CMSC250, Spring 2004 — Homework 5 Answers

Due Wednesday, March 3 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.

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.

1. For all integers a, b, and c, if $a + b = c$ and $a \mid b$, then $a \mid c$.

   Answer: TRUE.
   Let a, b, and c be arbitrary integers.
   Assume $a + b = c$ and $a \mid b$.
   Since $a \mid b$, $\exists k \in \mathbf{Z}$ $ak = b$ by definition of divides.
   $ak + a = b + a$ by adding a to both sides.
   $a(k + 1) = c$ by algebra and substitution.
   $k + 1 \in \mathbf{Z}$ by closure of the integers under addition.
   $a \mid c$ by definition of divides.
   $\forall a, b, c \in \mathbf{Z}$ $(a + b = c) \wedge (a \mid b) \rightarrow (a \mid c)$ by closing of conditional world and generalizing from the generic particular.

2. $\forall a, b, c \in \mathbf{Z}$ $[(a \mid c) \wedge (b \mid c)] \rightarrow [(a \mid b) \vee (b \mid a)]$

   Answer: FALSE.
   Counterexample: Let $a = 2$, $b = 3$, and $c = 6$.
   Then $a \mid c$ and $b \mid c$ since $2 \mid 6$ and $3 \mid 6$. However, $2 \nmid 3$ and $3 \nmid 2$.

3. $\forall a, b, c \in \mathbf{Z}$ $[(a \mid b) \wedge (a \mid c)] \rightarrow [(b \mid c) \vee (c \mid b)]$

   Answer: FALSE.
   Counterexample: Let $a = 2$, $b = 4$, and $c = 6$.
   Then $a \mid b$ and $a \mid c$ since $2 \mid 4$ and $2 \mid 6$. However, $4 \nmid 6$ and $6 \nmid 4$.

4. If $a \mid b$ and $b \mid c$, then $a \mid c$, for any integers a, b, and c.

   Answer: TRUE.
   Let a, b, and c be arbitrary integers.
   Assume $a \mid b$ and $b \mid c$.
   Then $\exists m, n \in Z$ $am = b \wedge bn = c$.
   Since $am = b$, then $(am)n = c$, which means $a(mn) = c$ by substitution and associativity.
   Since $mn \in \mathbf{Z}$ by closure of the integers under multiplication,
   $a \mid c$ by definition of divides.
   $\forall a, b, c \in \mathbf{Z}$ $(a \mid b) \wedge (b \mid c) \rightarrow (a \mid c)$ by closing of conditional world and generalizing from the generic particular.

5. If x is an odd integer, then $x^2 - 1$ is divisible by 4.

Answer: TRUE.
Let x be an arbitrary odd integer.
Since x is odd, $\exists k \in \mathbf{Z}\ x = 2k + 1$.
Then $x^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k^2 + 4k$ by substitution and algebra.
Then $x^2 - 1 = 4(k^2 + k)$ by algebra.
Since $k^2 + k \in \mathbf{Z}$ by closure of the integers under positive exponentiation and addition,
$4 \mid (x^2 - 1)$ by definition of divides.
$\forall x \in \mathbf{Z}^{\text{odd}}\ 4 \mid (x^2 - 1)$ by generalizing from the generic particular.

6. If a prime greater than 2 can be represented as $3k + 2$ for some integer k, then that prime can be represented as $6m + 5$ for some integer m.

Answer: TRUE.
Let p be an arbitrary prime greater than 2.
Assume $\exists k \in \mathbf{Z}\ p = 3k + 2$.
Since k is an integer, k is either even or odd.

Assume k is even.
Then $\exists g \in \mathbf{Z}\ k = 2g$.
Then $p = 3k + 2 = 3(2g) + 2 = 6g + 2 = 2(3g + 1)$ by substitution and algebra.
Since $3g + 1 \in \mathbf{Z}$ by closure of the integers under multiplication and addition,
$2 \mid p$ by definition of divides.
However, this is a contradiction since p is a prime greater than 2.

So we know k is not even, and therefore, k is odd.
Then $\exists g \in \mathbf{Z}\ k = 2g + 1$. Then $p = 3k + 2 = 3(2g + 1) + 2 = 6g + 3 + 2 = 6g + 5$ by substitution and algebra.
$\forall p \in \mathbf{Z}^{\text{prime}>2}\ (\exists k \in \mathbf{Z}\ p = 3k + 2) \rightarrow (\exists m \in \mathbf{Z}\ p = 6m + 5)$ by closing conditional world and generalizing from the generic particular.

7. For any integer n, $n^3 \not\equiv_4 2$.

Answer: TRUE.
Let n be an arbitrary integer.
Assume (by the way of contradiction) that $n^3 \equiv_4 2$.
Therefore $4 \mid (n^3 - 2)$ by definition of mod, which means
$\exists k \in \mathbf{Z}\ n^3 = 4k + 2$.
By the quotient-remainder theorem, there exist unique integers q and r such that $n = 4q + r$ and $0 \leq r < 4$.

Case 1: assume $r = 0$.
So $n = 4q$ by substitution.
Then $n^3 = (4q)^3 = 64q^3$ by substitution and algebra.
Since $n^3 = 4k + 2$, then we know $4k + 2 = 64q^3$ by substitution.
Then $1/2 = 16q^3 - k$ by algebra.
We know that $16q^3 - k \in \mathbf{Z}$ by closure of the integers under multiplication, addition, and positive exponentiation, however, $1/2 \notin \mathbf{Z}$. Contradiction.

Case 2: assume $r = 1$.
So $n = 4q + 1$ by substitution.
Then $n^3 = (4q + 1)^3 = 64q^3 + 48q^2 + 12q + 1$ by substitution and algebra.
Since $n^3 = 4k + 2$, then we know $4k + 2 = 64q^3 + 48q^2 + 12q + 1$ by substitution.

Then $1/4 = 16q^3 + 12q^2 + 3q - k$ by algebra.
We know that $16q^3 + 12q^2 + 3q - k \in \mathbf{Z}$ by closure of the integers under multiplication, addition, and positive exponentiation, however, $1/4 \notin \mathbf{Z}$. Contradiction.

Case 3: assume $r = 2$.
So $n = 4q + 2$ by substitution.
Then $n^3 = (4q + 2)^3 = 64q^3 + 96q^2 + 48q + 8$ by substitution and algebra.
Since $n^3 = 4k + 2$, then we know $4k + 2 = 64q^3 + 96q^2 + 48q + 8$ by substitution.
Then $1/4 = 16q^3 + 24q^2 + 12q + 2 - k$ by algebra.
We know that $16q^3 + 24q^2 + 12q + 2 - k \in \mathbf{Z}$ by closure of the integers under multiplication, addition, and positive exponentiation, however, $1/2 \notin \mathbf{Z}$. Contradiction.

Case 3: assume $r = 3$.
So $n = 4q + 3$ by substitution.
Then $n^3 = (4q + 3)^3 = 64q^3 + 144q^2 + 108q + 27$ by substitution and algebra.
Since $n^3 = 4k + 2$, then we know $4k + 2 = 64q^3 + 144q^2 + 108q + 27$ by substitution.
Then $-25/4 = 16q^3 + 36q^2 + 27q - k$ by algebra.
We know that $16q^3 + 36q^2 + 27q - k \in \mathbf{Z}$ by closure of the integers under multiplication, addition, and positive exponentiation, however, $-25/4 \notin \mathbf{Z}$. Contradiction.

So all four cases lead to contradictions. However, one of the cases must be true by the quotient-remainder theorem, which is in itself another contradiction, which means our original assumption must be false.

So $n^3 \not\equiv_4 2$.
$\forall n \in \mathbf{Z}\ n^3 \not\equiv_4 2$ by generalizing from the generic particular.

8. $\forall x \in \mathbf{Z}^{\text{even}}\ (3 \nmid x) \to (4 \mid x^2)$

Answer: Let x be an arbitrary even integer.
Assume that $3 \nmid x$.
By the quotient-remainder theorem, there exist unique integers q and r such that $x = 3q + r$ and $0 \leq r < 3$.
So $(x = 3q) \vee (x = 3q + 1) \vee (x = 3q + 2)$ by enumerating all the possibilities.

Case 1: assume $x = 3q$.
Then $3 \mid x$ by definition of divides, which is a contradiction. So case 1 can never occur.

Case 2: assume $x = 3q + 1$.
Since q is an integer, q is either odd or even.

Assume that q is even.
Then $\exists k \in \mathbf{Z}\ q = 2k$ by definition of even.
Then $x = 3(2k) + 1 = 6k + 1$ by algebra and substitution.
However, we claimed that x was even, which means $\exists m \in \mathbf{Z}\ x = 2m$. Then $6k + 1 = 2m$ by substitution.
$1/2 = m - 3k$ by algebra, which is a contradiction since $m - 3k \in \mathbf{Z}$ by closure of the integers under multiplication and subtraction, but $1/2 \notin \mathbf{Z}$.

So q cannot be even, and therefore q is odd (by disjunctive syllogism).
Then $\exists k \in \mathbf{Z}\ q = 2k + 1$ by definition of odd.
Then $x = 3(2k + 1) + 1 = 6k + 3 + 1 = 6k + 4$ by algebra and substitution.
$x^2 = (6k + 4)^2 = 36k^2 + 48k + 4 = 4(9k^2 + 12k + 1)$ by substitution and algebra.

Since $9k^2+12k+1 \in \mathbf{Z}$ by closure of the integers under multiplication, addition, and positive exponentiation,
$4 \mid x^2$ by definition of divides.

Case 3: assume $x = 3q + 2$.
Since q is an integer, q is either odd or even.

Assume that q is odd.
Then $\exists k \in \mathbf{Z}\ q = 2k + 1$ by definition of odd.
Then $x = 3(2k + 1) + 1 = 6k + 3 + 2 = 6k + 5$ by algebra and substitution.
However, we claimed that x was even, which means $\exists m \in \mathbf{Z}\ x = 2m$. Then $6k + 5 = 2m$ by substitution.
$5/2 = m-3k$ by algebra, which is a contradiction since $m-3k \in \mathbf{Z}$ by closure of the integers under multiplication and subtraction, but $5/2 \notin \mathbf{Z}$.

So q cannot be odd, and therefore q is even (by disjunctive syllogism).
Then $\exists k \in \mathbf{Z}\ q = 2k$ by definition of even.
Then $x = 3(2k) + 2 = 6k + 2$ by algebra and substitution.
$x^2 = (6k + 2)^2 = 36k^2 + 24k + 4 = 4(9k^2 + 6k + 1)$ by substitution and algebra.
Since $9k^2+6k+1 \in \mathbf{Z}$ by closure of the integers under multiplication, addition, and positive exponentiation,
$4 \mid x^2$ by definition of divides.

Since case 1 never occurs, and cases 2 and 3 both lead to $4 \mid x^2$, we can conclude that $4 \mid x^2$.
$\forall x \in \mathbf{Z}^{\text{even}}\ (3 \nmid x) \rightarrow (4 \mid x^2)$ by closing the conditional world and generalizing from the generic particular.

Note: This problem could also be done by invoking the quotient-remainder theorem using 6 as the divisor instead of 3. There would be six cases, but four of them would lead to contradiction (like case 1 did here).

9. There exists an integer $m > 1$ such that $m^4 - 1$ is prime.

Answer: FALSE.
Note: We are going to prove an existential statement false. This is equivalent to proving that its negation is true. And the negation of an existential statement is a universal statement. So we must do this proof using the generic particular, just like all the other universal proofs.

Let m an arbitrary integer, and assume m is greater than 1. (We want to show that no matter what integer we pick, $m^4 - 1$ will not be prime).
By algebra, $m^4 - 1 = (m^2 - 1)(m^2 + 1)$.
Since $m > 1$, both $m^2 - 1$ and $m^2 + 1$ are greater than 1.
Therefore $m^4 - 1$ cannot be prime because a prime number has only two factors: itself and 1.
$\forall m \in \mathbf{Z}\ (m > 1) \rightarrow [(m^4 - 1) \notin \mathbf{Z}^{\text{prime}})]$ by closing the conditional world and generalizing from the generic particular.