CSE 311: Foundations of Computing I

Section : Sets and Modular Arithmetic Solutions

0. 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) $B = \{\{\}, \{\{\}\}, \{\{\}, \{\}\}, \{\{\}, \{\}, \{\}\}, \dots\}$

Solution:

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

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 $F = \{\varnothing, \{\varnothing\}\}$.

1. 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 $S = \overline{\overline{S}}$.

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

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:

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

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

Solution:

Let x be arbitrary.

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

Thus, since $x \in A \cup B \to x \in (A \cup B) \cup C$, 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.

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

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

2. 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.
You may use without proof that $a \equiv b \pmod m \to a^i \equiv b^i \pmod m$.

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 $10 \bmod 9 = 1$. Simplifying, we have:

$$
\begin{aligned}
n \equiv 0 \pmod 9 &\leftrightarrow \sum_{i=0}^{m} x_i 10^i \equiv 0 \pmod 9 && \text{[Definition of } n\text{]} \\
&\leftrightarrow \sum_{i=0}^{m} (x_i 10^i \bmod 9) \equiv 0 \pmod 9 && \text{[Additivity of Congruences]} \\
&\leftrightarrow \sum_{i=0}^{m} (x_i \bmod 9)(10^i \bmod 9) \equiv 0 \pmod 9 && \text{[Multiplicity of Congruences]} \\
&\leftrightarrow \sum_{i=0}^{m} x_i((10 \bmod 9)^i) \equiv 0 \pmod 9 && \text{[***]} \\
&\leftrightarrow \sum_{i=0}^{m} x_i((1 \bmod 9)^i) \equiv 0 \pmod 9 && \text{[Definition of mod]} \\
&\leftrightarrow \sum_{i=0}^{m} (x_i(1)) \bmod 9 \equiv 0 \pmod 9 && \text{[Simplifying]} \\
&\leftrightarrow \sum_{i=0}^{m} x_i \equiv 0 \pmod 9 && \text{[Simplifying]}
\end{aligned}
$$

This is what we were trying to prove.

*****:** This step is justified by the property you were allowed to assume which we haven't proven yet.

3. 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 the definition of divides, we have $a \neq 0$, $b \neq 0$ and $b = ka, a = jb$ for some integers k, j. Combining these equations, we see that $a = j(ka)$.

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 $b = a$.

(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.