Section 04: Solutions

1. It's Prime Time

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

Solution:

Let p be an arbitrary prime greater than two, and suppose for the sake of contradiction that it does not satisfy either $p \equiv 3 \pmod 4$ or $p \equiv 1 \pmod 4$. We proceed by case analysis on the remaining values of $p \pmod 4$:

(a) **Case** $p \equiv 0 \pmod 4$. Then by definition of modular equivalence, $4|p$ and so p cannot be prime which is a contradiction.

(b) **Case** $p \equiv 2 \pmod 4$. Then by definition of modular equivalence, $4|p-2$, and by definition of divides, there exists an integer k so that $p - 2 = 4k$. But then rearranging we see,

$$p = 4k + 2 = 2(2k + 1).$$

Since $2k+1$ is an integer, we have $2|p$, and since $p > 2$, this means p cannot be prime which is a contradiction.

Since these cases were exhaustive and in both cases we found a contradiction, it must be that the contradiction assumption is false and so the original claim must hold.

2. A Visit to Primes Square

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

Solution:

Let $g = \gcd(a, b^2)$. We want to show $g = 1$. By Bezout's theorem, there must exist integers s, t such that

$$1 = \gcd(a, b) = sa + tb.$$

Multiplying both sides by b, we get that

$$b = sba + tb^2.$$

By definition of gcd, $g|a$ and $g|b^2$, so there exist integers k, j such that

$$a = gk \quad \text{and} \quad b^2 = gj.$$

Then we can combine these facts to get,

$$b = sb(gk) + tgj = g(sbk + tj).$$

This shows that $g|b$, since $sbk + tj$ is an integer. Then since $g|b$ and $g|a$, by definition of $\gcd(a, b)$, $g \leq \gcd(a, b)$. But since its given that $\gcd(a, b) = 1$, and $\gcd(\cdot, \cdot) \geq 1$, it must be that $g = 1$, which completes the proof.

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

Solution:

(a) 3

(b) 2 It may seem at first like there are ∞, but the third elements onwards are all just $\{\emptyset\}$, so they are not distinct elements.

(c) 0

(d) 1

(e) 2

4. Set Equality

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

We need to prove two directions. First we prove $A \cap (A \cup B) \subseteq A$.

Proof. Let $x \in A \cap (A \cup B)$ be arbitrary. We want to show $x \in A$. By definition of $\cap$, $x \in A \wedge x \in (A \cup B)$, so $x \in A$ and we are done. Since x was arbitrary, this shows $A \cap (A \cup B) \subseteq A$. $\square$

Now we prove the other direction.

Proof. Let $x \in A$ be arbitrary. We want to show $x \in A \cap (A \cup B)$. By definition of $\cup$, $x \in A \cup B$, since clearly $x \in A \vee x \in B$. Then since we know $x \in A$ and $x \in A \cup B$, by definition of $\cap$, we conclude $x \in A \cap (A \cup B)$, so we are done. Since x was arbitrary, this shows $A \subseteq A \cup B$. $\square$

Since we proved both $A \cap (A \cup B) \subseteq A$ and $A \subseteq A \cap (A \cup B)$, we have shown $A = A \cap (A \cup B)$.

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:

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

Solution:

Proof. To show such a B exists, we explicitly construct it: define $B \in \mathcal{P}(B)$ as the set

$$B := X \setminus A.$$

$B \in \mathcal{P}(B)$ since clearly $X \setminus A \subseteq X$ (can you prove why?). Now it remains to show that this choice of B satisfies both conditions. We prove the first condition:

Proof. Suppose for contradiction that $A \cap B$ is non-empty. Then there exists some $x \in A \cap B$. By choice of B, $x \in A \cap (X \setminus A)$, and by definition of $\cap$, then $x \in A$ and $x \in (X \setminus A)$. But $x \in (X \setminus A)$ means that $x \in X$ and $x \notin A$, but we already showed $x \in A$ which is a contradiction. Thus $A \cap B = \emptyset$. $\square$

And the second:

Proof. Since $A, B \in \mathcal{P}(X)$, it is sufficient to prove that $A \cup B \supseteq X$ (can you prove the other direction?). Let $x \in X$ be arbitrary. There are two cases:

Case 1. If $x \in A$ then we are already done, since by definition of $\cup$, $x \in A \cup B$.

Case 2. If $x \notin A$, then by definition of $\setminus$, since also $x \in X$, $x \in X \setminus A$. But this means $x \in B$ and so $x \in A \cup B$.

Thus we have shown $x \in A \cup B$ in all cases. Since x was arbitrary this shows $X \subseteq A \cup B$. □

Then we have shown that this choice of B satisfies all the required conditions. □

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 $\forall$.

Solution:

$$\neg\exists n(n \equiv 3 \pmod 4) \land \exists a \exists b(n = a^2 + b^2).$$
$$\forall n((n \equiv 3 \pmod 4) \to \forall a \forall b(n \neq a^2 + b^2)).$$

(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.*

Solution:

Proof. There are two cases: either c is odd or c is even.

Case 1. If c is odd then $c = 2k + 1$ for some integer k. Then,

$$c^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1.$$

Which means $c^2 - 1 = 4(k^2 + k)$. Since $k^2 + k$ is an integer, $4|c^2 - 1$ and by the definition of modular equivalence, we have $c^2 \equiv 1 \pmod 4$. Thus the claim holds for this case.

Case 2. If c is even then $c = 2k$ for some integer k. Then,

$$c^2 = (2k)^2 = 4k^2.$$

Which means $c^2 - 0 = 4(k^2)$. Since k^2 is an integer, $4|c^2$ and by the definition of modular equivalence, we have $c^2 \equiv 0 \pmod 4$. Thus the claim holds for this case.

Since the claim holds in both cases and the cases are exhaustive the proof is complete. □

(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.

Solution:

$$S := \{(a^2 + b^2) \,\%\, 4 : a, b \in \mathbb{Z}\}.$$

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

Solution:

We need to prove two things. First we prove $S \subseteq \{0, 1, 2\}$:

Proof. Let $s \in S$ be arbitrary. Then $s = (a^2 + b^2) \,\%\, 4$ for some integers a, b. We want to show that $s \in \{0, 1, 2\}$.

From part (b) we proved that $a^2 \equiv 0 \pmod 4$ or $a^2 \equiv 1 \pmod 4$, and the same for b^2. Then using the equivalence of mod % proved in class, we know $a^2 \,\%\, 4 \leq 1$ and $b^2 \,\%\, 4 \leq 1$ and so $(a^2 \,\%\, 4) + (b^2 \,\%\, 4) \leq 2$. Then Using the properties of %, this means $s = (a^2 + b^2) \,\%\, 4 \leq 2$, but by definition of %, s is a non-negative integer so $0 \leq s \leq 2$ and we have $s \in \{0, 1, 2\}$. Since s was arbitrary, this shows $S \subseteq \{0, 1, 2\}$. $\square$

Now we prove the other direction, $S \supseteq \{0, 1, 2\}$:

Proof. Let $s \in \{0, 1, 2\}$ be arbitrary. There are three cases.

Case 0. If $s = 0$, then observe that by choosing $a = 2$ and $b = 4$, we have $(a^2 + b^2) \,\%\, 4 = (4 + 16) \,\%\, 4 = 20 \,\%\, 4 = 0$, so there exist $a, b \in \mathbb{Z}$ such that $0 = s = a^2 + b^2 \,\%\, 4$, showing $s \in S$.

Case 1. If $s = 1$, then choose $a = 1$ and $b = 2$, we have $(a^2 + b^2) \,\%\, 4 = (1 + 4) \,\%\, 4 = 5 \,\%\, 4 = 1$, so there exist $a, b \in \mathbb{Z}$ such that $1 = s = a^2 + b^2 \,\%\, 4$, showing $s \in S$.

Case 2. If $s = 2$, then choose $a = 1$ and $b = 3$, we have $(a^2 + b^2) \,\%\, 4 = (1 + 9) \,\%\, 4 = 10 \,\%\, 4 = 2$, so there exist $a, b \in \mathbb{Z}$ such that $2 = s = a^2 + b^2 \,\%\, 4$, showing $s \in S$.

Since $s \in S$ in all three cases and the cases were exhaustive, we conclude $S \supseteq \{0, 1, 2\}$. $\square$

Since we have proved both directions, we conclude $S = \{0, 1, 2\}$.

(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.

Solution:

Let n be an arbitrary integer which satisfies $n \equiv 3 \pmod 4$ and let a, b be arbitrary integers. By part (d), and the equivalence of % and mod, $a^2 + b^2 \,\%\, 4 \in \{0, 1, 2\}$, but this means $a^2 + b^2 \,\%\, 4 \neq 3$ and so by equivalence of mod and %, $a^2 + b^2 \not\equiv 3 \pmod 4$, but this means that $n \neq a^2 + b^2$. Thus we have proved the second expression in part (a), which is equivalent to the desired claim.

Note: There are lots of ways to do this, it may make sense to show how to make this proof by contradiction using the non-DeMorgan's law'd expression in (a).