Enteros módulo P

- Conjunto — ej. $\{1, 3, 5, 7\}$
- Grupo: conjunto con una operación

$\{1, 2, 3\}$ y $\oplus$

$a \oplus b = a + b$

$1 \oplus 2 = 3$, $1 \oplus 3 = 1 + 3 = 4$ ✗ no es cerrado!

∴ no es grupo.

$ax + by + cz \oplus dx + ey + fz$

$(a+d)x + (b+e)y + (c+f)z$ sí es cerrado

$a \oplus (b \oplus c) = (a \oplus b) \oplus c$ Asociativo

$a \oplus 0 = a$ existe identidad

$a \oplus (-a) = 0$ existe inverso

$\{0, 1, 2, 3\}$ $\oplus$ = suma módulo 4

0 es su mismo inverso, identidad

$1 \oplus 3 = 0$

$2 \oplus 2 = 0$

$2 \oplus 3 = 1$ cerrado

$\{0,1,2,3,4\}$ es campo con $\oplus$ y $\otimes$ mód. 5. ?

$2*(3+4) = 2*2 = 4$

$2*3 + 2*4 = 1 + 3 = 4$

$\{0,1,2,3\}$ es campo con $\oplus$ y $\otimes$ mod 4 ?

$2(2+3) = 2*1 = 2$

$2*2 + 2*3 = 4 + 2 = 2$

$2 \otimes 0 = 0$ ←

$2 \otimes 1 = 2$ ← no da 1, por tanto

$2 \otimes 2 = 4 = 0$ ↙ 2 no tiene inverso $\otimes$

$2 \otimes 3 = 6 = 2$ ↙

$\Rightarrow$ no es campo

$\{0,1,2,\ldots,p-1\}$ es campo con $\oplus$ y $\otimes$ mod. p $\Leftrightarrow$ p es primo

$\{0,1,2,3,4,5,6\}$ es campo con $\oplus$ y $\otimes$ mod 7.

$a, b \in \mathbb{R}$ $\exists\, c \neq a < c < b$

$a \neq b$