

in \mathbb{Z}_{10}

$$2 + 2 = 4$$

$$2 \cdot 2 = 4$$

$$2^2 = 4$$

$$2^8 \equiv 5 \pmod{101}$$

$$5 \cdot 101 \equiv 0 \pmod{101}$$

in \mathbb{Z}_7

$$\frac{1}{4} = x : (1 \equiv 4x \pmod{7}) = 2$$

$$-4 \equiv 3 \pmod{7}$$

$$\text{Defn } f(x) = 3 + 2x - x^2$$

$$\bullet f(0) = 3$$

$$\bullet f(5) = -12 \equiv 2 \pmod{7}$$

$$\bullet f(x) = 0$$

$$x^2 - 2x - 3 \equiv 0 \pmod{7}$$

$$x_1 = -1 \equiv 6 \pmod{7} \quad x_2 = 3$$

• Def: Is f a permutation of the ring? i.e. it maps each element of \mathbb{Z}_7 to a unique element in \mathbb{Z}_7

$$\forall y \in \mathbb{R}, \exists! x \in \mathbb{R} \text{ s.t. } f(x) = y$$

$$f(0) = 3$$

$$f(1) = 4$$

$$f(2) = 3$$

$$f(3) = 0$$

$$f(4) = 0$$

$$f(5) = 2$$

$$f(6) = 2$$

condition violated. The answer is no.