Relations

Modular Congruence

$$a \equiv b \pmod n \iff n \mid (a - b)$$

The difference between a and b is divisible by n, there exists some integer k such that:

$$a - b = kn$$

Alternate Definition

$$a \equiv b \pmod n$$

Interpreted as: a and b , both leave the **same remainder** when divided by n, that is:

$$a \pmod n = b \pmod n$$

To find the Datum(tag)

$$a \pmod n$$

That is :

$$a \pmod n = r$$

Which gives the **least non-negative** value in this class.

Introduction

First, we begin with a set S. We propose a relation $\sim$ on S (on **itself**), for example

$$a \equiv r \pmod 4 \iff a - r \in 4\mathbf{Z}$$

We then **prove** that this is a *equivalent* relation, it must be :

- **Reflexive** : $(a, a) \in S$ for all $a \in S$
- **Symetric** : if $(a, b) \in S$, then $(b, a) \in S$
- **Transitive** : if (a, b),$(b, c) \in S$, then $(a, c) \in S$

That confirms that $\sim$ is an *equivalent relation.* For this example to analyze the structure of each element with :

$$a \pmod 4$$

This value (the **datum**, or **tag**) tells us which other elements

$$a$$

is related to, and is used to **label** the equivalence class:

$$[a] = \{x \in S \mid x \equiv a \pmod 4\}$$

We then group all such related elements into **equivalence classes**. Finally, the set of all these *disjoint classes* forms a *partition* $\mathcal{P}_\sim$ of S, which creates a set of the *datum.*

$$\mathcal{P}_\sim = \{[a] \mid a \in S\}$$

The 'union' $\bigcup \mathcal{P}_\sim$ takes the elements to which the partition points and 'union' them obtaining S

$$\bigcup \mathcal{P}_| = \bigcup_{a \in S} [a] = S$$

Summary: One starts with a *set.* Give the set structure by means of a *relation.* A *datum* (tag) is computed in some fashion based on the relation and stablish which element relates to which so an *equivalent class* is created. Group all datum (tags) in a set called *partition.* If one 'union' the elements that the partition is pointing then the original element is obtained.