Lezione 9

Prerequisiti: Lezione 8.

Congruenze lineari.
Teorema Cinese del Resto.

Nella Lezione 8 abbiamo visto che, a causa della compatibilità della congruenza modulo n rispetto alle operazioni aritmetiche, le relazioni di congruenza modulo n possono essere sottoposte a trasformazioni algebriche analoghe a quelle valide per le uguaglianze. Questa lezione è dedicata alla risoluzione dei problemi che sono, nell'ambito della congruenza modulo n, l'equivalente delle equazioni lineari.

Definizione 9.1 Sia n un intero positivo. Si dice *congruenza lineare (modulo n)* il problema di trovare tutti i numeri interi x che soddisfano una relazione di congruenza della forma

$$ax \equiv b \pmod{n},$$

dove $a, b \in \mathbb{Z}$ ed $a \neq 0$.

Proposizione 9.2 *(Risolubilità di congruenze lineari)* Sia n un intero positivo e siano $a, b \in \mathbb{Z}$, dove $a \neq 0$. Sia, inoltre, $d = \mathrm{MCD}(a, n)$. Allora la congruenza lineare

$$ax \equiv b \pmod{n} \tag{1}$$

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

$$x_k = x_0 + \frac{n}{d}k, \tag{2}$$

con $k \in \mathbb{Z}$.

Dimostrazione: Supponiamo dapprima che d divida b. Allora si ha $b = dq$ per qualche $q \in \mathbb{Z}$. In base al Lemma di Bézout (Proposizione 6.15), esistono $s, t \in \mathbb{Z}$ tali che $sa + tn = d$. Di conseguenza $saq + tnq = dq = b$. Pertanto $asq - b = ntq$, e quindi $asq \equiv b \pmod{n}$. Ciò prova che $x = sq$ è una soluzione di (1).
Viceversa, supponiamo che la (1) ammetta soluzione. Allora, detta x una sua soluzione, n divide $ax - b$, quindi esiste $y \in \mathbb{Z}$ tale che $ax - b = ny$, ossia $ax - ny = b$. Poiché d divide ax e ny, segue che d divide b.
Sia ora x un'arbitraria soluzione della (1). Essendo x_0 una soluzione, si ha $ax_0 \equiv b \pmod{n}$, e quindi, $ax \equiv ax_0 \pmod{n}$. Pertanto esiste $q \in \mathbb{Z}$ tale che $a(x - x_0) = nq$, da cui si deduce che $\frac{a}{d}(x - x_0) = \frac{n}{d}q$, così che l'intero $\frac{n}{d}$ divide l'intero $\frac{a}{d}(x - x_0)$. Essendo $\frac{a}{d}$ ed $\frac{n}{d}$ coprimi, in virtù del Corollario 6.25, dalla Proposizione 6.24 segue che $\frac{n}{d}$ divide $x - x_0$. Quindi, per qualche $k \in \mathbb{Z}$,

$x-x_0=\frac{n}{d}k,$ ossia $x=x_0+\frac{n}{d}k.$ Ciò prova che ogni soluzione della (1) è data dalla formula (2). Viceversa, si ha che, per ogni $k\in\mathbb{Z}$,

$$ax_k=ax_0+a\frac{n}{d}k=ax_0+n\frac{a}{d}k\equiv ax_0\equiv b \pmod{n},$$

e quindi x_k è soluzione della (1). □

Esempio 9.3 (a) La congruenza lineare $124x\equiv 117 \pmod{356}$ non è risolubile: infatti $d=\mathrm{MCD}(356,124)$ è pari, e quindi non divide 117.
(b) La congruenza lineare $13x\equiv 2 \pmod{29}$ è risolubile: infatti $d=\mathrm{MCD}(13,29)=1$, poiché 13 e 29 sono numeri coprimi.
In generale, ogni congruenza lineare (1) in cui a e n sono coprimi è risolubile.
(c) La congruenza lineare $12x\equiv 9 \pmod{75}$ è risolubile: infatti $d=\mathrm{MCD}(12,75)=3$ divide 9.

Osservazione 9.4 Supponiamo che la congruenza lineare (1) abbia soluzione, ossia che d divida b. Allora $n=\frac{n}{d}d$ divide $ax-b=\left(\frac{a}{d}x-\frac{b}{d}\right)d$ se e solo se $\frac{n}{d}$ divide $\frac{a}{d}x-\frac{b}{d}$. Quindi, in tal caso, la congruenza (1) equivale alla congruenza lineare

$$\frac{a}{d}x\equiv\frac{b}{d} \pmod{\frac{n}{d}} \tag{3}$$

ove $\frac{a}{d}$ e $\frac{n}{d}$ sono coprimi.
Una soluzione particolare della (3) si trova nel modo seguente. Prima si determinano i coefficienti di un'identità di Bézout

$$\frac{a}{d}s+\frac{n}{d}t=1,$$

e quindi si prende $x_0=\frac{b}{d}s.$

Esercizio 9.5 Risolvere la congruenza lineare $12x\equiv 9 \pmod{75}$.
Come stabilito nell'Esempio 9.3 (c), la congruenza è risolubile e $d=3.$ Essa equivale quindi, in base all'Osservazione 9.4, alla congruenza lineare,

$$4x\equiv 3 \pmod{25}$$

Si ha l'identità di Bézout $4\cdot(-6)+25\cdot 1=1,$ quindi una soluzione particolare è $x_0=3(-6)=-18.$
Quindi la soluzione generale è $x_k=-18+25k,$ con $k\in\mathbb{Z}$.
Un'altra soluzione particolare (che si individua immediatamente) è $x_0=7.$ Quindi la formula per la soluzione generale si può anche scrivere nella forma $x_k=7+25k,$ con $k\in\mathbb{Z}$.

Osservazione 9.6 La congruenza lineare (1) equivale alla seguente equazione in $\mathbb{Z}_n$:

$$[a]_n z=[b]_n \tag{4}$$

di cui si cercano le soluzioni $z\in\mathbb{Z}_n$.

Corollario 9.7 Se l'equazione (4) è risolubile, essa ha esattamente $d = \mathrm{MCD}(a,n)$ soluzioni, e precisamente:

$$z_0 = [x_0]_n,\ z_1 = \left[x_0 + \frac{n}{d}\right]_n,\ z_2 = \left[x_0 + 2\frac{n}{d}\right]_n,\ \ldots,\ z_{d-1} = \left[x_0 + (d-1)\frac{n}{d}\right]_n.$$

Dimostrazione: In base alla Proposizione 9.2, se la (4) è risolubile, la sua soluzione generale è $z_k = [x_k]_n = \left[x_0 + \frac{n}{d}k\right]_n$, ove $k \in \mathbb{Z}$. Fissiamo un indice $k \in \mathbb{Z}$. Siano q ed r il quoziente ed il resto della divisione di k per d. Allora $r \in \{0,\ldots,d-1\}$ e

$$z_k = \left[x_0 + \frac{n}{d}k\right]_n = \left[x_0 + \frac{n}{d}(dq+r)\right]_n = \left[x_0 + nq + \frac{n}{d}r\right]_n = \left[x_0 + \frac{n}{d}r\right]_n = z_r,$$

e ciò prova che ogni soluzione della (4) è compresa fra quelle elencate nell'enunciato. Resta da provare che queste ultime sono a due a due distinte. Siano h e k numeri interi tali che $0 \le k < h \le d-1$. Allora

$$0 < x_0 + \frac{n}{d}h - \left(x_0 + \frac{n}{d}k\right) = \frac{n}{d}(h-k) < \frac{n}{d}d = n,$$

da cui segue che n non divide $x_0 + \frac{n}{d}h - \left(x_0 + \frac{n}{d}k\right)$, ossia $x_h \not\equiv x_k \pmod{n}$, ossia $z_h \neq z_k$. □

Nota L'enunciato del Corollario 9.7 si può riassumere dicendo che la congruenza (1) ha d soluzioni a due a due *non congrue* modulo n, che sono $x_0, x_1, x_2, \ldots, x_{d-1}$. Queste forniscono un sistema completo di rappresentanti per le classi che sono soluzioni dell'equazione (4).

Esempio 9.8 Consideriamo la congruenza lineare $12x \equiv 9 \pmod{75}$ dell'Esercizio 9.5. Essa ha $d = 3$ soluzioni a due a due non congrue modulo 75, e precisamente,

$$x_0 = 7, \quad x_1 = 32, \quad x_2 = 57.$$

Le soluzioni dell'equazione $[12]_{75}\, z = [9]_{75}$ di $\mathbb{Z}_{75}$ sono

$$z_0 = [7]_{75}, \quad z_1 = [32]_{75}, \quad z_2 = [57]_{75}.$$

Passiamo ora alla risoluzione di sistemi di più congruenze lineari.

Teorema 9.9 *(Prima formulazione del Teorema Cinese del Resto)* Sia s un intero maggiore di 1, siano $n_1, n_2, \ldots, n_s$ interi positivi a due a due coprimi, e siano $b_1, b_2, \ldots, b_s$ interi. Allora il sistema di congruenze lineari

$$\begin{cases} x & \equiv & b_1 & (\text{mod } n_1) \\ x & \equiv & b_2 & (\text{mod } n_2) \\ \vdots & \vdots & \vdots & \vdots \\ x & \equiv & b_s & (\text{mod } n_s) \end{cases} \tag{5}$$

è risolubile. Inoltre, detta x_0 una soluzione particolare, la soluzione generale è $x_k = x_0 + (n_1 n_2 \cdots n_s)k$, ove $k \in \mathbb{Z}$.

Dimostrazione: Sia $N = n_1 n_2 \cdots n_s$ e, per ogni $i = 1,..., s$, sia $N_i = \frac{N}{n_i} = \prod_{j \neq i} n_j$. Allora, per ogni indice i, non avendo n_i, per ogni indice $j \neq i$, alcun fattore primo in comune con n_j, segue che n_i non ha fattori primi in comune con N_i, ossia $\text{MCD}(N_i, n_i) = 1$. Pertanto, alla luce della Proposizione 9.2, per ogni $i = 1,..., s$, la congruenza lineare

$$N_i x \equiv b_i \pmod{n_i} \tag{i}$$

ammette una soluzione c_i. Sia ora $c = \sum_{i=1}^{s} N_i c_i$. Fissiamo un indice i. Osserviamo che, per ogni $j \neq i$, n_i divide N_j, e quindi anche $N_j c_j$. Pertanto

$$c = N_i c_i + \sum_{j \neq i} N_j c_j \equiv N_i c_i \equiv b_i \ (\text{mod } n_i),$$

dove l'ultima congruenza è dovuta al fatto che c_i verifica la (i). Ciò prova che c è una soluzione del sistema (5).
Sia ora $k \in \mathbb{Z}$. Allora, essendo $N \equiv 0 \pmod{n_i}$ per ogni $i = 1,.., s$, si ha che

$$x_k \equiv x_0 \equiv b_i \pmod{n_i}$$

per ogni $i = 1,..., s$, ossia x_k è soluzione del sistema (5).
Sia ora x una soluzione di (5). Allora, per ogni indice i, $x \equiv x_0 \pmod{n_i}$, quindi n_i divide $x - x_0$. Poiché gli n_i sono a due a due coprimi, segue che il loro prodotto, ossia N, divide $x - x_0$: ciò è conseguenza del Teorema Fondamentale dell'Aritmetica (Teorema 7.6). Allora, per qualche $k \in \mathbb{Z}$, $x - x_0 = kN$, cioè $x = x_k$. □

Esempio 9.10 Il sistema

$$\begin{cases} x & \equiv & 2 & (\text{mod } 4) \\ x & \equiv & 6 & (\text{mod } 7) \end{cases}$$

è risolubile. Ne determiniamo la soluzione generale secondo il procedimento indicato nella dimostrazione del Teorema Cinese del Resto. Si ha $N = 4 \cdot 7 = 28$, $N_1 = 7$, $N_2 = 4$. Consideriamo le congruenze lineari

$$7x \equiv 2 \pmod 4$$
$$4x \equiv 6 \pmod 7$$

Una soluzione della prima è $c_1 = 2$, una soluzione della seconda è $c_2 = 5$. Quindi la soluzione generale del sistema è $x_k = N_1 c_1 + N_2 c_2 + Nk = 34 + 28k$, ove $k \in \mathbb{Z}$. La più piccola soluzione positiva è $x_{-1} = 34 - 28 = 6$.