CSE 311: Foundations of Computing I

Section 4: English Proofs, Sets, and Modular Arithmetic Solutions

1. Primality Checking

When running a brute force check to see whether a number n is prime, you only need to check possible factors up to $\sqrt{n}$. In this problem, you'll prove why that is the case using a proof by contradiction. Prove that if $n = ab$, then either a or b is at most $\sqrt{n}$.
(*Hint:* You want to prove an implication by contradiction; so, start by assuming $n = ab$. Then, continue by writing out the rest of your assumption for the contradiction.)

Solution:

Suppose that $n = ab$. Also suppose for contradiction that both $a > \sqrt{n}$ and $b > \sqrt{n}$. It follows that $ab > \sqrt{n}\sqrt{n} = n$. We clearly can't have both $n = ab$ and $n < ab$; so, this is a contradiction. It follows that a or b is at most $\sqrt{n}$.

2. How Many Elements?

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

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

3. Set = Set

Prove the following set identities.

(a) 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.

(b) Prove that $(A \cap B) \times C \subseteq A \times (C \cup D)$ for any sets A, B, C, D.

Solution:

Let x be an arbitrary element of $(A \cap B) \times C$. Then, by definition of Cartesian product, x must be of the form (y, z) where $y \in A \cap B$ and $z \in C$. Since $y \in A \cap B$ by definition of $\cap$, $y \in A$ and $y \in B$; in particular, all we care about is that $y \in A$. Since $z \in C$, by definition of $\cup$, we also have $z \in C \cup D$. Therefore since $y \in A$ and $z \in C \cup D$, by definition of Cartesian product we have $x = (y, z) \in A \times (C \cup D)$.

Since x was an arbitrary element of $(A \cap B) \times C$ we have proved that $(A \cap B) \times C \subseteq A \times (C \cup D)$ as required.

4. 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 that $a \mid b$ 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.