Week 10

Juan Patricio Carrizales Torres
Section 1: Proof involving divisibility of integers

September 26, 2021

Definition Let $a, b \in \mathbb{Z}$. We say that a **divides** b if there is some integer c such that $b = ca$. We express this as $a \mid b$. Also, if $a \mid b$, we say that a is **divisor** of b and that b is a **multiple** of a.
Note that if $b \neq 0$ and $a = 0$, then $a \mid b$ would lead to a contradiction, namely, $b = 0 \cdot c = 0$ for all integers c.

Problem 1. Let a and b be integers, where $a \neq 0$. Prove that if $a \mid b$, then $a^2 \mid b^2$.

Proof. Assume that $a \mid b$. Then $b = ax$ for some $x \in \mathbb{Z}$. Therefore,

$$b^2 = (ax)^2 = a^2x^2$$

Since x^2 is an integer, it follows that $a^2 \mid b^2$. □

Problem 2. Let $a, b \in \mathbb{Z}$, where $a \neq 0$ and $b \neq 0$. Prove that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.

Proof. Assume $a \mid b$ and $b \mid a$. Then $b = ca$ and $a = xb$ for some $x, c \in \mathbb{Z}$. Thus,

$$a = x(ca) = a(xc)$$

Therefore, $xc = 1$ and so $x = c = \pm 1$. Thus, $a = \pm b$. □

Problem 3. Let $m \in \mathbb{Z}$.

(a) Give a direct proof of the following: If $3 \mid m$, then $3 \mid m^2$.

Proof. Assume $3 \mid m$. Then $m = 3c$ for some $c \in \mathbb{Z}$. Therefore,

$$m^2 = 3^2c^2 = 3(3c^2)$$

Because $3c^2$ is an integer, $3 \mid m^2$. □

(b) State the contrapositive of the implication in (a)

Solution b. Let $m \in \mathbb{Z}$. If $3 \nmid m^2$, then $3 \nmid m$

(c) Give a direct proof of the following: If $3 \nmid m$, then $3 \nmid m^2$.

Solution c. Assume $3 \nmid m$. Then either $m = 3q + 1$ or $m = 3q + 2$ for some $q \in \mathbb{Z}$. We consider these two cases.
Case 1. $m = 3q + 1$ for some integer q. Then

$$m^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$$

Since $3q^2 + 2q \in \mathbb{Z}$, $3 \nmid m^2$.
Case 2. $m = 3q + 2$ for some integer q. Then

$$m^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$$

Because $3q^2 + 4q + 1 \in \mathbb{Z}$, $3 \nmid m^2$.

(d) State the contrapositive of the implication in (c).

Solution d. Let $m \in \mathbb{Z}$. If $3 \mid m^2$, then $3 \mid m$.

(e) State the conjunction of the implications in (a) and (c) using "if and only if."

Solution e. Let $m \in \mathbb{Z}$. $3 \mid m$ if and only if $3 \mid m^2$.

Problem 4. Let $x, y \in \mathbb{Z}$. Prove that if $3 \nmid x$ and $3 \nmid y$, then $3 \mid (x^2 - y^2)$.

Proof. Assume $3 \nmid x$ and $3 \nmid y$. Then, by Result 6, $x^2 - 1 = 3q$ and $y^2 - 1 = 3c$ for some $q, c \in \mathbb{Z}$. Then,

$$\begin{aligned} x^2 &= 3q + 1 \\ y^2 &= 3c + 1 \\ x^2 - y^2 &= 3q + 1 - 3c - 1 = 3(q - c) \end{aligned}$$

Since $q - c \in \mathbb{Z}$, $3 \mid (x^2 - y^2)$. □

Problem 5. Let $a, b, c \in \mathbb{Z}$, where $a \neq 0$. Prove that if $a \nmid bc$, then $a \nmid b$ and $a \nmid c$.

Proof. Assume $a \mid b$ or $a \mid c$. Without loss of generality, let $a \mid b$ and so $b = ax$ for some $x \in \mathbb{Z}$. Therefore, $bc = (ax)c = a(xc)$. Since $xc \in \mathbb{Z}$, $a \mid bc$. □

Problem 6. Let $a \in \mathbb{Z}$. Prove that if $3 \mid 2a$, then $3 \mid a$.

Proof. Assume $3 \nmid a$. Then, either $a = 3q + 1$ or $a = 3q + 2$ for some $q \in \mathbb{Z}$. We consider these two cases.
Case 1. Let $a = 3q + 1$ for some $q \in \mathbb{Z}$. Then, $2(3q + 1) = 6q + 2 = 3(2q) + 2$. Because $2q$ is an integer, $3 \nmid 2a$.
Case 2. Let $a = 3q + 2$ for some $q \in \mathbb{Z}$. Then, $2(3q + 2) = 6q + 3 + 1 = 3(2q + 1) + 1$. Because $2q + 1 \in \mathbb{Z}$, $3 \nmid 2a$. □

Problem 7. Let $n \in \mathbb{Z}$. Prove that $3 \mid (2n^2 + 1)$ if and only if $3 \nmid n$.

Proof. Let $3 \mid n$. Then $n = 3q$ for some $q \in \mathbb{Z}$.Therefore,

$$2(3q)^2 + 1 = 18q^2 + 1 = 3(6q^2) + 1$$

Because $6q^2 \in \mathbb{Z}$, $3 \nmid (2n^2 + 1)$.

For the converse, assume $3 \nmid n$. Then, either $n = 3c + 1$ or $n = 3c + 2$ for some integer c. We consider these two cases.
Case 1. $n = 3c + 1$. So,

$$2(3c + 1)^2 + 1 = 2(9c^2 + 6c + 1) + 1 = 18c^2 + 12c + 3 = 3(6c^2 + 4c + 1)$$

Since $6c^2 + 4c + 1$ is an integer, $3 \mid (2n^2 + 1)$.
Case 1. $n = 3c + 2$. So,

$$2(3c + 2)^2 + 1 = 2(9c^2 + 12c + 4) + 1 = 18c^2 + 24c + 9 = 3(6c^2 + 8c + 3)$$

Because $6c^2 + 8c + 3 \in \mathbb{Z}$, $3 \mid (2n^2 + 1)$. □

Problem 9. (a) Let $x \in \mathbb{Z}$. Prove that if $2 \mid (x^2 - 5)$, then $4 \mid (x^2 - 5)$.

Solution a. Assume $2 \mid (x^2 - 5)$. Then $x^2 - 5 = 2c$, where $c \in \mathbb{Z}$, and so $x^2 = 2c + 5 = 2c + 4 + 1 = 2(c + 2) + 1$. Since $c + 2 \in \mathbb{Z}$, x^2 is odd and by Theorem 3.12 x is odd. Therefore, $x = 2y + 1$ for some $y \in \mathbb{Z}$. Then

$$x^2 - 5 = (2y + 1)^2 - 5 = 4y^2 + 4y + 1 - 5 = 4y^2 + 4y - 4 = 4(y^2 + y - 1)$$

Since $y^2 + y - 1$ is an integer, $4 \mid (x^2 - 5)$.

(b) Give an example of an integer x such that $2 \mid (x^2 - 5)$ but $8 \nmid (x^2 - 5)$.

Solution b. One such example is $x = 5$.

Problem 10. Let $n \in \mathbb{Z}$. Prove that $2 \mid (n^4 - 3)$ if and only if $4 \mid (n^2 + 3)$.

Proof. Assume $2 \mid (n^4 - 3)$. Then $n^4 - 3 = 2c$, where $c \in \mathbb{Z}$. The integer $n^4 = 2c + 3 = 2(c + 1) + 1$ is odd since $c + 1 \in \mathbb{Z}$. By Theorem 3.12, n^2 is odd and so n is odd. Therefore, $n = 2m + 1$ for some integer m. Then,

$$n^2 + 3 = (2m + 1)^2 + 3 = 4m^2 + 4m + 4 = 4(m^2 + m + 1)$$

Because $m^2 + m + 1 \in \mathbb{Z}$, $4 \mid (n^2 + 3)$.
For the converse, let $2 \nmid (n^4 - 3)$. Then $n^4 - 3 = 2c + 1$ for some integer c and so $n^4 = 2c + 4 = 2(c + 2)$. Since $c + 2 \in \mathbb{Z}$, n^4 is an even integer. By Theorem 3.12, n^2 is even and so n is even. Then, $n = 2k$ for some integer k. Therefore,

$$n^2 + 3 = 4k^2 + 3$$

Since $k^2 \in \mathbb{Z}$, it follows that $4 \nmid (n^2 + 3)$. □

Problem 13. Prove that if $a, b, c \in \mathbb{Z}$ and $a^2 + b^2 = c^2$, then $3 \mid ab$.

Proof. Assume $3 \nmid ab$. By Result 5, $3 \nmid a$ and $3 \nmid b$. Then □