Recall <u>Definition 2.3</u>: <u>the residue class of a modulo n</u> is $[a]_n = a + n\mathbb{Z} = \{a, a \pm n, a \pm 2n, \dots\} \subseteq \mathbb{Z}$

Note: $a \equiv b \mod n \iff [a]_n = [b]_n \iff n \mid (a-b)$

Example: $19 \equiv 14 \equiv 9 \equiv 4 \equiv -1 \mod 5$

so $[19]_5 = \dots = [4]_5 = [-1]_5 = \{\dots, -1, 4, 9, 14, 19, \dots\} = 4 + 5\mathbb{Z} \subseteq \mathbb{Z}$

Note: Since $[a]_n = [b]_n$ where $0 \leq r \leq n$ the remainder after division by n, any residue class mod n coincides with exactly one of the following:

$[0]_n, [1]_n, \dots, [n-1]_n \quad ([0]_n = [n]_n)$

(just n distinct residue classes!)

<u>Definition 2.4</u>: The <u>ring of integers modulo n</u> is $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$ (finite set of n elements)

together with addition and multiplication defined as

$[a]_n + [b]_n = [a+b]_n$ and $[a]_n \times [b]_n = [ab]_n$.

Note: To find $[a]_n + [b]_n$, we find $a+b$, take its remainder r, then $[a]_n + [b]_n = [a+b]_n = [r]_n$.

the same for $[a]_n \times [b]_n = \dots$

Example: $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$;

$[1]_5 + [2]_5 = [1+2]_5 = [3]_5$

$[3]_5 + [4]_5 = [3+4]_5 = [7]_5 = [2]_5$

$[4]_5 \times [4]_5 = [4 \times 4]_5 = [16]_5 = [1]_5$

Remark: To simplify notation, we will write $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ (i.e. write a instead of $[a]_n$)

with addition and multiplication mod n, e.g. in $\mathbb{Z}_5$:

$2+3=0$ (as $2+3 \equiv 0 \mod 5$ so $[2+3]_5 = [0]_5$)

$2 \times 3 = 1$ (as $2 \times 3 = 6 \equiv 1 \mod 5$)

Thus, $a+b=c$ in $\mathbb{Z}_n$ means $a+b \equiv c \mod n$ or equiv.

$[a]_n + [b]_n = [c]_n$

Example 2.6: $n=2$. Then $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$ (or simply $\mathbb{Z}_2 = \{0,1\}$)

Here $[0]_2 = 0 + 2\mathbb{Z} = \{\text{all even integers}\}$

$[1]_2 = 1 + 2\mathbb{Z} = \{\text{all odd integers}\}$;

$0+0=0$, $0+1=1$, $1+0=1$, $1+1=0$, so

+	0	1
0	0	1
1	1	0 ← 1+1

×	0	1
0	0	0
1	0	1

Cayley Tables

Example: $n=4$. $\mathbb{Z}_4 = \{0,1,2,3\}$

Caley Table for $\times$ in $\mathbb{Z}_4$:

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2 ← $2\cdot 3$ mod 4
3	0	3	2	1 ← $3\cdot 3$ mod 4

Definition 2.8: $a \in \mathbb{Z}_n$ is invertible if $\exists\, b \in \mathbb{Z}_n$ s.t. $ab = 1$ ($[a]_n \cdot [b]_n = [1]_n$). In that case b is is the inverse of a, written as $b = a^{-1}$.

Remark 2.9: (1) $1 \in \mathbb{Z}_n$ is invertible as $1 \cdot 1 = 1$

(2) we can find invertible elements by looking for 1 in the Cayley table, e.g. for $\mathbb{Z}_4$,

$1^{-1} = 1$, $3^{-1} = 3$

Lemma 2.13: Let $a, b, c \in \mathbb{Z}_n$. Suppose a is invertible. Then the equation $ax + b = c$ has a unique solution in $\mathbb{Z}_n$.

Proof: $ax + b = c \Rightarrow ax = c - b \Rightarrow a^{-1}(ax) = a^{-1}(c-b)$

$\Rightarrow x = a^{-1}(c-b)$ a unique solution.

(equivalent $[a]_n [x]_n + [b]_n = [c]_n$

Example 2.14: $3x + 2 = 1$ in $\mathbb{Z}_5$; $x = ?$ Note $3^{-1} = 2$ as $3 \times 2 = 1$ mod 5)

so $3x + 2 = 1 \Rightarrow 3x = 1 - 2 = -1 = 4 \Rightarrow x = 3^{-1} \times 4 = 2 \times 4 = 8 = 3$ mod 5.

thus $x = 3$