Week 11

Juan Patricio Carrizales Torres

Section 2: Proofs involving congruence of integers

September 29, 2021

For integers $a, b, n \in \mathbb{Z}$, where $n \geq 2$, we say that a **is congruent to** b **modulo of** n ($a \equiv b(\text{mod } n)$) if and only if $n \mid (a-b)$. In other words, a and b must have the same remainder when divided by n.

Let $n \in \mathbb{Z}$ such that $n \geq 2$. For all integers a, there is exactly one $b \in \{0, 1, 2, \ldots, n-1\}$ for which the following holds

$$a \equiv b(\text{mod } n)$$

This means that a can have only one of $b \in \{0, 1, 2, \ldots, n-1\}$ as a remainder when divided by n.

Interesting results of congruence of integers

Result 9 Let a, b, k and n be integers where $n \geq 2$. If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{n}$

Result 10 Let $a, b, c, d, n \in \mathbb{Z}$ where $n \geq 2$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

Result 11 Let $a, b, c, d, n \in \mathbb{Z}$ where $n \geq 2$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

EXERCISES

Problem 14. Let $a, b, n \in \mathbb{Z}$, where $n \geq 2$. Prove that if $a \equiv b(\text{mod } n)$, then $a^2 \equiv b^2(\text{mod } n)$.

Proof. Assume $a \equiv b(\text{mod } n)$. Then, $n \mid (a-b)$. Hence, $a - b = nx$ for some $x \in \mathbb{Z}$. Note that

$$a^2 - b^2 = (a-b)(a+b) = n(x(a+b))$$

Since $x(a+b) \in \mathbb{Z}$, $n \mid (a^2 - b^2)$ and so $a^2 \equiv b^2(\text{mod } n)$. $\square$

Problem 15. Let $a, b, c, n \in \mathbb{Z}$, where $n \geq 2$. Prove that if $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $b \equiv c \pmod{n}$.

Proof. Assume $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$. Then $n \mid (a-b)$ and $n \mid (a-c)$. Therefore, $a - b = xn$ and $a - c = yn$, where $x, y \in \mathbb{Z}$, and so $a = xn + b$. Therefore,

$$\begin{aligned}(xn + b) - c &= yn \\ b - c &= yn - xn = n(y - x)\end{aligned}$$

Since $y - x \in \mathbb{Z}$, $n \mid (b - c)$ and so $b \equiv c \pmod{n}$

(Since $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, both a and b have the same residue when divided by n.) □

Problem 16. Let $a, b \in \mathbb{Z}$. Prove that if $a^2 + 2b^2 \equiv 0 \pmod{3}$, then either both a and b are congruent to 0 module of 3 or neither is congruent to 0 module of 3.

Proof. Assume that exactly one of a and b is congruent to 0 module of 3. We consider two cases.
Case 1. $a \equiv 0 \pmod{3}$ and $b \not\equiv 0 \pmod{3}$. By Result 4.6, $a^2 \equiv 0 \pmod{3}$ and $b^2 \equiv 1 \pmod{3}$. Then, $2b^2 \equiv 2 \pmod{3}$. Thus, $a^2 + 2b^2 \equiv 2 \pmod{3}$ and so $a^2 + 2b^2 \not\equiv 0 \pmod{3}$.

Case 2. $b \equiv 0 \pmod{3}$ and $a \not\equiv 0 \pmod{3}$. By Result 4.6, $a^2 \equiv 1 \pmod{3}$ and $b^2 \equiv 0 \pmod{3}$. Then, $2b^2 \equiv 0 \pmod{3}$. Thus, $a^2 + 2b^2 \equiv 1 \pmod{3}$ and so $a^2 + 2b^2 \not\equiv 0 \pmod{3}$. □

Problem 17. (a) Prove that if a is an integer such that $a \equiv 1 \pmod{5}$, then $a^2 \equiv 1 \pmod{5}$.

Solution a. Assume $a \equiv 1 \pmod{5}$. Then $5 \mid (a - 1)$ and so $a - 1 = 5x$ for some $x \in \mathbb{Z}$. Note that

$$\begin{aligned}(a - 1)(a + 1) &= 5x(a + 1) \\ a^2 - 1 &= 5(x(a + 1))\end{aligned}$$

Because $(x(a + 1)) \in \mathbb{Z}$, $5 \mid (a^2 - 1)$ and so $a^2 \equiv 1 \pmod{5}$.

Problem 18. Let $m, n \in \mathbb{N}$ such that $m \geq 2$ and $m \mid n$. Prove tha if a and b are integers such that $a \equiv b \pmod{n}$, then $a \equiv b \pmod{m}$.

Proof. Let $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$. Then, $n \mid (a-b)$. Therefore, $a-b = nk$ for some $k \in \mathbb{Z}$. Note that $m \mid n$ and so $n = mx$, where $x \in \mathbb{Z}$. Therefore, $a - b = (mx)k = m(xk)$. Since $xk \in \mathbb{Z}$, $m \mid (a - b)$ and so $a \equiv b \pmod{m}$. □

Problem 19. Let $a, b \in \mathbb{Z}$. Show that if $a \equiv 5 \pmod{6}$ and $b \equiv 3 \pmod{4}$, then $4a + 6b \equiv 6 \pmod{8}$.

Proof. Assume $a \equiv 5 \pmod{6}$ and $b \equiv 3 \pmod{4}$. Then $6 \mid (a-5)$ and $4 \mid (b-3)$. Therefore, $a-5 = 6x$ and $b-3 = 4y$ for some integers x and y. So $a = 6x+5$ and $b = 4y+3$. Therefore,

$$4(6x + 5) + 6(4y + 3) = 24x + 20 + 24y + 18 = 24x + 24y + 38 = 8(3x + 3y + 4) + 6$$

Thus, $(4a + 6b) - 6 = 8(3x + 3y + 4)$. Since $3x + 3y + 4 \in \mathbb{Z}$, $8 \mid ((4a + 6b) - 6)$ and so $4a + 6b \equiv 6 \pmod{8}$. □

Problem 20. Result 12 states: Let $n \in \mathbb{Z}$. If $n^2 \not\equiv n \pmod 3$, then $n \not\equiv 0 \pmod 3$ and $n \not\equiv 1 \pmod 3$. State and prove the converse of this result.

Let $n \in \mathbb{Z}$. If $n \not\equiv 0 \pmod 3$ and $n \not\equiv 1 \pmod 3$, then $n^2 \not\equiv n \pmod 3$.

Proof. Assume $n \not\equiv 0 \pmod 3$ and $n \not\equiv 1 \pmod 3$. Then $n \equiv 2 \pmod 3$ and so $3 \mid (n-2)$. Therefore $n - 2 = 3x$ for some $x \in \mathbb{Z}$ and so $n = 3x + 2$. Note that

$$n^2 - n = (3x+2)^2 - 3x - 2 = 9x^2 + 12x + 4 - 3x - 2 = 9x^2 + 9x + 2 = 3(3x^2 + 3x) + 2$$

Since $3x^2 + 3x \in \mathbb{Z}$, $3 \nmid (n^2 - 2)$ and so $n^2 \not\equiv n \pmod 3$. □

(b) State the conjunction of Result 12 and its converse using "if and only if".

Solution b. Let $n \in \mathbb{Z}$. Then $n^2 \not\equiv n \pmod 3$ if and only if $n \not\equiv 0 \pmod 3$ and $n \not\equiv 1 \pmod 3$.

Problem 21. Let $a \in \mathbb{Z}$. Prove that $a^3 \equiv a \pmod 3$.

Proof. Assume $a \in \mathbb{Z}$. Then either $a = 3q$, $a = 3q + 1$ or $a = 3q + 2$ for some $q \in \mathbb{Z}$. We consider these 3 cases.
Case 1. $a = 3q$, where $q \in \mathbb{Z}$. Note that

$$a^3 - a = (3q)^3 - 3q = 27q^3 - 3q = 3(9q^3 - q)$$

Since $9q^3 - q \in \mathbb{Z}$, $3 \mid (a^3 - a)$ and so $a^3 \equiv a \pmod 3$.
Case 2. $a = 3q + 1$, where $q \in \mathbb{Z}$. Note that

$$a^3 - a = (3q+1)^3 - 3q - 1 = 27q^3 + 27q^2 + 9q + 1 - 3q - 1 = 3(9q^3 + 9q^2 + 2q)$$

Since $9q^3 + 9q^2 + 2q \in \mathbb{Z}$, $3 \mid (a^3 - a)$ and so $a^3 \equiv a \pmod 3$.
Case 3. $a = 3q + 2$, where $q \in \mathbb{Z}$. Note that

$$a^3 - a = (3q+2)^3 - 3q - 2 = 27q^3 + 54q^2 + 36q + 8 - 3q - 2 = 3(9q^3 + 18q^2 + 11q + 2)$$

Since $9q^3 + 18q^2 + 11q + 2 \in \mathbb{Z}$, $3 \mid (a^3 - a)$ and so $a^3 \equiv a \pmod 3$.

□

Problem 24. Let x and y be even integers. Prove that $x^2 \equiv y^2 \pmod{16}$ if and only if either (1) $x \equiv 0 \pmod 4$ and $y \equiv 0 \pmod 4$ or (2) $x \equiv 2 \pmod 4$ and $y \equiv 2 \pmod 4$.

Proof. Let x and y be even integers. Then, each of x and y is either congruent to 0 or 2 modulo of 4. First, we assume that either (1) $x \equiv 0 \pmod 4$ and $y \equiv 0 \pmod 4$ or (2) $x \equiv 2 \pmod 4$ and $y \equiv 2 \pmod 4$. We consider the following two cases.
Case 1. $x \equiv 0 \pmod 4$ and $y \equiv 0 \pmod 4$. Then, $4 \mid x$ and $4 \mid y$, and so $x = 4n$ and $y = 4m$ for some $n, m \in \mathbb{Z}$. Note that,

$$x^2 - y^2 = (x+y)(x-y) = (4n+4m)(4n-4m) = 4(n+m)4(n-m) = 16((n+m)(n-m))$$

Since $(n+m)(n-m) \in \mathbb{Z}$, $16 \mid (x^2 - y^2)$ and so $x^2 \equiv y^2 \pmod{16}$.
Case 2. $x \equiv 2 \pmod 4$ and $y \equiv 2 \pmod 4$. Then, $4 \mid (x-2)$ and $4 \mid (y-2)$, and so $x - 2 = 4n$ and $y - 2 = 4m$ for some $n, m \in \mathbb{Z}$. Therefore, $x = 4n+2$ and $y = 4m+2$. Note that,

$$\begin{aligned} x^2 - y^2 &= (x+y)(x-y) = (4n+2+4m+2)(4n+2-4m-2) = (4n+4m+4)(4n-4m) \\ &= 4(n+m+1)4(n-m) = 16(n+m+1)(n-m) \end{aligned}$$

Since $(n+m+1)(n-m) \in \mathbb{Z}$, $16 \mid (x^2 - y^2)$ and so $x^2 \equiv y^2 \pmod{16}$.

For the converse, let x and y be even integers such that exactly one of them is congruent to 0 modulo of 4 and the other is congruent to 2 modulo of 4. Without loss of generality, assume $x \equiv 2 \pmod 4$ and $y \equiv 0 \pmod 4$. Then, $4 \mid (x-2)$ and $4 \mid y$, and so $x = 4n+2$ and $y = 4m$ for some $n, m \in \mathbb{Z}$. Note that,

$$x^2 - y^2 = (4n+2)^2 - (4m)^2 = 16n^2 + 16n + 4 - 16m^2 = 16(n^2 + n - m^2) + 4$$

Since $n^2 + n - m^2 \in \mathbb{Z}$, $16 \nmid (x^2 - y^2)$ and so $x^2 \not\equiv y^2 \pmod{16}$. $\square$