

ARITMETICA.

Siamo $a, b \in \mathbb{Z}$. Un intero $d \in \mathbb{Z}$ si dice un **MASSIMO COMUNE DIVISORE** di a e b \Leftrightarrow $\begin{cases} d \mid a, d \mid b \\ \text{se } c \mid a, c \mid b \Rightarrow c \mid d \end{cases}$

$$\text{MCD}(a, b) = \text{MCD}(-a, b) = \text{MCD}(a, -b) = \text{MCD}(-a, -b)$$

Algoritmo euclideo delle divisioni successive

Vogliamo determinare il $\text{MCD}(a, b)$ con $a, b > 0$
TRAMITE LA DIVISIONE EUCLIDEA $a = b q_1 + r_1$

Se $r_1 \neq 0$ applico la divisione di b per r_1

$$b = r_1 q_2 + r_2 \rightarrow r_2 = r_1 q_3 + r_3 = 0$$

e così via.

Dopo un numero finito di passi si ottiene un resto $r_m = 0 \Rightarrow r_{m+1} = \text{MCD}(a, b)$

Th. di Bezout

Siamo $a, b \in \mathbb{Z}$ e sia $d = \text{MCD}(a, b)$. Allora esistono $\alpha, \beta \in \mathbb{Z}$ tali che

$$d = \alpha a + \beta b$$

Una coppia così fatta (α, β) si dice **COPPIA DI COEFFICIENTI DI BEZOUT**

Def. Siano $a, b \in \mathbb{Z}$. Un intero $m \in \mathbb{Z}$ si dice **MINIMO COMUNE MULTIPLO** di a e b \Leftrightarrow

$$\begin{cases} a \mid m \quad \& \quad b \mid m \\ \text{se } a \mid c \quad \& \quad b \mid c \Rightarrow m \mid c \end{cases}$$

Esercizio

Utilizzando l'algoritmo euclideo delle divisioni successive, determinare $\text{MCD}(-363, 770)$

$$\text{MCD}(-363, 770) = \text{MCD}(363, 770)$$

$$363 = \underbrace{770}_{a} \cdot \underbrace{0}_{b} + \underbrace{363}_{r_1}$$

Ora si passa alla divisione tra b ed r_1

$$770 = \underbrace{363}_{r_1} \cdot \underbrace{2}_{q_1} + \underbrace{44}_{r_2}$$

$$363 = \underbrace{44}_{r_2} \cdot \underbrace{8}_{q_2} + \underbrace{11}_{r_3}$$

$$r_3 = 0 \Rightarrow r_4 = 11 = \text{MCD}(-363, 770)$$

$$\text{ad} \approx 2 \quad 363 = \underbrace{44}_{\textcircled{5}} \cdot 8 + \underbrace{11}_{\textcircled{0}}$$

$$44 = \underbrace{11}_{\textcircled{5}} \cdot 4 + \underbrace{0}_{\textcircled{0}}$$

Esercizio $a \ b$
 $\text{MCD}(100, 45)$

$$100 = \underbrace{45}_{\textcircled{5}} \cdot 2 + \underbrace{10}_{\textcircled{2}}$$

$$\rightarrow 45 = \underbrace{10}_{\textcircled{2}} \cdot 4 + \underbrace{5}_{\textcircled{1}}$$

$$10 = 5 \cdot 2 + 0$$

$$\text{MCD}(100, 45) = 5$$

$$5 = \alpha \cdot 100 + \beta \cdot 45$$

$$5 = 45 + 10 \cdot (-4) = 45 + [100 + 45(-2)](-4) =$$

$$= 45 + 100(-4) + 45 \cdot 8 = (-4) \cdot 100 + 9 \cdot 45$$

$$\begin{aligned} \alpha &= -4 \\ \beta &= 9 \end{aligned} \quad (-4, 9)$$

Esercizio

Det MCD(731, 250) è una coppia di coeff. di Bezout:

$$731 = 731 + 250(-2) \quad \leftarrow 731 = \underbrace{250}_{\textcircled{1}} \cdot 2 + \underbrace{731}_{\textcircled{2}}$$

$$19 = 250 + 731 \cdot (-1) \quad \leftarrow 250 = \underbrace{731}_{\textcircled{2}} \cdot 1 + \underbrace{19}_{\textcircled{1}}$$

$$3 = 731 + 19(-12) \quad \leftarrow 731 = \underbrace{19}_{\textcircled{1}} \cdot 12 + 3$$

$$1 = 19 + 3(-6) \quad \leftarrow 19 = \underbrace{3}_{\textcircled{1}} \cdot 6 + 1$$

$$3 = 1 \cdot 3 + 0$$

$$\Rightarrow \text{MCD}(731, 250) = 1$$

$$1 = \alpha \cdot 731 + \beta \cdot 250$$

$$1 = 19 + 3(-6) = 19 + [731 + 19 \cdot (-12)] \cdot (-6) = 19 + 731 \cdot (-6) + 19 \cdot (72) =$$

$$= 231 \cdot (-6) + 19 \cdot 73 = 231 \cdot (-6) + \underbrace{[250 + 731(-1)]}_{19} \cdot 73 = 231 \cdot (-6) + 250 \cdot 73 + 231 \cdot (-73) =$$

$$= 231 \cdot (-79) + 250 \cdot 73 =$$

$$= [\underbrace{731 + 250 \cdot (-2)}_{19}] \cdot (-79) + 250 \cdot 73 =$$

$$= 731 \cdot (-79) + 250 \cdot 231$$

$$1 = \alpha \cdot 731 + \beta \cdot 250$$

$$\alpha = -79 \quad \beta = 231 \quad (-79, 231)$$

ESERCIZIO

$\text{MCD}(1716, -7040)$ è una copia di coeff di Bezout

$$\text{MCD}(1716, -7040) = \text{MCD}(1716, 7040)$$

$$7040 = 1716 \cdot 4 + 176$$

$$1716 = 176 \cdot 9 + 132$$

$$176 = 132 \cdot 1 + 44$$

$$132 = 44 \cdot 3 + 0$$

$$\Rightarrow \text{MCD}(1716, -7040) = 44$$

$$44 = \alpha \cdot 1716 + \beta (-7040)$$

$$44 = 176 + 1716 \cdot (-1) =$$

$$= 176 + [1716 + 176 \cdot (-9)] \cdot (-1) = 176 + 1716 \cdot (-1) + 176 \cdot 9$$

$$= 176 \cdot 10 + 1716 \cdot (-1) =$$

$$= [7040 + 1716 \cdot (-4)] \cdot 10 + 1716 \cdot (-1) =$$

$$= 7040 \cdot 10 + 1716 \cdot (-40) + 1716 \cdot (-1) =$$

$$= 7040 \cdot 10 + 1716 \cdot (-41)$$

$$= (-7040) \cdot (-10) + 1716 \cdot (-41)$$

$$\boxed{\begin{array}{l} \alpha = -41 \\ \beta = -10 \end{array}}$$

$$(-41, -10)$$

EQ. CON GRUENZIAU

diamo $a, m, b \in \mathbb{Z}$. Diziamo che $a \equiv b$ modulo m

$$a \equiv_m b$$

$$\Leftrightarrow m | a - b$$

è una relazione in \mathbb{Z} ; in particolare è una relazione di equivalenza.

$$[a]_{\equiv_m} = [a]_m = \{x \in \mathbb{Z} : a \equiv_m x\} = \{x \in \mathbb{Z} : m | a - x\} =$$

$$= \{x \in \mathbb{Z} : a - x = mq \quad q \in \mathbb{Z}\} =$$

$$= \{x \in \mathbb{Z} : x = a - mq \quad q \in \mathbb{Z}\} = \{a - mq : q \in \mathbb{Z}\} = \{a + mq : q \in \mathbb{Z}\}$$

$$[1]_m = \{1, 6, 11, \dots\}$$

$$q \wedge c \cdot c = \underline{a - mq} \quad q \in \mathbb{Z} \quad q \in \mathbb{Z} - \mathbb{Z}q + mq : q \in \mathbb{Z}$$

$$[1]_5 = \{1, 6, 11, \dots\}$$

PROPOSIZIONE

$$a \equiv_m b \quad \text{e} \quad c \equiv_m d \Rightarrow \begin{bmatrix} a+c \equiv_m b+d \\ a \cdot c \equiv_m b \cdot d \end{bmatrix}$$

Un'equazione congruenziale lineare è un'equazione del tipo:
 $a \cdot x \equiv_m b \pmod{m}$

HA SOLUZIONI $\Leftrightarrow \frac{\text{MCD}(a, m)}{d} \mid b$

La soluzione è data da $k \cdot d$ dove $k = \frac{b}{\frac{\text{MCD}(a, m)}{d}}$ e d : 1° coeff di Bézout

Th. 1

l'eq. $a \cdot x \equiv_m b$ cond = $\text{MCD}(a, m)$ divide b , è equivalente a

$$\frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

Th. 2 se $c \in \mathbb{Z}$ è soluzione dell'equazione allora ogni $s \in [c]_m$ è soluzione dell'equazione.

Th. CHINESE DEL RESTO

Un sistema

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_t \pmod{m_t} \end{cases}$$

e cioè ammette soluzione, per essere compatibile i moduli devono essere a 2 a 2 coprimi cioè $\text{MCD}(m_i, m_j) = 1$

Inoltre se $c \in \mathbb{Z}$ è soluzione del sistema, tutti gli elementi in $[c]_{m_1 \cdot m_2 \cdots m_t}$ saranno soluzione del sistema.

Esercizio.

Determinare tutte le soluzioni dell'equazione

$$121x \equiv 77 \pmod{22}$$

$$\left(\begin{array}{l} a \cdot x \equiv b \pmod{m} \\ \text{MCD}(a, m) \mid b \end{array} \right)$$

Iniziamo vediamo se l'equazione è compatibile, e cioè se $\text{MCD}(121, 22) \mid 77$

$$\text{MCD}(121, 22)$$

$$121 = 22 \cdot 5 + 11 \quad \left(\begin{array}{l} \\ \\ \end{array} \right) \Rightarrow \text{MCD}(121, 22) = 11$$

$$22 = 11 \cdot 2 + 0$$

Dato che $11 \mid 77$ allora l'eq. è compatibile cioè ammette soluzioni.

Per il Th. 1) l'equazione iniziale è equivalente a:

$$\frac{11x \equiv 7 \pmod{2}}{a b m}$$

La soluzione dell'equazione è data da $c = \alpha \cdot k$ dove α : 1° coeff. di Bézout e $k = \frac{b}{\text{MCD}(a, m)}$

$$\text{MCD}(a, m) = \text{MCD}(11, 2)$$

$$\begin{aligned} \textcircled{*} \quad 11 &= 2 \cdot 5 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned} \quad \Rightarrow \text{MCD}(11, 2) = 1 \quad \Rightarrow k = \frac{1}{1} = 1 \quad \Rightarrow c = \alpha \cdot k = 1$$

$$1 = \alpha \cdot 11 + \beta \cdot 2$$

$$\textcircled{*} \Rightarrow 1 = 11 + 2(-5) \Rightarrow \alpha = 1^{\circ} \text{ coeff. di Bézout} = 1$$

Quindi $c=1$ è una soluzione dell'equazione $11x \equiv 7 \pmod{2}$

Per il Th. 2) tutte le soluzioni di $11x \equiv 7 \pmod{2}$ costituiscono la classe $[7]_2 \subset \{7 + 2 \cdot q : q \in \mathbb{Z}\}$

Esercizio

Si determinino tutte le soluzioni POSITIVE dell'eq. congruenza

$$\frac{84x \equiv 108 \pmod{500}}{a b m}$$

$$\text{MCD}(84, 500)$$

$$\begin{aligned} 500 &= 84 \cdot 5 + 80 \\ 84 &= 80 \cdot 1 + 4 \\ 80 &= 4 \cdot 20 + 0 \end{aligned} \quad \Rightarrow \text{MCD}(84, 500) = 4 \text{ che divide } 108$$

\Rightarrow l'eq. è compatibile ed è equivalente a

$$\frac{21x \equiv 27 \pmod{125}}{a b m}$$

$$\text{MCD}(21, 125)$$

$$\begin{aligned} c &= \alpha \cdot k \\ k &= \frac{b}{\text{MCD}(a, m)} = \frac{27}{1} = 27 \end{aligned}$$

$$\begin{aligned} \textcircled{1} \quad 125 &= 21 \cdot 5 + 20 \\ \textcircled{2} \quad 21 &= 20 \cdot 1 + 1 \end{aligned} \quad \Rightarrow \text{MCD}(21, 125) = 1$$

$$\textcircled{2} \quad 21 = \underline{20} \cdot 1 + \underline{1} \quad \left. \begin{array}{l} \\ \end{array} \right) \Rightarrow \text{NCD}(21, 125) = 1$$

$$20 = 1 \cdot 20 + 0 \qquad \qquad \qquad 1 = \alpha \cdot 21 + \beta \cdot 125$$

$$\textcircled{3} \Rightarrow 1 = 21 + 20 \cdot (-1) = 21 + (125 + 21 \cdot (-5)) \cdot (-1) =$$

$$= 21 + 125 \cdot (-1) + 21 \cdot (5) = \textcircled{6} \cdot 21 + (-1) \cdot 125$$

$\rightarrow \bar{\epsilon} \alpha$

\Rightarrow una soluzione

$$\text{dell' eq. } \bar{x} = \underset{\alpha}{\overset{6}{\uparrow}} \cdot \underset{\beta}{\overset{27}{\uparrow}} = 162$$

Tutte le soluzioni costituiscono

$$[162]_{125} = \{162 + 125 \cdot q : q \in \mathbb{Z}\}$$

Le soluzioni positive si fanno per $q \geq -1$.