ALGO

WWW.ALGORITMOSTEM.IT

SCIENCE TECHNOLOGY ENGINEERING MATHEMATICS

Appunti di Algebra1: Congruenze

UNI - Matematica

rev.0.1 - 05 set 2023

Draft version

Appunti in formato bozza, intesi esclusivamente di ausilio alle lezioni, che le integrano nelle descrizioni e nei ragionamenti su quanto viene riportato in queste pagine.

- definizioni e proprietà
- eq. congruenziali

CONGRUENZE

1) congruenze ed aritmetica modulare
2) criteri di divisibilità

Divisione euclidea (quoziente, resto)

dati $a, b \in \mathbb{Z}, b \neq 0 \Rightarrow \exists! q, r \in \mathbb{N} \mid a = bq + r$ con $0 \leq r \leq |b|$

Es $a = 12 \quad b = 5 \Rightarrow 12 = 4 \cdot 2 + 3$

congruenze

Def 1 dati $a, b, m \in \mathbb{Z}$ con $m > 0$, si dice che a e b sono congrui modulo m se danno lo stesso resto quando vengono divisi per m $\quad a \equiv b \pmod{m}$

Def 2 $(a-b)$ multiplo di $m \Rightarrow a \equiv b \pmod{m}$

Es $57 = 2 \pmod 5 \qquad -6 = 2 \pmod 4$

Proprietà

1) La congruenza è una relazione di equivalenza
   - riflessiva $\forall a \in \mathbb{Z} : a \equiv a \pmod m$
   - simmetrica $\forall a,b \in \mathbb{Z} : a \equiv b \pmod m \to b \equiv a \pmod m$
   - transitiva $\forall a,b,c \in \mathbb{Z} : a \equiv b \pmod m,\ b \equiv c \pmod m \to a \equiv c \pmod m$

   * m classi di equivalenza $[0], [1], \dots [m-1]$

   Es mod 3 ho tre classi di equivalenza

$$[0] = \{0, 3, -3, 6, -6, \dots\}$$
$$[1] = \{1, 4, -2, 7, -5, \dots\}$$
$$[2] = \{2, 5, -1, 8, -4, \dots\}$$

2) Se m divide $a \iff a \equiv 0 \pmod m$

3) Se m è numero primo (legge annullamento del prodotto)
   $a \cdot b \equiv 0 \pmod m \iff a \equiv 0 \pmod m$ oppure $b \equiv 0 \pmod m$
   Un numero primo divide un prodotto $a \cdot b$ sse divide almeno uno dei suoi fattori.

4) se $a \equiv c \pmod m$, $b \equiv d \pmod m$ $\Rightarrow a \pm b \pmod m \equiv c \pm d \pmod m$

5) se $a \equiv b \pmod m \Rightarrow$ $a^n \equiv b^n \pmod m$ anche viceversa se $n \neq 0$ con $n \in \mathbb{Z}$
   $na \equiv nb \pmod m$ anche viceversa se $MCD(n,m) = 1$

6) se $ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod{\frac{m}{MCD(c,m)}}$

Esempio

trovare il resto della divisione tra 2021^{2020} e 3

$2021 = 3 \cdot 674 - 1 \longrightarrow 2021 \equiv -1 \pmod 3$

proprietà 5 $\longrightarrow$ $2021^{2020} \equiv -1^{2020} \pmod 3$

$2021^{2020} \equiv 1 \pmod 3$

resto = 1

Alternativa: $2021 = 3 \cdot 673 + 2 \longrightarrow 2021 \equiv 2 \pmod 3$

proprietà 5 $\longrightarrow$ $2021^{2020} \equiv 2^{2020} \pmod 3$

... calcoli più complessi

ESERCIZIO

Ricavare il criterio di divisibilità per 11

notaz. base 10 $a = a_n 10^n + a_{n-1} 10^{n-1} + \dots a_1 10 + a_0 \quad n \geq 0$

es $314 = 3 \cdot 10^2 + 1 \cdot 10 + 4$

poiché $10 \equiv -1 \pmod{11}$, si ottiene

$$a \equiv \left[(-1)^n \cdot a_n + (-1)^{n-1} a_{n-1} + \dots (-1) a_1 + a_0\right] \pmod{11}$$

le cifre di indice pari avranno segno positivo
le cifre di indice dispari avranno segno negativo

Supponiamo n pari:

$11 \mid a \iff a \equiv 0 \pmod{11}$

11 divide a

$\iff (a_0 + a_2 + \dots a_n) - (a_1 + a_3 + \dots a_{n-1}) \equiv 0 \pmod{11}$

ESERCIZIO

Ricavare la cifra delle unità di 12567^{9506}

12567^{9506} corrisponde alle cifra delle unità del numero 7^{9506}

equivale a cercare il resto della divisione euclidea del numero per 10 o, in altri termini cercare la congruenza del numero modulo 10

cifra unità

$7^0 \to 1$ $\quad 7^4 \to 1$ $\quad 7^8 \to 1$ $\quad 7^{4k} \to 1$

$7^1 \to 7$ $\quad 7^5 \to 7$ $\quad \dots$ $\quad 7^{4k+1} \to 7$

$7^2 \to 9$ $\quad 7^6 \to 9$ $\quad 7^{4k+2} \to 9$

$7^3 \to 3$ $\quad 7^7 \to 3$ $\quad 7^{4k+3} \to 3$

$4k+3 \equiv 3 \pmod 4$

quindi per risolvere l'esempio basterà capire a cosa è congruo 9506 (esponente) mod 4.

poiché $9506 \equiv 2 \pmod 4$, la cifra delle unità di 12567^{9506} è 9

ESERCIZIO

calcolare $16 + 39 \cdot 25 \pmod{12}$

$16 \equiv 4 \pmod{12}$

$39 \equiv 3 \pmod{12}$

$25 \equiv 1 \pmod{12}$

$16 + 39 \cdot 25 \pmod{12} \equiv (4 + 3 \cdot 1) \pmod{12}$

$\equiv 7 \pmod{12}$

CONGRUENZE LINEARI

$$ax \equiv b \pmod n$$

equivale a: la differenza tra ax e b è multiplo di n

$$ax \equiv b \pmod n \iff ax - b = ny \quad \text{per } y \in \mathbb{Z}$$

$$ax - ny = b$$

quindi risolvere $ax \equiv b \pmod n$

equivale a risolvere $ax - ny = b$ **eq. diofantea**

o a risolvere $ax + ny = b$ perché $y \in \mathbb{Z}$ e arbitrario

$ax \equiv b \pmod n$ ha soluzione $\iff MCD(a,n)$ divide b

$$x = x_0 + \frac{n}{MCD(a,n)} \cdot t \qquad \text{al variare di } t \in \mathbb{Z}$$

x_0 → sol. particolare (id Bezout)

se $b = 0 \Rightarrow x_0 = 0$

Altre strategie per risolvere $ax \equiv b \pmod n$

* provo a sostituire le classi resto modulo n ($[0], [1], \dots [n-2] [n-1]$) fino a trovare quella giusta

** Uso l'inverso modulare, ovvero riduco il coeff. di x ad 1 moltiplicando per l'inverso di $a \pmod n$ e, di seguito, applico la funzione ϕ di eulero

ESEMPIO Risolvere $5x \equiv 4 \pmod{14}$

1) Verifichiamo se esiste soluzione:

$MCD(5,14) = 1$ divide $4 \Leftrightarrow \exists$ soluzione

2) Risolviamo l'ep. diofantea $5x + 14y = 4$

2.1) Risolviamo l'id Bezout: cerchiamo le sol. particolare

$\tilde{x}$ e $\tilde{y}$ / $5\tilde{x} + 14\tilde{y} = 1$ ← $MCD(5,14) = 1$

$14 = 5 \cdot 2 + 4 \longrightarrow 4 = 14 - 5 \cdot 2$

$5 = 4 \cdot 1 + 1 \longrightarrow 1 = 5 - 4 = 5 - (14 - 5 \cdot 2) = 5 \cdot 3 - 1 \cdot 14$

$4 = 4 \cdot 1 + 0 \longrightarrow \tilde{x} = 3, \ \tilde{y} = -1 \rightarrow x_0 = 4\tilde{x} = 12$

$\longrightarrow x = 12 + 14t, \ t \in \mathbb{Z}$

$x \equiv 12 \pmod{14}$

Altro modo **

$3 \cdot 5x \equiv 3 \cdot 4 \pmod{14}$

$x \equiv 12 \bmod 14$

moltiplichiamo per l'inverso di $5 \pmod{14} = 3$

$5 \cdot y - 1 = 14 \Rightarrow y = 3$

Teorema cinese del resto

fornisce una condizione sufficiente affinché un sistema lineare di congruenze ammetta soluzione

dato il sistema con $a_i \in \mathbb{Z}$

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \dots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

se n_i sono coprimi a coppie ↳ MCD = 1 $\Rightarrow$ ∃ soluzioni se ∀ eq. è risolubile

per determinare le soluzioni si procede come segue:

Algoritmo per trovare le soluzioni

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ x \equiv a_3 \pmod{n_3} \end{cases}$$

0) Controllo che gli n_i siano a due a due coprimi.

1) Calcolo: $N = n_1 \cdot n_2 \cdot n_3$

$N_1 = n_2 \cdot n_3$

$N_2 = n_1 \cdot n_3$

$N_3 = n_1 \cdot n_2$

2) Risolvo le congruenze:

$N_1 y_1 \equiv 1 \pmod{n_1}$

$N_2 y_2 \equiv 1 \pmod{n_2}$

$N_3 y_3 \equiv 1 \pmod{n_3}$

3) La soluzione del sistema è:

$$x \equiv a_1 N_1 y_1 + a_2 N_2 y_2 + a_3 N_3 y_3 \pmod{N}.$$

Esempio

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

0) 5, 6 e 7 sono a due a due coprimi.

1) $N = 5 \cdot 6 \cdot 7 = 210$

$N_1 = 6 \cdot 7 = 42$

$N_2 = 5 \cdot 7 = 35$

$N_3 = 5 \cdot 6 = 30$

2) Risolvo le congruenze:

$42 y_1 \equiv 1 \pmod 5 \longrightarrow 2 y_1 \equiv 1 \pmod 5 \rightarrow y_1 \equiv 3 \pmod 5$

$35 y_2 \equiv 1 \pmod 6 \longrightarrow -y_2 \equiv 1 \pmod 6 \rightarrow y_2 \equiv -1 \pmod 6$

$30 y_3 \equiv 1 \pmod 7 \longrightarrow 2 y_3 \equiv 1 \pmod 7 \rightarrow y_3 \equiv 4 \pmod 7$

3) La soluzione del sistema è:

$x \equiv (2 \cdot 42 \cdot 3) + (3 \cdot 35 \cdot (-1)) + (1 \cdot 30 \cdot 4) \pmod{210} \longrightarrow x \equiv 57 \pmod{210}.$

ESERCIZIO

2. Per quanti interi n, $1 \le n \le 143$ il numero $n^2 - 5n + 6$ è un multiplo di 143?

SOLUZIONE

Scompongo: $n^2 - 5n + 6 = (n-2)(n-3)$ e $143 = 11 \cdot 13$.

Quattri casi possibili:

a) $n-2$ è multiplo di 143; $\longrightarrow$ $n-2 = 0 \rightarrow n = 2$ (perché $1 \le n \le 143$)

b) $n-3$ è multiplo di 143; $\longrightarrow$ $n-3 = 0 \rightarrow n = 3$ // //

c) $n-2$ è multiplo di 11 e $n-3$ è multiplo di 13;

d) $n-2$ è multiplo di 13 e $n-3$ è multiplo di 11.

Il caso c) equivale a:

$$\begin{cases} n \equiv 2 \pmod{11} \\ n \equiv 3 \pmod{13} \end{cases} \longrightarrow \text{1 soluzione modulo 143 } (n = 68)$$

Il caso d) equivale a:

$$\begin{cases} n \equiv 3 \pmod{11} \\ n \equiv 2 \pmod{13} \end{cases} \longrightarrow \text{1 soluzione modulo 143 } (n = 80)$$

In totale, 4 interi.

con algoritmo cinese

con algoritmo cinese

SCHEMA × ESERCIZI (ep. congruenziali)

1) se $a \equiv c \pmod m$, $b \equiv d \pmod m$ $\Rightarrow a \pm b \pmod m \equiv c \pm d \pmod m$

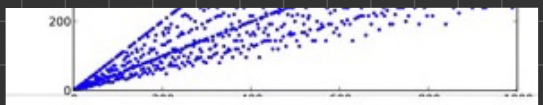
2) se $a \equiv b \pmod m \Rightarrow$ $a^n \equiv b^n \pmod m$ anche viceversa se $n \neq 0$ con $n \in \mathbb{Z}$
$na \equiv nb \pmod m$ anche viceversa se $MCD(n,m)=1$

3) se $ac = bc \pmod m \Rightarrow a \equiv b \pmod{\frac{m}{MCD(c,m)}}$

---

1) Piccolo Teorema di Fermat: p num. primo $\rightarrow a^p \equiv a \pmod p$

2) Teorema Eulero-Fermat:
a, b coprimi* $\rightarrow a^{\varphi(b)} \equiv 1 \pmod b$
con $\varphi(b)$ funzione di Eulero, $b \in \mathbb{N}$
(*) coprimi se $MCD=1$



In matematica, la **funzione φ di Eulero** o semplicemente **funzione di Eulero** o **toziente**, è una funzione definita, per ogni intero positivo n, come il numero degli interi compresi tra 1 e n che sono coprimi con n. Ad esempio, $\varphi(8) = 4$ poiché i numeri coprimi di 8 sono quattro: 1, 3, 5, 7.

---

3) Risolvere $ax \equiv b \pmod m$
- riduzione a forma normale
- controllare se $\exists$ soluzione ($MCD(a,m)$ divide b)
- moltiplicare per l'inverso di $a \pmod m$

4) Risolvere sistema
$$\begin{cases} ax \equiv b \pmod m \\ a'x \equiv b' \pmod{m'} \\ \vdots \\ a''x \equiv b'' \pmod{m''} \end{cases}$$
- verificare compatibilità ($\exists$ soluzioni)
m_i coprimi a coppie $\Rightarrow$ OK!
- applicare punto 3) $\forall$ equazione
- risolvere con Teor. cinese del resto

ESEMPI DI APPLICAZIONE del teorema di Eulero Fermat

ESERCIZIO 3 pag. 35

Calcolare le cifre che indica le unità di 327^{82}

equivale a calcolare $327^{82} \pmod{10}$ ← resto della divisione per 10 del numero dato

$327 \equiv 7 \pmod{10}$

$327^{82} \equiv 7^{82} \pmod{10}$

possiamo applicare il teorema di Eulero Fermat

$MCD(7,10) = 1 \rightarrow \varphi(10) = 4 \rightarrow 7^4 \equiv 1 \pmod{10}$

$7^{82} \pmod{10} = 7^{(4 \cdot 20 + 2)} \pmod{10} = (7^4)^{20} \cdot 7^2 \pmod{10} = 1 \cdot 49 \pmod{10}$

$= 9 \pmod{10}$

ESERCIZIO 5 pag. 35

Calcolare 1836^{1910} in $\mathbb{Z}_7$

$1836^{1910} \pmod{7}$

$1836 \equiv 2 \pmod{7}$

$1836^{1910} \pmod{7} \equiv 2^{1910} \pmod{7}$

possiamo applicare il teorema di Eulero Fermat

$MCD(2,7) = 1 \rightarrow \varphi(7) = 6 \rightarrow 2^6 \equiv 1 \pmod{7}$

$2^{1910} \pmod{7} \equiv 2^{(6 \cdot 318 + 2)} \pmod{7} \equiv (2^6)^{318} \cdot 2^2 \pmod{7} \equiv 1 \cdot 4 \pmod{7}$

$\equiv 4 \pmod{7}$

ESERCIZIO 8 ~~pag~~ 41

Stabilire se il sistema ammette soluzioni e, eventualmente, determinarle

$$\begin{cases} x+2 \equiv 3(x-1) \pmod 4 \\ 2x \equiv 3 \pmod 5 \\ x+1 \equiv 2-x \pmod 3 \end{cases}$$

$$ax \equiv b \pmod n \implies ax + ny = b$$

$$\begin{cases} x+2 \equiv 3(x-1) \pmod 4 \\ 2x \equiv 3 \pmod 5 \\ x+1 \equiv 2-x \pmod 3 \end{cases} \Rightarrow \begin{cases} x+2+4y = 3(x-1) \\ 2x+5y = 3 \\ x+1+3y = 2-x \end{cases} \Rightarrow \begin{cases} 2x-4y = 5 \\ 2x+5y = 3 \\ 2x+3y = 1 \end{cases}$$

$$\begin{cases} 2x \equiv 5 \pmod 4 \\ 2x \equiv 3 \pmod 5 \\ 2x \equiv 1 \pmod 3 \end{cases} \longrightarrow MCD(2,4) \nmid 1 \quad [1]$$

Il sistema non ammette soluzioni $\in \mathbb{Z}$ perché non è verificata la condizione [1], ovvero il max com. div. tra 2 e 4 non divide 1

NORMALIZZAZIONE

$$ax \equiv b \pmod m \Rightarrow x \equiv b'' \pmod{m'}$$

Hp: $ax \equiv b \pmod m$ risolubile, ovvero $MCD(a,m) \mid b$

1) se $MCD(a,m) = c \neq 1$

$\hookrightarrow \frac{a}{c} x \equiv \frac{b}{c} \pmod{\frac{m}{c}} \Rightarrow a' x \equiv b' \pmod{m'}$

2) Si moltiplica per l'inverso di $a' \pmod{m'}$, ovvero per quel numero che moltiplicato ad a' è congruo uno mod m' $\quad a'y \equiv 1 \pmod{m'}$

$$\underbrace{y \cdot a'}_{1 \pmod{m'}} x \equiv \underbrace{y \cdot b'}_{b'' \pmod{m'}} \pmod{m'} \Rightarrow x \equiv b'' \pmod{m'}$$

ESEMPIO: $6x \equiv 9 \pmod{15}$

- Verifichiamo la risolubilità: $MCD(6,15) \mid 9 \Rightarrow$ ok!
- Riscriviamo l'equazione nel tipo $x \equiv a \pmod m$

1) Dividiamo per $MCD(6,15) = 3$

$$\frac{6}{3} x \equiv \frac{9}{3} \pmod{\frac{15}{MCD(6,15)=3}} \Rightarrow 2x \equiv 3 \pmod 5$$

2) moltiplichiamo per l'inverso di $2 \pmod 5$, ovvero per il numero y tale che $2 \cdot y \equiv 1 \pmod 5$

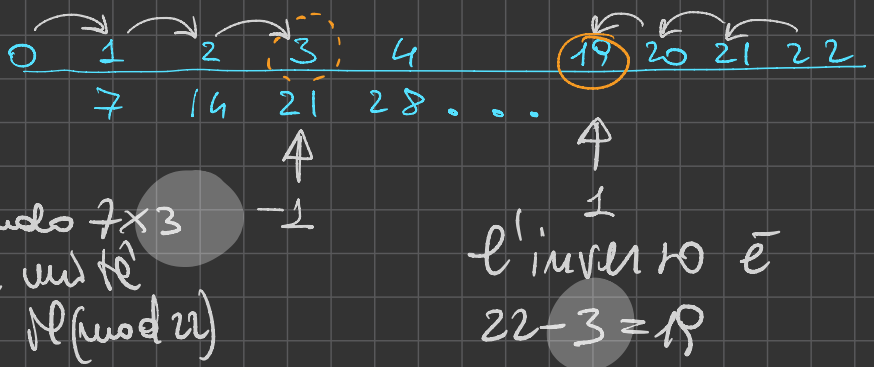
$$3 \cdot 2x \equiv 3 \cdot 3 \bmod 5 \Rightarrow 6x \equiv 9 \pmod 5$$

$$x \equiv 4 \pmod 5$$

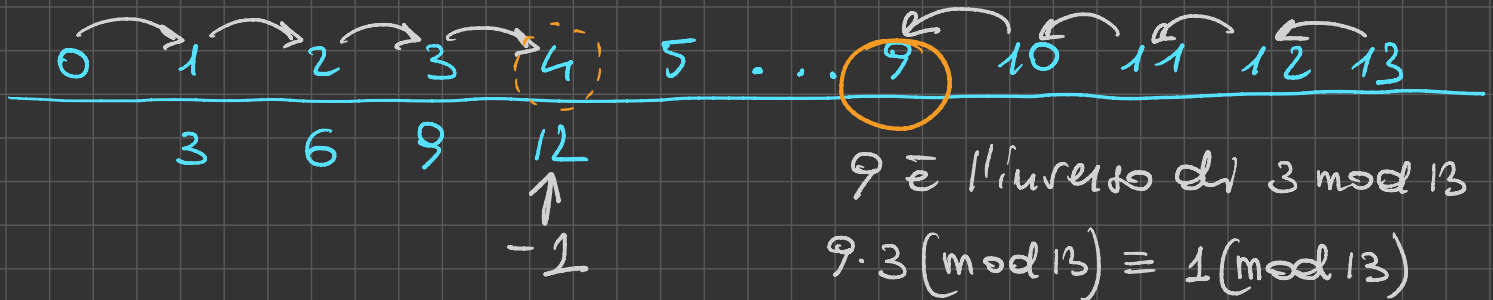
CALCOLO DELL'INVERSO

* METODO PRATICO

calcolo dell'inverso
$7 \pmod{22}$



altro esempio: calcolo dell'inverso $3 \pmod{13}$



* * METODO TEORICO

poiché $x^{\varphi(m)} = 1 \pmod{m}$ Teor. di Eulero - Fermat

allora l'inverso sarà $y = x^{\varphi(m)-1} \pmod{m}$

infatti $x \cdot y = x \cdot x^{\varphi(m)-1} = x^{\varphi(m)} \equiv 1 \bmod m$

Esempio: calcolo dell'inverso di $5 \pmod{18}$

$\varphi(18)=6 \rightarrow 5^{(6-1)} = 3125 \equiv 11 \pmod{18}$ 11 è l'inverso di $5 \pmod{18}$

infatti $5 \cdot 11 = 55 \equiv 1 \pmod{18}$

altro esempio: calcolo dell'inverso $3 \pmod{13}$

$\varphi(13)=12 \rightarrow 3^{11} = 177147 \equiv 9 \pmod{13}$ l'inverso è 9

ESERCIZIO (Sistema di eq. congruenziali)

$$\begin{cases} 2x \equiv 1 \pmod 3 \\ 7x \equiv 5 \pmod{22} \end{cases}$$

$$\ast \begin{cases} 2 \cdot 2x \equiv 2 \cdot 1 \pmod 3 \\ 19 \cdot 7x \equiv 19 \cdot 5 \pmod{22} \end{cases}$$

moltiplico per l'inverso di $2 \pmod 3 = 2$

moltiplico per l'inverso di $7 \pmod{22} = 19$

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 7 \pmod{22} \end{cases} \Rightarrow x \equiv 29 \pmod{66}$$

per prove $0 \leq x < 66$

per il teorema cinese del resto $\text{mcd}(m_1, m_2) = \text{mcd}(3, 22)$