ALGEBRA e LOGICA

CdL in Ingegneria Informatica

prof. Fabio GAVARINI

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

Esame scritto del 18 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] Per ogni $a \in \mathbb{Z}$, si consideri la funzione $f_a : \mathbb{Q} \longrightarrow \mathbb{Q}$ definita da $f_a(q) := a\,(a-2)\,q + 7$ per ogni $q \in \mathbb{Q}$; sia poi $f_a^{\mathbb{Z}} : \mathbb{Z} \longrightarrow \mathbb{Z}$ la restrizione di f_a al sottoinsieme $\mathbb{Z}$ dei numeri interi — così $f_a^{\mathbb{Z}}(z) := a\,(a-2)\,z + 7\,, \ \forall\, z \in \mathbb{Z}$.

(a) Determinare tutti i valori di $a \in \mathbb{Z}$ per i quali la funzione f_a sia *iniettiva*.

(b) Determinare tutti i valori di $a \in \mathbb{Z}$ per i quali la funzione f_a sia *suriettiva*.

(c) Determinare tutti i valori di $a \in \mathbb{Z}$ per i quali la funzione $f_a^{\mathbb{Z}}$ sia *suriettiva*.

[2] Determinare tutte le soluzioni del sistema di equazioni congruenziali

$$\circledast : \begin{cases} -26\,x \equiv 2 & (\bmod 14) \\ 33\,x \equiv -57 & (\bmod 30) \\ 32\,x \equiv 44 & (\bmod 18) \end{cases}$$

[3] Sia $E := \mathcal{P}(\mathbb{N})$ l'insieme delle parti di $\mathbb{N}$, e si consideri in E la relazione "$\multimap$" definita da

$$F' \multimap F'' \iff \left|F'\right| \leq \left|F''\right| \qquad \forall \ \ F', F'' \in E$$

dove $\left|F\right|$ indica la cardinalità di un qualunque sottoinsieme F di $\mathbb{N}$.

(a) Dimostrare che la relazione $\multimap$ è *riflessiva*.

(b) Dimostrare che la relazione $\multimap$ è *transitiva*.

(c) Dimostrare che la relazione $\multimap$ *non è di equivalenza*.

(d) Dimostrare che la relazione $\multimap$ *non è d'ordine*.

(continua...)

[4] *(a)* Determinare — se esiste — il più piccolo valore di $x \in \mathbb{Z}$ tale che

$$x \equiv 543^{80431} \pmod{20} \qquad \text{e} \qquad 35 \leq x \leq 78$$

(b) Calcolare tutte le soluzioni dell'equazione modulare $\overline{-317}\,\overline{x} = \overline{543^{80431}}$ nell'anello $\mathbb{Z}_{20}$ delle classi resto modulo 20.

[5] Si consideri l'insieme $\mathbb{H} := \{3, 1, 2, 6, 15, 10, 60, 30, 20\}$ ed in esso la relazione di divisibilità, indicata con δ, per la quale la coppia $(\mathbb{H}; \delta)$ costituisce un insieme ordinato. Si risolvano i seguenti problemi:

(a) L'insieme ordinato $(\mathbb{H}; \delta)$ è un'*algebra di Boole*? Perché?

(b) Disegnare il *diagramma di Hasse* dell'insieme ordinato $(\mathbb{H}; \delta)$.

(c) Esiste $\sup(\{15, 3, 6, 10, 2\})$ in $(\mathbb{H}; \delta)$? In caso negativo, spiegare perché; in caso affermativo, precisare quale sia tale estremo superiore.

(d) Dimostrare che $(\mathbb{H}; \delta)$ è un reticolo, *precisando i valori di* $a \vee b := sup(\{a, b\})$ *e di* $a \wedge b := inf(\{a, b\})$ in tutti i casi non banali (cioè quando $a \not\delta b$ e $b \not\delta a$, *evitando* di calcolare $b \vee a$ e $b \wedge a$ se quando si siano già calcolati $a \vee b$ e $a \wedge b$...).

(e) Esistono degli elementi $\vee$*–irriducibili* in $(\mathbb{H}; \delta)$? In caso negativo, spiegare perché non esistano; in caso affermativo, precisare quali siano.

— ⋆ —

SOLUZIONI

[1] — *(a)* Ricordiamo che una funzione si dice *iniettiva* se si verifica che *due elementi del dominio hanno la stessa immagine soltanto se coincidono*: nel caso della funzione $f_a : \mathbb{Q} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Q}$, questa condizione in formule si esprime così: per ogni $q_1, q_2 \in \mathbb{Q}$, *se* $f_a(q_1) = f_a(q_2)$ *allora* $q_1 = q_2$.

Consideriamo dunque un $a \in \mathbb{Q}$ — che definisce la funzione f_a — e due elementi $q_1, q_2 \in \mathbb{Q}$ tali che $f_a(q_1) = f_a(q_2)$, e vediamo quali condizioni ne discendono.

Esplicitando la condizione $f_a(q_1) = f_a(q_2)$ abbiamo

$$a(a-2)q_1 + 7 =: f_a(q_1) = f_a(q_2) := a(a-2)q_2 + 7 \implies$$
$$\implies a(a-2)q_1 + 7 = a(a-2)q_2 + 7 \implies a(a-2)q_1 = a(a-2)q_2 \implies$$
$$\implies a(a-2)(q_1 - q_2) = 0 \implies \begin{cases} a(a-2) = 0 \\ \text{oppure} \\ (q_1 - q_2) = 0 \end{cases} \implies \begin{cases} a \in \{0, 2\} \\ \text{oppure} \\ q_1 = q_2 \end{cases}$$

Pertanto, l'implicazione $f_a(q_1) = f_a(q_2) \implies q_1 = q_2$ è valida se e soltanto se $a \in \mathbb{Q} \setminus \{0\,,2\}$, e quindi *$f_a$ è iniettiva se e soltanto se $a \in \mathbb{Q} \setminus \{0\,,2\}$*.

Per completezza, osserviamo poi che nei casi $a \in \{0\,,2\}$ abbiamo che (direttamente dalla definizione) *le funzioni f_0 e f_2 coincidono entrambe con la funzione costante di valore 7*, cioè $f_0(q) = 7 = f_2(q)$ per ogni $q \in \mathbb{Q}$; in particolare $f_0 = f_2$ *non è iniettiva.*

(b) Ricordiamo che una funzione si dice *suriettiva* se si verifica che *per ogni elemento del codominio esiste (almeno) un elemento del dominio del quale il primo è l'immagine*; nel caso della funzione $f_a : \mathbb{Q} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Q}$, questa condizione in formule si esprime così: per ogni $b \in \mathbb{Q}$, esiste un $q \in \mathbb{Q}$ tale che $f_a(q) = b$.

Consideriamo dunque un $a \in \mathbb{Q}$ — che definisce la funzione f_a: cerchiamo allora sotto quali condizioni per a si verifichi che per ogni $b \in \mathbb{Q}$ l'equazione $f_a(q) = b$ — in cui l'incognita è $q \in \mathbb{Q}$ — abbia (almeno) una soluzione.

Esplicitando l'equazione $f_a(q) = b$ si trova

$$f_a(q) = b \iff a\,(a-2)\,q + 7 \,=\, b \iff a\,(a-2)\,q \,=\, b - 7 \qquad (1)$$

Ora, *per qualsiasi valore di $b \in \mathbb{Q}$* si ha che *l'equazione più a destra in (1) ha soluzioni se e soltanto se esiste $\big(a\,(a-2)\big)^{-1} \in \mathbb{Q}$, cioè $a\,(a-2) \neq 0$, cioè $a \in \mathbb{Q}\setminus\{0\,,2\}$, e in tal caso la soluzione è unica, data da $q := \big(a\,(a-2)\big)^{-1}\,(b-7)$*. Pertanto, possiamo concludere che *f_a è suriettiva se e soltanto se $a \in \mathbb{Q} \setminus \{0\,,2\}$*.

(c) Come prima, la funzione $f_a^{\mathbb{Z}} : \mathbb{Z} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}$ sarà *suriettiva* se *per ogni elemento del codominio esiste (almeno) un elemento del dominio del quale il primo è l'immagine*; nel caso attuale, questa condizione diventa: per ogni $b \in \mathbb{Z}$, esiste un $z \in \mathbb{Z}$ tale che $f_a^{\mathbb{Z}}(z) = b$.

N.B.: attenzione alla differenza col caso di $f_a : \mathbb{Q} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Q}$ ... Nel confronto, la funzione $f_a^{\mathbb{Z}}$ ha un codominio più piccolo — $\mathbb{Z}$ invece di $\mathbb{Q}$ — il che "facilita le cose", perché dobbiamo considerare molte meno equazioni (perché sono di meno i possibili termini noti b). D'altra parte, la funzione $f_a^{\mathbb{Z}}$ ha anche un dominio più piccolo — di nuovo $\mathbb{Z}$ invece di $\mathbb{Q}$ — dunque l'insieme in cui cercare soluzioni delle nostre equazioni è molto più ridotto! In breve, posto che la suriettività è la condizione per cui "ogni bersaglio è colpito da (almeno) un arciere", per la funzione $f_a^{\mathbb{Z}}$ rispetto alla funzione f_a ci sono molti meno bersagli da colpire, ma anche molti meno arcieri che possano colpirli...

Consideriamo dunque una generica funzione $f_a^{\mathbb{Z}}$ — per un qualsiasi $a \in \mathbb{Q}$ — e vediamo per quali condizioni su a si verifichi che per ogni $b \in \mathbb{Z}$ l'equazione $f_a^{\mathbb{Z}}(z) = b$ — in cui l'incognita è $z \in \mathbb{Z}$ — abbia (almeno) una soluzione.

Procedendo come prima, l'equazione $f_a^{\mathbb{Z}}(z) = b$ ci dà

$$f_a^{\mathbb{Z}}(z) = b \iff a\,(a-2)\,z + 7 \,=\, b \iff a\,(a-2)\,z \,=\, b - 7 \qquad (2)$$

Ora, *per qualsiasi valore di $b \in \mathbb{Z}$* abbiamo che *l'equazione più a destra in (2) ha soluzioni se e soltanto se esiste $\big(a\,(a-2)\big)^{-1} b \in \mathbb{Z}$: dato che $b \in \mathbb{Z}$ è arbitrario,*

l'unica possibilità è che esiste $\big(a\,(a-2)\big)^{-1} \in \mathbb{Z}$, *cioè* $a\,(a-2) \in \{+1\,,-1\}$ — *e in tal caso la soluzione è unica, data da* $z := \big(a\,(a-2)\big)^{-1}\,(b-7)$. L'analisi diretta (facile) ci mostra che

$$a\,(a-2)\,\in\,\{+1\,,-1\} \quad\Longleftrightarrow\quad a=1$$

e in tal caso — cioè per $a=1$ — si ha $a\,(a-2)\,=\,-1$. Pertanto, possiamo concludere che $f_a^{\mathbb{Z}}$ *è suriettiva se e soltanto se* $a=1$.

In alternativa, possiamo procedere anche così. Per ogni $z\in\mathbb{Z}$, la sua immagine $f_a^{\mathbb{Z}}(z) := a\,(a-2)\,z+7$ è sempre congruente a 7 modulo $a\,(a-2)$; più precisamente, variando z queste immagini formano complessivamente tutta la classe di congruenza di 7 modulo $a\,(a-2)$, in formule $Im\big(f_a^{\mathbb{Z}}\big) := \big\{f_a^{\mathbb{Z}}(z)\,\big|\,z\in\mathbb{Z}\big\} = [7]_{\equiv_{a(a-2)}}$. Ora, $f_a^{\mathbb{Z}}$ è suriettiva (per definizione) se e soltanto se $Im\big(f_a^{\mathbb{Z}}\big) = \mathbb{Z}$, quindi se e soltanto se $[7]_{\equiv_{a(a-2)}} = \mathbb{Z}$, per l'analisi precedente. Ma

$$[7]_{\equiv_{a(a-2)}} = \mathbb{Z} \quad\Longleftrightarrow\quad \equiv_{a(a-2)} = id_{\mathbb{Z}} \quad\Longleftrightarrow\quad a\,(a-2)\,\in\,\{+1\,,-1\} \quad\Longleftrightarrow\quad a\,=\,1$$

e così troviamo che $f_a^{\mathbb{Z}}$ *è suriettiva se e soltanto se* $a=1$ (come già visto prima).

[2] — Per risolvere il sistema $\circledast$ in prima battuta semplifichiamo le sue singole equazioni congruenziali; questo ci dà

$$\circledast\,:\begin{cases} -26\,x\,\equiv\,2 & (\,\mathrm{mod}\,14\,) \\ 33\,x\,\equiv\,-57 & (\,\mathrm{mod}\,30\,) \\ 32\,x\,\equiv\,44 & (\,\mathrm{mod}\,18\,) \end{cases} \quad\Longleftrightarrow\quad \begin{cases} 2\,x\,\equiv\,2 & (\,\mathrm{mod}\,14\,) \\ 3\,x\,\equiv\,3 & (\,\mathrm{mod}\,30\,) \\ -4\,x\,\equiv\,8 & (\,\mathrm{mod}\,18\,) \end{cases}$$

A questo punto, ciascuna delle equazioni congruenziali, separatamente, è ammette soluzioni, perché in ciascun caso il M.C.D. tra il coefficiente della incognita e il modulo divide il termine noto. Allora possiamo procedere a semplificare ciascuna di tali equazioni dividendo coefficiente della incognita, modulo e termine noto per il suddetto M.C.D. Questo passaggio ci porta a

$$\circledast \quad\Longleftrightarrow\quad \begin{cases} 2\,x\,\equiv\,2 & (\,\mathrm{mod}\,14\,) \\ 3\,x\,\equiv\,3 & (\,\mathrm{mod}\,30\,) \\ -4\,x\,\equiv\,8 & (\,\mathrm{mod}\,18\,) \end{cases} \quad\Longleftrightarrow\quad \begin{cases} 1\,x\,\equiv\,1 & (\,\mathrm{mod}\,7\,) \\ 1\,x\,\equiv\,1 & (\,\mathrm{mod}\,10\,) \\ -2\,x\,\equiv\,4 & (\,\mathrm{mod}\,9\,) \end{cases}$$

che a sua volta ci dà (ovviamente)

$$\circledast \quad\Longleftrightarrow\quad \circledcirc\,:\begin{cases} x\,\equiv\,+1 & (\,\mathrm{mod}\,7\,) \\ x\,\equiv\,+1 & (\,\mathrm{mod}\,10\,) \\ x\,\equiv\,-2 & (\,\mathrm{mod}\,9\,) \end{cases} \tag{3}$$

Quest'ultimo è un sistema (equivalente a quello iniziale) *in forma cinese*, con moduli a due a due coprimi: quindi ammette soluzioni, che possiamo ottenere tramite il *Teorema Cinese del Resto*. Oppure, possiamo risolverlo per sostituzioni successive.

Primo metodo (tramite il Teorema Cinese del Resto): Consideriamo i numeri

$$R := 7 \cdot 10 \cdot 9 = 630 \,, \quad R_1 := R/7 = 90 \,, \quad R_2 := R/10 = 63 \,, \quad R_3 := R/9 = 70$$

e le tre equazioni congruenziali

$$\begin{array}{rcl} R_1\, x_1 \equiv +1 \pmod 7 & & 90\, x_1 \equiv +1 \pmod 7 \\ R_2\, x_2 \equiv +1 \pmod{10} & \iff & 63\, x_2 \equiv +1 \pmod{10} \\ R_3\, x_3 \equiv -2 \pmod 9 & & 70\, x_3 \equiv -2 \pmod 9 \end{array}$$

che riducendo i coefficienti delle incognite — tramite $90 \equiv_7 -1$, $63 \equiv_1 03$, $70 \equiv_7 -2$ — ci danno

$$\begin{array}{rcl} -1\, x_1 \equiv +1 \pmod 7 & & x_1 \equiv -1 \pmod 7 \\ 3\, x_2 \equiv +1 \pmod{10} & \iff & x_2 \equiv +7 \pmod{10} \\ -2\, x_3 \equiv -2 \pmod 9 & & x_3 \equiv +1 \pmod 9 \end{array}$$

A questo punto prendendo le tre soluzioni particolari $x_1 = -1$, $x_2 = +7$, $x_3 = -1$, di ciascuna di queste tre equazioni congruenziali troviamo una soluzione particolare del sistema $\circledcirc$ — e quindi del sistema iniziale $\circledast$ — con la formula

$$x_0 \;:=\; R_1\, x_1 + R_2\, x_2 + R_3\, x_3 \;=\; 90 \cdot (-1) + 63 \cdot 7 + 70 \cdot 1 \;=\; -90 + 441 + 70 \;=\; 421$$

Infine, *tutte* le soluzioni del sistema $\circledast$ si trovano sommando alla soluzione particolare $x_0 = 421$ tutti i multipli interi di $R = 630$: pertanto, *le soluzioni del sistema* $\circledast$ *sono tutti e soli i numeri interi della forma*

$$x \;=\; x_0 + 630\, z \;=\; 421 + 630\, z \qquad\qquad \forall\; z \in \mathbb{Z} \tag{4}$$

Secondo metodo (tramite Sostituzioni Successive): Andiamo ora a risolvere la prima equazione, poi sostituiamo la sua soluzione generica nella seconda equazione, risolviamo quest'ultima, poi sostituiamo nella terza e risolviamo. Dunque, partendo dalla (3), abbiamo

$$\circledast \iff \circledcirc : \begin{cases} x \equiv +1 \pmod 7 \\ x \equiv +1 \pmod{10} \\ x \equiv -2 \pmod 9 \end{cases} \iff \begin{cases} x = 1 + 7\, z \;, \quad z \in \mathbb{Z} \\ x \equiv +1 \pmod{10} \\ x \equiv -2 \pmod 9 \end{cases}$$

dove abbiamo risolto la prima equazione; poi sostituendo nella seconda, risolvendo quest'ultima (nella nuovaincognita z), e così via, troviamo

$$\left\{\begin{array}{lll} x = 1+7z\ , & z\in\mathbb{Z} & \\ x\equiv +1 & (\mathrm{mod}\ 10) \\ x\equiv -2 & (\mathrm{mod}\ 9) \end{array}\right. \iff \left\{\begin{array}{lll} x = 1+7z\ , & z\in\mathbb{Z} & \\ 1+7z\equiv 1 & (\mathrm{mod}\ 10) \\ x\equiv -2 & (\mathrm{mod}\ 9) \end{array}\right. \iff$$

$$\iff \left\{\begin{array}{lll} x = 1+7z\ , & z\in\mathbb{Z} & \\ 7z\equiv 0 & (\mathrm{mod}\ 10) \\ x\equiv -2 & (\mathrm{mod}\ 9) \end{array}\right. \iff \left\{\begin{array}{lll} x = 1+7z\ , & z\in\mathbb{Z} & \\ z\equiv 0 & (\mathrm{mod}\ 10) \\ x\equiv -2 & (\mathrm{mod}\ 9) \end{array}\right. \iff$$

$$\iff \left\{\begin{array}{lll} x = 1+7z\ , & z\in\mathbb{Z} & \\ z = 0+10y\ , & y\in\mathbb{Z} & \\ x\equiv -2 & (\mathrm{mod}\ 9) \end{array}\right. \iff \left\{\begin{array}{lll} x = 1+7(10y)\ , & y\in\mathbb{Z} & \\ x\equiv -2 & (\mathrm{mod}\ 9) \end{array}\right. \iff$$

$$\iff \left\{\begin{array}{lll} x = 1+70y\ , & y\in\mathbb{Z} & \\ 1+70y\equiv -2 & (\mathrm{mod}\ 9) \end{array}\right. \iff \left\{\begin{array}{lll} x = 1+70y\ , & y\in\mathbb{Z} & \\ -2y\equiv -3\equiv 6 & (\mathrm{mod}\ 9) \end{array}\right. \iff$$

$$\iff \left\{\begin{array}{lll} x = 1+70y\ , & y\in\mathbb{Z} & \\ y\equiv -3 & (\mathrm{mod}\ 9) \end{array}\right. \iff \left\{\begin{array}{lll} x = 1+70y\ , & y\in\mathbb{Z} & \\ y = -3+9k\ , & k\in\mathbb{Z} & \end{array}\right. \iff$$

$$\iff x = 1+70y = 1+70(-3+9k) = 1-210+630k = -209+630k\ ,\ \ k\in\mathbb{Z}$$

e così concludiamo che *le soluzioni del sistema* $\circledast$ *sono tutti e soli i numeri interi della forma*

$$x = -209 + 630k \qquad \forall\ k\in\mathbb{Z} \tag{5}$$

N.B.: a dispetto delle apparenze, *la (4) e la (5) non sono in contraddizione tra loro*, in quanto definiscono lo stesso insieme di numeri interi, soltanto che sono parametrizzati in due modi diversi! Si noti infatti che

$$421 + 630z = x = -209 + 630k \qquad \Longleftrightarrow \qquad k - z = 1$$

<u>*NOTA:*</u> Un'ulteriore semplificazione possibile è la seguente. *Prima* di procedere alla sua risoluzione, osserviamo che il sistema $\circledcirc$ può ancora essere drasticamente semplificato, riducendo le equazioni congruenziali da tre a due. Infatti, le prime due equazioni congruenziali in $\circledcirc$ ammettono chiaramente la soluzione comune $x_0 = 1$, che dunque è una soluzione particolare del sottosistema formato da queste due sole equazioni congruenziali. Dalla teoria generale — ad esempio, dal *Teorema Cinese del Resto* — sappiamo allora che tale sottosistema avrà per soluzioni tutti e soli i numeri interi della forma

$$x = 1 + 7\cdot 10\cdot z = 1 + 70z \qquad \forall\ z\in\mathbb{Z}$$

o in altre parole

$$x \equiv 1 \pmod{70} \tag{6}$$

In conclusione, le prime due equazioni congruenziali nel sistema $\circledcirc$ sono complessivamente equivalenti (nel senso che hanno lo stesso insieme di soluzioni) alla singola equazione congruenziale (6): pertanto, abbiamo un'equivalenza di sistemi

$$\circledast \quad \Longleftrightarrow \quad \circledcirc : \begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 1 \pmod{10} \\ x \equiv 2 \pmod 9 \end{cases} \quad \Longleftrightarrow \quad \otimes : \begin{cases} x \equiv 1 \pmod{70} \\ x \equiv 2 \pmod 9 \end{cases}$$

A questo punto si può risolvere il sistema $\otimes$ — tramite il *Teorema Cinese del Resto* o per sostituzioni successive — che è equivalente a quello iniziale, per cui le sue soluzioni saranno esattamente tutte e sole le soluzioni del sistema $\circledast$; va da sé perla risoluzione questa volta sarà molto più veloce rispetto a prima perché si starà trattando un sistema di *due* sole equazioni congruenziali invece che tre.

[3] — *(a)* Dobbiamo dimostrare che per ogni $F \in \mathcal{P}(\mathbb{N})$ si ha $F \multimap F$. Ma questo è ovvio perché, certamente $|F| = |F|$, e quindi (per definizione) anche $F \multimap F$, q.e.d.

(b) Dobbiamo dimostrare che per ogni $F_1, F_2, F_3 \in \mathcal{P}(\mathbb{N})$ si ha che, *se* $F_1 \multimap F_2$ e $F_2 \multimap F_3$, *allora* $F_1 \multimap F_3$. Ora, per definizione di $\multimap$ le ipotesi danno

$$F_1 \multimap F_2 \implies \big|F_1\big| \leq \big|F_2\big| \qquad \text{e} \qquad F_2 \multimap F_3 \implies \big|F_2\big| \leq \big|F_3\big|$$

da cui ricaviamo $\big|F_1\big| \leq \big|F_2\big| \leq \big|F_3\big|$ e quindi $\big|F_1\big| \leq \big|F_3\big|$, che significa esattamente che $F_1 \multimap F_3$, q.e.d.

(c) Ricordiamo che una relazione è di equivalenza se è riflessiva, transitiva e simmetrica. Visto che sappiamo già che la relazione $\multimap$ è riflessiva e transitiva, dobbiamo dimostrare che *non è simmetrica*. A tal fine, dobbiamo verificare che esistono $F_1, F_2 \in \mathcal{P}(\mathbb{N})$ tali che $F_1 \multimap F_2$ e $F_2 \not\multimap F_1$. Ora, le condizioni $F_1 \multimap F_2$ e $F_2 \not\multimap F_1$ equivalgono a $\big|F_1\big| \leq \big|F_2\big|$ e $\big|F_2\big| \not\leq \big|F_1\big|$, che complessivamente equivalgono all'unica condizione $\big|F_1\big| \lneqq \big|F_2\big|$. Pertanto, ogni scelta di sottoinsiemi $F_1, F_2 \in \mathcal{P}(\mathbb{N})$ tali che $\big|F_1\big| \lneqq \big|F_2\big|$ ci darà una violazione della condizione di simmetria: ad esempio, possiamo scegliere $F_1 := \{9\}$ e $F_2 := \{2\,,4\,,8\}$, con i quali abbiamo appunto $F_1 \multimap F_2$ e $F_2 \not\multimap F_1$, q.e.d.

(d) Ricordiamo che una relazione è di equivalenza se è riflessiva, transitiva e antisimmetrica. Visto che sappiamo già che la relazione $\multimap$ è riflessiva e transitiva, dobbiamo dimostrare che *non è antisimmetrica*. A tal fine, dobbiamo verificare che esistono $F_1, F_2 \in \mathcal{P}(\mathbb{N})$ tali che $F_1 \multimap F_2$ e $F_2 \multimap F_1$ ma $F_1 \not\multimap F_2$. Ora, le condizioni $F_1 \multimap F_2$ e $F_2 \multimap F_1$ equivalgono a $\big|F_1\big| \leq \big|F_2\big|$ e $\big|F_2\big| \leq \big|F_1\big|$, che complessivamente equivalgono all'unica condizione $\big|F_1\big| = \big|F_2\big|$. Pertanto, ogni scelta di sottoinsiemi $F_1, F_2 \in \mathcal{P}(\mathbb{N})$ tali che $\big|F_1\big| = \big|F_2\big|$ ma $F_1 \neq F_2$ ci darà una violazione della condizione di simmetria: ad esempio, possiamo scegliere $F_1 :=$

$\{13\,,9\,,25\}$ e $F_2 := \{72\,,4\,,8\}$, con i quali abbiamo appunto $F_1 \multimap F_2$ e $F_2 \multimap F_1$ ma $F_1 \neq F_2$. Un altro esempio, con sottoinsiemi infiniti, può essere fatto scegliendo $F_1 := 2\,\mathbb{N}$ (= tutti i numeri naturali pari) e $F_1 := \big(1 + 2\,\mathbb{N}\big)$ (= tutti i numeri naturali dispari), che di nuovo danno $F_1 \multimap F_2$ e $F_2 \multimap F_1$ ma $F_1 \neq F_2$, q.e.d.

[4] — *(a)* Per trovare il più piccolo valore di $x \in \mathbb{Z}$ tale che $x \equiv_{20} 543^{\,80431}$ e $35 \leq x \leq 78$, lavoriamo con l'anello $\mathbb{Z}_{20}$ delle classi di congruenza modulo 20 — indicate tramite i rappresentanti $\overline{0}\,,\overline{1}\,,\ldots\,,\overline{19}$ — e vediamo di capire quale sia la classe $\overline{543^{\,80431}}$. Una volta fatto questo, cerchiamo (se esiste...) il più piccolo rappresentante della classe trovata che sia compreso nell'intervallo tra 35 e 78. In particolare, osserviamo che ogni classe di congruenza modulo 20 è formata da numeri interi che sono disposti a intervalli di ampiezza 20, quindi ogni tale classe ha certamente almeno un rappresentante nell'intervallo tra 35 e 78, dato che quest'ultimo ha ampiezza 44 (e $44 > 20$). Perciò sappiamo già che *un intero x del tipo richiesto esiste certamente*.

Per cominciare (per definizione del prodotto in $\mathbb{Z}_{20}$ e poiché $543 \equiv_{20} 3$) abbiamo

$$\overline{543^{\,80431}} \;=\; \overline{543}^{\,80431} \;=\; \overline{3}^{\,80431}$$

A questo punto osserviamo che $M.C.D.(3,20) = 1$, quindi di può applicare il *Teorema di Eulero* che ci dà $\overline{3}^{\,\varphi(20)} = \overline{1}$ in $\mathbb{Z}_{20}$, dove φ è la funzione di Eulero; possiamo allora "ridurre modulo 20 l'esponente 80431". Siccome $\varphi(20) = \varphi\big(5 \cdot 2^2\big) = \varphi(5) \cdot \varphi\big(2^2\big) = (5-1)\cdot(2-1)\,2 = 8$, ciò significa che $\overline{3}^{\,8} = \overline{1}$ in $\mathbb{Z}_{20}$; quindi, dividendo 80431 per $\varphi(2) = 8$, abbiamo $80431 = 8 \cdot q + 7$ per un certo quoziente $q \in \mathbb{Z}$ — che non è necessario conoscere esattamente! Ci basta sapere che $80431 \equiv_8 7$ — e quindi

$$\overline{543^{\,80431}} \;=\; \overline{3}^{\,80431} \;=\; \overline{3}^{\,8\cdot q+7} \;=\; \big(\overline{3}^{\,8}\big)^{q} \cdot \overline{3}^{\,7} \;=\; \big(\overline{1}\big)^{q} \cdot \overline{3}^{\,7} \;=\; \overline{1} \cdot \overline{3}^{\,7} \;=\; \overline{3}^{\,7}$$

Infine, andiamo a calcolare $\overline{3}^{\,7}$: dal calcolo diretto abbiamo

$$\overline{3}^{\,2} \;=\; 9\,, \qquad \overline{3}^{\,3} \;=\; \overline{27} \;=\; \overline{7}\,, \qquad \overline{3}^{\,4} \;=\; \overline{3}^{\,3} \cdot \overline{3} \;=\; \overline{7} \cdot \overline{3} \;=\; \overline{21}^{\,4} \;=\; \overline{1} \tag{7}$$

da cui anche

$$\overline{543^{\,80431}} \;=\; \overline{3}^{\,7} \;=\; \overline{3}^{\,4} \cdot \overline{3}^{\,3} \;=\; \overline{1} \cdot \overline{7} \;=\; \overline{7} \tag{8}$$

Per concludere, da quanto già ottenuto sappiamo che il nostro x richiesto dev'essere il più piccolo possibile che soddisfi le condizioni $x \equiv_{20} 543^{\,80431} \equiv_{20} 7$ e $35 \leq x \leq 78$. La prima condizione ci dice che $x \in \big\{\, 7 + 20\,z \,\big|\, z \in \mathbb{Z} \,\big\}$; la seconda quindi ci impone $35 \leq 7 + 20\,z \leq 78$ da cui ricaviamo i due possibili valori 47 e 67: tra questi, il più piccolo è 47, dunque in conclusione *la soluzione è* $x = 47$.

<u>*NOTA:*</u> Anche senza saper nulla del *Teorema di Eulero*, dalle formule in (7) — che vengono da calcoli elementari... — si appura che $\overline{3}^{\,4} = \overline{1}$ in $\mathbb{Z}_{20}$ — che è

un risultato anche più forte di quello garantito dal suddetto teorema. Sfruttando questa informazione, dividendo l'esponente 80431 per 4, abbiamo $80431 = 4 \cdot q' + 3$ per un certo quoziente $q' \in \mathbb{Z}$ — che non è necessario conoscere esattamente! Ci basta sapere che $80431 \equiv_8 3$, che è ben più facile da capire — e quindi

$$\overline{543}^{\,80431} \;=\; \overline{3}^{\,80431} \;=\; \overline{3}^{\,4\cdot q'+3} \;=\; \left(\overline{3}^{\,4}\right)^{q'} \cdot \overline{3}^{\,3} \;=\; \left(\overline{1}\right)^{q'} \cdot \overline{3}^{\,3} \;=\; \overline{1} \cdot \overline{3}^{\,3} \;=\; \overline{3}^{\,3} \;=\; \overline{7}$$

(b) Per risolvere l'equazione modulare assegnata $\overline{-317}\,\overline{x} = \overline{543^{80431}}$ in $\mathbb{Z}_{20}$ cominciamo con il "ridurre a forma più semplice" il coefficiente e il termine noto: per quanto già visto in (8) abbiamo $\overline{543^{80431}} = \overline{7}$ per il termine noto, mentre $\overline{-317} = \overline{-17} = \overline{3}$ per il coefficiente della incognita $\overline{x}$. Quindi la nostra equazione diventa

$$\overline{3}\,\overline{x} = \overline{7} \qquad\qquad \text{in} \quad \mathbb{Z}_{20} \tag{9}$$

Per risolvere quest'ultima, osserviamo che *esiste* $\overline{3}^{\,-1} \in \mathbb{Z}_{20}$, percé $M.C.D.(3,20) = 1$, quindi *esiste un'unica soluzione, data da* $\overline{x} = \overline{3}^{\,-1}\,\overline{7}$. Per calcolarla, occorre conoscere $\overline{3}^{\,-1}$: con facili calcoli (oppure per tentativi e verifiche, al limite...) troviamo che $\overline{3}^{\,-1} = \overline{7}$, infatti $\overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$. Pertanto concludiamo che *la soluzione richiesta esiste ed è unica, data da*

$$\overline{x} \;=\; \overline{3}^{\,-1}\,\overline{7} \;=\; \overline{7}\,\overline{7} \;=\; \overline{49} \;=\; \overline{9} \qquad\qquad \text{in} \quad \mathbb{Z}_{20} \tag{10}$$

In alternativa, possiamo calcolare la soluzione della equazione modulare (9) passando alla equazione diofantea associata

$$3\,x \,+\, 20\,y \;=\; 7 \qquad\qquad \text{in} \quad \mathbb{Z} \tag{11}$$

che certamente ammette soluzioni perché $M.C.D.(3,20) = 1 \,\Big|\, 7$. Per calcolare una soluzione della (11) cerchiamo prima una *identità di Bézout* per $M.C.D.(3,20) = 1$ utilizzando l'algoritmo euclideo delle divisioni successive. I calcoli danno le divisioni successive

$$\begin{aligned} 3 \;&=\; 20 \cdot 0 \,+\, 3 \\ 20 \;&=\; 3 \cdot 6 \,+\, 2 \\ 3 \;&=\; 2 \cdot 1 \,+\, 1 \end{aligned} \tag{12}$$

da queste identità ricaviamo

$$\begin{aligned} \underline{3} \;&=\; 3 \,+\, 20 \cdot (-0) \\ \underline{2} \;&=\; 20 \,+\, \underline{3} \cdot (-6) \\ 1 \;&=\; 3 \,+\, \underline{2} \cdot (-1) \end{aligned}$$

e infine sostituendo a ritroso i termini sottolineati con le loro espressioni alla riga precedente otteniamo

$$\begin{aligned} 1 \;=\; 3 + 2 \cdot (-1) \;&=\; 3 + \big(20 \,+\, 3 \cdot (-6)\big) \cdot (-1) \;=\; 20 \cdot (-1) \,+\, 3 \cdot 7 \;= \\ &=\; 20 \cdot (-1) \,+\, \big(3 \,+\, 20 \cdot (-0)\big) \cdot 7 \;=\; 3 \cdot 7 \,+\, 20 \cdot (-1) \end{aligned}$$

(si noti che sia in (12) sia in questo ultimo calcolo c'è un "passaggio a vuoto", che si potrebbe saltare: l'ho invece mantenuto per sottolineare che l'algoritmo, nella sua automaticità, lo fa comunque, senza trovare "intoppi"...). Dunque abbiamo trovato

$$3 \cdot 7 \, + \, 20 \cdot (-1) \; = \; 1 \tag{13}$$

che è un'identità di Bézout per $M.C.D.(3, 20)$. Da questa segue che $3 \cdot 7 \equiv_{20} 1$ e quindi $\overline{3} \cdot \overline{7} = \overline{1}$ in $\mathbb{Z}_{20}$, che significa che esiste $\overline{3}^{\,-1} = \overline{7} \in \mathbb{Z}_{20}$ (di cui abbiamo fatto uso in precedenza). Inoltre, moltiplicando ambo i membri della (13) per 7 otteniamo

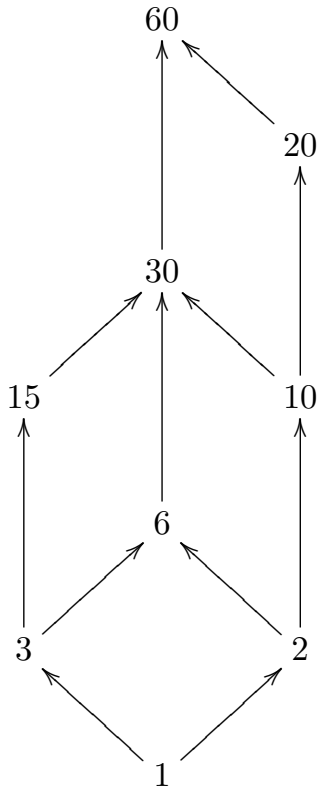
$$7 \; = \; 7 \cdot 1 \; = \; 7 \cdot \big(3 \cdot 7 \, + \, 20 \cdot (-1)\big) \; = \; 3 \cdot 49 \, + \, 20 \cdot (-7)$$

da cui leggiamo che la coppia $(49, -7)$ è una soluzione dell'equazione diofantea in (11). A questo punto da $3 \cdot 49 + 20 \cdot (-7) = 7$ ricaviamo che $3 \cdot 49 \equiv_{20} 7$ e quindi $\overline{3} \cdot \overline{49} = \overline{7}$ in $\mathbb{Z}_{20}$, cioè $\overline{x} = \overline{49} = \overline{9} \in \mathbb{Z}_{20}$ *è una soluzione (unica!) dell'equazione modulare di partenza*, in accordo con (10).

[5] — *(a)* L'insieme $\mathbb{H}$ è finito, con esattamente 9 elementi. Ora, come conseguenza del *Teorema di Rappresentazione di Stone* sappiamo che ogni algebra di Boole *finita* ha un numero di elementi che è una potenza di 2, cioè è del tipo 2^n per un certo esponente $n \in \mathbb{N}$. Siccome $|\mathbb{H}| = 9$ *non è una potenza di 2*, possiamo concludere che $\big(\mathbb{H}; \delta\big)$ *non è un'algebra di Boole*. Si noti che con questo metodo non c'è nemmeno bisogno di analizzare come sia fatta la relazione d'ordine fissata in $\mathbb{H}$: qualunque essa sia, la conclusione sarà sempre la stessa, in quanto dipende soltanto da una proprietà insiemistica di $\mathbb{H}$ stesso.

In alternativa, possiamo procedere anche come segue. Dall'analisi del diagramma di Hasse di $\big(\mathbb{H}; \delta\big)$ — quindi analizzando come sia fatta la relazione d'ordine δ — troviamo che tale insieme ordinato ha un minimo (e in un'algebra di Boole effettivamente ciò è richiesto!), in relazione a tale minimo l'insieme ordinato ha esattamente *due atomi* (che sono 2 e 3); inoltre, esso è un reticolo che ha esattamente *cinque elementi* $\vee$*–irriducibili non banali (cioè diversi dal minimo)* (che sono 2, 3, 15, 10 e 20). Ma in ogni algebra di Boole finita gli elementi $\vee$–irriducibili coincidono con gli atomi, perciò possiamo concludere che $\big(\mathbb{H}; \delta\big)$ *non è un'algebra di Boole*, come sopra (ma in modo ben più macchinoso!...).

(b) Il *diagramma di Hasse* di $\big(\mathbb{H};\delta\big)$ è il seguente:



(c) Sì, esiste $\sup\big(\{\,15\,,3\,,6\,,10\,,2\,\}\big)$ *in* $\big(\mathbb{H}\,;\delta\big)$*, che è*

$$\sup\big(\{\,15\,,3\,,6\,,10\,,2\,\}\big) \;=\; 30 \;\in\; \big(\mathbb{H}\,;\delta\big)$$

Invece non esiste $\max\big(\{\,15\,,3\,,6\,,10\,,2\,\}\big)$, mentre ci sono in $\{\,15\,,3\,,6\,,10\,,2\,\}$ ben *tre elementi massimali distinti*, precisamente 15, 6 e 10.

N.B.: Questo è un errore tipico, dovuto a confusione nella comprensione di somiglianze e differenze tra i concetti di "estremo superiore" (="sup") e di "massimo" (="max"). In particolare, l'estremo superiore di un dato sottoinsieme lo "cerchiamo" in *tutto* l'insieme ordinato in cui si trova il sottoinsieme, mentre invece il massimo lo cerchiamo all'interno del sottoinsieme stesso.

(d) Direttamente dall'analisi del diagramma di Hasse, deduciamo che l'insieme ordinato $\big(\mathbb{H};\delta\,\big)$ è effettivamente un reticolo, in cui $\sup\big(\{a,b\}\big)$ e $\inf\big(\{a,b\}\big)$ nei casi non banali sono dati da

$$\sup\big(\{2,3\}\big)=6\;,\quad \sup\big(\{2,15\}\big)=30\;,\quad \sup\big(\{3,10\}\big)=30\;,\quad \sup\big(\{3,20\}\big)=60$$
$$\sup\big(\{6,10\}\big)\;=\;30\;\;,\quad \sup\big(\{6,15\}\big)\;=\;30\;\;,\quad \sup\big(\{6,20\}\big)\;=\;60$$
$$\sup\big(\{10,15\}\big)\;=\;30\;\;,\quad \sup\big(\{15,20\}\big)\;=\;60\;\;,\quad \sup\big(\{20,30\}\big)\;=\;60$$
$$\inf\big(\{2,3\}\big)=1\;,\quad \inf\big(\{2,15\}\big)=1\;,\quad \inf\big(\{3,10\}\big)=1\;,\quad \inf\big(\{3,20\}\big)=1$$
$$\inf\big(\{6,10\}\big)\;=\;2\;\;,\quad \inf\big(\{6,15\}\big)\;=\;3\;\;,\quad \inf\big(\{6,20\}\big)\;=\;2$$
$$\inf\big(\{10,15\}\big)\;=\;1\;\;,\quad \inf\big(\{15,20\}\big)\;=\;1\;\;,\quad \inf\big(\{20,30\}\big)\;=\;10$$

NOTA: Vale la pena sottolineare che, in generale, a priori *non possiamo sapere se* $\sup\big(\{a,b\}\big) = m.c.m.(a,b)$ né se $\inf\big(\{a,b\}\big) = M.C.D.(a,b)$, sebbene la relazione d'ordine sia la divisibilità! Infatti, dalla tavola qui sopra possiamo osservare che si ha $\sup\big(\{a,b\}\big) = m.c.m.(a,b)$ per ogni $a,b \in \mathbb{H}$ mentre invece

e

$$\inf\big(\{10,15\}\big) \;=\; 1 \;\neq\; 5 \;=\; M.C.D.(10,15)$$
$$\inf\big(\{15,20\}\big) \;=\; 1 \;\neq\; 5 \;=\; M.C.D.(15,20)$$

In effetti, tale (apparente) "anomalia" si verifica proprio perché si tratta di casi di elementi $a,b \in \mathbb{H}$ per i quali $M.C.D.(a,b) \notin \mathbb{H}$.

(e) Nel caso di un reticolo (non vuoto) *finito* — qual è $\big(\mathbb{H}\,;\delta\big)$ — ci sono sicuramente elementi $\vee$–irriducibili, ed è particolarmente facile riconoscerli, in quanto sono semplicemente *quelli che hanno meno di due "segmenti di copertura" al di sotto di sé* — se ce n'è proprio zero vuol dire che stiamo guardando il minimo (caso banale), mentre se ce n'è esattamente uno abbiamo un $\vee$–irriducibile non banale. Per il caso di $\big(\mathbb{H};\delta\,\big)$, guardando il diagramma di Hasse vediamo dunque che *esistono elementi $\vee$–irriducibili, che sono 1, 3, 2, 15, 10, 20.*