Section 04: Propositions and Proofs

1. Formal Spoofs

For each of the following proofs, determine why the proof is incorrect. Then, consider whether the conclusion of the proof is true or not. If it is true, state how the proof could be fixed. If it is false, give a counterexample.

(a) Show that $\exists z \, \forall x \, P(x, z)$ follows from $\forall x \, \exists y \, P(x, y)$.

1.	$\forall x \, \exists y \, P(x, y)$	[Given]
2.	$\forall x \, P(x, c)$	[$\exists$ Elim: 1, c special]
3.	$\exists z \, \forall x P(x, z)$	[$\exists$ Intro: 2]

(b) Show that $\exists z \, (P(z) \wedge Q(z))$ follows from $\forall x \, P(x)$ and $\exists y \, Q(y)$.

1.	$\forall x \, P(x)$	[Given]
2.	$\exists y \, Q(y)$	[Given]
3.	Let z be arbitrary	
4.	$P(z)$	[$\forall$ Elim: 1]
5.	$Q(z)$	[$\exists$ Elim: 2, let z be the object that satisfies $Q(z)$]
6.	$P(z) \wedge Q(z)$	[$\wedge$ Intro: 4, 5]
7.	$\exists z \, P(z) \wedge Q(z)$	[$\exists$ Intro: 6]

2. Prime Checking

You wrote the following code, `isPrime(int n)` which you are confident returns `true` if and only if n is prime (we assume its input is always positive).

```
public boolean isPrime(int n) {
    int potentialDiv = 2;
    while (potentialDiv < n) {
        if (n % potenttialDiv == 0)
            return false;
        potentialDiv++;
    }
    return true;
}
```

Your friend suggests replacing `potentialDiv < n` with `potentialDiv <= Math.sqrt(n)`. In this problem, you'll argue the change is ok. That is, your method still produces the correct result if n is a positive integer.

(a) Call a positive integer k a "nontrivial divisor" of n if $k \mid n$, $k \neq 1$, and $k \neq n$. Argue that if n has a nontrivial divisor, then it has a nontrivial divsior at most $\sqrt{n}$. Hint: you may want to divide into cases at the end!

(b) Informally explain why this fact about integers lets you change the code safely.

3. 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) $F = \mathcal{P}(\{\varnothing\})$

4. Set = Set

Prove the following set identities.

(a) Let the universal set be $\mathcal{U}$. Prove $A \cap \overline{B} \subseteq A \backslash B$ 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.

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

6. Trickier Set Theory

Note, this problem requires a little more thinking. The solution will cover both the answer as well as the intuition used to arrive at it.

Show that for any set X and any set A such that $A \in \mathcal{P}(X)$, there exists a set $B \in \mathcal{P}(X)$ such that $A \cap B = \emptyset$ and $A \cup B = X$.