Math 239 Problem Set 7 Solution

Problem 1. Prove that for all integers a, b, and d with $d \neq 0$, if d divides a or d divides b then d divides ab.

Proof. The proof is in two cases, d divides a and d divides b.

For the first case, we assume that d divides a and show that d divides ab. Since d divides a, $a = kd$ for some integer k. Thus $ab = kdb = kbd$, which proves, since kb is an integer, that d divides ab.

For the second case, we assume that d divides b and show that d divides ab. Since d divides b, $b = kd$ for some integer k. Thus $ab = akd$. Since ak is an integer, this proves that d divides ab.

(The two cases here are essentially identical, and "real world" proofs would probably just say something such as "for the second case we assume d divides b and proceed similarly to case 1" rather than repeat the same logic a second time.) $\square$

Problem 2. Determine whether the following proposition is true or false, and prove it if true.

Proposition 1. For all integers m and n, 4 divides $m^2 - n^2$ if and only if m and n are both even or m and n are both odd.

Proof. We prove each direction separately.

For the first part of the proof, we show that if m and n are both even or m and n are both odd, then 4 divides $m^2 - n^2$. The proof has in two cases, m and n are both odd, and m and n are both even.

In the first case, we assume that m and n are both odd and show that 4 divides $m^2 - n^2$. Since m and n are both odd, there exist integers a and b such that $m = 2a + 1$ and $n = 2b + 1$. Thus

$$\begin{aligned} m^2 - n^2 &= (2a+1)^2 - (2b+1)^2 \\ &= 4a^2 + 4a + 1 - 4b^2 - 4b - 1 \\ &= 4(a^2 + a - b^2 - b) \end{aligned}$$

Since $a^2 + a - b^2 - b$ is an integer, this shows that 4 divides $m^2 - n^2$.

For the second case, we assume that m and n are both even and show that 4 divides $m^2 - n^2$. Since m and n are both even, there exist integers a and b

such that $m = 2a$ and $n = 2b$. Thus

$$\begin{aligned} m^2 - n^2 &= (2a)^2 - (2b)^2 \\ &= 4a^2 - 4b^2 \\ &= 4(a^2 - b^2) \end{aligned}$$

Since $a^2 - b^2$ is an integer, this shows that 4 divides $m^2 - n^2$.

We have now completed the proof for the first direction, namely if m and n are both even or m and n are both odd, then 4 divides $m^2 - n^2$.

For the second part of the proof, we assume that 4 divides $m^2 - n^2$ and show that either m and n are both even or m and n are both odd. We prove the contrapositive, i.e., that if one of m or n is even and the other odd, then 4 does not divide $m^2 - n^2$. Once again the proof has two cases, first that m is odd and n even, and second that m is even and n odd.

In the first case (m is odd and n even), there exist integers a and b such that $m = 2a + 1$ and $n = 2b$. Thus

$$\begin{aligned} m^2 - n^2 &= (2a+1)^2 - (2b)^2 \\ &= 4a^2 + 4a + 1 - 4b^2 \\ &= 4(a^2 + a - b^2) + 1 \end{aligned}$$

Since $a^2 + a - b^2$ is an integer, 4 cannot divide $4(a^2 + a - b^2) + 1$, and so we have shown that if m is odd and n even, then 4 does not divide $m^2 - n^2$.

For the second case (m is even and n odd), there exist integers a and b such that $m = 2a$ and $n = 2b + 1$. Thus

$$\begin{aligned} m^2 - n^2 &= (2a)^2 - (2b+1)^2 \\ &= 4a^2 - 4b^2 - 4b - 1 \\ &= 4(a^2 - b^2 - b) - 1 \end{aligned}$$

Since $a^2 - b^2 - b$ is an integer, 4 cannot divide $4(a^2 - b^2 - b) - 1$, and we have shown that if m is even and n odd, then 4 does not divide $m^2 - n^2$.

These two cases show that if one of m or n is even and the other odd, then 4 does not divide $m^2 - n^2$, and thus its contrapositive, if 4 divides $m^2 - n^2$ then either m and n are both even or m and n are both odd.

We have now established both directions of the biconditional, and so we have proven that for all integers m and n, 4 divides $m^2 - n^2$ if and only if m and n are both even or m and n are both odd. □

Problem 3. Prove that for all real numbers x and y, $|xy| = |x||y|$.

Proof. The proof is in four cases, namely $x < 0$ and $y < 0$, $x < 0$ and $y \geq 0$, $x \geq 0$ and $y < 0$, and $x \geq 0$ and $y \geq 0$.

In the first case $x < 0$ and $y < 0$, so $xy > 0$. This in turn means $|xy| = xy = (-x)(-y) = |x||y|$.

In the second case $x < 0$ and $y \geq 0$, so $xy \leq 0$, which in turn means $|xy| = -(xy) = (-x)y = |x||y|$.

In the third case $x \geq 0$ and $y < 0$, so $xy \leq 0$, which in turn means $|xy| = -(xy) = x \times (-y) = |x||y|$.

In the fourth case $x \geq 0$ and $y \geq 0$, so $xy \geq 0$ and thus $|xy| = xy = |x||y|$.

We have now shown that in all possible cases $|xy| = |x||y|$, proving that for all real numbers x and y, $|xy| = |x||y|$. □

Problem 4. Prove that if a is an integer and $a \equiv 0 \pmod 5$ then $a^2 \equiv 0 \pmod 5$. Then prove that 5,344,580,232,468,953,153 is not a perfect square.

Proposition 2. If a is an integer and $a \equiv 0 \pmod 5$ then $a^2 \equiv 0 \pmod 5$.

Proof. We assume that $a \equiv 0 \pmod 5$. Then by Part 3 of Sundstrom's Theorem 3.28, $a^2 \equiv 0^2 \pmod 5$. Since $0^2 = 0$, this proves that if a is an integer and $a \equiv 0 \pmod 5$ then $a^2 \equiv 0 \pmod 5$. □

Proposition 3. The number 5,344,580,232,468,953,153 is not a perfect square.

Proof. Notice that $5,344,580,232,468,953,153 \equiv 3 \pmod 5$. The proof then proceeds by contradiction. Assume that 5,344,580,232,468,953,153 is a perfect square. Then there exists an integer a such that $a^2 = 5,344,580,232,468,953,153$. We now consider two cases, namely a is congruent to $0 \pmod 5$ and a is not congruent to $0 \pmod 5$.

In the first case, $a \equiv 0 \pmod 5$, we know from Proposition 2 that $a^2 \equiv 0 \pmod 5$, but we have already determined that $5,344,580,232,468,953,153 \equiv 3 \pmod 5$.

In the second case, a is not congruent to $0 \pmod 5$, Sundstrom's Proposition 3.33 tells us that $a^2 \equiv 1 \pmod 5$ or $a^2 \equiv 4 \pmod 5$, but we have already determined that $5,344,580,232,468,953,153 \equiv 3 \pmod 5$.

Thus, in both possible cases the assumption that 5,344,580,232,468,953,153 is a perfect square leads to a contradiction. We have therefore proven that 5,344,580,232,468,953,153 is not a perfect square. □