
Case 1: $n \equiv_8 1$
$n^2 \equiv_8 1$, therefore $n^2 \not\equiv_8 5$, by algebra
Case 2: $n \equiv_8 2$
$n^2 \equiv_8 4$, therefore $n^2 \not\equiv_8 5$, by algebra
Case 3: $n \equiv_8 3$
$n^2 \equiv_8 9$, therefore $n^2 \equiv_8 1$, therefore $n^2 \not\equiv_8 5$, by algebra
Case 4: $n \equiv_8 4$
$n^2 \equiv_8 16$, therefore $n^2 \equiv_8 0$, therefore $n^2 \not\equiv_8 5$, by algebra
Case 5: $n \equiv_8 5$
$n^2 \equiv_8 25$, therefore $n^2 \equiv_8 1$, therefore $n^2 \not\equiv_8 5$, by algebra
Case 6: $n \equiv_8 6$
$n^2 \equiv_8 36$, therefore $n^2 \equiv_8 4$, therefore $n^2 \not\equiv_8 5$, by algebra
Case 7: $n \equiv_8 7$
$n^2 \equiv_8 49$, therefore $n^2 \equiv_8 1$, therefore $n^2 \not\equiv_8 5$, by algebra

$n^2 \not\equiv_8 5$, by dilemma.
$\forall n \in \mathbf{Z}, n^2 \not\equiv_8 5$, by universal instantiation.
QED

5. There are an infinite number of pairs of integers $\{n, m\}$ such that $(n^2 + m^2) \equiv_8 5$.

Let $n \equiv_8 1$ and $m \equiv_8 2$.
Then $n^2 + m^2 \equiv_8 1^2 + 2^2 \equiv_8 5$, by substitution and algebra.
But there are an infinite number of integers satisfying $n \equiv_8 1$,
and an infinite number of integers satisfying $m \equiv_8 2$, by the definition of mod.
So there are an infinite number of pairs of integers $\{n, m\}$ such that $(n^2 + m^2) \equiv_8 5$.
QED

6. $\forall n \in \mathbf{Z}$, n^3 is odd if and only if n is odd.

TRUE.

We must show that if n is even then n^3 is odd then n is odd, and if n is odd then n^3 is odd. For the first statement, we construct the contrapositive and show that if n is even then n^3 is even. So we need to prove the following two statements:

$\forall n \in \mathbf{Z}$, if n is even then n^3 is even. $\quad$ $\forall n \in \mathbf{Z}$, if n is odd then n^3 is odd.

Proof.

Let n be arbitrary in Z.

|Assume n is even.
|Then $\exists k \in Z, n = 2k$, by definition of even.
|Let k satisfy $n = 2k$, by existential instantiation.
|$n^3 = (2k)^3 = 8k^3 = 2(4k^3)$, by substitution and algebra.
|$4k^3$ is an integer, by closure of Z under multiplication.
|So, n^3 is even, by the definition of even.

So, n is even $\rightarrow n^3$ is even, CCW w/o contradiction.
So, n^3 is odd $\rightarrow n$ is odd, by contrapositive.

|Assume n is odd.
|Then $\exists k \in Z, n = 2k+1$, by definition of odd.
|Let k satisfy $n = 2k+1$, by existential instantiation.
|$n^3 = (2k+1)^3 = 8k^3 + 4k^2 + 2k + 1 = 2(4k^3 + 2k^2 + k) + 1$, by substitution and algebra.
|$4k^3 + 2k^2 + k$ is an integer, by closure of Z under multiplication.
|So, n^3 is odd, by the definition of odd.

So, n is odd $\rightarrow n^3$ is odd, CCW w/o contradiction.

So, n^3 is odd $\rightarrow n$ is odd $\wedge$ n is odd $\rightarrow n^3$ is odd, by conjuctive addition.
So, n^3 is odd $\leftrightarrow n$ is odd, by the definiton of biconditional.
$\forall n \in \mathbf{Z}$, n^3 is odd if and only if n is odd, by universal generalization.
QED

7. $\forall p \in \mathbf{Z}^{prime}$, $\sqrt[3]{p}$ is irrational.

   TRUE.

   Proof (by contradiction).

Let p be arbitrary in Z^{prime}.

|Assume $\sqrt[3]{p}$ is rational.
|Then $\exists a, b \in Z, b \neq 0 \ \wedge \ \sqrt[3]{p} = \frac{a}{b}$, |by the definition of rational.
|Let $a, b \in Z$ satisfy $b \neq 0 \ \wedge \ \sqrt[3]{p} = \frac{a}{b}$, |by existential instantiation.
|Then $p = \frac{a^3}{b^3}$, by algebra.
|So $pb^3 = a^3$, by algebra.
|$\exists c \in Z^{\geq 0}, d \in Z^+, \ b = p^c d \ \wedge \ p \nmid d$, by the prime factorization theorem.
|$\exists e \in Z^{\geq 0}, f \in Z^+, \ a = p^e f \ \wedge \ p \nmid f$, by the prime factorization theorem.
|Hence, $p(p^c d)^3 = (p^e f)^3$, by substitution.
|Hence, $p^{3c+1} d^3 = p^{3e} f^3$, by algebra.
|So $3c + 1 = 3e$, since $p \nmid d$ and $p \nmid f$.
|So $3(e - c) = 1$, by algebra.
|So $3|1$, by definition of divides.
|Which is false.

So $\sqrt[3]{p}$ is irrational, CCW with contradiction.
$\forall p \in \mathbf{Z}^{prime}$, $\sqrt[3]{p}$ is irrational, by universal generalization.
QED

8. $\forall n \in \mathbf{Z}^{\geq 2}$, $\sqrt[n]{7}$ is irrational.

   TRUE.

Proof (by contradiction).

Let n be arbitrary in $Z^{\geq 2}$.
$|$Assume $\sqrt[n]{7}$ is rational.
$|$Then $\exists a, b \in Z, b \neq 0 \ \wedge \ \sqrt[n]{7} = \frac{a}{b}$, $\quad |$by the definition of rational.
$|$Let $a, b \in Z$ satisfy $b \neq 0 \ \wedge \ \sqrt[n]{7} = \frac{a}{b}$, $\quad |$by existential instantiation.
$|$Then $7 = \frac{a^n}{b^n}$, by algebra.
$|$So $7b^n = a^n$, by algebra.
$|\exists c \in Z^{\geq 0}, d \in Z^+, \ b = 7^c d \ \wedge \ 7 \not| d$, by the prime factorization theorem.
$|\exists e \in Z^{\geq 0}, f \in Z^+, \ a = 7^e f \ \wedge \ 7 \not| f$, by the prime factorization theorem.
$|$Hence, $7(7^c d)^n \ = \ (7^e f)^n$, by substitution.
$|$Hence, $7^{nc+1} d^n \ = \ (7^{ne} f^n)$, by algebra.
$|$So $nc + 1 = ne$, since $7 \not| d$ and $7 \not| f$.
$|$So $n(e - c) = 1$, by algebra.
$|$So $n|1$, by definition of divides.
$|$Which is false, since $n \geq 2$.
So $\sqrt[n]{7}$ is irrational, CCW with contradiction.
$\forall n \in \mathbf{Z}^{\geq 2}$, $\sqrt[n]{7}$ is irrational, by universal generalization.
QED

9. Let $p, q \in \mathbf{Z}^{prime}$ such that $p \neq q$. Then $\forall n \in \mathbf{Z}$ such that $0 < n < pq$, it is not the case that $p|n$ and $q|n$.

TRUE.

Proof.

Let p, q be arbitrary in Z^+.
Let $n < pq$, where $n \in Z^+$.
$|$Assume $p|n$.
$|$Then there exists a such that $n = ap$ by definition of divides.
$|ap < pq$, by substitution, since $n < pq$.
$|$So, $a < q$, by algebra.
$|q \not| a$, since $a < q$.
$|q \not| p$, since p is prime.
$|$Thus, $q \not| ap$, by the prime factorization theorem.
$|$So, $q \not| n$, by substitution.
Thus, $p|n \rightarrow q \not| n$, CCW without contradiction.
So, $p \not| n \vee q \not| n$ by definition of conditional.
So, $\sim (p|n \wedge q|n)$, by deMorgan.
Thus, $\forall n \in \mathbf{Z}$ such that $0 < n < pq$, $\sim (p|n \wedge q|n)$, by universal generalization.
QED

10. Let $a, b, c \in \mathbf{Z}$ such that $a^3 = b^4 = c$, and let p be a prime number. If $p|a$, then $p^3|b$.

TRUE.

Proof (by contradiction).

$\exists c \in Z^{\geq 0}, d \in Z^{+},\ a = p^c d \ \wedge \ p \not| d$, by the prime factorization theorem.
$\exists e \in Z^{\geq 0}, f \in Z^{+},\ b = p^e f \ \wedge \ p \not| f$, by the prime factorization theorem.
So, $(p^c d)^3 \ = \ (p^e f)^4$, by substitution.
So, $p^{3c} d^3 \ = \ p^{4e} f^4$, by substitution.
So, $3c \ = \ 4e$
$c > 1$, since $p|a$, by the prime factorization theorem.
So, $3c > 1$, by algebra.
So, $4e > 1$, by substitution.
So, $e > 1$, since e is an integer.
So, $p|b$, by the prime factorization theorem.
QED