北京景山学校
jiguanglaoshi@gmail.com
http://beijingshanmaths.org

CONGRUENCES in $\mathbb{Z}$

Definition and operations in $\mathbb{Z}/n\mathbb{Z}$

I- Definition of CONGRUENCE in $\mathbb{Z}$:

If a and b are Integers, and n is a Natural number : $\forall(a;b)\in\mathbb{Z}\times\mathbb{Z},\quad \forall n\in\mathbb{N},$

$$\text{"}a \text{ is congruent to } b \text{ modulo } n\text{"} \Leftrightarrow a\equiv b\ [n] \quad \Leftrightarrow \quad a-b=k.n$$

1. **Properties of Congruence :**

   i. $a\equiv b\ [n] \Leftrightarrow$ *a and b have the* **same Rest** *in the Euclidian division by n*

   ii. $\left\{\begin{array}{c} a\equiv b \quad [n] \\ a'\equiv b'\ [n]\end{array}\right\} \Rightarrow \left\{\begin{array}{c} a+a'\equiv b+b' \quad [n] \\ a.a'\equiv b.b'\ [n]\end{array}\right\}$

   iii. $\forall p\in\mathbb{N},\quad a\equiv b\quad [n]\ \Rightarrow a^p\equiv b^p\quad [n]$

" Congruence ***is a relationship*** **compatible** ***with Addition and Multiplication"***

2. **Equivalence relationship :** $\forall(a;b)\in\mathbb{Z}\times\mathbb{Z},\quad \forall n\in\mathbb{N},$

   i. Reflexivity : $a\equiv a\ [n]$

   ii. Symetry : $b\equiv a\ [n]\ \Leftrightarrow a\equiv b\ [n]$

   iii. Transitivity : $\left\{\begin{array}{c} a\equiv b \quad [n] \\ b\equiv c \quad [n]\end{array}\right\} \Rightarrow a\equiv c \quad [n]$

3. **Classes of Congruence** :

   Let $a\in[0, 1, 2, \ldots(n-1)]$, then the set $\{x\in\mathbb{Z},\ \ x\equiv a\ \ [n]\}$ is noted $\dot{a}$

   and is called the **CLASS** of ***a*** **Modulo** ***n***.

   • Any integer *x* belongs to one of the *n* classes modulo *n*.

   • *The set of all classes modulo n is noted* $\mathbb{Z}/n\mathbb{Z}$

   <u>Example</u> : $\mathbb{Z}/6\mathbb{Z}=\{\dot{0}\,;\dot{1}\,;\dot{2}\,;\dot{3}\,,\dot{4}\,;\dot{5}\}$ with $\dot{2}=\{x\in\mathbb{Z},\ \ x=2+k.6\}$

   $\dot{2}=\{2\ ;8\ ;14\ ;20\ ;\ldots;-4\ ;-10\ ;-16\ ;\ldots\}$

   Hence we can say that $\dot{2}\oplus\dot{4}=\dot{0}$ and $\dot{3}\otimes\dot{4}=\dot{0}$