

ALGEBRA 1 — 2008/2009

Prof. Fabio Gavarini

Sessione estiva anticipata — prova scritta del 9 Febbraio 2009

Svolgimento completo

N.B.: lo svolgimento qui presentato è chilometrico... Questo non vuol dire che lo svolgimento ordinario di tale compito (nel corso di un esame scritto) debba essere altrettanto lungo. Semplicemente, questo lo è perché si è colta l'occasione per spiegare — anche in diversi modi, con lunghe digressioni, ecc. ecc. — in dettaglio e con dovizia di particolari tutti gli aspetti della teoria toccati in maggiore o minore misura dal testo in esame.

..... *

[1] — Siano $n \in \mathbb{N}_+$, $E := \{1, \dots, n\} \times \{1, \dots, n\} \times \{1, \dots, n\}$, e sia $\sim$ la relazione su E definita da

$$(x, y, z) \sim (x', y', z') \iff \exists \sigma \in \mathcal{S}_n : \sigma(x) = x', \sigma(y) = y', \sigma(z) = z'.$$

- (a) Dimostrare che $\sim$ è una relazione di equivalenza;
- (b) determinare la classe di equivalenza di $(1, 1, 1)$;
- (c) descrivere l'insieme quoziente $E/\sim$.

Soluzione: (a) Per ogni $(x, y, z) \in E$, esiste $id \in \mathcal{S}_n$ tale che $id(x) = x$, $id(y) = y$, $id(z) = z$; perciò $(x, y, z) \sim (x, y, z)$ per ogni $(x, y, z) \in E$, il che significa che la relazione $\sim$ è riflessiva.

Inoltre, se per $(x_1, y_1, z_1), (x_2, y_2, z_2) \in E$ si ha $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, allora esiste $\sigma \in \mathcal{S}_n$ tale che $\sigma(x_1) = x_2$, $\sigma(y_1) = y_2$, $\sigma(z_1) = z_2$; allora si ha anche $\sigma^{-1} \in \mathcal{S}_n$, e $\sigma^{-1}(x_2) = x_1$, $\sigma^{-1}(y_2) = y_1$, $\sigma^{-1}(z_2) = z_1$, per cui $(x_2, y_2, z_2) \sim (x_1, y_1, z_1)$. Quindi la relazione $\sim$ è simmetrica.

Infine, se per $(x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3) \in E$ si ha $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, $(x_2, y_2, z_2) \sim (x_3, y_3, z_3)$, allora esistono $\sigma, \tau \in \mathcal{S}_n$ tali che $\sigma(x_1) = x_2$, $\sigma(y_1) = y_2$, $\sigma(z_1) = z_2$ e $\tau(x_2) = x_3$, $\tau(y_2) = y_3$, $\tau(z_2) = z_3$. Ne segue quindi che $(\tau \circ \sigma) \in \mathcal{S}_n$, e $(\tau \circ \sigma)(x_1) = \tau(\sigma(x_1)) = x_3$, $(\tau \circ \sigma)(y_1) = \tau(\sigma(y_1)) = y_3$, $(\tau \circ \sigma)(z_1) = \tau(\sigma(z_1)) = z_3$, per cui $(x_3, y_3, z_3) \sim (x_1, y_1, z_1)$. Quindi la relazione $\sim$ è transitiva.

In conclusione, la relazione $\sim$ è riflessiva, simmetrica e transitiva, dunque è una relazione di equivalenza, il che risolve il punto (a).

- (b) La classe di equivalenza di $(1, 1, 1)$ per la relazione $\sim$ è, per definizione,

$$\begin{aligned} [(1, 1, 1)]_{\sim} &:= \{ (x', y', z') \in E \mid (1, 1, 1) \sim (x', y', z') \} = \\ &= \{ (x', y', z') \in E \mid \exists \sigma \in \mathcal{S}_n : \sigma(1) = x', \sigma(1) = y', \sigma(1) = z' \} \quad ; \end{aligned}$$

ma allora chiaramente si ha

$$[(1, 1, 1)]_{\sim} = \{ (\sigma(1), \sigma(1), \sigma(1)) \in E \mid \sigma \in \mathcal{S}_n \} .$$

Ora, per ogni $i \in \{1, 2, \dots, n\}$ esiste certamente una permutazione $\sigma_i \in \mathcal{S}_n$ tale che $\sigma_i(1) = i$: ad esempio, una permutazione di questo tipo è

$$\sigma_i := \begin{pmatrix} 1 & 2 & \cdots & i-1 & i & i+1 & \cdots & n \\ i & 2 & \cdots & i-1 & 1 & i+1 & \cdots & n \end{pmatrix} = (1\ i) .$$

Allora si ha $\{ \sigma(1) \mid \sigma \in \mathcal{S}_n \} = \{1, 2, \dots, n\}$, e quindi si conclude che

$$[(1, 1, 1)]_{\sim} = \{ (u, u, u) \in E \mid u \in \{1, 2, \dots, n\} \} = \{ (1, 1, 1), (2, 2, 2), \dots, (n, n, n) \}$$

(c) Cominciamo osservando che se $n = 1$ allora $E = \{(1, 1, 1)\}$, e non c'è molto da dire: semplicemente si ha

$$[(1, 1, 1)]_{\sim} = \{(1, 1, 1)\} , \quad E/\sim = \{ [(1, 1, 1)]_{\sim} \} = \{ \{(1, 1, 1)\} \} .$$

Se invece $n \geq 2$, allora procediamo come segue

Nella parte (b) si è calcolata una classe di equivalenza particolare — quella di $(1, 1, 1)$ — per la relazione $\sim$, e si è trovato che essa è composta esattamente da *tutte e sole le terne (in E) i cui elementi sono tutti uguali*. Analizzando il procedimento con cui si è ottenuto questo risultato, è chiaro — spero... — che questo segue dal fatto che queste terne sono del tipo $(x', y', z') = (\sigma(x), \sigma(y), \sigma(z))$, al variare di $\sigma \in \mathcal{S}_n$, e inoltre x, y e z sono tutti uguali tra loro — e precisamente sono uguali a 1 (ma questo è irrilevante!).

Per l'analisi successiva, consideriamo ora una terna in cui ci siano invece *esattamente due* elementi uguali, ad esempio i primi due, dunque del tipo $(x, y, z) = (x, x, z)$, cioè con $x = y \neq z$: ad esempio, consideriamo il caso di $(x, y, z) := (1, 1, 2)$. Ora, la classe di equivalenza di $(1, 1, 2)$ per la relazione $\sim$ è (sempre per definizione)

$$\begin{aligned} [(1, 1, 2)]_{\sim} &:= \{ (x', y', z') \in E \mid (1, 1, 2) \sim (x', y', z') \} = \\ &= \{ (x', y', z') \in E \mid \exists \sigma \in \mathcal{S}_n : \sigma(1) = x', \sigma(1) = y', \sigma(2) = z' \} ; \end{aligned}$$

e quindi chiaramente si ha

$$[(1, 1, 2)]_{\sim} = \{ (\sigma(1), \sigma(1), \sigma(2)) \in E \mid \sigma \in \mathcal{S}_n \} .$$

Ora, per ogni scelta $i, j \in \{1, 2, \dots, n\}$ con $i \neq j$, abbiamo che

$$\text{esiste sempre una permutazione } \sigma_{i,j} \in \mathcal{S}_n \text{ tale che } \sigma_{i,j}(1) = i, \sigma_{i,j}(2) = j . \quad (1)$$

N.B.: Per il compito, non era strettamente necessario spiegare perché valesse la (1); in ogni caso ora lo spieghiamo, cioè facciamo vedere come si possa scegliere una possibile σ come in (1). Dobbiamo distinguere tre casi diversi, che esauriscono le varie possibilità:

— caso I: se $\{i, j\} \cap \{1, 2\} = \emptyset$, e supponendo che sia $i < j$ (tanto per comodità di scrittura), una possibile permutazione di tale tipo è

$$\sigma_{i,j} := \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & j & \cdots & n-1 & n \\ i & j & 3 & 4 & \cdots & 1 & \cdots & 2 & \cdots & n-1 & n \end{pmatrix} = (1\ i)(2\ j) = (2\ j)(1\ i)$$

— caso II: se $\{i, j\} \cap \{1, 2\} \neq \emptyset$, e $|\{i, j\} \cap \{1, 2\}| = 1$, sia ad esempio $\{i, j\} \cap \{1, 2\} = \{1\}$; allora una possibile permutazione del tipo richiesto (con $j = 1$) è

$$\sigma_{i,j} = \sigma_{i,1} := \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ i & 1 & 3 & 4 & \cdots & 2 & \cdots & n-1 & n \end{pmatrix} = (1\ i)(2\ 1) = (1\ i\ 2)$$

— caso III: se $\{i, j\} \cap \{1, 2\} \neq \emptyset$, e $|\{i, j\} \cap \{1, 2\}| = 2$, una possibile permutazione del tipo richiesto (con $i = 2, j = 1$) è

$$\sigma_{i,j} := \sigma_{2,1} := \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n-1 & n \\ 2 & 1 & 3 & 4 & \cdots & n-1 & n \end{pmatrix} = (1\ 2)$$

In ogni caso, la (1) ci assicura che esiste una $\sigma_{i,j} \in \mathcal{S}_n$ tale che

$$(\sigma_{i,j}(1), \sigma_{i,j}(1), \sigma_{i,j}(2)) = (i, i, j)$$

Pertanto, si conclude che

$$[(1, 1, 2)]_{\sim} = \{(i, i, j) \in E \mid i, j \in \{1, 2, \dots, n\}, i \neq j\}$$

che in parole si esprime così: la classe di equivalenza di $(1, 1, 2)$ è costituita da tutte le terne in cui il primo e il secondo elemento sono uguali, e il terzo invece è diverso.

Notiamo che questo segue in particolare dal fatto che nella terna $(1, 1, 2)$ ci sono due elementi uguali, mentre è diverso quello che sta in terza posizione. Allora, con analoga analisi si dimostra ovviamente che

$$[(1, 2, 1)]_{\sim} = \{(i, j, i) \in E \mid i, j \in \{1, 2, \dots, n\}, i \neq j\}$$

che significa che la classe di equivalenza di $(1, 2, 1)$ è costituita da tutte le terne in cui il primo e il terzo elemento sono uguali, e il secondo invece è diverso; analogamente si ha

$$[(2, 1, 1)]_{\sim} = \{(j, i, i) \in E \mid i, j \in \{1, 2, \dots, n\}, i \neq j\}$$

cioè la classe di equivalenza di $(2, 1, 1)$ è costituita da tutte le terne in cui il secondo e il terzo elemento sono uguali, e il primo invece è diverso.

Se $n = 2$, allora i casi presentati esauriscono tutte le possibilità, e si ha

$$E/\sim = \{[(1, 1, 1)]_{\sim}, [(1, 1, 2)]_{\sim}, [(1, 2, 1)]_{\sim}, [(2, 1, 1)]_{\sim}\}.$$

Se invece $n \geq 3$, allora si presenta ancora un'altra possibilità, e cioè quella delle terne (x, y, z) in cui tutti e tre i coefficienti x, y e z sono a due a due distinti, cioè $x \neq y, y \neq z, z \neq x$. In effetti, queste costituiscono un'unica classe, un rappresentante della quale è, ad esempio, la terna $(1, 2, 3)$: in altre parole, si ha

$$[(1, 2, 3)]_{\sim} = \{(i, j, k) \in E \mid i, j, k \in \{1, 2, \dots, n\}, i \neq j, j \neq k, k \neq i\} \quad (2)$$

Infatti, per definizione abbiamo

$$\begin{aligned} [(1, 2, 3)]_{\sim} &:= \{(x', y', z') \in E \mid (1, 2, 3) \sim (x', y', z')\} = \\ &= \{(x', y', z') \in E \mid \exists \sigma \in \mathcal{S}_n : \sigma(1) = x', \sigma(2) = y', \sigma(3) = z'\} ; \end{aligned}$$

e quindi chiaramente — poiché ogni $\sigma \in \mathcal{S}_n$ è *iniettiva* — si ha

$$\begin{aligned} [(1, 2, 3)]_{\sim} &= \{(\sigma(1), \sigma(2), \sigma(3)) \in E \mid \sigma \in \mathcal{S}_n\} \subseteq \\ &\subseteq \{(i, j, k) \in E \mid i, j, k \in \{1, 2, \dots, n\}, i \neq j, j \neq k, k \neq i\} . \end{aligned}$$

Viceversa, vale anche l'inclusione inversa. Infatti, per ogni scelta $i, j, k \in \{1, 2, \dots, n\}$ con $i \neq j, j \neq k, k \neq i$, abbiamo che

$$\text{esiste sempre una } \sigma_{i,j,k} \in \mathcal{S}_n \text{ tale che } \sigma_{i,j,k}(1) = i, \sigma_{i,j,k}(2) = j, \sigma_{i,j,k}(3) = k . \quad (3)$$

N.B.: Di nuovo, per il compito non era strettamente necessario spiegare perché valesse la (1); in ogni caso ora lo spieghiamo. Potremmo procedere come in precedenza per verificare la (1), ma seguiamo invece un ragionamento alternativo, che va bene anche per la (1).

Consideriamo in $\{1, 2, 3, \dots, n\}$ i sottoinsiemi $\{1, 2, 3\}$ e $\{i, j, k\}$, in cui i, j e k sono a due a due distinti. Dato che $\{1, 2, 3\}$ e $\{i, j, k\}$ sono equipotenti (in breve, hanno entrambi tre elementi!) esiste una biiezione tra loro, diciamo $\sigma' : \{1, 2, 3\} \rightarrow \{i, j, k\}$; e c'è anche una biiezione $\sigma'' : (\{1, 2, 3, \dots, n\} \setminus \{1, 2, 3\}) \rightarrow (\{1, 2, 3, \dots, n\} \setminus \{i, j, k\})$ tra i loro complementari, perché anche questi ultimi sono equipotenti l'uno con l'altro (hanno entrambi $n-3$ elementi). Allora possiamo definire in modo univoco un'applicazione $\sigma_{i,j,k} : \{1, 2, 3, \dots, n\} \rightarrow \{1, 2, 3, \dots, n\}$ stabilendo che sul sottoinsieme $\{1, 2, 3\}$ sia data da σ' , e sul complementare $\{1, 2, 3, \dots, n\} \setminus \{1, 2, 3\}$ sia data da σ'' . In formule, si scrive

$$\sigma_{i,j,k}(x) := \begin{cases} \sigma'(x) & \text{se } x \in \{1, 2, 3\} \\ \sigma''(x) & \text{se } x \in \{1, 2, 3, \dots, n\} \setminus \{1, 2, 3\} \end{cases}$$

Per concludere, è immediato osservare che una tale $\sigma_{i,j,k}$ è certamente una biiezione — perché lo sono σ' e σ'' — dunque $\sigma_{i,j,k} \in \mathcal{S}_n$.

Infine, la (3) ci garantisce proprio che vale anche l'inclusione inversa, cioè

$$\begin{aligned} [(1, 2, 3)]_{\sim} &= \{(\sigma(1), \sigma(2), \sigma(3)) \in E \mid \sigma \in \mathcal{S}_n\} \supseteq \\ &\supseteq \{(i, j, k) \in E \mid i, j, k \in \{1, 2, \dots, n\}, i \neq j, j \neq k, k \neq i\} . \end{aligned}$$

e quindi vale l'uguaglianza, cioè la (2).

Sintesi finale (della parte (c)): Dalle definizioni abbiamo che una qualsiasi classe di equivalenza $[(a, b, c)]_{\sim}$ è data da

$$\begin{aligned} [(a, b, c)]_{\sim} &:= \{ (x, y, z) \in E \mid (a, b, c) \sim (x, y, z) \} = \\ &= \{ (x, y, z) \in E \mid \exists \sigma \in \mathcal{S}_n : \sigma(a) = x, \sigma(b) = y, \sigma(c) = z \} ; \end{aligned}$$

e quindi $[(a, b, c)]_{\sim} = \{ (\sigma(a), \sigma(b), \sigma(c)) \in E \mid \sigma \in \mathcal{S}_n \}$. Poiché ogni permutazione in particolare è iniettiva, eventuali uguaglianze tra coefficienti della terna di partenza (a, b, c) implicano analoghe uguaglianze nelle terne “trasformate” $(\sigma(a), \sigma(b), \sigma(c))$, precisamente

$$a = b \implies \sigma(a) = \sigma(b) , \quad b = c \implies \sigma(b) = \sigma(c) , \quad c = a \implies \sigma(c) = \sigma(a) ; \quad (4)$$

viceversa, siccome ogni permutazione in particolare è suriettiva, eventuali disuguaglianze tra coefficienti della terna di partenza (a, b, c) implicano analoghe disuguaglianze nelle terne $(\sigma(a), \sigma(b), \sigma(c))$, precisamente

$$a \neq b \implies \sigma(a) \neq \sigma(b) , \quad b \neq c \implies \sigma(b) \neq \sigma(c) , \quad c \neq a \implies \sigma(c) \neq \sigma(a) . \quad (4)$$

La (4) e la (5) insieme ci danno

$$\begin{aligned} (\forall a) \quad & [(a, a, a)]_{\sim} := \{ (\sigma(a), \sigma(a), \sigma(a)) \in E \mid \sigma \in \mathcal{S}_n \} \subseteq \\ & \subseteq \{ (x, y, z) \in E \mid x = y, y = z, z = x \} \\ (\forall a \neq c) \quad & [(a, a, c)]_{\sim} := \{ (\sigma(a), \sigma(a), \sigma(c)) \in E \mid \sigma \in \mathcal{S}_n \} \subseteq \\ & \subseteq \{ (x, y, z) \in E \mid x = y, y \neq z, z \neq x \} \\ (\forall a \neq b) \quad & [(a, b, a)]_{\sim} := \{ (\sigma(a), \sigma(b), \sigma(a)) \in E \mid \sigma \in \mathcal{S}_n \} \subseteq \\ & \subseteq \{ (x, y, z) \in E \mid x \neq y, y \neq x, z = x \} \\ (\forall b \neq a) \quad & [(a, b, b)]_{\sim} := \{ (\sigma(a), \sigma(b), \sigma(b)) \in E \mid \sigma \in \mathcal{S}_n \} \subseteq \\ & \subseteq \{ (x, y, z) \in E \mid x \neq y, y = z, z \neq x \} \\ (\forall a \neq b \neq c \neq a) \quad & [(a, b, c)]_{\sim} := \{ (\sigma(a), \sigma(b), \sigma(c)) \in E \mid \sigma \in \mathcal{S}_n \} \subseteq \\ & \subseteq \{ (x, y, z) \in E \mid x \neq y, y \neq z, z \neq x \} \end{aligned}$$

Osserviamo anche che l'ultimo tipo di classe esiste se e soltanto se $n \geq 3$, per $n = 2$ esistono i primi quattro casi, per $n = 1$ è possibile soltanto il primo.

Con un'altra osservazione, ci rendiamo conto che le inclusioni insiemistiche qui sopra sono in effetti delle *uguaglianze*. Inoltre, la classe di una qualsiasi terna coincide necessariamente con una delle precedenti, determinata a seconda di quali coincidenze ci siano (eventualmente nessuna) tra i coefficienti della terna stessa. Infine, osserviamo che possiamo scegliere come rappresentanti, per tali classi, rispettivamente le terne $(1, 1, 1)$, $(1, 1, 2)$, $(1, 2, 1)$, $(2, 1, 1)$ e $(1, 2, 3)$.

In tutto questo, l'idea chiave è data dalle proprietà (4) e (5). In base a queste, le classi di equivalenza di terne le abbiamo individuate e catalogate secondo questo principio. Una terna è fatta di tre elementi, scelti nell'insieme $\{1, \dots, n\}$, e disposti in tre possibili

posizioni: quel che siamo andati a guardare era dunque *in quali posizioni, eventualmente, tali elementi fossero coincidenti*. In altre parole, ad ogni terna $(x_1, x_2, x_3) \in E$ abbiamo associato una *partizione* $\Pi(x, y, z)$ di $\{1, \dots, n\}$, definita così: ogni singola parte di $\Pi(x, y, z)$ raccoglie tutte e sole le posizioni della terna in cui si trova uno stesso elemento di $\{1, \dots, n\}$, quindi (scartando le “parti vuote” che così verrebbero definite)

$$\begin{aligned}\Pi(x, y, z) &:= \{ \Pi(x, y, z)_j \mid \Pi(x, y, z)_j \neq \emptyset \} \\ \Pi(x, y, z)_j &:= \{ i \in \{1, 2, 3\} \mid x_i = j \} \quad , \quad \forall j \in \{1, \dots, n\}\end{aligned}$$

In questo modo abbiamo definito un’applicazione

$$\Pi : E := \{1, \dots, n\}^{\times 3} \longrightarrow \mathcal{P}tz_n(\{1, 2, 3\}) \quad , \quad (x, y, z) \mapsto \Pi(x, y, z)$$

dall’insieme di terne $E := \{1, \dots, n\}^{\times 3}$ all’insieme $\mathcal{P}tz_n(\{1, 2, 3\})$ di tutte le partizioni dell’insieme $\{1, 2, 3\}$ in al più n parti. Ebbene, *la relazione $\sim$ in E considerata in questo esercizio non è altro che la relazione associata a tale applicazione!* E come tale, sappiamo dalla teoria generale che essa è *una relazione di equivalenza...*

Se questo è chiaro, non sarà difficile generalizzare quanto abbiamo fatto al caso dell’insieme $E := \{1, \dots, n\}^{\times k}$ delle k -uple ($:=$ stringhe di lunghezza k) di elementi in $\{1, \dots, n\}$, invece delle semplici terne. Ma questo è un altro esercizio...

..... *

[2] — Risolvere il sistema di congruenze lineari in $\mathbb{Z}$

$$\begin{cases} 2x \equiv -11 & (\text{mod } 5) \\ -x \equiv 13 & (\text{mod } 8) \\ 12x \equiv 30 & (\text{mod } 21) \end{cases}$$

Soluzione: Procediamo per passi successivi.

(1): Per prima cosa, possiamo semplificare il sistema sostituendo i vari numeri che compaiono nelle singole congruenze con altri numeri ad essi congruenti (modulo l’intero opportuno). Nel caso in esame, è sufficiente operare soltanto sui termini noti delle congruenze, per i quali abbiamo

$$-11 \equiv -1 \pmod{5} \quad , \quad 13 \equiv 5 \pmod{8} \quad , \quad 30 \equiv 9 \pmod{21}$$

quindi il sistema di partenza è equivalente al sistema

$$\begin{cases} 2x \equiv -1 & (\text{mod } 5) \\ -x \equiv 5 & (\text{mod } 8) \\ 12x \equiv 9 & (\text{mod } 21) \end{cases} \quad (5)$$

(2): Adesso studiamo la risolubilità — separatamente — delle varie congruenze che compaiono nel sistema. In ciascun caso, sappiamo che condizione necessaria e sufficiente per la risolubilità è che il *M.C.D.* tra il coefficiente dell'incognita e il modulo della congruenza divida il termine noto. Nel caso in esame abbiamo

$$\begin{aligned} M.C.D.(2, 5) = 1 \mid -1 &\implies \text{la prima congruenza è risolubile} \\ M.C.D.(-1, 8) = 1 \mid 5 &\implies \text{la seconda congruenza è risolubile} \\ M.C.D.(12, 21) = 3 \mid 9 &\implies \text{la terza congruenza è risolubile} \end{aligned}$$

dunque le tre congruenze, separatamente, sono tutte risolubili. Calcoliamo ora una soluzione — separatamente — di ciascuna delle tre congruenze del nostro sistema.

(2-I): La prima congruenza

$$2x_1 \equiv -1 \pmod{5}$$

ha chiaramente soluzione $x_1 \equiv 2 \pmod{5}$, cioè $x_1 = 2 + 5z_1$ ($\forall z_1 \in \mathbb{Z}$), o in altri termini $x_1 \in \{2 + 5z_1 \mid z_1 \in \mathbb{Z}\}$. Infatti la soluzione generica si trova sommando ad una soluzione particolare — nel nostro caso, 2 — un qualunque multiplo intero del modulo diviso per il *M.C.D.* tra il coefficiente dell'incognita e il modulo: in questo caso quindi un multiplo di 5. Il fatto che 2 sia una soluzione (particolare) si può ricavare osservando che

$$2x_1 \equiv -1 \pmod{5} \iff [2]_5 [x_1]_5 = [-1]_5 \pmod{5} \iff [x_1]_5 = [2]_5^{-1} [-1]_5 \pmod{5}$$

da cui, calcolando che l'inverso di $[2]_5$ in $\mathbb{Z}_5$ è $[2]_5^{-1} = [3]_5$, si ottiene appunto

$$[x_1]_5 = [2]_5^{-1} [-1]_5 = [3]_5 [-1]_5 = [-3]_5 = [2]_5$$

(2-II): La seconda congruenza

$$-x_2 \equiv 5 \pmod{8}$$

è chiaramente equivalente alla congruenza $x_2 \equiv -5 \pmod{8}$ — basta moltiplicare per -1 i due membri della congruenza — a sua volta equivalente a $x_2 \equiv 3 \pmod{8}$ — tanto per far sparire i segni meno... — le cui soluzioni sono $x_2 = 3 + 8z_2$ ($\forall z_2 \in \mathbb{Z}$), vale a dire $x_2 \in \{3 + 8z_2 \mid z_2 \in \mathbb{Z}\}$.

(2-III): Infine, la terza congruenza

$$12x_3 \equiv 9 \pmod{21}$$

la risolviamo procedendo ad applicare l'algoritmo standard con tutti i dettagli. In particolare, dobbiamo risolvere l'equazione diofantea $12 \cdot x_3 + 21 \cdot y_3 = 9$, perché la componente x_3 di una sua qualsiasi soluzione sarà una soluzione della congruenza che ci interessa.

Per prima cosa, dobbiamo calcolare il $M.C.D.$ tra il coefficiente della incognita x_3 e quello della y_3 (in origine, il modulo della congruenza), cioè $M.C.D.(12, 21)$, tramite l'algoritmo euclideo delle divisioni successive. Il calcolo esplicito ci dà

$$\begin{aligned} 12 &= 21 \cdot 0 + 12 \\ 21 &= 12 \cdot 1 + 9 \\ 12 &= 9 \cdot 1 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned} \tag{6}$$

dove l'ultimo resto non nullo è il $M.C.D.$ cercato, dunque $M.C.D.(12, 21) = 3$.

In seconda battuta, verifichiamo se il suddetto $M.C.D.$ tra il coefficiente della incognita x_3 e quello della y_3 (cioè il modulo) divide il termine noto — cosa che prima abbiamo affermato al volo... In effetti abbiamo

$$M.C.D.(12, 21) = 3 \mid 9, \quad \text{con} \quad 3 \cdot 3 = 9 \tag{7}$$

per cui la congruenza in esame è effettivamente risolubile.

In terzo luogo, per calcolare una soluzione particolare della nostra congruenza ci calcoliamo una identità di Bézout per $M.C.D.(12, 21)$, utilizzando — a ritroso — le identità ottenute in (6) tramite l'algoritmo euclideo delle divisioni successive. Tramite tali identità, riscrivo ogni resto come combinazione lineare del dividendo e del divisore, ottenendo

$$\begin{aligned} 12 &= 12 + 21 \cdot (-0) \\ 9 &= 21 + 12 \cdot (-1) \\ M.C.D.(12, 21) &= 3 = 12 + 9 \cdot (-1) \end{aligned}$$

Da qui, sostituendo nella seconda identità l'espressione per 12 nella prima, e poi l'espressione così ottenuta nella terza (al posto di 9), si ha $M.C.D.(12, 21) = 3 = 12 \cdot 2 + 21 \cdot (-1)$, che riscriviamo nella forma

$$12 \cdot 2 + 21 \cdot (-1) = 3$$

Da quest'ultima identità e dalla (7) otteniamo

$$12 \cdot 6 + 21 \cdot (-3) = (12 \cdot 2 + 21 \cdot (-1)) \cdot 3 = 3 \cdot 3 = 9$$

in altre parole, troviamo che la coppia $(x_3, y_3) := (6, -3)$ è soluzione dell'equazione diofantea $12 \cdot x_3 + 21 \cdot y_3 = 9$. Da questo segue, infine, che $x_3 = 6$ è una soluzione (particolare) della congruenza $12x_3 \equiv 9 \pmod{21}$ a cui siamo interessati. Infine, l'insieme di tutte le soluzioni si ottiene, in generale, sommando ad una soluzione particolare un qualunque multiplo intero dell'intero d ottenuto dividendo il modulo (della congruenza) per il $M.C.D.$ tra il coefficiente (della congruenza) e il modulo stesso: nel nostro caso, è

$$d := \frac{21}{M.C.D.(12, 21)} = \frac{21}{3} = 7$$

e quindi la *soluzione generale* cercata è $x_3 \equiv 6 \pmod{7}$, cioè $x_3 = 6 + 7z_3$ ($\forall z_3 \in \mathbb{Z}$), o in altri termini $x_3 \in \{6 + 7z_3 \mid z_3 \in \mathbb{Z}\}$.

In alternativa, osserviamo che si può procedere anche al modo seguente. La terza congruenza si può *ridurre*, dividendo il suo coefficiente, termine noto e modulo per il *M.C.D.*(12, 21), che è 3: così facendo si ottiene la congruenza equivalente

$$4x_3 \equiv 3 \pmod{7}$$

Osservando che $4 \equiv -3 \pmod{7}$, troviamo subito la soluzione particolare $x_3 = -1$, dalla quale otteniamo la soluzione generica sommando un qualunque multiplo intero del modulo 7 (che adesso è coprimo col coefficiente dell'incognita!): in breve, la soluzione generica è $x_3 = -1 + 7\zeta$ ($\forall \zeta \in \mathbb{Z}$), o in altre parole $x_3 \in \{-1 + 7\zeta \mid \zeta \in \mathbb{Z}\}$. Dato che $-1 \equiv 6 \pmod{7}$, è chiaro che i due insiemi di soluzioni — trovati con i due procedimenti seguiti — coincidono, anche se le due soluzioni particolari considerate (6 nel primo caso, -1 nel secondo) sono diverse.

(3): Adesso dobbiamo preoccuparci della compatibilità del sistema, cioè della possibilità di risolvere le tre congruenze *simultaneamente*. Siccome i tre moduli — 5, 8 e 21 — sono a due a due coprimi, dal Teorema Cinese del Resto sappiamo che il sistema è compatibile, e conosciamo anche un algoritmo esplicito per risolverlo. Seguiamo due metodi:

Primo metodo: Consideriamo il nostro sistema di congruenze riscritto nella forma in cui ogni congruenza appaia risolta, cioè (viste le soluzioni particolari che abbiamo calcolato in precedenza!)

$$\begin{cases} x \equiv 2 & \pmod{5} \\ x \equiv 3 & \pmod{8} \\ x \equiv 6 & \pmod{7} \end{cases} \quad (8)$$

(la cosiddetta “forma cinese”). Consideriamo poi i numeri

$$R_1 := 8 \cdot 7 = 56, \quad R_2 := 5 \cdot 7 = 35, \quad R_3 := 5 \cdot 8 = 40, \quad R := 5 \cdot 8 \cdot 7 = 280 \quad (9)$$

e le tre congruenze

$$56x_1 \equiv 2 \pmod{5}, \quad 35x_2 \equiv 3 \pmod{8}, \quad 40x_3 \equiv 6 \pmod{7}$$

ottenute da quelle in (8) moltiplicando il coefficiente dell'incognita nella prima, seconda e terza congruenza rispettivamente per R_1 , per R_2 e per R_3 . Esse sono equivalenti a

$$1x_1 \equiv 2 \pmod{5}, \quad 3x_2 \equiv 3 \pmod{8}, \quad 5x_3 \equiv 6 \pmod{7}$$

le quali hanno soluzioni

$$x'_1 \equiv 2 \pmod{5}, \quad x'_2 \equiv 1 \pmod{8}, \quad x'_3 \equiv 4 \pmod{7} \quad (10)$$

Infine, una *soluzione particolare* del sistema è data dalla formula

$$x' = R_1 \cdot x'_1 + R_2 \cdot x'_2 + R_3 \cdot x'_3 = 307$$

— ottenuta sostituendo i valori di x'_1 , x'_2 e x'_3 dati in (10) — mentre la *soluzione generica* è data da

$$x = x' + R \cdot z = 307 + 280 \cdot z, \quad \forall z \in \mathbb{Z}$$

che possiamo riscrivere anche dicendo che l'insieme di tutte le soluzioni del sistema è dato da

$$\{x' + R \cdot z \mid z \in \mathbb{Z}\} = \{307 + 280 \cdot z \mid z \in \mathbb{Z}\} = \{27 + 280 \cdot \zeta \mid \zeta \in \mathbb{Z}\} \quad (11)$$

Secondo metodo: Consideriamo il nostro sistema di congruenze nella forma (5), i numeri R_1 , R_2 , R_3 e R definiti in (9), e le tre congruenze

$$168 \cdot 2x_1 \equiv -1 \pmod{5}, \quad 105 \cdot (-1)x_2 \equiv 5 \pmod{8}, \quad 40 \cdot 12x_3 \equiv 9 \pmod{21}$$

ottenute da quelle in (5) moltiplicando il coefficiente dell'incognita nella prima, seconda e terza congruenza rispettivamente per R_1 , per R_2 e per R_3 . Esse sono equivalenti a

$$1x_1 \equiv -1 \pmod{5}, \quad (-1)x_2 \equiv 5 \pmod{8}, \quad (-3)x_3 \equiv 9 \pmod{21}$$

le quali hanno soluzioni

$$x'_1 \equiv -1 \pmod{5}, \quad x'_2 \equiv -5 \pmod{8}, \quad x'_3 \equiv -3 \pmod{7} \quad (12)$$

Infine, una *soluzione particolare* del sistema è data dalla formula

$$x' = R_1 \cdot x'_1 + R_2 \cdot x'_2 + R_3 \cdot x'_3 = -813$$

— ottenuta sostituendo i valori di x'_1 , x'_2 e x'_3 dati in (12) — mentre la *soluzione generica* è data da

$$x = x' + R \cdot z = -813 + 280 \cdot z, \quad \forall z \in \mathbb{Z}$$

in quanto, grazie all'analisi fatta in precedenza (per il sistema in forma cinese), sappiamo che le soluzioni si ripetono modulo 280. Il risultato ottenuto lo possiamo riscrivere anche dicendo che l'insieme di tutte le soluzioni del sistema è dato da

$$\{x' + R \cdot z \mid z \in \mathbb{Z}\} = \{-813 + 280 \cdot z \mid z \in \mathbb{Z}\} = \{27 + 280 \cdot \zeta \mid \zeta \in \mathbb{Z}\} \quad (13)$$

dal che si vede che l'insieme delle soluzioni espresso in (13) è lo stesso descritto in (11). $\square$

..... *

(continua ...)

[3] — Sia $n \in \mathbb{N}$, $n > 2$, siano $\sigma, \rho \in \mathcal{S}_n$ gli elementi definiti nel modo seguente

$$\begin{aligned}\sigma(i) &:= n + 1 - i, & \forall i = 1, 2, \dots, n, \\ \rho(i) &:= i + 1, & \forall i = 1, 2, \dots, n-1, & \rho(n) := 1,\end{aligned}$$

e sia $D_n := \langle \sigma, \rho \rangle$ il sottogruppo di $\mathcal{S}_n$ generato da σ e ρ .

- (a) Dimostrare che $\sigma^2 = id$, $\rho^n = id$, $\sigma \rho \sigma = \rho^{-1}$;
- (b) dimostrare che $|D_n| = 2n$;
- (c) descrivere esplicitamente D_n , come sottogruppo di $\mathcal{S}_n$, nei casi di $n = 3, 4$.

Soluzione: (a) Per verificare che $\sigma^2 = id$ operiamo un calcolo diretto, che ci dà

$$\sigma^2(i) = \sigma(\sigma(i)) = \sigma(n + 1 - i) = n + 1 - (n + 1 - i) = i = id(i) \quad \forall i = 1, 2, \dots, n$$

che significa appunto che $\sigma^2 = id$. Per verificare che $\rho^n = id$ invece, osserviamo che l'applicazione ρ manda ogni numero da 1 a $n-1$ nel suo successivo: se intendiamo con “successivo di n ” il numero 1, possiamo dire che questo vale anche per n stesso. Da questo è chiaro che ρ^n è proprio l'applicazione identità, perché dopo n applicazioni di ρ ogni elemento i ritorna nella posizione iniziale.

Esplicitamente possiamo verificarlo così. Dimostriamo, per induzione su k , che

$$\rho^k(1) := k + 1, \quad \forall k = 1, \dots, n-1 \quad (14)$$

La base dell'induzione è l'enunciato per $k = 1$, che si verifica direttamente: $\rho(1) := 1 + 1$. Il passo induttivo poi lo dimostriamo in questo modo: preso un $k > 1$ (e $k \leq n-1$), facciamo l'*ipotesi induttiva* che sia valido l'enunciato per $k-1$, cioè $\rho^{k-1}(1) := (k-1) + 1 (= k)$, e dimostriamo l'enunciato per k così:

$$\rho^k(1) = \rho^{1+(k-1)}(1) = (\rho \circ \rho^{(k-1)})(1) = \rho(\rho^{k-1}(1)) = \rho(k) := k + 1$$

La conclusione è che per $k = n-1$ la (14) ci dà $\rho^{n-1}(1) = (n-1) + 1 = n$. Ma allora abbiamo anche $\rho^n(1) = \rho(\rho^{n-1}(1)) = \rho(n) := 1$, e più in generale

$$\begin{aligned}\rho^n(h) &= \rho^n((h-1) + 1) = \rho^n(\rho^{h-1}(1)) = (\rho^n \circ \rho^{(h-1)})(1) = \rho^{n+h-1}(1) = \\ &= (\rho^{(h-1)} \circ \rho^n)(1) = \rho^{h-1}(\rho^n(1)) = \rho^{h-1}(1) = (h-1) + 1 = h\end{aligned}$$

per ogni $h = 1, \dots, n$; quindi abbiamo $\rho^n = id$, q.e.d.

Infine, dimostriamo che $\sigma \rho \sigma = \rho^{-1}$. Per cominciare, osserviamo che dalle definizioni si ricava subito

$$\rho^{-1}(1) = n, \quad \rho^{-1}(h) = h - 1, \quad \forall h = 2, \dots, n.$$

Da questo, e dai risultati precedenti, otteniamo

$$(\sigma \rho \sigma)(h) = \sigma(\rho(\sigma(h))) = \sigma(\rho(n + 1 - h)) = \sigma(n + 2 - h) = h - 1 = \rho^{-1}(h)$$

per $h = 2, \dots, n$, mentre per $h = 1$ abbiamo

$$(\sigma \rho \sigma)(1) = \sigma(\rho(\sigma(1))) = \sigma(\rho(n)) = \sigma(1) = n = \rho^{-1}(1)$$

Complessivamente, questo ci dice che $(\sigma \rho \sigma)(k) = \rho^{-1}(k)$ per ogni $k = 1, \dots, n$, e quindi in conclusione $\sigma \rho \sigma = \rho^{-1}$, q.e.d.

(b) Per definizione $D_n := \langle \sigma, \rho \rangle$ il sottogruppo di $\mathcal{S}_n$ generato da σ e ρ ; pertanto, dalla teoria generale sappiamo che esso è il sottoinsieme di $\mathcal{S}_n$ costituito da tutte le permutazioni della forma

$$\tau_1 \tau_2 \cdots \tau_{k-1} \tau_k, \quad k \in \mathbb{N}, \quad \tau_1, \dots, \tau_k \in \{ \rho, \rho^{-1}, \sigma, \sigma^{-1} (= \sigma) \} \quad (15)$$

cioè da prodotti arbitrari di fattori — in numero arbitrario — che possono essere del tipo ρ , ρ^{-1} , σ oppure σ^{-1} (che però è uguale a σ). Ad esempio, un tipico elemento di D_n è la permutazione $\rho \rho \sigma \rho^{-1} \sigma \sigma^{-1} \sigma^{-1} \rho \rho \rho^{-1} \sigma \rho^{-1} \sigma^{-1} \sigma^{-1}$; lo si può anche riscrivere come $\rho^2 \sigma^1 \rho^{-1} \sigma^{-1} \rho^1 \sigma^1 \rho^{-1} \sigma^{-2}$, accorpare fattori vicini uguali o inversi in potenze con esponente intero), e anche come $\rho^2 \sigma^1 \rho^{-1} \sigma^1 \rho^1 \sigma^1 \rho^{-1} \sigma^2$ visto che $\sigma^{-1} = \sigma$. In generale, questo si può fare per ogni elemento del tipo in (15), per cui in definitiva gli elementi di D_n sono tutti e soli della forma

$$\rho^{e_1} \sigma^{f_1} \rho^{e_2} \sigma^{f_2} \dots \rho^{e_{s-1}} \sigma^{f_{s-1}} \rho^{e_s} \sigma^{f_s} \quad (16)$$

con $s \in \mathbb{N}$ (intendendo che per $s = 0$ si tratta di un “prodotto vuoto”, dunque uguale per convenzione a id) e $e_1 \in \mathbb{Z}$, $f_1, e_2, f_2, \dots, e_{s-1}, f_{s-1}, e_s \in \mathbb{Z} \setminus \{0\}$, $f_s \in \mathbb{Z}$.

Analizziamo ora le singole potenze ρ^e e σ^f che figurano in (16). Chiaramente $\rho^e \in \langle \rho \rangle$ e $\sigma^f \in \langle \sigma \rangle$, dove $\langle \rho \rangle$ e $\langle \sigma \rangle$ sono *gruppi ciclici* di ordine rispettivamente $|\langle \rho \rangle| = o(\rho)$ e $|\langle \sigma \rangle| = o(\sigma)$, dove indichiamo con $o(\tau)$ l'ordine di una permutazione τ . Osserviamo che dalle relazioni $\sigma^2 = id$ e $\rho^n = id$ segue subito che $o(\sigma) \mid 2$, $o(\rho) \mid n$. Poiché chiaramente $\sigma \neq id$, abbiamo certamente $o(\sigma) = 2$. D'altra parte, la (14) per $k = 1, 2, \dots, n-1$ ci dà $\rho^k(1) = k+1 \neq 1 = id(1)$, dunque $\rho^k \neq id$; pertanto è necessariamente $o(\rho) = n$. La conclusione è che i due gruppi ciclici in esame sono

$$\langle \sigma \rangle = \{ \sigma^f \mid f \in \mathbb{Z} \} = \{ id, \sigma \}, \quad \langle \rho \rangle = \{ \rho^e \mid e \in \mathbb{Z} \} = \{ id, \rho, \rho^2, \dots, \rho^{n-1} \} \quad (17)$$

il primo con esattamente due elementi (distinti), il secondo con n ; perciò, i prodotti in (16) possono essere riscritti con esponenti — magari diversi — scelti in $\mathbb{N}$ invece che in $\mathbb{Z}$.

Ora, la formula $\sigma \rho \sigma = \rho^{-1}$ dimostrata in (a) è equivalente alla formula $\sigma \rho = \rho^{-1} \sigma^{-1}$ (basta moltiplicare entrambi i membri a destra per σ^{-1}). Inoltre, osservando che $\sigma^{-1} = \sigma$ tale formula si può riscrivere come $\sigma \rho = \rho^{-1} \sigma$, o anche come $\sigma \rho = \rho^{n-1} \sigma$ dato che $\rho^{-1} = \rho^{n-1}$ perché $o(\rho) = n$. Ma allora, quando si considera un prodotto $\rho^{e_1} \sigma^{f_1} \rho^{e_2} \sigma^{f_2} \dots \rho^{e_{s-1}} \sigma^{f_{s-1}} \rho^{e_s} \sigma^{f_s}$ come in (16) — ma con esponenti scelti in $\mathbb{N}$ — ogni volta che compaiono due fattori consecutivi del tipo $\tau_i \tau_{i+1} = \sigma \rho$ possiamo sostituirli con $\rho^{-1} \sigma$, o anche con $\rho^{n-1} \sigma$. Iterando più volte — ma comunque, un numero *finito* di volte — questo tipo di operazione, otterremo alla fine una riscrittura dell'elemento di partenza

del tipo $\rho^{e_1} \sigma^{f_1} \rho^{e_2} \sigma^{f_2} \dots \rho^{e_{s-1}} \sigma^{f_{s-1}} \rho^{e_s} \sigma^{f_s} = \rho^e \sigma^f$, con $e, f \in \mathbb{Z}$, e più precisamente $e \in \{0, 1, \dots, n-1\}$, $f \in \{0, 1\}$. La conclusione è che

$$D_n := \langle \sigma, \rho \rangle = \{ \rho^e \sigma^f \mid e = 0, 1, \dots, n-1; f = 0, 1 \} = \\ = \{ id, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma \}$$

In modo del tutto analogo, si può dimostrare anche che

$$D_n := \langle \sigma, \rho \rangle = \{ \sigma^f \rho^e \mid e = 0, 1, \dots, n-1; f = 0, 1 \} = \\ = \{ id, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \dots, \sigma\rho^{n-1} \}$$

In ogni caso, abbiamo in particolare che $|D_n| \leq 2n$.

Per concludere che $|D_n| = 2n$, possiamo seguire due diverse strade:

1° *metodo*: Dalla inclusione $\langle \rho \rangle \leq \langle \sigma, \rho \rangle =: D_n$ del sottogruppo $\langle \rho \rangle$ nel gruppo D_n e dal Teorema di Lagrange segue che $|\langle \rho \rangle| \mid |D_n|$. Ricordando che $|\langle \rho \rangle| = o(\rho) = n$, ricaviamo che $|D_n|$ è un multiplo di n . D'altra parte, una verifica immediata dimostra che $\sigma \neq \rho^k$ per ogni $k = 0, 1, \dots, n-1$, quindi (in forza dell'analisi precedente) $D_n = \{ id, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma \}$ contiene almeno $n+1$ elementi distinti, precisamente $\sigma, id, \rho, \rho^2, \dots, \rho^{n-1}$. Quindi il numero $|D_n|$, essendo un multiplo di n che soddisfa le disuguaglianze $n+1 \leq |D_n| \leq 2n$, è necessariamente $|D_n| = 2n$, q.e.d.

N.B.: Quando n è dispari, si può concludere anche come segue. Analogamente a prima, dalle due inclusioni di sottogruppi $\langle \sigma \rangle \leq \langle \sigma, \rho \rangle =: D_n$ e $\langle \rho \rangle \leq \langle \sigma, \rho \rangle =: D_n$, dal Teorema di Lagrange e da $|\langle \sigma \rangle| = o(\sigma) = 2$ e $|\langle \rho \rangle| = o(\rho) = n$ segue che $|D_n|$ è un multiplo di n e un multiplo di 2; allora, se n è dispari si può concludere che $|D_n|$ è un multiplo di $2n$. Infine, da $|D_n| \leq 2n$ si può concludere che $|D_n| = 2n$.

Però per n pari questo argomento non è sufficiente...

2° *metodo*: Avendo provato che $D_n = \{ id, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma \}$, ci sarà sufficiente dimostrare che i $2n$ elementi che compaiono in questa descrizione di D_n sono tutti a due a due distinti. Supponiamo dunque di avere

$$\rho^e \sigma^f = \rho^\epsilon \sigma^\varphi, \quad (e, f), (\epsilon, \varphi) \in \{0, 1, \dots, n-1\} \times \{0, 1\}$$

e procediamo a dimostrare che allora è necessariamente $(e, f) = (\epsilon, \varphi)$. Abbiamo

$$\rho^e \sigma^f = \rho^\epsilon \sigma^\varphi \implies \rho^{-\epsilon} \rho^e = \sigma^\varphi \sigma^{-f} \implies \rho^{e-\epsilon} = \sigma^{\varphi-f} \quad (18)$$

Ora, una verifica elementare mostra che $\rho^r = \sigma^s \iff \rho^r = id = \sigma^s$, quindi dall'ultima uguaglianza a destra nella (18) otteniamo, in pochi passaggi, quanto richiesto:

$$\rho^{e-\epsilon} = \sigma^{\varphi-f} \implies \rho^{e-\epsilon} = id = \sigma^{\varphi-f} \implies \\ \implies e - \epsilon \equiv 0 \pmod{n}, \quad \varphi - f \equiv 0 \pmod{2} \implies e = \epsilon, \quad \varphi = f \implies (e, f) = (\epsilon, \varphi)$$

(c) Per $n = 3$ abbiamo $|D_3| = 2 \cdot 3 = 6$, dunque $D_3 \leq \mathcal{S}_3$ con $|D_3| = 6 = 3! = |\mathcal{S}_3|$. Pertanto $D_3 = \mathcal{S}_3$, e volendo essere espliciti scriviamo

$$D_3 = \mathcal{S}_3 = \{id, (12), (23), (31), (123), (321)\}$$

Per $n = 4$ abbiamo $|D_n| = 2n = 2 \cdot 4 = 8$, e $8 \not\leq 24 = 4! = |\mathcal{S}_4|$. Pertanto D_4 è un sottogruppo *proprio* di $\mathcal{S}_4$. Per descriverlo esplicitamente, applichiamo l'uguaglianza (generale) $D_n = \{id, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma\}$ al caso attuale, che ci dà

$$D_4 = \{id, \rho, \rho^2, \rho^3, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma\}$$

Per definizione abbiamo $\sigma = (1,4)(2,3)$, $\rho = (1,2,3,4)$, e con il calcolo diretto (elementare) otteniamo

$$\begin{aligned} \rho^2 &= (1,3)(2,4), & \rho^3 &= (1,4,3,2), & \rho\sigma &= (1,2,3,4)(1,4)(2,3) = (2,4), \\ \rho^2\sigma &= (1,3)(2,4)(1,4)(2,3) = (1,2)(3,4), & \rho^3\sigma &= (1,4,3,2)(1,4)(2,3) = (1,3) \end{aligned}$$

In conclusione, abbiamo quindi

$$D_4 = \{id, (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,4)(2,3), (2,4), (1,2)(3,4), (1,3)\} \quad \square$$

..... *

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

$$(a) \quad (2-i) \cdot x + (3+i) \cdot y = 1+2i$$

$$(b) \quad (3+i) \cdot x + (2-7i) \cdot y = 5+2i$$

(c) Indicato con $I := (1-3i, 7+2i)$ l'ideale di $\mathbb{Z}[i]$ generato da $1-3i$ e da $7+2i$, determinare un elemento $t \in \mathbb{Z}[i]$ tale che $I = (t)$, cioè t sia un (unico) generatore di I . Inoltre, si determinino $\alpha, \beta \in \mathbb{Z}[i]$ tali che

$$t = (1-3i) \cdot \alpha + (7+2i) \cdot \beta$$

Soluzione: La CNES perché una data equazione diofantea in $\mathbb{Z}[i]$ sia risolubile è che il *M.C.D.* tra i suoi coefficienti divida il termine noto. Nel caso in esame, dobbiamo quindi calcolare detto *M.C.D.*, per le due equazioni date: tale calcolo può essere — e sarà — effettuato tramite l'algoritmo euclideo delle divisioni successive.

(a) Effettuiamo le divisioni euclidee successive per calcolare *M.C.D.*($2-i, 3+i$): si ha

$$2-i = (3+i) \cdot 0 + (2-i)$$

$$3+i = (2-i) \cdot (1+i) + 0$$

da cui ricaviamo che $M.C.D.(2-i, 3+i) = 2-i$. Nel calcolo, il primo passaggio è ovvio, perché $N(3+i) := 3^2 + 1^2 = 10 \not\geq 5 = 2^2 + (-1)^2 = N(2-i)$, dunque la divisione euclidea da effettuare è quella ovvia (quoziente nullo, resto uguale al dividendo). Il secondo passaggio segue dal calcolo effettuato nel campo $\mathbb{C}$ dei numeri complessi, che dà

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

Ora, ancora un calcolo diretto ci dà

$$\begin{aligned} (1+2i) \cdot (M.C.D.(2-i, 3+i))^{-1} &= (1+2i) \cdot (2-i)^{-1} = \frac{1+2i}{2-i} = \\ &= \frac{1+2i}{2-i} \cdot \frac{2+i}{2+i} = \frac{(1+2i)(2+i)}{2^2 + (-1)^2} = \frac{5i}{5} = i \end{aligned}$$

dunque il termine noto $(1+2i)$ è multiplo di (è divisibile per) il $M.C.D.(2-i, 3+i)$, con fattore di molteplicità pari a i . Pertanto l'equazione diofantea (a) è risolubile. Per trovare una soluzione, calcoliamo prima una identità di Bézout per $M.C.D.(2-i, 3+i)$ tramite le formule ricavate in precedenza per il calcolo di tale $M.C.D.$, e poi moltiplichiamo il risultato — cioè la coppia di coefficienti che avremo trovato — per il fattore di molteplicità i .

Un'identità di Bézout come richiesto è data da

$$2-i = (2-i) \cdot 1 + (3+i) \cdot 0$$

(è un caso particolarmente banale, dovuto al fatto che $2-i$ divide $3+i$), e quindi moltiplicando per i otteniamo

$$1+2i = (2-i)i = ((2-i) \cdot 1 + (3+i) \cdot 0) \cdot i = (2-i) \cdot 1 \cdot i + (3+i) \cdot 0 \cdot i = (2-i) \cdot i + (3+i) \cdot 0$$

vale a dire

$$(2-i) \cdot i + (3+i) \cdot 0 = 1+2i$$

cioè la coppia $(\bar{x}, \bar{y}) := (i, 0)$ è una soluzione (particolare) dell'equazione diofantea in (a) .

(b) Come in (a) , effettuiamo ora le divisioni euclidee per calcolare $M.C.D.(3+i, 2-7i)$:

$$3+i = (2-7i) \cdot 0 + (3+i)$$

$$2-7i = (3+i) \cdot (-2i) + (-i)$$

$$3+i = (-i) \cdot (-1+3i) + 0$$

da cui ricaviamo che $M.C.D.(3+i, 2-7i) = -i$. Nel calcolo, il primo passaggio è ovvio, perché $N(2-7i) := 2^2 + (-7)^2 = 53 \not\geq 10 = 3^2 + 1^2 = N(3+i)$, dunque la divisione euclidea da effettuare è quella ovvia (quoziente nullo, resto uguale al dividendo). Il secondo passaggio procede così: dal calcolo effettuato in $\mathbb{C}$ si ottiene

$$(2-7i) \cdot (3+i)^{-1} = \frac{2-7i}{3+i} = \frac{(2-7i)(3-i)}{3^2 + (-1)^2} = \frac{(-1) + (-23)i}{10} = \frac{-1}{10} + \frac{-23}{10}i$$

e il risultato si riscrive come

$$\frac{-1}{10} + \frac{-23}{10}i = (-2i) + \frac{-1}{10} + \frac{-3}{10}i$$

dove $(-2i) \in \mathbb{Z}[i]$ è l'intero di Gauss che meglio approssima il numero $(\frac{-1}{10} + \frac{-23}{10}i) \in \mathbb{Q}[i]$. Il terzo passaggio invece è ovvio — speriamo!... — tenuto conto che $-i$ è invertibile, con inverso $(-i)^{-1} = i$. Inoltre, sempre perché $-i$ è invertibile, ovviamente divide $(5+2i)$, che è il termine noto dell'equazione diofantea in esame, la quale quindi è risolubile. Precisamente, per uso successivo osserviamo che

$$5 + 2i = (-i)(-i)^{-1}(5 + 2i) = (-i)i(5 + 2i) = (-i)(-2 + 5i)$$

così il termine noto $(5+2i)$ è multiplo di (è divisibile per) $M.C.D.(3+i, 2-7i) = -i$, con fattore di molteplicità pari a $(-2 + 5i)$. Quindi, per trovare una soluzione dell'equazione diofantea (b), calcoliamo prima una identità di Bézout per $-i = M.C.D.(3+i, 2-7i)$, tramite le formule ricavate in precedenza, e poi moltiplichiamo il risultato — cioè la coppia di coefficienti che avremo trovato — per il fattore di molteplicità $(-2 + 5i)$.

Un'identità di Bézout come richiesto è data da

$$-i = (3+i) \cdot (2i) + (2-7i) \cdot 1 \quad (19)$$

(la si ricava facilmente dalla seconda divisione euclidea), e moltiplicando per $(-2 + 5i)$ otteniamo

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

vale a dire

$$(3+i) \cdot (-10 - 4i) + (2-7i) \cdot (-2 + 5i) = 5 + 2i$$

cioè la coppia $(\bar{x}, \bar{y}) := (-10 - 4i, 2 - 7i)$ è una soluzione (particolare) dell'equazione diofantea in (b).

(c) Dalla teoria generale sappiamo che $\mathbb{Z}[i]$ è un dominio euclideo; ne segue allora anche che esso è un dominio a ideali principali. In particolare, l'ideale $I := (1 - 3i, 7 + 2i)$ di $\mathbb{Z}[i]$ generato da $1 - 3i$ e da $7 + 2i$ è necessariamente un ideale principale, del quale dobbiamo determinare un generatore t . Sempre dalla teoria generale, dall'identità tra ideali $(1 - 3i, 7 + 2i) = (t)$ sappiamo che dev'essere $t = M.C.D.(1 - 3i, 7 + 2i)$, quindi ci basta calcolare tale $M.C.D.$, cosa che possiamo fare — ancora una volta — tramite l'algoritmo euclideo delle divisioni successive. Ma invece di (ri)fare dei calcoli come prima, osserviamo che

$$1 - 3i = (3+i) \cdot (-i) \quad , \quad 7 + 2i = (2-7i) \cdot i \quad (20)$$

e siccome $(-i)$ e i sono invertibili in $\mathbb{Z}[i]$, abbiamo che

$$t = M.C.D.(1 - 3i, 7 + 2i) = M.C.D.(3+i, 2-7i) = -i$$

cioè $t = -i$ è (un) generatore di I come richiesto.

Infine, per determinare $\alpha, \beta \in \mathbb{Z}[i]$ tali che $t = (1 - 3i) \cdot \alpha + (7 + 2i) \cdot \beta$, possiamo rifarci alla identità (19). Infatti, invertendo le identità in (29) otteniamo

$$3 + i = (1 - 3i) \cdot (-i)^{-1} = (1 - 3i) \cdot i, \quad 2 - 7i = (7 + 2i) \cdot i^{-1} = (7 + 2i) \cdot (-i)$$

e da queste congiuntamente alla (19) ricaviamo

$$t := -i = (1 - 3i) \cdot i \cdot (2i) + (7 + 2i) \cdot (-i) \cdot 1 = (1 - 3i) \cdot (-2) + (7 + 2i) \cdot (-i)$$

cioè $t = (1 - 3i) \cdot (-2) + (7 + 2i) \cdot (-i)$, dunque $(\alpha, \beta) = (-2, -i)$ è una coppia del tipo richiesto. $\square$

