

I criteri di divisibilità e le congruenze ①

Il concetto di **congruenza** è dovuto a **Gauss** e risale circa al 1798.

Definizione

Due numeri si dicono **congruenti modulo n** se, nella divisione per n , danno lo stesso resto.

Per esempio i numeri 1, 4, 7, 10 sono congruenti modulo 3 perché divisi per 3 danno tutti resto 1, si scrive per es. $4 \equiv 7 \pmod{3}$.

Raggruppando i numeri congruenti si ottengono le **classi resto**.

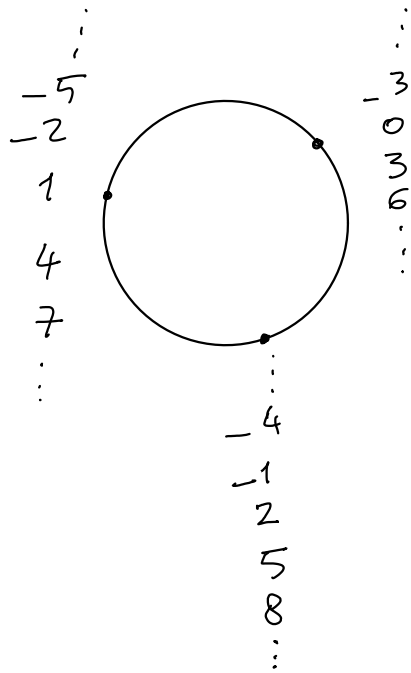
Nel caso della divisione per 3 si ottengono 3 **classi resto** che contengono tutti i numeri interi:

$$[0]_{\text{mod } 3} = \{ \dots, -6, -3, 0, 3, 6, 9, \dots \}$$

$$[1]_{\text{mod } 3} = \{ \dots, -5, -2, 1, 4, 7, 10, \dots \}$$

$$[2]_{\text{mod } 3} = \{ \dots, -4, -1, 2, 5, 8, 11, \dots \} \quad (2)$$

Una rappresentazione geometrica dei numeri interi modulo 3 è la seguente:



I numeri **congruenti a zero modulo 3** sono **tutti e soli** quelli **divisibili per 3**.

La relazione di congruenza è una **relazione di equivalenza**.

Le relazioni di equivalenza su un insieme A sono quelle per le quali valgono le proprietà:

1) *riflessiva* : $\forall a \in A \Rightarrow a R a$ (3)

quantificatore universale (per ogni) simbolo di appartenenza implica

(ogni elemento di A è in relazione con se stesso)

2) *simmetrica* : $a R b \Leftrightarrow b R a$

3) *transitiva* : $a R b$ e $b R c \Rightarrow a R c$

Un esempio di relazione di equivalenza è l'uguaglianza.

Gli insiemi di elementi in relazione tra loro sono chiamati *classi di equivalenza*.

La congruenza è una relazione di equivalenza, infatti ogni numero è congruente a se stesso, inoltre la congruenza è simmetrica e transitiva (esempio se $4 \equiv 7 \pmod{3}$ e $7 \equiv 10 \pmod{3} \Rightarrow 4 \equiv 10 \pmod{3}$)

Le classi di equivalenza della congruenza sono le classi resto.

Le classi di equivalenza sono insiemi **disgiunti** (separati) e **ricoprono** l'insieme dei numeri interi.

Nel linguaggio matematico si dice che le classi di equivalenza costituiscono una **partizione** dell'insieme.

Proprietà delle congruenze

Per le congruenze valgono alcune proprietà che valgono anche per le uguaglianze.

Se $a \equiv a'$ e $b \equiv b' \pmod{n}$, si ha:

- 1) $a + b \equiv a' + b'$
- 2) $a - b \equiv a' - b'$
- 3) $ab \equiv a'b'$

Infatti se $a \equiv a' \pmod{n}$ significa che $a = a' + n \cdot t$, cioè che a ed a'

5
differiscono per un multiplo del
divisore.

Allora se $a' \equiv a$ e $b' \equiv b \pmod{n}$

significa che

$$a' = a + t \cdot n \quad \text{e} \quad b' = b + s \cdot n,$$

dove t ed s sono numeri interi.

Se si eseguono per esempio le
somme si ottiene:

$$\begin{aligned} a' + b' &= a + t \cdot n + b + s \cdot n = \\ &= a + b + (t + s) \cdot n \end{aligned}$$

Si vede che anche $a' + b' \equiv a + b$ perché
differiscono per un multiplo del
divisore n .

In modo simile si dimostra che
se $a \equiv a'$ e $b \equiv b' \pmod{n}$ allora

$$a - b \equiv a' - b' \pmod{n} \quad \text{e}$$

$$a \cdot b \equiv a' \cdot b' \pmod{n}.$$

Esempio

6

$$7 \equiv 1 \quad \text{e} \quad 5 \equiv 2 \quad \text{mod } 3$$

allora

$$1) \quad 7 + 5 \equiv 1 + 2 = 3 \equiv 0 \quad \text{mod } 3$$

(infatti $7 + 5 = 12 \equiv 0$)

$$2) \quad 7 - 5 \equiv 1 - 2 = -1 \equiv 2 \quad \text{mod } 3$$

(infatti $7 - 5 = 2 \equiv 2$)

$$3) \quad 7 \cdot 5 \equiv 1 \cdot 2 = 2 \equiv 2 \quad \text{mod } 3$$

(infatti $7 \cdot 5 = 35 \equiv 2$)

Congruenze e divisibilità

Un numero è divisibile per n se è congruente a zero modulo n .

Ogni numero, nel sistema decimale, può essere scritto come somma dei prodotti delle sue cifre per le successive potenze di 10.

Esempio

$$253 = 2 \cdot 100 + 5 \cdot 10 + 3 \cdot 1$$

Se siamo interessati, per esempio, alla divisibilità per 3, è utile studiare la congruenza delle potenze di 10 modulo 3:

$1 \equiv 1$	Come si vede tutte le potenze di 10 sono congruenti a 1.
$10 \equiv 1$	
$100 = 10 \cdot 10 \equiv 1 \cdot 1 = 1$	
.....	

Di conseguenza:

$$253 = 2 \cdot 100 + 5 \cdot 10 + 3 \cdot 1 \equiv 2 \cdot 1 + 5 \cdot 1 + 3 \cdot 1 = 2 + 5 + 3 = 10 \equiv 1$$

non è divisibile per 3 perché non è congruente a 0 (da resto 1), mentre 252 è divisibile per 3.

La divisibilità per 3 si ha quindi se e solo se la somma delle cifre del numero è divisibile per 3.

Questo metodo si può applicare al problema della divisibilità per qualunque numero.

Esempi

8

1) Divisibilità per 2

Le congruenze modulo 2 delle potenze di 10 sono:

$$1 \equiv 1, \quad 10 \equiv 0, \quad 100 = 10 \cdot 10 \equiv 0 \cdot 0 = 0$$

$$1000 = 100 \cdot 10 \equiv 0 \cdot 0 = 0, \quad \dots$$

Tutte le potenze di 10 sono congruenti a zero. Solo l'unità è congruente a 1, quindi un numero qualsiasi, come 1234, risulta divisibile per 2 se la cifra delle unità lo è.

Per esempio 1234 è divisibile per 2, infatti

$$1234 = 1 \cdot 1000 + 2 \cdot 100 + 3 \cdot 10 + 4 \cdot 1 \equiv$$

$$\equiv 1 \cdot 0 + 2 \cdot 0 + 3 \cdot 0 + 4 \cdot 1 = 4 \equiv 0 \pmod{2}$$

3) Divisibilità per 7

Le congruenze delle potenze di 10 modulo 7 sono:

$$1 \equiv 1 \pmod{7}$$

$$10 \equiv 3$$

$$100 = 10 \cdot 10 \equiv 3 \cdot 3 = 9 \equiv 2$$

$$1000 = 100 \cdot 10 \equiv 2 \cdot 3 = 6 \equiv -1$$

9

$$10000 = 1000 \cdot 10 \equiv -1 \cdot 3 = -3$$

$$100000 = 10000 \cdot 10 \equiv -3 \cdot 3 = -9 \equiv -2$$

$$1000000 = 100000 \cdot 10 \equiv -2 \cdot 3 = -6 \equiv 1$$

- - -

Un numero è quindi divisibile per 7 se la somma delle sue cifre, a partire dalle unità, moltiplicate per la sequenza di numeri 1, 3, 2, -1, -3, -2, ... da un numero divisibile per 7 (cioè congruente a zero modulo 7).

Per esempio il numero

$$1234 = 1 \cdot 1000 + 2 \cdot 100 + 3 \cdot 10 + 4 \cdot 1 \equiv$$

$$= 1 \cdot (-1) + 2 \cdot 2 + 3 \cdot 3 + 4 \cdot 1 =$$

$$= -1 + 4 + 9 + 4 \cdot 1 = 16 \equiv 2 \pmod{7}$$

non è divisibile per 7 (il resto è 2),

mentre lo è il numero $1232 \equiv 0$,

infatti:

$$1 \cdot (-1) + 2 \cdot 2 + 3 \cdot 3 + 2 \cdot 1 =$$

$$= -1 + 4 + 9 + 2 = 14 \equiv 0 \pmod{7}$$

4) Divisibilità per 11

10

Anche in questo caso si parte dalle congruenze delle potenze di 10 (mod 11):

$$1 \equiv 1$$

$$10 \equiv -1$$

$$100 = 10 \cdot 10 \equiv 1$$

$$1000 = 100 \cdot 10 \equiv -1$$

- - -

Si ottiene il noto criterio di divisibilità

un numero è divisibile per 11 se e solo se la somma delle sue cifre, a partire dalle unità, moltiplicate per la sequenza di numeri 1, -1, 1, -1, ... dà un numero divisibile per 11.

Per esempio $1234 = 1 \cdot 1000 + 2 \cdot 100 + 3 \cdot 10 + 4 \cdot 1 \equiv$

$$\equiv 1 \cdot (-1) + 2 \cdot 1 + 3 \cdot (-1) + 4 \cdot 1 =$$

$$= -1 + 2 - 3 + 4 = 2 \equiv 2 \pmod{11}$$

non è divisibile per 11 (dà resto 2)

mentre 1232 lo è ($1232 : 11 = 112$).