Chapter 2 part 4

Solving the equation $[a] \odot x = [1]$ in $\mathbb{Z}_n$

The set-up: $n > 0$ is a fixed integer

$a \in \mathbb{Z}$ - an integer, 1 - number One.

To solve this equation is to find $x \in \mathbb{Z}_n$ such that $[a] \odot x = [1]$ in $\mathbb{Z}_n$

An analysis of the equation is always available as soon as $\mathbb{Z}_n$ is a finite set.

Examples $[3] \odot x = [1]$ in $\mathbb{Z}_6$ has no solutions:

$$\left.\begin{array}{ll} 3\cdot 0 = 0 & 3\cdot 3 = 9 = 3 \\ 3\cdot 1 = 3 & 3\cdot 4 = 12 = 0 \\ 3\cdot 2 = 6 = 0 & 3\cdot 5 = 15 = 3 \end{array}\right] \text{ in } \mathbb{Z}_6$$

$\mathbb{Z}_6 = \{[0], [1], \ldots [5]\}$

$[5] \odot x = [1]$ in $\mathbb{Z}_6$

$x = [5]$ is a solution

$$\begin{array}{ll} 5\cdot 0 = 0 & 5\cdot 3 = 15 = 3 \\ 5\cdot 1 = 5 & 5\cdot 4 = 20 = 2 \\ 5\cdot 2 = 10 = 4 & \underline{5\cdot 5 = 25 = 1} \end{array}$$

$5\cdot 5 \equiv 1 \pmod 6$