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

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

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

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

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,

$$\begin{aligned} x^2 - 1 &= (2k+1)^2 - 1 \\ &= 4k^2 + 4k + 1 - 1 = 4(k^2 + k). \end{aligned}$$

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

$$\begin{aligned} [0] &= \{x \in \mathbb{Z} : x\ R\ 0\} \\ &= \{x \in \mathbb{Z} : 4 \mid x^3\}. \end{aligned}$$

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

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

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,

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

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:

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