$m \in \mathbb{N}$

$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$

Other Authors write $[0], [1], \ldots$ or $[0]_m, [1]_m, \ldots$ which is a cumberson notation.

example

In $\mathbb{Z}_{25}$, $7 \times 4 = 3$.

In $\mathbb{Z}_{26}$, $7 \times 4 = 2$.

Make sure the context is clear that you're working in $\mathbb{Z}_{25}$ not $\mathbb{Z}_{26}$.

example multiplication table for $\mathbb{Z}_5 = \{0,1,2,3,4\}$

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

← entry for row i and column k equals $i \times k$

$0 \times a = 0 = a \times 0$

$1 \times a = a = 1 \times a$

$a \times b = b \times a$

$a + b = b + a$

Solving equations in $\mathbb{Z}_m$?

linear equation in $\mathbb{Z}_m$

$ax + b = 0$ where $a, b \in \mathbb{Z}_m$ (*)

Are there any values for $x \in \mathbb{Z}_m$ making this equation true?

examples

① $x + b = 0$ $(a = 1)$

$x = -b = m - b$

Conclude: This equation can always be solved.

$\mathbb{Z}_5 = \{0,1,2,3,4\}$

In $\mathbb{Z}_5$, $-3 = 2 \Rightarrow$ solution of $x+3=0$ is $x=2$.

② $ax - 1 = 0$ $(b = -1)$

$ax = 1$ ← doesn't always have a solution

It does have a solution when a has a multiplicative inverse in $\mathbb{Z}_m$.

③ In $\mathbb{Z}_5$, the equation $2x + b = 0$ can always be solved.

Reason $3(2x+b) = 3 \cdot 2x + 3b = x + 3b$

So $x + 3b = 3(2x+b) = 3(0) = 0$

$\Rightarrow x = -3b = 2b$

④ In $\mathbb{Z}_6$, the equation $2x + b = 0$ can be written as $b = -2x$

x	$-2x$
0	0
1	$-2 = 4$
2	$-4 = 2$
3	$-6 = 0$
4	$-8 = 4$
5	$-10 = 2$

← So this shows that $2x + b = 0$ only has a solution in $\mathbb{Z}_6$ if $b = 0, 2$ or 4.

For example, $2x + 3 = 0$ has no solution.