CSE 390z: Mathematics for Computation Workshop

Week 4 Workshop Solutions

Conceptual Review

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

Solution:

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

(b) What's the definition of "a is congruent to b mod m" ($a \equiv b \pmod{m}$)?

Solution:

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

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

Solution:

(1) For each "for all" quantifier, introduce an arbitrary variable.
(2) If there is an implication, assume the left-hand side of the statement.
(3) Unroll the definitions using given predicates and theorems.
(4) Use propositional logic rules and / or math to manipulate the definitions. This is the creative part of the proof.
(5) Re-roll your definitions to derive the desired outcome.
(6) 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 $\exists k \in \mathbb{Z}\ (b = ak)$.

(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 $m|(b-a)$.

(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. Divisibility Proof

Consider the following claim where the domain is the integers:

$$\forall n \forall d \ ((d \mid n) \to (-d \mid n))$$

(a) Write a **formal proof** to show that the claim holds.

Solution:

Let a and b be arbitrary integers.

1.1.1	$b \mid a$	(Assumption)
1.1.2	$\exists k \ (a = kb)$	(Definition of divides: 1.1.1)
1.1.3	$a = jb$	(Elim $\exists$: 1.1.2)
1.1.4	$a = (-j)(-b)$	(Algebra: 1.1.3)
1.1.5	$\exists k \ (a = k(-b))$	(Intro $\exists$: 1.1.4)
1.1.6	$-b \mid a$	(Definition of divides: 1.1.5)
1.1	$(b \mid a) \to (-b \mid a)$	(Direct proof)
1.	$\forall n \forall d \ ((d \mid n) \to (-d \mid n))$	(Intro $\forall$)

(b) Translate the claim into English.

Solution:

For integers n, d, if $d \mid n$, then $-d \mid n$.

(c) Write an **English proof** to show that the claim holds.

Solution:

Let d, n be arbitrary integers, and suppose $d|n$. By definition of divides, there exists some integer k such that $n = kd = 1 \cdot kd$. Note that $-1 \cdot -1 = 1$. Substituting, we see $n = (-1)(-1)kd$. Rearranging, we have $n = (-k)(-d)$. Therefore, by definition of divides, $-d|n$. Since d and n were arbitrary, we have shown that for all integers d and n, if $d|n$, then $-d|n$.

3. Proofs by Contrapositive Part 1

Prove the following statement.

For all integers a, b, n, with $n > 0$: If $a^2 \not\equiv b^2 \pmod{n}$, then $a \not\equiv b \pmod{n}$.

(a) Why is this statement hard to prove with a Direct Proof? Try it out. Where do you get stuck?

Solution:

A direct proof would go something like: Let a, b, n be arbitrary integers with $n > 0$. Suppose $a^2 \not\equiv b^2 \pmod{n}$. By definition of mod, this means $n \nmid (b^2 - a^2)$, and by definition of divides this means there does not exist an integer k such that $(b^2 - a^2) = nk$. And now...what do I do with this? Knowing that something *isn't* true doesn't give you much to work with. Knowing that something *is* true does.

(b) What is the contrapositive of the statement?

Solution:

If $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$

(c) Prove the original statement by contrapositive (using an English proof).

Solution:

We argue by contrapositive. Let a, b, n be arbitrary integers with $n > 0$. Suppose $a \equiv b \pmod{n}$. Then, by definition of mod, $n|(b - a)$ and by definition of divides, there exists some integer k such that $b - a = nk$. Multiplying both sides of the equation by $b + a$, we get

$$(b - a)(b + a) = b^2 - a^2 = nk(b + a)$$

Since k, a, and b are integers, $k(a + b)$ must be an integer. Therefore, $n|b^2 - a^2$ by definition of divides and $a^2 \equiv b^2 \pmod{n}$ by definition of mod. Since a, b, n were arbitrary, we have shown that for all integers a, b and positive integers n, if $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.

Since the contrapositive holds iff the original statement holds, we have also shown that for all integers a, b and positive integers n, if $a^2 \not\equiv b^2 \pmod{n}$, then $a \not\equiv b \pmod{n}$.

4. 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 $c = d + mj$. Multiplying gives us:

$$ac = (b + mk)(d + mj) = bd + mkd + mjb + m^2jk = bd + m(kd + jb + mjk)$$

Subtracting bd from both sides we get, $ac - bd = m(kd + jb + mjk)$. Since k, d, j, b, m are all integers, $(kd + jb + mjk)$ is also an integer. By definition of divides, $m \mid ac - bd$. Then by definition of congruence, $ac \equiv bd \pmod{m}$. Since $m > 0$, a, b, c, d were arbitrary integers, the claim holds for all integers a, b, c, d and positive integers m.

5. An Odd Proof

Write and English proof of the following statement: 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 and $m = 2j + 1$ for some integer j. Then

$$2n + m = 2(2k + 1) + 2j + 1 = 4k + 2 + 2j + 1 = 2(2k + j + 1) + 1$$

Since k, j are integers, $2k + j + 1$ is an integer. Then by definition, $2n + m$ is odd. Since n and m were arbitrary odd integers, we have shown that for all integers n, m, if n and m are odd then $2n + 1$ is odd.

6. Proofs by Contrapositive Part 2

Prove the following statement.

For all integers a, b: If $3 \nmid ab$, then $3 \nmid a$ and $3 \nmid b$.

(a) Why is this statement hard to prove with a Direct Proof? Try it out. Where do you get stuck?

Solution:

A direct proof would go something like: Let a, b be arbitrary integers. Suppose $3 \nmid ab$. By definition of divides, there does not exist an integer k such that $ab = 3k$. Ok..and...I'm stuck. Knowing that something *isn't* true doesn't give you much to work with. Knowing that something *is* true does.

(b) What is the contrapositive of the statement?

Solution:

If $3 \mid a$ or $3 \mid b$ then $3 \mid ab$

(c) Prove the original statement by contrapositive (using an English proof).

Solution:

We argue by contrapositive. Let a, b be an arbitrary integers. Suppose $3 \mid a$ or $3 \mid b$. There are two cases to consider:
Case 1 ($3 \mid a$):
Suppose $3 \mid a$. By definition of divides, there exists some integer k such that $a = 3k$. Multiplying both sides by b, we get $ab = 3kb$. Since k and b are both integers, kb is an integer. So, by definition of divides, $3 \mid ab$.
Case 2 ($3 \mid b$):
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 j and a are both integers, ja is an integer. So, by definition of divides, $3 \mid ab$.

We have shown that in both cases, $3 \mid ab$. Since a, b were arbitrary, we have shown that for all integers a, b, if $3 \mid a$ or $3 \mid b$ then $3 \mid ab$.

Since the contrapositive holds iff the original statement holds, we have also shown that for all integers a, b, if $3 \nmid ab$ then $3 \nmid a$ and $3 \nmid b$.

7. Proofs by Contradiction

Prove each statement by contradiction (using an English proof).

(a) Recall that a real number x is **rational** iff there exists integers p and q, with $q \neq 0$, such that $x = \frac{p}{q}$.
Prove: For all real numbers a, b, if a is rational and ab is irrational, then b is irrational.

Solution:

Note: When doing a proof by contradiction, we start by assuming the claim is false. To do that, we negate the claim and assume the negation is true.

When we negate something that looks like $\forall x(P(x) \to Q(x))$, we get

$$\neg\forall x(P(x) \to Q(x)) \equiv \exists x\neg(P(x) \to Q(x)) \equiv \exists x\neg(\neg P(x) \vee Q(x)) \equiv \exists x(P(x) \wedge \neg Q(x))$$

So, to prove something of the form $\forall x(P(x) \to Q(x))$ by contradiction, start by assuming $\exists x(P(x) \wedge \neg Q(x))$, (i.e., assume that there is some value of x for which the hypothesis of the implication is true and the conclusion is false). We will then use only true statements and arrive at something impossible. This will allow us to conclude that our assumption must be false, and the original statement therefore must be true.

Proof:
Suppose for the sake of contradiction that this statement is false, meaning there exists real numbers 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 s, t, x, y are all integers, sx, ty are integers. And since $t \neq 0$ and $y \neq 0$, $ty \neq 0$. Thus, by definition of rational, ab is rational. But we said earlier that ab was irrational. This is a contradiction. Therefore, the original statement must be true.

(b) For all integers n, $4 \nmid n^2 - 3$.
Hint: It may be helpful to use cases.

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 $n = 2a$ into $n^2 - 3 = 4k$, we get $(2a)^2 - 3 = 4a^2 - 3 = 4k$.
Dividing both sides by 4, we get $a^2 - \frac{3}{4} = k$
Rearranging gives us $a^2 - k = \frac{3}{4}$
Since a and k are both integers, $a^2 - k$ is an integer. This means that $\frac{3}{4}$ must be an integer, which it of course isn't. This is a contradiction.
Case 2: n is odd
By definition of odd, there is some integer b where $n = 2b + 1$
Substituting $n = 2b + 1$ into $n^2 - 3 = 4k$, we get $(2b + 1)^2 - 3 = 4b^2 + 4b + 1 - 3 = 4b^2 + 4b - 2 = 4k$.
Dividing both sides by 4 we get $b^2 + b - \frac{1}{2} = k$
Rearranging gives us $b^2 + b - k = \frac{1}{2}$
Since b and k are both integers, $b^2 + b - k$ is an integer. Therefore $\frac{1}{2}$ must be an integer, which it is not. This is a contradiction.

Since these cases are exhaustive and all led to a contradiction, we conclude that original statement is true.

8. More Number Theory Practice

Prove or disprove each of the following claims. Remember, you can disprove a "for all" claim by providing a counter example.

(a) For all $a, b, c \in \mathbb{Z}$, If $a \mid b$ and $c \mid (-a)$, then $(-c) \mid b$.

Solution:

Let a, b, c be arbitrary integers. Suppose $a \mid b$ and $c \mid (-a)$. By definition of divides, $b = ka$ and $-a = cj$ for some integers k, j. Rearranging, we get $a = -cj$. Substituting $a = -cj$ into $b = ka$, we get $b = k(-cj) = (-c)(kj)$. Since k, j are integers, kj is an integer. Then, by definition of divides, $(-c) \mid b$. Since a, b, c were arbitrary integers, the claim holds for all integers a, b, c.

(b) For all $a, b, n, x \in \mathbb{Z}$ with $n > 0$, $a \equiv b \pmod{n}$ implies $x^a \equiv x^b \pmod{n}$.

Solution:

We can disprove this through counterexample. Let $a = 2, b = 5, n = 3, x = 2$.
Since $2 \equiv 5 \pmod{3}$, we have $a \equiv b \pmod{n}$.
We saw in lecture that $a\%n = b\%n$ if and only if $a \equiv b \pmod{n}$.
We have: $2^2 \ \% \ 3 = 4 \ \% \ 3 = 1$ and $2^5 \ \% \ 3 = 32 \ \% \ 3 = 2$.
Since $1 \neq 2$, $2^2 \ \% \ 3 \neq 2^5 \ \% \ 3$, and we therefore know, by our theorem from lecture, that $2^2 \not\equiv 2^5 \pmod{3}$.
This is a counterexample, and the statement is therefore 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 mod and divides, $3 \mid (n-1)$ so $n - 1 = 3k$ for some integer k. Rearranging, we get $n = 3k + 1$. So, $n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. Subtracting 1 from both sides we get, $n^2 - 1 = 3(3k^2 + 2k)$. Since k is an integer, $3k^2 + 2k$ is an integer, so $3 \mid (n^2 - 1)$ by definition of divides. By definition of mod, $n^2 \equiv 1 \pmod{3}$

Case 2: $n \equiv 2 \pmod{3}$
By definition of mod and divides, $3|(n-2)$ so $n - 2 = 3j$ for some integer j. Rearranging, we get $n = 3j + 2$. So, $n^2 = 9j^2 + 12j + 4 = 3(3j^2 + 4j + 1) + 1$. Subtracting 1 from both sides we get, $n^2 - 1 = 3(3j^2 + 4j + 1)$. Since j is an integer, $3j^2 + 4j + 1$ is an integer, so $3 \mid (n^2 - 1)$ by definition of divides. By definition of mod, $n^2 \equiv 1 \pmod{3}$.

These cases are exhaustive, and in all cases, $n^2 \equiv 1 \pmod{3}$. Since n was arbitrary, we have shown that for all integers n, if n is not divisible by 3, then $n^2 \equiv 1 \pmod{3}$.