CdL in Matematica

ALGEBRA 1

prof. Fabio GAVARINI

a.a. 2018–2019

Esame scritto del 18 Giugno 2019 — Sessione Estiva, I appello

Testo & Svolgimento

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

[1] — Sia $\mathbb{Q}^* := \mathbb{Q} \times \{0\}$, e sia $\eta \subseteq \mathbb{Q}^* \times \mathbb{Q}^*$ la relazione (binaria) in $\mathbb{Q}^*$ definita da

$$a \,\eta\, b \quad \Longleftrightarrow \quad \exists\ z \in \mathbb{Z}\ :\ a\, b^{-1} = 2^z \qquad\qquad \forall\ a\,,\, b \in \mathbb{Q}^*$$

(a) Dimostrare che la relazione η è compatibile con l'operazione prodotto in $\mathbb{Q}^*$.

(b) Dimostrare che la relazione η è un'equivalenza.

(c) Descrivere esplicitamente le quattro classi di η–equivalenza $\big[\,28/15\,\big]_\eta$, $\big[\,8\,\big]_\eta$, $\big[\,14/60\,\big]_\eta$, $\big[\,1/4\,\big]_\eta$;

(d) Determinare esplicitamente una funzione biiettiva $\mathbb{Q}^*_\times \lhook\joinrel\longrightarrow\!\!\!\!\!\rightarrow \mathbb{Q}^* \Big/ \eta$ dall'insieme $\mathbb{Q}^*_\times := \big\{\, n/d \;\big|\; n\,, d \in (1 + 2\,\mathbb{Z}) \big\}$ all'insieme quoziente $\mathbb{Q}^* \Big/ \eta$ (di $\mathbb{Q}^*$ modulo η).

[2] — Dimostrare che, per ogni $n \in \mathbb{N}$, il numero

$$f(n) \ := \ n^{55} + 2\, n^{50} + 3\, n^{45} + 4\, n^3 + 5\, n^2 + 6\, n$$

è divisibile per 7.

[3] — Dato $n \in \mathbb{N}$ con $n > 1$, sia $\mathbb{Z}_n$ l'anello degli interi modulo n e consideriamo le due funzioni

$$\begin{aligned} \tau : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \ , \quad \overline{z} \mapsto \tau(\,\overline{z}\,) := -\overline{z} \qquad\qquad \forall\ \overline{z} \in \mathbb{Z}_n \\ \rho : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \ , \quad \overline{z} \mapsto \rho(\,\overline{z}\,) := \overline{z} + \overline{1} \qquad\qquad \forall\ \overline{z} \in \mathbb{Z}_n \end{aligned}$$

Dimostrare che:

(a) τ e ρ sono permutazioni di $\mathbb{Z}_n$ (cioè sono invertibili, o — equivalentemente — sono biiettive);

(b) come elementi del gruppo $\big(\mathcal{S}(\mathbb{Z}_n)\,;\circ\big)$ delle permutazioni di $\mathbb{Z}_n$, la permutazione τ ha ordine 2 e la permutazione ρ ha ordine n;

(c) per ogni $k \in \mathbb{Z}$, vale nel gruppo $\big(\mathcal{S}(\mathbb{Z}_n)\,;\circ\big)$ l'identità $\tau \circ \rho^k = \rho^{n-k} \circ \tau$;

(d) per ogni $\ell \in \mathbb{Z}$ si ha $\rho^\ell \neq \tau$;

(e) il sottogruppo $\big\langle\, \tau\,, \rho \,\big\rangle$ di $\big(\mathcal{S}(\mathbb{Z}_n)\,;\circ\big)$ generato da τ e ρ ha cardinalità $2\,n$.

[4] — Sia $\mathbb{Z}_{35}$ l'anello degli interi modulo 35 .

(a) Descrivere esplicitamente l'insieme $U\big(\mathbb{Z}_{35}\big)$ degli elementi invertibili di $\mathbb{Z}_{35}$.

(b) Determinare se nel gruppo moltiplicativo $\big(U\big(\mathbb{Z}_{35}\big)\,;\,\cdot\,\big)$ esistano elementi di ordine 2, 3, 4, 5, 6, 7, 9, 10 .

[5] — Sia $A := \mathbb{Z}[\,x\,]$ l'anello dei polinomi nella variabile x a coefficienti in $\mathbb{Z}$, e sia $I := 5\,\mathbb{Z}[\,x\,] = \big\{\,5\,p(x)\,\big|\,p(x) \in \mathbb{Z}[\,x\,]\,\big\}$.

(a) Dimostrare che I è un ideale di $\mathbb{Z}[\,x\,]$.

(b) Dimostrare che l'anello quoziente $\mathbb{Z}[\,x\,]\Big/I$ è isomorfo all'anello $\mathbb{Z}_5[\,x\,]$ dei polinomi in x a coefficienti nell'anello $\mathbb{Z}_5$ degli interi modulo 5 , trovando un isomorfismo esplicito da $\mathbb{Z}[\,x\,]\Big/I$ a $\mathbb{Z}_5[\,x\,]$.

[6] — Nell'anello $\mathbb{Z}[\,i\,]$ degli interi di Gauss, si determini l'eventuale risolubilità, ed in caso positivo si determini anche una soluzione esplicita, per ciascuna delle seguenti equazioni diofantee:

(a) $\qquad (-3-i\,)\cdot x \;+\; (1+2\,i\,)\cdot y \;=\; -2+5\,i$

(b) $\qquad (1-3\,i\,)\cdot x \;+\; (-2+7\,i\,)\cdot y \;=\; 2-5\,i$

(c) Indicato con $I := \big(1-3\,i\,,7+2\,i\big)$ l'ideale di $\mathbb{Z}[\,i\,]$ generato dai due elementi $(1-3\,i\,)$ e $(7+2\,i\,)$, si determini un elemento $\delta \in \mathbb{Z}[\,i\,]$ tale che $I = \big(\,\delta\,\big)$ — cioè δ sia un (unico) generatore dell'ideale I .

(d) Determinare quali tra i numeri $(1+2\,i\,)$, $(-3-i\,)$ e $(7+2\,i\,)$ siano riducibili e quali irriducibili in $\mathbb{Z}[\,i\,]$.

— ⋆ —

SVOLGIMENTO

N.B.: lo svolgimento qui presentato è molto lungo... Questo non significa *che lo svolgimento ordinario di tale compito (nel corso di un esame scritto) debba essere altrettanto lungo. Semplicemente, questo lo è perché si approfitta per spiegare — in diversi modi, con lunghe digressioni, ecc. ecc. — in dettaglio e con molti particolari tutti gli aspetti della teoria toccati più o meno a fondo dal testo in questione.*

[1] — Rispondiamo ai diversi quesiti uno a uno.

(a) Ricordiamo che, date in un insieme E una relazione ρ e un'operazione $\star$, si dice che ρ è compatibile con $\star$ se

$$\forall\ x_1, x_2, y_1, y_2 \in E\ , \qquad \big(x_1\,\rho\,x_2\big)\ \&\ \big(y_1\,\rho\,y_2\big)\implies \big(x_1\star y_1\big)\,\rho\,\big(x_2\star y_2\big)$$

Nel caso in esame — con $E := \mathbb{Q}^*$, $\rho := \eta$ e $\star := \cdot$ — consideriamo $x_1, x_2, y_1, y_2 \in \mathbb{Q}^*$ tali che $\big(x_1\,\eta\,x_2\big)$ e $\big(y_1\,\eta\,y_2\big)$, cioè $x_1\,x_2^{-1} = 2^{z_x}$ e $y_1\,y_2^{-1} = 2^{z_y}$ per opportuni $z_x\,,\,z_y \in \mathbb{Z}$. Da questo segue che

$$(x_1\,y_1)\,(x_2\,y_2)^{-1} \;=\; x_1\,y_1\,x_2^{-1}\,y_2^{-1} \;=\; x_1\,x_2^{-1}\,y_1\,y_2^{-1} \;=\; 2^{z_x}\,2^{z_y} \;=\; 2^{z_x - z_y}$$

dunque $(x_1\,y_1)\,(x_2\,y_2)^{-1} = 2^{z_x+z_y}$ con $(z_x+z_y)\in\mathbb{Z}$, perciò $(x_1\,y_1)\,\eta\,(x_2\,y_2)$, q.e.d.

(b) Ricordiamo che una relazione è una equivalenza se è riflessiva, transitiva e simmetrica. Nel caso della relazione η, abbiamo:

<u>*Riflessività:*</u> Per ogni $q\in\mathbb{Q}^*$ abbiamo $q\,q^{-1} = 1 = 2^0$ con $0\in\mathbb{Z}$, dunque $q\,\eta\,q$, perciò η è riflessiva, q.e.d.

<u>*Transitività:*</u> Per ogni $h\,,k\,,\ell\in\mathbb{Q}^*$ tali che $h\,\eta\,k$ e $k\,\eta\,\ell$ abbiamo $h\,k^{-1} = 2^{z'}$ e $k\,\ell^{-1} = 2^{z''}$ per opportuni $z', z''\in\mathbb{Z}$; da questo segue che $h\,\ell^{-1}k = h\,k^{-1}\,k\,\ell^{-1} = 2^{z'}\,2^{z''} = 2^{z'+z''}$ con $\big(z'+z''\big)\in\mathbb{Z}$, dunque $h\,\eta\,\ell$, e concludiamo che η è transitiva, q.e.d.

<u>*Simmetria:*</u> Per ogni $h\,,k\in\mathbb{Q}^*$ tali che $h\,\eta\,k$ abbiamo $h\,k^{-1} = 2^z$ con $z\in\mathbb{Z}$; da questo segue che $k\,h^{-1} = \big(h\,k^{-1}\big)^{-1} = \big(2^z\big)^{-1} = 2^{-z}$ con $-z\in\mathbb{Z}$, dunque è anche $k\,\eta\,h$; possiamo così concludere che η è simmetrica, q.e.d.

In sintesi, η è riflessiva, transitiva e simmetrica, quindi è un'equivalenza, q.e.d.

(c) Ricordiamo che, per definizione, per ogni $q\in\mathbb{Q}^*$ la sua classe di η–equivalenza è l'insieme $[\,q\,]_\eta := \big\{\,x\in\mathbb{Q}^*\,\big|\,x\,\eta\,q\,\big\}$. Inoltre, dalla forma esplicita di η otteniamo che $x\,\eta\,q \iff x\,q^{-1} = 2^z \iff x = 2^z\,q$ con $z\in\mathbb{Z}$ arbitrario. Perciò abbiamo anche

$$[\,q\,]_\eta \;:=\; \big\{\,x\in\mathbb{Q}^*\,\big|\,x\,\eta\,q\,\big\} \;=\; \big\{\,x\in\mathbb{Q}^*\,\big|\,x = 2^z\,q\,,\ z\in\mathbb{Z}\,\big\} \;=\; \big\{\,2^z\,q\,\big|\,z\in\mathbb{Z}\,\big\} \qquad (1)$$

Applicando ora la (1) ai casi specifici di $q\in\big\{\,28/15\,,8\,,14/60\,,1/4\,\big\}$ otteniamo

$$\begin{aligned}
\big[\,28/15\,\big]_\eta \;&:=\; \big\{\,2^z\cdot 28/15\,\big|\,z\in\mathbb{Z}\,\big\} \;=\; \big\{\,2^s\cdot 7/15\,\big|\,s\in\mathbb{Z}\,\big\}\\
\big[\,8\,\big]_\eta \;&:=\; \big\{\,2^z\cdot 8\,\big|\,z\in\mathbb{Z}\,\big\} \;=\; \big\{\,2^s\,\big|\,s\in\mathbb{Z}\,\big\}\\
\big[\,14/60\,\big]_\eta \;&:=\; \big\{\,2^z\cdot 14/60\,\big|\,z\in\mathbb{Z}\,\big\} \;=\; \big\{\,2^s\cdot 7/15\,\big|\,s\in\mathbb{Z}\,\big\}\\
\big[\,1/4\,\big]_\eta \;&:=\; \big\{\,2^z\cdot 1/4\,\big|\,z\in\mathbb{Z}\,\big\} \;=\; \big\{\,2^s\,\big|\,s\in\mathbb{Z}\,\big\}
\end{aligned}$$

Si noti in particolare che $\big[\,28/15\,\big]_\eta = \big[\,14/60\,\big]_\eta$ e $\big[\,8\,\big]_\eta = \big[\,1/4\,\big]_\eta$.

(d) Dovendo trovare una biiezione $\mathbb{Q}^*_\times \xhookrightarrow{\ \ } \mathbb{Q}^*\Big/\eta$ dall'insieme $\mathbb{Q}^*_\times$ all'insieme quoziente $\mathbb{Q}^*\Big/\eta$, ricordiamo che esiste una funzione suriettiva $\pi : \mathbb{Q}^* \twoheadrightarrow \mathbb{Q}^*\Big/\eta$ da $\mathbb{Q}^*$ al suo quoziente $\mathbb{Q}^*\Big/\eta$, detta *proiezione canonica*, definita da $\pi(q) := [\,q\,]_\eta$ per

ogni $q \in \mathbb{Q}^*$. Passiamo allora considerare la restrizione di tale funzione al sottoinsieme $\mathbb{Q}^*_\times := \big\{\, n/d \;\big|\; n\,,d \in (1+2\,\mathbb{Z}) \big\}$ del suo dominio, cioè

$$\pi' : \mathbb{Q}^*_\times \longrightarrow \mathbb{Q}^* \Big/ \eta \quad , \qquad \pi'(q) := [\,q\,]_\eta \quad q \in \mathbb{Q}^* \tag{2}$$

e andiamo a dimostrare che tale π' è effettivamente biiettiva, cioè suriettiva e iniettiva.

Suriettività: Per ogni $[\,q\,]_\eta \in \mathbb{Q}^* \Big/ \eta$, scriviamo q nella forma $q = n'/d'$ con $n', d' \in \mathbb{Z}^* := \mathbb{Z}\backslash\{0\}$. Siano poi 2^{e_n} la massima potenza di 2 che divida n' (in $\mathbb{Z}$) e 2^{e_d} la massima potenza di 2 che divida d', con $e_n\,, e_d \in \mathbb{N}$: allora $n' = 2^{e_n} n$ e $d' = 2^{e_d} d$ con n e d entrambi non divisibili per 2, cioè $n\,, d \in (1+2\,\mathbb{Z})$. Pertanto $n/d = \big(2^{e_n} n\big) \Big/ \big(2^{e_d} d\big) = 2^{e_n - e_d}\, n/d$ con $(e_n - e_d) \in Z$, quindi $\big(n'/d'\big)\big(n/d\big)^{-1} = 2^{e_n - e_d}$ che significa che $\big(n'/d'\big)\,\eta\,\big(n/d\big)$. Ma allora $\big[\,n'/d'\,\big]_\eta = \big[\,n/d\,\big]_\eta = \pi\big(n/d\big) = \pi'\big(n/d\big)$ con $n/d \in \mathbb{Q}^*_\times$; perciò abbiamo $n'/d' \in Im\big(\pi'\big)$, e possiamo così concludere che π' è suriettiva, q.e.d.

Iniettività: Per ogni $q_1\, q_2 \in \mathbb{Q}^*_\times$ tali che $\pi'(q_1) = \pi'(q_2)$, abbiamo

$$\pi'(q_1) = \pi'(q_2) \implies \big[\,q_1\,\big]_\eta = \big[\,q_2\,\big]_\eta \implies q_1\,\eta\,q_2 \implies \exists\, z \in \mathbb{Z} \,:\, q_1\, q_2^{-1} = 2^z \tag{3}$$

Ora, per ipotesi abbiamo $q_1 = n_1/d_1$ e $q_2 = n_2/d_2$ con $n_1\,, d_1\,, n_2\,, d_2 \in (1+2\,\mathbb{Z})$. Ma dalla (3) otteniamo anche $q_1 = 2^z\, q_2$, da cui $n_1\, d_2 = 2^z\, n_2\, d_1$: quest'ultima identità è compatibile con $n_1\,, d_1\,, n_2\,, d_2 \in (1+2\,\mathbb{Z})$ — tutti dispari! — se e soltanto se $z = 0$, che a sua volta implica che $q_1 = q_2$. Perciò concludiamo che la funzione π' è iniettiva, q.e.d.

Quanto sopra dimostra che la funzione π' considerata in (2) è biiettiva, e quindi è una biiezione del tipo richiesto: questo risolve il quesito *(d)*.

[2] — Per ogni $n \in \mathbb{N}$, osserviamo che il numero

$$f(n) \;:=\; n^{55} + 2\,n^{50} + 3\,n^{45} + 4\,n^3 + 5\,n^2 + 6\,n$$

è divisibile per 7 se e soltanto se è congruente a 0 modulo 7; a sua volta, questo equivale a dire che la classe di congruenza modulo 7 di $f(n)$ — che indichiamo con $\overline{f(n)}$, ed è elemento di $\mathbb{Z}\big/\equiv_7 \;=: \mathbb{Z}_7$, l'anello degli interi modulo 7 — è uguale a quella di 0 — indicata con $\overline{0}$. In formule, per ogni $n \in \mathbb{N}$ abbiamo

$$7 \,\Big|\, f(n) \iff f(n) \equiv_7 0 \iff \overline{f(n)} = \overline{0} \;\; \big(\in \mathbb{Z}_7\big)$$

Pertanto, per dimostrare l'enunciato ci basta dimostrare che $\overline{f(n)} = \overline{0}$ nell'anello $\mathbb{Z}_7$.

Per cominciare abbiamo

$$\overline{f(n)} \;=\; \overline{n^{55} + 2\,n^{50} + 3\,n^{45} + 4\,n^3 + 5\,n^2 + 6\,n} \;=\; \overline{n}^{\,55} + \overline{2}\,\overline{n}^{\,50} + \overline{3}\,\overline{n}^{\,45} + \overline{4}\,\overline{n}^{\,3} + \overline{5}\,\overline{n}^{\,2} + \overline{6}\,\overline{n}$$

dunque $\overline{f(n)}$ è dato da un'espressione polinomiale in $\overline{n}$ a coefficienti in $\mathbb{Z}_7$ con termine noto nullo.

Ora, per ogni $n \in \mathbb{N}$ tale che $\overline{n} = \overline{0}$ la suddetta espressione polinomiale ci dà

$$\overline{f(0)} \;=\; \overline{0}^{\,55} + \overline{2}\cdot\overline{0}^{\,50} + \overline{3}\cdot\overline{0}^{\,45} + \overline{4}\cdot\overline{0}^{\,3} + \overline{5}\cdot\overline{0}^{\,2} + \overline{6}\cdot\overline{0} \;=\; \overline{0} + \overline{0} + \overline{0} + \overline{0} + \overline{0} + \overline{0} \;=\; \overline{0}$$

così che $\overline{f(0)} = \overline{0}$, q.e.d. Per ogni $n \in \mathbb{N}$ invece tale che $\overline{n} \neq \overline{0}$ il Piccolo Teorema di Fermat si ha $\overline{n}^{\,6} = \overline{1}$ (perché 7 è primo e $7 - 1 = 6$), da cui segue anche che

$$\overline{n}^{\,55} = \overline{n}^{\,6\cdot 9+1} = \overline{n} \quad , \quad \overline{n}^{\,50} = \overline{n}^{\,6\cdot 8+2} = \overline{n}^{\,2} \quad , \quad \overline{n}^{\,45} = \overline{n}^{\,6\cdot 7+3} = \overline{n}^{\,3}$$

Allora la precedente espressione polinomiale di $\overline{f(n)}$ ci dà

$$\begin{aligned}\overline{f(n)} \,&=\, \overline{n}^{\,55} + \overline{2}\,\overline{n}^{\,50} + \overline{3}\,\overline{n}^{\,45} + \overline{4}\,\overline{n}^{\,3} + \overline{5}\,\overline{n}^{\,2} + \overline{6}\,\overline{n} \,=\, \overline{n} + \overline{2}\,\overline{n}^{\,2} + \overline{3}\,\overline{n}^{\,3} + \overline{4}\,\overline{n}^{\,3} + \overline{5}\,\overline{n}^{\,2} + \overline{6}\,\overline{n} \,= \\ &=\, \big(\overline{1} + \overline{6}\big)\,\overline{n} + \big(\overline{2} + \overline{5}\big)\,\overline{n}^{\,2} + \big(\overline{3} + \overline{4}\big)\,\overline{n}^{\,3} \,=\, \overline{0}\,\overline{n} + \overline{0}\,\overline{n}^{\,2} + \overline{0}\,\overline{n}^{\,3} \,=\, \overline{0} + \overline{0} + \overline{0} \,=\, \overline{0}\end{aligned}$$

così che $\overline{f(n)} = \overline{0}$, q.e.d.

[3] — Richiamiamo le due funzioni da studiare, che sono

$$\begin{aligned}&\tau : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \quad , \quad \overline{z} \mapsto \tau(\overline{z}) := -\overline{z} && \forall\ \overline{z} \in \mathbb{Z}_n \\ &\rho : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \quad , \quad \overline{z} \mapsto \rho(\overline{z}) := \overline{z} + \overline{1} && \forall\ \overline{z} \in \mathbb{Z}_n\end{aligned}$$

(a) La funzione τ è senz'altro invertibile perché ha per inversa $\tau^{-1} = \tau$, in quanto $-(-\overline{z}) = \overline{z}$ per ogni $\overline{z} \in \mathbb{Z}_n$. Analogamente, la funzione ρ è anch'essa invertibile, perché ne esiste la funzione inversa ρ^{-1} descritta da $\rho^{-1}(\overline{z}) := \overline{z} - \overline{1}$, per ogni $\overline{z} \in \mathbb{Z}_n$.

(b) Per τ abbiamo $\tau^2 = id_{\mathbb{Z}_n}$ perché $\tau^2(\overline{z}) = \tau\big(\tau(\overline{z})\big) = -(-\overline{z}) = \overline{z} = id_{\mathbb{Z}_n}(\overline{z})$ per $\overline{z} \in \mathbb{Z}_n$; d'altra parte chiaramente $\tau \neq id_{\mathbb{Z}_n}$ e quindi concludiamo che τ ha ordine 2.

Per ρ abbiamo $\rho^s(\overline{z}) = \overline{z} + \overline{s}$ per ogni $\overline{z} \in \mathbb{Z}_n$ e $s \in \mathbb{Z}$; allora da $\overline{z} + \overline{n} = \overline{z}$ segue che $\rho^n = id_{\mathbb{Z}_n}$, mentre da $\overline{z} + \overline{s} \neq \overline{z}$ per ogni s tale che $0 < s < n$ segue che $\rho^s \neq id_{\mathbb{Z}_n}$ per $0 < s < n$. In conclusione tutto questo significa appunto che ρ ha ordine n, q.e.d.

(c) Nel dimostrare il punto *(b)* abbiamo visto che $\rho^s(\overline{z}) = \overline{z} + \overline{s}$ per ogni $\overline{z} \in \mathbb{Z}_n$ e $s \in \mathbb{Z}$. Da questo segue che, per ogni $\overline{z} \in \mathbb{Z}_n$ e $k \in \mathbb{Z}$, si ha

$$\begin{aligned}\big(\tau \circ \rho^k\big)(\overline{z}) \,&=\, \tau\big(\rho^k(\overline{z})\big) \,=\, \tau\big(\overline{z} + \overline{k}\big) \,=\, \tau\big(\overline{z+k}\big) \,=\, -\big(\overline{z+k}\big) \,=\, -\overline{z} - \overline{k} \\ \big(\rho^{n-k} \circ \tau\big)(\overline{z}) \,&=\, \rho^{n-k}\big(\tau(\overline{z})\big) \,=\, \rho^{n-k}\big(-\overline{z}\big) \,=\, \rho^{n-k}\big(\overline{-z}\big) \,= \\ &= \overline{-z} + \overline{n-k} \,=\, -\overline{z} + \overline{n} - \overline{k} \,=\, -\overline{z} - \overline{k}\end{aligned}$$

dunque per ogni $k \in \mathbb{Z}$ abbiamo $\big(\tau \circ \rho^k\big)(\overline{z}) = \big(\rho^{n-k} \circ \tau\big)(\overline{z})$ per ogni $\overline{z} \in \mathbb{Z}_n$, quindi in sintesi $\tau \circ \rho^k = \rho^{n-k} \circ \tau$, q.e.d.

(d) Ricordiamo ancora che nel dimostrare il punto *(b)* abbiamo trovato che $\rho^s(\overline{z}) = \overline{z} + \overline{\ell}$ per ogni $\overline{z} \in \mathbb{Z}_n$ e $\ell \in \mathbb{Z}$. Da questo segue che $\rho^\ell = \tau$ se e soltanto se $\overline{z} + \overline{\ell} = \rho^\ell(\overline{z}) = \tau(\overline{z}) = -\overline{z}$, cioè $\overline{z} + \overline{\ell} = -\overline{z}$, per ogni $\overline{z} \in \mathbb{Z}_n$. In particolare, per $\overline{z} = \overline{0}$ ciò implica $\overline{\ell} = \overline{0}$, il che significa che $\ell \in n\,\mathbb{Z}$, cioè $\ell = n\,\zeta$ per un certo $z \in \mathbb{Z}$. Siccome sappiamo già che ρ ha ordine n, otteniamo allora che $\rho^\ell = \rho^{n\,\zeta} = \big(\rho^n\big)^\zeta = \big(id_{\mathbb{Z}_n}\big)^\zeta = id_{\mathbb{Z}_n}$; d'altra parte $id_{\mathbb{Z}_n} \neq \tau$, dunque l'ipotesi $\rho^\ell = \tau$ è assurda, quindi $\rho^\ell \neq \tau$ per ogni $\ell \in \mathbb{Z}$, q.e.d.

(e) Dalla teoria generale sappiamo che il sottogruppo $\big\langle\, \tau\,, \rho\,\big\rangle$ di $\big(\mathcal{S}(\mathbb{Z}_n)\,;\,\circ\big)$ generato da τ e ρ è descritto da prodotti di fattori in sequenza che sono alternativamente una potenza non banale di τ e una potenza non banale di ρ: in particolare, in ogni tale

prodotto il primo fattore può essere una potenza (non banale) di τ o di ρ. Inoltre, poiché τ ha ordine 2, ogni sua potenza non banale è uguale a $\tau^1 = \tau$, e analogamente poiché ρ ha ordine n ogni sua potenza non banale è uguale a una della forma ρ^e con $0 < e < n$. Perciò esplicitamente abbiamo

$$\big\langle \tau\,,\rho \big\rangle \;=\; \Big\{ \tau\circ\rho^{e_1}\circ\tau\circ\rho^{e_2}\circ\cdots\,,\; \rho^{e_1}\circ\tau\circ\rho^{e_2}\circ\tau\circ\cdots \;\Big|\; e_1\,,e_2\,,\cdots\in\{0\,,1\,,\dots n-1\}\Big\}$$

Ora, dal punto *(c)* ricordiamo le identità $\tau\circ\rho^k = \rho^{n-k}\circ\tau$ — per ogni $\overline{z}\in\mathbb{Z}_n$. Sfruttando più volte queste identità, ogni prodotto della forma $\tau\circ\rho^{e_1}\circ\tau\circ\rho^{e_2}\circ\cdots$ oppure $\rho^{e_1}\circ\tau\circ\rho^{e_2}\circ\tau\circ\cdots$ può essere riscritto (in un numero finito di passi) nella forma $\tau^s\circ\rho^\ell$ con $s\in\mathbb{N}$ e $\ell\in\mathbb{Z}$: ad esempio,

$$\begin{aligned}\tau\circ\rho^{e_1}\circ\tau\circ\rho^{e_2}\circ\tau\circ\rho^{e_3}\circ\cdots\circ\tau\circ\rho^{e_s} \;&=\; \tau\circ\tau\circ\rho^{n-e_1}\circ\rho^{e_2}\circ\tau\circ\rho^{e_3}\circ\cdots\circ\tau\circ\rho^{e_s} \;=\\ =\;\tau^2\circ\rho^{n-e_1+e_2}\circ\tau\circ\rho^{e_3}\circ\cdots\circ\tau\circ\rho^{e_s} \;&=\; \tau^2\circ\tau\circ\rho^{n-(n-e_1+e_2)}\circ\rho^{e_3}\circ\cdots\circ\tau\circ\rho^{e_s} \;=\\ =\;\tau^3\circ\rho^{e_1-e_2+e_3}\circ\cdots\circ\tau\circ\rho^{e_s} \;&=\; \cdots \;=\; \tau^s\circ\rho^{e_1-e_2+e_3-\cdots+(-1)^{s+1}e_s}\end{aligned}$$

Inoltre, ricordando che τ ha ordine 2 e ρ ha ordine n possiamo riscrivere $\tau^s = \tau^t$ e $\rho^\ell = \rho^e$ per opportuni esponenti $t\in\{0\,,1\}$ ed $e\in\{0\,,1\,,\dots,n-1\}$. Pertanto otteniamo che il sottogruppo $\big\langle \tau\,,\rho\big\rangle$ può essere riscritto nella forma

$$\big\langle \tau\,,\rho \big\rangle \;=\; \Big\{ \tau^t\circ\rho^e \;\Big|\; t\in\{0\,,1\}\,,\; e\in\{0\,,1\,,\dots,n-1\}\Big\}$$

Abbiamo quindi una funzione suriettiva

$$\phi : \{0\,,1\}\times\{0\,,1\,,\dots,n-1\} \;\twoheadrightarrow\; \big\langle \tau\,,\rho\big\rangle\;, \qquad (t\,,e)\;\mapsto\; \phi(\,t\,,e) := \tau^t\circ\rho^e \tag{4}$$

perciò a livello di cardinalità abbiamo

$$\big|\big\langle \tau\,,\rho\big\rangle\big| \;\le\; \big|\{0\,,1\}\times\{0\,,1\,,\dots,n-1\}\big| \;=\; \big|\{0\,,1\}\big|\cdot\big|\{0\,,1\,,\dots,n-1\}\big| \;=\; 2\,n$$

In aggiunta, la funzione ϕ in (4) è anche iniettiva, e quindi biiettiva. Infatti, se abbiamo $(\,t_1\,,e_1)\,,(\,t_2\,,e_2)\in\{0\,,1\}\times\{0\,,1\,,\dots,n-1\}$ tali che $\phi(\,t_1\,,e_1) = \phi(\,t_2\,,e_2)$ ne segue

$$\begin{aligned}\tau^{t_1}\circ\rho^{e_1} \;=\; \phi(\,t_1\,,e_1) \;=\; \phi(\,t_2\,,e_2) \;=\; \tau^{t_2}\circ\rho^{e_2} \;\Longrightarrow\\ \Longrightarrow\; \rho^{e_1}\circ\rho^{-e_2} = \tau^{-t_1}\circ\tau^{t_2} \;\Longrightarrow\; \rho^{e_1-e_2} \;=\; \tau^{-t_1+t_2} \;\Longrightarrow\; \rho^e \;=\; \tau^t\end{aligned}$$

con $e := e_1 - e_2\in\mathbb{Z}$ e $t := -t_1 + t_2\in\mathbb{Z}$. Ricordando che τ ha ordine 2 l'identità $\rho^e = \tau^t$ diventa $\rho^e = \tau$ se $t\equiv 1 \pmod 2$ e $\rho^e = id_{\mathbb{Z}_n}$ se $t\equiv 0 \pmod 2$. Ora, la prima eventualità è impossibile, in forza del punto *(d)*; dunque deve valere la seconda, perciò abbiamo $t\equiv 0 \pmod 2$, che significa che $t_1 = t_2$ (dato che $t_1\,,t_2\in\{0\,,1\}$), $\rho^e = id_{\mathbb{Z}_n}$, che significa che $e\equiv 0 \pmod n$ e quindi $e_1 = e_2$ (dato che $e_1\,,e_2\in\{0\,,1\,,\dots,n-1\}$). Dunque $(t_1\,,e_1) = (t_2\,,e_2)$, e possiamo concludere che la funzione ϕ è iniettiva, dunque — essendo anche suriettiva — è biiettiva.

Infine, dall'esistenza della biiezione $\phi : \{0\,,1\}\times\{0\,,1\,,\dots,n-1\} \;\hookrightarrow\!\!\!\!\!\rightarrow\; \big\langle \tau\,,\rho\big\rangle$ definita in (4) possiamo concludere che

$$\big|\big\langle \tau\,,\rho\big\rangle\big| \;=\; \big|\{0\,,1\}\times\{0\,,1\,,\dots,n-1\}\big| \;=\; \big|\{0\,,1\}\big|\cdot\big|\{0\,,1\,,\dots,n-1\}\big| \;=\; 2\,n$$

dunque in conclusione $\big|\big\langle \tau\,,\rho\big\rangle\big| = 2\,n$, q.e.d.

[4] — Ricordiamo che in ogni anello unitario R si indica con $U(R)$ il sottoinsieme di tutti gli elementi di R che siano invertibili rispetto alla moltiplicazione; tale insieme è (automaticamente) un gruppo rispetto alla moltiplicazione di R. Nel caso in esame abbiamo $R := \mathbb{Z}_{35}$, l'anello degli interi modulo 35.

(a) Dalla teoria generale sappiamo che in ogni anello del tipo $\mathbb{Z}_n$ il gruppo $U(\mathbb{Z}_n)$ è dato da $U(\mathbb{Z}_n) = \left\{ \overline{z} \,\middle|\, \text{M.C.D.}(z\,,n) = 1 \right\}$. Nel caso in esame quindi abbiamo

$$U\big(\mathbb{Z}_{35}\big) \;=\; \left\{ \overline{z} \,\middle|\, \text{M.C.D.}(z\,,n) = 1 \right\} \;= \\ = \; \left\{ \overline{1}\,,\overline{2}\,,\overline{3}\,,\overline{4}\,,\overline{6}\,,\overline{8}\,,\overline{9}\,,\overline{11}\,,\overline{12}\,,\overline{13}\,,\overline{16}\,,\overline{17}\,,\overline{18}\,,\overline{19}\,,\overline{22}\,,\overline{23}\,,\overline{24}\,,\overline{26}\,,\overline{27}\,,\overline{29}\,,\overline{31}\,,\overline{32}\,,\overline{33}\,,\overline{34} \right\}$$

(b) Dall'analisi esplicita fatta al punto *(a)* vediamo che il gruppo $U\big(\mathbb{Z}_{35}\big)$ ha ordine $\big|U\big(\mathbb{Z}_{35}\big)\big| = 24$. Questo possiamo anche ottenerlo senza bisogno di descrivere $U\big(\mathbb{Z}_{35}\big)$ esplicitamente: infatti, dalla teoria generale sappiamo che $\big|U\big(\mathbb{Z}_n\big)\big| = \varphi(n)$, dove $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ è la *funzione di Eulero*. Nel caso in esame abbiamo allora

$$\big|U\big(\mathbb{Z}_{35}\big)\big| \;=\; \varphi(35) \;=\; \varphi(7\cdot 5) \;=\; \varphi(7)\cdot\varphi(5) \;=\; (7-1)\cdot(5-1) \;=\; 6\cdot 4 \;=\; 24$$

Ora, per il Teorema di Lagrange sappiamo che ogni elemento di un gruppo gruppo finito ha ordine che divide l'ordine del gruppo stesso. In particolare, ogni elemento di $U\big(\mathbb{Z}_{35}\big)$ ha ordine che divide $\big|U\big(\mathbb{Z}_{35}\big)\big| = 24$. Poiché l'insieme dei divisori di 24 è $\{1\,,2\,,3\,,4\,,6\,,8\,,12\,,24\}$, in relazione al quesito *(b)* possiamo già rispondere che certamente *non possono esistere* in $U\big(\mathbb{Z}_{35}\big)$ elementi di ordine 5, 7, 9 oppure 10, mentre invece *possono esistere* elementi di ordine 2, 3, 4 oppure 6: per sapere però se elementi del secondo tipo effettivamente esistano davvero dobbiamo fare un'indagine esplicita.

L'elemento più "semplice" di ordine maggiore di 1 — dunque diverso da $\overline{1}$ — è $\overline{2}$, quindi iniziamo cercando l'ordine di quest'ultimo, per cui ne calcoliamo le potenze. Siccome il suo ordine può essere soltanto uno dei valori in $\{2\,,3\,,4\,,6\,,8\,,12\,,24\}$, basta in effetti calcolare le potenze con questi esponenti (e anche meno se a un certo punto troviamo che una potenza pari a $\overline{1}$). Il conto esplicito ci dà

$$\overline{2}^{\,2} = \overline{4}\;\;,\quad \overline{2}^{\,3} = \overline{8}\;\;,\quad \overline{2}^{\,4} = \overline{16}\;\;,\quad \overline{2}^{\,6} = \big(\overline{2}^{\,3}\big)^2 = \overline{8}^{\,2} = \overline{64} = -\overline{6}\;\;, \\ \overline{2}^{\,8} = \overline{2}^{\,6}\cdot\overline{2}^{\,2} = -\overline{6}\cdot\overline{4} = -\overline{24}\;\;,\quad \overline{2}^{\,12} = \big(\overline{2}^{\,6}\big)^2 = \big(-\overline{6}\big)^2 = \overline{36} = \overline{1}$$

da cui otteniamo che $\overline{2}$ ha ordine 12. Ora, ricordiamo che se un elemento g in un gruppo G ha ordine finito N, allora per ogni divisore d di N si ha automaticamente che g^d ha ordine N/d. Applicando questo risultato generale al caso specifico di $\overline{2}$ — nel gruppo $U\big(\mathbb{Z}_{35}\big)$ — che ha ordine finito 12, e ai divisori 6, 4, 3 e 2 di 12, otteniamo che

(b.I) $\overline{2}^{\,6} = \overline{64} = \overline{29}$ ha ordine $12/6 = 2$,

(b.II) $\overline{2}^{\,4} = \overline{16}$ ha ordine $12/4 = 3$,

(b.III) $\overline{2}^{\,3} = \overline{8}$ ha ordine $12/3 = 4$,

(b.IV) $\overline{2}^{\,2} = \overline{4}$ ha ordine $12/2 = 6$.

[5] — Ricordiamo la notazione: $A := \mathbb{Z}[\,x\,]$ è l'anello dei polinomi nella variabile x a coefficienti in $\mathbb{Z}$, e $I := 5\,\mathbb{Z}[\,x\,] = \big\{\, 5\,p(x) \,\big|\, p(x) \in \mathbb{Z}[\,x\,] \,\big\}$.

(a) Per dimostrare che I è un ideale di $\mathbb{Z}[\,x\,]$ dobbiamo provare che è non vuoto, chiuso per le differenze, e che assorbe i prodotti. A tal fine abbiamo:

(a.I) $0 = 5 \cdot 0 \in I$, pensando a 0 come polinomio in $\mathbb{Z}[\,x\,]$; quindi $I \neq \emptyset$, q.e.d.

(a.II) per ogni $h(x)\,,k(x) \in I$ si ha $h(x) = 5\,p_h(x)$ e $k(x) = 5\,p_k(x)$ per certi $p_h(x)\,,p_k(x) \in \mathbb{Z}[\,x\,]$; allora $h(x) - k(x) = 5\,p_h(x) - 5\,p_k(x) = 5\,\big(\,p_h(x) - p_k(x)\big)$ con $\big(\,p_h(x) - p_k(x)\big) \in \mathbb{Z}[\,x\,]$, quindi concludiamo che $\big(h(x) - k(x)\big) \in I$, q.e.d.

(a.III) per ogni $\ell(x) \in I$ e $f(x) \in \mathbb{Z}[\,x\,]$ si ha $\ell(x) = 5\,p(x)$ per un certo $p(x) \in \mathbb{Z}[\,x\,]$; allora $\ell(x)\,f(x) = 5\,p(x)\,f(x) = 5\,\big(\,p(x)\,f(x)\big)$ con $\big(\,p(x)\,f(x)\big) \in \mathbb{Z}[\,x\,]$, quindi concludiamo che $\ell(x)\,f(x) \in I$, q.e.d.

In alternativa, si può anche provare che I è un ideale con un diverso approccio, seguito nella trattazione del punto *(b)* qui sotto.

(b) Consideriamo la funzione $\phi : \mathbb{Z}[\,x\,] \longrightarrow \mathbb{Z}_5[\,x\,]$ definita in questo modo: per ogni $p(x) \in \mathbb{Z}[\,x\,]$ scritto nella forma $p(x) = \sum_{n=0}^{N} z_n\,x^n$ per opportuni $z_0\,,\ldots,z_N \in \mathbb{Z}$, definiamo

$$\phi\big(\,p(x)\big) \;=\; \phi\Big(\,\textstyle\sum_{n=0}^{N} z_n\,x^n\Big) \;:=\; \sum_{n=0}^{N} \overline{z_n}\,x^n$$

dove indichiamo con $\overline{z} \in \mathbb{Z}_5$ la classe modulo 5 di ogni intero $z \in \mathbb{Z}$.

Osserviamo subito che tale funzione ϕ è chiaramente suriettiva, perché per ogni possibile polinomio $\sum_{n=0}^{N} \overline{c_n}\,x^n \in \mathbb{Z}_5[\,x\,]$ esiste (ovviamente!...) $\sum_{n=0}^{N} c_n\,x^n \in \mathbb{Z}_5[\,x\,]$ tale che $\phi\Big(\,\sum_{n=0}^{N} c_n\,x^n\Big) = \sum_{n=0}^{N} \overline{c_n}\,x^n$. Inoltre, tale ϕ è anche un morfismo di anelli, come si verifica direttamente (in breve, perché le operazioni di somma e prodotto in un qualsiasi anello di polinomi sono definite sempre allo stesso modo, e perché la funzione $\mathbb{Z} \longrightarrow \mathbb{Z}_5\,\big(\,z \mapsto \overline{z}\,\big)$ è un morfismo di anelli). Pertanto, dal *Teorema Fondamentale di Omomorfismo per Anelli* otteniamo che ϕ induce un isomorfismo di anelli

$$\begin{aligned} \phi_* \,:\, \mathbb{Z}[\,x\,]\Big/\mathit{Ker}\,(\phi) \lhook\joinrel\longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}_5[\,x\,] \quad , \qquad \overline{p(x)} \;\mapsto\; \phi_*\big(\,\overline{p(x)}\,\big) \;=\; \phi\big(\,p(x)\big) \\ \forall\;\; \overline{p(x)} := p(x) + \mathit{Ker}\,(\phi) \;\in\; \mathbb{Z}[\,x\,]\Big/\mathit{Ker}\,(\phi) \end{aligned} \tag{5}$$

Andiamo ora a calcolare il nucleo $\mathit{Ker}\,(\phi)$ di ϕ. Dalle definizioni abbiamo

$$\mathit{Ker}\,(\phi) \;:=\; \big\{\, p(x) \in \mathbb{Z}[\,x\,] \,\big|\, \phi\big(\,p(x)\big) = 0 \,\big\} = \left\{ \sum_{n=0}^{N} z_n\,x^n \in \mathbb{Z}[\,x\,]\, g|\, \phi\left(\sum_{n=0}^{N} z_n\,x^n\right) = 0 \right\} =$$

$$= \left\{ \sum_{n=0}^{N} z_n\,x^n \in \mathbb{Z}[\,x\,] \;\middle|\; \textstyle\sum_{n=0}^{N} \overline{z_n}\,x^n = \,0 \right\} = \left\{ \sum_{n=0}^{N} z_n\,x^n \in \mathbb{Z}[\,x\,] \;\middle|\; \overline{z_n} = \,\overline{0} \;\;\forall\, n \right\} =$$

$$= \left\{ \sum_{n=0}^{N} z_n\,x^n \in \mathbb{Z}[\,x\,] \;\middle|\; \textstyle\sum_{n=0}^{N} \overline{z_n}\,x^n \in 5\,\mathbb{Z} \right\} \;=\; 5\,\mathbb{Z}[\,x\,] =: I$$

dunque in conclusione $\mathit{Ker}\,(\phi) \;=\; I$. Ciò dimostra che I è un ideale di $\mathbb{Z}[\,x\,]$ — rispondendo così al quesito in *(a)* — e inoltre, per quanto già visto, dimostra anche che $\mathbb{Z}[\,x\,]\Big/I \;=\; \mathbb{Z}[\,x\,]\Big/\mathit{Ker}\,(\phi)$ è isomorfo all'anello $\mathbb{Z}_5[\,x\,]$, e un possibile isomorfismo esplicito da $\mathbb{Z}[\,x\,]\Big/I \;=\; \mathbb{Z}[\,x\,]\Big/\mathit{Ker}\,(\phi)$ a $\mathbb{Z}_5[\,x\,]$ e quello dato in (5), q.e.d.

[6] — Ricordiamo che l'anello degli interi di Gauss $\mathbb{Z}[\,i\,]$ è *euclideo*, con valutazione $v : \mathbb{Z}[\,i\,] \longrightarrow \mathbb{N}$ definita da $v(a+i\,b) := a^2+b^2$ per ogni $a+i\,b \in \mathbb{Z}[\,i\,]$. In particolare tale valutazione è *moltiplicativa*, cioè si ha $v(\alpha\,\beta) = v(\alpha)\,v(\beta)$ per ogni $\alpha\,,\beta \in \mathbb{Z}[\,i\,]$.

Da questo fatto segue che si può usare l'algoritmo delle divisioni successive per calcolare il M.C.D. tra due qualunque elementi in $\mathbb{Z}[\,i\,]$, nonché una identità di Bézout per tale M.C.D.; questo a sua volta permette anche di risolvere ogni equazione diofantea. Inoltre, ogni ideale $\mathbb{Z}[\,i\,]$ è senz'altro principale, e se è generato da due elementi sarà anche generato (singolarmente) dal M.C.D. tra tali elementi, che potremo calcolare esplicitamente come osservato poc'anzi. Infine, la riducibilità o irriducibilità di un qualunque elemento potrà essere analizzata in prima battuta considerando la riducibilità o irriducibilità della valutazione dell'elemento stesso.

(a) Dovendo risolvere l'equazione diofantea

$$(-3-i\,)\cdot x \;+\; (1+2\,i\,)\cdot y \;=\; -2+5\,i$$

nell'anello euclideo $\mathbb{Z}[\,i\,]$, per prima cosa calcoliamo il M.C.D. tra i coefficienti delle incognite nell'equazione diofantea assegnata, mediante *l'algoritmo euclideo delle divisioni successive*. I calcoli espliciti ci danno

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

quindi l'algoritmo si arresta al primo passo dandoci $\mathrm{MCD}\big(-3-i\,,1+2\,i\,\big) \sim (\,1+2\,i\,)$; si noti che la divisione con resto (banale!) è ottenuta tramite i seguenti calcoli in $\mathbb{C}$:

$$(-3-i\,)\,(1+2\,i\,)^{-1} \;=\; \frac{(-3-i\,)\,(1-2\,i\,)}{v(1+2\,i\,)} \;=\; \frac{-5+5\,i}{5} \;=\; -1+i$$

Ora dobbiamo verificare se $\mathrm{MCD}\big(-3-i\,,1+2\,i\,\big) \sim (\,1+2\,i\,)$ divida il termine noto $(-2+5\,i\,)$ dell'equazione diofantea sotto esame: in caso positivo l'equazione ha soluzioni, in caso negativo invece non ne ha. Di nuovo, il calcolo esplicito ci dà

$$-2+5\,i \;=\; (1+2\,i\,)\,(2+2\,i\,) \;+\; (-i\,)$$

dunque $(1+2\,i\,)$ *non divide* $(-2+5\,i\,)$, e quindi concludiamo che *l'equazione diofantea considerata non ha soluzioni*.

(b) Come al punto *(a)*, dovendo risolvere l'equazione diofantea

$$(1-3\,i\,)\cdot x \;+\; (-2+7\,i\,)\cdot y \;=\; 2-5\,i$$

cominciamo calcolando il M.C.D. tra i coefficienti delle incognite, mediante *l'algoritmo euclideo delle divisioni successive*. I calcoli espliciti ci danno

$$\begin{aligned} 1-3\,i \;&=\; (-2+7\,i\,)\,0 \;+\; (\,1-3\,i\,) && \text{con} \quad v(\,1-3\,i\,) = 10 < 59 = v(-2+7\,i\,) \\ -2+7\,i \;&=\; (\,1-3\,i\,)\,(-2) \;+\; i && \text{con} \quad v(i\,) = 1 < 10 = v(\,1-3\,i\,) \\ 1-3\,i \;&=\; i\,(\,1-3\,i\,) \;+\; 0 \end{aligned}$$

da cui troviamo che $\mathrm{M.C.D.}\big(1-3\,i\,,-2+7\,i\,\big) \;\sim\; i$: quest'ultimo è un elemento invertibile in $\mathbb{Z}[\,x\,]$, e quindi senz'altro divide il termine noto dell'equazione diofantea assegnata, per cui tale equazione ammette soluzioni.

Per trovare una soluzione esplicita, cominciamo calcolando una *identità di Bézout* per $\text{M.C.D.}\big(1-3\,i\,,-2+7\,i\big)\sim i$, che possiamo ricavare invertendo i calcoli precedenti. Da questi infatti ("invertendo" ciascuna delle prime due identità, e poi invertendo l'ordine tra di loro) ricaviamo

$$\begin{aligned} i \;&=\; -2+7\,i+(\,1-3\,i\,)\,(+2) \\ 1-3\,i \;&=\; (\,1-3\,i\,)\;+\;(-2+7\,i\,)\,0 \end{aligned}$$

e quindi

$$i \;=\; (\,1-3\,i\,)\cdot 2+(-2+7\,i\,)\cdot 1 \tag{6}$$

che è appunto un'identità di Bézout come richiesto.

A questo punto scriviamo il termine noto della nostra equazione diofantea, che è $(2-5\,i\,)$, come multiplo di $i\sim\text{M.C.D.}\big(1-3\,i\,,-2+7\,i\big)$, precisamente

$$2-5\,i \;=\; i\,(-5-2\,i\,) \tag{7}$$

Dalla (6) e dalla (7) insieme otteniamo allora

$$\begin{aligned} 2-5\,i \;=\; i\,(-5-2\,i\,) \;&=\; \big((\,1-3\,i\,)\cdot 2+(-2+7\,i\,)\cdot 1\big)\,(-5-2\,i\,) \;= \\ &=\; (\,1-3\,i\,)\cdot(-10-4\,i\,)+(-2+7\,i\,)\cdot(-5-2\,i\,) \end{aligned}$$

in breve $(\,1-3\,i\,)\cdot(-10-4\,i\,)+(-2+7\,i\,)\cdot(-5-2\,i\,)\;=\;2-5\,i$, che ci dice che la coppia $(x\,,y)\;:=\;\big(-10-4\,i\,,-5-2\,i\big)$ è una soluzione dell'equazione diofantea in esame.

(c) Ricordiamo che $I:=\big(1-3\,i\,,7+2\,i\big)$ è l'ideale di $\mathbb{Z}[\,i\,]$ generato dai due elementi $(1-3\,i\,)$ e $(7+2\,i\,)$. Siccome l'anello $\mathbb{Z}[\,i\,]$ è euclideo, esso è anche a ideali principali, quindi in particolare l'ideale I è principale, cioè della forma $I=\big(\,\delta\,\big)$ per un opportuno generatore $\delta\in\mathbb{Z}[\,i\,]$; allora dalle identità $\big(1-3\,i\,,7+2\,i\big)=:I=\big(\,\delta\,\big)$ segue subito che abbiamo $\delta\sim\text{M.C.D.}\big(\,1-3\,i\,,7+2\,i\,\big)$, quindi dobbiamo soltanto determinare tale M.C.D. A tal fine, osserviamo che $7+2\,i\;=\;(-i\,)\,(-2+7\,i\,)$, con $(-i\,)$ invertibile in $\mathbb{Z}[\,i\,]$: perciò $(7+2\,i\,)$ e $(-2+7\,i\,)$ hanno esattamente gli stessi divisori, e quindi ne segue che $\text{M.C.D.}\big(\,1-3\,i\,,7+2\,i\,\big)\;\sim\;\text{M.C.D.}\big(\,1-3\,i\,,-2+7\,i\,\big)$. Siccome trattando il punto *(b)* abbiamo già calcolato che $\text{M.C.D.}\big(\,1-3\,i\,,-2+7\,i\,\big)\sim i$, possiamo concludere che $\text{M.C.D.}\big(\,1-3\,i\,,7+2\,i\,\big)\;\sim\;i$ e quindi in conclusione $\delta=i$ è un generatore dell'ideale I. In particolare, dato che i è invertibile in $\mathbb{Z}[\,i\,]$ abbiamo $I=\big(i\big)=\big(1\big)=\mathbb{Z}[\,i\,]$.

(d) Dato $\alpha\in\mathbb{Z}[\,i\,]\setminus\{0\}$, osserviamo che ogni sua fattorizzazione $\alpha=\beta\,\gamma$ in $\mathbb{Z}[\,i\,]\setminus\{0\}$ induce una fattorizzazione $v(\alpha)=v(\beta)\,v(\gamma)$. Ora, α è *riducibile* se esiste una sua fattorizzazione *non banale*, cioè del tipo $\alpha=\beta\,\gamma$ come sopra con β e γ *non invertibili*, che equivale a dire che $v(\beta)\neq 1\neq v(\gamma)$ — in quanto l'insieme degli invertibili in un anello euclideo A, com'è $\mathbb{Z}[\,i\,]$, è caratterizzato da $U(A)=\big\{\,a\in A\,\big|\,v(a)=v(1)\,\big\}$, e in $\mathbb{Z}[\,i\,]$ si ha $v(1)=1$. Allora la fattorizzazione non banale $\alpha=\beta\,\gamma$ in $\mathbb{Z}[\,i\,]\setminus\{0\}$ induce una fattorizzazione $v(\alpha)=v(\beta)\,v(\gamma)$ che è a sua volta *non banale*, perché $v(\beta)\neq 1\neq v(\gamma)$.

Ciò premesso, se $\alpha\in\mathbb{Z}[\,i\,]\setminus\{0\}$ è un elemento tale che $v(\alpha)$ sia *irriducibile* (o *primo*) in $\mathbb{N}\setminus\{0\}$ un'eventuale fattorizzazione $\alpha=\beta\,\gamma$ in $\mathbb{Z}[\,i\,]\setminus\{0\}$ induce la fattorizzazione $v(\alpha)=v(\beta)\,v(\gamma)$ di $v(\alpha)$ che è necessariamente banale, cioè con $v(\beta)=1$ oppure $v(\gamma)=1$, dunque β invertibile o γ invertibile, per cui la fattorizzazione iniziale $\alpha=\beta\,\gamma$ è banale. In conclusione, *se $v(\alpha)$ è irriducibile in $\mathbb{N}$, allora α è irriducibile in $\mathbb{Z}[\,i\,]$*.

Venendo al caso in esame, abbiamo

$$v(1+2\,i\,)=1^2+2^2=5\;,\;\; v(-3-i\,)=(-3)^2+(-1)^2=10\;,\;\; v(\,7+2\,i\,)=7^2+2^4=53$$

Poiché 5 e 53 sono numeri primi, dunque irriducibili in $\mathbb{N}$, dall'analisi precedente concludiamo che $(1+2\,i\,)$ e $(\,7+2\,i\,)$ sono *irriducibili* in $\mathbb{Z}[\,i\,]$.

Quanto a $(-3-i\,)$, osserviamo che la sola fattorizzazione non banale possibile di $v(-3-i\,)=10$ è $v(-3-i\,)=2\cdot 5$. Ora, se $(-3-i\,)=\beta\,\gamma$ è una fattorizzazione non banale di $(-3-i\,)$ in $\mathbb{Z}[\,i\,]$, abbiamo anche una fattorizzazione non banale $v(-3-i\,)=v(\beta)\cdot v(\gamma)$, che deve coincidere con $v(-3-i\,)=2\cdot 5$, quindi $\big\{v(\beta)\,,v(\gamma)\big\}=\{2\,,5\}$, diciamo

$$\begin{aligned} &v(\beta)=2\;\;, \qquad \text{e quindi} \qquad \beta\in\big\{\,\pm(1+i\,)\,,\pm(1-i\,)\big\} \\ &v(\gamma)=5\;\;, \qquad \text{e quindi} \qquad \gamma\in\big\{\,\pm(1+2\,i\,)\,,\pm(1-2\,i\,)\,,\pm(2+i\,)\,,\pm(2-i\,)\big\} \end{aligned} \tag{8}$$

A questo punto, analizzando tutti i vari possibili prodotti fatti scegliendo un fattore β e un fattore γ scelti nei due insiemi indicati in (8) troviamo che effettivamente esistono per $(-3-i\,)$ tutte e sole le seguenti fattorizzazioni non banali di $(-3-i\,)$

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

dunque concludiamo che $(-3-i\,)$ è *riducibile*.