sostituisco in v i valori trovati

$$v = 2c\begin{pmatrix}1\\2\\0\end{pmatrix} + c\begin{pmatrix}0\\5\\0\end{pmatrix} = c\begin{pmatrix}2\\9\\0\end{pmatrix} + 0\begin{pmatrix}6\\9\\1\end{pmatrix} \in \text{span}\begin{pmatrix}2\\9\\0\end{pmatrix}$$

Ricevimento

$a_0 = 1 \qquad a_{n+1} = 2a_n + 3$

$a_1 = 2a_0 + 3 = 2 + 3$

$a_2 = 2a_1 + 3 = 2(2+3) + 3 = 2^2 + 2\cdot 3 + 3$

$a_3 = 2a_2 + 3 = 2(2^2 + 2\cdot 3 + 3) + 3 = 2^3 + 2^2\cdot 3 + 2\cdot 3 + 3$

congettura

$$a_n = 2^n + 3\underbrace{(1 + 2 + 2^2 + \dots + 2^{n-1})}$$

successione geometrica

$2^n - 1$

$$\sum_{i=0}^{n} x^n = \frac{x^{n+1} - 1}{x - 1}$$

$a_n = 2^n + 3\cdot 2^n - 3$

↓ da dimostrare

$a_0 = 2^0 + 3\cdot 2^0 - 3 = 1 + 3 - 3 = 1$ tesi

$a_{n+1} = 2a_n + 3 \qquad 2^{n+1} + 3\cdot 2^{n+1} - 3 = b_{n+1}$

$b_{n+1} = 2b_n + 3$

$2b_n + 3 = (2^n + 32^n - 3) + 3$

$2^{n+1} + 32^{n+1} - 6 + 3 = 2^{n+1} + 32^{n+1} - 3$

esattamente b_{n+1}

$a_n = 2^n + 3\cdot 2^n - 3$

$p(n)$ $\qquad$ $p(0)$ vera

dimostro $p(n+1)$

$a_{n+1} = 2^{n+1} + 3\cdot 2^{n+1} - 3$?

$a_{n+1} = 2a_n + 3$

per ipotesi induttiva

$a_n = 2^n + 32^n - 3$

$+3+2(2^n+3\cdot 2^n+3) = 2^{n+1}+3\cdot 2^{n+1}-3$

✓

Bene mantenere lo schema delle operazioni. Ripassare successioni aritmetiche e geometriche.

ES:

$8x \equiv 2^{99}\ (17)$

① capire quanto fa $2^{99}\ (17)$

$8x \equiv 2^{99}\ (17)$

↓ moltiplico per 2

$-x \equiv 2^{50}\ (17)$

$x \equiv -2^{50}\ (17)$

$2^{50}\ (17)$? $\quad 2^{17} \equiv 2\ (17)$ per il teorema di Fermat

$2^{16} \equiv 1\ (17)$

↓ divisore di 16 può essere il più piccolo esponente (faccio i tentativi)

2^1	2^2	2^4	2^8
≠1	≠1	≠1	=1
2	4	−1	1

$2^8 \equiv 1\ (17)$

$2^{8k} \equiv 1\ (17)$

$2^{50} = 2^{6\cdot 8+2} = \underbrace{2^{8\cdot 6}}_{\equiv 1 \text{ perché multiplo di } 8} \cdot 2^2$

$2^{50} \equiv 4\ (17)$

allora $\quad x \equiv -4\ (17)$

$x \equiv 13\ (17)$ → porto a positivo.

Trovare tutte le soluzioni di

- $2^x \equiv 1 \ (17)$

  $x \equiv 0 \ (8)$

- $2^y \equiv 2 \ (17)$

$2^{x+1} \equiv 2 \ (17)$

$\Leftrightarrow \quad y = x+1$

$x = y-1$

sostituisco y in $x \equiv 0 \ (8)$

$y-1 \equiv 0 \ (8) \Rightarrow y \equiv 1 \ (8)$.

↓ minimo esponente.

ES: $p(x) = (x-2)^3 =$

$= x^3 - 6x^2 + 12x - 8 = 0$

$x^3 = 6x^2 - 12 + 8$

da qui la successione

$a_{n+3} = 6a_{n+2} - 12a_{n+1} + 8a_n$

↑ a regola facilitata della successione di polinomio.

$a_0 =$

$a_1 =$ tutto con

$a_2 =$

$a_n = 2^n$

$a_n = n2^n$ } perché la radice è tripla

$a_n = n^2 2^n$

$a_n = A2^n + Bn2^n + Cn^2 2^n$

es:

$$a_{n+1} = a_n + 6a_{n-1} \quad \text{con} \quad a_0 = 2, \; a_1 = 1$$

$$a_{n+1} - a_n - 6a_{n-1} = 0$$

tento con $a_n = \alpha^n$

$$\alpha^{n+1} - \alpha^n - 6\alpha^{n-1} = 0$$

divido per α^n

$$\alpha^2 - \alpha - 6 = 0$$

$$\Downarrow$$

$$p(x) = x^2 - x - 6 = 0$$

quali sono le radici? → α che verifica a_n

$$\alpha = \frac{1 \pm \sqrt{1+24}}{2}$$

$$\alpha = \frac{1 \pm 5}{2} \begin{cases} 3 \\ -2 \end{cases} \Big] \text{ radici}$$

$$\Downarrow$$

$$p(x) = (x-3)(x+2)$$

quando ho le radici
so anche come fattorizzarlo

tentativo: 3^n

tentativo: -2^n

tentativo finale: $A3^n + B(-2^n)$

[se avessimo avuto
$(x-3)(x+2)^2$ dovevamo provare
anche con $C(-2^n n)$]

$$a_0 = A3^0 + B(-2^0)$$

$$a_1 = A3 + B(-2)$$

sistema:

$$\begin{cases} A + B = 2 \\ 3A - 2B = 1 \end{cases} \qquad \begin{cases} A = 2 - B \\ 6 - 3B - 2B = 1 \end{cases}$$

$$\begin{cases} B = 1 \\ A = 1 \end{cases} \Rightarrow a_n = 3^n - 2^n$$

ES:

$L: V \to W \qquad w = L(v)$

$B \qquad C$

$B \to \{b_1, b_2\}$

$[L]_C^B \cdot v_B = w_C \qquad C \to \{c_1, c_2, c_3\}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix}$$

Come devo scegliere v_B cancendo $v_B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$v = b_1$

calcolo $L(b_1)$ per capire come è fatta $[L]$

Quando mi calcolo la matrice, ho la funzione che la descrive e voglio rappresentarla non in base canonica

1) Applico la L ai vettori della prima base

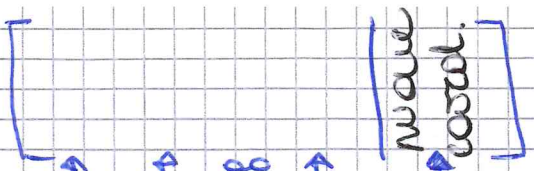
$L(b_1) = \begin{pmatrix} \text{nuove} \\ \text{coord.} \end{pmatrix}$

$L(b_2) = \begin{pmatrix} \text{nuove} \\ \text{coord.} \end{pmatrix} \quad \infty \quad L(b_n) = \begin{pmatrix} \text{nuove} \\ \text{coord.} \end{pmatrix}$

2) Le nuove coordinate devono essere scritte come combinazione lineare dei vettori della base di arrivo.

$\#$

metto a sistema (matrice)



c_1 c_2 ∞ c_n

le coordinate trovate dopo l'applicazione di L ai vettori di B. (base di partenza)

↓ uomo di riga ⇒ riduciamo a scalini della matrice.

es.

$$\begin{cases} 5x \equiv 4\ (13) \\ 6x \equiv 2\ (7) \end{cases}$$

$5x \equiv 4\ (13)$ $\quad 5 \cdot 5 = 25 \quad 13 \to 26$

$-x \equiv 20\ (13)$

$x \equiv -7\ (13)$

$x = -7 + 13k$

$6(-7+13k) \equiv 2\ (7)$

$6(-1+k) \equiv 2\ (7)$

$-6 - 6k \equiv 2\ (7)$

$6k \equiv -8\ (7)$

$3k \equiv -4\ (7)$

$-k \equiv -12\ (7)$

$k \equiv 12\ (7) \quad k = 12 + 7t$

$x = -7 + 13(12 + 7t)$

$x = -7 + 156 + 91t$

149

$x \equiv 149\ (91)$

$x \equiv 58\ (91)$

es: $L: \mathbb{R}^2 \to \mathbb{R}^2$ $\quad v_1 = \begin{pmatrix}1\\1\end{pmatrix}$ $\quad v_2 \begin{pmatrix}2\\1\end{pmatrix}$

$w_1 = \begin{pmatrix}0\\-1\end{pmatrix}$ $\quad w_2 = \begin{pmatrix}-2\\1\end{pmatrix}$

$v_1 \xrightarrow{L} \begin{pmatrix}0\\0\end{pmatrix}$

$v_2 \xrightarrow{L} w_1 + w_2$ Scrivere la matrice di L rispetto alle basi:

$$[L]^{v_1, v_2}_{w_1, w_2}$$

$L(v_1)$

$$\begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix}$$

$L(v_2)$

$$\begin{pmatrix}0\\0\end{pmatrix} = a\begin{pmatrix}0\\-1\end{pmatrix} + b\begin{pmatrix}-2\\1\end{pmatrix}$$

$a = 0$
$b = 0$

$$\begin{pmatrix}-2\\0\end{pmatrix} = a'\begin{pmatrix}0\\-1\end{pmatrix} + b'\begin{pmatrix}-2\\1\end{pmatrix}$$

$a' = 1$
$b' = 1$

$$[L]\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}$$

ES:

$$A = \begin{bmatrix}1 & 1 & 1 & 1\\1 & 1 & 2 & 2\\2 & 2 & 3 & 3\end{bmatrix}$$

Quante soluzioni ha?

riduco a scalini:

$$\begin{matrix}R_2 - R_1\\ R_3 - 2R_1\end{matrix}\begin{bmatrix}1 & 1 & 1 & 1\\0 & 0 & 1 & 1\\0 & 0 & 1 & 1\end{bmatrix} \xrightarrow{R_3 - R_2} \begin{bmatrix}1 & 1 & 1 & 1\\0 & 0 & 1 & 1\\0 & 0 & 0 & 0\end{bmatrix}$$

2 variabili libere $\Rightarrow$ infinite soluzioni

poiché

$0 \cdot t = 0 \quad \forall t \in \mathbb{R}$

$0 \cdot y = 0 \quad \forall y \in \mathbb{R}$

$K_1 - K_2$

$$\to \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \Rightarrow \begin{pmatrix} -y \\ y \\ -t \\ t \end{pmatrix}$$

$$y\begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t\begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \end{pmatrix} \quad \text{indipendenti}$$

~~base~~ dee ker $\dim(\ker A) = 2$.

Ha soluzioni $\forall b \in \mathbb{R}^3$?

Passo il sistema in matrice aumentata ad un generico vettore $\in \mathbb{R}^3$

$$\left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & b_1 \\ 1 & 1 & 2 & 2 & b_2 \\ 2 & 2 & 3 & 3 & b_3 \end{array}\right]$$

stesse mosse di riga

$$\left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & b_1 \\ 0 & 0 & 1 & 1 & b_2 - b_1 \\ 0 & 0 & 0 & 0 & b_3 - b_2 - b_1 \end{array}\right]$$

$b_3 - b_2 - b_1 = 0$ non sempre è verificata per esempio con il vettore

$b = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ la condizione non è valida.

es: Numero delle soluzioni del sistema:

$$\begin{cases} x_1 + kx_2 + (1+4k)x_3 = 1+4k \\ 2x_1 + (k+1)x_2 + (2+7k)x_3 = 1+7k \\ 3x_1 + (k+2)x_2 + (3+9k)x_3 = 1+9k \end{cases}$$

k è un parametro.

Metto nella matrice e riduco a scalini:

$$\left[\begin{array}{ccc|c} 1 & k & 1+4k & 1+4k \\ 2 & k+1 & 2+7k & 1+7k \\ 3 & k+2 & 3+9k & 1+9k \end{array}\right] \begin{array}{l} \\ R_2-2R_1 \\ R_3-3R_1 \end{array}$$

$2+7k \quad 2-6k$

$k+2 \quad -3k$

$$\left[\begin{array}{ccc|c} 1 & k & 4k+1 & 1+4k \\ 0 & 1-k & -k & -1-k \\ 0 & 2-2k & -3k & -3k-2 \end{array}\right] \begin{array}{l} \\ \\ R_3-2R_2 \end{array}$$

$-3+9k \quad -3-12k$

$$\left[\begin{array}{ccc|c} 1 & k & 4k+1 & 1+4k \\ 0 & 1-k & -k & -1-k \\ 0 & 0 & -k & -k \end{array}\right]$$

sono i PIVOT

$1-k \neq 0$

$-k \neq 0$

casi speciali:

$k=0$

$$\left[\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

infinite soluzioni

$k=1$

$$\left[\begin{array}{ccc|c} 1 & 1 & 5 & 5 \\ 0 & 0 & -1 & -2 \\ 0 & 0 & -1 & 1 \end{array}\right] \rightarrow \left[\begin{array}{ccc|c} 1 & 1 & 5 & 5 \\ 0 & 0 & -1 & -2 \\ 0 & 0 & 0 & -1 \end{array}\right]$$

nessuna soluzione

$0 \cdot z = -1$ IMPOSSIBILE

se $k \neq 0, 1$ abbiamo una sola soluzione

es:

$$\begin{cases} (k+2)x + 2ky - z = 1 \\ x - 2y + kz = -k \\ y + z = k \end{cases}$$

per quali valori di k abbiamo una soluzione? matrice (ridurre a scalini)

$$\left[\begin{array}{ccc|c} k+2 & 2k & -1 & 1 \\ 1 & -2 & k & -k \\ 0 & 1 & 1 & k \end{array}\right]$$

$$\left[\begin{array}{ccc|c} 1 & -2 & k & k \\ 0 & 1 & 1 & k \\ k+2 & 2k & -1 & 1 \end{array}\right] \xrightarrow{R_3 - (k+2)R_1}$$

$$\left[\begin{array}{ccc|c} 1 & -2 & k & k \\ 0 & 1 & 1 & k \\ 0 & 4k+4-(k+1) & & (k+1)^2 \end{array}\right] \xrightarrow{R_3 - 4(k+1)R_2}$$

$$\left[\begin{array}{ccc|c} 1 & -2 & k & -k \\ 0 & 1 & 1 & k \\ 0 & 0 & -(k+1)(k+5) & (k+1)(-3k+1) \end{array}\right]$$

$-(k+1) \neq 0 \quad k \neq -1$

$k \neq -5$

$\Rightarrow$ unica soluzione

casi speciali

$k = -1$

$$\left[\begin{array}{ccc|c} 1 & -2 & -1 & k \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

infinite soluzioni

es: Trovare le coordinate del vettore $C=\begin{pmatrix}2\\1\end{pmatrix}$ delle rispettive basi $u_1\begin{pmatrix}3\\2\end{pmatrix}$ e $u_2\begin{pmatrix}2\\3\end{pmatrix}$

$$x_1\begin{pmatrix}3\\2\end{pmatrix}+x_2\begin{pmatrix}2\\3\end{pmatrix}=\begin{pmatrix}2\\1\end{pmatrix}$$

$2+3x=0$ $\quad x=-\frac{2}{3}$

$$\left[\begin{array}{cc|c}3&2&2\\2&3&1\end{array}\right]\xrightarrow{R_2-\frac{2}{3}R_1}\left[\begin{array}{cc|c}3&2&2\\0&5/3&-\frac{1}{3}\end{array}\right]$$

$$x_2=-\frac{1}{3}\cdot\frac{3}{5}=-\frac{1}{5}$$

$$3x_1=\frac{1}{5}+2 \qquad x_1=\frac{4}{5} \qquad C\left(\tfrac{4}{5},-\tfrac{1}{5}\right)$$

Trovare le coordinate del polinomio $p(x)=2+x$ rispetto alla base $q_1(3+2x)$, $q_2(2+3x)$

scrivo rispetto alla base canonica $e_1=1$, $e_2=x$

$p(x)=2e_1(x)+e_2(x) \Rightarrow \begin{pmatrix}2\\1\end{pmatrix}$

$q_1(x)=3e_1(x)+2e_2(x) \Rightarrow \begin{pmatrix}3\\2\end{pmatrix}$

$q_2(x)=2e_1(x)+3e_2(x) \Rightarrow \begin{pmatrix}2\\3\end{pmatrix}$

per scrivere $p(x)$ rispetto a q_1, q_2

$$x_1\begin{pmatrix}3\\2\end{pmatrix}+\begin{pmatrix}2\\3\end{pmatrix}=\begin{pmatrix}2\\1\end{pmatrix}$$ stesso sistema di prima

es: $V=\text{span}(v_1, v_2, v_3)$

$v_1\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$ $\quad v_2\begin{pmatrix}2\\2\\2\\3\end{pmatrix}$ $\quad v_3\begin{pmatrix}1\\1\\2\\-1\end{pmatrix}$

$\dim V$? metto a matrice 4 righe 3 vettori.

$$\begin{bmatrix} 1 & 2 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 2 \\ 1 & 3 & -1 \end{bmatrix} \begin{matrix} R_2-R_1 \\ \longrightarrow \\ R_3-R_1 \\ R_4-R_1 \end{matrix} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -2 \end{bmatrix} \longrightarrow$$

$$\begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

I vettori v_1, v_2, v_3 sono indipendenti $\Rightarrow$ 3 pivot

$\Downarrow$

dim di $V = 3$

es: $U = \text{span}\left(\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}\right)$

$W = \text{span}\left(\begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\2\\0\\2\end{pmatrix}\right)$

Trovare una base per $U+W$ e $U \cap W$

Metto a matrice i vettori dello SPAN di entrambi i [illegible] e riduco a scalini; i vettori dove ci sono i pivot sono indipendenti e saranno una BASE di $U+W$.

$$\left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 2 \\ 1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 2 \end{array}\right] \begin{matrix} R_2-R_1 \\ R_3-R_1 \\ R_4-R_1 \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & -1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & -2 & -1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & -2 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

I colonna II colonna IV colonna

III colonna

i vettori $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}, \begin{pmatrix}1\\2\\0\\2\end{pmatrix}$

$\Rightarrow$

$\dim U = 2 \quad \dim V = 2$

$\Rightarrow$ Per Grassman $\dim(U \cap W) = \dim U + \dim V - \dim(U+W)$

$= 2 + 2 - 3 = 1$.

Es: $V = \text{span}(v_1, v_2)$

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \qquad v_2 = \begin{pmatrix} 1 \\ 3 \\ 1 \\ 0 \end{pmatrix}$$

$$W = \begin{cases} x_1 + x_2 + 2x_4 = 0 \\ 2x_1 + x_2 + x_3 = 0 \end{cases}$$

trovare una base di $V+W$ $V \cap W$

$$\left[\begin{array}{cc|c} 1 & 1 & x_1 \\ 1 & 3 & x_2 \\ 1 & 1 & x_3 \\ 0 & 0 & x_4 \end{array}\right] \xrightarrow[R_3 - R_1]{R_2 - R_1}$$

generico vettore

$$\left[\begin{array}{cc|c} 1 & 1 & x_1 \\ 0 & 2 & x_2 - x_1 \\ 0 & 0 & x_3 - x_1 \\ 0 & 0 & x_4 \end{array}\right]$$

perché sia verificata questa matrice non ci devono essere più dopo la barra in corrispondenza dei gradini zeri

$$\begin{cases} x_3 - x_1 = 0 \\ x_4 = 0 \end{cases}$$

siccome cerchiamo $V \cap W$ le varie condizioni devono valere per W.

$$\begin{cases} x_3 - x_1 = 0 \\ x_4 = 0 \\ x_1 + x_2 + 2x_4 = 0 \\ 2x_1 + x_2 - x_3 = 0 \end{cases}$$

$$\left[\begin{array}{cccc} -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 2 \\ 2 & 1 & -1 & 0 \end{array}\right]$$

$$\begin{bmatrix} 1 & 1 & 0 & 2 \\ 2 & 1 & -1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[R_3+R_1]{R_2-2R_1} \begin{bmatrix} 1 & 1 & 0 & 2 \\ 0 & -1 & -1 & -2 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 0 & 2 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

x_3 libera

scrivo in funzione di questa

$$\begin{cases} x_1 - x_3 = 0 \\ x_2 + x_3 = 0 \\ x_4 = 0 \end{cases}$$

$$\begin{pmatrix} x_3 \\ -x_3 \\ x_3 \\ 0 \end{pmatrix} \longrightarrow x_3 \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix} \longrightarrow \text{base di } U \cap W$$

Per la somma mettiamo in matrice i vettori che generano i due spazi

$$\begin{cases} x_1 + x_2 + 2x_4 = 0 \\ 2x_1 + x_2 - x_3 = 0 \end{cases}$$

$$\begin{bmatrix} 1 & 1 & 0 & 2 \\ 2 & 1 & -1 & 0 \end{bmatrix} \xrightarrow{R_2-2R_1} \begin{bmatrix} 1 & 1 & 0 & 2 \\ 0 & -1 & -1 & -4 \end{bmatrix}$$

$-1 \quad 1 \quad 4$

x_4, x_3 libere

$$\begin{pmatrix} +x_3+4x_4-2x_4 \\ -x_3-4x_4 \\ x_3 \\ x_4 \end{pmatrix} \Rightarrow \begin{pmatrix} x_3+2x_4 \\ -x_3-4x_4 \\ x_3 \\ x_4 \end{pmatrix}$$

separo i coefficienti

$$x_3\begin{pmatrix}1\\-1\\1\\0\end{pmatrix}+x_4\begin{pmatrix}2\\-4\\0\\1\end{pmatrix}$$

$$W=\text{span}\left(\begin{pmatrix}1\\-1\\1\\0\end{pmatrix},\begin{pmatrix}2\\-4\\0\\1\end{pmatrix}\right)$$

matrice con i 4 vettori (per la somma).

$$\begin{bmatrix}1&1&1&2\\1&3&-1&-4\\1&1&1&0\\0&0&0&1\end{bmatrix}\begin{matrix}R_2-R_1\\ \longrightarrow\\ R_3-R_1\end{matrix}\begin{bmatrix}1&1&1&2\\0&2&-2&-6\\0&0&0&-2\\0&0&0&1\end{bmatrix}$$

$$\underrightarrow{R_4+\tfrac{1}{2}R_3}\begin{bmatrix}1&1&1&2\\0&2&-2&-6\\0&0&0&-2\\0&0&0&0\end{bmatrix}$$

↑ ↑ ↑

Pivot ⇒ vettori indipendenti

$$\begin{pmatrix}1\\1\\1\\0\end{pmatrix},\begin{pmatrix}1\\3\\1\\0\end{pmatrix},\begin{pmatrix}2\\-4\\0\\1\end{pmatrix}$$ vettori base di $V+W$.

$$\begin{cases} 18x \equiv 232 \pmod{34} \\ 220x \equiv 80 \pmod{30} \end{cases}$$

$$\begin{cases} 18x \equiv 18 \pmod{34} \\ 10x \equiv 20 \pmod{30} \end{cases}$$

$$\begin{cases} 9x \equiv 9 \pmod{17} \\ x \equiv 2 \pmod{3} \end{cases}$$

es:

$$\begin{cases} 18x \equiv 232 \pmod{34} \\ 220x \equiv 80 \pmod{30} \end{cases} \longrightarrow 9x \equiv 116 \pmod{17}$$

$$9x \equiv 19 \pmod{17}$$

$$\downarrow$$

$$22x \equiv 8 \pmod{3}$$

$$11x \equiv 4 \pmod{3}$$

$$-x \equiv 1 \pmod{3}$$

$$\begin{cases} 9x \equiv 19 \pmod{17} \\ x \equiv -1 \pmod{3} \end{cases}$$

$(17, 9) \xrightarrow{17-9} (8, 9) \rightarrow$

$(8, 1) \rightarrow (1, 0) = 1$

$17 = 1 \cdot 17 + 0 \cdot 9$

$9 = 0 \cdot 17 + 1 \cdot 9$

$8 = 1 \cdot 17 + (-1) \cdot 9$

$1 = -1 \cdot 17 + 2 \cdot 9$

$$\begin{cases} x \equiv 11 \pmod{17} \\ x \equiv 2 \pmod{3} \end{cases}$$

$x = 11 + 17k$

$11 + 17k \equiv 2 \pmod{3}$

$2 + 2k \equiv 2 \pmod{3}$

$1 + k \equiv 1 \pmod{3}$

$k \equiv 0 \pmod{3}$ $\quad k = 3\ell$

$x = 11 + 51\ell$

$x \equiv 11 \pmod{51}$

es: $\begin{cases} 22x \equiv 29 \ (39) \\ 196^{2903} \equiv x \ (19) \end{cases}$

$(39,22) \xrightarrow{39-22} (22,17) \xrightarrow{22-17} (17,5) \xrightarrow{17-3\cdot5} (5,2)$

$\xrightarrow{5-2\cdot2} (2,1) \longrightarrow (1,0)$

$39 = 1\cdot39 + 0\cdot22$

$22 = 0\cdot39 + 1\cdot22$

$17 = 1\cdot39 + (-1)22$

$5 = -1\cdot39 + 2\cdot22$

$2 = 4\cdot39 + (-7)22$

$1 = -9(39) + 16\cdot22$

$\begin{cases} x \equiv 35 \ (39) \\ 196^{2903} \equiv x \ (19) \end{cases}$

$196 \equiv 13 \ (19)$

$\Rightarrow 13^{2903} \equiv x \ (19)$

per il piccolo teorema di fermat

$13^{18} \equiv 1 \ (19)$

$2903 = 3\cdot3\cdot3\cdot(18\cdot4+11) = (18\cdot4+11)\cdot27$

$13^{27\cdot(18\cdot4+11)} \quad ((13)^{18\cdot4+11})^{27}$

$(13^{16}\cdot13^{1})^{27} = 13^{16\cdot27} = 13^{297} = 13^{18\cdot16+9}$

1

$\equiv 13^{9}$

$13^9 \equiv x\ (19)$

$13 \equiv -6\ (19) \rightarrow 13^2 \equiv 36 \equiv -2\ (19)$

$\underline{13^9} \equiv (13^2)^4 \cdot 13 \equiv (-2)^4(-6) \equiv$

$\equiv (-3)(-6) \equiv \underline{-1\ (19)}$

$$\begin{cases} x \equiv 18\ (19) \\ x \equiv 35\ (39) \end{cases}$$

$x = 18 + 19k$

$18 + 19k \equiv 35\ (39)$

$19k \equiv 17\ (39)$

$(39, 19) \xrightarrow{39 - 2 \cdot 19} (19, 1)$

$-k \equiv 34\ (39)$

$k \equiv -34\ (39)$

$k \equiv 5\ (39)$

$k = 5 + 39\ell$

$x = 18 + 19(5 + 39\ell)$

$x = 18 + 95 + 741\ell$

$x \equiv 1710\ (741)$

$x \equiv 228\ (741)$

es:

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 2 \end{pmatrix} \quad v_2 = \begin{pmatrix} 1 \\ 2 \\ -1 \\ 1 \end{pmatrix} \quad v_3 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & -1 & 1 \\ 2 & 1 & 2 \end{pmatrix} \begin{matrix} R_2 - R_1 \\ R_3 - R_1 \\ R_4 - 2R_1 \end{matrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & -2 & 1 \\ 0 & -1 & 2 \end{pmatrix}$$

$$\begin{matrix} R_3 + 2R_2 \\ R_4 + R_2 \end{matrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & -1 & 1 \\ 2 & 1 & 2 \end{bmatrix}$$

fare mosse di colonna

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & -2 & 3 \\ 2 & -1 & 3 \end{bmatrix}$$

$$\begin{matrix} 0 \\ 0 \\ 0 \\ 1 \end{matrix}$$

Induzione:

$$\sum_{k=1}^{n} (2k)^3 = 2n^2(n+1)^2$$

$p(n)$

$p(n+1)$?

$(1) = 8 = 2(1+1)^2 = \checkmark$

$(2) = 8 + 64 = 2 \cdot 2^2 \cdot (3)^2$ ✓

$$\sum_{k=1}^{n+1} (2k)^3 = \sum_{k=1}^{n} (2k)^3 + (2n+2)^3$$

$$2n^2(n+1)^2 + (2n+2)^3 = 2(n+1)^2(n+1+1)^2$$

Tesina. ↑ ricevimento

Matematica discreta 20/04/2017

Ripasso congruenze esponenziali:

$k > 0 \quad k \in \mathbb{R}$

$a^{-k} \mod m$

Se a è invertibile modulo m

allora $a^{-1} \cdot a \equiv 1 \ (m)$

$$a^{-k} = \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ volte}} = (a^{-1})^k$$

$$a^{-k} \cdot a^{k} = \underbrace{a^{-1} \cdot a^{-1} \ldots a^{-1}}_{k} \cdot \underbrace{a \cdot a \ldots a}_{k} \equiv 1 \ (m)$$

- $a^{x+y} \equiv a^x \cdot a^y \ (m) \quad \forall x, y$ (anche negativi).

es: $a^{-5} \cdot a^7 \equiv a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a \cdot a \cdot a \cdot a \cdot a \cdot a \cdot a = a^2 \ (m)$

$a^{-8} \cdot a^2 \equiv \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{6} \cdot a \cdot a = a^{-6} \ (m)$

Teorema

Se a è invertibile mod $(m) \Rightarrow$

$\exists k > 0, \in \mathbb{Z}$ t.c. $a^k \equiv 1 \ (m)$

es: $4^k \equiv 1 \ (15)$ sicuramente c'è un k.

dimostrazione:

n	1	2	3	4	5	6	...
a^n	a^1	a^2	a^3	a^4	a^5	a^6	...

mod (m)

sono tutti più piccoli di m. → ad un certo punto si ripetono

cioè $\exists s, t$ t.c. $a^s \equiv a^t \ (m)$

$0 < s < t$

$a^{t-s} = a^t \cdot a^{-s} \equiv a^s a^{-s} \equiv 1 \ (m)$

$a^t \equiv a^s$ è ovviamente.

ha senso perché a è invertibile

es:

$3^2 \equiv 1 \ (4)$ ← positivo

il più piccolo k che funziona (= da 1) si chiama ordine di $a \ (m)$

$\Downarrow$

$\text{ord}(a)_m$

Per risolvere le congruenze esponenziali possiamo calcolare gli ordini.

es: ordine di $14 \bmod (101)$

cioè il più piccolo $k > 0$ t.c.

$14^k \equiv 1 \ (101)$ sicuramente esiste 101 è primo.

⇒ per il piccolo teorema di Fermat:

$14^{101} \equiv 14 \ (101)$

↳ divido per 14

$14^{100} \equiv 1 \ (101)$

passaggio possibile perché 14 e non ha fattori comuni con 101.

100 è il più piccolo ?
se c'è allora il k divide 100.

Teorema
se k è il più piccolo positivo t.c. $a^k \equiv 1 \pmod m$
$\Rightarrow$ $a^x \equiv 1$ vale se $x = yk$ (multiplo).
$\Updownarrow$
$x \equiv 0 \pmod k$

da sapere
dimostrazione.

1) se $x \equiv 0 \pmod k \Rightarrow \exists e$ t.c. $ke = x$

$$a^x = a^{ke} = (a^k)^e \underset{(m)}{\equiv} (1)^e \equiv 1 \pmod m$$

2) Se $a^x \equiv 1 \pmod m$ voglio dimostrare che x è un multiplo di k.

$$\begin{array}{c|c} x & k \\ \hline r & q \end{array}$$

$x = kq + r \quad 0 \le r < k$

sostituisco

$$a^x = a^{kq+r} = a^{kq} \cdot a^r \equiv 1 \cdot a^r$$

$a^r \equiv 1 \pmod m$ questo vuol dire che $r = 0$
quindi k è il più piccolo.
$\Downarrow$
$k \mid x$

$x \equiv 0 \pmod k$

torniamo all'es:

$14^{100} \equiv 1 \pmod{101}$

è minimo t.c. $14^k \equiv 1 \pmod{101}$

$\Rightarrow k \mid 100 \qquad 10 \cdot 10 = 2^2 \cdot 5^2$

$k = 2, 4, 10, 5, 25, 20, 50, 100$

n	2	4	5	10	20	25	50	100
14^n	-6	36	-1	1				

è il k

ordine di 14 (101) è 10

es: trovare tutte le soluzioni di

$$14^{3z+2} \equiv 1 \ (101)$$

$3z+2 = y \qquad 14^y \equiv 1 \ (10)$

↓ quando y è multiplo di 10.

vale $\forall y$ anche < 10. $\Rightarrow y \equiv 0 \ (10)$ ↳ ordine

$$14^{3z+2} \equiv 1 \ (101) \iff 3z+2 \equiv 0 \ (10)$$

$$3z \equiv +8 \ (10)$$

$\cdot 3$ ($-z \equiv 4 \ (10)$

$$\underline{z \equiv 6 \ (10)}$$ soluzione

es:

$$14^x \equiv 1 \ (303)$$

1° metodo (sconsigliato)

stesso caso: cerco il k ma non ho più il teorema di Fermat poiché 303 non è primo.

2° metodo

$$\begin{cases} 14^x \equiv 1 \ (101) \\ 14^x \equiv 1 \ (3) \end{cases}$$

$x \equiv 0 \ (10)$ → per la prima congruenza

$14^x \equiv 1 \ (3)$

posso ridurre la BASE rispetto al modulo. (Mai l'esponente)

$2^x \equiv 1 \ (3) \qquad x \equiv 0 \ (2)$ ↳ ordine di 2 (3)

$$\begin{cases} x \equiv 0 \ (10) \\ x \equiv 0 \ (2) \end{cases} \Rightarrow x \equiv 0 \ (10)$$

$\downarrow$

$mcm(10, 2)$

es:

$$14^{77+5} \equiv 95 \ (101)$$

95 è $14^?$ mod (101) ?

$$95 \equiv 14^{+2} \ (101)$$

sostituisco:

$$14^{77+5} \equiv 14^2 \ (101)$$

$\cdot 14^{-2}$ (↳

$$1 4^{77+3} \equiv 1 \ (101)$$

$77+3 \equiv 0 \ (10)$ ↑ ordine di 14 mod 101

$$77 \equiv 7 \ (10)$$
$$7 \equiv 1 \ (10)$$

Teorema

p e q numeri primi. $0 \leq m < p \cdot q$

d, e t.c. $d \cdot e \equiv 1 \ (p-1)(q-1)$ (⇔ uno è l'inverso dell'altro)

$$\Rightarrow m^{de} \equiv m \ (p \cdot q).$$

esempio:

$p = 3$, $q = 11$, $p \cdot q = 33$,

$(p-1)(q-1) = 2 \cdot 10 = 20$

$e = 7$ ↑ deve essere invertibile mod 20

$$d7 \equiv 1 \ (20)$$

$$d = 3$$

A conosce tutto

A rende pubblico $p \cdot q = 33$, $e = 7$

(coi numeri molto grandi non è facile risalire a p e q sapendo solo $p \cdot q$)

B vuole spedire un messaggio m ad A, $m < 33$

B spedisce $m^e \ (33)$

A deve elevare per d così ricava m.

es:

$m = 2$ B spedisce ad A

$c = 2^7 \ (33)$ ← codice

$\downarrow$

$29 \ (33)$

B spedisce ad A $c = 29$ (messaggio cifrato).

A lo decodifica elevando per d (dato che conosce solo A).

$(29)^d = 29^3 \ (33)$

$29 \equiv -4^3 \ (33)$

$= 16 \cdot (-4) \ (33) \equiv 2 \ (33)$

↳ esattamente m.

dimostrazione del teorema:

$m^{ed} \equiv m \ (p \cdot q)$

$\Downarrow$

$\begin{cases} m^{ed} \equiv m \ (p) \\ m^{ed} \equiv m \ (q) \end{cases}$

$e \cdot d \equiv 1 \ (p-1)(q-1)$

$\Downarrow$

$e \cdot d = 1 + k(p-1)(q-1)$

$m^{ed} \equiv m^1 \cdot m^{k(p-1)(q-1)} \ (p)$

$m^{(p-1)} \equiv 1 \ (p)$ per il teorema di Fermat

↳ $m \cdot 1 \ (p)$

$m^{ed} \equiv m^1 \cdot m^{k(p-1)(q-1)} \pmod{q}$

$m^{(q-1)} \equiv 1 \pmod{q} \Rightarrow m \cdot 1 \pmod{q}$

per il piccolo teorema di Fermat

Quindi $m^{ed} \equiv m \pmod{pq}$.

Matematica Discreta 26/04/2017

dalle 9 alle 10 in N1 giovedì 27 correzione compitini. 10 e 17 maggio aula E (invece che in B.) dalle 14-16

$\mathrm{ord}(a)_p \equiv$ il minimo $k>0$ $a \equiv 1 \pmod{p}$

teorema $k \mid p-1$

$a^x \equiv 1 \pmod{p} \iff k \mid x$ cioè $x \equiv 0 \pmod{k}$

Cosa succede se p non è primo?

- ϕ di Eulero

  Il funzione $n>0 \in \mathbb{Z}$

  $\phi(n) = \#\{x \mid 0 \le x < n, x \text{ è invertibile mod } n\}$

  $\phi(5) = 4$

  $0, \underbrace{1, 2, 3, 4}_{\text{invertibili}}$

  Se p è primo $\phi(p) = p-1$.

ma quando non è primo?

es: $\phi(15) = ?$ ~~0~~, 1, 2, ~~3~~, 4, ~~5~~, ~~6~~, 7, 8, ~~9~~, ~~10~~, 11, ~~12~~, 13, 14, ~~15~~

$\phi(15) = 8$

$15 = 3 \cdot 5$

$\phi(15) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8$

teorema

Se a e b sono coprimi $(a, b) = 1$

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

es:

$$\phi(30) = \phi(2) \cdot \phi(5) \cdot \phi(3) = 1 \cdot 2 \cdot 4 = 8$$

$$30 = 2 \cdot 3 \cdot 5$$

teorema: $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ p primo.

$$\phi(n) = \phi(p_1^{e_1}) \cdot \phi(p_2^{e_2}) \cdots \phi(p_k^{e_k})$$

es: $\phi(18) = \phi(3^2) \cdot \phi(2)$

$= 3^2 \cdot 2$ | non so

non so

$$\phi(5^2) = 5^2 - 5 = 5(5-1) = 20$$

Quanto fa

$$\phi(p^2) = \#\{0 \le x < p^2 \mid x \text{ invertibile mod } p^2\} =$$

con p primo

$$= p^2 - \#\text{non invertibile}$$

$$\Downarrow$$

multipli di p.

$$\Downarrow$$

$$\#\{p \cdot i \mid 0 \le i \le p-1\}$$

$\phi(p^k) = p^k - p^{k-1}$ ci sono p^{k-1} non invertibili mod p^k =

sono i multipli di p

$$p \cdot 0 \quad p \cdot 1 \quad p \cdot 2 \cdots p(p^{k-1} - 1)$$

in tutto sono p^{k-1}

$$\phi(p^k) = p^{k-1}(p-1)$$

teorema di Fermat a confronto con il teorema di Eulero

$a^{p-1} \equiv 1 \ (p)$ p primo
$a \not\equiv 0 \ (p)$

$$a^{\phi(n)} \equiv 1 \ (n)$$
se $(a, n) = 1$

$$a^{\phi(n)} = a \cdot a^{\phi(n)-1}$$
↑ inverso di a

Se $a^k \equiv 1 \ (n)$ a è invertibile con inverso a^{k-1}

$ord(a)_n$ = minimo $k \cdot a^k \equiv 1 \ (n)$

il rapporto tra k e $\phi(n)$

$k \mid \phi(n)$ (come per Fermat).

$a^x \equiv 1 \ (n)$ x multiplo del minimo k
$k>0$ t.c. $a^k \equiv 1 (n)$

$k = ord(a)_n \Rightarrow x \equiv 0 \ (k)$

Con Eulero sappiamo in più che

$k \mid \phi(n) \Rightarrow$ la ricerca degli ordini è limitata.

es:
$\phi(30) = \phi(2 \cdot 3 \cdot 5) = \phi(2) \cdot \phi(3) \cdot \phi(5) = 8$

$\exists k . \ 6^k \equiv 1 (30)$? no perché $(6, 30) \neq 1$.

$\exists k . \ 7^k \equiv 1 \ (30)$? si

se al posto di k ci metto $\phi(n)$ sicuramente vale la congruenza

$7^8 \equiv 1 (30)$ è il minimo ? bisogna provare

proviamo i k che dividono 8:

2, 4, 8

$7^2 \equiv 19 \ (30)$

$7^4 \equiv 19 \cdot 19 \equiv 361 \equiv 1 \ (30)$

$k = ord(7)_{30} = 4$

$7^x \equiv 1 \ (30)$

$\Updownarrow$

$x \equiv 0 \ (4)$ soluzione della congruenza iniziale.

es: $7^x \equiv 19 \ (30)$

devo poterlo scrivere come una potenza di 7 perché sennò mai sarebbe risolvibile.

$7^x \equiv 7^2 \ (30)$

$\Updownarrow$

$7^{x-2} \equiv 1 \ (30)$

$x - 2 \equiv 0 \ (4)$

$7^4 \equiv 1 \ (30)$

$y = x - 2 \Rightarrow y \equiv 0 \ (4)$

es: $11^{66} \equiv ? \ (30)$

teorema Eulero dice che

$\phi(30) = 8 \Rightarrow 11^8 \equiv 1 \ (30)$

$11^{66} \equiv 11^{2 \cdot 8 + 2} \ (30)$

$11^{66} \equiv 11^2 \ (30)$

$121 \equiv 1 \ (30)$ ✓

es: $7^{13} \equiv ?\ (30)$

$\phi(30) = 8 \qquad 7^8 \equiv 1\ (30)$ ma

$13 = 4 \cdot 3 + 1 \qquad ord(7)_{30} = 4$

$7^4 \equiv 1\ (30)$

$7^{13} \equiv 7^{4 \cdot 3} \cdot 7 \equiv 7^1\ (30)$

$7^{13} \equiv 7\ (30)$

l'ordine divide sempre la ϕ di Eulero

dimostrazione del teorema di Eulero

$a^{\phi(n)} \equiv 1\ (n)$

se $(a,n) = 1$

caso facile: $n = p_1 p_2 \cdots p_k$ distinti

applico il teorema cinese dei resti e Fermat:

$\phi(n) = \phi(p_1) \cdot \phi(p_2) \cdot \cdots \cdot \phi(p_k) = (p_1 - 1) \cdots (p_k - 1)$

fermat:

$$\begin{cases} a^{(p_1-1)(p_2-1)\cdots(p_k-1)} \equiv 1\ (p_1) \\ a^{(p_1-1)(p_2-1)\cdots(p_k-1)} \equiv 1\ (p_1) \\ \vdots \\ a^{(p_1-1)(p_2-1)\cdots(p_k-1)} \equiv 1\ (p_k) \end{cases}$$

cinese:

$$\begin{cases} x \equiv 1\ (p_1) \\ x \equiv 1\ (p_2) \\ \vdots \\ x \equiv 1\ (p_k) \end{cases} \iff x \equiv 1\ (p_1 p_2 \cdots p_k)$$

quindi

$$a^{\underbrace{(p_1-1)(p_2-1)\cdots(p_k-1)}_{\phi(n)}} \equiv 1\ (\underbrace{p_1 \cdot p_2 \cdots p_k}_{n})$$

$a^{\phi(n)} \equiv 1\ (n)$ ✓.

es: $5^{12} \equiv 1 \ (72)$ come lo vedo senza tuccco?

diviso:

$$\begin{cases} 5^{12} \equiv 1 \ (2) \\ 5^{12} \equiv 1 \ (3) \\ 5^{12} \equiv 1 \ (7) \end{cases}$$

Fermat:

$$\begin{cases} 5^{1} \equiv 1 \ (2) \\ 5^{2} \equiv 1 \ (3) \\ 5^{6} \equiv 1 \ (7) \end{cases}$$

tutto funziona bene perché sono primi distinti:
Quando si ripetono è un problema più difficile:

$99 = 7 \cdot 7$ diviso non si può applicare.

$2^{?} \equiv 1 \ (99)$ $\quad 99 = 7 \cdot 7$ $\quad \phi(99) = \phi(7^2)$

$7^2 - 7 = 42$

$2^{42} \equiv 1 \ (99)$ ma grazie al teorema diviso

dimostrazione:

$a^{p^2-p} \equiv 1 \ (p^2)$ $\quad p$ primo $(a,p) = 1$.

$a^{p-1} \equiv 1 \ (p)$ per Fermat.

$a^{p-1} = 1 + pk$

$$a^{p^2-p} = (a^{p-1})^p = (1+kp)^p = \sum_{i=0}^{p} \binom{p}{i} 1^{p-i} (kp)^i =$$

$$= \binom{p}{0} + \binom{p}{1}(kp)^1 + \binom{p}{2}(kp)^2 + \dots + \binom{p}{p}(kp)^p \equiv 1 \ (p^2)$$

$\binom{p}{0} = 1$ $\quad \binom{p}{p} = 1$

tutti multipli di p^2 e rimane solo il primo

teorema
$(a,b) = 1$

teorema cinese dei resti espresso in modo più astratto.

$F : \mathbb{Z}/(a,b) \longrightarrow \mathbb{Z}/(a) \times \mathbb{Z}/(b)$

$F([x]_{ab}) = \langle [x]_a , [x]_b \rangle$

classe di x mod (ab)

funziona biunivoca

es: $a=3 \quad b=5 \quad F: \mathbb{Z}/(15) \longrightarrow \mathbb{Z}/(3) \times \mathbb{Z}/(5)$

$F([7]_{15}) = \langle [7]_3 , [7]_5 \rangle$

$= \langle [1]_3 , [2]_5 \rangle$

15 classi

3 classi · 5 classi = 15 classi

F è iniettiva e surgettiva.

dimostriamo con $a=3$, $b=5$ (dimostriamo analogo con a, b qualsiasi)

prendo un qualsiasi elemento di $\mathbb{Z}/(3) \times \mathbb{Z}/(5)$

$\langle [a]_3 , [b]_5 \rangle$

devo trovare x tale che

$F([x]_{15}) = \langle [a]_3 , [b]_5 \rangle$

$\|$ def

$\langle [x]_3 , [x]_5 \rangle$ cioè voglio x tale che

$$\begin{cases} [x]_3 = [a]_3 \\ [x]_5 = [b]_5 \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv a(3) \\ x \equiv b(5) \end{cases}$$

per il teorema cinese dei resti si può risolvere sicuramente il sistema.

$\Rightarrow F$ è surgettiva

è inoltre raro perdere ho due insiemi con la stessa cardinalità (stesso numero di elementi).
Il teorema inverso dei resti dice che la soluzione del sistema è una sola mod( ).