CSE 311: Foundations of Computing I

Sets and Modular Arithmetic 4 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 $S = \overline{\overline{S}}$.

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

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.

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 $a \equiv b \pmod m \to a^i \equiv b^i \pmod m$ for $i \in \mathbb{N}$.

Solution:

Let $n \in \mathbb{N}$ be arbitrary where $n \equiv 0 \pmod 9$. Furthermore, consider the base-10 representation of n, where x_i is the ith digit from the right; so, $n = (x_m x_{m-1} \cdots x_1 x_0)_{10} = \sum_{i=0}^{m} x_i 10^i$. Then, note:

$$\begin{aligned}
\sum_{i=0}^{m} x_i &\equiv \sum_{i=0}^{m} x_i 1^i \pmod 9 && \text{[Multiplying by 1]} \\
&\equiv \sum_{i=0}^{m} x_i 10^i \pmod 9 && [10 \equiv 1 \pmod 9 \text{ and Theorem}] \\
&\equiv n \pmod 9 && [\text{Base-10 Definition of } n] \\
&\equiv 0 \pmod 9 && \text{[By assumption]}
\end{aligned}$$

Therefore, by the definition of modular congruence, $9 \mid \sum_{i=0}^{m} x_i - 0$, so $\sum_{i=0}^{m} x_i$ is divisible by 9.

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.

New Definitions

- We say $(\mathcal{M}, \star)$ is a *magma* iff $\forall(x \in \mathcal{M})\forall(y \in \mathcal{M})\ x \star y \in \mathcal{M}$.
- We say "e is a *left-identity*, in a magma $(\mathcal{M}, \star)$, iff $\forall(a \in \mathcal{M})\ e \star a = a$.
- We say "e is a *right-identity*, in a magma $(\mathcal{M}, \star)$, iff $\forall(a \in \mathcal{M})\ a \star e = a$.
- We say "x^{-1} is a *right-inverse of* x, in a magma $(\mathcal{M}, \star)$, iff for all right-identities, e, in $\mathcal{M}$, $x \star x^{-1} = e$.

(a) Let $(\mathcal{Q}, \triangle)$ be a magma. Prove that if a and b are both right-identities and all $m \in \mathcal{Q}$ have right-inverses, then $a = b$.

Solution:

Suppose a and b are both right-identities. Let $c \in \mathcal{Q}$ be arbitrary. Furthermore, note that c has a right-inverse (call it c^{-1}). We now show $a = b$ via a series of equalities:

$$\begin{aligned}
a &= a \triangle a && [a \text{ is a right-identity}] \\
&= (c \triangle c^{-1}) \triangle a && [c \text{ has a right-inverse}] \\
&= b \triangle a && [b \text{ is a right-identity}] \\
&= b && [a \text{ is a right-identity}]
\end{aligned}$$

(b) Let $(\mathcal{R}, \square)$ be an associative magma with a left and right identity $e \in \mathcal{R}$. Prove for all $a \in \mathcal{R}$, if a has a right-inverse a^{-1}, then $(a^{-1})^{-1} = a$.

Solution:

Let $a \in \mathcal{R}$ be arbitrariy. Suppose $a^{-1} \in \mathcal{R}$ is a right-inverse of a. We now show $(a^{-1})^{-1} = a$ via a series of equalities:

$$\begin{aligned}
(a^{-1})^{-1} &= e \square (a^{-1})^{-1} && [e \text{ is a left-identity}] \\
&= (a \square a^{-1}) \square (a^{-1})^{-1} && [a^{-1} \text{ is a right-inverse of } a] \\
&= a \square (a^{-1} \square (a^{-1})^{-1}) && [\text{associtivity}] \\
&= a \square e && [(a^{-1})^{-1} \text{ is a right-inverse of } a^{-1}] \\
&= a && [e \text{ is a right-identity}]
\end{aligned}$$