Congruenze

Nell'insieme dei numeri relativi introduciamo la relazione di congruenza modulo m.

Dati due numeri relativi a e b, diciamo che sono congrui modulo m se la loro differenza è divisibile per m e scriveremo

$a-b=km$ oppure

$a\equiv b(\mathrm{mod}\,m)$

dove m viene chiamato modulo della congruenza.
Inoltre possiamo dire che:
Due numeri relativi a e b, sono congrui modulo m se divisi per m danno lo stesso resto.

Teorema Due numeri relativi a e b sono congrui modulo m se e solo se la loro differenza è divisibile per m.
Sia

i) $a\equiv b(\mathrm{mod}\,m)$ allora

$a=mq_1+r$

$b=mq_2+r$

e quindi

$a-b=mq_1+r-(mq_2+r)=mq_1+r-mq_2-r=mq_1-mq_2=m(q_1-q_2)$

pertanto $a-b$ è divisibile per m

ii) $a-b$ sia divisibile per m
per cui

$a-b=mq$

e quindi

$a=b+mq$

dividendo b per m otteniamo

$b=mq_1+r$

sostituendo avremo

$a=mq_1+r+mq$

$a=m(q_1+q)+r$

cioè, a diviso per m fornisce lo stesso resto r. Ne consegue che

$a\equiv b(\mathrm{mod}\,m)$.

Teorema Condizione necessaria e sufficiente affinché due numeri a e b siano congrui modulo m è che a e b divisi per m diano lo stesso resto.
Dim.

$a=mq_1+r_1$

$b=mq_2+r_2$ per ipotesi

Ts $a-b=km$

Si ha

$a-b=(q_1-q_2)\,m+r_1-r_2$

Confrontando con la

$a-b=km$, poiché $m\,|\,(a-b)$ dovrà necessariamente essere

$r_1 = r_2$.

Per le congruenze modulo un prefissato un intero m e $a,b,c \in \mathbb{Z}$ valgono le seguenti proprietà

1) $a \equiv a \pmod m$ proprietà riflessiva

2) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ proprietà simmetrica

3) $a \equiv b \pmod m \vee b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ proprietà transitiva

4) $a \equiv b \pmod m \Rightarrow (a+d) \equiv (b+d) \pmod m$

5) $a \equiv b \pmod m \Rightarrow ad \equiv bd \pmod m$

Da queste proprietà segue la:

Def. Per ogni m appartenente a $\mathbb{Z}$, alla relazione $a \equiv b \pmod m$ associamo una partizione in classi di equivalenza e l'insieme quoziente modulo la relazione di equivalenza sarà l'insieme $\{[0],[1],[2],....,[m-1]\}$ che prende il nome di **insieme delle classi resto modulo m**

Le classi resto distinte modulo m sono tante quanto sono i resti possibili che si hanno nella divisione modulo m, cioè

$0,1,2,....., m-1$

Poiché le classi resto modulo m distinte tra loro sono m, possiamo scegliere come loro rappresentanti gli m numeri non negativi minori di m (cioè i resti delle divisioni per m) in modo che le classi resto modulo m siano

$[0],[1],[2],....,[m-1]$

dove

$[0] = \{...,-3m,-2m,-m,0,m,2m,3m,...\}$

cioè l'insieme dei multipli di m, in generale

$[k] = \{..., k-4m, k-3m, k-2m, k-m, k, k+m, k+2m, k+3m,...\}$

……

$[m-1] = \{...,-1-3m,-1-2m,-1-m,-1,2m-1,3m-1,...\}$

Consideriamo due classi $[a];[b]$ e due elementi generici, uno della prima ed uno della seconda

$a_k = a + km$

$b_h = b + km$ con $h,k \in \mathbb{Z}$

Si ha:

$a_k + b_h = a + km + b + km = a + b + (h+k)m$

e quindi

$a_k + b_h \equiv (a+b) \bmod m$

per cui avremo:

$[a+b] = [a_k + b_h]$

Cioè, comunque si prende un elemento $a_k \in [a]$ e $b_k \in [b]$ la somma $\in [a+b]$; pertanto possiamo introdurre l'operazione di addizione così definita

$[a] + [b] = [a+b]$

Analogamente per la moltiplicazione si ha

$a_k b_h = (a+km)(b+km) = ab + (bk + ah + khm)m$

e quindi

$a_k b_h \equiv (ab) \bmod m$

cioè

$$[ab]=[a_k b_h]$$

Comunque si prenda un elemento $a_k \in [a]$ e $b_k \in [b]$ il loro prodotto $\in [ab]$ e quindi

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

Esempi

Risolvere la congruenza

$$12x \equiv 15 (\mathrm{mod} 39)$$

La congruenza ammette soluzioni perché

$$(39,12)=3 \mid 15$$

Per determinare una soluzione applichiamo l'algoritmo di Euclide

39	12
3	3

$$39=(3\cdot 12)+3$$

$$3=39+(-3)\cdot 12$$

essendo

$$15=3\cdot 5$$ avremo

$$15=5\cdot 3=5\cdot 39+(-15)\cdot 12$$

$$12\cdot(-15)-15=39\cdot 5$$

e quindi possiamo scrivere

$$12\cdot(-15)\equiv 15(\mathrm{mod}39)$$

per cui -15 è una soluzione

Tutte le altre si ottengono da essa aggiungendo un arbitrario multiplo di $\frac{m}{(m,a)}$

Essendo $(m,a)=(39,12)=3$

avremo

$$x=-15+k\frac{39}{3}$$

cioè

$$x=-15+13k \quad \text{con} \quad k\in\mathbb{Z}$$

Risolvere la congruenza

$$12x \equiv 33 (\mathrm{mod} 57)$$

La congruenza ammette soluzioni perché

$$(12,57)=3 \mid 33$$

Per determinare una soluzione applichiamo l'algoritmo di Euclide

57	12
21	3

$57 = (3 \cdot 12) + 21$ e quindi

$21 = 57 + (-3) \cdot 12$

Si deve trovare pertanto un fattore tale che 33 sia multiplo di 21

Si ha $[33]_{57} = [90]_{57} = [147]_{57}$

Essendo 147 divisibile per 21 possiamo scrivere

$[33]_{57} = [147]_{57}$

e quindi

$147 = 7 \cdot 21$ od anche

$147 = 7 \cdot [57 + (-3) \cdot 12]$

$147 = 7 \cdot 57 + (-21) \cdot 12$

e quindi possiamo scrivere

$12 \cdot (-21) - 147 = 57 \cdot 7$ ovvero

$12 \cdot (-21) \equiv 147 (\mathrm{mod} 57)$

per cui -21 è una soluzione

Tutte le altre si ottengono da essa aggiungendo un arbitrario multiplo di $\frac{m}{(m, a)}$

avremo

$$x = -21 + k \frac{57}{(57,12)}$$

cioè

$$x = -21 + \frac{57}{3} k$$

$x = -21 + 19k$ con $k \in \mathbb{Z}$