G. PARMEGGIANI 1/3/2019

ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)

Corso di Laurea: Informatica

CONGRUENZE

Def Sia $m \in \mathbb{N}, m > 0$. Una CONGRUENZA LINEARE MODULO m è un'espressione del tipo

$$(*) \qquad ax \equiv b \mod m$$

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

$x_0 \in \mathbb{Z}$ è UNA SOLUZIONE DI $(*)$ se

$$ax_0 \equiv b \mod m$$

ossia se $\exists k \in \mathbb{Z}$ tale che $ax_0 = b + mk$.

NB Non tutte le congruenze hanno soluzione (come tutte le equazioni lineari in $\mathbb{R}$ hanno soluzione).

ESEMPIO 1 $2x \equiv 3 \mod 4$ non ha soluzione: se esistesse $x_0 \in \mathbb{Z}$ soluzione di $2x \equiv 3 \mod 4$, esisterebbe $k \in \mathbb{Z}$ tale che

$$2x_0 = 3 + 4k$$

e se ne ricaverebbe $3 = 2x_0 - 4k = 2(x_0 - 2k)$.
Ma $2(x_0 - 2k)$ è un numero intero pari $\forall x_0, k \in \mathbb{Z}$, mentre 3 è dispari.

PROPOSIZIONE Sia $(*)$ $ax \equiv b \mod m$

con $m \in \mathbb{N}$, $m > 0$, $a, b \in \mathbb{Z}$.

Si supponga che $(*)$ abbia soluzioni, e sia x_0 una sua soluzione. Allora

SI PROVA CHE LE SOLUZIONI DI $(*)$ SONO TUTTI E SOLI i NUMERI INTERI IN

$$[x_0]_m = \{x_0 + tm \mid t \in \mathbb{Z}\}.$$

Dalla Proposizione segue che

LA CONGRUENZA (*) $ax \equiv b \bmod n$

CORRISPONDE AD UNA EQUAZIONE LINEARE IN $\mathbb{Z}_n$

$$(**) \qquad [a]_n x = [b]_n$$

NEL SENSO CHE

SE x_0 E' UNA SOLUZIONE DI (*), ALLORA $[x_0]_n$ E' UNA SOLUZIONE DI (**). E VICEVERSA

SE $[x_0]_n$ E' UNA SOLUZIONE DI (**), ALLORA

c E' UNA SOLUZIONE DI (*), $\forall c \in [x_0]_n$

(ossia $\forall k \in \mathbb{Z}$ si ha che $x_0 + kn$ è una soluzione di (*))

"Risolvere la congruenza" $ax \equiv b \bmod n$

significa:
- dire se ha soluzioni
- nel caso abbia soluzioni, trovarle tutte. Come numeri interi, esse sono infinite, dire in quante classi di congruenza modulo n questi numeri interi si ripartiscono.

$\boxed{\text{NB}}$ Non tutte le equazioni lineari in $\mathbb{Z}_n$ che hanno soluzione ne hanno una sola (mentre ogni equazione lineare in $\mathbb{R}$, oltre ad avere sempre una soluzione, ne ha esattamente una).

$\boxed{\text{ESEMPIO 2}}$ $2x \equiv 4 \bmod 6$

$a=2$
$b=4$
$n=6$

"pensata" come equazione lineare in $\mathbb{Z}_6$

$$[2]_6 x = [4]_6$$

ha due distinte soluzioni: $[2]_6$ e $[5]_6$

Infatti: $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ e

$[2]_6 \cdot [0]_6 = [0]_6 \neq [4]_6$

$[2]_6 \cdot [1]_6 = [2]_6 \neq [4]_6$

$[2]_6 \cdot [2]_6 = [4]_6 \Rightarrow [2]_6$ è una soluzione

$[2]_6 \cdot [3]_6 = [6]_6 = [0]_6 \neq [4]_6$

$[2]_6 \cdot [4]_6 = [8]_6 = [2]_6 \neq [4]_6$

$[2]_6 \cdot [5]_6 = [10]_6 = [4]_6 \Rightarrow [5]_6$ è una soluzione

Dunque ci sono infiniti numeri interi che sono soluzioni di $2x \equiv 4 \bmod 6$ ed essi si ripartiscono nelle due classi di congruenza modulo 6

$[2]_6 = \{2+6k \mid k \in \mathbb{Z}\}$ e $[5]_6 = \{5+6k \in \mathbb{Z}\}$.

(L'insieme di tutte le soluzioni in $\mathbb{Z}$ è

$$\{2+6k \mid k \in \mathbb{Z}\} \cup \{5+6k \mid k \in \mathbb{Z}\}.$$

TEOREMA 1 (ESISTENZA DI SOLUZIONI DI UNA CONGRUENZA)

Siano $n \in \mathbb{N}, n>0$, $a, b \in \mathbb{Z}$.
Sia $d = MCD(a,n)$. Allora

$$[ax \equiv b \bmod n \text{ HA SOLUZIONI}] \iff d \mid b$$

DIMOSTRAZIONE

"$\Rightarrow$" Si suppone che $ax \equiv b \bmod n$ abbia soluzioni e sia $x_0 \in \mathbb{Z}$ una sua soluzione.

Allora $\exists k \in \mathbb{Z}$ tale che $ax_0 = b + kn$, per cui
$$b = ax_0 - kn$$

$$d = MCD(a,n) \Rightarrow \begin{cases} d \mid a \Rightarrow d \mid (ax_0) \\ d \mid n \Rightarrow d \mid (-kn) \end{cases} \Rightarrow d \mid (ax_0) + (-kn) = b$$

Dunque $d \mid b$.

"$\Leftarrow$" Sapendo che $d = MCD(a,n)$ e $d \mid b$ vogliamo provare che esiste $x_0 \in \mathbb{Z}$ tale che $ax_0 \equiv b \bmod n$.

Essendo $d = MCD(a,n)$, dall'identità di Bezout segue che

$$\boxed{d = \alpha a + \beta n \quad \text{per opportuni } \alpha, \beta \in \mathbb{Z}.} \quad \star$$

Essendo $d \mid b$, si ha che $b = dq$ per un opportuno $q \in \mathbb{Z}$.

Moltiplico $\star$ per q:

$$q \cdot d = q(\alpha a + \beta n)$$

da cui $\underbrace{\boxed{qd}}_{b} = q\alpha a + q\beta n \rightarrow$ multiplo di n

Quindi $q\alpha = x_0$ tale che $a \cdot x_0 \equiv b \bmod n$

(posto $x_0 = q\alpha$, $k = -q\beta$ si ha che $b = ax_0 + kn$)

TEOREMA 2 Si suppone che $ax \equiv b \bmod n$ abbia soluzioni.

Sia $d = MCD(a,n)$ (dunque si suppone $d \mid b$).
e sia x_0 una soluzione.

Allora le soluzioni di $ax \equiv b \bmod n$ sono tutti e soli i numeri interi del tipo

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

Ci sono infiniti numeri interi soluzioni di $ax \equiv b \bmod n$ e si ripartiscono in esattamente d classi di congruenza modulo n:

$$[x_0]_n = \{x_0 + tn \mid t \in \mathbb{Z}\}$$
$$[x_1]_n = \{x_1 + tn \mid t \in \mathbb{Z}\}$$
$$[x_2]_n = \{x_2 + tn \mid t \in \mathbb{Z}\}$$
$$\vdots$$
$$[x_{d-1}]_n = \{x_{d-1} + tn \mid t \in \mathbb{Z}\}$$

N.B.: $[x_d]_n = [x_0 + n]_n = [x_0]_n$

$$\boxed{x_d = x_0 + \cancel{d} \cdot \frac{n}{\cancel{d}} = x_0 + n}$$

ESERCIZI Si risolvano le seguenti congruenze

$\boxed{1}$ $2x \equiv 5 \bmod 8$

a b n

$\boxed{a = 2 \\ n = 8}$

$\boxed{\text{I}}$ Calcolo $d = MCD(a,n) = MCD(2,8) = 2$

$\boxed{\text{II}}$ Siccome $d = 2 \nmid 5 = b$ allora la congruenza NON HA SOLUZIONI

$\boxed{2}$ $3x \equiv 4 \bmod 7$

$\boxed{2}$ $3x \equiv 4 \mod 7$

a, b, n

$\boxed{I}$ Calcolo $d = MCD(a,n) = MCD(3,7) = 1$

$\boxed{\begin{array}{l} a=3 \\ n=7 \end{array}}$

$\boxed{II}$ Siccome $d = 1 \mid 4 = b$, la congruenza ha infinite soluzioni intere che si ripartiscono in $d = 1$ classe di congruenze modulo $n = 7$.

$\boxed{III}$ Cerco x_0 una soluzione di $3x \equiv 4 \mod 7$

a, b, n

$d = MCD(a,n) \Rightarrow \exists \alpha, \beta \in \mathbb{Z} \mid d = \alpha a + \beta n$ in questo caso:

$1 = MCD(3,7) \Rightarrow \exists \alpha, \beta \in \mathbb{Z} \mid 1 = \alpha \cdot 3 + \beta \cdot 7$

Dall'algoritmo di Euclide: $7 = 3 \cdot 2 + 1$

$\Rightarrow 1 = 7 - 3 \cdot 2$
$= 7 \cdot 1 + 3 \cdot (-2)$

β, α

moltiplico $\boxed{1 = 7 \cdot 1 + 3 \cdot (-2)}$

per q tale che $b = q \cdot d$

$\left.\begin{array}{l} b = 4 \\ d = 1 \end{array}\right\} \Rightarrow q = b = 4$

quindi moltiplico $\boxed{1 = 7 \cdot 1 + 3(-2)}$ per 4:

$4 = 7 \cdot 4 + 3 \cdot \boxed{(-2) \cdot 4}$

b, n, a

cerco x_0 tale che $b = n \cdot k + a \cdot \boxed{x_0}$

Quindi $x_0 = (-2) \cdot 4 = -8$.

[IV] La ha come soluzioni tutti e soli i numeri interi in

$$[x_0]_7 = [-8]_7 = [6]_7 = \{6 + 7k \mid k \in \mathbb{Z}\}$$

Scelgo un rappresentante positivo della classe di congruenza $[-8]_7$: prendo $c \in [-8]_7$ con

$0 \le c < 7$

per cui $c = -8 + 2 \cdot 7 = -8 + 14 = 6$

---

3 $2x \equiv 10 \mod 12$

a b n

[I] Calcolo $d = MCD(a, n) = MCD(2, 12) = 2$

[II] Siccome $d = 2 \mid 10 = b$, la congruenza ha infinite soluzioni intere che si ripartiscono in $d = 2$ classi di congruenza modulo $n = 12$

[III] Cerco una soluzione x_0 di $2x \equiv 10 \mod 12$

Quando l'avrò trovata otterrò da x_0

$x_1, x_2, \dots, x_{d-1}$ (IN QUESTO CASO, ESSENDO $d = 2$ E QUINDI $d-1 = 1$, OTTERRÒ SOLO x_1)

con $x_k = x_0 + k \cdot \frac{n}{d}$, $k = 1, \dots, d-1$

(IN QUESTO CASO

$$x_1 = x_0 + 1 \cdot \frac{n}{d} \underset{\substack{n=12 \\ d=2}}{=} x_0 + \frac{12}{2} = x_0 + 6)$$

e concluderò che le soluzioni sono esattamente gli interi che si ripartiscono nelle classi $[x_0]_{12}$ e $[x_1]_{12}$

$d = MCD(a,m) \Rightarrow \exists\, \alpha, \beta \in \mathbb{Z} \mid d = \alpha a + \beta m$

$$\left.\begin{matrix} a=2 \\ m=12 \end{matrix}\right\} \Rightarrow d = MCD(2,12) = 2$$

$$\underset{d}{2} = \underset{m}{12} \cdot 0 + \underset{a}{2}$$

$\Rightarrow \alpha = 1$ e $\beta = 0$

$d \mid b \Rightarrow \exists\, q \mid b = qd$

$$\left.\begin{matrix} b=10 \\ d=2 \end{matrix}\right\} \Rightarrow q = 5 \Rightarrow \text{moltiplico } \boxed{2 = 12 \cdot 0 + 2} \text{ per } 5:$$

$$\underbrace{2 \cdot 5}_{10=b} = \underset{m}{12} \cdot 0 \cdot 5 + \underset{a}{2} \cdot \boxed{5}$$

Cerco x_0 tale che $\quad b = m \cdot k + a \cdot \boxed{x_0}$

Dunque $\quad x_0 = 5$

$$x_1 = 5 + \frac{m}{d} = 5 + \frac{12}{2} = 5 + 6 = 11$$

e le soluzioni della congruenza si ripartiscono nelle due seguenti classi di congruenza modulo 12:

$[x_0]_{12} = [5]_{12} = \{5 + 12k \mid k \in \mathbb{Z}\}$ e

$[x_1]_{12} = [11]_{12} = \{11 + 12k \mid k \in \mathbb{Z}\}$.

(L'insieme di tutte le soluzioni è:

$\{5 + 12k \mid k \in \mathbb{Z}\} \cup \{11 + 12k \mid k \in \mathbb{Z}\}$).

PER CASA: ESERCIZIO 7 (file: I19casaT1.pdf)

INVERTIBILI IN $\mathbb{Z}_n$ E LORO CALCOLO

DEF $n \in \mathbb{N}, n > 0, a \in \mathbb{Z}$ si dice INVERTIBILE MODULO n se la congruenza $ax \equiv 1 \bmod n$ ha soluzione

(quindi $\iff d = MCD(a,n) \mid 1 \iff d = MCD(a,n) = 1$
Si dice che a ed n sono COPRIMI)

ANALOGAMENTE

DEF $n \in \mathbb{N}, n > 0$

$[a]_n \in \mathbb{Z}_n$ si dice INVERTIBILE IN $\mathbb{Z}_n$ se

$\exists [b]_n \in \mathbb{Z}_n$ tale che $[a]_n [b]_n = [1]_n$.

In questo caso $[b]_n$ si dice un inverso di $[a]_n$, ed essendo $[b]_n$ unico (perchè $d = 1$), $[b]_n$ è L'INVERSO di $[a]_n$ e si indica $[b]_n = [a]_n^{-1}$

ESEMPIO ① 6 non è invertibile modulo 9:
$6x \equiv 1 \bmod 9$ non ha soluzione perchè $MCD(6,9) = 3 \neq 1$
(6 e 9 non sono coprimi)

② 4 è invertibile modulo 9 perchè 4 e 9 sono coprimi (ossia $MCD(4,9) = 1$ per cui la congruenza $4x \equiv 1 \bmod 9$ ha soluzione)

Chi è $[4]_9^{-1}$?

Cerco x_0 soluzione di $4x \equiv 1 \mod 9$ e avrò $[4]_9^{-1} = [x_0]_9$

$1 = d = MCD(4,9) \Rightarrow \exists\, \alpha, \beta \in \mathbb{Z} \mid 4\alpha + 9\beta = 1$

$9 = 4 \cdot 2 + 1 \Rightarrow 1 = \underbrace{9}_{\beta = 1} + 4 \boxed{\underbrace{(-2)}_{\alpha}}$

Cerco x_0 tale che $1 = 4\boxed{x_0} + 9k$ con $k \in \mathbb{Z}$

$\Rightarrow x_0 = -2$ e $[4]_9^{-1} = [-2]_9 = [-2+9]_9 = [7]_9$

PER CASA: ESERCIZIO 8 (file: I19CasaT1.pdf)

$\mathbb{Z}_p$ (CON p UN NUMERO PRIMO)

Siano p un numero primo positivo ed $[a]_p \in \mathbb{Z}_p$.

Posso supporre $0 \leq a < p$.

SE $a = 0$ ALLORA $[a]_p = [0]_p$

SE $a \neq 0$ ALLORA (essendo p un primo) $MCD(a,p) = 1$

E QUINDI a E' INVERTIBILE MODULO p

IN $\mathbb{Z}_p$ TUTTI GLI ELEMENTI $\neq [0]_p$ SONO INVERTIBILI (equivalentemente, se p è un numero primo ed $a \in \mathbb{Z}$, allora

o $p \mid a$

oppure a è invertibile modulo p.

Quindi il numero degli invertibili in $\mathbb{Z}_p$ è $p-1$.

QUANTI SONO GLI ELEMENTI INVERTIBILI IN $\mathbb{Z}_n$?

Tanti quanti sono i numeri a con $\begin{cases} 0 \le a < n \\ MCD(a,n) = 1 \end{cases}$

ad esempio

se $n = 10$

0
$\boxed{1}$
2
$\boxed{3}$
4
5
6
$\boxed{7}$
8
$\boxed{9}$

COPRIMI CON 10 E QUINDI INVERTIBILI MODULO 10