ALGEBRA e LOGICA

CdL in Ingegneria Informatica

prof. Fabio GAVARINI

a.a. 2016–2017 — Sessione Estiva, I appello

Esame scritto del 5 Luglio 2017

. . . . . .

Testo & 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] *(a)* Si consideri il seguente polinomio booleano

$$P(x,y,z,w) \;:=\; \Big(\big(w \wedge y' \big) \vee \big(z' \wedge w'' \wedge x \wedge y' \big) \Big)' \vee \Big(y' \wedge \big(w' \vee \big(z' \wedge 1'' \wedge x \big) \big) \Big)'$$

nelle quattro variabili booleane x, y, z, w.

(a) Calcolare la *Forma Normale Disgiuntiva* del polinomio $P(x,y,z,w)$.

(b) Calcolare la *somma di tutti gli implicanti primi* del polinomio $P(x,y,z,w)$.

(c) Calcolare una *forma minimale* del polinomio $P(x,y,z,w)$.

[2] Dimostrare per induzione che per ogni $n \in \mathbb{N}$, $n \geq 4$, vale la disuguaglianza

$$3^n - 5\,n \;>\; 2^n + 4\,n$$

[3] Si consideri in $\mathbb{Z}$ la relazione "$\sim$" definita da

$$u \sim v \quad \Longleftrightarrow \quad 3\,u^2 + 7\,v^2 - 12 \;\equiv\; 8\,u + 2\,v + 28 \pmod 5 \qquad \forall\; u, v \in \mathbb{Z}$$

(a) Dimostrare che $\sim$ è una relazione di equivalenza.

(b) Data la funzione $f : \mathbb{Z} \longrightarrow \mathbb{Z}_5$, $x \mapsto f(x) := \overline{x}\,\big(\overline{x} - \overline{1}\big)$, dimostrare che

$$u \sim v \iff f(u) = f(v) \qquad \forall\; u, v \in \mathbb{Z}$$

(c) Descrivere esplicitamente la classe di $\sim$–equivalenza di 1.

(d) Descrivere esplicitamente la classe di $\sim$–equivalenza di 3.

(e) Descrivere esplicitamente tutte le classi di $\sim$–equivalenza in $\mathbb{Z}$.

[4] Sia $\mathcal{P}\big(\{S,P,Q,R\}\big)$ l'insieme delle parti dell'insieme $\{S,P,Q,R\}$ e "$\supseteq$" la consueta relazione di "inclusione inversa" in $\mathcal{P}\big(\{S,P,Q,R\}\big)$, definita da $\mathcal{A}\supseteq\mathcal{B}$ se e soltanto se $\mathcal{A}$ contiene $\mathcal{B}$ — per ogni $\mathcal{A},\mathcal{B}\in\mathcal{P}\big(\{S,P,Q,R\}\big)$.

Sia poi $D_{60}:=\big\{\,d\in\mathbb{N}\,\big|\,d \text{ è divisore di } 60\,\big\}$ l'insieme dei divisori di 60, e sia "$\big|$" la consueta relazione di divisibilità in D_{60}.

Nell'insieme $E:=\mathcal{P}\big(\{S,P,Q,R\}\big)\times D_{60}$ prodotto cartesiano di $\mathcal{P}\big(\{S,P,Q,R\}\big)$ con D_{60} consideriamo la relazione $\preceq$ definita da

$$\big(\mathcal{A},d\big)\preceq\big(\mathcal{B},q\big)\quad\Longleftrightarrow\quad\mathcal{A}\supseteq\mathcal{B}\ ,\ \ d\,\big|\,q$$

per ogni $\big(\mathcal{A},d\big),\big(\mathcal{B},q\big)\in\mathcal{P}\big(\{S,P,Q,R\}\big)\times D_{60}=:E$.

(a) Dimostrare che $\preceq$ è una relazione d'ordine in E.

(b) Esiste un *minimo* nell'insieme ordinato $\big(E\,;\preceq\big)$? In caso negativo, spiegare perché; in caso affermativo, precisare quale sia tale minimo.

(c) Esiste un *massimo* nell'insieme ordinato $\big(E\,;\preceq\big)$? In caso negativo, spiegare perché; in caso affermativo, precisare quale sia tale massimo.

(d) Dimostrare che l'insieme ordinato $\big(E\,;\preceq\big)$ è un reticolo, *precisando come siano fatte le operazioni* "$\vee:=$ *sup*" e "$\wedge:=$ *inf*" in tale reticolo.

(e) Determinare se esista una $\vee$–fattorizzazione in $\vee$–irriducibili per l'elemento $\big(\{S,Q\}\,,30\big)$ nel reticolo $\big(E\,;\preceq\big)$. In caso negativo, si spieghi perché una tale $\vee$–fattorizzazione non esista; in caso affermativo, si determini esplicitamente una tale $\vee$–fattorizzazione.

[5] Siano $\mathbb{Z}_{11}$ e $\mathbb{Z}_{12}$ i consueti anelli di classi di congruenza modulo 11 e modulo 12 rispettivamente, con le consuete operazioni di somma e prodotto.

(a) Calcolare esplicitamente gli insiemi di elementi invertibili $U\big(\mathbb{Z}_{11}\big)$ e $U\big(\mathbb{Z}_{12}\big)$ in $\mathbb{Z}_{11}$ e in $\mathbb{Z}_{12}$ rispettivamente.

(b) Calcolare esplicitamente l'insieme di tutte le soluzioni in $\mathbb{Z}$ dell'equazione congruenziale $45\,x\equiv-135\ \big(\mathrm{mod}\ 12\big)$.

(c) Per *entrambi* i valori $q=11$ e $q=12$, determinare se esista un elemento $\overline{z}\in\mathbb{Z}_q\setminus\big\{\,\overline{0}\,\big\}$ tale che $\overline{z}^{\,n}=\overline{0}$ per qualche esponente $n\in\mathbb{N}$. In caso negativo, si spieghi il perché; in caso affermativo, si determinino esplicitamente un tale elemento $\overline{z}$ e un esponente n tali che $\overline{z}^{\,n}=\overline{0}$.

— ⋆ —

(...continua)

SOLUZIONI

[1] — Questo che segue è un possibile modo di svolgere il problema; natralmente sono possibili diverse varianti e anche metodi alternativi.

Partendo dal polinomio booleano assegnato lo riscriviamo in forme (diverse ma) equivalenti, con l'obiettivo di trovarne un'espressione come *somma di prodotti*, dalla quale poi cercheremo di ottenere la *Forma Normale Disgiuntiva (=: F.N.D.)*, la *somma di tutti gli implicanti primi (=: s.t.i.p.)* e una *forma minimale (=: f.m.)*, che sono tutti casi particolari di *sommedi prodotti* equivalenti al polinomio assegnato. Dunque procediamo:

$$\begin{aligned} P(x,y,z,w) \;:=\; \Big(\big(w \wedge y'\big) \vee \big(z' \wedge w'' \wedge x \wedge y'\big)\Big)' \vee \Big(y' \wedge \big(w' \vee \big(z' \wedge 1'' \wedge x\big)\big)\Big)' \;\sim \\ \sim\; \Big(\big(\underline{w \wedge y'}\big) \vee \big(\big(z' \wedge x\big) \wedge \big(\underline{w \wedge y'}\big)\big)\Big)' \vee \Big(y' \wedge \big(w' \vee \big(z' \wedge 1'' \wedge x\big)\big)\Big)' \;\sim \\ \sim\; \Big(\big(w \wedge y'\big)\Big)' \vee \Big(y' \wedge \big(w' \vee \big(z' \wedge 1'' \wedge x\big)\big)\Big)' \end{aligned}$$

dove abbiamo sfruttato i (sotto)passaggi $w'' \sim w$ e l'identità di *assorbimento* $a \vee (b \wedge a) \sim a$ applicata in questo caso a $a := w \wedge y'$ e $b := z' \wedge x$. Poi sfruttiamo l'identità di *De Morgan* $(a \wedge b)' = a' \vee b'$ due volte, precisamente nei due casi $a := w$, $b := y'$ e $a := y'$, $b := \big(z' \wedge 1'' \wedge x\big)$. Così otteniamo

$$\begin{aligned} P(x,y,z,w) \;\sim\; \Big(\big(w \wedge y'\big)\Big)' \vee \Big(y' \wedge \big(w' \vee \big(z' \wedge 1'' \wedge x\big)\big)\Big)' \;\sim \\ \sim\; \big(w' \vee y''\big) \vee \Big(y'' \vee \big(w' \vee \big(z' \wedge 1'' \wedge x\big)\big)'\Big) \;\sim \\ \sim\; \big(w' \vee y\big) \vee \Big(y \vee \big(w' \vee \big(z' \wedge x\big)\big)'\Big) \end{aligned}$$

dove nell'ultimo passaggio abbiamo sfruttato le proprietà $y'' \sim y$ (due volte!...), $1'' \sim 1$ e $a \wedge 1 \wedge b \sim a \wedge b$. Adesso applichiamo le due identità di De Morgan $(a \vee b)' = a' \wedge b'$ e $(c \wedge d\,)' = c' \vee d'$ ai casi (in quest'ordine!) $a := w'$, $b := z' \wedge x$ e $c := z'$, $d := x$: così troviamo

$$\begin{aligned} P(x,y,z,w) \;\sim\; \big(w' \vee y\big) \vee \Big(y \vee \big(w' \vee \big(z' \wedge x\big)\big)'\Big) \;\sim \\ \sim\; \big(w' \vee y\big) \vee \Big(y \vee \big(w'' \wedge \big(z' \wedge x\big)'\big)\Big) \;\sim\; \big(w' \vee y\big) \vee \Big(y \vee \big(w'' \wedge \big(z'' \vee x'\big)\big)\Big) \;\sim \\ \sim\; \big(w' \vee y\big) \vee \Big(y \vee \big(w \wedge \big(z \vee x'\big)\big)\Big) \end{aligned}$$

dove nell'ultimo passaggio abbiamo sfruttato le proprietà $w'' \sim w$ e $z'' \sim z$. Adesso per la associatività dell'operazione $\vee$ e la sua idempotenza — per cui in particolare abbiamo $y \vee y \sim y$ — possiamo riscrivere

$$\begin{aligned} P(x,y,z,w) \;\sim\; \big(w' \vee y\big) \vee \Big(y \vee \big(w \wedge \big(z \vee x'\big)\big)\Big) \;\sim \\ \sim\; w' \vee y \vee\; y \vee \big(w \wedge \big(z \vee x'\big)\big) \;\sim\; w' \vee y \vee \big(w \wedge \big(z \vee x'\big)\big) \end{aligned}$$

Infine usiamo la distributività di $\wedge$ rispetto a $\vee$ per ottenere $\big(w \wedge \big(z \vee x'\big) \sim \big(w \wedge z\big) \vee \big(w \wedge x'\big)$, e in conseguenza

$$P(x,y,z,w) \sim w' \vee y \vee \big(w \wedge \big(z \vee x'\big)\big) \sim$$
$$\sim w' \vee y \vee \Big(\big(w \wedge z\big) \vee \big(w \wedge x'\big)\Big) \sim w' \vee y \vee \big(w \wedge z\big) \vee \big(w \wedge x'\big) \sim$$
$$\sim w' \vee y \vee \big(z \wedge w\big) \vee \big(x' \wedge w\big)$$

Così in definitiva abbiamo ottenuto

$$P(x,y,z,w) \sim w' \vee y \vee \big(z \wedge w\big) \vee \big(x' \wedge w\big) \tag{1}$$

dove l'elemento di destra è effettivamente una *somma di prodotti*, come richiesto.

(a) Per ottenere la *F.N.D.* di $P(x,y,z,w)$, partiamo dalla somma di prodotti — equivalente a $P(x,y,z,w)$ — nella formula (1) e "completiamo" ciascun prodotto che ci compare, cioè lo sostituiamo con la somma di prodotti *completi* e *non ridondante* ad esso equivalente: questo si calcola inserendo nel suddetto prodotto tutte le variabili mancanti, una volta senza segno di complemento e una volta invece con: così in particolare se le variabili mancanti sono k il prodotto considerato sarà equivalente alla somma di 2^k prodotti completi. Applicando questa strategia a ciascuno dei quattro prodotti (non completi) che figurano nella (1) otteniamo

$$w' \sim \big(x \wedge y \wedge z \wedge w'\big) \vee \big(x' \wedge y \wedge z \wedge w'\big) \vee \big(x \wedge y' \wedge z \wedge w'\big) \vee \big(x \wedge y \wedge z' \wedge w'\big) \vee$$
$$\vee \big(x' \wedge y' \wedge z \wedge w'\big) \vee \big(x' \wedge y \wedge z' \wedge w'\big) \vee \big(x \wedge y' \wedge z' \wedge w'\big) \vee \big(x' \wedge y' \wedge z' \wedge w'\big)$$
$$y \sim \big(x \wedge y \wedge z \wedge w\big) \vee \big(x' \wedge y \wedge z \wedge w\big) \vee \big(x \wedge y \wedge z' \wedge w\big) \vee \big(x \wedge y \wedge z \wedge w'\big) \vee$$
$$\vee \big(x' \wedge y \wedge z' \wedge w\big) \vee \big(x' \wedge y \wedge z \wedge w'\big) \vee \big(x \wedge y \wedge z' \wedge w'\big) \vee \big(x' \wedge y \wedge z' \wedge w'\big)$$
$$z \wedge w \sim \big(x \wedge y \wedge z \wedge w\big) \vee \big(x' \wedge y \wedge z \wedge w\big) \vee \big(x \wedge y' \wedge z \wedge w\big) \vee \big(x' \wedge y' \wedge z \wedge w\big)$$
$$x' \wedge w \sim \big(x' \wedge y \wedge z \wedge w\big) \vee \big(x' \wedge y' \wedge z \wedge w\big) \vee \big(x' \wedge y \wedge z' \wedge w\big) \vee \big(x' \wedge y' \wedge z' \wedge w\big)$$

Il nostro polinomio $P(x,y,z,w)$ è dunque equivalente alla somma dei 24 prodotti completi così*ottenuti*! Tuttavia, tra questi 24 prodotti ci sono molte ripetizioni, mentre nella *F.N.D.* ogni prodotto (completo) deve comparire al più *una sola volta*. Pertanto, dalla suddetta somma di 24 prodotti dobbiamo scartare gli eventuali "doppioni" — prendendoli però una volta (e soltanto una!): non dobbiamo cancellarli *tutti*... — e il risulato sarà proprio la *F.N.D.* cercata. Abbiamo dunque

$$P(x,y,z,w) \sim w' \vee y \vee \big(z \wedge w\big) \vee \big(x' \wedge w\big) \sim$$
$$\sim \big(x \wedge y \wedge z \wedge w\big) \vee \big(x \wedge y \wedge z \wedge w'\big) \vee \big(x \wedge y \wedge z' \wedge w\big) \vee \big(x \wedge y \wedge z' \wedge w'\big) \vee \big(x' \wedge y \wedge z \wedge w\big) \vee \sim$$
$$\sim \big(x' \wedge y \wedge z \wedge w'\big) \vee \big(x' \wedge y \wedge z' \wedge w\big) \vee \big(x' \wedge y \wedge z' \wedge w'\big) \vee \big(x \wedge y' \wedge z \wedge w'\big) \vee \big(x \wedge y' \wedge z' \wedge w'\big) \vee \sim$$
$$\sim \big(x' \wedge y' \wedge z \wedge w'\big) \vee \big(x' \wedge y' \wedge z' \wedge w'\big) \vee \big(x' \wedge y' \wedge z \wedge w\big) \vee \big(x' \wedge y' \wedge z' \wedge w\big) \vee \big(x \wedge y' \wedge z \wedge w\big)$$

e <u>*questa è la F.N.D. di* $P(x,y,z,w)$</u> .

Metodo alternativo (tramite le Tavole di Verità): In generale, la *F.N.D.* di un polinomio è la somma di tutti e soli i prodotti completi e non ridondanti che corrispondono alle stringhe di valori 0 e 1 su cui il polinomio assegnato vale 1. Oppure, in modo equivalente ma detto con una prospettiva rovesciata, è la somma di tutti i possibili prodotti completi e non ridondanti *tranne* quelli corrispondenti alle stringhe su cui il polinomio vale 0.

Ora, nel nostro caso dalla espressione (1) è particolaremente facile calcolare le stringhe su cui il polinomio $P(x,y,z,w)$ assume vale 0. Infatti, per ogni tale stringa $(a,b,c,d) \in \{0,1\}^{\times 4}$ dalla (1) abbiamo

$$\begin{aligned} P(a,b,c,d) \;&=\; \big(P(x,y,z,w)\big)(a,b,c,d) \;= \\ &=\; \Big(w' \vee y \vee \big(z \wedge w\big) \vee \big(x' \wedge w\big)\Big)(a,b,c,d\,) \;=\; d' \vee b \vee \big(c \wedge d\,\big) \vee \big(a' \wedge d\,\big) \end{aligned}$$

e inoltre

$$d' \vee b \vee \big(c \wedge d\,\big) \vee \big(a' \wedge d\,\big) = 0 \iff \begin{cases} d' \,=\, 0 \\ b \,=\, 0 \\ c \wedge d \,=\, 0 \\ a' \wedge d \,=\, 0 \end{cases} \iff \begin{cases} d' \,=\, 0 \\ b \,=\, 0 \\ c \,=\, 0 \\ a' \,=\, 0 \end{cases} \iff \begin{cases} a \,=\, 1 \\ b \,=\, 0 \\ c \,=\, 0 \\ d \,=\, 1 \end{cases}$$

così che

$$P(a,b,c,d) \;=\; 0 \quad \iff \quad (a,b,c,d) \;=\; (1,0,0,1)$$

Infine, il prodotto completo non ridondante corrispondente alla stringa $(1,0,0,1)$ è $x \wedge y' \wedge z' \wedge w$. Perciò, in conclusione, *la F.N.D. di* $P(a,b,c,d)$ *è la somma di tutti i prodotti completi non ridondanti ad esclusione di* $x \wedge y' \wedge z' \wedge w$. Notate che questo ci dà nuovamente la somma (di 15 prodotti...) ottenuta in precedenza.

NOTA: Vale la pena di osservare che, per determinare la *F.N.D.* di $P(a,b,c,d)$ tramite l'analisi delle tavole di verità (dunque tramite il calcolo dei diversi valori di $P(a,b,c,d)$ su tutte le stringhe di 0 e 1) invece di utilizzare la (1) si può usare un'altra espressione equivalente per $P(a,b,c,d)$ che rende i calcoli ancora più semplici. Infatti, ripartendo dalla (1) possiamo ottenere, tramite il *metodo del consenso*, le trasformazioni

$$\begin{aligned} P(x,y,z,w) \;&\sim\; w' \vee y \vee \big(z \wedge w\big) \vee \big(x' \wedge w\big) \;\sim \\ &\sim\; \underline{w'} \vee y \vee \big(\,\underline{z \wedge w}\,\big) \vee \big(x' \wedge w\big) \;\sim\; \underline{w'} \vee y \vee \big(\,\underline{z \wedge w}\,\big) \vee \underline{\underline{z}} \vee \big(x' \wedge w\big) \;\sim \\ &\sim\; w' \vee y \vee z \vee \big(x' \wedge w\big) \end{aligned}$$

ottenute per *consenso* e per *assorbimento*; analogamente, otteniamo poi

$$\begin{aligned} P(x,y,z,w) \;&\sim\; w' \vee y \vee z \vee \big(x' \wedge w\big) \;\sim \\ &\sim\; \underline{w'} \vee y \vee z \vee \big(\,\underline{x' \wedge w}\,\big) \;\sim\; \underline{w'} \vee y \vee z \vee \big(\,\underline{x' \wedge w}\,\big) \vee \underline{\underline{x'}} \;\sim \\ &\sim\; w' \vee y \vee z \vee x' \;\sim\; x' \vee y \vee z \vee w' \end{aligned}$$

dove nell'ultimo passaggio abbiamo usato le ovvie relazioni $r \vee s \sim s \vee r$ (conseguenza della commutatività di $\vee$). Dunque abbiamo trovato che

$$P(x,y,z,w) \;\sim\; x' \vee y \vee z \vee w' \tag{2}$$

che è ancora un'espressione di $P(x,y,z,w)$ come somma di prodotti, analoga alla (1) ma che risulta "migliore" di quella se puntiamo a calcolare la *F.N.D.* Infatti, procedendo come prima troviamo subito che

$$P(a,b,c,d) \;=\; \big(P(x,y,z,w)\big)(a,b,c,d) \;= \\ = \; \big(x' \vee y \vee z \vee w'\big)(a,b,c,d) \;=\; a' \vee b \vee c \wedge d'$$

e inoltre

$$a' \vee b \vee c \wedge d' \iff \begin{cases} a' \,=\, 0 \\ b \,=\, 0 \\ c \,=\, 0 \\ d' \,=\, 0 \end{cases} \iff (a,b,c,d) \,=\, (1,0,0,1)$$

così che troviamo nuovamente

$$P(a,b,c,d) \,=\, 0 \quad \iff \quad (a,b,c,d) \,=\, (1,0,0,1)$$

ma con passaggi intermedi più semplici. Da qui poi si conclude trovando la *F.N.D.* di $P(x,y,z,w)$ come prima.

D'altra parte, se pensiamo di calcolare la suddetta *F.N.D.* partendo da una espressione di $P(x,y,z,w)$ come somma di prodotti è più conveniente partire dalla (1) che non dalla (2). Infatti, in entrambi i casi si tratta di somme di 4 prodotti, però nella (2) tali prodotti hanno tutti grado 1, dunque uguale o più basso a quanto si ha nella (1) — così che la (2) è un'espressione *più semplice*, in senso stretto, della (1): ma ogni prodotto di grado 1 in 4 variabili quando "si completa" (inserendo le 3 variabili mancanti) è equivalente ad una somma di $2^3 = 8$ prodotti completi; così completando i quattro prodotti da 1 grado nella (2) il polinomio $P(x,y,z,w)$ si ritrova equivalente ad una somma di $4 \times 8 = 32$ prodotti completi, dalla quale poi dovremo scartare molti "doppioni" (a posteriori, sappiamo che dobbiamo scartarne esattamente 17, e ne restano 15; d'altra parte, i prodotti completi non ridondanti in 4 variabili sono in tutto 16, quindi già *a priori* sappiamo che dai 32 che abbiamo certamente ne dovremo scartare almeno $32 - 16 = 16$... Invece partendo dalla (1) avevamo trovato una somma di "soli" 24 prodotti (completi e non ridondanti), quindi l'operazione di "scarto dei doppioni" è certamente meno pesante.

(b) Per calcolare la *s.t.i.p.* di $P(x,y,z,w)$ possiamo applicare il *metodo del consenso* partendo da una qualsiasi somma di prodotti equivalente a $P(x,y,z,w)$ stesso. Se partiamo dalla (1), in due passi — del tipo "consenso + assorbimento" — arriviamo alla (2); oppure possiamo partire direttamente dalla (2)... Come che sia,

una volta giunti alla (2) non c'è consenso tra i prodotti in questa somma, e quindi il procedimento si arresta: pertanto *la (2) esprime proprio la s.t.i.p. di* $P(x,y,z,w)$, cioè *la s.t.i.p. di* $P(x,y,z,w)$ *è data da*

$$P(x,y,z,w) \;\sim\; x' \vee y \vee z \vee w' \;=:\; \underline{s.t.i.p.} \tag{3}$$

(c) Per calcolare una *f.m.* di $P(x,y,z,w)$ possiamo (ri)partire dalla *s.t.i.p.*, cioè dalla (3). In questa espressione è chiaro che nessuno dei quattro addendi — che sono, x', $;y$, z e w' — può essere cancellato. Infatti, vediamo cosa succede se sostituiamo ogni addendo con la sua F.N.D., che in ciascun caso è somma di $2^{4-1} = 2^3 = 8$ prodotti completi non ridondanti: in tutti questi 8 prodotti, l'addendo considerato compare sempre allo stesso modo (cioè sempre senza o sempre con il segno di ccomplemento). Considerando ad esempio l'addendo x', facciamo vedere che nella sua F.N.D. compare un addendo che non figura tra i $3 \times 8 = 24$ prodotti che compaiono complessivamente nelle F.N.D. di y, z e w': infatti, il prodotto (normale e completo) $x' \wedge y' \wedge z' \wedge w$ non compare tra quei 24 prodotti (non tra gli 8 di y perché c'è il fattore y', non tra gli 8 di z perché c'è il fattore z', e non tra gli 8 di w' perché c'è il fattore w), ma d'altra parte è senz'altro uno degli 8 prodotti che compaiono nella F.N.D. di x'. Pertanto, l'addendo x' *non può essere cancellato dalla somma in (3).* Analogamente, nessuno degli altri tre addendi può essere cancellato. Concludiamo allora che la (3) esprime anche una *f.m.* (l'unica esistente, in effetti, a meno di permutazioni degli addendi) di $P(x,y,z,w)$, cioè *una f.m. di* $P(x,y,z,w)$ *è data da*

$$P(x,y,z,w) \;\sim\; x' \vee y \vee z \vee w' \;=:\; \underline{f.m.} \tag{4}$$

[2] — La nostra tesi è che, per ogni $n \in \mathbb{N}$ con $n \geq 4$, vale la disuguaglianza $3^n - 5\,n \;>\; 2^n + 4\,n$. Volendo dimostrarla per induzione, proviamo l'*induzione debole* (o *semplice*), che procede in due passi: *Base dell'Induzione* e *Passo Induttivo.*

Base dell'Induzione: La tesi è vera per il più piccolo valore utile di n (per il quale l'enunciato abbia senso).

Nel caso in esame, dato che l'enunciato deve valere per ogni $n \geq 4$ tale valore più piccolo è $n_0 = 4$, dunque la base dell'induzione consiste nel dimostrare che $3^{n_0} - 5\,n_0 \;>\; 2^{n_0} + 4\,n_0$ per $n_0 := 4$.

Dimostrazione: La disuguaglianza da dimostrare è $3^{n_0} - 5\,n_0 \;>\; 2^{n_0} + 4\,n_0$ per $n_0 := 4$, cioè $3^4 - 5 \cdot 4 \;>\; 2^4 + 4 \cdot 4$. Il calcolo diretto ci dà

$$3^4 - 5 \cdot 4 \;=\; 81 - 20 \;=\; 61$$

per il membro di sinistra e

$$2^4 - 4 \cdot 4 \;=\; 16 - 16 \;=\; 0$$

e quindi, visto che $61 > 0$, la disuguaglianza è effettivamente dimostrata.

NOTA: osserviamo che invece la disuguaglianza $3^{n_0} - 5\,n_0 > 2^{n_0} + 4\,n_0$ *non è valida per* $n_0 := 3$, in quanto a sinistra si ha $3^3 - 5 \cdot 3 = 27 - 12 = 15$ e a destra $2^3 + 4 \cdot 3 = 8 + 12 = 20$, con $15 \not> 20$. Dunque $n = 4$ è effettivamente il valore più piccolo per il quale valga la disuguaglianza in esame.

Passo Induttivo (in forma debole): Per ogni valore utile di n, *SE è vero l'enunciato per* n *ALLORA è vero anche l'enunciato per* $n+1$.

Nel caso in esame, tale passo induttivo assume questa forma:
Sia $n \in \mathbb{N}$, $n \geq 4$. *SE (Ipotesi Induttiva)* $3^n - 5\,n > 2^n + 4\,n$,
ALLORA (Tesi Induttiva) $3^{n+1} - 5\,(n+1) > 2^{n+1} + 4\,(n+1)$.

Dimostrazione: Osserviamo prima di tutto che

$$3^x - 5\,x > 2^x + 4\,x \iff 3^x > 5\,x + 2^x + 4\,x \iff 3^x > 2^x + 9\,x$$

e quindi ponendo $x := n$ possiamo riscrivere l'Ipotesi Induttiva nella forma

$$\text{Hp. Ind.:} \quad 3^n > 2^n + 9\,n \tag{4}$$

e analogamente ponendo $x := n+1$ possiamo riscrivere la Tesi Induttiva nella forma

$$\text{Th. Ind.:} \quad 3^{n+1} > 2^{n+1} + 9\,(n+1) \tag{5}$$

Ora, il calcolo diretto ci dà

$$\begin{aligned} 3^{n+1} &= 3 \cdot 3^n \overset{\circledast}{>} 3 \cdot \big(2^n + 9\,n\big) = 3 \cdot 2^n + 3 \cdot 9\,n = \\ &= 2^n \cdot 2 + 2^n + 9\,n + 2 \cdot 9\,n > 2^{n+1} + 2^n + 9\,(n+1) - 9 + 9\,n = \\ &= 2^{n+1} + 9\,(n+1) + 2^n + 9\,(n-1) > 2^{n+1} + 9\,(n+1) \end{aligned}$$

dove nel fare la maggiorazione $\circledast$ (la prima!) abbiamo sfruttato l'Ipotesi Induttiva, nella forma (4). Dunque abbiamo ottenuto $3^{n+1} > 2^{n+1} + 9\,(n+1)$ che è proprio la Tesi Induttiva nella forma (5), q.e.d.

(*N.B.:* in quest'ultimo passo, dato che si tratta di dimostrare una disuguaglianza, è possibile procedre in vari modi diversi — quanto meno, diversi nei dettagli; il punto chiave però è che *prima o poi dovremo nell'arco del procedimento seguito dovremo far uso della Ipotesi Induttiva*, sia nella formulazione originaria, sia nella forma (4), sia in qualsiasi altra forma equivalente)

[3] — *(a)* Per definizione, la relazione "$\sim$" è di equivalenza se è *(R) riflessiva*, *(T) transitiva* e *(S) simmetrica*; dimostriamo dunque queste proprietà.

(R): dobbiamo dimostrare che $u \sim u$ per ogni $u \in \mathbb{Z}$. A tal fine, abbiamo

$$\begin{aligned} u \sim u &\iff 3\,u^2 + 7\,u^2 - 12 \equiv 8\,u + 2\,u + 28 \pmod 5 \iff \\ &\iff 10\,u^2 - 12 \equiv 10\,u + 28 \pmod 5 \iff 10\,u^2 \equiv 10\,u + 40 \pmod 5 \iff \\ &\iff 0\,u^2 - 12 \equiv 0\,u + 0 \pmod 5 \iff 0 \equiv 0 \pmod 5 \end{aligned}$$

e quindi siccome effettivamente $0 \equiv 0 \pmod 5$ possiamo concludere che $u \sim u$ per ogni $u \in \mathbb{Z}$, q.e.d.

(T): dobbiamo dimostrare che, per ogni $u, v, w \in \mathbb{Z}$, *se* $u \sim v$ e $v \sim w$ *allora* $u \sim w$. A tal fine, abbiamo

$$\begin{aligned} u \sim v &\iff 3\,u^2 + 7\,v^2 - 12 \equiv 8\,u + 2\,v + 28 \pmod 5 \\ v \sim w &\iff 3\,v^2 + 7\,w^2 - 12 \equiv 8\,v + 2\,w + 28 \pmod 5 \end{aligned}$$

Sommando prima riga e seconda riga, e utilizzando la notazione $A \equiv_5 B$ invece che $A \equiv B \pmod 5$, otteniamo

$$\begin{gathered} \big(3\,u^2 + 7\,v^2 - 12\big) + \big(3\,v^2 + 7\,w^2 - 12\big) \equiv_5 \big(8\,u + 2\,v + 28\big) + \big(8\,v + 2\,w + 28\big) \implies \\ \implies 3\,u^2 + 10\,v^2 + 7\,w^2 - 24 \equiv_5 8\,u + 10\,v + 2\,w + 56 \implies \\ \implies 3\,u^2 + 7\,w^2 - 12 \equiv_5 8\,u + 2\,w + 56 + 12 \implies 3\,u^2 + 7\,w^2 - 12 \equiv_5 8\,u + 2\,w + 28 \implies \\ \implies 3\,u^2 + 7\,w^2 - 12 \equiv_5 8\,u + 2\,w + 28 \implies u \sim w \end{gathered}$$

e dunque effettivamente $u \sim w$, q.e.d.

(S): dobbiamo dimostrare che, per ogni $u, v \in \mathbb{Z}$, *se* $u \sim v$ e $v \sim w$ *allora* $u \sim w$. A tal fine, abbiamo

$$\begin{gathered} u \sim v \iff 3\,u^2 + 7\,v^2 - 12 \equiv_5 8\,u + 2\,v + 28 \overset{\cdot(-1)}{\iff} \\ \overset{\cdot(-1)}{\iff} -3\,u^2 - 7\,v^2 + 12 \equiv_5 -8\,u - 2\,v - 28 \iff \\ \iff 7\,u^2 + 3\,v^2 + 12 \equiv_5 2\,u + 8\,v - 28 \iff \\ \iff 3\,v^2 + 7\,u^2 + 12 \equiv_5 8\,v + 2\,u - 28 \iff \\ \overset{-24}{\iff} 3\,v^2 + 7\,u^2 - 12 \equiv_5 8\,v + 2\,u - 52 \iff \\ \iff 3\,v^2 + 7\,u^2 - 12 \equiv_5 8\,v + 2\,u + 28 \iff v \sim u \end{gathered}$$

e dunque $u \sim v \implies v \sim u$, q.e.d.

In alternativa, sapendo che $u \sim v \iff f(u) = f(v)$ per la funzione f di cui alpunto *(b)* — in altre parole, assumendo come già provato il risultato in *(b)* — possiamo subito concludere che $\sim$ è un'equivalenza, perché ciò vale per tutte le relazioni di questo tipo, cioè associate in questo modo ad una funzione che abbia per dominio l'insieme in cui si considera la relazione stessa. Infatti si ha:

(R): $u \sim u$ per ogni $u \in \mathbb{Z}$, perché $u \sim u \iff f(u) = f(u)$ e certamente l'identità $f(u) = f(u)$ è sempre verificata.

(T): per ogni $u, v, w \in \mathbb{Z}$, se $u \sim v$ e $v \sim w$ allora abbiamo $f(u) = f(v)$ e $f(v) = f(w)$, da cui segue $f(u) = f(w)$ e quindi $u \sim w$, q.e.d.

(S): per ogni $u, v \in \mathbb{Z}$, se $u \sim v$ allora abbiamo $f(u) = f(v)$, da cui segue $f(v) = f(u)$ e quindi $v \sim u$, q.e.d.

(b) Sia $f : \mathbb{Z} \longrightarrow \mathbb{Z}_5$ la funzione data da $x \mapsto f(x) := \overline{x}\left(\overline{x} - \overline{1}\right)$. Abbiamo allora che

$$\begin{aligned}
u \sim v \iff 3\,u^2 + 7\,v^2 - 12 \equiv_5 8\,u + 2\,v + 28 \iff \\
\iff 3\,u^2 - 8\,u - 12 \equiv_5 -7\,v^2 + 2\,v + 28 \iff \\
\iff 3\,u^2 - 3\,u \equiv_5 3\,v^2 - 3\,v + 28 + 12 \iff \\
\iff 3\,u\,(u-1) \equiv_5 3\,v\,(v-1) + 40 \iff \\
\iff 3\,u\,(u-1) \equiv_5 3\,v\,(v-1) \overset{\cdot 2}{\iff} \\
\iff 6\,u\,(u-1) \equiv_5 6\,v\,(v-1) \iff \\
\iff u\,(u-1) \equiv_5 v\,(v-1) \iff \\
\iff \overline{u}\left(\overline{u} - \overline{1}\right) \equiv_5 \overline{v}\left(\overline{v} - 1\right) \quad \text{in} \quad \mathbb{Z}_5 \iff \\
\iff f(u) = f(v)
\end{aligned}$$

dunque $u \sim v \iff f(u) = f(v)$, q.e.d.

(c)–(d)–(e) Per definizione, per ogni $z \in \mathbb{Z}$ la sua classe di $\sim$–equivalenza è

$$[z]_\sim := \left\{ a \in \mathbb{Z} \,\middle|\, a \sim z \right\}$$

e quindi in forza del punto *(b)* abbiamo

$$[z]_\sim := \left\{ a \in \mathbb{Z} \,\middle|\, a \sim z \right\} = \left\{ a \in \mathbb{Z} \,\middle|\, f(a) = f(z) \right\} = f^{-1}\big(f(z)\big) \tag{6}$$

Per $\underline{z := 1}$ dalla (6) abbiamo

$$\begin{aligned}
[1]_\sim := f^{-1}\big(f(1)\big) := f^{-1}\big(\overline{0}\big) = \left\{ a \in \mathbb{Z} \,\middle|\, f(a) := \overline{a}\left(\overline{a} - \overline{1}\right) = \overline{0} \right\} = \\
= \left\{ a \in \mathbb{Z} \,\middle|\, \overline{a} = \overline{0} \text{ oppure } \overline{a} = \overline{1} \right\} = \left\{ a \in \mathbb{Z} \,\middle|\, a \equiv_5 0 \text{ oppure } a \equiv_5 1 \right\} = \\
= [0]_{\equiv_5} \cup [1]_{\equiv_5} = 5\,\mathbb{Z} \cup \big(1 + 5\,\mathbb{Z}\big)
\end{aligned}$$

Per $\underline{z := 3}$ dalla (6) abbiamo

$$\begin{aligned}
[3]_\sim := f^{-1}\big(f(3)\big) := f^{-1}\big(\overline{1}\big) = \left\{ a \in \mathbb{Z} \,\middle|\, f(a) := \overline{a}\left(\overline{a} - \overline{1}\right) = \overline{1} \right\} = \\
= [3]_{\equiv_5} = 3 + 5\,\mathbb{Z}
\end{aligned}$$

Per ogni $\underline{z \in \mathbb{Z}}$: Da quanto già visto in precedenza, abbiamo:

$$[z]_\sim = f^{-1}\big(f(z)\big)$$

quindi per determinare le classi di $\sim$–equivalenza dobbiamo conoscere la funzione f: il calcolo diretto ci dà

$$\overline{z}\left(\overline{z} - \overline{1}\right) = \begin{cases} \overline{0} & \text{per} \quad \overline{z} = \overline{0} \\ \overline{0} & \text{per} \quad \overline{z} = \overline{1} \\ \overline{2} & \text{per} \quad \overline{z} = \overline{2} \\ \overline{1} & \text{per} \quad \overline{z} = \overline{3} \\ \overline{2} & \text{per} \quad \overline{z} = \overline{4} \end{cases}$$

e quindi

$$f(z) \;=\; \begin{cases} \overline{0} & \text{per} \quad z \in 5\,\mathbb{Z} \\ \overline{0} & \text{per} \quad z \in \big(1+5\,\mathbb{Z}\big) \\ \overline{2} & \text{per} \quad z \in \big(2+5\,\mathbb{Z}\big) \\ \overline{1} & \text{per} \quad z \in \big(3+5\,\mathbb{Z}\big) \\ \overline{2} & \text{per} \quad z \in \big(4+5\,\mathbb{Z}\big) \end{cases}$$

Pertanto, ci sono esattamente tre classi di $\sim$–equivalenza, corrispondenti ai tre diversi valori assunti dalla funzione f, precisamente le classi

$$\begin{aligned} C_0 \;&=\; f^{-1}\big(\,\overline{0}\,\big) \;=\; \big(1+5\,\mathbb{Z}\big) \cup 5\,\mathbb{Z} \;=\; [0]_{\equiv_5} \cup [1]_{\equiv_5} \\ C_1 \;&=\; f^{-1}\big(\,\overline{1}\,\big) \;=\; \big(3+5\,\mathbb{Z}\big) \;=\; [3]_{\equiv_5} \\ C_2 \;&=\; f^{-1}\big(\,\overline{2}\,\big) \;=\; \big(2+5\,\mathbb{Z}\big) \cup \big(4+5\,\mathbb{Z}\big) \;=\; [2]_{\equiv_5} \cup [4]_{\equiv_5} \end{aligned}$$

[4] — *(a)* In breve, $\preceq$ è una relazione d'ordine perché è il "prodotto" di due relazioni d'ordine. In dettaglio, dobbiamo verificare che $\preceq$ sia *(R) riflessiva*, *(T) transitiva* e *(A) antisimmetrica*.

(R): Dobbiamo dimostrare che $(\mathcal{A}\,,d\,) \preceq (\mathcal{A}\,,d\,)$ per ogni coppia $(\mathcal{A}\,,d\,) \in E := \mathcal{P}\big(\{S,P,Q,R\}\big) \times D_{60}$. A tal fine, osserviamo che

$$(\mathcal{A}\,,d\,) \preceq (\mathcal{A}\,,d\,) \quad\Longleftrightarrow\quad \mathcal{A} \supseteq \mathcal{A} \quad \text{e} \quad d\,\big|d$$

e poiché entrambe le condizioni sono sempre soddisfatte — poiché le relazioni $\supseteq$ e $\big|$ sono entrambe riflessive! — possiamo concludere che $(\mathcal{A}\,,d\,) \preceq (\mathcal{A}\,,d\,)$ per ogni $(\mathcal{A}\,,d\,) \in E := \mathcal{P}\big(\{S,P,Q,R\}\big) \times D_{60}$, q.e.d.

(T): Dobbiamo dimostrare che, per ogni $\big(\mathcal{A}\,,d\big), \big(\mathcal{A}'\,,d'\big), \big(\mathcal{A}''\,,d''\big) \in E := \mathcal{P}\big(\{S,P,Q,R\}\big) \times D_{60}$, se $\big(\mathcal{A}\,,d\big) \preceq \big(\mathcal{A}'\,,d'\big)$ e $\big(\mathcal{A}'\,,d'\big) \preceq \big(\mathcal{A}''\,,d''\big)$ allora è anche $\big(\mathcal{A}\,,d\big) \preceq \big(\mathcal{A}''\,,d''\big)$. Ora, per definizione abbiamo

$$\begin{aligned} \big(\mathcal{A}\,,d\big) \preceq \big(\mathcal{A}'\,,d'\big) \quad&\Longrightarrow\quad \mathcal{A} \supseteq \mathcal{A}'\,,\; d\,\big|d' \\ \big(\mathcal{A}'\,,d'\big) \preceq \big(\mathcal{A}''\,,d''\big) \quad&\Longrightarrow\quad \mathcal{A}' \supseteq \mathcal{A}''\,,\; d'\,\big|d'' \end{aligned}$$

da cui — poiché le relazioni $\supseteq$ e $\big|$ sono entrambe transitive! — otteniamo

$$\mathcal{A} \supseteq \mathcal{A}''\,,\; d\,\big|d'' \quad\Longrightarrow\quad \big(\mathcal{A}\,,d\big) \preceq \big(\mathcal{A}''\,,d''\big)\,, \quad \text{q.e.d.}$$

(A): Dobbiamo dimostrare che, per ogni scelta di due coppie $\big(\mathcal{A}\,,d\big), \big(\mathcal{A}'\,,d'\big) \in E := \mathcal{P}\big(\{S,P,Q,R\}\big) \times D_{60}$, se $\big(\mathcal{A}\,,d\big) \preceq \big(\mathcal{A}'\,,d'\big)$ e $\big(\mathcal{A}'\,,d'\big) \preceq \big(\mathcal{A}\,,d\big)$ allora è necessariamente $\big(\mathcal{A}\,,d\big) = \big(\mathcal{A}'\,,d'\big)$. Ora, per definizione abbiamo

$$\begin{aligned} \big(\mathcal{A}\,,d\big) \preceq \big(\mathcal{A}'\,,d'\big) \quad&\Longrightarrow\quad \mathcal{A} \supseteq \mathcal{A}'\,,\; d\,\big|d' \\ \big(\mathcal{A}'\,,d'\big) \preceq \big(\mathcal{A}\,,d\big) \quad&\Longrightarrow\quad \mathcal{A}' \supseteq \mathcal{A}\,,\; d'\,\big|d \end{aligned}$$

da cui — poiché le relazioni $\supseteq$ e $\big|$ sono entrambe antisimmetriche! — otteniamo

$$\mathcal{A} = \mathcal{A}' \,,\; d = d' \quad \Longrightarrow \quad \big(\mathcal{A}\,, d\,\big) \preceq \big(\mathcal{A}'\,, d'\,\big) \,, \quad \text{q.e.d.}$$

(b) In sintesi, esiste un minimo in $\big(E\,; \preceq\,\big)$ perché ṗrodotto diretto di due insiemi ordinati aventi entrambi un minimo, così che la coppia formata dai due minimi è il minimo di $\big(E\,; \preceq\,\big)$. In dettaglio, possiamo procedere come segue.

Cerchiamo un elemento $(\mathcal{M}_-\,, m_-) \in E := \mathcal{P}\big(\{S,P,Q,R\}\big) \times D_{60}$ che sia *minimo*, dunque caratterizzato dalla proprietà che

$$(\mathcal{M}_-\,, m_-) \preceq (\mathcal{A}\,, d\,) \qquad\qquad \forall\;\; (\mathcal{A}\,, d\,) \in E := \mathcal{P}\big(\{S,P,Q,R\}\big) \times D_{60}$$

dunque — per come è definita la relazione d'ordine $\preceq$ — dalla proprietà che

$$\mathcal{M}_- \supseteq \mathcal{A}\,, \;\; m_- \,\big|d \qquad\qquad \forall\;\; \mathcal{A} \in \mathcal{P}\big(\{S,P,Q,R\}\big)\,, \;\; d \in \times D_{60}$$

Queste condizioni sono soddisfatte da un'unica scelta di $\mathcal{M}_- \in \mathcal{P}\big(\{S,P,Q,R\}\big)$ e di $m_- \in D_{60}$, rispettivamente il minimo di $\big(\,\mathcal{P}\big(\{S,P,Q,R\}\big)\,; \supseteq\,\big)$, che è $\mathcal{M}_- := \{S,P,Q,R\}$ — attenzione, NON è $\emptyset$, perché la relazione d'ordine usata è $\supseteq$ e non $\subseteq$... — e il minimo di $\big(D_{60}\,; \,\big|\,\big)$, che è $m_- = 1$. In conclusione, *esiste il minimo di* $\big(E\,; \preceq\,\big)$*, che è la coppia* $\big(\{S,P,Q,R\}\,, 1\big)$.

(c) Si può "dualizzare" il discorso fatto per *(b* e concludere... In sintesi, esiste un massimo in $\big(E\,; \preceq\,\big)$ perché ṗrodotto diretto di due insiemi ordinati aventi entrambi un massimo, così che la coppia formata dai due massimi è il massimo di $\big(E\,; \preceq\,\big)$. In dettaglio, possiamo procedere come segue.

Cerchiamo un elemento $(\mathcal{M}_+\,, m_+) \in E := \mathcal{P}\big(\{S,P,Q,R\}\big) \times D_{60}$ che sia *minimo*, dunque caratterizzato dalla proprietà che

$$(\mathcal{A}\,, d\,) \preceq (\mathcal{M}_+\,, m_+) \qquad\qquad \forall\;\; (\mathcal{A}\,, d\,) \in E := \mathcal{P}\big(\{S,P,Q,R\}\big) \times D_{60}$$

dunque — per come è definita la relazione d'ordine $\preceq$ — dalla proprietà che

$$\mathcal{A} \supseteq \mathcal{M}_+\,, \;\; d \,\big|m_+ \qquad\qquad \forall\;\; \mathcal{A} \in \mathcal{P}\big(\{S,P,Q,R\}\big)\,, \;\; d \in \times D_{60}$$

Queste condizioni sono soddisfatte da una e una sola coppia $\mathcal{M}_+ \in \mathcal{P}\big(\{S,P,Q,R\}\big)$ e di $m_+ \in D_{60}$, rispettivamente il massimo di $\big(\,\mathcal{P}\big(\{S,P,Q,R\}\big)\,; \supseteq\,\big)$, che è $\mathcal{M}_+ := \emptyset$ — attenzione, NON è $\{S,P,Q,R\}$, perché la relazione d'ordine usata è $\supseteq$ e non $\subseteq$... — e il massimo di $\big(D_{60}\,; \,\big|\,\big)$, che è $m_+ = 60$. In conclusione, *esiste il massimo di* $\big(E\,; \preceq\,\big)$*, che è la coppia* $\big(\emptyset\,, 60\big)$.

(d) Ricordiamo che un insieme ordinato $\big(\,E\,; \preceq\,\big)$ è un reticolo se per ogni $e', e'' \in E$ esistono $\inf_{\preceq}\big(e', e''\big) \in E$ e $\sup_{\preceq}\big(e', e''\big) \in E$. Nel caso in esame,

l'insieme ordinato considerato è il prodotto diretto di due insiemi ordinati — precisamente $\big(\,\mathcal{P}\big(\{S,P,Q,R\}\big)\,;\,\supseteq\,\big)$ e $\big(D_{60}\,;\,\big|\,\big)$ — che sono reticoli, e quindi anche $\big(\,E\,;\,\preceq\,\big)$ è a sua volta un reticolo, con $\inf_{\preceq}$ e $\sup_{\preceq}$ dati da

$$\begin{aligned}
\inf\nolimits_{\preceq}\Big(\big(\mathcal{A}',d'\,\big)\,,\big(\mathcal{A}'',d''\,\big)\Big) \;&=\; \Big(\inf\nolimits_{\supseteq}\big(\mathcal{A}',\mathcal{A}''\,\big)\,,\inf\nolimits_{|}\big(d',d''\,\big)\Big) \;= \\
&=\; \Big(\sup\nolimits_{\subseteq}\big(\mathcal{A}',\mathcal{A}''\,\big)\,,\inf\nolimits_{|}\big(d',d''\,\big)\Big) \;=\; \Big(\mathcal{A}'\cup\mathcal{A}''\,,M.C.D.\big(d',d''\big)\Big) \\
\sup\nolimits_{\preceq}\Big(\big(\mathcal{A}',d'\,\big)\,,\big(\mathcal{A}'',d''\,\big)\Big) \;&=\; \Big(\sup\nolimits_{\supseteq}\big(\mathcal{A}',\mathcal{A}''\,\big)\,,\sup\nolimits_{|}\big(d',d''\,\big)\Big) \;= \\
&=\; \Big(\inf\nolimits_{\subseteq}\big(\mathcal{A}',\mathcal{A}''\,\big)\,,\sup\nolimits_{|}\big(d',d''\,\big)\Big) \;=\; \Big(\mathcal{A}'\cap\mathcal{A}''\,,m.c.m.\big(d',d''\big)\Big)
\end{aligned}$$

(e) Il reticolo $\big(\,E\,;\,\preceq\,\big)$ è finito, e quindi ogni elemento in esso ammette una $\vee$–fattorizzazione non ridondante in $\vee$–irriducibili. Inoltre, il reticolo $\big(\,E\,;\,\preceq\,\big)$ è prodotto diretto dei due reticoli $\big(\,\mathcal{P}\big(\{S,P,Q,R\}\big)\,;\,\supseteq\,\big)$ e $\big(D_{60}\,;\,\big|\,\big)$ che sono anche *distributivi*, perciò anche $\big(\,E\,;\,\preceq\,\big)$ è a sua volta distributivo: ne segue che la suddetta $\vee$–fattorizzazione non ridondante in $\vee$–irriducibili di un qualunque elemento in $\big(\,E\,;\,\preceq\,\big)$ è necessariamente *unica*, a meno dell'ordine dei fattori.

Nel caso dell'elemento $\big(\{S,Q\}\,,30\big)$ calcoliamo prima come si $\vee$–fattorizzano le sue due componenti $\{S,Q\}$ e 30. Abbiamo

$$\{S,Q\} \;=\; \{S,P,Q\}\cap\{P,Q,R\} \;=\; \{S,P,Q\}\vee\{P,Q,R\} \tag{7}$$

con $\{S,P,Q\}$ e $\{P,Q,R\}$ due $\vee$–irriducibili nel reticolo $\big(\,\mathcal{P}\big(\{S,P,Q,R\}\big)\,;\,\supseteq\,\big)$, nel quale l'operazione "$\vee$" è "$\cap$" — e NON "$\cup$", perché la relazione d'ordine in uso è $\supseteq$, e non $\subseteq$. Inoltre

$$30 \;=\; 2\vee 3\vee 5 \tag{8}$$

con 2, 3 e 5 che sono $\vee$–irriducibili nel reticolo $\big(\,D_{60}\,;\,\big|\,\big)$, nel quale l'operazione "$\vee$" è "$m.c.m.$". A questo punto da (7) e (8) insieme otteniamo che

$$\begin{aligned}
\big(\{S,Q\}\,,30\big) \;&=\; \big(\{S,P,Q\}\vee\{P,Q,R\}\,,\,2\vee 3\vee 5\big) \;= \\
&=\; \big(\{S,P,Q\}\,,\,1\,\big)\vee\big(\{P,Q,R\}\,,\,1\,\big)\vee \\
&\qquad \vee\big(\{S,P,Q,R\}\,,\,2\,\big)\;\vee\;\big(\{S,P,Q,R\}\,,\,3\,\big)\;\vee\;\big(\{S,P,Q,R\}\,,\,5\,\big)
\end{aligned}$$

dove l'ultima espressione è la (unica) $\vee$–fattorizzazione non ridondante in $\vee$–irriducibili di $\big(\{S,Q\}\,,30\big)$ richiesta.

[5] — *(a)* Ricordiamo che, per definizione,

$$U\big(\mathbb{Z}_n\big) \;:=\; \big\{\, \overline{a} \in \mathbb{Z}_n \,\big|\, \overline{a} \text{ è invertibile in } \mathbb{Z}_n \big\}$$

e inoltre

$$\begin{aligned} &\overline{a} \;\big(\in \mathbb{Z}_n\big) \text{ è invertibile in } \mathbb{Z}_n \iff \\ &\iff \exists\, \overline{x} \in \mathbb{Z}_n : \overline{a}\cdot\overline{x} = \overline{1} \iff \exists\, x \in \mathbb{Z} :\, a\,x \equiv 1 \pmod{n} \iff \\ &\iff \text{l'equazione congruenziale } a\,x \equiv 1 \pmod{n} \text{ ammette soluzioni} \iff \\ &\iff M.C.D.(a,n) = 1 \end{aligned}$$

Pertanto abbiamo, in generale,

$$U\big(\mathbb{Z}_n\big) \;=\; \big\{\, \overline{a} \in \mathbb{Z}_n \,\big|\, M.C.D.(a,n) = 1 \big\} \tag{9}$$

e quindi applicando questo risultato al caso $n = 11$ otteniamo

$$U\big(\mathbb{Z}_{11}\big) \;=\; \big\{\, \overline{a} \in \mathbb{Z}_{11} \,\big|\, M.C.D.(a,11) = 1 \big\} \;=\; \big\{\, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10} \,\big\}$$

e applicandolo invece al caso $n = 12$ otteniamo

$$U\big(\mathbb{Z}_{12}\big) \;=\; \big\{\, \overline{a} \in \mathbb{Z}_{12} \,\big|\, M.C.D.(a,12) = 1 \big\} \;=\; \big\{\, \overline{1}, \overline{5}, \overline{7}, \overline{11} \,\big\}$$

N.B.: Dalla (9) abbiamo anche che

$$\begin{aligned} \big|U\big(\mathbb{Z}_n\big)\big| \;&=\; \big|\big\{\, \overline{a} \in \mathbb{Z}_n \,\big|\, M.C.D.(a,n) = 1 \big\}\big| \;= \\ &=\; \big|\big\{\, s \in \{0,1,\ldots,n-1\} \,\big|\, M.C.D.(s,n) = 1 \,\big\}\big| \;=:\; \varphi(n) \end{aligned}$$

dove φ è la *funzione di Eulero*. Allora, ricordando come si calcola tale funzione, abbiamo

$$\begin{aligned} \big|U\big(\mathbb{Z}_{11}\big)\big| \;&=\; \varphi(11) \;=\; 11 - 1 \;=\; 10 \\ \big|U\big(\mathbb{Z}_{12}\big)\big| \;&=\; \varphi(12) \;=\; \varphi\big(2^2\,3\big) \;=\; \varphi\big(2^2\big)\,\varphi(3) \;=\; (2-1)\,2\,(3-1) \;=\; 4 \end{aligned}$$

Nel primo caso, abbiamo che $\big|U\big(\mathbb{Z}_{11}\big)\big| = 10$. Dato che certamente $\overline{0} \notin U\big(\mathbb{Z}_{11}\big)$ — cioè $\overline{0}$ *non è invertibile* in $\mathbb{Z}_{11}$ — abbiamo $U\big(\mathbb{Z}_{11}\big) \subseteq \mathbb{Z}_{11}\setminus\big\{\overline{0}\big\}$, con $\big|\mathbb{Z}_{11}\setminus\big\{\overline{0}\big\}\big| = \big|\mathbb{Z}_{11}\big| - \big|\big\{\overline{0}\big\}\big| = 11 - 1 = 10 = \big|U\big(\mathbb{Z}_{11}\big)\big|$. Possiamo allora concludere che

$$U\big(\mathbb{Z}_{11}\big) \;=\; \mathbb{Z}_{11} \setminus \big\{\overline{0}\big\} \;=\; \big\{\, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10} \,\big\}$$

così abbiamo (ri)trovato $U\big(\mathbb{Z}_{11}\big)$ dalla sola conoscenza di $\varphi(11)$ e dall'osservazione (ovvia) che $\overline{0} \notin U\big(\mathbb{Z}_{11}\big)$.

Nel secondo caso, sappiamo che $U\big(\mathbb{Z}_{12}\big)$ ha quattro elementi. Ora, un elemento invertibile di qualunque anello unitario è sempre l'unità stessa! In particolare, in ogni $\mathbb{Z}_n$ abbiamo che $\overline{1}$ è certamente invertibile: dunque nel nostro caso $\overline{1} \in U\big(\mathbb{Z}_{12}\big)$.

Inoltre, ricordiamo che in ogni anello unitario se a è invertibile allora anche $-a$ è invertibile, in quanto ha per inverso l'elemento $(-a)^{-1} := -\big(a^{-1}\big)$. Nel nostro caso, prendendo $a := \overline{1}$ troviamo che anche $-\overline{1} = \overline{12-1} = \overline{11}$ è invertibile in $\mathbb{Z}_{12}$, cioè $\overline{11} \in U\big(\mathbb{Z}_{12}\big)$. Così abbiamo trovato due dei quattro elementi di $U\big(\mathbb{Z}_{12}\big)$. Infine, se in qualche modo troviamo un *terzo* elemento invertibile, ad esempio $\overline{5} \in U\big(\mathbb{Z}_{12}\big)$ — oppure $\overline{7} \in U\big(\mathbb{Z}_{12}\big)$ — allora possiamo subito dedurre anche che $-\overline{5} = \overline{12-5} = \overline{7} \in U\big(\mathbb{Z}_{12}\big)$ — oppure che $-\overline{7} = \overline{12-7} = \overline{5} \in U\big(\mathbb{Z}_{12}\big)$ — e dunque abbiamo anche un *quarto* elemento in $U\big(\mathbb{Z}_{12}\big)$. Siccome sappiamo già che $U\big(\mathbb{Z}_{12}\big)$ ha esattamente quattro elementi, possiamo concludere che li abbiamo trovati tutti.

Questo per dire che anche con un approccio indiretto, a partire da informazioni parziali come quelle su $\big|U\big(\mathbb{Z}_{12}\big)\big|$ possiamo eventualmente trovare tutto l'insieme $U\big(\mathbb{Z}_{12}\big)$ con poco sforzo (e pochi calcoli).

(b) Dovendo risolvere l'equazione congruenziale $45\,x \equiv -135 \pmod{12}$, procediamo come segue. Per prima cosa, sostituiamo il coefficiente 45 e il termine noto -135 con altri numeri a loro congruenti modulo 12 ma più piccoli in valore assoluto: quindi, osservando che $45 \equiv 9 \pmod{12}$ e $-135 \equiv 9 \pmod{12}$, otteniamo

$$45\,x \equiv -135 \pmod{12} \quad \Longleftrightarrow \quad 9\,x \equiv 9 \pmod{12} \tag{10}$$

e dall'espressione a destra vediamo subito che una ovvia soluzione è $x_0 = 1$. A questo punto, l'insieme di *tutte* le soluzioni si ottiene sommando a questa soluzione particolare tutti i possibili multipli interi di $\frac{12}{M.C.D.(9,12)} = \frac{12}{3} = 4$; dunque le soluzioni della nostra equazione congruenziale sono tutti e soli gli interi della forma

$$x \;=\; 1 \,+\, 4\,z \quad , \qquad \forall\; z \in \mathbb{Z} \tag{11}$$

Come *variante*, possiamo procedere così: una volta giunti alla (10), osserviamo che $M.C.D.(9,12) = 3$ — cioè il M.C.D. tra il coefficiente dell'incognita e il modulo) divide il termine noto 9, e quindi — se anche non ce ne fossimo accorti — *l'equazione è compatibile, cioè ammette soluzioni*; per trovarle tutte, *semplifichiamo* l'ultima equazione congruenziale trovata (equivalente all'originale) dividendo tutti i numeri coinvolti (coefficiente dell'incognita, termine noto e modulo) per $M.C.D.(9,12) = 3$, così da ottenere

$$45\,x \equiv -135 \pmod{12} \quad \Longleftrightarrow \quad 9\,x \equiv 9 \pmod{12} \quad \Longleftrightarrow \quad 3\,x \equiv 3 \pmod{4}$$

Adesso, osservando che una soluzione particolare di $3\,x \equiv 3 \pmod{4}$ è chiaramente $x_0 = 1$, otteniamo tutte le soluzioni sommando a questa i vari multipli interi di $\frac{4}{M.C.D.(3,4)} = \frac{4}{1} = 4$, e così facendo ritroviamo proprio quanto già ottenuto in (11).

(c) Dobbiamo trovare — se esiste... — una classe non nulla $\overline{z} \in \mathbb{Z}_s \setminus \big\{\overline{0}\big\}$ (per $s = 11$ e per $s = 12$) che abbia una potenza $\overline{z}^{\,n}$ pari a zero; inoltre possiamo sempre scegliere che sia $z > 1$. Fattorizziamo z in potenze di primi distinti, sia $z = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$; allora avremo anche $z^n = p_1^{n\,e_1} p_2^{n\,e_2} \cdots p_k^{n\,e_k}$. Ora avremo

$$\overline{z}^{\,n} \,=\, \overline{0} \;\Longleftrightarrow\; \overline{z^n} \,=\, \overline{0} \;\Longleftrightarrow\; z^n \in [0]_s = s\,\mathbb{Z} \;\Longleftrightarrow\; s \,\big|\, z^n$$

Se adesso fattorizziamo anche s in potenze di primi distinti, sia $s = q_1^{f_1} q_2^{f_2} \cdots q_h^{f_h}$, avremo che

$$\overline{z}^{\,n} = \overline{0} \iff s \,|\, z^n \iff q_1^{f_1} q_2^{f_2} \cdots q_h^{f_h} \,\Big|\, p_1^{n\,e_1} p_2^{n\,e_2} \cdots p_k^{n\,e_k} \iff$$
$$\iff \forall\ i = 1, \ldots, h\,,\ \exists\ j_i \in \{1, \ldots, k\}\ :\ q_i = p_{j_i}\,,\ \ f_i \leq n\,e_{j_i}$$

cioè, a parole, ogni fattore primo di s dev'essere anche uno dei fattori primi di z, e il suo esponente in s dev'essere minore o uguale di quello che ha in z^n. Ora, la seconda condizione — cioè che $f_i \leq n\,e_{j_i}$ — è certamente soddisfatta se si prende un esponente n abbastanza grande; dunque la sola, vera condizione stringente è la prima, precisamente che ogni fattore primo di s sia anche fattore primo di z.

Nel caso $s = 11$ c'è soltanto il fattore primo $q_1 = 11$. Dunque abbiamo che $\overline{z}$ ha una potenza nulla se e soltanto se 11 è fattore primo di z, cioè se 11 divide z: ma in tal caso abbiamo anche $\overline{z} = \overline{0} \in \mathbb{Z}$, dunque concludiamo che *NON esiste una classe* $\overline{z} \in \mathbb{Z}_{11} \setminus \{\overline{0}\}$ *tale che* $\overline{z}^{\,n} = \overline{0}$ *per un qualche esponente* $n \in \mathbb{N}$.

Nel caso $s = 12 = 2^2\,3$ ci sono i due fattori primi $q_1 = 2$ e $q_2 = 3$. Dunque abbiamo che $\overline{z}$ ha una potenza nulla se e soltanto se 2 e 3 sono entrambi fattori primi di z, cioè se z è divisibile per 6. Scegliendo un rappresentante z tra 1 e 11, troviamo una e una sola possibilità $z = 6$. Così concludiamo che *esiste una (e una sola!) classe* $\overline{z} \in \mathbb{Z}_{12} \setminus \{\overline{0}\}$ *tale che* $\overline{z}^{\,n} = \overline{0}$ *per un qualche esponente* $n \in \mathbb{N}$, *precisamente* $\overline{z} = \overline{6}$. Il minimo esponente che dia potenza zero è $n = 2$, in quanto abbiamo $\overline{6}^{\,2} = \overline{6^2} = \overline{36} = \overline{12 \cdot 3} = \overline{0}$.

(*N.B.:* naturalmente, qui sopra ho sviluppato un discorso generale, ma nello svolgere il compito d'esame basta anche molto meno: con pochi calcoli in $\mathbb{Z}_{12}$ e poi in $\mathbb{Z}_{11}$ ci si rende rapidamente conto di come vanno le cose, e della differenza tra i due casi, così che si può risolvere il problema senza bisogno di un'analisi generale)