CSE 311: Foundations of Computing I

Section: Sets and Modular Arithmetic Solutions

How Many Elements?

For each of these, how many elements are in the set? If the set has infinitely many elements, say so.

(a) $A = \{1, 2, 3, 2\}$

Solution: 3

(b) $B = \{\{\}, \{\{\}\}, \{\{\}, \{\}\}, \{\{\}, \{\}, \{\}\}, \ldots\}$

Solution:

$$\begin{aligned} B &= \{\{\}, \{\{\}\}, \{\{\}, \{\}\}, \{\{\}, \{\}, \{\}\}, \ldots\} \\ &= \{\{\}, \{\{\}\}, \{\{\}\}, \{\{\}\}, \ldots\} \\ &= \{\varnothing, \{\varnothing\}\} \end{aligned}$$

So, there are two elements in B.

(c) $C = A \times (B \cup \{7\})$

Solution: $C = \{1, 2, 3\} \times \{\varnothing, \{\varnothing\}, 7\} = \{(a, b) \mid a \in \{1, 2, 3\}, b \in \{\varnothing, \{\varnothing\}, 7\}\}$. It follows that there are $3 \times 3 = 9$ elements in C.

(d) $D = \varnothing$

Solution: 0.

(e) $E = \{\varnothing\}$

Solution: 1.

(f) $F = \mathcal{P}(\{\varnothing\})$

Solution: $2^1 = 2$. The elements are $F = \{\varnothing, \{\varnothing\}\}$.

Set = Set

Prove the following set identities.

(a) Let the universal set be $\mathcal{U}$. Prove $\overline{\overline{X}} = X$ for any set X.

Solution: We want to prove that $S = \overline{\overline{S}}$.

$$\begin{aligned} S &= \{x \ : \ x \in S\} \\ &= \{x \ : \ \neg\neg(x \in S)\} && \text{[Negation]} \\ &= \{x \ : \ \neg(x \notin S)\} && \text{[Definition of } \notin\text{]} \\ &= \{x \ : \ \neg(x \in \overline{S})\} && \text{[Definition of } \overline{S}\text{]} \\ &= \{x \ : \ (x \notin \overline{S})\} && \text{[Definition of } \notin\text{]} \\ &= \{x \ : \ x \in \overline{\overline{S}}\} && \text{[Definition of } \overline{\overline{S}}\text{]} \\ &= \overline{\overline{S}} \end{aligned}$$

It follows that $S = \overline{\overline{S}}$.

(Note that if we did not have a universal set, this whole proof would be garbage.)

(b) Prove $(A \oplus B) \oplus B = A$ for any sets A, B.

Solution:

$$\begin{aligned} (A \oplus B) \oplus B &= \{x \ : \ x \in (A \oplus B) \oplus B\} && \text{[Set Comprehension]} \\ &= \{x \ : \ (x \in A \oplus x \in B) \oplus (x \in B)\} && \text{[Definition of } \oplus\text{]} \\ &= \{x \ : \ x \in A \oplus (x \in B \oplus x \in B)\} && \text{[Associativity of } \oplus\text{]} \\ &= \{x \ : \ x \in A \oplus (\mathsf{F})\} && \text{[Definition of } \oplus\text{]} \\ &= \{x \ : \ x \in A\} && \text{[Definition of } \oplus\text{]} \\ &= A && \text{[Set Comprehension]} \end{aligned}$$

(c) Prove $A \cup B \subseteq A \cup B \cup C$ for any sets A, B, C.

Solution: Let x be arbitrary.

$$\begin{aligned} x \in A \cup B \quad &\rightarrow \quad (x \in A \cup B) \vee (x \in C) \\ &\rightarrow \quad x \in (A \cup B) \cup C && \text{[Definition of } \cup\text{]} \end{aligned}$$

Thus, since $x \in A \cup B \rightarrow x \in (A \cup B) \cup C$, it follows that $A \cup B \subseteq A \cup B \cup C$, by definition of subset.

(d) Let the universal set be $\mathcal{U}$. Prove $A \cap \overline{B} \subseteq A \setminus B$ for any sets A, B.

Solution: Let x be arbitrary.

$$\begin{aligned} x \in A \cap \overline{B} \quad &\rightarrow \quad x \in A \wedge x \in \overline{B} && \text{[Definition of } \cap\text{]} \\ &\rightarrow \quad x \in A \wedge x \notin B && \text{[Definition of } \overline{B}\text{]} \\ &\rightarrow \quad x \in A \setminus B && \text{[Definition of } \setminus\text{]} \end{aligned}$$

Thus, since $x \in A \cap \overline{B} \rightarrow x \in A \setminus B$, it follows that $A \cap \overline{B} \subseteq A \setminus B$, by definition of subset.

Casting Out Nines

Let $n \in \mathbb{N}$. Prove that if $n \equiv 0 \pmod 9$, then the sum of the digits of n is a multiple of 9.

Solution: Suppose $n \equiv 0 \pmod 9$, where $n = (x_m x_{m-1} \cdots x_1 x_0)_{10}$ (This is because we are working with a base-10 number). Then, it follows that $\sum_{i=0}^{m} x_i 10^i \equiv 0 \pmod 9$. Note that $10 \bmod 9 = 1$. So, the previous summation is the same as $\sum_{i=0}^{m} x_i 1^i \equiv 0 \pmod 9$. Simplifying, we see that $\sum_{i=0}^{m} x_i \equiv 0 \pmod 9$, which is what we were trying to prove.

Modular Arithmetic

(a) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Solution: Suppose $a \mid b$ and $b \mid a$, where a, b are integers. By definition of divides, we have $b = ka, a = jb$ for some integers k, j. Combining these equations, we see that $a = j(ka)$. We go by cases on if a is zero or not.

Case 1: $a = 0$. Then, we have $b = k \cdot 0 = 0$. So, $a = b = 0$, and the theorem holds.

Case 2: $a \neq 0$. Then, dividing both sides by a, we get $1 = jk$. So, $\frac{1}{j} = k$. Note that j and k are integers, which is only possible if $j, k \in \{1, -1\}$. It follows that $b = -a$ or $b = a$, as required.

Since the theorem is true in both cases, it is true.

(b) Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod m$, where a and b are integers, then $a \equiv b \pmod n$.

Solution: Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod m$. By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$. By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$. Combining the two equations, we see that $a - b = (knj) = n(kj)$. By definition of congruence, we have $a \equiv b \pmod n$, as required.