Section 04: Number Theory and Sets

1. It's Prime Time

Prove for all prime numbers $p > 2$, either $p \equiv 3 \pmod 4$ or $p \equiv 1 \pmod 4$.

2. A Visit to Primes Square

Prove that for all positive integers a and b which have $\gcd(a, b) = 1$, that $\gcd(a, b^2) = 1$.

3. How many?

In each problem, count the number of elements in each set. If the set has infinitely many elements, say so.

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

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

(c) $C = \emptyset$

(d) $D = \{\emptyset\}$

(e) $E = \mathcal{P}(\{\emptyset\})$

4. Set Equality

Let $\mathcal{U}$ be the universal set. Prove that $A \cap (A \cup B) = A$ for all sets A and B.

5. Tricky Set Equality

This problem should only be covered in section if there is extra time. Prove that for any set X and set $A \in \mathcal{P}(X)$, there exists a set B such that the following conditions are both true:

- $A \cap B = \emptyset$
- $A \cup B = X$

6. No number is...

Note: only parts (a) and (b) are necessary, c-e are bonus material although they are good practice. In this problem we will walk through how to prove the following claim about numbers: No integer n which satisfies $n \equiv 3 \pmod 4$ is the sum of two squares. That is to say, there do not exist integers a, b such that $n = a^2 + b^2$.

(a) Translate the claim into logic, using quantifiers as necessary. You may assume the domain of discourse is positive integers. Then, using DeMorgan's law for quantifiers, remove any $\neg\exists$ so that all quantifiers are $\forall$.

(b) Prove the following (slightly) easier claim: Every integer c has either $c^2 \equiv 0 \pmod 4$ or $c^2 \equiv 1 \pmod 4$. *Hint: Prove it for two cases, one when c is odd and one when c is even.*

(c) Let S be the set of values which $(a^2 + b^2) \,\%\, 4$ may take on for integers a, b. Write a definition for S in set builder notation.

(d) Using what you proved in part(b), prove that $S = \{0, 1, 2\}$.

(e) Prove the claim from the beginning of the problem. This should be very short since you can cite what you have proved in any above part.