Section 8.5: Congruence Modulo n

Juan Patricio Carrizales Torres

May 30, 2022

This chapter discusses the previously seen topic of **Congruence Modulo n**, but now with the lens of **Equivalence relations**. Basically, the author proved that every relation on $\mathbb{Z}$ defined by the congruence modulo of some $n \geq 2$ is an equivalence relation with n equivalence classes. This follows from the **Division Algorithm**, namely in the case for $n \geq 2$, any integer m can be expressed uniquely as $m = kn + r$, where $k \in \mathbb{Z}$ and $0 \leq r < n$.

Another interesting idea is the logical equivalence between coditions that define equivalence relations. For example, let R_1 and R_2 be relations on some nonempty set defined by $a \ R_1 \ b$ if $P(a, b)$ and $a \ R_2 \ b$ if $Q(a, b)$. The fact that $P(a, b) \iff Q(a, b)$ for some other condition $Q(n)$, implies that $R_1 = R_2$. Hence, one can show that two relations have the same distinct equivalence classes by just showing that there is a biconditional relation between the conditions that define them.

Problem 47. The relation R on $\mathbb{Z}$ defined by $a \ R \ b$ if $a^2 \equiv b^2 \pmod{4}$ is known to be an equivalence relation. Determine the distinct equivalence classes.

Solution 47. Let's first consider $[0]$. We know that

$$
\begin{aligned}
[0] &= (x \in \mathbb{Z} : x \ R \ 0) \\
&= \left(x \in \mathbb{Z} : x^2 = 4k, \ k \in \mathbb{Z}\right) \\
&= \left(x \in \mathbb{Z} : 4 \mid x^2\right) = \left(x \in \mathbb{Z} : 2 \mid x^2\right) \\
&= (x \in \mathbb{Z} : 2 \mid x).
\end{aligned}
$$

Hence, $[0]$ is the set of all even integers. Now we are left with the odd ones, so let's check what are the elements of $[1]$. We know that

$$
\begin{aligned}
[1] &= (x \in \mathbb{Z} : x \ R \ 1) \\
&= \left(x \in \mathbb{Z} : 4 \mid (x^2 - 1)\right)
\end{aligned}
$$

We know that x^2 is either even or odd. If it is even, then $x^2 - 1$ is odd (sum of an even and odd integer) which contradicts the assumption that it is a multiple of 4. Hence, we may

assume that x^2 is odd. Recall that x^2 is odd if and only if x is odd and so $x = 2k + 1$ for some $k \in \mathbb{Z}$. Hence,

$$x^2 - 1 = (2k + 1)^2 - 1$$
$$= 4k^2 + 4k + 1 - 1 = 4(k^2 + k).$$

Since $k^2 + k$ is an integer, it follows that $4 \mid (x^2 - 1)$. Hence, x being odd is a necessary and sufficient condition for $4 \mid (x^2 - 1)$ to be true, and so $[1]$ is the set of odd integers.

Problem 48. The relation R defined on $\mathbb{Z}$ by $x \, R \, y$ if $x^3 \equiv y^3 \pmod{4}$ is known to be an equivalence relation . Determine the distinct equivalence classes.

Solution 48. Let's first consider the equivalence class $[0]$. Then

$$[0] = \{x \in \mathbb{Z} : x \, R \, 0\}$$
$$= \{x \in \mathbb{Z} : 4 \mid x^3\}.$$

Consider some $x \in [0]$. We know that either x is odd or even. If it is odd, then x^3 is odd which contradicts our assumption that $4 \mid x^3$. Hence, $x = 2k$ for some $k \in \mathbb{Z}$ and so $x^3 = 8k^3 = 4\,(2k^3)$. Since $2k^3 \in \mathbb{Z}$, it follows that x being even is a necessary and sufficient condition for $4 \mid x^3$ to be true. Thus, $[0]$ is the set of even integers.

Now, we are left with the odd integers. Consider the equivalence class $[1]$. Then

$$[1] = \{x \in \mathbb{Z} : x \, R \, 1\}$$
$$= \left\{x \in \mathbb{Z} : 4 \mid (x^3 - 1)\right\}.$$

Let $x \in [1]$. Then x must be odd because $[0]$ contains all even integers. Thus, $x = 2k + 1$ for some $k \in \mathbb{Z}$ and so $x^3 = 8k^3 + 6k + 12k^2 + 1$. Then, $x^3 - 1 = 8k^3 + 6k + 12k^2$. Note that $4 \mid (3(2k))$ if and only if $2 \mid k$. Hence, $4 \mid (x^3 - 1)$ if and only if $x = 2k + 1$ for some even integer k.

Now, we are left with the set of odd integers $2k + 1$ where k is an odd integer. Consider the equivalence class $[3]$. Then,

$$[3] = \{x \in \mathbb{Z} : x \, R \, 3\}$$
$$= \left\{x \in \mathbb{Z} : 4 \mid (x^3 - 27)\right\}.$$

Let $x \in [3]$. Then $x = 2k + 1$ for some odd integer $k = 2b + 1$, where $b \in \mathbb{Z}$. Thus, $x^3 - 27 = (8k^3 + 12k^2 + 6k + 1) - 27 = 8k^3 + 12k^2 + 12b - 20 = 4(2k^3 + 3k^2 + 3b - 5)$. Because $2k^3 + 3k^2 + 3b - 5$ is an integer, it follows that $4 \mid (x^3 - 27)$ if and only if $x = 2k + 1$, where k is an odd integer. Therefore, the distinct equivalence classes are as follows:

$$[0] = \{x \in \mathbb{Z} : x \text{ is even}\}$$
$$[1] = \{x \in \mathbb{Z} : x = 2k + 1, \text{ where } k \text{ is even}\}$$
$$[3] = \{x \in \mathbb{Z} : x = 2k + 1, \text{ where } k \text{ is odd}\}.$$

Problem 49. A relation R is defined on $\mathbb{Z}$ by $a \mathrel{R} b$ if $5a \equiv 2b \pmod 3$. Prove that R is an equivalence relation. Determine the distinct equivalence classes.

Solution 49. We first show that R is an equivalence relation.

Proof. We first show that R is reflexive. Consider some integer x. Then, $5x - 2x = 3x$. Hence, $5x \equiv 2x \pmod 3$. Consider some integers x, y such that $5x \equiv 2y \pmod 3$. Then, $5x - 2y = 3k$ for some integer k. Note that

$$5y - 2x = (3k - 5x + 7y) + (3k + 2y - 7x)$$
$$= 6k - 12x + 9y = 3(2k - 4x + 3y).$$

Since $2k - 4x + 3y \in \mathbb{Z}$, it follows that $5y \equiv 2x \pmod 3$ and so R is symmetric. Now, consider some integers x, y, z such that $5x \equiv 2y \pmod 3$ and $5y \equiv 2z \pmod 3$, namely, $x \mathrel{R} y$ and $y \mathrel{R} z$. Then $5x - 2y = 3a$ and $5y - 2z = 3b$ for some integers a, b. Note that

$$5x - 2z = (5x - 2y) + (5y - 2z) - 3y$$
$$= 3a + 3b - 3y = 3(a + b - y).$$

Because $a + b - y$ is an integer, it follows that $5x \equiv 2z \pmod 3$ ($x \mathrel{R} z$) and so R is transitive. $\qquad\square$

Now, all we have left to do is determine the equivalence classes. We initially consider $[0]$. Then

$$[0] = \{x \in \mathbb{Z} : 3 \mid 5x\}$$
$$= \{x \in \mathbb{Z} : 3 \mid x\}$$

since 5 is prime. Now, we are left with the set of every integer x such that either $x \equiv 1 \pmod 3$ or $x \equiv 2 \pmod 3$. Thus, let's check $[1]$. Then

$$[1] = \{x \in \mathbb{Z} : 3 \mid (5x - 2)\}.$$

Consider some $x \in [1]$. If $x \equiv 2 \pmod 3$, then $x = 3a + 2$, where $a \in \mathbb{Z}$, and so $5(3a+2) - 2 = 15a + 8 = 15k + 6 + 2$ which contradicts our assumption that $3 \mid (5x - 2)$. Hence, $x \equiv 1 \pmod 3$ and so $x = 3b + 1$ for some integer b. Therefore, $5(3b + 1) - 2 = 15a + 3 = 3(5a + 1)$ which implies that $3 \mid (5x - 2)$. Thus, $x \equiv 1 \pmod 3$ is a necessary and sufficient condition for $3 \mid (5x - 2)$ to be true and so

$$[1] = \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\}.$$

Since we are left with the set of every integer x such that $x \equiv 2 \pmod 3$, it follows that it makes sense to consider $[2]$. We know that

$$[2] = \{x \in \mathbb{Z} : 3 \mid (5x - 4)\}.$$

Note that $x \in [2]$ implies that $x \equiv 2 \pmod 3$ due to the partition nature of equivalence classes. If $x \equiv 2 \pmod 3$, then $x = 3k + 2$ for some $k \in \mathbb{Z}$ and so $5x - 4 = 5(3k + 2) - 4 = 15k + 10 - 4 = 15k + 6$, which implies that $3 \mid (5x - 4)$ and $x \in [2]$. Hence,

$$[2] = \{x \in \mathbb{Z} : x \equiv 2 \pmod 3\}.$$

Therefore, the equivalence classes are as follows:

$$[0] = \{x \in \mathbb{Z} : x \equiv 0 \pmod 3\}$$
$$[1] = \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\}$$
$$[2] = \{x \in \mathbb{Z} : x \equiv 2 \pmod 3\}.$$