Teorema cinese dei resti

Sia n un intero positivo. Una *congruenza lineare modulo n* è il problema di trovare tutti i numeri interi x che soddisfano una relazione di congruenza della forma

$$ax \equiv b \pmod{n}, \text{ dove } a, b, \in \mathbf{Z} \text{ e } a \neq 0$$

In altre parole, si cercano gli interi x tali che nell'anello $\mathbf{Z_n}$ degli interi modulo n valga l'uguaglianza:

$$[a]\,[x] = [b] \pmod{n}, \text{ dove } a, b, \in \mathbf{Z} \text{ e } a \neq 0$$

Proposizione 1 (Risolubilità di congruenze lineari) Sia n un intero positivo e siano $a, b, \in \mathbf{Z}$ con $a \neq 0$. Sia, inoltre, $d = \text{MCD}(a, n)$. Allora la congruenza lineare

$$ax \equiv b \pmod{n} \quad (*)$$

ammette soluzione se e solo se $d \mid b$. In tal caso, detta x_0 una soluzione particolare, le soluzioni sono tutti e soli i numeri interi della forma

$$x_k = x_0 + k \cdot \frac{n}{d} \quad \text{al variare di } k \in \mathbf{Z}.$$

In particolare, se a e n sono coprimi, la congruenza (*) è sempre risolubile.

Dimostrazione: Supponiamo che d divida b, cioè $b = hd$ per un opportuno $h \in \mathbf{Z}$. Consideriamo l'identità di Bézout $sa + tn = d$, con $s, t \in \mathbf{Z}$; moltiplicando per h, si ricava che

$$hsa + htn = hd = b.$$

Pertanto $hsa - b = (ht) \cdot n$, e quindi $(hs) \cdot a \equiv b \pmod{n}$. Posto $x = hs$, abbiamo mostrato che x è una soluzione di (*).

Viceversa, supponiamo che la congruenza (*) ammetta soluzione e chiamiamo x una sua soluzione. Sappiamo quindi che n divide $ax - b$, e pertanto esiste $t \in \mathbf{Z}$ tale che $ax - b = nt$, ossia $b = ax + nt$. Poiché d divide sia ax che nt, segue che d divide b, e la prima affermazione è dimostrata.

Si tratta ora di descrivere l'insieme delle soluzioni, sotto l'ipotesi che l'equazione (*) ammetta almeno una soluzione x_0. Sia x una qualsiasi soluzione di (*). Poiché sia x che x_0 sono soluzioni di (*), si deve avere che $a\,x = a\,x_0 \equiv b \pmod{n}$, e quindi $a\,x - a\,x_0 \equiv 0 \pmod{n}$, cioè $a\,x - a\,x_0$ è un multiplo di n. Esiste dunque $q \in \mathbf{Z}$ tale che $a\,x - a\,x_0 = qn$, da cui si deduce che $a\,(x - x_0) = qn$; poiché d divide sia a che n, si ottiene anche che $\frac{a}{d}\,(x - x_0) = q\,\frac{n}{d}$: ma $\frac{a}{d}$ e $\frac{n}{d}$ sono coprimi, e dunque $\frac{n}{d}$ divide $(x - x_0)$. Quindi, per qualche $k \in \mathbf{Z}$, si ha che $x = x_0 + k \cdot \frac{n}{d}$ (e x coincide quindi con una delle soluzioni attese $x_k = x_0 + k \cdot \frac{n}{d}$).

Ora verifichiamo che tutti i numeri $x_k = x_0 + k \cdot \frac{n}{d}$ (al variare di $k \in \mathbf{Z}$), sono sempre soluzioni; sostituendo nell'equazione, $ax_k = a\,(x_0 + k \cdot \frac{n}{d}) = a\,x_0 + a\,k \cdot \frac{n}{d} \equiv a\,x_0 \equiv b \pmod{n}$: dunque x_k è soluzione di (*) per ogni $k \in \mathbf{Z}$.

Metodo pratico Illustriamo come ricavare una soluzione x_0 di (*), sotto l'ipotesi che $d \mid b$, cioè $b = hd$, con $h \in \mathbf{Z}$. Calcolata l'identità di Bézout $d = s\,a + t\,n$, moltiplichiamo per $h = \frac{b}{d}$ ottenendo

$$b = \frac{b}{d}\,d = \frac{b}{d}s\,a + \frac{b}{d}\,t\,n \;\equiv\; (\frac{b}{d}\,s)\,a \pmod{n}$$

dunque, una soluzione x_0 di (*) è data da $x_0 = (\frac{b}{d}\,s)$.

In $\mathbf{Z_n}$, le soluzioni di $[a]\,[x] = [b] \pmod{n}$ sono $[x_k] = [\,x_0 + k \cdot \frac{n}{d}]$ al variare di $k \in \mathbf{Z}$: si ottengono in questo modo d soluzioni differenti:

$$[x_0]\,,\ [x_1] = [\,x_0 + \frac{n}{d}\,]\,,\ [x_2] = [\,x_0 + 2 \cdot \frac{n}{d}],\ \ldots,\ [x_{d-1}] = [\,x_0 + (d-1) \cdot \frac{n}{d}]\,.$$

Si noti che, quando $d = 1$, la classe $[a]$ è invertibile in $\mathbf{Z_n}$, e l'unica soluzione è $[x_0] = [a]^{-1}\,[b]$.

Esempi (a) La congruenza lineare $412\,x \equiv 135 \pmod{2486}$ non è risolubile, perché $d = \text{MCD}(412, 2486)$ è pari e non divide 135.

(b) La congruenza lineare $48x \equiv 24 \pmod{324}$ è risolubile: infatti $d = \text{MCD}\,(48,324) = 12$, che divide 24. Per trovare una soluzione, calcoliamo i coefficienti di un'identità di Bézout $d\,(=12) = s\,48 + t\,324$. Svolgendo i calcoli, si vede che una possibilità è data da $s = 7$ e $t = -1$, di modo che $12 = 7 \cdot 48 - 324$.

Moltiplicando per 2 = 24/12, ricaviamo che 24= 14 · 48 – 2 ·324 e quindi x_0 = 14 è una soluzione della congruenza lineare. Le soluzioni sono 14 + k (324/12) = 14 + k 27 al variare di $k \in \mathbf{Z}$.

Teorema Cinese del Resto Sia t un intero maggiore di 1, siano r_1, r_2,..., r_t interi positivi a due a due coprimi, e siano b_1, b_2,..., b_t interi. Allora il sistema di congruenze lineari

(**)
$$\begin{cases} x \equiv b_1 \ (mod\ r_1) \\ x \equiv\ b_2 \ (mod\ r_2) \\ x \equiv\ b_3 \ (mod\ r_3) \\ \quad\quad ... \\ \quad\quad ... \\ x \equiv b_t \ (mod\ r_t) \end{cases}$$

è risolubile. Se x_0 è una soluzione e R = $r_1 r_2 ... r_t$, le soluzioni sono tutte e sole $x_k = x_0 + k\,R$ al variare di $k \in \mathbf{Z}$.

Dimostrazione: Posto R = $r_1 r_2 ... r_t$, definiamo R_i = R/r_i (per i= *1, ...t*) e consideriamo il nuovo sistema

$$\begin{cases} R_1 x_1 \equiv b_1 \ (mod\ r_1) \\ R_2 x_2 \equiv\ b_2 \ (mod\ r_2) \\ R_3 x_3 \equiv b_3 \ (mod\ r_3) \\ \quad\quad ... \\ \quad\quad ... \\ R_t x_t \equiv b_t \ (mod\ r_t) \end{cases}$$

Nel nuovo sistema ogni equazione ha una variabile diversa, e può essere risolta separatamente. Sia $\bar{x}_i \in \mathbf{Z}$ una soluzione della i-ma congruenza lineare, cioè $R_i \bar{x}_i \equiv b_i \ (mod\ r_i)$ per i= *1, ...t.*
Il numero

$$x_0 = R_1 \bar{x}_1 + \ R_2 \bar{x}_2 + \cdots + R_t \bar{x}_t$$

è una soluzione del sistema (**), perché R_j è congruo a zero modulo r_i non appena $i \neq j$. Dunque, il sistema (**) ammette almeno una soluzione. La descrizione di tutte le rimanenti soluzioni segue ricordando la Proposizione 1.