

Le tre lineette (\equiv)

Le **tre lineette** (\equiv) in matematica rappresentano il simbolo di **congruenza modulo**. Indicano una relazione tra due numeri in cui la loro differenza è divisibile per un terzo numero, detto **modulo**. In pratica, $a \equiv b \pmod{n}$ significa che a e b danno lo stesso resto quando vengono divisi per n .

Significato Formale

La scrittura $a \equiv b \pmod{n}$ si legge come “ **a è congruo a b modulo n** ” e significa:

$$a - b = k n$$

dove k è un numero intero. Equivalentemente, vuol dire che **a e b hanno lo stesso resto** quando divisi per n .

Un esempio pratico

Se diciamo:

$$17 \equiv 5 \pmod{6}$$

significa che la differenza tra 17 e 5 (ovvero 12) è un multiplo di 6. Dividendo 17 per 6, infatti, otteniamo un resto di 5, esattamente come dividendo 5 per 6.

Perché è utile nelle esponenziazioni modulari

Nell’RSA e in altre operazioni crittografiche, lavorare con esponenziazioni modulari significa ridurre i risultati intermedi al modulo n per mantenere i numeri entro una dimensione praticabile, poiché elevare un numero a grandi esponenti produce numeri enormi. Vi sono delle criticità per numeri veramente enormi e complessità nell’elaborarli.