ESERCIZIO N. 2 Sia $n>0$ e siano $a,b,c \in \mathbb{Z}$. Valgono le seguenti uguaglianze:

(1) $([a]_n+[b]_n)+[c]_n \overset{?}{=} [a]_n+([b]_n+[c]_n)$ PROPRIETÀ ASSOCIATIVA DELLA SOMMA SU $\mathbb{Z}/n\mathbb{Z}$

$$([a]_n+[b]_n)+[c]_n = [a+b]_n+[c]_n = [(a+b)+c]_n = [a+b+c]_n = [a+(b+c)]_n = [a]_n+[b+c]_n = [a]_n+([b]_n+[c]_n)$$

$\mathbb{Z} \rightsquigarrow \mathbb{Z}/n\mathbb{Z}$

PER CASO VEDERE LE ALTRE

⋮

(5) $[a]_n+[0]_n = [0]_n+[a]_n = [a]_n$ ESISTENZA DELL'ELEMENTO NEUTRO DELLA SOMMA, CIOÈ DELLO ZERO di $\mathbb{Z}/n\mathbb{Z}$.

$$[a]_n+[0]_n = [a+0]_n = [a]_n \qquad [0]_n+[a]_n = [0+a]_n = [a]_n$$

.

(7) $[a]_n[1]_n = [a\cdot 1]_n = [a]_n = [1]_n[a]_n$ ESISTENZA DELL'ELEMENTO NEUTRO DELLA MOLTIPLICAZIONE, CIOÈ DELL'UNITÀ DI $\mathbb{Z}/n\mathbb{Z}$

(8) $[a]_n([b]_n+[c]_n) = [a]_n[b]_n+[a]_n[c]_n$

OSSERVAZIONE 11.18

(1) $m = 6$ $\qquad \underset{\neq [0]_6}{[2]_6} \cdot \underset{\neq [0]_6}{[3]_6} = [2 \cdot 3]_6 = [6]_6 = [0]_6$

(2) $n > 0$ qualsiasi $\qquad \overbrace{[1]_n + [1]_n + [1]_n + \dots + [1]_n}^{n\text{-volte}} = [n]_n = [0]_n$

IL TEOREMA CINESE DEL RESTO (p. 32)

TEOREMA 12.1 (TEOREMA CINESE DEL RESTO)

Siano $n, m > 0$ e siano $a, b \in \mathbb{Z}$. Consideriamo il seguente sistema di congruenze

$$\begin{cases} x \in \mathbb{Z} \\ x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases} \quad \text{o equivalentemente} \quad \begin{cases} x \in \mathbb{Z} \\ [x]_n = [a]_n \\ [x]_m = [b]_m \end{cases}$$

Sia S l'insieme delle soluzioni del precedente sistema ovvero

$$S = \{ x \in \mathbb{Z} \mid x \equiv a \pmod{n} \text{ e } x \equiv b \pmod{m} \}.$$

Allora il precedente sistema è COMPATIBILE, cioè ammette almeno una soluzione, cioè $S \neq \emptyset$ se e soltanto se

$$(n, m) \mid a - b.$$

Se $S \neq \emptyset$ e $c \in S$, allora

$$S = [c]_{[n,m]} = \{ c + k[n,m] \in \mathbb{Z} \mid k \in \mathbb{Z} \}.$$

DIM. COMPATIBILITÀ Dobbiamo provare che

$$S \neq \emptyset \iff (n,m) \mid a-b.$$

$\Rightarrow$) Supp. che $S \neq \emptyset$. Scegliamo $c \in S$, ovvero $c \equiv a \pmod{n}$ e $c \equiv b \pmod{m}$, ovvero $\exists\, k,h \in \mathbb{Z}$ t.c. $c = a+kn$ e $c = b+hm$

$$\Rightarrow \left(\underline{a+kn} = \cancel{c} = \underline{b+hm} \iff a-b = -kn+hm \right)$$

Lemma utile (Lezione 01-04-2021)

Ricordando che $(n,m) \mid n$ e $(n,m) \mid m \Rightarrow (n,m) \mid a-b$

$\Leftarrow$) Supp. che $(n,m) \mid a-b$, ovvero $\exists\, k \in \mathbb{Z}$ t.c. $\underline{a-b = k(n,m)}$. (1)

Grazie all'alg. di Euclide con sostituzione "a ritroso", $\exists\, r,s \in \mathbb{Z}$

$$\underline{(n,m) = rn+sm} \quad (2)$$

Da (1) e (2), segue che $a-b \overset{(1)}{=} k(n,m) \overset{(2)}{=} k(rn+sm) = (kr)n+(ks)m$

$$\Leftrightarrow \quad a-b = (kr)n + (ks)m$$

$$\Updownarrow$$

$$c := a - krn = b + ksm$$

$$\Rightarrow \quad \begin{array}{l} c = a - krn \Rightarrow c \equiv a \pmod{n} \\ c = b + ksm \Rightarrow c \equiv b \pmod{m} \end{array} \Bigg\} \Rightarrow c \in S.$$

$$\begin{cases} x \in \mathbb{Z} \\ x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

$$\Updownarrow$$

$$\begin{cases} x \in \mathbb{Z} \\ [x]_n = [a]_n \\ [x]_m = [b]_m \end{cases}$$

INSIEME DELLE SOLUZIONI S Dobbiamo provare che $S = [c]_{[n,m]} \subset \mathbb{Z}$, dove $c \in S$.

$S \subset [c]_{[n,m]}$ Sia $c' \in S$. Poiché $c \in S$, valgono:

- $c \equiv a \pmod{n} \Leftrightarrow c = a + kn$ per qualche $k \in \mathbb{Z}$
- $c \equiv b \pmod{m} \Leftrightarrow c = b + hm$ .... $h \in \mathbb{Z}$
- $c' \equiv a \pmod{n} \Leftrightarrow c' = a + k'n$ ...... $k' \in \mathbb{Z}$
- $c' \equiv b \pmod{m} \Leftrightarrow c' = b + h'm$ ...... $h' \in \mathbb{Z}$

$c' - c = \cancel{a} - \cancel{a} + (k'-k)n$

$\Downarrow$

$n \mid c' - c$

$c' - c = \cancel{b} - \cancel{b} + (h'-h)m$

$\Downarrow$

$m \mid c' - c$

$$\Rightarrow \quad n \mid c'-c \quad e \quad m \mid c'-c \quad \xRightarrow[\text{m.c.m}]{\text{per definizione di}} \quad [n,m] \mid c'-c$$

$$\Updownarrow$$

$$c' \in [c]_{[n,m]} \quad \Longleftrightarrow \quad c' \equiv c \pmod{[n,m]}$$

$$\Rightarrow \quad S \subset [c]_{[n,m]}. \quad \checkmark$$

$[c]_{[n,m]} \subset S$ Sia $c' \in [c]_{[n,m]}$, ovvero $c' = c + k[n,m]$ per qualche $k \in \mathbb{Z}$.

$$\Rightarrow [c']_n = [c + k[n,m]]_n = [c]_n + [k]_n [[n,m]]_n =$$

$$= [a]_n + [k]_n [0]_n =$$

$$= [a + k \cdot 0]_n = [a]_n$$

$$\Rightarrow [c']_m = [c + k[n,m]]_m = [c]_m + [k]_m [[n,m]]_m =$$

$$= [b]_m + [k]_m [0]_m = [b + k \cdot 0]_m = [b]_m$$

$$\Rightarrow c' \in S \Longrightarrow [c]_{[n,m]} \subset S.$$

Appello del 21/06/2016

ESERCIZIO 2 Si determinino tutte le soluzioni del seguente sistema di congruenze

$\cancel{x \in \mathbb{Z}}$

$$\begin{cases} x \equiv 33 \pmod{77} \\ x \equiv -2 \pmod{56} \end{cases}$$

Si dimostri inoltre che tutte le soluzioni di tale sistema sono divisibili per 11.

SOLUZ. Sia S l'insieme delle soluzioni del sistema. Calcoliamo S.

PASSO 1: COMPATIBILITÀ Calcoliamo il MCD tra 77 e 56:

$$\begin{array}{r|l} 77 & 7 \\ 11 & 11 \\ 1 & \end{array} \quad 77 = 7 \cdot 11, \quad \begin{array}{r|l} 56 & 2 \\ 28 & 2 \\ 14 & 2 \\ 7 & 7 \\ 1 & \end{array} \quad 56 = 2^3 \cdot 7 \Rightarrow (77,56) = 7.$$

Poiché $(77,56) \mid 33-(-2) \iff 7 \mid 35$ ok, il teorema cinese del resto assicura che $S \neq \emptyset$, ovvero il sistema è compatibile.

Inoltre vale:

$$\underline{33-(-2)} = \cancel{5 \cdot 7} \cancel{=} \underline{5 \cdot (77,56)} \qquad (1)$$

PASSO 2. CALCOLO DI UNA SOLUZIONE C

Applichiamo l'algoritmo di Euclide a 77 e 56 con sostituz. "a ritroso":

$$\begin{array}{l|l}
77 = 1 \cdot 56 + 21 & 21 = 77 - 1 \cdot 56 \\
56 = 2 \cdot 21 + 14 & 14 = 56 - 2 \cdot 21 \\
21 = 1 \cdot 14 + \boxed{7} & 7 = 21 - 1 \cdot 14 = 21 - 1(56 - 2 \cdot 21) = \\
\cancel{14 = 2 \cdot 7 + 0} & = 3 \cdot 21 - 56 = 3(77-56) - 56 = \\
 & = 3 \cdot 77 - 4 \cdot 56
\end{array}$$

Dunque: $\underline{(77,56)} \cancel{=} \cancel{7} = \underline{3 \cdot 77 - 4 \cdot 56}$. (2)

Dalla (1) e dalla (2), segue che:

$$33-(-2) \overset{(1)}{=} 5\cdot(77,56) \overset{(2)}{=} 5\,(3\cdot 77-4\cdot 56) =$$

$$= 15\cdot 77 - 20\cdot 56,$$

ovvero

$$33-(-2) = 15\cdot 77 - 20\cdot 56. \qquad (3)$$

Segue che

$$33-15\cdot 77 = -2-20\cdot 56$$

$$c := -1122 \qquad\qquad -1122,$$

ovvero $c=-1122 \in S$.

$$33-(-2)=5\cdot(77,56) \quad (1)$$

$$(77,56)=3\cdot 77-4\cdot 56 \quad (2)$$

$$\begin{cases} x\equiv 33 \pmod{77} \\ x\equiv -2 \pmod{56} \end{cases}$$

ESERCIZIO

$$33-(-2)=15\cdot 77-20\cdot 56$$

$$\begin{cases} x\equiv -33 \pmod{56} \\ x\equiv 2 \pmod{77} \end{cases}$$

PASSO 3: INSIEME DELLE SOLUZIONI

Calcoliamo $[77, 56]$:

$$[77,56] = \frac{77\cdot 56}{(77,56)} = \frac{77\cdot 56}{7} = 616.$$

Grazie al teorema cinese del resto, vale

$$S = [-1122]_{616} = \{\overset{110}{\cancel{-1122}} + k\cdot 616 \in \mathbb{Z} \mid k\in\mathbb{Z}\}$$

$$\| $$

$$[-1122+616]_{616} = [-1122+2\cdot 616]_{616} = [110]_{616} \subset \mathbb{Z}$$

$$110 \equiv 33 \pmod{77}$$

$$\Updownarrow$$

$$77 \mid 110-33=77 \ \checkmark$$

$$110 \equiv -2 \pmod{56}$$

$$\Updownarrow$$

$$56 \mid 110-(-2) = 112 = 2\cdot 56 \ \checkmark$$