CSE 390Z: Mathematics for Computation Workshop

Week 4 Workshop Solutions

Conceptual Review

Set Theory

(a) **Definitions**

Set Equality: $A = B := \forall x(x \in A \leftrightarrow x \in B)$
Subset: $A \subseteq B := \forall x(x \in A \rightarrow x \in B)$
Union: $A \cup B := \{x \ : \ x \in A \lor x \in B\}$
Intersection: $A \cap B := \{x \ : \ x \in A \land x \in B\}$
Set Difference: $A \setminus B = A - B := \{x \ : \ x \in A \land x \notin B\}$
Set Complement: $\overline{A} = A^C := \{x \ : \ x \notin A\}$
Powerset: $\mathcal{P}(A) := \{B \ : B \subseteq A\}$
Cartesian Product: $A \times B := \{(a, b) \ : a \in A, \ b \in B\}$

(b) How do we prove that for sets A and B, $A \subseteq B$?

Solution:

Let $x \in A$ be arbitrary... thus $x \in B$. Since x was arbitrary, $A \subseteq B$.

(c) How do we prove that for sets A and B, $A = B$?

Solution:

Use two subset proofs to show that $A \subseteq B$ and $B \subseteq A$.

Number Theory

(d) **Definitions**

a divides b: $a \mid b \quad \leftrightarrow \quad \exists k \in \mathbb{Z}\ (b = ka)$
a is congruent to b modulo m: $a \equiv b \ (\text{mod } m) \quad \leftrightarrow \quad m \mid (a - b)$

(e) What's the Division Theorem?

Solution:

For $a \in \mathbb{Z}$, $d \in \mathbb{Z}$ with $d > 0$, there exist unique integers q, r with $0 \leq r < d$, such that $a = dq + r$.

Set Theory

1. Set Operations

Let $A = \{1, 2, 5, 6, 8\}$ and $B = \{2, 3, 5\}$.

(a) What is the set $A \cap (B \cup \{2, 8\})$?

Solution:

$\{2, 5, 8\}$

(b) What is the set $\{10\} \cup (A \setminus B)$?

Solution:

$\{1, 6, 8, 10\}$

(c) What is the set $\mathcal{P}(B)$?

Solution:

$\{\{2, 3, 5\}, \{2, 3\}, \{2, 5\}, \{3, 5\}, \{2\}, \{3\}, \{5\}, \emptyset\}$

(d) How many elements are in the set $A \times B$? List 3 of the elements.

Solution:

15 elements, for example $(1, 2), (1, 3), (1, 5)$.

2. Standard Set Proofs

(a) Prove that $A \cap B \subseteq A \cup B$ for any sets A, B.

Solution:

Let $x \in A \cap B$ be arbitrary. Then by definition of intersection, $x \in A$ and $x \in B$. So certainly $x \in A$ or $x \in B$ (using the Elim $\wedge$ and Intro $\vee$ rules). Then by definition of union, $x \in A \cup B$. Since x was arbitrary, $A \cap B \subseteq A \cup B$.

(b) Prove that $A \cap (A \cup B) = A$ for any sets A, B.

Solution:

$\Rightarrow$

Let $x \in A \cap (A \cup B)$ be arbitrary. Then by definition of intersection, $x \in A$ and $x \in A \cup B$. So, $x \in A$ must be true (Elim $\wedge$). Since x was arbitrary, $A \cap (A \cup B) \subseteq A$.

$\Leftarrow$

Let $x \in A$ be arbitrary. So certainly $x \in A$ or $x \in B$ (by the Intro $\vee$ rule). Then by definition of union, $x \in A \cup B$. Since $x \in A$ and $x \in A \cup B$, by definition of intersection, $x \in A \cap (A \cup B)$. Since x was arbitrary, $A \subseteq A \cap (A \cup B)$.

Thus we have shown that $A \cap (A \cup B) = A$ through two subset proofs.

(c) Prove that $A \cap (A \cup B) = A \cup (A \cap B)$ for any sets A, B.

Solution:

$\Rightarrow$

Let $x \in A \cap (A \cup B)$ be arbitrary. Then by definition of intersection $x \in A$ and $x \in A \cup B$. Since $x \in A$, then certainly $x \in A$ or $x \in A \cap B$ (Intro $\vee$). Then by definition of union. $x \in A \cup (A \cap B)$. Thus since x was arbitrary, we have shown $A \cap (A \cup B) \subseteq A \cup (A \cap B)$.

$\Leftarrow$

Let $x \in A \cup (A \cap B)$ be arbitrary. Then by definition of union, $x \in A$ or $x \in A \cap B$. Then by definition of intersection, $x \in A$, or $x \in A$ and $x \in B$. Then by distributivity, $x \in A$ or $x \in A$, and $x \in A$ or $x \in B$. Then by idempotency, $x \in A$, and $x \in A$ or $x \in B$. Then by definition of union, $x \in A$, and $x \in A \cup B$. Then by definition of intersection, $x \in A \cap (A \cup B)$. Thus since x was arbitrary, we have shown that $A \cup (A \cap B) \subseteq A \cap (A \cup B)$.

Thus we have shown $A \cap (A \cup B) = A \cup (A \cap B)$ through two subset proofs.

3. Cartesian Product Proof

Write an English proof to show that $A \times C \subseteq (A \cup B) \times (C \cup D)$.

Solution:

Let $x \in A \times C$ be arbitrary. Then x is of the form $x = (y, z)$, where $y \in A$ and $z \in C$. Then certainly $y \in A$ or $y \in B$ (by the Intro $\vee$ rule). Then by definition of union, $y \in (A \cup B)$. Similarly, since $z \in C$, certainly $z \in C$ or $z \in D$. Then by definition, $z \in (C \cup D)$. Since $x = (y, z)$, then $x \in (A \cup B) \times (C \cup D)$. Since x was arbitrary, we have shown $A \times C \subseteq (A \cup B) \times (C \cup D)$.

4. Powerset Proof

Suppose that $A \subseteq B$. Prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Solution:

Let X be an arbitrary set in $\mathcal{P}(A)$. By definition of power set, $X \subseteq A$. We need to show that $X \in \mathcal{P}(B)$, or equivalently, that $X \subseteq B$. Let $x \in X$ be arbitrary. Since $X \subseteq A$, it must be the case that $x \in A$. We were given that $A \subseteq B$. By definition of subset, any element of A is an element of B. So, it must also be the case that $x \in B$. Since x was arbitrary, we know any element of X is an element of B. By definition of subset, $X \subseteq B$. By definition of power set, $X \in \mathcal{P}(B)$. Since X was an arbitrary set, any set in $\mathcal{P}(A)$ is in $\mathcal{P}(B)$, or, by definition of subset, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

5. Set Prove or Disprove

(a) Prove or disprove: For any sets A and B, $A \cup B \subseteq A \cap B$.

Solution:

We wish to disprove this claim via a counterexample. Choose $A = \{1\}$, $B = \varnothing$. Note that $A \cup B = \{1\} \cup \varnothing = \{1\}$ by definition of set union. Note that $A \cap B = \{1\} \cap \varnothing = \varnothing$ by definition of set intersection. $\{1\} \not\subseteq \varnothing$, so the claim does not hold for these sets. Since we found a counterexample to the claim, we have shown that it is not the case that $A \cup B \not\subseteq A \cap B$ for all sets A and B.

(b) Prove or disprove: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Solution:

Let A, B, C be sets, and suppose $A \subseteq B$ and $B \subseteq C$. Let x be an arbitrary element of A. Then, by definition of subset, $x \in B$, and by definition of subset again, $x \in C$. Since x was an arbitrary element of A, we see that all elements of A are in C, so by definition of subset, $A \subseteq C$. So, for any sets A, B, C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Number Theory

6. 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

7. Modular Addition

Let m be a positive integer. Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

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 $(a - b) + (c - d) = mk + mj$. Rearranging, $(a+c)-(b+d) = m(k+j)$. Then by definition of divides, $m \,|(a+c)-(b+d)$. Then by definition of congruence, $a + c \equiv b + d \pmod{m}$.

8. Divisibility Proof

Let the domain of discourse be integers. Consider the following claim:

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

(a) Translate the claim into English.

Solution:

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

(b) Write an English proof 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 $n = dk = 1 \cdot dk$. Note that $-1 \cdot -1 = 1$. Substituting, we see $n = (-1)(-1)dk$. Rearranging, we have $n = (-d)(-1 \cdot k)$. Since k is an integer, $-1 \cdot k$ is an integer because the integers are closed under multiplication. So, by definition of divides, $-d|n$. Since d and n were arbitrary, it follows that for any integers d and n, if $d|n$, then $-d|n$.

9. 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, $ac \equiv bd \pmod{m}$.

10. Another Divisibility Proof

Write an English proof to prove that if k is an odd integer, then $4 \,|\, k^2 - 1$.

Solution:

Let k be an arbitrary odd integer. Then by definition of odd, $k = 2j + 1$ for some integer j. Then $k^2 - 1 = (2j + 1)^2 - 1 = 4j^2 + 4j + 1 - 1 = 4j^2 + 4j = 4(j^2 + j)$. Then by definition of divides, $4 \mid k^2 - 1$.