ALGEBRA 1 — 2008/2009

Prof. Fabio Gavarini

Sessione estiva anticipata — prova scritta del 23 Giugno 2009

Svolgimento completo

N.B.: lo svolgimento qui presentato è molto lungo... Questo non vuol dire *che lo svolgimento ordinario di tale compito (nel corso di un esame scritto) debba esserlo altrettanto. Semplicemente, questo lo è perché si è colta l'occasione per spiegare in dettaglio i vari esercizi, anche prospettando diversi modi possibili di svolgerli.*

. . . . . * . . . . . .

[1] — Sia G un gruppo ciclico finito di ordine 54.

(a) Determinare tutti i generatori di G.

(b) Determinare se esistano o meno elementi in G di ordine 9, oppure 13, oppure 18; in caso affermativo, specificare esplicitamente un elemento con tale ordine.

(c) stabilire — giustificando la conclusione — se il gruppo G sia isomorfo oppure no al gruppo $\big(U(\mathbb{Z}_{81})\,;\,\cdot\big)$ degli elementi invertibili dell'anello $\big(\mathbb{Z}_{81}\,;\,+\,,\,\cdot\big)$.

Soluzione: *(a)* Per cominciare, sappiamo che ogni gruppo ciclico di ordine 54, sia G, è isomorfo al gruppo $\big(\mathbb{Z}_{54}\,;\,+\big)$; precisamente, un isomorfismo esplicito si può ottenere scegliendo un generatore del gruppo G, sia g, e considerando l'applicazione $\mathbb{Z}_{54} \longrightarrow G$ definita da $(z \mod 54) \mapsto g^z$. Tramite un tale isomorfismo, i generatori di G corrispondono ai generatori di $\big(\mathbb{Z}_{54}\,;+\big)$, i quali sono esattamente gli elementi invertibili nell'*anello unitario* $\big(\mathbb{Z}_{54}\,;\,+\,,\,\cdot\big)$. Questi ultimi formano l'insieme

$$U(\mathbb{Z}_{54}) \,=\, \big\{\, \overline{z} := (z \mod 54) \,\big|\, M.C.D.(z,54) = 1 \,\big\}$$

delle classi resto modulo 54 rappresentate da numeri interi *coprimi* con 54. Sappiamo anche che — indicando con φ la funzione di Eulero — tale insieme ha cardinalità

$$\Big|U(\mathbb{Z}_{54})\Big| \,=\, \varphi(54) \,=\, \varphi\big(2\cdot 3^3\big) \,=\, \varphi(2)\cdot\varphi\big(3^3\big) \,=\, (2-1)\cdot(3-1)\,3^{3-1} \,=\, 1\cdot 2\cdot 9 \,=\, 18$$

cioè i generatori cercati sono in tutto esattamente 18, e il calcolo diretto ci dà

$$U(\mathbb{Z}_{54}) \,=\, \big\{\, \overline{1}\,,\,\overline{5}\,,\,\overline{7}\,,\,\overline{11}\,,\,\overline{13}\,,\,\overline{17}\,,\,\overline{19}\,,\,\overline{23}\,,\,\overline{25}\,,\,\overline{29}\,,\,\overline{31}\,,\,\overline{35}\,,\,\overline{37}\,,\,\overline{41}\,,\,\overline{43}\,,\,\overline{47}\,,\,\overline{49}\,,\,\overline{53}\,\big\}$$

Si noti che in questo calcolo teniamo conto del fatto che

$$M.C.D.(z,54) = 1 \implies M.C.D.(-z,54) = 1$$

e quindi $\overline{z} \in U(\mathbb{Z}_{54}) \implies -\overline{z} = \overline{-z} \in U(\mathbb{Z}_{54})$; perciò, ad esempio, da $\overline{1} \in U(\mathbb{Z}_{54})$ deduciamo che $\overline{53} = -\overline{1} = \overline{-1} \in U(\mathbb{Z}_{54})$, oppure da $\overline{5} \in U(\mathbb{Z}_{54})$ deduciamo che $\overline{49} = -\overline{5} = \overline{-5} \in U(\mathbb{Z}_{54})$, o da $\overline{13} \in U(\mathbb{Z}_{54})$ che $\overline{41} = -\overline{13} = \overline{-13} \in U(\mathbb{Z}_{54})$, e così via.

In conclusione, se g è un qualunque generatore del gruppo ciclico G di ordine 54, i generatori di G sono tutte e soli gli elementi

$$g^1 = g\,,\ g^5\,,\ g^7\,,\ g^{11},\ g^{13},\ g^{17},\ g^{19},\ g^{23},\ g^{25},\ g^{29},\ g^{31},\ g^{35},\ g^{37},\ g^{41},\ g^{43},\ g^{47},\ g^{49},\ g^{53}$$

(b) Per il Teorema di Lagrange, l'ordine di un elemento in un gruppo finito è un divisore dell'ordine del gruppo: nel caso in esame, l'ordine di un elemento di G dev'essere divisore di 54, dunque appartiene all'insieme $\{\,1\,,\,2\,,\,3\,,\,6\,,\,9\,,\,18\,,\,27\,,\,54\,\}$. Quindi *possono esistere* (ma non sappiamo ancora se esistano effettivamente...) elementi di ordine 9 o di ordine 18, ma certamente *non esiste* alcun elemento di ordine 13.

In aggiunta, per i gruppi finiti che siano *ciclici* vale anche *l'inverso del Teorema di Lagrange*, in questo senso: *per ogni divisore, sia d, dell'ordine (finito) del gruppo esiste un elemento che abbia ordine esattamente d*. Precisamente, se g è un qualunque generatore di G un elemento di ordine d è dato da $g^{n/d}$, dove $n := |G|$ è l'ordine del gruppo G.

Applicando tutto ciò al caso in esame, concludiamo che esistono in G (di ordine 54) un elemento di ordine 9, precisamente $g^{54/9} = g^6$, e un elemento di ordine 18, precisamente $g^{54/18} = g^3$, dove g è un fissato generatore di G.

(c) Come prima, da risultati generali sappiamo che il gruppo $\big(U(\mathbb{Z}_{81})\,;\,\cdot\,\big)$ degli elementi invertibili dell'anello $\big(\mathbb{Z}_{81}\,;\,+\,,\,\cdot\,\big)$ ha esattamente

$$\Big|U(\mathbb{Z}_{81})\Big| \;=\; \varphi(81) \;=\; \varphi\big(3^4\big) \;=\; (3-1)\,3^{4-1} \;=\; 2\cdot 27 \;=\; 54$$

quindi $\Big|U(\mathbb{Z}_{81})\Big|$ e $\mathbb{Z}_{54}$ sono gruppi dello stesso ordine, perciò *potrebbero* anche essere isomorfi... (ma non è detto!)

Operando come prima — e osservando che $\overline{z} \in U(\mathbb{Z}_{81}) \iff M.C.D.(z,81) = 1 \iff M.C.D.(z,3) = 1$ — il calcolo diretto ci dà

$$\begin{aligned} U(\mathbb{Z}_{81}) \;=\; \big\{\,&\overline{1}\,,\,\overline{2}\,,\,\overline{4}\,,\,\overline{5}\,,\,\overline{7}\,,\,\overline{8}\,,\,\overline{10}\,,\,\overline{11}\,,\,\overline{13}\,,\,\overline{14}\,,\,\overline{16}\,,\,\overline{17}\,,\,\overline{19}\,,\,\overline{20}\,,\,\overline{21}\,,\,\overline{22}\,,\,\overline{23}\,,\,\overline{25}\,,\,\overline{26}\,,\\ &\overline{28}\,,\,\overline{29}\,,\,\overline{31}\,,\,\overline{32}\,,\,\overline{34}\,,\,\overline{35}\,,\,\overline{37}\,,\,\overline{38}\,,\,\overline{40}\,,\,\overline{41}\,,\,\overline{43}\,,\,\overline{44}\,,\,\overline{46}\,,\,\overline{47}\,,\,\overline{49}\,,\,\overline{50}\,,\,\overline{52}\,,\,\overline{53}\,,\\ &\overline{55}\,,\,\overline{56}\,,\,\overline{58}\,,\,\overline{59}\,,\,\overline{61}\,,\,\overline{62}\,,\,\overline{64}\,,\,\overline{65}\,,\,\overline{67}\,,\,\overline{68}\,,\,\overline{70}\,,\,\overline{71}\,,\,\overline{73}\,,\,\overline{74}\,,\,\overline{76}\,,\,\overline{77}\,,\,\overline{79}\,,\,\overline{80}\,\big\} \end{aligned}$$

Ora, il gruppo $\big(U(\mathbb{Z}_{81})\,;\,\cdot\,\big)$ è isomorfo al gruppo $\big(\mathbb{Z}_{54}\,;\,+\,,\,\cdot\,\big)$ se e soltanto se è ciclico (di ordine 54), dunque se e soltanto se contiene almeno un elemento di ordine 54. Perciò dobbiamo appurare se esiste o no in $U(\mathbb{Z}_{81})$ un tale elemento.

Per cominciare, calcoliamo l'ordine di $\overline{2}$ in $U(\mathbb{Z}_{81})$, tenendo conto che — ancora per il Teorema di Lagrange — esso è un divisore di 54, dunque è uno tra i numeri 1, 2, 3, 6, 9, 18, 27 oppure 54. Il calcolo diretto ci dà (mostrando anche come fare i conti...)

$$\overline{2}^{\,1} = \overline{2} \neq \overline{1}\,,\ \ \overline{2}^{\,2} = \overline{4} \neq \overline{1}\,,\ \ \overline{2}^{\,3} = \overline{8} \neq \overline{1}\,,\ \ \overline{2}^{\,6} = \overline{64} \neq \overline{1}\,,\ \ \overline{2}^{\,9} = \overline{512} = \overline{81\cdot 6 + 26} = \overline{26} \neq \overline{1}$$

per cui l'ordine di $\overline{2}$ non è né 1, né 2, né 3, né 6, né 9. Adesso osserviamo che

$$\overline{2}^{\,10} = \overline{2}^{\,9+1} = \overline{2}^{\,9} \cdot \overline{2} = \overline{26} \cdot \overline{2} = \overline{26 \cdot 2} = \overline{52}$$
$$\overline{2}^{\,8} = \overline{2}^{\,9-1} = \overline{2}^{\,9} \cdot \overline{2}^{\,-1} = \overline{26} \cdot \overline{2}^{\,-1} = \overline{13} \cdot \overline{2} \cdot \overline{2}^{\,-1} = \overline{13}$$

da cui calcoliamo

$$\overline{2}^{\,18} = \overline{2}^{\,10+8} = \overline{2}^{\,10} \cdot \overline{2}^{\,8} = \overline{52} \cdot \overline{13} = \overline{676} = \overline{81 \cdot 8 + 28} = \overline{28} \neq \overline{1}$$

e quindi l'ordine di $\overline{2}$ non è neppure 18. Infine, abbiamo che

$$\overline{2}^{\,27} = \overline{2}^{\,18+9} = \overline{2}^{\,18} \cdot \overline{2}^{\,9} = \overline{28} \cdot \overline{26} = \overline{28 \cdot 26} = \overline{4 \cdot 7 \cdot 2 \cdot 13} =$$
$$= \overline{4 \cdot 2 \cdot 7 \cdot 13} = \overline{4 \cdot 2} \cdot \overline{7 \cdot 13} = \overline{8} \cdot \overline{91} = \overline{8} \cdot \overline{10} = \overline{80} = \overline{-1} = -\overline{1} \neq \overline{1}$$

e quindi l'ordine di $\overline{2}$ non è neppure 21, quindi è necessariamente 54.

La morale della favola è che, alla fine, possiamo concludere che il gruppo $\big(U(\mathbb{Z}_{81})\,;\,\cdot\big)$, contenendo un elemento di ordine 54 — pari all'ordine del gruppo stesso — è ciclico, e quindi è isomorfo al gruppo $\big(\mathbb{Z}_{54}\,;\,+\big)$. □

. . . . . * . . . . . .

[2] — Sia G un gruppo, e sia H un sottogruppo di G contenuto nel centro $Z(G)$ di G.

(a) Dimostrare che H è sottogruppo normale di G.

(b) Dimostrare che, se il gruppo quoziente G/H è ciclico, allora il gruppo G è abeliano.

Soluzione: *(a)* Sappiamo già che H è sottogruppo di G, quindi per dimostrare che è *normale* dobbiamo soltanto verificare che è chiuso rispetto alla coniugazione, cioè che $g\,H\,g^{-1} \subseteq H$ per ogni $g \in G$.

Ora, per ipotesi si ha $H \subseteq Z(G) := \{\,\gamma \in G \,|\, g\,\gamma = \gamma\,g\,,\ \forall\, g \in G\,\}$. In particolare allora $g\,h = h\,g$ per ogni $g \in G$ e ogni $h \in H$; quindi

$$g\,H\,g^{-1} = H\,g\,g^{-1} = H \subseteq H \qquad\qquad \forall\ g \in G$$

e perciò concludiamo che H è normale, q.e.d.

(b) Supponiamo che G/H sia ciclico, generato dalla classe laterale (sinistra) $\overline{g} = gH$. Per dimostrare che G è abeliano, dobbiamo verificare che, presi due qualsiansi elementi $x, y \in G$ si ha $x\,y = y\,x$. Ora, per le classi laterali $\overline{x} = xH$ e $\overline{y} = yH$ esistono due interi $e(x), e(y) \in \mathbb{Z}$ tali che

$$xH = \overline{x} = \overline{g}^{\,e(x)} = g^{e(x)}H\,, \qquad yH = \overline{y} = \overline{g}^{\,e(y)} = g^{e(y)}H$$

Allora da $xH = g^{e(x)}H$ e da $yH = g^{e(y)}H$ segue che esistono due elementi $h_x\,, h_y \in H$ tali che $x = g^{e(x)}\,h_x$ e $y = g^{e(y)}\,h_y$. A questo punto calcoliamo:

$$\begin{aligned} x\,y \;&=\; g^{e(x)}\,h_x\,g^{e(y)}\,h_y \;=\; g^{e(x)}\,g^{e(y)}\,h_x\,h_y \;=\; g^{e(x)+e(y)}\,h_x\,h_y \;= \\ &=\; g^{e(y)+e(x)}\,h_y\,h_x \;=\; g^{e(y)}\,g^{e(x)}\,h_y\,h_x \;=\; g^{e(y)}\,h_y\,g^{e(x)}\,h_x \;=\; y\,x \end{aligned}$$

dove abbiamo sfruttato il fatto che gli elementi h_x e h_y commutano con tutti gli altri elementi — perché $h_x\,, h_y \in H \subseteq Z(G)$ — e le potenze di g commutano tra di loro. E il risultato è che $x\,y = y\,x$, q.e.d. □

. . . . . * . . . . . .

[3] — Risolvere il sistema di congruenze lineari nell'anello $\mathbb{Z}[i]$

$$\begin{cases} (5+3\,i)\,x \;\equiv\; -2 & \mod\,(2-i) \\ (3+2\,i)\,x \;\equiv\; 1-7\,i & \mod\,(1+i) \end{cases}$$

<u>Soluzione</u>*:* Per prima cosa, calcoliamo il $M.C.D.\big(2-i\,,1+i\big)$ tramite l'algoritmo euclideo delle divisioni successive. Otteniamo

$$\begin{aligned} 2-i \;&=\; (1+i)\cdot(1-i) \;-\; i \\ 2-i \;&=\; (-i)\cdot(1-2\,i) \;+\; 0 \end{aligned}$$

da cui ricaviamo che $M.C.D.(2-i,1+i) = -i$, o anche $M.C.D.(2-i,1+i) = -i$, in quanto $-i$, essendo invertibile in $\mathbb{Z}[i]$, è associato a 1.

Nel calcolo, il secondo passaggio è elementare, mentre il primo segue dal calcolo effettuato nel campo $\mathbb{C}$ dei numeri complessi, che dà

$$(2-i)\cdot(1+i)^{-1} \;=\; \frac{2-i}{1+i} \;=\; \frac{(2-i)\,(1-i)}{(1+i)\,(1-i)} \;=\; \frac{1-3\,i}{2} \;=\; (1-i) + \frac{-1-i}{2}$$

per cui il quoziente q della divisione euclidea di $(2-i)$ per $(1+i)$ è $q = (1-i)$, e quindi il resto r è $r = (2-i) - (1+i)\cdot(1-i) = -i$.

Dunque $M.C.D.(2-i,1+i) = -i$ significa che nel nostro sistema di congruenze i due moduli sono coprimi, quindi le due congruenze sono tra loro compatibili. Pertanto, se le due congruenze, separatamente, hanno una soluzione, anche il sistema ammette soluzione.

Studiamo ora la risolublità delle due congruenze. In entrambe possiamo semplificare il coefficiente della x, come segue:

$$5+3\,i \;\equiv\; (2-i)\,(2+i) \;+\; 3\,i \;\equiv\; 3\,i \mod\,(2-i)$$

per la prima congruenza, e

$$3+2\,i \;\equiv\; 2\,(1+i) \;+\; 1 \;\equiv\; 1 \mod\,(1+i)$$

per la seconda. Perciò il nostro sistema di partenza è equivalente a

$$\begin{cases} (3\,i)\;x \;\equiv\; -2 & \mod (2-i) \\ x \;\equiv\; 1-7\,i & \mod (1+i) \end{cases}$$

Analogamente, possiamo modificare anche i termini noti, come segue:

$$-2 \;\equiv\; -(2-i) \;-\; i \;\equiv\; -i \mod (2-i)$$

per la prima congruenza, e

$$1-7\,i \;\equiv\; (1-i) \;-\; 6\,i \;\equiv\; (1-i) \;-\; 3\,(1+i)\,(1-i)\,i \;\equiv\; 1-i \mod (1+i)$$

per la seconda. Perciò il nostro sistema di partenza è equivalente a

$$\begin{cases} (3\,i)\;x \;\equiv\; -i & \mod (2-i) \\ x \;\equiv\; 1-i & \mod (1+i) \end{cases}$$

Adesso moltiplichiamo la prima congruenza (membro a membro) per i^{-1} (cioè "dividiamo per i"), e così il sistema diventa

$$\begin{cases} 3\;x \;\equiv\; -1 & \mod (2-i) \\ x \;\equiv\; 1-i & \mod (1+i) \end{cases}$$

Procediamo ora a risolvere tale sistema, con due metodi alternativi.

Primo metodo: La seconda congruenza del sistema si presenta in forma già risolta: precisamente, le sue soluzioni sono tutti e soli gli interi della forma

$$x_2 \;=\; (1-i) \;+\; k\,(1+i) \;\;, \qquad \forall\;\; k \in \mathbb{Z}[i] \tag{1}$$

Sostituendo una tale soluzione nella prima congruenza si trova

$$\begin{aligned} 3\,x_2 \;&=\; 3\,\big((1-i) \;+\; k\,(1+i)\big) \;\equiv\; -1 \mod (2-i) \quad \Longrightarrow \\ &\Longrightarrow \quad 3-3\,i \;+\; (3+3\,i)\,k \;\equiv\; -1 \mod (2-i) \quad \Longrightarrow \\ \Longrightarrow \quad &(3+3\,i)\,k \;\equiv\; -4+3\,i \;=\; -2\,(2-i) \;+\; i \;\equiv\; i \mod (2-i) \quad \Longrightarrow \\ &\Longrightarrow \quad (3+3\,i)\,k \;\equiv\; i \mod (2-i) \end{aligned}$$

Risolviamo ora la congruenza $\copyright : (3+3\,i)\,k \;\equiv\; i \mod (2-i)$, con incognita $k \in \mathbb{Z}[i]$. Tramite l'algoritmo euclideo delle divisioni successive, calcoliamo il $M.C.D.\big(3+3\,i\,,\,2-i\big)$ e una identità di Bézout per esso. Il calcolo esplicito ci dà

$$\frac{3+3\,i}{2-i} \;=\; \frac{(3+3\,i)\,(2+i)}{(2-i)\,(2+i)} \;=\; \frac{3+9\,i}{5} \;=\; (1+2\,i) - \left(\frac{2}{5} + \frac{1}{5}\,i\right)$$

da cui otteniamo

$$3+3\,i \;=\; (2-i)\cdot(1+2\,i) \;+\; (-1)$$

dunque $M.C.D.\big(3+3\,i\,,\,2-i\big) = -1 \sim 1$. Inoltre da questo ricaviamo

$$\begin{aligned}(3+3\,i) \;&=\; (2-i)\cdot(1+2\,i) \,+\, (-1) \qquad \Longrightarrow \\ \Longrightarrow \qquad (3+3\,i)\cdot 1 \,+\, (2-i)\cdot(-1-2\,i) \;&=\; (-1) \qquad \Longrightarrow \\ \Longrightarrow \qquad (3+3\,i)\cdot(-i) \,+\, (2-i)\cdot(-2+i) \;&=\; i\end{aligned}$$

dove la seconda uguaglianza è una identità di Bézout per $M.C.D.\big(3+3\,i\,,\,2-i\big)$, mentre la terza ci dice che $\overline{x} := -i$ *è una soluzione particolare della congruenza* ©.

La *soluzione generale* di © poi è chiaramente data dalla formula

$$k_z \;=\; -i \,+\, (2-i)\,z \quad , \qquad \forall\;\, z \in \mathbb{Z}[i] \tag{2}$$

Infine, sostituendo k nella (1) con l'espressione per k_z nella (2) otteniamo che la *soluzione generale* del sistema è di congruenze in esame è data dalla formula

$$x_z \;=\; (1-i) \,+\, \big(-i+(2-i)\,z\big)\,(1+i) \;=\; (2-2\,i) \,+\, (3+i)\,z \quad , \qquad \forall\;\, z \in \mathbb{Z}[i] \tag{3}$$

<u>*Secondo metodo:*</u> Applichiamo il *Teorema Cinese del Resto*. Per prima cosa, dobbiamo però trasformare il nostro sistema di congruenze in uno che sia *in forma cinese*, cioè in cui le diverse congruenze si presentino già in forma risolta. Partendo dunque dal sistema

$$\begin{cases} 3\;x_1 \;\equiv\; -1 & \mod (2-i) \\ \;\;\, x_2 \;\equiv\; 1-i & \mod (1+i) \end{cases}$$

Ora, poichè $3 \,=\, 5-2 \,=\, (2-i)\,(2+i) \;\equiv\; -2 \mod (2-i)$, e analogamente abbiamo $-1 \;\equiv\; (2-i)\,(2+i)-1 \,=\, 5-1 \,=\, 4 = (-2)\,(-2) \mod (2-i)$, possiamo riscrive la prima congruenza in © come $-2\,x \;\equiv\; (-2)\,(-2)$. Poichè -2 è coprimo con $(2-i)$, quest'ultima congruenza è equivalente a quella che si ottiene cancellando da ambo i membri il fattore comune -2, cioè $x \equiv -2 \mod (2-i)$. Pertanto il nostro sistema diventa (cioè, "è equivalente a") il sistema

$$\circledast \begin{cases} \;\;\, x \;\equiv\; -2 & \mod (2-i) \\ \;\;\, x \;\equiv\; 1-i & \mod (1+i) \end{cases}$$

il quale è in forma cinese, e possiamo quindi applicargli il *Teorema Cinese del Resto*.

Per prima cosa, poniamo $R := (2-i)\,(1+i) = 3+i$, $R_1 := (1+i)$, $R_2 := (2-i)$. Ora, dobbiamo risolvere *separatamente* le due congruenze

$$\left[\begin{array}{ll} R_1 \cdot x_1 \;\equiv\; -2 & \mod (2-i) \\ R_2 \cdot x_2 \;\equiv\; 1-i & \mod (1+i) \end{array}\right. \qquad \text{cioè} \qquad \left[\begin{array}{ll} (1+i)\cdot x_1 \;\equiv\; -2 & \mod (2-i) \\ (2-i)\cdot x_2 \;\equiv\; 1-i & \mod (1+i) \end{array}\right.$$

Si può semplificare la prima congruenza, osservando che $-2 = -(1-i)\,(1+i)$, e quindi si può cancellare da ambo i membri della congruenza il fattore comune — e coprimo con il modulo $(2-i)$ — $(1+i)$, per cui la congruenza diventa $x_1 \;\equiv\; -(1-i) \mod (2-i)$. Questa è già in forma risolta, precisamente una soluzione particolare è $\overline{x}_1 = -(1-i) = -1+i$.

Per la seconda congruenza, osserviamo che $2 = (1+i)(1-i) \equiv 0 \mod (1+i)$, quindi $2 - i \equiv -i \mod (1+i)$ e la congruenza diventa $(-i)\,x_2 \equiv 1 - i \mod (2-i)$. Dato che il coefficiente $(-i)$ è invertibile in $\mathbb{Z}[i]$, con inverso $(-i)^{-1} = i$ moltiplicando entrambi i membri della congruenza per i otteniamo $x_2 \equiv 1 + i \equiv 0 \mod (1+i)$, cioè $x_2 \equiv 0 \mod (1+i)$, che è una congruenza equivalente già in forma risolta: una sua soluzione particolare è $\overline{x}_2 = 0$.

Per concludere, il Teorema Cinese del Resto ci dice che la soluzione generale del sistema $\circledast$ — e quindi, in definitiva, del nostro sistema di partenza — è data da

$$x_\zeta \;=\; (1+i)\,\overline{x}_1 \;+\; (2-i)\,\overline{x}_2 \;+\zeta\,R \;\;, \qquad \forall\;\; \zeta \in \mathbb{Z}[i]$$

cioè

$$x_\zeta \;=\; (1+i)\,(-1+i) \;+\; (2-i)\,0 \;+z\,(3+i) \;=\; -2 \;+\; \zeta\,(3+i) \;\;, \qquad \forall\;\; \zeta \in \mathbb{Z}[i] \;\;. \quad (4)$$

NOTA: Confrontando la (4)con la (3) può sembrare che rappresentino soluzioni diverse! Ma invece si riconosce subito che esse rappresentano — al variare di $z \in \mathbb{Z}[i]$ e di $\zeta \in \mathbb{Z}[i]$ — *lo stesso insieme* di numeri interi. Infatti, siccome abbiamo l'identità

$$2 - 2\,i \;=\; -2 + (1-i)\,(3+i)$$

possiamo passare dalla (3) alla (4) ponendo $\zeta = z + (1-i)$, e viceversa dalla (3) alla (4) ponendo $z = \zeta - (1-i)$. Pertanto la (3) e la (4) esprimono la stessa soluzione. □

. . . . . * . . . . . .

[4] — Si considerino due insiemi A e B tali che $A \cap B = \emptyset$, e sia $C := A \cup B$ l'insieme unione dei primi due. Si considerino poi gli insiemi di applicazioni

$$\begin{aligned}
\mathcal{E}(C) \;&:=\; C^C \;\equiv\; \big\{\textit{applicazioni da } C \textit{ a } C\,\big\} \\
\mathcal{S}(C) \;&:=\; \big\{\textit{permutazioni di } C \textit{ in sé}\,\big\} \\
\mathcal{E}(A\,|\,B) \;&:=\; \big\{f \in \mathcal{E}(C)\,\big|\,f(A) \subseteq A\,,\; f(B) \subseteq B\big\} \\
\mathcal{E}(C : A) \;&:=\; \big\{f \in \mathcal{E}(C)\,\big|\,f(C) \subseteq A\big\}
\end{aligned}$$

Osserviamo che la composizione di applicazioni dà un'operazione su $\mathcal{E}(C)$, denotata con $\circ$, e precisamente $\big(\mathcal{E}(C)\,;\circ\big)$ è un monoide (=gruppoide associativo unitario). Analogamente, $\big(\mathcal{S}(C)\,;\circ\big)$ è un gruppo.

(a) Dimostrare che $\mathcal{E}(A\,|\,B)$ è chiuso rispetto al prodotto di composizione, cioè che $\mathcal{E}(A\,|\,B) \circ \mathcal{E}(A\,|\,B) \;\subseteq\; \mathcal{E}(A\,|\,B)$.

(b) Dimostrare che $\mathcal{S}(C) \cap \mathcal{E}(A\,|\,B)$ è un sottogruppo di $\big(\mathcal{S}(C)\,;\circ\big)$.

(c) Dimostrare che $\mathcal{E}(C : A) \circ \mathcal{E}(C) \;\subseteq\; \mathcal{E}(C : A)$.

Soluzione: *(a)* Date due qualsiasi $f, \ell \in \mathcal{E}(A \,|\, B)$, dobbiamo dimostrare che

$$f \circ \ell \,\in\, \mathcal{E}(A \,|\, B) \quad , \qquad \text{cioè} \qquad (f \circ \ell)(a) \in A \,,\; (f \circ \ell)(b) \in B \,, \quad \forall\; a \in A \,,\; b \in B \tag{5}$$

Ora, dalle ipotesi deduciamo

$$\begin{aligned} (f \circ \ell)(a) \,&=\, f\big(\ell(a)\big) \,\subseteq\, f(A) \,\subseteq\, A \quad \forall\, a \in A \,, \qquad \text{perché} \qquad \ell(a) \in A \,,\; f(A) \subseteq A \\ (f \circ \ell)(b) \,&=\, f\big(\ell(b)\big) \,\subseteq\, f(B) \,\subseteq\, B \quad \forall\, b \in B \,, \qquad \text{perché} \qquad \ell(b) \in B \,,\; f(B) \subseteq B \end{aligned}$$

il che prova la (5), e quindi la *(a)*.

(b) Per dimostrare che $\mathcal{S}(C) \cap \mathcal{E}(A \,|\, B)$ è un sottogruppo di $\big(\mathcal{S}(C)\,;\circ\big)$, ci basta verificare che è non vuoto, che è chiuso (rispetto a $\circ$) e che contiene l'inverso di ogni suo elemento.

La prima proprietà segue dal fatto che entrambi i sottoinsiemi $\mathcal{S}(C)$ e $\mathcal{E}(A \,|\, B)$ contengono l'elemento id_C, il quale quindi appartiene a $\mathcal{S}(C) \cap \mathcal{E}(A \,|\, B)$, perciò tale (sotto)insieme è non vuoto.

La seconda proprietà segue dal fatto che entrambi i sottoinsiemi $\mathcal{S}(C)$ e $\mathcal{E}(A \,|\, B)$ sono chiusi (in $\mathcal{E}(C)$). In dettaglio, dati $f, \ell \in \mathcal{S}(C) \cap \mathcal{E}(A \,|\, B)$, quanto detto implica che

$$f, \ell \in \mathcal{S}(C) \cap \mathcal{E}(A|B) \Rightarrow \begin{cases} f, \ell \in \mathcal{S}(C) \Rightarrow (f \circ \ell) \in \mathcal{S}(C) \\ f, \ell \in \mathcal{E}(A|B) \Rightarrow (f \circ \ell) \in \mathcal{E}(A|B) \end{cases} \Longrightarrow (f \circ \ell) \in \mathcal{S}(C) \cap \mathcal{E}(A|B)$$

che appunto significa che $\mathcal{S}(C) \cap \mathcal{E}(A|B)$ è chiuso.

Per la seconda proprietà, sia $f \in \mathcal{S}(C) \cap \mathcal{E}(A \,|\, B)$. Poiché $\mathcal{S}(C)$ è un sottogruppo, in particolare contiene l'inverso di ogni suo elemento: in particolare, si ha $f^{-1} \in \mathcal{S}(C)$. Dobbiamo allora soltanto dimostrare che $f^{-1} \in \mathcal{E}(A \,|\, B)$.

Sia dunque $a \in A$. Se per assurdo fosse $f^{-1}(a) \in B$, allora avremmo $f\big(f^{-1}(a)\big) \in B$, perché $f(A) \subseteq A$, dato che $f \in \mathcal{E}(A \,|\, B)$. Ma d'altra parte $f\big(f^{-1}(a)\big) = a \in A$, quindi — siccome $A \cap B = \emptyset$ — abbiamo un assurdo. Questo dimostra che $f^{-1}(a) \in A$, per ogni $a \in A$, cioè $f^{-1}(A) \subseteq A$. Allo stesso modo, si dimostra che $f^{-1}(B) \subseteq B$. In conclusione, abbiamo dunque $f^{-1} \in \mathcal{E}(A \,|\, B)$, q.e.d.

(c) Per ogni $h \in \mathcal{E}(C : A)$, $t \in \mathcal{E}(C)$, si ha $h(C) \subseteq A$, $t(C) \subseteq C$, per definizione. Allora

$$(h \circ t)(C) \;=\; h\big(t(C)\big) \;\subseteq\; h(C) \;\subseteq\; A$$

che significa appunto che $(h \circ t) \in \mathcal{E}(C : A)$, q.e.d. □