ALGEBRA 1 PB-Z
EXTRA I. 6 IV 2012

Esercizio 1. I. Descrivere $\mathbb{Z} / \equiv_0$ e $\mathbb{Z} / \equiv_1$ come *insiemi*; **II.** dire se le operazioni di somma e prodotto su $\mathbb{Z}$ inducono analoghe operazioni su $\mathbb{Z} / \equiv_0$ e $\mathbb{Z} / \equiv_1$; **III.** dire se $\mathbb{Z} / \equiv_0$ e $\mathbb{Z} / \equiv_1$ ammettono una struttura di gruppo additivo; **IV.** dire se $\mathbb{Z} / \equiv_0$ e $\mathbb{Z} / \equiv_1$ ammettono una struttura di anello commutativo unitario.

Soluzione. In quanto segue, per denotare la classe di equivalenza modulo $\equiv_0$ o modulo $\equiv_1$ ([1]) di un intero $a \in \mathbb{Z}$ scriveremo $\overline{a}$.

I. caso 0 Per ogni $a_1, a_2 \in \mathbb{Z}$ si ha $a_1 \equiv_0 a_2$ se e solo se esiste $q \in \mathbb{Z}$ tale che $a_1 = a_2 + q0$; ossia, se e solo se $a_1 = a_2$. Pertanto, la relazione di equivalenza $\equiv_0$ coincide con la relazione **diagonale** $\{(a,a) | a \in \mathbb{Z}\} \subset \mathbb{Z} \times \mathbb{Z}$. Da qui segue che la classe di equivalenza modulo $\equiv_0$ di un elemento $a \in \mathbb{Z}$ è $\overline{a} = \{a\} \in \mathcal{P}(\mathbb{Z})$. Quindi([2])

$$(\mathbb{Z} / \equiv_0) \ = \ \{ \ \overline{a} \mid a \in \mathbb{Z} \ \} \ = \ \{ \ \{a\} \mid a \in \mathbb{Z} \ \} \ \cong \ \mathbb{Z}.$$

I. caso 1. Per $a_1, a_2 \in \mathbb{Z}$ si ha $a_1 \equiv_1 a_2$ se e solo se esiste $q \in \mathbb{Z}$ tale che $a_1 = a_2 + q1$; ossia, se e solo se esiste $q \in \mathbb{Z}$ tale che $a_1 = a_2 + q$. Ora, poiché dati comunque $a_1, a_2 \in \mathbb{Z}$, essendo $(\mathbb{Z}, +)$ un gruppo, un tale q esiste sempre (è $q = a_1 - a_2$), la relazione di equivalenza $\equiv_1$ coincide con la relazione **totale** $\{(a,b) | a, b \in \mathbb{Z}\} \subset \mathbb{Z} \times \mathbb{Z}$. Da qui segue che la classe di equivalenza modulo $\equiv_1$ di un (anzi, ogni!) elemento $a \in \mathbb{Z}$ è $\overline{a} = \mathbb{Z} \in \mathcal{P}(\mathbb{Z})$. Quindi

$$(\mathbb{Z} / \equiv_0) \ = \ \{ \ \overline{a} \mid a \in \mathbb{Z} \ \} \ = \ \{ \ \mathbb{Z} \ \} \ \cong \ \{\text{un punto}\}.$$

II. La risposta è **sì** in entrambi i casi (per verificare questo fatto si può procedere esattamente come nel caso della relazione di congruenza modulo $m \in \mathbb{Z}$, $|m| \geq 2$).

II.bis. caso 0. Osserviamo che l'addizione e il prodotto che le operazioni su $\mathbb{Z}$ inducono su

$$(\mathbb{Z} / \equiv_0) \ \cong \ \mathbb{Z}$$

coincidono con le operazioni di somma e prodotto naturalmente definite sull'insieme $\mathbb{Z}$ alla destra della precedente "uguaglianza" tra insiemi.

III-IV. caso 0. Per quanto detto appena sopra, $((\mathbb{Z} / \equiv_0), +)$ è un gruppo additivo e $((\mathbb{Z} / \equiv_0), +, \times)$ è un anello commutativo unitario.

---

[1] La paragrafazione sarà tale da impedire ogni confusione tra i due casi.

[2] In quanto segue il simbolo $\cong$ significa *esiste una corrispondenza biunivoca tra* **insiemi**.

III-IV. caso 1. L'insieme $(\mathbb{Z} \,/\, \equiv_1)$, possedendo un solo elemento, ammette un'unica struttura di gruppo. Infatti, denotando $\diamond$ l'unico elemento di $(\mathbb{Z} \,/\, \equiv_1)$, si scriva $(\mathbb{Z} \,/\, \equiv_1) = \{\diamond\}$ e si osservi che, allora, l'unica operazione binaria che è possibile definire su $\{\diamond\}$ è

$$\begin{array}{ccccc} \star & : & \{\diamond\} \times \{\diamond\} & \to & \{\diamond\} \\ & & (\diamond, \diamond) & \mapsto & \diamond \end{array}$$

È immediato verificare che la coppia $(\{\diamond\}, \star)$; ossia, $((\mathbb{Z} \,/\, \equiv_1), \star)$, forma un gruppo, tutte le condizioni della definizione di gruppo essendo soddisfatte. Ora, per l'unicità di $\star$, abbiamo

$$((\mathbb{Z} \,/\, \equiv_1), \star) \;=\; ((\mathbb{Z} \,/\, \equiv_1), +)$$

e, quindi, l'insieme $(\mathbb{Z} \,/\, \equiv_1)$ ammette una (unica) struttura di gruppo, come volevasi dimostrare.

D'altra parte, $\mathbb{Z} \,/\, \equiv_1$ **non** ammette alcuna struttura di anello (commutativo) unitario. Per provare questo fatto, basta osservare che la cardinalità dell'insieme $(\mathbb{Z} \,/\, \equiv_1)$ è uguale a 1, mentre un qualsiasi anello unitario A ha cardinalità almeno pari a 2 ([3]).

[3] A deve contenere almeno 0_A e $1_A \neq 0_A$.

Esercizio 2. Sia $m \in \mathbb{Z}$, $m \geq 2$ un intero fissato. Si mostri che $\mathbb{Z} \,/\, \equiv_m$ è un anello commutativo unitario.

Soluzione. In quanto segue, per denotare la classe di equivalenza modulo $\equiv_m$ di un intero $a \in \mathbb{Z}$, scriveremo $[a]$.

$(\mathbb{Z} \,/\, \equiv_m, +)$ è un gruppo commutativo.

La somma è associativa. Dati comunque $a_1, a_2, a_3 \in \mathbb{Z}$, risulta

$$([a_1] + [a_2]) + [a_3] = [a_1] + ([a_2] + [a_3]).$$

Infatti

$$\begin{array}{rcl} ([a_1] + [a_2]) + [a_3] & = & [(a_1 + a_2)] + [a_3] \\ & = & [(a_1 + a_2) + a_3] \\ & = & [a_1 + (a_2 + a_3)] \\ & = & [a_1] + [(a_2 + a_3)] \\ & = & [a_1] + ([a_2] + [a_3]). \end{array}$$

Esistenza di un elemento neutro. Dato comunque $a \in \mathbb{Z}$, risulta

$$[a] + [0] = [a] \quad \text{e} \quad [0] + [a] = [a].$$

Infatti $[a] + [0] = [a + 0] = [a]$ e $[0] + [a] = [0 + a] = [a]$.

Esistenza dell'opposto di ogni elemento. Dato comunque $a \in \mathbb{Z}$, esiste $u \in \mathbb{Z}$ tale che

$$[a] + [u] = [0].$$

Infatti basta prendere $u = -a$, 'ché, allora,

$$[a] + [u] = [a] + [-a] = [a + (-a)] = [a - a] = [0].$$

La somma è commutativa. Dati comunque $a_1, a_2 \in \mathbb{Z}$, risulta

$$[a_1] + [a_2] = [a_2] + [a_1].$$

Infatti, $[a_1] + [a_2] = [a_1 + a_2] = [a_2 + a_1] = [a_2] + [a_1]$.

$(\mathbb{Z} \,/\, \equiv_m, \times)$ è un monoide commutativo.

Il prodotto è associativo. Dati comunque $a_1, a_2, a_3 \in \mathbb{Z}$, risulta

$$([a_1] \times [a_2]) \times [a_3] = [a_1] \times ([a_2] \times [a_3]).$$

Infatti

$$\begin{aligned}([a_1] \times [a_2]) \times [a_3] &= [(a_1 \times a_2)] \times [a_3] \\ &= [(a_1 \times a_2) \times a_3] \\ &= [a_1 \times (a_2 \times a_3)] \\ &= [a_1] \times [(a_2 \times a_3)] \\ &= [a_1] \times ([a_2] \times [a_3]).\end{aligned}$$

Esistenza di un elemento neutro. Dato comunque $a \in \mathbb{Z}$, risulta

$$[a] \times [1] = [a] \quad \text{e} \quad [1] \times [a] = [a].$$

Infatti $[a] \times [1] = [a \times 1] = [a]$ e $[1] \times [a] = [1 \times a] = [a]$.

Il prodotto è commutativo. Dati comunque $a_1, a_2 \in \mathbb{Z}$, risulta

$$[a_1] \times [a_2] = [a_2] \times [a_1].$$

Infatti, $[a_1] \times [a_2] = [a_1 \times a_2] = [a_2 \times a_1] = [a_2] \times [a_1]$.

Distributività del prodotto sulla somma. Dati comunque $a, a_1, a_2 \in \mathbb{Z}$, risulta

$$[a] \times ([a_1] + [a_2]) = [a] \times [a_1] + [a] \times [a_2].$$

Infatti

$$\begin{aligned}[a] \times ([a_1] + [a_2]) &= [a] \times [a_1 + a_2] \\ &= [a \times (a_1 + a_2)] \\ &= [a \times a_1 + a \times a_2] \\ &= [a \times a_1] + [a \times a_2] \\ &= [a] \times [a_1] + [a] \times [a_2].\end{aligned}$$

Esercizio 3. Risolvere le equazioni

$$\bigstar_1 \;\; 20\mathrm{X} \equiv_{30} 50; \qquad \bigstar_2 \;\; 81\mathrm{X} \equiv_{15} 6; \qquad \bigstar_3 \;\; 17\mathrm{X} \equiv_5 1.$$

Soluzione. In quanto segue, dati comunque $a, b \in \mathbb{Z}$, indicheremo con (a, b) l'unico **positivo** tra i massimi divisori comuni di a e b; cioè $\{(a, b)\} = \mathrm{MCD}(a, b) \cap \mathbb{N}$.

$\bigstar_1$. Poiché $(20, 30) = 10$ e $10|50$, l'equazione è compatibile. Il numero delle soluzioni che essa ammette è pari a $(20, 30)$; ossia, 10. Un'identità di Bezout per $(20, 30)$ è, ad esempio, la seguente, ottenuta dividendo 30 per 20 (si ha $30 = 1 \cdot 20 + 10$):

$$10 = 1 \cdot 30 + (-1) \cdot 20$$

Abbiamo allora

$$\begin{array}{rcl} 50 & = & 5 \cdot 10 \\ & = & 5 \cdot (1 \cdot 30 + (-1) \cdot 20) \\ & = & 5 \cdot 30 + (-5) \cdot 20 \end{array}$$

Quindi $50 \equiv_{30} (-5) \cdot 20$; ossia, $50 \equiv_{30} 20 \cdot (-5)$, così che -5 è una soluzione particolare di $\bigstar_1$.

Un sistema completo di soluzioni è, ad esempio, il seguente (scriviamo $3 = \frac{30}{10}$)

$$\{-5, -5{+}3, -5{+}2{\cdot}3, -5{+}3{\cdot}3, -5{+}4{\cdot}3, -5{+}5{\cdot}3, -5{+}6{\cdot}3, -5{+}7{\cdot}3, -5{+}8{\cdot}3, -5{+}9{\cdot}3\};$$

ossia,

$$\Sigma_1 = \{-5, -2, 1, 4, 7, 10, 13, 16, 19, 22\}.$$

Un altro sistema completo di soluzioni è, ad esempio,

$$\mathrm{S}_1 = \{1, 4, 7, 10, 13, 16, 19, 22, 25, 28\}.$$

Naturalmente, l'insieme delle classi resto modulo 30 degli elementi di Σ_1 e l'insieme delle classi resto modulo 30 degli elementi di S_1 coincidono.

$\bigstar_2$. Poiché $(81, 15) = 3$ e $3|6$, l'equazione è compatibile. Il numero delle soluzioni che essa ammette è pari a $(81, 15)$; ossia, 3. Un'identità di Bezout per $(81, 15)$ è, ad esempio, la seguente, ottenuta dividendo 81 per 15 (si ha $81 = 5 \cdot 15 + 6$) e, successivamente, 15 per 6 (si ha $15 = 2 \cdot 6 + 3$):

$$\begin{array}{rcl} 3 & = & 1 \cdot 15 + (-2) \cdot 6 \\ & = & 1 \cdot 15 + (-2) \cdot (81 - 5 \cdot 15) \\ & = & 11 \cdot 15 + (-2) \cdot 81. \end{array}$$

Abbiamo allora

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= 2 \cdot (11 \cdot 15 + (-2) \cdot 81) \\ &= 22 \cdot 15 + (-4) \cdot 81 \end{aligned}$$

Quindi $6 \equiv_{15} (-4) \cdot 81$; ossia, $6 \equiv_{30} 81 \cdot (-4)$, così che -4 è una soluzione particolare di $\bigstar_2$.

Un sistema completo di soluzioni è, ad esempio, il seguente (scriviamo $5 = \frac{15}{3}$)

$$\{-4, -4 + 5, -4 + 2 \cdot 5\};$$

ossia,

$$\Sigma_2 = \{-4, 1, 6\}.$$

Un altro sistema completo di soluzioni è, ad esempio,

$$\mathrm{S}_2 = \{1, 6, 11\}.$$

Naturalmente, l'insieme delle classi resto modulo 15 degli elementi di Σ_2 e l'insieme delle classi resto modulo 15 degli elementi di S_2 coincidono.

$\bigstar_3$. $17\mathrm{X} \equiv_5 1$ Poiché $(17, 5) = 1$ e $1|1$, l'equazione è compatibile. Il numero delle soluzioni che essa ammette è pari a $(17, 5)$; ossia, 1. Un'identità di Bezout per $(17, 5)$ è, ad esempio, la seguente, ottenuta dividendo 17 per 5 (si ha $17 = 3 \cdot 5 + 2$) e, successivamente, 5 per 2 (si ha $5 = 2 \cdot 2 + 1$):

$$\begin{aligned} 1 &= 1 \cdot 5 + (-2) \cdot 2 \\ &= 1 \cdot 5 + (-2) \cdot (17 - 3 \cdot 5) \\ &= 7 \cdot 5 + (-2) \cdot 17. \end{aligned}$$

Abbiamo allora

$$\begin{aligned} 1 &= 1 \cdot 1 \\ &= 1 \cdot (7 \cdot 5 + (-2) \cdot 17) \\ &= 7 \cdot 5 + (-2) \cdot 17 \end{aligned}$$

Quindi $1 \equiv_5 (-2) \cdot 17$; ossia, $1 \equiv_5 17 \cdot (-2)$, così che -2 è una soluzione particolare di $\bigstar_3$.

Un sistema completo di soluzioni è, ad esempio, il seguente (scriviamo $5 = \frac{5}{1}$)

$$\Sigma_3 = \{-2\}.$$

Un altro sistema completo di soluzioni è, ad esempio,

$$\mathrm{S}_3 = \{3\}.$$

Naturalmente, l'insieme delle classi resto modulo 5 degli elementi di Σ_3 e l'insieme delle classi resto modulo 5 degli elementi di S_3 coincidono.

Esercizio 4. Dire se i seguenti elementi sono invertibili oppure no:

$$\overline{3} \in \mathbb{Z}_5; \quad \overline{3} \in \mathbb{Z}_6; \quad \overline{17} \in \mathbb{Z}_{26}; \quad \overline{2} \in \mathbb{Z}_{2h}; \quad \overline{2} \in \mathbb{Z}_{2h+1}.$$

Soluzione. In quanto segue, dato comunque $m \in \mathbb{Z}$, per denotare la classe di equivalenza modulo $\equiv_m$ di un intero $a \in \mathbb{Z}$ scriveremo $\overline{a}$.

In quanto segue, dati comunque $a_1, a_2 \in \mathbb{Z}$, indicheremo con (a_1, a_2) l'unico **positivo** tra i massimi divisori comuni di a_1 e a_2, così che $\{(a_1, a_2)\} = \mathrm{MCD}(a_1, a_2) \cap \mathbb{N}$.

L'elemento $\overline{3} \in \mathbb{Z}_5$ **è** invertibile, essendo $(3, 5) = 1$.

Usando identità di Bezout, è possibile trovare l'inverso aritmetico di $\overline{3} \in \mathbb{Z}_5$. Infatti, da $5 = 1 \cdot 3 + 2$ e $3 = 1 \cdot 2 + 1$, abbiamo $1 = (-1) \cdot 5 + 2 \cdot 3$; ossia $1 \equiv_5 2 \cdot 3$. Così $\overline{2} \in \mathbb{Z}_5$ è l'inverso di $\overline{3}$ in $\mathbb{Z}_5$.

L'elemento $\overline{3} \in \mathbb{Z}_6$ **non è** invertibile, essendo $(3, 6) = 2 \neq 1$.

L'elemento $\overline{17} \in \mathbb{Z}_{26}$ **è** invertibile, essendo $(17, 26) = 1$.

Usando identità di Bezout, è possibile trovare l'inverso aritmetico di $\overline{17} \in \mathbb{Z}_{26}$. Infatti, da $26 = 1 \cdot 17 + 9$, $17 = 1 \cdot 9 + 8$ e $9 = 1 \cdot 8 + 1$, abbiamo $1 = 2 \cdot 26 + (-3) \cdot 17$; ossia $1 \equiv_2 6(-3) \cdot 17$. Così $\overline{-3} \in \mathbb{Z}_{26}$; ossia, $\overline{23} \in \mathbb{Z}_{26}$, è l'inverso di $\overline{17}$ in $\mathbb{Z}_{26}$.

L'elemento $\overline{2} \in \mathbb{Z}_{2h}$ **non è** invertibile. Infatti, poiché 2 divide ogni elemento di $\mathrm{MCD}(2, 2h)$, risulta $(2, 2h) \geq 2 \gneq 1$.

L'elemento $\overline{2} \in \mathbb{Z}_{2h+1}$ **è** invertibile; infatti, poiché 2 non appare nella fattorizzazione in primi degli elementi di $\mathrm{MCD}(2, 2h + 1)$, risulta $(2, 2h + 1) = 1$.

Usando identità di Bezout, è possibile trovare l'inverso aritmetico di $\overline{2} \in \mathbb{Z}_{2h+1}$. Infatti, da $2h+1 = h \cdot 2+1$, abbiamo $1 = 1 \cdot (2h+1)+(-h) \cdot 2$; ossia $1 \equiv_{2h+1} (-h) \cdot 2$. Così $\overline{-h} \in \mathbb{Z}_{2h+1}$; ossia, $\overline{h+1} \in \mathbb{Z}_{2h+1}$, è l'inverso di $\overline{2}$ in $\mathbb{Z}_{2h+1}$.

Esercizio 5. Risolvere i sistemi cinesi

$$\mathrm{K}_1 \begin{cases} \mathrm{X} \equiv_5 4 \\ \mathrm{X} \equiv_6 5 \\ \mathrm{X} \equiv_7 6 \end{cases} \qquad \mathrm{K}_2 \begin{cases} \mathrm{X} \equiv_5 2 \\ \mathrm{X} \equiv_6 5 \\ \mathrm{X} \equiv_{11} 6 \end{cases}$$

Soluzione. In quanto segue, dati comunque $a_1, a_2 \in \mathbb{Z}$, indicheremo con (a_1, a_2) l'unico **positivo** tra i massimi divisori comuni di a_1 e a_2, così che $\{(a_1, a_2)\} = \mathrm{MCD}(a_1, a_2) \cap \mathbb{N}$.

K_1.

Poiché $(5, 6) = 1$, $(5, 7) = 1$ e $(6, 7) = 1$, il sistema è compatibile.

Al sistema K_1 associamo i tre seguenti sistemi

$$\mathrm{K}_1^1 \begin{cases} \mathrm{X} \equiv_5 1 \\ \mathrm{X} \equiv_6 0 \\ \mathrm{X} \equiv_7 0 \end{cases} \qquad \mathrm{K}_1^2 \begin{cases} \mathrm{X} \equiv_5 0 \\ \mathrm{X} \equiv_6 1 \\ \mathrm{X} \equiv_7 0 \end{cases} \qquad \mathrm{K}_1^3 \begin{cases} \mathrm{X} \equiv_5 0 \\ \mathrm{X} \equiv_6 0 \\ \mathrm{X} \equiv_7 1 \end{cases}$$

Usando identità di Bezout per esprimere $(5, 6 \cdot 7) = 1$, $(6, 5 \cdot 7) = 1$ e $(7, 5 \cdot 6) = 1$, abbiamo

$$\begin{aligned} \kappa_1^1 \qquad 1 &= (17) \cdot 5 + (-2) \cdot (6 \cdot 7) \\ \kappa_1^2 \qquad 1 &= (6) \cdot 6 + (-1) \cdot (5 \cdot 7) \\ \kappa_1^3 \qquad 1 &= (13) \cdot 7 + (-3) \cdot (5 \cdot 6) \end{aligned}$$

Possiamo quindi affermare che,

grazie a κ_1^1, l'intero $-2 \cdot (6 \cdot 7)$; ossia, -84, è soluzione di K_1^1

grazie κ_1^2, l'intero $-1 \cdot (5 \cdot 7)$; ossia, -35, è soluzione di K_1^2

grazie κ_1^3, l'intero $-3 \cdot (5 \cdot 6)$; ossia, -90, è soluzione di K_1^3

Ne segue che l'intero

$$4 \cdot (-84) + 5 \cdot (-35) + 6 \cdot (-90);$$

ossia, -601, è soluzione del sistema originale K_1.

K_2.

Poiché $(5, 6) = 1$, $(5, 11) = 1$ e $(6, 11) = 1$, il sistema è compatibile.

Al sistema K_2 associamo i tre seguenti sistemi

$$\mathrm{K}_2^1 \begin{cases} \mathrm{X} & \equiv_5 & 1 \\ \mathrm{X} & \equiv_6 & 0 \\ \mathrm{X} & \equiv_{11} & 0 \end{cases} \qquad \mathrm{K}_2^2 \begin{cases} \mathrm{X} & \equiv_5 & 0 \\ \mathrm{X} & \equiv_6 & 1 \\ \mathrm{X} & \equiv_{11} & 0 \end{cases} \qquad \mathrm{K}_2^3 \begin{cases} \mathrm{X} & \equiv_5 & 0 \\ \mathrm{X} & \equiv_6 & 0 \\ \mathrm{X} & \equiv_{11} & 1 \end{cases}$$

Usando identità di Bezout per esprimere $(5, 6\cdot 11) = 1$, $(6, 5\cdot 11) = 1$ e $(11, 5\cdot 6) = 1$, abbiamo

$$\begin{aligned} \kappa_2^1 \qquad 1 &= (-13)\cdot 5 + (1)\cdot(6\cdot 11) \\ \kappa_2^2 \qquad 1 &= (-9)\cdot 6 + (1)\cdot(5\cdot 11) \\ \kappa_2^3 \qquad 1 &= (11)\cdot 11 + (-4)\cdot(5\cdot 6) \end{aligned}$$

Possiamo quindi affermare che,

grazie a κ_2^1, l'intero $1\cdot(6\cdot 11)$; ossia, 66, è soluzione di K_2^1
grazie a κ_2^2, l'intero $1\cdot(5\cdot 11)$; ossia, 55, è soluzione di K_2^2
grazie a κ_2^3, l'intero $-4(5\cdot 6)$; ossia, -120, è soluzione di K_2^3.

Ne segue che l'intero

$$2\cdot(66) + 5\cdot(55) + 6\cdot(-120);$$

ossia, -313, è soluzione del sistema originale K_2.

Esercizio 6. Risolvere i sistemi generali

$$\Gamma_1 \begin{cases} 4\mathrm{X} & \equiv_{22} & 2 \\ 3\mathrm{X} & \equiv_7 & 2 \end{cases} \qquad \Gamma_2 \begin{cases} 2\mathrm{X} & \equiv_6 & 2 \\ 3\mathrm{X} & \equiv_7 & 2 \\ 2\mathrm{X} & \equiv_8 & 4 \end{cases}$$

Soluzione. In quanto segue, dati comunque $a_1, a_2 \in \mathbb{Z}$, indicheremo con (a_1, a_2) l'unico **positivo** tra i massimi divisori comuni di a_1 e a_2; così che $\{(a_1, a_2)\} = \mathrm{MCD}(a_1, a_2) \cap \mathbb{N}$.

Γ_1.

Iniziamo osservando che $(4, 22) = 2$ divide 2, che $(3, 7) = 1$ divide 2 e che $(22, 7) = 1$.

Quindi Γ_1 è compatibile ed equivalente al sistema

$$\bar{\Gamma}_1 \begin{cases} 2\mathrm{X} & \equiv_{11} & 1 \\ 3\mathrm{X} & \equiv_7 & 2 \end{cases}$$

Un inverso aritmetico di 2 mod 11 è 6 ([4]).

Un inverso arimetico di 3 mod 7 è 5 ([5]).

Pertanto $\bar{\Gamma}_1$ e Γ_1 sono equivalenti al seguente sistema cinese

$$\bar{\mathrm{K}} \begin{cases} \mathrm{X} & \equiv_{11} & 6 \\ \mathrm{X} & \equiv_7 & 10 \end{cases}$$

che, come deve essere, è compatibile, essendo $(11, 7) = 1$.

Al sistema $\bar{\mathrm{K}}$ associamo i due seguenti sistemi

$$\bar{\mathrm{K}}^1 \begin{cases} \mathrm{X} & \equiv_{11} & 1 \\ \mathrm{X} & \equiv_7 & 0 \end{cases} \qquad \bar{\mathrm{K}}^2 \begin{cases} \mathrm{X} & \equiv_{11} & 0 \\ \mathrm{X} & \equiv_7 & 1 \end{cases}$$

Usando identità di Bezout per esprimere $(11, 7) = 1$, abbiamo

$$\bar{\kappa} \quad 1 = (2) \cdot 11 + (-3) \cdot 7$$

Possiamo quindi affermare che,

grazie a $\bar{\kappa}$, l'intero $-3 \cdot 7$; ossia, -21, è soluzione di $\bar{\mathrm{K}}^1$

grazie a $\bar{\kappa}$, l'intero $2 \cdot 11$; ossia, 22, è soluzione di $\bar{\mathrm{K}}^2$

Ne segue che l'intero

[4] Si può trovare un inverso usando identità di Bezout; qui osserviamo solo che $2 \cdot 6 = 12 \equiv_{11} 1$.

[5] Si può trovare un inverso usando identità di Bezout; qui ci osserviamo solo che $3 \cdot 5 = 15 \equiv_7 1$.

$$6 \cdot (-21) + 10 \cdot (11);$$

ossia, -16, è soluzione di $\bar{\mathrm{K}}$ e, quindi, del sistema originale Γ_1.

Γ_2.

Iniziamo osservando che $(2,6) = 2$ divide 2, che $(3,7) = 1$ divide 2, che $(2,8) = 2$ divide 4; che $(6,7) = 1$, che $(6,8) = \mathbf{2} \neq 1$, che $(7,8) = 1$.

Quindi, la semplice analisi dei moduli e dei coefficienti del sistema **non** ci permette di dire che il sistema Γ_2 è compatibile, **né**, d'altra parte, il contrario.

Procediamo, dunque, risolvendo le equazioni di Γ_2 una alla volta. Per comodità, ci riferiremo alla prima, alla seconda e alla terza equazione di Γ_2 scrivendo $\Gamma_{2,1}$, $\Gamma_{2,2}$ e, rispettivamente, $\Gamma_{2,3}$.

Iniziamo studiando la prima equazione del sistema; ossia

$$\Gamma_{2,1} \qquad 2\mathrm{X} \equiv_6 2.$$

Poiché $(2,6) = 2$ e $2|2$, l'equazione $\Gamma_{2,1}$ è compatibile. Il numero delle soluzioni che essa ammette è pari a $(2,6)$; ossia, 2. Un'identità di Bezout per $(2,6)$ è, ad esempio, la seguente, ottenuta dividendo 2 per 6 (si ha $2 = 0 \cdot 6 + 2$):

$$2 = (0) \cdot 6 + (1) \cdot 2$$

Abbiamo allora

$$2 = 1 \cdot 2 = 1 \cdot 1 \cdot 2 = 1 \cdot 2.$$

Quindi, $2 \equiv_6 1 \cdot 2$; ossia, $2 \equiv_6 2 \cdot 1$, così che 1 è una soluzione particolare dell'equazione $\Gamma_{2,1}$.

Un sistema completo di soluzioni di $\Gamma_{2,1}$ è, ad esempio, il seguente (scriviamo $3 = \frac{6}{2}$)

$$\{1, 1+3\};$$

ossia,

$$\{1, 4\}.$$

Ne segue che l'insieme di tutte le soluzioni di $\Gamma_{2,1}$ è $1 + 3\mathbb{Z}$; ossia, tutte e sole le soluzioni x di $\Gamma_{2,1}$ sono della forma $x = 1 + 3y$, con $y \in \mathbb{Z}$.

Procediamo, ora, sostituendo nella seconda equazione di Γ_2 una soluzione generica di $\Gamma_{2,1}$, cioè un intero x della forma $x = 1 + 3y$. Vediamo che, così facendo, l'espressione dell'equazione $\Gamma_{2,2}$ cambia. Infatti, da $3x \equiv_7 2$; ossia, da $3(1+3y) \equiv_7 2$, abbiamo $9y \equiv_7 2 - 3$; ossia, $9y \equiv_7 -1$.

Studiamo, dunque, la congruenza

$$\bar{\Gamma}_{2,2} \qquad 9\mathrm{Y} \equiv_7 -1.$$

Poiché $(9,7) = 1$ e $1|(-1)$, essa è compatibile. Il numero delle soluzioni che essa ammette è pari a $(9,7)$; ossia, 1. Un'identità di Bezout per $(9,7)$ è, ad esempio, la seguente, ottenuta dividendo 9 per 7 (si ha $9 = 1 \cdot 7 + 2$) e, successivamente, 7 per 2 (si ha $7 = 3 \cdot 2 + 1$):

$$1 = (4) \cdot 7 + (-3) \cdot 9$$

Abbiamo allora

$$-1 = (-1) \cdot 1 = (-1) \cdot (4 \cdot 7 - 3 \cdot 9);$$

ossia, $-1 = (-4) \cdot 7 + 3 \cdot 9$.

Quindi $-1 \equiv_7 3 \cdot 9$; ossia, $-1 \equiv_7 9 \cdot 3$, così che 3 è una soluzione particolare di $\bar{\Gamma}_{2,2}$.

Un sistema completo di soluzioni di tale equazione è, ad esempio, il seguente

$$\{3\}.$$

Ne segue che l'insieme di tutte le soluzioni di $\bar{\Gamma}_{2,2}$ è $3 + 7\mathbb{Z}$; ossia, tutte e sole le soluzioni y di $\bar{\Gamma}_{2,2}$ sono della forma $y = 1 + 7z$, con $z \in \mathbb{Z}$.

Da quanto detto sopra, possiamo dedurre che un intero x che soddisfa $\Gamma_{2,1}$ e $\bar{\Gamma}_{2,2}$; ossia, un intero x che soddisfa $\Gamma_{2,1}$ e $\Gamma_{2,2}$, è della forma $x = 1 + 3y$, con y della forma $y = 3 + 7z$, $z \in \mathbb{Z}$ perché soluzione di $\bar{\Gamma}_{2,2}$. Ne segue che la forma che un tale intero x deve avere è la seguente $x = 1 + 3y = 1 + 3(3 + 7z)$, $z \in \mathbb{Z}$; ossia

$$x = 10 + 21z, \quad \text{con} \quad z \in \mathbb{Z}.$$

Procediamo, ora, sostituendo nella terza equazione di Γ_2 una soluzione generica delle prime due equazioni; cioè un intero x della forma $x = 10 + 21z$. Vediamo che, così facendo, l'espressione dell'equazione $\Gamma_{2,3}$ cambia. Infatti, dda $2x \equiv_8 4$; ossia, da $2(10 + 21z) \equiv_8 4$; abbiamo $42z \equiv_8 4 - 20$; ossia, $42z \equiv_8 -16$; ossia, $42z \equiv_8 0$.

Studiamo, dunque, la congruenza

$$\bar{\Gamma}_{2,3} \qquad 42\mathrm{Z} \equiv_8 0.$$

Poiché $(42,8) = 2$ e $2|0$, essa è compatibile. Il numero delle soluzioni che essa ammette è pari a $(42,8)$; ossia, 2. Un'identità di Bezout per $(42,8)$ è, ad esempio, la seguente, ottenuta dividendo 42 per 8 (si ha $42 = 5 \cdot 8 + 2$):

$$2 = (-5) \cdot 8 + (1) \cdot 42$$

Abbiamo allora

$$0 = 0 \cdot 2 = 0 \cdot ((-5) \cdot 8 + 1 \cdot 42);$$

ossia, $0 = 0 \cdot 8 + 0 \cdot 42$.

Quindi $0 \equiv_8 0 \cdot 42$; ossia, $0 \equiv_8 42 \cdot 0$, così che 0 è una soluzione particolare di $\bar{\Gamma}_{2,3}$.

Un sistema completo di soluzioni di tale equazione è, ad esempio, il seguente (scriviamo $4 = \frac{8}{2}$)

$$\{0, 0+4\};$$

ossia,

$$\{0, 4\}.$$

Ne segue che l'insieme di tutte le soluzioni di $\bar{\Gamma}_{2,3}$ è $0 + 4\mathbb{Z}$; ossia, tutte e sole le soluzioni z di $\bar{\Gamma}_{2,3}$ sono della forma $z = 4u$, con $u \in \mathbb{Z}$.

Da quanto detto sopra, possiamo dedurre che un intero x che soddisfa $\Gamma_{2,1}$, $\bar{\Gamma}_{2,2}$ e $\bar{\Gamma}_{2,3}$; ossia, un intero x che soddisfa tutte e tre le equazioni $\Gamma_{2,1}$, $\Gamma_{2,2}$ e $\Gamma_{2,3}$ del sistema Γ_2, è della forma $x = 1 + 3y$, con y della forma $y = 3 + 7z$ perché soluzione di $\bar{\Gamma}_{2,2}$ e con $z \in \mathbb{Z}$ della forma $z = 7u$, $u \in \mathbb{Z}$ perché soluzione di $\bar{\Gamma}_{2,3}$. Ne segue che la forma che un tale intero x deve avere è la seguente $x = 1 + 3y = 1 + 3(3 + 7z) = 1 + 3(3 + 7 \cdot 4u)$; ossia

$$x = 10 + 84u, \quad \text{con} \quad u \in \mathbb{Z}.$$

Quindi Γ_2 è compatibile e l'insieme delle sue soluzioni è quello formato degli interi x tali che $x \equiv_{84} 10$.

Esercizio 7. Dimostrare che per ogni $n \in \mathbb{N}$ le ultime cifre delle espressioni in base 10 di n e di n^5 sono uguali; ossia che

$$\nabla_n. \qquad n^5 \equiv_{10} n.$$

Soluzione. Se $n = 0$, allora $n^5 = 0^5 = 0 = n$. Quindi, per la riflessività della relazione (di equivalenza) $\equiv_{10}$, risulta $n^5 \equiv_{10} n$. Dunque ∇_0 è vera.

Sia, dunque, d'ora in poi, $n \in \mathbb{N}$ un naturale diverso da 0; cioè, sia $n \in \mathbb{N} \setminus \{0\}$. Dimostreremo la validità di ∇_n per induzione.

Base. Se $n = 1$, allora $n^5 = 1^5 = 1 = n$. Quindi, come nel caso $n = 0$, per la riflessività della relazione $\equiv_{10}$, risulta $n^5 \equiv_{10} n$. Dunque ∇_1 è vera.

Passo. Mostriamo che per ogni $n \in \mathbb{N}$, se ∇_n è vera, allora anche ∇_{n+1} è vera.

Innanzi tutto traduciamo l'eventuale veridicità di ∇_h per un qualsiasi $h \in \mathbb{N}$.

Abbiamo che ∇_h è vera se e solo se $h^5 \equiv_{10} h$; ossia, se e solo se $h^5 - h \equiv_{10} 0$; ossia, se e solo se esiste $q_h \in \mathbb{Z}$ tale che $h^5 - h = q_h 10$.

Ora, poiché, per ipotesi induttiva, ∇_n è vera, esiste $q_n \in \mathbb{Z}$ tale che

$$\triangle_n. \qquad n^5 - n = q_n 10.$$

D'altra parte, traduciamo l'eventuale veridicità di ∇_{n+1}. Per quanto appena visto, ∇_{n+1} è vera se e solo se esiste $q_{n+1} \in \mathbb{Z}$ tale che $(n+1)^5 - (n+1) = q_{n+1}10$; ossia, se e solo se esiste $q_{n+1} \in \mathbb{Z}$ tale che

$$(n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1) - (n + 1) = q_{n+1}10;$$

ossia, se e solo se esiste $q_{n+1} \in \mathbb{Z}$ tale che

$$(n^5 - n) + 5n(n^3 + 1) + (n^3 + n^2)10 = q_{n+1}10;$$

ossia, grazie all'ipotesi induttiva e ricordando $\triangle_n$, se e solo se esiste $q_{n+1} \in \mathbb{Z}$ tale che

$$q_n 10 + 5n(n^3 + 1) + (n^3 + n^2)10 = q_{n+1}10.$$

Pertanto resta da dimostrare che esiste $q'_n \in \mathbb{Z}$ tale che

$$\diamondsuit_n. \qquad 5n(n^3 + 1) = q'_n 10.$$

Infatti, se un tale q'_n esistesse, allora avremmo che ∇_{n+1} sarebbe vera se e solo se esistesse un intero $q_{n+1} \in \mathbb{Z}$ tale che

$$q_n 10 + q'_n 10 + (n^3 + n^2)10 = q_{n+1}10;$$

ossia, sempre, 'ché, in tal caso, un tale intero q_{n+1} sempre esisterebbe: è $q_{n+1} = q_n + q'_n + (n^3 + n^2)$.

Dimostriamo, dunque, la validità di $\diamondsuit_n$, ricordando che, per quanto detto prima, $n \geq 1$.

Ora, se n è pari; cioè se $n = 2m$, allora, riscrivendo il primo membro di $\diamondsuit_n$ come segue

$$\begin{aligned} 5n(n^3+1) &= 5(2m)(8m^3+1) \\ &= 10m(8m^3+1) \\ &= (8m^3+1)m10 \\ &= (8\tfrac{n^3}{2^3}+1)\tfrac{n}{2}10 \\ &= (n^3+1)\tfrac{n}{2}10, \end{aligned}$$

vediamo immediatamente che l'intero $q'_n = (n^3+1)\frac{n}{2}$ fa al caso nostro.

Se, n è dispari; cioè se $n = 2m+1$, allora, riscrivendo il primo membro di $\diamondsuit_n$ come segue

$$\begin{aligned} 5n(n^3+1) &= 5(2m+1)((2m+1)^3+1) \\ &= 5(2m+1)((2m)^3+3(2m)^2+3(2m)+1+1) \\ &= 5(2m+1)(2(2^2m^3)+2(3(2m^2))+2(3m)+2) \\ &= 5\cdot 2(2m+1)((2^2m^3)+3(2m^2)+3m+1) \\ &= (2m+1)((2^2m^3)+3(2m^2)+3m+1)10 \\ &= n(4(\tfrac{n-1}{2})^3+6(\tfrac{n-1}{2})^2+3(\tfrac{n-1}{2})+1)10 \\ &= n(\tfrac{1}{2}(n-1)^3+\tfrac{3}{2}(n-1)^2+\tfrac{3}{2}(n-1)+1)10, \end{aligned}$$

vediamo immediatamente che l'intero $q'_n = n(\frac{1}{2}(n-1)^3+\frac{3}{2}(n-1)^2+\frac{3}{2}(n-1)+1)$ fa al caso nostro.