CSE 311: Foundations of Computing I

Section 4: English Proofs, Sets, and Modular Arithmetic

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.)

2. How Many Elements?

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

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

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

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

(d) $D = \varnothing$

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

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

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.

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

4. Modular Arithmetic

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

(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 $a \equiv b \pmod{n}$.