CONGRUENZE

Note Title 10/18/2017

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

Si dice che a è congruo a b modulo m, e si scrive $a \equiv b \bmod m$, se $m \mid a-b$

$$a \equiv b \pmod m \qquad c \equiv d \pmod m$$

$$\Rightarrow \quad a+c \equiv b+d \pmod m$$
$$ac \equiv bd \pmod m$$

① Risolvere le congruenze

$$7X \equiv 6 \pmod{21}$$

$$\iff \quad 21 \mid (7X-6)$$

$$\iff \begin{cases} 3 \mid (7X-6) \\ 7 \mid (7X-6) \end{cases} \qquad \begin{cases} 7X \equiv 6 \ (3) \\ 7X \equiv 6 \ (7) \end{cases}$$

$$\iff \begin{cases} 3 \mid 7X \\ 7 \mid 6 \end{cases} \quad \not\Rightarrow \quad 7X - (7X-6)$$

IMPOSSIBILE,

non ci sono soluzioni

$$3X \equiv 6 \pmod{21}$$

$$\iff 21 \mid 3X - 6$$

$$\iff \begin{cases} 3 \mid 3X-6 \\ 7 \mid 3X-6 \end{cases} \quad \text{AUTOMATICO} \quad \begin{cases} 3X \equiv 6 \pmod 3 \\ 3X \equiv 6 \pmod 7 \end{cases}$$

$$\iff 3X \equiv 6 \mod 7$$

$$\overset{?}{\iff} X \equiv 2 \mod 7$$

$$3X \equiv 6 \mod 7 \iff 7 \mid 3X - 6$$

$$\iff 7 \mid 3(X-2)$$

$$\iff 7 \mid X-2$$

$$\iff X \equiv 2 \mod 7$$

$$2X \equiv 8 \pmod{14} \overset{?}{\iff} X \equiv 4 \mod 14$$

NO

ad esempio

$X = 11$ rispetta $2X \equiv 8 \ (14)$

ma non $X \equiv 4 \mod (14)$

$$\Updownarrow$$

$$14 \mid 2X - 8$$

$\Leftrightarrow \quad 2 \cdot 7 \mid 2 \cdot (x-4)$

$\Leftrightarrow \quad \begin{cases} 2 \mid 2(x-4) \\ 7 \mid 2(x-4) \end{cases}$ AUTOMATICA

$\Leftrightarrow \quad x \equiv 4 \mod 7$

In altre parole, anche il modulo risulta diviso per due

$5x \equiv 3 \pmod{48}$

$\Leftrightarrow \quad 48 \mid 5x - 3$

$\Leftrightarrow \quad \exists y \text{ t.c. } 5x - 3 = 48y$

$\Leftrightarrow \quad \exists y \text{ t.c. } 5x - 48y = 3$

Risolubile $\Leftrightarrow \quad (48, 5) \mid 3$

$48 = 9 \cdot 5 + 3$

$5 = 3 + 2$

$3 = 2 + 1$

$1 = 3 - 2 = 3 - (5-3) = 2 \cdot 3 - 5$

$= 2 \cdot (48 - 9 \cdot 5) - 5$

$$= 2 \cdot 48 - 19 \cdot 5$$

$$\Rightarrow \quad 3 = 6 \cdot 48 - 57 \cdot 5$$

Una soluzione dell'eqz iniziale è $x = -57$

E' vero che $5x \equiv 3 \ (48)$?

$$\Leftrightarrow \quad -285 \equiv 3 \ (48)$$

$$\Leftrightarrow \quad -288 \equiv 0 \ (48)$$

$$\| \quad -6 \cdot 48$$

La soluz. generale è $x = -57 + 48k$

$y = 6 + 5k$

Ovvero $x \equiv -57 \pmod{48}$

$\equiv -9 \pmod{48}$

Modo migliore di pensare questa soluzione

$$1 = 2 \cdot 48 - 19 \cdot 5$$

$$1 \equiv 0 + (-19) \cdot 5 \pmod{48}$$

$5x \equiv 3 \pmod{48} \xrightarrow{\times(-19)} -5 \cdot 19 x \equiv -57 \ (48)$

$x \equiv -57 \ (48)$

Si scrive anche $5^{-1} \equiv (-19) \mod 48$

Teorema Siano $a \in \mathbb{Z}$, $m \in \mathbb{Z}_{>0}$. Se $(a, m) = 1$, allora $\exists b \in \mathbb{Z}$ t.c. $ab \equiv 1 \mod m$. b è detto l'INVERSO di a modulo m.

TEOREMA CINESE DEL RESTO

$$\begin{cases} X \equiv 132 \mod 125 = 5^3 \\ X \equiv 3 \mod 100 = 2^2 \cdot 5^2 \end{cases}$$

$\Downarrow$

$$\begin{cases} X \equiv 7 \mod 5^3 \\ X \equiv 3 \mod 4 \\ X \equiv 3 \mod 5^2 \end{cases}$$

$\Downarrow$ CR

$$\begin{cases} X \equiv 3 \mod 4 \\ X \equiv 3 \mod 25 \end{cases}$$

$\Downarrow$

$$\begin{cases} X \equiv 7 \equiv 2 \mod 5 \\ X \equiv 3 \mod 5 \end{cases}$$

IMPOSSIBILE

$$\begin{cases} X \equiv 132 \mod 125 \\ X \equiv 107 \mod 100 \end{cases}$$

TCR $(\Longleftarrow)$

$$\begin{cases} X \equiv 7 \mod 125 \\ X \equiv 107 \equiv 3 \mod 4 \\ X \equiv 107 \equiv 7 \mod 25 \end{cases}$$

$(\Longleftarrow)$

$$\begin{cases} X \equiv 7 \mod 125 = 5^3 \\ X \equiv 7 \mod 4 \end{cases}$$

$(\Longleftarrow)$ TCR $X \equiv 7 \mod 500$

① esiste un'unica soluzione (mod 125×4)

② 7 è una soluzione

$X \equiv 7 \mod 5$

2, 7, 12, 17 ...

$X \equiv 7 \mod 125$

7, 132, 257, ...

$$\begin{cases} X \equiv 2 \mod 13 \\ X \equiv 4 \mod 5 \end{cases}$$

$$\begin{cases} X \equiv 1 \mod 13 \\ X \equiv 0 \mod 5 \end{cases} \qquad \begin{cases} X \equiv 0 \mod 13 \\ X \equiv 1 \mod 5 \end{cases}$$

"vogliamo un X multiplo di 5 che sia anche $\equiv 1 \mod 13$, ovvero vogliamo y ($x = 5y$) tale che $5y \equiv 1 \mod 13$"

$$5y \equiv 1 \ (13) \xrightarrow{\cdot 5} 25y \equiv 5 \mod 13$$

$$\longrightarrow (-1)y \equiv 5 \mod 13$$

$$\xrightarrow{\cdot(-1)} y \equiv 8 \equiv -5 \mod 13$$

Unicità nel TCR

CONCLUSIONE la soluzione di $\begin{cases} X \equiv 1 \ (13) \\ X \equiv 0 \ (5) \end{cases}$ è $X \equiv 40 \pmod{65}$

Altro sistema: $\begin{cases} X \equiv 0 \mod 13 \\ X \equiv 1 \mod 5 \end{cases}$

$\Longleftrightarrow X \equiv 26 \mod 65$

$$\begin{cases} X \equiv 2 \mod 13 \\ X \equiv 4 \mod 5 \end{cases}$$

$$2 \cdot 40 \equiv \begin{matrix} 2 \mod 13 \\ 0 \mod 5 \end{matrix}$$

$$4 \cdot 26 \equiv \begin{matrix} 0 \mod 13 \\ 4 \mod 5 \end{matrix}$$

Soluzione: $X \equiv 2 \cdot 40 + 4 \cdot 26 \mod 65$

In generale: dati a, b interi coprimi,

siano X_a una soluz. di $\begin{cases} X \equiv 1 \mod a \\ X \equiv 0 \mod b \end{cases}$

e X_b ——— $\begin{cases} X \equiv 0 \mod a \\ X \equiv 1 \mod b \end{cases}$

Allora la soluzione di $\begin{cases} X \equiv m \mod a \\ X \equiv n \mod b \end{cases}$

è $X \equiv m \cdot X_a + n \cdot X_b \pmod{ab}$

Infatti modulo a abbiamo

$$X \equiv m \cdot X_a + n \cdot X_b \equiv m \cdot 1 + n \cdot 0 \equiv m \pmod a$$

CONGRUENZE QUADRATICHE

Risolvere $(x+1)(x+2) \equiv 0 \pmod{24}$

$\iff 24 \mid (x+1)(x+2)$

$\iff \begin{cases} 3 \mid (x+1)(x+2) \\ 8 \mid (x+1)(x+2) \end{cases}$

$\iff \begin{cases} 3 \mid x+1 \text{ oppure } 3 \mid x+2 \quad (3 \text{ primo}) \\ 8 \mid x+1 \text{ oppure } 8 \mid x+2 \quad (x+1 \text{ o } x+2 \text{ disp}) \end{cases}$

$\iff \begin{cases} x \equiv -1 \pmod 3 \text{ o } x \equiv -2 \pmod 3 \\ x \equiv -1 \pmod 8 \text{ o } x \equiv -2 \pmod 8 \end{cases}$

$\iff \begin{cases} x \equiv -1 \ (3) \\ x \equiv -1 \ (8) \end{cases} \vee \begin{cases} x \equiv -1 \ (3) \\ x \equiv -2 \ (8) \end{cases} \vee \begin{cases} x \equiv -2 \overset{\equiv 1}{} \ (3) \\ x \equiv -1 \ (8) \end{cases}$

$\vee \begin{cases} x \equiv -2 \ (3) \\ x \equiv -2 \ (8) \end{cases}$

$\begin{cases} x \equiv 2 \ (3) \\ x \equiv 7 \ (8) \end{cases}$

$\iff x \equiv -1 \ (24) \vee x \equiv 14 \ (24) \vee x \equiv 7 \ (24) \vee x \equiv -2 \ (24)$

$(x+1)(x+2) \equiv 0 \ (24)$

(Scritto del 28/06/2006)

Determinare in funzione di $a \in \mathbb{Z}$ le soluz. di

$$\begin{cases} (6a-1)x \equiv 1 \mod 21 \\ x \equiv a \mod 35 \end{cases}$$

TCR $\Leftrightarrow$

$$\begin{cases} (6a-1)x \equiv 1 \mod 3 \\ (6a-1)x \equiv 1 \mod 7 \\ x \equiv a \mod 7 \\ x \equiv a \mod 5 \end{cases}$$

$6a \equiv 0 \ (3)$

$6a-1 \equiv -1 \ (3)$

$(6a-1)x \equiv -x \ (3)$

$\Leftrightarrow$

$$\begin{cases} -x \equiv 1 \ (3) \\ (-a-1)x \equiv 1 \ (7) \\ x \equiv a \ (7) \\ x \equiv a \ (5) \end{cases}$$

Guardiamo 2^a e 3^a eqz e cerchiamo di capire se sono compatibili

$a \bmod 7$	0	1	2	3	4	5	6
	NO	NO	SI	NO	SI	NO	NO

└ la 2^a eq diventa $0 \cdot x \equiv 1 \ (7)$

$$\begin{cases} -2 \cdot x \equiv 1 \ (7) \\ x \equiv 1 \ (7) \end{cases} \qquad \begin{cases} -2 \equiv 1 \ (7) \\ x \equiv 1 \ (7) \end{cases} \text{ NO}$$

$\boxed{a \equiv 2 \ (7)}$

$$\begin{cases} -3x \equiv 1 \ (7) \\ x \equiv 2 \ (7) \end{cases}$$

$\boxed{a \equiv 4 \ (7)}$

$$\begin{cases} -5x \equiv 1 \ (7) \\ x \equiv 4 \ (7) \end{cases}$$

CONCLUSIONE (FINORA) Se a non è congruo a 2 o a 4 modulo 7 non ci sono soluzioni. Se invece $a \equiv 2$ o $4 \pmod 7$, allora le soluz. ci sono, il sistema è equivalente a

$$\begin{cases} X \equiv 2 & (3) \\ X \equiv a & (5) \\ X \equiv a & (7) \end{cases}$$

$$\iff \begin{cases} X \equiv 2 & \text{mod } 3 \\ X \equiv a & \text{mod } 35 \end{cases} \quad (*)$$

$$\begin{cases} X \equiv 1 & \text{mod } 3 \\ X \equiv 0 & \text{mod } 35 \end{cases} \qquad \begin{cases} X \equiv 0 & \text{mod } 3 \\ X \equiv 1 & \text{mod } 35 \end{cases}$$

$$X \equiv 70 \text{ mod } 105 \qquad X \equiv 36 \text{ mod } 105$$

$(*)$ ha soluzione

$$x \equiv 2 \cdot 70 + 36 \cdot a \text{ mod } 105$$

$$\equiv 35 + 36 \cdot a \text{ mod } 105$$

CONCLUSIONE DEFINITIVA:

- per $a \equiv 0, 1, 3, 5, 6 \pmod 7$ non ci sono soluzioni;

- per $a \equiv 2, 4 \mod 7$ ci sono infinite soluzioni, date da

$$X \equiv 35 + 36a \mod 105$$

Oss $X \equiv 35 + 36a \pmod{105}$ è sempre la soluzione di (*): il problema è che questo sistema non è sempre equivalente al sistema di partenza