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:

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

Problem 49. A relation R is defined on $\mathbb{Z}$ by $a\ R\ b$ 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

$$\begin{aligned} 5y - 2x &= (3k - 5x + 7y) + (3k + 2y - 7x) \\ &= 6k - 12x + 9y = 3(2k - 4x + 3y). \end{aligned}$$

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, $x\ R\ y$ and $y\ R\ z$. Then $5x - 2y = 3a$ and $5y - 2z = 3b$ for some integers a, b. Note that

$$\begin{aligned} 5x - 2z &= (5x - 2y) + (5y - 2z) - 3y \\ &= 3a + 3b - 3y = 3(a + b - y). \end{aligned}$$

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

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

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

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:

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv 0 \pmod 3\} \\
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\} \\
[2] &= \{x \in \mathbb{Z} : x \equiv 2 \pmod 3\}\,.
\end{aligned}$$

Problem 52. Let R be the relation defined on $\mathbb{Z}$ by $a\ R\ b$ if $a^2 \equiv b^2 \pmod 5$. Prove that R is an equivalence relation and determine the distinct equivalence classes.

Solution 52. We prove that R is an equivalence relation.

Proof. Consider some integer x. Then $x^2 - x^2 = 0$ and so $x^2 \equiv x^2 \pmod 5$. Thus, R is reflexive. Now, consider some integers x, y such that $x^2 \equiv y^2 \pmod 5$. Then, $x^2 - y^2 = 5k$ for some integer k. Note that

$$\begin{aligned}
y^2 - x^2 &= -(x^2 - y^2) \\
&= -5k = 5(-k).
\end{aligned}$$

Hence, $y^2 \equiv x^2 \pmod 5$ and so R is symmetric. Let x, y, z be integers such that $x^2 \equiv y^2 \pmod 5$ and $y^2 \equiv z^2 \pmod 5$, namely, $x\ R\ y$ and $y\ R\ z$. Then, $x^2 - y^2 = 5a$ and $y^2 - z^2 = 5b$ for integers a, b. Note that

$$\begin{aligned}
(x^2 - y^2) + (y^2 - z^2) &= x^2 - y^2 \\
&= 5(a + b).
\end{aligned}$$

Thus, $x^2 \equiv z^2 \pmod 5$ and so R is transitive. $\square$

Once we know that R is an equivalence relations, let's determine its equivalence classes. Let's check $[0]$. Then

$$\begin{aligned}
[0] &= \left\{x \in \mathbb{Z} : 5 \mid x^2\right\} \\
&= \{x \in \mathbb{Z} : 5 \mid x\}
\end{aligned}$$

since 5 is a prime numbers. We are left with the set of integers not multiples of 5, for instance, 1. Then,

$$\begin{aligned}
[1] &= \left\{x \in \mathbb{Z} : 5 \mid (x^2 - 1)\right\} \\
&= \{x \in \mathbb{Z} : 5 \mid (x - 1)(x + 1)\} \\
&= \{x \in \mathbb{Z} : 5 \mid (x - 1) \text{ or } 5 \mid (x + 1)\} \quad = \{x \in \mathbb{Z} : x = 5a + 1 \text{ or } x = 5b + 4,\ a, b \in \mathbb{Z}\}
\end{aligned}$$

since 5 is a prime number. Therefore, we are left with the set of all integers such that $x^2 \equiv 2 \pmod 5$ and $x^2 \equiv 3 \pmod 5$. Hence, consider $[2]$. Then,

$$\begin{aligned}
[2] &= \left\{x \in \mathbb{Z} : 5 \mid (x^2 - 4)\right\} \\
&= \{x \in \mathbb{Z} : 5 \mid (x + 2)(x - 2)\} \\
&= \{x \in \mathbb{Z} : 5 \mid (x + 2) \text{ or } 5 \mid (x - 2)\} \quad = \{x \in \mathbb{Z} : x = 5a + 3 \text{ or } x = 5b + 2,\ a, b \in \mathbb{Z}\}\,.
\end{aligned}$$

Hence, the distinct equivalence classes are as follows:

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv \pmod 5\} \\
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \pmod 5 \text{ or } x \equiv 4 \pmod 5\} \\
[2] &= \{x \in \mathbb{Z} : x \equiv 2 \pmod 5 \text{ or } x \equiv 3 \pmod 5\}
\end{aligned}$$

The argument of this proof suggests an interesting conjecture. Let n be a prime number. Then the distinct equivalence classes of R defined on $\mathbb{Z}$ by $a\ R\ b$ if $a^2 \equiv b^2 \pmod n$ are $[0] = \{x \in \mathbb{Z} : x \equiv \pmod n\}$ and $[k] = \{x \in \mathbb{Z} : x \equiv k \pmod n \text{ or } x \equiv (n-k) \pmod n\}$. It's like taking the edges, namely

$$\underbrace{x \equiv \pmod n}_{[0]}\ \underbrace{x \equiv 1 \pmod n}_{[1]}\ \underbrace{x \equiv 2 \pmod n}_{[2]} \ldots \underbrace{x \equiv (n-1) \pmod n}_{[2]}\ \underbrace{x \equiv n \pmod n}_{[1]}.$$

Problem 53. For an integer $n \geq 2$, the relation R defined on $\mathbb{Z}$ by $a\ R\ b$ if $a \equiv b \pmod n$ is an equivalence relation. Equivalently, $a\ R\ b$ if $a - b = kn$ for some integer k. Define a relation R on the set $\mathbb{R}$ by $a\ R\ b$ if $a - b = k\pi$ for some $k \in \mathbb{Z}$. Is this relation R on $\mathbb{R}$ an equivalence relation? If not, explain why. If yes, prove this and determine $[0], [\pi]$ and $[\sqrt{2}]$.

Solution 53. Yes, it is. In fact, for any real number r, any relation R on the set $\mathbb{R}$ defined by $a\ R\ b$ if $a - b = kr$ for some $k \in \mathbb{Z}$ is an equivalence relation.

Proof. Let $r \in \mathbb{R}$. Consider some real number x. Then, $x - x = 0 = 0r$ and so R is reflexive. Consider some real numbers x, y such that $x - y = kr$ for some $k \in \mathbb{Z}$. Note that $y - x = -(x-y) = -kr = r(-k)$¡++¿ and so R is symmetric. Lastly, consider some real numbers x, y, z such that $x - y = ar$ and $y - z = br$ for some $a, b \in \mathbb{Z}$. Note that $(x-y) + (y-z) = x - z = r(a+b)$. Since $a + b \in \mathbb{Z}$, it follows that R is transitive. □

Then, let's determine the asked equivalence classes. First, consider $[0]$. Then,

$$[0] = \{x \in \mathbb{R} : x = \pi k,\ k \in \mathbb{Z}\}.$$

Since $\pi = \pi \cdot 1$, it follows that $[\pi] = [0]$. Note that they only contain irrational numbers, being 0 and exception. Now, consider $[\sqrt{2}]$. Then,

$$\begin{aligned}
[\sqrt{2}] &= \left\{x \in \mathbb{R} : x - \sqrt{2} = \pi k,\ k \in \mathbb{Z}\right\} \\
&= \left\{x \in \mathbb{R} : x = \pi k + \sqrt{2},\ k \in \mathbb{Z}\right\}.
\end{aligned}$$

Note that both πk and $\sqrt{2}$ are irrational. Thus, $\pi k + \sqrt{2}$ is irrational and so $[\sqrt{2}]$ only contains irrational numbers.