

Trabajando con  $\mathbb{Z}_n$   $n \in \mathbb{N}$   $n = 3, 4, 5, 6$

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$$

$$n=5 \quad \mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

$$150 \quad \mathbb{Z}_{150} = \{[0], [1], [2], [3], \dots, [149]\}$$

$$77 \quad \mathbb{Z}_{77} = \{[0], [1], [2], \dots, [76]\}$$

$$\mathbb{Z}_3 = \{[0], [1], [2]\}$$

$$[p] + [q] = [p+q] \quad [p] \cdot [q] = [p \cdot q]$$

$$\mathbb{Z}_3 = \{[0], [1], [2]\}$$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$[3] = [0]$$

$$\begin{array}{r} 3 \overline{) 12} \\ \underline{0} \phantom{0} \\ 12 \phantom{0} \\ \underline{12} \\ 0 \end{array} \quad [4] = 1 \quad \mathbb{Z}_3 \rightarrow \text{Es un cuerpo}$$

$$[-1] = [2]$$

$$\begin{array}{r} -1 \overline{) 1} \\ \underline{-1} \\ 0 \end{array}$$

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$$\begin{array}{r} 4 \overline{) 14} \\ \underline{0} \phantom{0} \\ 14 \phantom{0} \\ \underline{12} \\ 2 \end{array} \quad \begin{array}{r} 5 \overline{) 14} \\ \underline{10} \\ 4 \end{array} \quad \begin{array}{r} 6 \overline{) 14} \\ \underline{12} \\ 2 \end{array} \quad \begin{array}{r} 7 \overline{) 14} \\ \underline{14} \\ 0 \end{array} \quad \begin{array}{r} 8 \overline{) 14} \\ \underline{8} \\ 6 \end{array} \quad \begin{array}{r} 9 \overline{) 14} \\ \underline{9} \\ 5 \end{array} \quad \begin{array}{r} 12 \overline{) 14} \\ \underline{12} \\ 2 \end{array} \quad \begin{array}{r} 15 \overline{) 14} \\ \underline{15} \\ -1 \end{array}$$

$$\mathbb{Z}_4 \rightarrow \text{No es un cuerpo}$$

$$\mathbb{Z}_5$$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	0	3
3	0	3	1	4	2
4	0	4	3	2	1

$$\begin{array}{r} 5 \overline{) 15} \\ \underline{0} \\ 15 \phantom{0} \\ \underline{15} \\ 0 \end{array} \quad \begin{array}{r} 6 \overline{) 15} \\ \underline{12} \\ 3 \end{array} \quad \begin{array}{r} 7 \overline{) 15} \\ \underline{14} \\ 1 \end{array} \quad \begin{array}{r} 8 \overline{) 15} \\ \underline{8} \\ 7 \end{array} \quad \begin{array}{r} 9 \overline{) 15} \\ \underline{9} \\ 6 \end{array} \quad \begin{array}{r} 12 \overline{) 15} \\ \underline{12} \\ 3 \end{array} \quad \begin{array}{r} 15 \overline{) 15} \\ \underline{15} \\ 0 \end{array}$$

$$\mathbb{Z}_5 \rightarrow \text{Es un cuerpo}$$

$\mathbb{Z}_n \rightarrow$  Es un cuerpo si  $n$  es un primo