

A che cosa serve il teorema che dice che le operazioni in \mathbb{Z} sono compatibili con la relazione di congruenza mod n , cioè che

$$\forall a, b, c, d \in \mathbb{Z} \quad \text{con } a \equiv c \pmod{n}, b \equiv d \pmod{n} \text{ si ha}$$
$$a+b \equiv c+d \pmod{n} \quad \text{e} \quad a \cdot b \equiv c \cdot d \pmod{n} \quad ?$$

① a fare dei conti più facilmente: ad esempio per calcolare

$$85 \cdot 79 \pmod{89}$$

basta osservare che $85 \equiv -4 \pmod{89}$, $79 \equiv -10 \pmod{89}$ e quindi

$$85 \cdot 79 \equiv (-4) \cdot (-10) \equiv 40 \pmod{89}.$$

Sfunteremo questa applicazione per dimostrare i criteri di divisibilità per 2, 5, 10, 3, 9, 11, 7...

② a introdurre in \mathbb{Z}_n le operazioni di somma \oplus_n e prodotto \odot_n :

$$\forall [a]_n, [b]_n \quad \begin{cases} [a]_n \oplus_n [b]_n = [a+b]_n \\ [a]_n \odot_n [b]_n = [ab]_n \end{cases}$$

(nella pratica scriveremo al posto di \oplus_n e \odot_n , + e · come si fa in \mathbb{Z} , ma sono operazioni diverse).

Perché? Proviamo a fare un esempio

$n=4$, $a=1$, $b=2$. Ho appena definito la somma con:

$$[1]_4 + [2]_4 = [1+2]_4 = [3]_4$$

Ma 1 e 2 sono solo due RAPPRESENTANTI delle classi di congruenza.

Che cosa succede se cambio i rappresentanti? La classe di congruenza somma sarà ancora la stessa?

$$\text{Ad es. } [1]_4 = [5]_4, [2]_4 = [-6]_4 \Rightarrow [5]_4 + [-6]_4 = [5-6]_4 = [-1]_4$$

Poi ché $3 \equiv -1 \pmod{4}$ posso dire che la classe è la stessa.

Ma dovrei verificare la stessa proprietà per gli infiniti altri rappresentanti di $[1]_4$ e $[2]_4$ (oltre che per tutte le 4^2 coppie di elementi di \mathbb{Z}_4 e per tutte le n^2 coppie ^{dist.} di \mathbb{Z}_n al variare di n ...!).

Se invece applico la proprietà $a+b \equiv c+d \pmod{n}$ se $a \equiv c \pmod{n}$ e $b \equiv d \pmod{n}$, e la proprietà che una classe di congruenza può essere rappresentata da un qualunque suo elemento trovo:

$$[a]_n + [b]_n = [a+b]_n = [c+d]_n = [c]_n + [d]_n$$

Idem per il prodotto. Quindi le due operazioni definite non dipendono dal rappresentante usato per ciascuno delle classi di congruenza.

La situazione è simile a quando d'istmo che in \mathbb{Q} :

$$\frac{1}{2} = \frac{5}{10}, \quad \frac{3}{5} = \frac{6}{10} \quad \text{e quindi} \quad \frac{1}{2} + \frac{3}{5} = \frac{5}{10} + \frac{6}{10} = \frac{11}{10} \quad (\text{ad es.})$$

Rispetto alla somma e al prodotto valgono in \mathbb{Z}_n proprietà (simili) a quelle che valgono in \mathbb{Z} :

0) $+$ e \cdot sono operazioni interne in \mathbb{Z}_n poiché ho definito:

$$\begin{aligned} [a]_n + [b]_n &= [a+b]_n & \text{e questo \u00e9 un elem. di } \mathbb{Z}_n \\ [a]_n \cdot [b]_n &= [ab]_n & \text{" " " " } \mathbb{Z}_n \end{aligned}$$

1) $+$ e \cdot sono associative poich\u00e9 $\forall [a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$

$$([a]_n + [b]_n) + [c]_n \stackrel{\text{DEF } \#_n}{=} [a+b]_n + [c]_n \stackrel{\text{DEF } \#_n}{=} [(a+b)+c]_n \stackrel{\text{Assoc. in } \mathbb{Z}}{=} [a+(b+c)]_n \stackrel{\text{DEF } \#_n}{=} [a]_n + [b+c]_n \stackrel{\text{DEF } \#_n}{=} [a]_n + ([b]_n + [c]_n)$$

$$([a]_n \cdot [b]_n) \cdot [c]_n = [a \cdot b]_n \cdot [c]_n = [(ab)c]_n = [a(bc)]_n = [a]_n \cdot [bc]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$$

2) $+$ e \cdot sono commutative poich\u00e9 $\forall [a]_n, [b]_n \in \mathbb{Z}_n$

$$[a]_n + [b]_n \stackrel{\text{DEF } \#_n}{=} [a+b]_n \stackrel{\text{comm in } \mathbb{Z}}{=} [b+a]_n \stackrel{\text{DEF } \#_n}{=} [b]_n + [a]_n$$

$$[a]_n \cdot [b]_n = [ab]_n = [ba]_n = [b]_n \cdot [a]_n$$

5) Vale la propriet\u00e0 di distributiva del prodotto rispetto alle somme

$$\begin{aligned} ([a]_n + [b]_n) \cdot [c]_n &\stackrel{\text{DEF } \#_n}{=} [a+b]_n \cdot [c]_n \stackrel{\text{DEF } \circ_n}{=} [(a+b) \cdot c]_n \stackrel{\text{DISTR in } \mathbb{Z}}{=} [ac+bc]_n \stackrel{\text{DEF } \#_n}{=} [ac]_n + [bc]_n \stackrel{\text{DEF } \circ_n}{=} \\ &= [a]_n \cdot [c]_n + [b]_n \cdot [c]_n \end{aligned}$$

(Fin qui la struttura delle verifiche \u00e9 sempre la stessa!!)

3) Esistono l'elem. neutro rispetto alla somma e rispetto al prodotto:

per la verifica conviene "provare a vedere se" le due classi di resto rappresentate da $0, 1 \in \mathbb{Z}$ si comportano come richiesto. In effetti

$$\forall [a]_n \in \mathbb{Z}_n \text{ si ha } \begin{aligned} [a]_n + [0]_n &= [a+0]_n = [a]_n \\ [a]_n \cdot [1]_n &= [a \cdot 1]_n = [a]_n \end{aligned}$$

il che, per l'unicit\u00e0 del neutro, prova che $[0]_n$ e $[1]_n$ sono proprio gli elem. neutri rispetto a somma e prodotto (in quest'ordine).

4) Per ogni $[a]_n \in \mathbb{Z}_n$ esiste l'opposto. Anche qui proviamo a prendere la classe $[-a]_n$:

$$[a]_n + [-a]_n = [a+(-a)]_n = [a-a]_n = [0]_n \Rightarrow -[a]_n = [-a]_n$$

(per l'unicit\u00e0 dell'opposto). Notare che dato che $[0]_n = [n]_n$ si pu\u00f2 anche scrivere $-[a]_n = [n-a]_n$, ci\u00f2 \u00e9 ad es. $-[1]_4 = [4-1]_4 = [3]_4$.

Ma se n \u00e9 primo in \mathbb{Z}_n tutte le classi di congruenza $\neq [0]_n$ sono invertibili, ci\u00f2 \u00e9 $\forall [a]_n \neq [0]_n$ esiste $[x]_n$ tale che $[a]_n [x]_n = [1]_n$

(in termini di congruenze significa $ax \equiv 1 \pmod n$, ci\u00f2 \u00e9 $\exists k \in \mathbb{Z}$ t.c.

$ax - 1 = kn$ o anche $ax - nk = 1$: EQ. DIOPANTEA in x e k); si dice che $(\mathbb{Z}_n, +, \cdot)$ \u00e9 un CAMPO, come $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

se n NON \u00e9 primo, $n = hk$ con $h, k \in \mathbb{Z} \setminus \{0, 1\}$, allora ci sono classi

di resto diversi da zero come $[h]_n$ e $[k]_n$ il cui prodotto \u00e9 $[n]_n = [0]_n$: si dice

che \mathbb{Z}_n ha divisori di zero. E non valgono pi\u00f9 le regole di semplificazione: $[a][a] = [h][b] \neq [a] = [b]$.