DEFINIZIONE Sia n un intero dato. Scriviamo $a \equiv b \bmod n$ se abbiamo che $n \mid (a - b)$.

La relazione ora definita si chiama *congruenza modulo n*, n si dice *modulo* della relazione, e $a \equiv b \bmod n$ si legge «a è congruo a b modulo n».

La relazione di congruenza gode delle seguenti proprietà fondamentali:

LEMMA

1. *La relazione di congruenza modulo n definisce una relazione di equivalenza sull'insieme degli interi.*
2. *Questa relazione di equivalenza ha n distinte classi di equivalenza.*
3. *Se* $a \equiv b \bmod n$ *e* $c \equiv d \bmod n$, *allora si ha* $a + c \equiv b + d \bmod n$ *e* $ac \equiv bd \bmod n$.
4. *Se* $ab \equiv ac \bmod n$ *e a è relativamente primo con n, allora* $b \equiv c \bmod n$.

Dim. Verifichiamo dapprima che la relazione di congruenza modulo n è una relazione di equivalenza. Poiché $n \mid 0$, abbiamo che $n \mid (a - a)$ da cui $a \equiv a \bmod n$ per ogni a. Inoltre, se $a \equiv b \bmod n$ allora $n \mid (a - b)$, e dunque $n \mid (b - a) = -(a - b)$; dunque $b \equiv a \bmod n$. Infine, se $a \equiv b \bmod n$ e $b \equiv c \bmod n$, allora $n \mid (a - b)$ e $n \mid (b - c)$, e quindi è $n \mid \{(a - b) + (b - c)\}$, cioè $n \mid (a - c)$, e ciò vuol dire che $a \equiv c \bmod n$.

Denotiamo con $[a]$ la classe di equivalenza di a in questa relazione; la chiamiamo *classe di congruenza* (mod n) di a. Dato un intero a, per l'algoritmo euclideo $a = kn + r$, con $0 \leq r < n$. Allora $a \in [r]$ e dunque $[a] = [r]$. Vi sono così al più n classi di congruenza distinte e cioè $[0]$, $[1]$, ..., $[n - 1]$, e queste sono effettivamente distinte poiché se $[i] = [j]$ con $0 \leq i < j < n$, allora $n \mid (j - i)$ dove $j - i$ è un intero positivo minore di n, cosa impossibile. Di conseguenza vi sono precisamente le n classi di equivalenza distinte $[0]$, $[1]$, ..., $[n - 1]$. Abbiamo così dimostrato i punti 1) e 2) del lemma.

Riguardo al punto 3), sia $a \equiv b \bmod n$ e $c \equiv d \bmod n$. Allora $n \mid (a - b)$ e $n \mid (c - d)$ da cui $n \mid \{(a - d) + (c - d)\}$, dunque $n \mid \{(a + c) - (b + d)\}$. Allora $a + c \equiv b + d \bmod n$. Inoltre, $n \mid \{(a - b)c + (c - d)b\} = ac - bd$, da cui $ac \equiv bd \bmod n$.

Si noti infine che se $ab \equiv ac \bmod n$ e se a è relativamente primo con n, allora il fatto che $n \mid a(b - c)$ implica, per il Lemma 1.3.2 che $n \mid (b - c)$, e dunque $b \equiv c \bmod n$.

Se a non è relativamente primo con n, il risultato del punto 4) può non essere vero. Per esempio, $2 \cdot 3 \equiv 4 \cdot 3 \bmod 6$ ma $2 \not\equiv 4 \bmod 6$.

Il Lemma 1.3.3 ci offre alcune interessanti possibilità. Sia J_n l'insieme delle classi di congruenza mod n : $J_n = \{[0], [1], \ldots, [n - 1]\}$. Dati due elementi $[i]$ e $[j]$ in J_n definiamo

$$[i] + [j] = [i + j] \qquad \text{(a)}$$

$$[i]\,[j] = [ij] \qquad \text{(b)}$$

Il lemma ci assicura che questa «addizione» e «moltiplicazione» sono *ben definite*, vale a dire che se $[i] = [i']$ e $[j] = [j']$, allora $[i] + [j] = [i + j] = [i' + j'] = [i'] + [j']$ e $[i]\,[j] = [i']\,[j']$ (verificare).

Queste operazioni in J_n godono delle seguenti interessanti proprietà, la cui dimostrazione lasciamo per esercizio: se $[i]$, $[j]$ e $[k]$ sono tre elementi di J_n, si ha:

1. $[i] + [j] = [j] + [i]$
2. $[i]\,[j] = [j]\,[i]$

} leggi commutative

3. $([i] + [j]) + [k] = [i] + ([j] + [k])$
4. $([i]\,[j])\,[k] = [i]\,([j]\,[k])$

} leggi associative

5. $[i]\,([j] + [k]) = [i]\,[j] + [i]\,[k]$ legge distributiva
6. $[0] + [i] = [i]$.
7. $[1]\,[i] = [i]$.

Ancora un'osservazione: se $n = p$, un numero primo e se $[a] \neq 0$ è in J_p, esiste un elemento $[b]$ in J_p tale che $[a]\,[b] = 1$.

L'insieme J_n gioca un ruolo importante in algebra e in teoria dei numeri. Si chiama insieme degli *interi* mod n. Avremo modo di conoscerlo a fondo.