

## Congruenze lineari

(9)

DEF. Siano:  $a, b \in \mathbb{Z}$ ,  $n \in \mathbb{N}$  con  $n > 1$ . L'equazione in  $x$

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

è detta congruenza lineare e ogni intero  
 $x_0$  tale che

$$ax_0 \equiv b \pmod{n}$$

è detta soluz. della congruenza lineare.

Es. Il 1° novembre nel 2012 cadeva di giovedì.

In quale giorno della settimana cadrà nel  
2015?

- nell'intervallo di tempo considerato non  
cede un  $29/2 \Rightarrow$  anni di 365 giorni;
- giovedì è il quarto giorno della settimana;
- dal 2012 al 2015 passano 3 anni.

Quindi il problema è modellizzato  
dalla congruenza lineare

$$(*) \quad x \equiv 4 + 3 \cdot 365 \pmod{7}$$

ove  $x$  indica il numero d'ordine del giorno  
della settimana.

Ricordando che  $365 \equiv 5 + 3 \cdot 6 + 2 \cdot 3 \equiv 1 \pmod{7}$

si trova

$$x \equiv_7 4 + 3 \equiv_7 0$$

cioè il 1° Novembre 2015 sarà domenica.

Nel problema ero interessata solo alle soluzioni  
 $x$  con  $0 \leq x < 7$ . Ma ovviamente (\*) ha infinite  
soluzioni del tipo  $x = 7k$ ,  $k \in \mathbb{Z}$ .

(92)  
In generale avrò 2 problemi

- risolubilità della congruenza lineare
- determinazione di tutte le possibili soluzioni.

A entrambi rispondono, sostanzialmente, le EQUAZIONI DIOFANTEE poiché

$$ax \equiv b \pmod{n} \Leftrightarrow ax = b + kn \text{ con } k \in \mathbb{Z}$$
$$\Leftrightarrow ax - nh = b$$

quindi si tratta di risolvere un'eq. a coefficienti interi, lineare nelle INCognite  $x$  e  $k$ .

Sappiamo che  $ax - nh = b$  ha soluzioni se e solo se

$$d = \text{MCD}(a, n) \text{ divide } b$$

e che, se  $(x_0, h_0)$  è una soluzione, tutte le altre hanno la forma

$$\begin{cases} x = x_0 + \frac{n}{d} k \\ h = h_0 + \frac{a}{d} k \end{cases} \quad k \in \mathbb{Z}$$

Quindi sono soluzioni della congruenza lineare gli  $x \in \mathbb{Z}$  t.c.

$$x = x_0 + \frac{n}{d} k \quad k \in \mathbb{Z}$$

e tra queste ce ne sono esattamente d non congrue tra loro mod n.

Infatti, posto  $n' = \frac{n}{d}$ ,  $x_0, x_1 = x_0 + n', x_2 = x_0 + 2n', \dots$

$x_{d-1} = x_0 + (d-1)n'$  sono a due a due non congrue tra loro (mod n) mentre  $\forall k \neq 0, 1, \dots, d-1$  si ha  $k = dq + r$  con  $0 \leq r < d$  e quindi...

Illustriamo l'idea su un esempio

La congruenza lineare

$$9x \equiv 6 \pmod{12}$$

è risolubile poiché

$$\text{MCD}(9, 12) = 3 \mid 6$$

$$(n=12, n'=\frac{12}{3}=4)$$

Si tratta di risolvere

$$9x - 12k = 6$$

cioè

$$3x - 4k = 2$$

che ammette tra le sol. la coppia  $(x_0, k_0) = (2, 1)$

Allora tutte e sole le soluzioni della congruenza lin.

Sono del tipo

$$x_k = 2 + 4k \quad k \in \mathbb{Z}.$$

Le sol.  $x_0 = 2, x_1 = 6, x_2 = 10$

... verifichiamo che sono soluzioni

$$18 \equiv_{12} 6, \quad 54 \equiv_{12} 6, \quad 90 \equiv_{12} 6 \quad \text{OK}$$

non sono congrue a due a due modulo 12

poiché se  $i \neq j$  e  $i, j \in \{0, 1, 2\}$  si ha

$$0 \neq |x_i - x_j| < 12.$$

Ma un'altra sol.

$$x_k = 2 + 4k \quad (k \in \mathbb{Z}, k \neq 0, 1, 2)$$

dato che

$$k = 3q + r \quad \text{con } 0 \leq r \leq 2$$

si può riscrivere

$$x_k = 2 + 12q + 4r \equiv_{12} 2 + 4r = x_r \quad r=0, 1, 2$$

$$\text{es. } 22 = x_5 = 2 + 4 \cdot 5 = 2 + 4(3 \cdot 1 + 2) \equiv_{12} 2 + 4 \cdot 2 = x_2$$

cioè un'altra sol. è congrua mod 12 a  $x_0$  o a  $x_1$  o a  $x_2$ .

Oss. 1. Se  $\text{MCD}(a, n) = 1$ , ha soluzione la congruenza lin.  
 $ax \equiv 1 \pmod{n}$

e c'è una sola soluzione  $x_0$  con  $0 < x_0 < n$ .

ESEMPIO  $a = 2$ ,  $n = 9$ ; la sola soluzione compresa tra 0 e 9 è  $x = 5$ .

Cioè

$$[2]_9 \cdot [5]_9 = [1]_9$$

$$\dots \text{ posso dire che } ([2]_9)^{-1} = [5]_9.$$

Oss. 2. Se  $\text{MCD}(a, n) = 1$  si ha

$$ab \equiv ac \pmod{n} \Leftrightarrow b \equiv c \pmod{n}$$

$\Leftarrow$  Ovio!

$\Rightarrow$  Per le ipotesi esiste  $\bar{x} \in \mathbb{Z}$  t.c.  $a\bar{x} \equiv 1 \pmod{n}$

moltiplico per tale  $\bar{x}$  la congruenza

$$ab \equiv ac \pmod{n}$$

$$\bar{x}(ab) \equiv \bar{x}(ac) \pmod{n}$$

pr. ass. e comm. del prodotto in  $\mathbb{Z}$ :

$$(a\bar{x})b \equiv (a\bar{x})c \pmod{n}$$

$$1 \cdot b \equiv 1 \cdot c \pmod{n}$$



Se non è rispettata la condizione  $\text{MCD}(a, n) = 1$  questa implicazione di solito è falsa. Ad es.

$$9 \cdot 2 \equiv 9 \cdot 6 \pmod{12}$$

ma

$$2 \not\equiv 6 \pmod{12}$$

NOTA. Dire che  $x_0$  è sol. della congruenza lineare  $ax \equiv b \pmod{n}$   $a, b \in \mathbb{Z}, n \in \mathbb{N} \setminus \{1\}$   
 significa che

$[x_0]_n$  è soluzione dell'equazione in  $\mathbb{Z}_n$

$$[a]_n \cdot X = [b]_n$$

(ove l'incognita  $X$  deve prendere valori in  $\mathbb{Z}_n$ )

Quindi dire che se  $d = \text{MCD}(a, n)$  divide  $b$  ci sono  $d$  soluzioni delle congruenze lineare non congrue l'una con l'altra mod  $n$  significa che l'equazione in  $\mathbb{Z}_n$

$$[a]_n X = [b]_n$$

ha d soluzioni distinte in  $\mathbb{Z}_n$ ; mentre dire che se  $d$  non divide  $b$  la congruenza lineare non ha soluz. significa che non ha soluzioni l'equazione in  $\mathbb{Z}_n$

$$[a]_n X = [b]_n$$

Esempio. L'equazione in  $\mathbb{Z}_{10}$  :  $[5]_{10} X = [1]_{10}$   
 significa  $5x \equiv 1 \pmod{10}$  congruenza lin.  
 impossibile poiché  $\text{MCD}(5, 10) = 5$  non divide il "termine noto"  $1 \Rightarrow$  l'eq. data in  $\mathbb{Z}_{10}$  è priva di soluzioni

Invece l'eq. in  $\mathbb{Z}_{14}$  :  $[8]_{14} X = [6]_{14}$  equivale alla congruenza lineare  $8x \equiv 6 \pmod{14}$   
 che è risolubile (poiché  $d = \text{MCD}(8, 14) = 2$  divide 6) e ha 2 soluzioni non congrue mod 14 :  $x_0 = -1$  e  $x_1 = 6 \Rightarrow$  l'eq. in  $\mathbb{Z}_{14}$  ha 2 sol. :  $X = [6]_{14}$  e  $X = [13]_{14}$

(95bis)

Conseguenza particolare della NOTA pag 95

Se  $n$  è un numero primo,  $\forall a \in \mathbb{Z} \setminus \{n\}$  si ha

$$\text{MCD}(a, n) = 1$$

e quindi per ogni classe di resto  $[a]_n$  diversa da zero ( $= [0]_n = [n]_n$ ) l'equazione

$$[a]_n x = [b]_n$$

ha 1 e 1 sola soluzione. In particolare  $[a]_n$   
e 1 sola soluzione

$$[a]_n x = [1]_n$$

cioè ogni elemento non nullo di  $\mathbb{Z}_n$  è  
dotato di inverso.

## Sistemi di congruenze lineari: il teor. cinese dei resti (95)

Noi siamo qui interessati a risolvere sistemi del tipo

$$\begin{cases} a_1x \equiv b_1 \pmod{n} \\ a_2x \equiv b_2 \pmod{n} \end{cases}$$

che, attraverso i discorsi appena fatti si ricadono a sistemi di equazioni in  $\mathbb{Z}_n$  che, come logica, si comportano come ordinari sistemi di equazioni.

Ci interessa invece il caso più semplice tra i sist. del tipo:

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \end{cases} \quad n_1 \neq n_2$$

(eventualmente con  $r > 2$  equazioni), cioè ci chiediamo se esistono condizioni sotto le quali

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \vdots \\ x \equiv b_r \pmod{n_r} \end{cases}$$

ha soluzioni, quante sono e come sono fatte.

Daremo una condizione solo sufficiente di esistenza:

TEOR. Cinese dei resti. Siano  $n_1, n_2, \dots, n_r \in \mathbb{N}$  e tutti  $> 1$ ; sia inoltre  $\text{MCD}(n_i, n_j) = 1$  se  $i \neq j$ . Allora il sistema

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \vdots \\ x \equiv b_r \pmod{n_r} \end{cases} \quad (b_i \in \mathbb{Z}_n)$$

ammette soluzioni e se c è una soluzione  
ogni altra sol. c' è tale che  $c \equiv c \pmod{n_1 n_2 \dots n_r}$ .

Oss:  $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{4} \end{cases}$  ha soluzioni  $c = 1, 5, 9, \dots, -3, -7, \dots$   
anche se  $\text{MCD}(2, 4) = 2 \Rightarrow$  condiz. data è solo sufficiente

ESEMPIO PRELIMINARE . Cerchiamo di risolvere

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

Osservo che le congruenze lineari  $\underline{5y \equiv 1 \pmod{3}}$  e  $\underline{3z \equiv 1 \pmod{5}}$

hanno sol. poiché  $\text{MCD}(3,5) = 1$  divide in entrambi i casi il termine noto 1.

Scelgo una sol. per ciascuna delle due congruenze lin., ad es.

$$y_0 = 2 \quad z_0 = 2$$

e considero il numero

$$2 \cdot 5y_0 + 3 \cdot 3z_0 = 38. \quad (b_1 \cdot 5y_0 + b_2 \cdot 3z_0)$$

Per costruzione

$$2 \cdot 5y_0 + 3 \cdot 3z_0 \equiv \frac{2 \cdot 5y_0}{3} \equiv \frac{2 \cdot 1}{3} = 2$$

$$2 \cdot 5y_0 + 3 \cdot 3z_0 \equiv \frac{3 \cdot 3z_0}{5} \equiv \frac{3 \cdot 1}{5} = 3$$

$\Rightarrow c = 38$  è una soluzione del sistema.

Se  $c'$  è un'altra soluzione, per la prop. transitiva

$$c' \equiv c \pmod{3} \Rightarrow 3 | c' - c$$

$$c' \equiv c \pmod{5} \Rightarrow 5 | c' - c$$

e, poiché  $\text{MCD}(3,5) = 1$ ,  $15 = 3 \cdot 5 | c' - c \Rightarrow c' \equiv c \pmod{15}$ .

Quindi, ad es.,  $c' = 8$  è un'altra soluzione...

come si vedeva anche ad occhio.

Il bello di questa soluzione è che è algoritmica (non dipende dal colpo d'occhio) e che è facilmente generalizzabile al caso di più di 2 congruenze e si presta a diventare una dimostrazione.

Allo scopo ricordare che se  $\text{MCD}(n_i, n_j) = 1$

$i \neq j$ , anche  $\text{MCD}(n_i, \frac{n_1 \cdot n_2 \cdot \dots \cdot n_r}{n_i}) = 1$ . PERCHÉ?

Perché se tale MCD fosse  $\neq 1$  e  $p$  fosse un suo fattore primo (98)  
 $p$  dividerebbe  $n_i$  e  $n_1 \cdot n_2 \cdot \dots \cdot n_{i-1} \cdot n_{i+1} \cdot \dots \cdot n_r$  e quindi uno dei fattori, per def.  
di primo e quindi esiste  $j \neq i$  non primo con  $n_i$ .

Distr. del T.C.D.R. - Sia  $N = n_1 \cdot n_2 \cdot \dots \cdot n_r$  e  $N_i = \frac{N}{n_i}$   
Considero il sist. ausiliario di congr. lin.

$$\begin{cases} N_1 y_1 \equiv 1 \pmod{n_1} \\ N_2 y_2 \equiv 1 \pmod{n_2} \\ \vdots \\ N_r y_r \equiv 1 \pmod{n_r} \end{cases}$$

Per ogni  $i$  si ha  $\text{MCD}(n_i, N_i) = 1$  e quindi le congruenze  
lin. hanno soluzioni: ne scelgo una per ciascuna

$$\bar{y}_1, \bar{y}_2, \dots, \bar{y}_r$$

$$\text{Considero } c = b_1 N_1 \bar{y}_1 + b_2 N_2 \bar{y}_2 + \dots + b_r N_r \bar{y}_r$$

Per ogni  $i$ :

$$c = b_1 N_1 \bar{y}_1 + b_2 N_2 \bar{y}_2 + \dots + b_i N_i \bar{y}_i + \dots + b_r N_r \bar{y}_r \equiv_{n_i} b_i N_i \bar{y}_i$$

poiché  $n_i | N_j \quad \forall j \neq i$

Inoltre

$$b_i N_i \bar{y}_i \equiv b_i \cdot 1 \pmod{n_i}$$

$$\Rightarrow c \equiv b_i \pmod{n_i}$$

Cioè c è una soluz. del sist.

$$\left\{ \begin{array}{l} x \equiv t_1 \pmod{n_1} \\ x \equiv t_2 \pmod{n_2} \\ \vdots \\ x \equiv t_r \pmod{n_r} \end{array} \right.$$

Se c' è un'altra soluz. di tale sistema,  $\forall i=1, 2, \dots, r$ :

$$c' \equiv c \pmod{n_i}$$

$$\Rightarrow n_i | c' - c \Rightarrow N | c' - c \text{ poiché } \text{MCD}(n_i, n_j) = 1 \quad \forall i \neq j.$$

□

Pare che Sun-Tse avesse trovato ispirazione per  
questo teorema nelle parate militari

Ho un esercito formato da  $x$  soldati e  
so che  $x$  è "divise centinaia". Come faccio  
a "contarli"?

Li faccio schierare per 2 e conto il resto  $b_1$   
per 3 e " " " "  $b_2$   
per 5 e " " " "  $b_3$   
per 7 e " " " "  $b_4$

Basterà?  $2 \cdot 3 \cdot 5 \cdot 7 = 210$ ; se  $x$  è "divise centinaia"  
può non bastare. Li faccio schierare anche per 11 e  
questo punto la sol.  $c' < 210 \cdot 11 = 2310$  dovrebbe andare  
bene. Supponiamo che sia

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 0 \pmod{5} \\ x \equiv 6 \pmod{7} \\ x \equiv 10 \pmod{11} \end{cases}$$

se la stima "divise centinaia" non peca  
per difetto (i soldati  
non devono essere  
più di  $2 \cdot 3 \cdot 5 \cdot 7$ )

Sist. associato

$$\begin{cases} 1155y_1 \equiv 1 \pmod{2} \rightarrow \text{inutile: va mult. per } 0 \\ 770y_2 \equiv 1 \pmod{3} \\ 462y_3 \equiv 1 \pmod{5} \rightarrow \text{IDEM} \\ 330y_4 \equiv 1 \pmod{7} \\ 210y_5 \equiv 1 \pmod{11} \end{cases}$$

Una Sol. è  $c = 0 \cdot 1155\bar{y}_1 + 1 \cdot 770\bar{y}_2 + 0 \cdot 462\bar{y}_3 + 6 \cdot 330\bar{y}_4 + 10 \cdot 210\bar{y}_5$

Si tratta di trovare  $\bar{y}_2, \bar{y}_4, \bar{y}_5$  ragionevolmente  
piccoli.

Osservo:  $770 \equiv 2 \pmod{3} \Rightarrow$  invece di  $770y_2 \equiv 1 \pmod{3}$   
risolvo  $2y_2 \equiv 1 \pmod{3} : \bar{y}_2 = -1$

$330 \equiv 1 \pmod{7} \Rightarrow$  invece di  $330y_4 \equiv 1 \pmod{7}$   
risolvo  $y_4 \equiv 1 \pmod{7} : \bar{y}_4 = 1$

$210 \equiv 1 \pmod{11} \Rightarrow$  invece di  $210y_5 \equiv 1 \pmod{11}$   
risolvo  $y_5 \equiv 1 \pmod{11} : \bar{y}_5 = 1$

$$\Rightarrow c = -770 + 6 \cdot 330 + 2100 = 4080 - 770 = 3310 > N = 2310$$

$$\Rightarrow c' = c - 2310 = 1000 \text{ dovrebbe essere la soluz. cercata.}$$

OSS. Il teor. cinese dei resti non dice che  $n_1, n_2, \dots, n_k$  siano numeri primi ma che siano primi tra loro.  
 Nell'esempio precedente avrei potuto far schierare i soldati per 4, per 25 e per 11

$$\begin{cases} x \equiv 0 \pmod{4} \\ x \equiv 0 \pmod{25} \\ x \equiv 10 \pmod{11} \end{cases}$$

Sist. associato

$$\begin{cases} 275y_1 \equiv 1 \pmod{4} \rightarrow \text{imutile} \\ 44y_2 \equiv 1 \pmod{25} \rightarrow \text{imutile} \\ 100y_3 \equiv 1 \pmod{11} \end{cases}$$

Una sol. è  $c = 0 \cdot 275\bar{y}_1 + 0 \cdot 44\bar{y}_2 + 10 \cdot 100\bar{y}_3 = 1000\bar{y}_3$   
 e visto che  $100 \equiv 1 \pmod{11}$  una sol di  $100y_3 \equiv 1 \pmod{11}$   
 è  $\bar{y}_3 = 1$   
 $\Rightarrow c = 1000$  è già la soluzione cercata.

Attenzione: gli esercizi 4.5 sul testo a pag 59 non c'entano col T.C.D.R.

1.

$$\begin{cases} x \equiv 1 \pmod{4} \Rightarrow \text{sol. 1^a congr. } x = 1 + 4k \quad k \in \mathbb{Z} \\ 3x \equiv 2 \pmod{5} \Rightarrow \text{sol. 2^a " } \quad x = 4 + 5h \quad h \in \mathbb{Z} \end{cases}$$

$$1 + 4k = 4 + 5h \quad \text{eq diofantica:}$$

$$4k - 5h = 3 \quad \text{MCD}(4, 5) = 1 \mid 3 : \text{la sol. esiste}$$

$$\begin{cases} k = 2 + 5l \\ h = 1 + 4l \end{cases} \quad l \in \mathbb{Z}$$

$\Rightarrow$  soluzioni del sistema di congruenze

$$x = 1 + 4(2 + 5l) \quad l \in \mathbb{Z}$$

Cioè

$$x = 9 + 20l \quad l \in \mathbb{Z}$$

Come avrei potuto ricaudurlo al TCDR?

Ossevo che  $3 \cdot 2 \equiv 1 \pmod{5}$  e che  $\text{MCD}(2, 5) = 1$ . Quindi

$$3x \equiv 2 \pmod{5} \Leftrightarrow 3 \cdot 2x \equiv 2 \cdot 2 \pmod{5} \Leftrightarrow x \equiv 4 \pmod{5}$$

Il sistema diventa  $\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 4 \pmod{5} \end{cases}$  ecc.

E' possibile la ricordanzione a TCDR anche per gli altri? (for)

2.  $\begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 2 \pmod{10} \end{cases}$

il TCDR non si riuscirebbe ad applicare comunque poiché  $\text{MCD}(5, 10) = 5 \neq 1$

comunque osservare che  $3 \cdot 2 \equiv 1 \pmod{5}$  e  $3 \cdot 7 \equiv 1 \pmod{10}$  semplifica il sistema

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 14 \pmod{10} \end{cases} \text{ cioè } x \equiv 4 \pmod{10} \quad \text{cioè deve essere } x = 3 + 5k = 4 + 10h \quad \text{IMPOSSIBILE}$$

3.  $\begin{cases} x \equiv 3 \pmod{4} \\ 5x \equiv 4 \pmod{3} \\ 6x \equiv 1 \pmod{7} \end{cases}$

$$5 \equiv_3 2, \quad 4 \equiv_3 1 \quad \Rightarrow \begin{cases} x \equiv 3 \pmod{4} \\ 2x \equiv 1 \pmod{3} \\ x \equiv 6 \pmod{7} \end{cases}$$

poiché  $2 \cdot 2 \equiv_3 1$  diventa

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{3} \\ x \equiv 6 \pmod{7} \end{cases}$$

Svolgerlo!

4.  $\begin{cases} 2x \equiv 5 \pmod{3} \\ x \equiv 1 \pmod{9} \end{cases}$

il TCDR non si applica poiché  $\text{MCD}(3, 9) = 3 \neq 1$ .

$5 \equiv_3 2$ ; inoltre  $2 \cdot 2 \equiv_3 1$  quindi il sistema diventa

$$\begin{cases} 2 \cdot 2 x \equiv 2 \cdot 2 \pmod{3} \\ x \equiv 1 \pmod{9} \end{cases} \Rightarrow \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{9} \end{cases} \text{ cioè} \\ x = 1 + 3k = 1 + 9h \quad (k, h \in \mathbb{Z})$$

possibile per  $k=3h$ . Quindi le soluzioni ESISTONO e hanno la forma

$$x = 1 + 9h \quad h \in \mathbb{Z}.$$

In tutti i casi i sistemi sono stati semplificati usando, in ogni congruenza  $ax \equiv b \pmod{n}$ ,  $a' \equiv a \pmod{n}$  con  $0 \leq a' < a$ ,  $b' \equiv b \pmod{n}$  con  $0 \leq b' < b$  e moltiplicando, ove possibile, i due membri delle congruenze per il "reciproco" di  $a'$  cioè per  $a''$  t.c.  $a' \cdot a'' \equiv 1 \pmod{n}$ .