ALGEBRA e LOGICA
CdL in Ingegneria Informatica
prof. Fabio GAVARINI

a.a. 2016–2017 — Sessione Autunnale, II appello
Esame scritto del 22 Settembre 2017 — *Testo e Svolgimento*

. . . .

N.B.: compilare il compito in modo sintetico ma **esauriente***, spiegando chiaramente quanto si fa, e scrivendo in corsivo con grafia leggibile.*

. . . . * . . . .

[1] Determinare tutti i numeri interi $x \in \mathbb{Z}$ per i quali si abbia *simultaneamente*

$$-93 \cdot x \equiv 378 \pmod{15} \qquad \text{e} \qquad [215]_7 \cdot [x]_7 = -[24]_7 \quad \big(\text{in } \mathbb{Z}_7\big)$$

[2] Si considerino i numeri naturali $M := 750486^{6457}$ e $N := 750483^{6455}$.

(a) Calcolare il resto della divisione di N per 20 .

(b) Determinare se esistano nell'anello $\mathbb{Z}_{20}$ degli interi modulo 20 le classi $\overline{M}^{\,-1}$ e $\overline{N}^{\,-1}$ inverse della classe $\overline{M} := [M]_{20}$ e della classe $\overline{N} := [N]_{20}$ rispettivamente. In caso negativo, si spieghi perché una tale classe inversa non esista; in caso affermativo, si calcoli esplicitamente la classe inversa in questione.

[3] Nell'insieme $\mathbb{N}$ dei numeri naturali si consideri la relazione $\lessdot$ definita da

$$h \lessdot k \iff \Big|\big\{\, x \in \{2,5\} \,\big|\, x \,\delta_{\mathbb{N}}\, h \,\big\}\Big| \leq \Big|\big\{\, y \in \{2,5\} \,\big|\, y \,\delta_{\mathbb{N}}\, k \,\big\}\Big| \qquad \forall\; h,k \in \mathbb{N}$$

dove $\delta_{\mathbb{N}}$ indica la consueta relazione di divisibilità in $\mathbb{N}$.

(a) Dimostrare che la relazione $\lessdot$ è una relazione di preordine in $\mathbb{N}$.

(b) Dimostrare che la relazione $\lessdot$ *non* è una relazione di ordine in $\mathbb{N}$.

(c) Dimostrare che la relazione $\Diamond := \lessdot \cap \gtrdot = \lessdot \cap \lessdot^{-1}$ è una relazione di equivalenza in $\mathbb{N}$.

(d) Determinare la cardinalità dell'insieme quoziente $\Big|\, \mathbb{N}\big/\Diamond \,\Big|$.

(e) Descrivere esplicitamente le cinque classi di $\Diamond$–equivalenza $[28]_{\Diamond}$, $[15]_{\Diamond}$, $[21]_{\Diamond}$, $[38]_{\Diamond}$ e $[30]_{\Diamond}$.

(continua...)

[4] Dimostrare *per induzione* che per ogni $n \in \mathbb{N}_+$ vale l'identità
$$\sum_{s=1}^{n} (2\,s-1) \;=\; n^2$$

[5] Dato l'insieme $\mathbb{T} := \{\,18\,,3\,,70\,,1\,,10\,,630\,,14\,\}$, si consideri in esso la relazione (d'ordine) di divisibilità, indicata qui di seguito con δ.

(a) Verificare che l'insieme ordinato $\big(\mathbb{T}\,;\delta\big)$ è un reticolo, scrivendo esplicitamente tutti i valori $\sup(x,y)$ e $\inf(x,y)$ per ogni $x,y \in \mathbb{T}$.

(b) Determinare il minimo, il massimo, tutti gli atomi e tutti gli elementi $\vee$–irriducibili del reticolo $\mathbb{T}$.

(c) Determinare se esista una $\vee$–fattorizzazione non ridondante in *fattori* $\vee$–*irriducibili* per l'elemento 630 nel reticolo $\mathbb{T}$. In caso affermativo, si determini esplicitamente (almeno) una tale $\vee$–fattorizzazione; in caso negativo, si spieghi perché essa non esista.

(d) Determinare se esista una $\vee$–fattorizzazione non ridondante in *atomi* per l'elemento 630 nel reticolo $\mathbb{T}$. In caso affermativo, si determini esplicitamente (almeno) una tale $\vee$–fattorizzazione; in caso negativo, si spieghi perché essa non esista.

(e) Stabilire, giustificando adeguatamente la risposta, se il reticolo $\big(\mathbb{T}\,;\delta\big)$ sia un'algebra di Boole oppure no.

— ⋆ —

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] — L'equazione modulare $[215]_7 \cdot [x]_7 \;=\; -[24]_7$ nell'anello $\mathbb{Z}_7$ chiaramente è equivalente all'equazione congruenziale $215 \cdot x \;=\; -24 \;(\bmod 7)$ in $\mathbb{Z}$; perciò risolvere il problema assegnato equivale a risolvere il sistema di equazioni congruenziali
$$\circledast\;:\;\begin{cases} -93\,x \;\equiv\; 378 \qquad (\bmod 15) \\ \\ 215\,x \;\equiv\; -24 \qquad (\bmod 7) \end{cases} \tag{1}$$

Riducendo i coefficienti e i termini noti nelle due equazioni congruenziali il sistema in (1) si trasforma nel sistema equivalente

$$\circledast : \begin{cases} -3\,x \equiv 3 & (\bmod 15) \\ \ \ 5\,x \equiv -3 & (\bmod 7) \end{cases}$$

che a sua volta, dividendo per 3 coefficiente, termine noto e modulo nella prima equazione, e sommando $28 = 4 \cdot 7$ al termine noto della seconda, si trasforma in

$$\circledast : \begin{cases} -1\,x \equiv 1 & (\bmod 5) \\ \ \ 5\,x \equiv 25 & (\bmod 7) \end{cases}$$

e infine (facile...) in

$$\circledast : \begin{cases} x \equiv 4 & (\bmod 5) \\ x \equiv 5 & (\bmod 7) \end{cases}$$

Quest'ultimo sistema di equazioni congruenziali è "in forma cinese" — cioè le due equazioni, separatamente, sono già risolte — con i due moduli tra loro coprimi; quindi tale sistema ammette soluzioni, che possono essere calcolate tramite il Teorema Cinese del Resto, o anche per sostituzione. In ogni caso, *l'insieme delle soluzioni cercato è* $\big\{\, x \in \mathbb{Z} \;\big|\; x \equiv 19 \; (\,mod\; 35\,) \big\} \;=\; 19 + 35\,\mathbb{Z}$.

[2] — Ricordiamo che una classe $[X]_{20}$ in $\mathbb{Z}_{20}$ è invertibile se e soltanto se si ha M.C.D.$(X, 20) = \pm 1$. Poiché M è divisibile per 2 che è un divisore comune anche a 20, si ha certamente M.C.D.$(M, 20) \neq \pm 1$, e quindi possiamo concludere che in $\mathbb{Z}_{20}$ una classe inversa di $\overline{M}$ *non esiste*. Invece per N osserviamo facilmente che M.C.D.$(N, 20) = 1$ — semplicemente perché i divisori primi di 20, che sono 2 e 5, *non* dividono 750483 e quindi non dividono neanche la potenza $750483^{6455} =: N$; concludiamo allora che *esiste* in $\mathbb{Z}_{20}$ una classe inversa di $\overline{N}$. Tutto ciò risponde alla prima parte del quesito in *(b)*.

Osservando che $\overline{750483} = \overline{3}$ in $\mathbb{Z}_{20}$, che $\varphi(20) = 8$ e che $6455 \equiv 7 \;\; (\bmod 8)$, il Teorema di Eulero ci permette di calcolare

$$\overline{750483^{6455}} \;=\; \overline{750483}^{\,6455} \;=\; \overline{3}^{\,6455} \;=\; \overline{3}^{\,7} \;=\; \overline{3}^{\,4} \cdot \overline{3}^{\,3} \;=\; \overline{81} \cdot \overline{27} \;=\; \overline{1} \cdot \overline{7} \;=\; \overline{7} \qquad (2)$$

dove abbiamo anche sfruttato l'osservazione che $\overline{3}^{\,4} = \overline{3^4} = \overline{81} = \overline{1}$, grazie alla quale troviamo che $\overline{3}^{\,4} = \overline{1}$ e quindi, se anche non conosciamo o non ricordiamo il Teorema di Eulero, possiamo procedere allo stesso modo sostituendo, nella potenza $\overline{3}^{\,6455}$, l'esponente 6455 con il suo resto nella divisione per 4, che è 3.

In particolare la (2) ci dice che $\overline{750483^{6455}} = \overline{7}$ in $\mathbb{Z}_7$, e quindi da questa uguaglianza di classi otteniamo che $750483^{6455} \equiv 7 \pmod{20}$: dato che $0 \leq 7 \lneqq 20$, questo ci permette di concludere che il resto di $N := 750483^{6455}$ nella divisione per 20 è $r = 7$, risolvendo così il quesito in *(a)*.

Sempre dalla (1) otteniamo anche che $\overline{N}^{\,-1} = \overline{7}^{\,-1}$. Inoltre, avendo osservato che

$$\overline{3}^{\,3} = \overline{27} = \overline{7} \qquad \text{e} \qquad \overline{3}^{\,3} \cdot \overline{3} = \overline{3}^{\,4} = \overline{81} = \overline{1}$$

concludiamo che $\overline{N}^{\,-1} = \overline{7}^{\,-1} = \overline{3}$. In alternativa, l'inversa $\overline{N}^{\,-1} = \overline{7}^{\,-1}$ richiesta è la soluzione (unica!) dell'equazione modulare $\overline{7} \cdot \overline{x} = \overline{1}$ in $\mathbb{Z}_{20}$, che equivale alla equazione congruenziale $7\,x \equiv 1 \pmod{20}$ in $\mathbb{Z}$, la quale a sua volta equivale all'equazione diofantea $7\,x + 20\,y = 1$; per quest'ultima, una possibile soluzione è data dalla coppia $(x, y) = (3, -1)$, da cui ricaviamo le soluzioni $x \equiv 3 \pmod{20}$ dell'equazione congruenziale intermedia e la soluzione $\overline{x} = \overline{3}$ dell'equazione modulare di partenza, per cui in conclusione $\overline{N}^{\,-1} = \overline{7}^{\,-1} = \overline{3}$.

In ogni caso, questo completa la risposta al quesito in *(b)*.

[3] — *(a)* Per semplificare la notazione (e magari chiarire le idee...) consideriamo la funzione $f : \mathbb{N} \longrightarrow \{0,1,2\}$ definita da $f(n) := \Big|\big\{\, x \in \{2,5\} \,\big|\, x\,\delta_{\mathbb{N}} n \,\big\}\Big|$. Dalle definizioni segue allora che

$$h \lessdot k \iff f(h) \leq f(k) \qquad\qquad \forall\; h, k \in \mathbb{N}$$

Da questa caratterizzazione della relazione $\lessdot$ segue subito che essa è riflessiva e transitiva, e dunque è un preordine.

(b) La relazione $\lessdot$ *non* è una relazione d'ordine perché *non* è antisimmetrica, in quanto esistono elementi $h, k \in \mathbb{N}$ per i quali si ha $h \lessdot k$ e $k \lessdot h$ *ma* $h \neq k$ (mentre l'antisimmetria imporrebbe che fosse $h = k$). Ad esempio, questo si verifica per $h := 14$ e $k := 15$, per i quali si ha

$$f(14) := \Big|\big\{\, x \in \{2,5\} \,\big|\, x\,\delta_{\mathbb{N}} 14 \,\big\}\Big| = 1 = \Big|\big\{\, y \in \{2,5\} \,\big|\, y\,\delta_{\mathbb{N}} 15 \,\big\}\Big| =: f(15) \qquad (3)$$

(perché $2\,\delta_{\mathbb{N}} 14$, $5\,\not\delta_{\mathbb{N}} 14$, dunque $f(14) = 1$, mentre dall'altra parte abbiamo $2\,\not\delta_{\mathbb{N}} 15$, $5\,\delta_{\mathbb{N}} 15$, così che $f(15) = 1$) per cui la (3) ci dà $14 \lessdot 15$ e $15 \lessdot 14$ con $14 \neq 15$.

(c) Per definizione la relazione $\Leftrightarrow$ è data da

$$m \Leftrightarrow n \qquad \iff \qquad m \lessdot n \quad \& \quad n \lessdot m \qquad\qquad \forall\; m, n \in \mathbb{N}$$

Ma allora dalla caratterizzazione di $\lessdot$ data in (4) otteniamo anche

$$m \Leftrightarrow n \qquad \iff \qquad f(m) \leq f(n) \quad \& \quad f(n) \leq f(m) \qquad \iff \qquad f(m) = f(n)$$

(per ogni $m, n \in \mathbb{N}$) così che $m \Leftrightarrow n \iff f(m) = f(n)$, da cui si vede facilmente che $\Leftrightarrow$ è una relazione di equivalenza (precisamente, è la relazione di equivalenza associata canonicamente alla funzione f).

(d) L'insieme quoziente $\left| \mathbb{N} \big/ \diamond \right|$ ha cardinalità 3, cioè esistono esattamente 3 classi di $\diamond$–equivalenza in $\mathbb{N}$. Precisamente (anche se non è richiesto), tali classi sono

$$C_0 := \big\{ \text{numeri in } \mathbb{N} \text{ che } \textit{non} \text{ siano multipli né di 2 né di 5} \big\} = \mathbb{N} \setminus \big(2\,\mathbb{N} \cup 5\,\mathbb{N} \big)$$
$$C_1 := \big\{ \text{multipli di 2 oppure di 5 ma } \textit{non di entrambi} \big\} = \big(2\,\mathbb{N} \cup 5\,\mathbb{N} \big) \setminus 10\,\mathbb{N}$$
$$C_2 := \big\{ \text{multipli sia di 2 sia di 5 (cioè multipli di 10)} \big\} = 10\,\mathbb{N}$$

Esprimendosi in termini dell'analisi fatta al punto al punto *(c)*, questo risultato si ottiene come segue. Siccome $\diamond$ è l'equivalenza ρ_f associata alla funzione $f : \mathbb{N} \longrightarrow \{0,1,2\}$ lì considerata, abbiamo automaticamente che le classi di $\diamond$–equivalenza sono tutte e sole le controimmagini — secondo f — dei valori assunti dalla funzione f: dato che f assume tutti e tre i possibili valori 0, 1 e 2, concludiamo che esistono esattamente tre classi di $\diamond$–equivalenza, precisamente

$$C_0 := f^{-1}(0) = \big\{ n \in \mathbb{N} \,\big|\, f(n) = 0 \big\} = \big\{ \text{numeri } \textit{non} \text{ multipli né di 2 né di 5} \big\}$$
$$C_1 := f^{-1}(1) = \big\{ n \in \mathbb{N} \,\big|\, f(n) = 1 \big\} = \big\{ \text{multipli di } \textit{uno solo} \text{ tra 2 e 5} \big\}$$
$$C_2 := f^{-1}(1) = \big\{ n \in \mathbb{N} \,\big|\, f(n) = 1 \big\} = \big\{ \text{multipli di } \textit{entrambi} \text{ 2 e 5} \big\}$$

(e) Utilizzando la notazione introdotta in *(d)*, le classi in esame sono

$$[28]_{\diamond} = C_1\ , \quad [15]_{\diamond} = C_1\ , \quad [21]_{\diamond} = C_0\ , \quad [38]_{\diamond} = C_1\ , \quad [30]_{\diamond} = C_2\ .$$

[4] — La tesi da dimostrare è che valga l'identità $\sum_{s=1}^{n} (2\,s-1) = n^2$ per ogni $n \in \mathbb{N}_+$. Vogliamo dimostrarla per 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, il suddetto "valore più piccolo" è $n_0 = 1$, dunque la base dell'induzione consiste nel dimostrare che $(\bigstar) : \sum_{s=1}^{n_0} (2\,s-1) = n_0^2$ per $n_0 := 1$.

Dimostrazione: Nella $(\bigstar)$ il membro di sinistra è

$$\sum_{s=1}^{n_0} (2\,s-1) = \sum_{s=1}^{1} (2\,s-1) = (2 \cdot 1 - 1) = 2 - 1 = 1$$

e quello di destra è $n_0^2 = 1^2 = 1$, quindi l'identità è effettivamente valida.

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, il suddetto passo induttivo assume la forma seguente:
Sia $n \in \mathbb{N}_+$. *SE (Ipotesi Induttiva) si ha* $\sum_{s=1}^{n} (2\,s-1) = n^2$,

ALLORA (Tesi Induttiva) si ha anche $(\otimes) : \sum_{s=1}^{n+1} (2\,s-1) = (n+1)^2$.

<u>*Dimostrazione:*</u> Per cominciare riscriviamo il membro di sinistra della $(\otimes)$ nella forma

$$\sum_{s=1}^{n+1} (2\,s-1) \;=\; \sum_{s=1}^{n} (2\,s-1) \;+\; \big(2\,(n+1)-1\big) \;=\; \sum_{s=1}^{n} (2\,s-1) \;+\; 2\,n+1 \tag{4}$$

e quello di destra nella forma

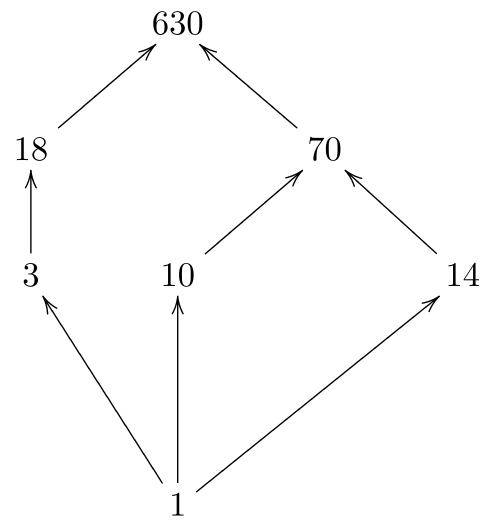
$$(n+1)^2 \;=\; n^2 + 2\,n + 1 \tag{5}$$

Ora, l'*Ipotesi Induttiva* garantisce che $\sum_{s=1}^{n} (2\,s-1) = n^2$, quindi utilizzando questa uguaglianza la (4) si riscrive nella forma

$$\sum_{s=1}^{n+1} (2\,s-1) \;=\; n^2 \;+\; 2\,n+1 \tag{6}$$

e a questo punto confrontando la (6) con la (5) otteniamo proprio la $(\otimes)$, q.e.d.

[5] — Per comodità di visualizzazione disegnamo qui sotto il *diagramma di Hasse* dell'insieme ordinato $\big(\mathbb{T}\,;\delta\big)$, che a priori non è necessario (e infatti non è richiesto...). Tale diagramma è



(a) Ovviamente, in tutti i "casi banali", cioè quelli in cui sia $a\,\delta_{\mathbb{N}}b$ oppure $b\,\delta_{\mathbb{N}}a$, abbiamo che esiste $\sup\big(\{a,b\}\big) = b$ e $\inf\big(\{a,b\}\big) = a$ se $a\,\delta_{\mathbb{N}}b$ mentre invece $\sup\big(\{a,b\}\big) \;=\; a$ e $\inf\big(\{a,b\}\big) \;=\; b$ se $b\,\delta_{\mathbb{N}}a$. Per tutti gli altri casi *non banali* possibili, direttamente dall'analisi del diagramma di Hasse vediamo che esistono

sempre $\sup\big(\{a,b\}\big)$ e $\inf\big(\{a,b\}\big)$, dati esplicitamente da

$$\sup\big(\{\,3\,,10\,\}\big) \;=\; 630 \quad , \quad \sup\big(\{\,10\,,14\,\}\big) \;=\; 70 \quad , \quad \sup\big(\{\,3\,,14\,\}\big) \;=\; 630$$
$$\sup\big(\{\,3\,,70\,\}\big) \;=\; 630 \quad , \quad \sup\big(\{\,18\,,10\,\}\big) \;=\; 630$$
$$\sup\big(\{\,18\,,14\,\}\big) \;=\; 630 \quad , \quad \sup\big(\{\,18\,,70\,\}\big) \;=\; 630$$
$$\inf\big(\{\,3\,,10\,\}\big) \;=\; 1 \quad , \quad \inf\big(\{\,10\,,14\,\}\big) \;=\; 1 \quad , \quad \inf\big(\{\,3\,,14\,\}\big) \;=\; 1$$
$$\inf\big(\{\,3\,,70\,\}\big) \;=\; 1 \quad , \quad \inf\big(\{\,18\,,10\,\}\big) \;=\; 1$$
$$\inf\big(\{\,18\,,14\,\}\big) \;=\; 1 \quad , \quad \inf\big(\{\,18\,,70\,\}\big) \;=\; 1$$

Così concludiamo che l'insieme ordinato $\big(\,\mathbb{T}\,;\delta\,\big)$ è effettivamente un reticolo.

NOTA: È opportuno sottolineare che, in generale, a priori *non possiamo sapere se* $\sup\big(\{a,b\}\big) = \mathrm{m.c.m.}(a,b)$ né se $\inf\big(\{a,b\}\big) = \mathrm{M.C.D.}(a,b)$, sebbene la relazione d'ordine sia la divisibilità! Di fatto, dalla tavola qui sopra possiamo osservare che in molti casi si ha $\sup\big(\{a,b\}\big) \neq \mathrm{m.c.m.}(a,b)$ e/o $\inf\big(\{a,b\}\big) \neq \mathrm{M.C.D.}(a,b)$. Questa apparente "anomalia" si verifica proprio perché si tratta di casi di elementi $a,b \in \mathbb{T}$ per i quali $\mathrm{m.c.m.}(a,b) \notin \mathbb{T}$ e/o $\mathrm{M.C.D.}(a,b) \notin \mathbb{T}$.

(b) Il minimo del reticolo $\mathbb{T}$ è 1, e il massimo è 630. Gli *atomi*, per definizione, sono gli elementi che coprono il minimo, quindi in questo caso sono 3, 10, 14. Tutti questi atomi sono ovviamente $\vee$–*irriducibili*; in aggiunta, gli unici altri elementi $\vee$–irriducibili sono quello "banale", cioè il minimo 1, e anche 18. Riassumendo,

$$\min(\,\mathbb{T}\,) \;=\; 1 \quad , \quad \max(\,\mathbb{T}\,) \;=\; 630$$
$$\big\{\textit{atomi di }\mathbb{T}\,\big\} \;=\; \big\{3\,,10\,,14\big\} \quad , \quad \big\{\vee\text{–}\textit{irriducibili di }\mathbb{T}\,\big\} \;=\; \big\{1\,,3\,,10\,,14\,,18\big\}$$

(c) Siccome il reticolo $\mathbb{T}$ è finito, sicuramente esiste (almeno) una $\vee$–fattorizzazione (non ridondante) in $\vee$–irriducibili per ogni suo elemento, quindi anche per 630. Analizzando direttamente il diagramma di Hasse, troviamo che *tutte le possibili* $\vee$*–fattorizzazioni non ridondanti in* $\vee$*–irriducibili per questo elemento sono date da*

$$630 \;=\; 18 \vee 10 \vee 14 \quad , \quad 630 \;=\; 3 \vee 10 \vee 14$$
$$630 \;=\; 18 \vee 10 \quad , \quad 630 \;=\; 18 \vee 14$$
$$630 \;=\; 3 \vee 10 \quad , \quad 630 \;=\; 3 \vee 14$$

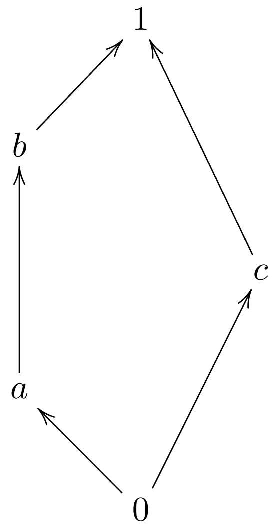
(d) A priori, una $\vee$–fattorizzazione (non ridondante) in *atomi* di 630 potrebbe esistere oppure no, diversamente da quanto possiamo dire per una fattorizzazione in $\vee$–irriducibili; in ogni caso, dato che ogni atomo è sempre $\vee$–irriducibile, un'eventuale $\vee$–fattorizzazione (non ridondante) in atomi sarebbe una particolare $\vee$–fattorizzazione (non ridondante) in $\vee$–irriducibili, che abbiamo trattato nel precedente punto *(c)*. Così analizzando quanto già trovato al punto *(c)* osserviamo che tra le sei $\vee$–fattorizzazioni (non ridondanti) in $\vee$–irriducibili di 630 lì elencate troviamo che *esistono esattamente tre* $\vee$*–fattorizzazioni non ridondanti di* 630 *in atomi, date da*

$$630 \;=\; 3 \vee 10 \vee 14 \quad , \quad 630 \;=\; 3 \vee 10 \quad , \quad 630 \;=\; 3 \vee 14$$

(e) L'insieme $\mathbb{T}$ è finito, con esattamente 7 elementi. Ora, come conseguenza del *Teorema di Rappresentazione di Stone* è noto 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 $|\mathbb{T}| = 7$ *non è una potenza di 2*, possiamo concludere che $\big(\mathbb{T}\,;\delta\big)$ *non è un'algebra di Boole.* In particolare si osservi che con questo metodo non c'è neanche bisogno di analizzare come sia fatta la relazione d'ordine fissata in $\mathbb{T}$: qualunque essa sia, la conclusione sarà sempre la stessa, perché dipende esclusivamente da una proprietà insiemistica di $\mathbb{T}$ stesso.

In alternativa, possiamo procedere tramite un'analisi diretta delle proprietà di reticolo di $\big(\mathbb{T}\,;\delta\big)$, come segue.

Ricordiamo che, per definizione, un reticolo è detto *algebra di Boole* se e soltanto se è limitato, distributivo e complementato. Ora, il reticolo $\mathbb{T}$ è limitato, con minimo 1 e massimo 630. D'altronde, dall'analisi del diagramma di Hasse deduciamo che *il reticolo* $\big(\mathbb{T}\,;\delta\big)$ *non è distributivo.* Infatti, ricordiamo che *un reticolo è distributivo se e soltanto se non contiene nessun sottoreticolo che sia isomorfo al reticolo* $\mathfrak{N}_5$, dove il reticolo indicato con $\mathfrak{N}_5$ è quello rappresentato dal diagramma di Hasse



Ora, il reticolo $\big(\mathbb{T}\,;\delta\big)$ contiene ben *sette* sottoreticoli isomorfi al reticolo $\mathfrak{N}_5$, precisamente

quattro di tipo $\mathbb{E}'_{x,y} := \big\{1\,, x\,, 70\,, y\,, 630\big\} \qquad \forall\, x \in \big\{10\,,14\big\},\ y \in \big\{3\,,18\big\}$
con l'isomorfismo $\mathbb{E}'_{x,y} \lhook\joinrel\twoheadrightarrow \mathfrak{N}_5\,, \quad 1 \mapsto 0\,,\ x \mapsto a\,,\ 70 \mapsto b\,,\ y \mapsto c\,,\ 630 \mapsto 1$
tre di tipo $\mathbb{E}''_{z} := \big\{1\,, z\,, 3\,, 18\,, 630\big\} \qquad \forall \;\; z \in \big\{10\,,14\,,70\big\}$
con l'isomorfismo $\mathbb{E}''_{z} \lhook\joinrel\twoheadrightarrow \mathfrak{N}_5\,, \quad 1 \mapsto 0\,,\ 3 \mapsto a\,,\ 18 \mapsto b\,,\ z \mapsto c\,,\ 630 \mapsto 1$

per cui possiamo concludere che il reticolo $\big(\mathbb{T}\,;\delta\big)$ non è distributivo.

Da un altro punto di vista, osserviamo che $\big(\mathbb{T}\,;\delta\big)$ è *complementato*, poiché ogni elemento ha un complemento. D'altra parte, ci sono casi in cui tale complemento non è unico; precisamente, la situazione è la seguente:

1 ha come complemento (unico) 630

3 ha come complementi 10 , 14 e 70

18 ha come complementi 10 , 14 e 70

10 ha come complementi 3 e 18

14 ha come complementi 3 e 18

70 ha come complementi 3 e 18

630 ha come complemento (unico) 1

Ma da questo ricaviamo di nuovo che il reticolo non è distributivo, perché in qualsiasi reticolo distributivo il complemento di un elemento, se esiste, è sempre unico, mentre in questo caso esiste sempre ma è unico soltanto nei casi di 630 e di 1 (com'è ovvio, perché questi sono il massimo e il minimo del reticolo), e non invece per gli altri cinque elementi.