CSE 390z: Mathematics for Computation Workshop

Week 4 Workshop Solutions

Conceptual Review

(a) What's the definition of "a divides b"?

Solution:

$a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$

(b) What's the definition of "a is congruent to b modulo m"?

Solution:

$a \equiv b \pmod{m} \ \leftrightarrow\ m \mid (a - b)$

(c) What's a good strategy for writing English proofs?

Solution:

- For each for all quantifier, introduce an arbitrary variable.
- If there is an implication, assume the left-hand side of the statement.
- Unroll the definitions using given predicates and theorems.
- Use propositional logic rules and / or math to manipulate the definitions. This is the creative part of the proof.
- Re-roll your definitions to derive the desired outcome.
- Conclude by summarizing your claim.

1. Modular Computation

(a) Circle the statements below that are true.
Recall for $a, b \in \mathbb{Z}$: $a|b$ iff $\exists k \in \mathbb{Z}\ (b = ka)$.

(a) $1|3$
(b) $3|1$
(c) $2|2018$
(d) $-2|12$
(e) $1 \cdot 2 \cdot 3 \cdot 4|1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

Solution:

(a) True
(b) False
(c) True
(d) True
(e) True

(b) Circle the statements below that are true.
Recall for $a, b, m \in \mathbb{Z}$ and $m > 0$: $a \equiv b \pmod{m}$ iff $m|(a-b)$.

(a) $-3 \equiv 3 \pmod{3}$

(b) $0 \equiv 9000 \pmod{9}$

(c) $44 \equiv 13 \pmod{7}$

(d) $-58 \equiv 707 \pmod{5}$

(e) $58 \equiv 707 \pmod{5}$

Solution:

(a) True

(b) True

(c) False

(d) True

(e) False

2. An Odd Proof

Prove that if n, m are odd, then $2n + m$ is odd.

Solution:

Let n, m be arbitrary odd integers. Then by definition of odd, $n = 2k + 1$ for some integer k. Similarly by definition of odd, $m = 2j + 1$ for some integer j. Then $2n + m = 2(2k + 1) + 2j + 1 = 4k + 2 + 2j + 1 = 4k + 2j + 3 = 2(2k + j + 1) + 1$. Since k, j are integers, and by closure of integers under multiplication and addition, $2k + j + 1$ is an integer. Then by definition, $2n + m$ is odd.

3. Proofs by Contrapositive

For each part, write a proof by contrapositive of the statement.

(a) If $a^2 \not\equiv b^2 \pmod{n}$, then $a \not\equiv b \pmod{n}$.

Solution:

We argue by contrapositive. Suppose $a \equiv b \pmod{n}$. Then, by definition of equivalence mod n, $n|(a-b)$ and by definition of divides, there exists some integer k such that $a - b = nk$. Multiplying both sides of the equation by $a + b$, we get $(a - b)(a + b) = a^2 - b^2 = nk(a + b)$. Since integers are closed under addition and multiplication, $k(a+b)$ must be an integer. Therefore, $n|a^2 - b^2$ by definition of divides and $a^2 \equiv b^2 \pmod{n}$ by definition of equivalence mod n.

(b) For all integers a, b, if $3 \nmid ab$, then $3 \nmid a$ and $3 \nmid b$.

Solution:

Let a, b be an arbitrary integers. We argue by contrapositive. Suppose $3 \mid a$ or $3 \mid b$. Thus, there are two cases to consider:

Case 1:

Suppose $3 \mid a$. Then, by definition of divides, there exists some integer k such that $a = 3k$. Multiplying both sides by b, we get $ab = 3kb$. Since integers are closed under multiplication, kb is an integer. Then, by definition of divides, $3 \mid ab$.

Case 2:

Suppose $3 \mid b$. Then, by definition of divides, there exists some integer j such that $b = 3j$. Multiplying

both sides by a, we get $ab = 3ja$. Since integers are closed under multiplication, ja is an integer. Then, by definition of divides, $3 \mid ab$.
In both cases, if $3 \mid a$ or $3 \mid b$, then $3 \mid ab$. Thus, the contrapositive is also true. Since a, b were arbitrary, this proves that the statement is true for all integers a, b.

4. Proofs by Contradiction

For each part, write a proof by contradiction of the statement.

(a) If a is rational and ab is irrational, then b is irrational.

Solution:

Suppose for the sake of contradiction that this statement is false, meaning there exists an a, b where a is rational and ab is irrational, and b is not irrational. Then, b is rational. By definition of rational, $a = \frac{s}{t}$ and $b = \frac{x}{y}$ for some integers s, t, x, y where $t \neq 0$ and $y \neq 0$. Multiplying these together, we get $ab = \frac{sx}{ty}$. Since integers are closed under multiplication, sx, ty are integers. And since the product of two non zero integers cannot be zero, $ty \neq 0$. Thus, ab is rational. This is a contradiction since we stated that ab was irrational. Therefore, the original statement must be true.

(b) For all integers n, $4 \nmid n^2 - 3$.

Solution:

Suppose for the sake of contradiction there exists an integer n such that $4 \mid (n^2 - 3)$. Then, by definition of divides, there exists an integer k such that $n^2 - 3 = 4k$. We will consider two cases:
Case 1: n is even
By definition of even, there is some integer a where $n = 2a$. Substituting n into the equation above, we get $(2a)^2 - 3 = 4a^2 - 3 = 4k$. By algebra,

$$k = \frac{4a^2 - 3}{4} = a^2 - \frac{3}{4}$$

Since integers are closed under multiplication, a^2 must be an integer. Since $\frac{3}{4}$ is not an integer, k must not be an integer. This is a contradiction, since k was introduced as an integer.
Case 2: n is odd
By definition of odd, there is some integer b where $n = 2b + 1$, Substituting n into the equation above, we get $(2b + 1)^2 - 3 = 4b^2 + 4b + 1 - 3 = 4k$. By algebra,

$$k = \frac{4b^2 + 4b - 2}{4} = b^2 + b - \frac{1}{2}$$

Since integers are closed under multiplication and addition, $b^2 + b$ must be an integer. Since $\frac{1}{2}$ is not an integer, k is not an integer. This is a contradiction, since k was introduced as an integer.
As shown, all cases led to a contradiction, so the original statement must be true.

5. Don't be Irrational!

Recall that the predicate Rational(x) is defined as $\exists a \exists b(\text{Integer}(a) \wedge \text{Integer}(b) \wedge b \neq 0 \wedge x = \frac{a}{b})$.
One of the following statements is true, and one is false:

- If xy and x are both rational, then y is also rational.
- If $x - y$ and x are both rational, then y is also rational.

Decide which statement is true and which statement is false. Prove the true statement, and disprove the false statement. For the disproof, it will be helpful to use proof by counterexample.

Solution:

Claim: If xy and x are both rational, then y is also rational.
We wish to disprove this through counterexample. Let x be 0, which is rational. $x * y$ will be 0 regardless of y, so for an irrational y like $y = \pi$, x and xy are rational, while y is not.

Claim: If $x - y$ and x are both rational, then y is also rational.

Proof. Suppose x and $x - y$ are rational. By the definition of rational numbers, if x and $x - y$ are rational, then there are $a, b, n, m \in \mathbb{Z}$ with $b, m \neq 0$ such that $x = \frac{a}{b}$ and $x - y = \frac{n}{m}$. Then:

$$\begin{aligned} x - y &= \frac{n}{m} && \text{Given} \\ y &= x - \frac{n}{m} && \text{Algebra} \\ y &= \frac{a}{b} - \frac{n}{m} && \text{Substituting } x = \frac{a}{b} \end{aligned}$$

Now we can rearrange this expression for y:

$$\begin{aligned} y &= \frac{a}{b} - \frac{n}{m} \\ &= \frac{a}{b} * \frac{m}{m} - \frac{n}{m} * \frac{b}{b} \\ &= \frac{am}{bm} - \frac{nb}{bm} \\ &= \frac{am - bn}{bm} \end{aligned}$$

Since integers are closed on multiplication and subtraction, $am, bn, bm \in \mathbb{Z}$, and therefore $am - bn \in \mathbb{Z}$. Since $b, m \neq 0$, $bm \neq 0$ also, and therefore for $p = am - bn$ and $q = bm$, $y = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ with $q \neq 0$. By the definition of rational, y is rational. □

6. More Number Theory Practice

For each of the following parts, prove or disprove the claim.

(a) If $a \mid b$ and $c \mid (-a)$, then $(-c) \mid b$.

Solution:

Suppose $a \mid b$ and $c \mid (-a)$. By definition of divides, $b = ka$ and $-a = cj$ for some integers k, j. By algebra, $a = -cj$. Substituting a into the first equation, we get $b = k(-cj) = (kj)(-c)$. Then, by definition of divides, $(-c) \mid b$ and the claim holds.

(b) For all $a, b, n, x \in \mathbb{Z}$, $a \equiv_n b$ implies $x^a \equiv_n x^b$.

Solution:

We can disprove this through counterexample. Let $a = 2, b = 5, n = 3, x = 2$. Since $2 \equiv_3 5$, $a \equiv_n b$. But $2^2 \not\equiv_3 2^5$ because $2^2 \pmod 3 = 4 \pmod 3 = 1$ and $2^5 \pmod 3 = 32 \pmod 3 = 2$, and $1 \neq 2$. Therefore, the implication is false.

(c) For all integers n, if n is not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

Solution:

Let n be an arbitrary integer and suppose that n is not divisible by 3. Then, there are two cases:
Case 1: $n \equiv 1 \pmod 3$
By definition of congruence and divides, $3 \mid (n-1)$ so $n-1 = 3k$ for some integer k. Rearranging, we get $n = 3k+1$. So, $n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. Then, $n^2 - 1 = 3(3k^2 + 2k)$. Since $3k^2 + 2k$ is an integer, $3 \mid (n^2 - 1)$ by definition of divides. By definition of congruence, $n^2 \equiv 1 \pmod 3$

Case 2: $n \equiv 2 \pmod 3$
By definition of congruence and divides, $3|(n-2)$ so $n - 2 = 3j$ for some integer j. Rearranging, we get $n = 3j + 2$. So, $n^2 = 9j^2 + 12j + 4 = 3(3j^2 + 4j + 1) + 1$. Then, $n^2 - 1 = 3(3j^2 + 4j + 1)$. Since $3j^2+4j+1$ is an integer, $3 \mid (n^2-1)$ by definition of divides. By definition of congruence, $n^2 \equiv 1 \pmod 3$. So, in all cases, $n^2 \equiv 1 \pmod 3$. Since n was arbitrary, the claim holds for all integers n.

7. Modular Multiplication

Write an English proof to prove that for an integer $m > 0$ and any integers a, b, c, d, if $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $ac \equiv bd \pmod m$.

Solution:

Let $m > 0$, a, b, c, d be arbitrary integers. Assume that $a \equiv b \pmod m$ and $c \equiv d \pmod m$. Then by definition of mod, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integer k such that $a - b = mk$, and there exists some integer j such that $c - d = mj$. Then $a = b + mk$ and $c = d + mj$. So, multiplying, $ac = (b + mk)(d + mj) = bd + mkd + mjb + m^2jk = bd + m(kd + jb + mjk)$. Subtracting bd from both sides, $ac - bd = m(kd + jb + mjk)$. By definition of divides, $m \mid ac - bd$. Then by definition of congruence, $ac \equiv bd \pmod m$.