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

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

Note that $x^2 - 1 = (x - 1)(x + 1)$ is an even integer. Thus, it is a necessary and sufficient condition that either $2 \mid (x-1)$ or $2 \mid (x+1)$. Therefore, $x = 2a+1$ or $x = 2b-1 = 2(b-1)+1$ for $a, b \in \mathbb{Z}$, and so $[1]$ is the set of odd integers.