**MATEMATICA DISCRETA**
**CdL in Informatica — a.a. 2017/2018**

*prof. Fabio GAVARINI*

Test scritto del 20 Dicembre 2017 — *Testo e Svolgimento*

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

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

. . . * . . .

**[1]** Calcolare tutte le soluzioni in $\mathbb{Z}$ del sistema di equazioni congruenziali

$$\circledast : \begin{cases} 17\,x \equiv -105 \pmod 5 \\ -55\,x \equiv 11 \pmod 3 \\ 23\,x \equiv 36 \pmod 7 \end{cases}$$

**[2]** Dato l'insieme $\mathbb{E} := \{0\,,1\,,2\,,3\,,4\,,5\,,6\,,7\,,8\,,9\,,\heartsuit,\spadesuit,\clubsuit,\diamondsuit\}$, determinare:

*(a)* una partizione $\pi'$ di $\mathbb{E}$ in cinque blocchi che abbiano cardinalità 5, 3, 3, 2, 1;

*(b)* una partizione $\pi''$ di $\mathbb{E}$ in quattro blocchi che abbiano cardinalità 7, 5, 1, 1.

**[3]** Si consideri l'insieme delle parti $\mathcal{P}\big(\{C,O,R,N,A\}\big)$ e in esso il sottoinsieme

$$\mathcal{E} := \big\{\{O\},\{C\},\{O,R\},\{O,N\},\{C,O,R\},\{O,R,N\},\{C,O,N\},\{C,N,A\},\{C,O,N,A\}\big\}$$

Nel suddetto insieme $\mathcal{E}$ consideriamo la relazione di inclusione $\subseteq$, rispetto alla quale abbiamo che $\big(\mathcal{E}\,;\subseteq\big)$ è un insieme ordinato.

*(a)* Disegnare il *diagramma di Hasse* dell'insieme ordinato $\big(\mathcal{E}\,;\subseteq\big)$.

*(b)* Esiste $\max(\mathcal{E})$? Se sì, precisare quale sia tale massimo; se no, spiegare il perché.

*(c)* Esistono elementi *minimali* in $\big(\mathcal{E}\,;\subseteq\big)$? Se sì, precisare quali siano; se no, spiegare perché non esistano.

*(d)* Esiste $\inf\big(\{C,O,N\},\{C,N,A\}\big)$? Se sì, precisare quale sia tale estremo inferiore; se no, spiegare perché non esista.

*(e)* Esiste $\inf\big(\{C,N,A\},\{O,R,N\}\big)$? Se sì, precisare quale sia tale estremo inferiore; se no, spiegare perché non esista.

*(f)* Esiste $\sup\big(\{C\},\{O\}\big)$? Se sì, precisare quale sia tale estremo inferiore; se no, spiegare perché non esista.

*(continua $\Longrightarrow$)*

**[4]** Dimostrare per induzione debole su $n \in \mathbb{N}$ che per ogni $n \in \mathbb{N}$ il numero naturale $A(n) := 3^{2n+1} + 2^{n+2}$ è un multiplo di 7 (in $\mathbb{N}$).

**[5]** *(a)* Determinare se esistano le classi inverse $\overline{9}^{\,-1}$, $\overline{5}^{\,-1}$, $\overline{7}^{\,-1}$, $\big(\overline{9}\cdot\overline{7}\big)^{-1}$ e $\big(\overline{5}\cdot\overline{7}\big)^{-1}$ nell'anello $\mathbb{Z}_{20}$ degli interi modulo 20. In caso negativo, si spieghi perché tale classe inversa non esista; in caso affermativo, si calcoli esplicitamente la suddetta classe inversa.

*(b)* Calcolare tutte le soluzioni dell'equazione modulare $\overline{647}\,\overline{x} = \overline{-516}$ in $\mathbb{Z}_{20}$.

*(c)* Calcolare tutte le soluzioni dell'equazione congruenziale $436\,x \equiv 92 \pmod{20}$ in $\mathbb{Z}$.

**[6]** Sia dato un insieme $A$ e due suoi sottoinsiemi $B, C \,(\subseteq A)$. Si consideri la funzione

$$f : \mathcal{P}(B) \longrightarrow \mathcal{P}\big(B \setminus C\big)\,, \quad D \mapsto f(D) := D \setminus C \qquad\qquad \forall\ D \in \mathcal{P}(B)$$

Dimostrare che:

*(a)* la funzione f è suriettiva;

*(b)* la funzione f è iniettiva $\iff$ $B \cap C = \emptyset$.

**[7]** *(a)* Sia $n$ il numero naturale che in base dieci è espresso dalla notazione posizionale $n := (9873)_{\text{DIECI}}$. Scrivere $n$ in base $b' :=$ OTTO e in base $b'' :=$ SETTE.

*(b)* Scrivere in base $b' :=$ DIECI il numero $S$ che in base $b :=$ CINQUE è espresso dalla scrittura posizionale $S := \big(41032\big)_b$.

*(c)* Scrivere in base $b' :=$ QUATTRO e in base $b'' :=$ DUE il numero $L$ che in base $b :=$ OTTO è espresso dalla scrittura posizionale $L := \big(3471\big)_b$.

*(d)* Utilizzando la notazione posizionale in base $\beta :=$ TRE, calcolare la somma $N + M$ dove $N$ ed $M$ sono i due numeri naturali espressi in base $\beta$ da

$$N := \big(12021\big)_\beta \qquad \text{e} \qquad M := \big(20102\big)_\beta$$

esprimendo a sua volta la suddetta somma con la scrittura posizionale in base $\beta :=$ TRE e con la scrittura posizionale in base $\beta' :=$ DIECI.

**[8]** Per ogni $\ell \in \mathbb{N}_+$, sia $\psi(\ell) := \big\{\, p \in \mathbb{N}_+ \,\big|\, p \text{ è primo}, p \text{ divide } \ell \,\big\}$. Sia $\lhd$ la relazione in $\mathbb{N}_+$ definita così: $\ell_1 \lhd \ell_2 \iff \psi\big(\ell_1\big) \subseteq \psi\big(\ell_2\big)$, per ogni $\ell_1, \ell_2 \in \mathbb{N}_+$. Dimostrare che:

*(a)* la relazione $\lhd$ è riflessiva e transitiva;

*(b)* la relazione $\lhd$ non è antisimmetrica;

*(c)* esiste un $\ell_\downarrow \in \mathbb{N}_+$ tale che $\ell_\downarrow \lhd \ell$ per ogni $\ell \in \mathbb{N}_+$;

*(d)* non esiste un $\ell^\uparrow \in \mathbb{N}_+$ tale che $\ell \lhd \ell^\uparrow$ per ogni $\ell \in \mathbb{N}_+$;

*(e)* la relazione $\asymp$ in $\mathbb{N}_+$ definita da $\ell_1 \asymp \ell_2 \iff \big(\ell_1 \lhd \ell_2\big) \wedge \big(\ell_2 \lhd \ell_1\big)$ è un'equivalenza.

*( continua $\Longrightarrow$ )*

**[9]** Calcolare il resto nella divisione per 20 dei tre numeri

$$a := 457^{35062867} \quad , \qquad b := 2384^{16} \quad , \qquad c := 645^{5607290843}$$

**[10]** Siano $\{E'_i\}_{i\in I}$ e $\{E''_j\}_{j\in J}$ due partizioni dell'insieme non vuoto $E$. Posto $K := \{(i,j) \in I \times J \,|\, E'_i \cap E''_j \neq \emptyset\}$, si dimostri che anche $\{E'_i \cap E''_j\}_{(i,j)\in K}$ è partizione di $E$.

— ⋆ —

SVOLGIMENTO

**[1]** — Per prima cosa, in ciascuna equazione modulare nel sistema in esame, ogni numero può essere sostituito con un altro ad esso congruente (modulo il numero che fa da modulo nella specifica equazione in esame). Procedendo in questo modo, e osservando che

$$\begin{array}{rcrcl} 17 \equiv 2 & \pmod 5 & , & -105 \equiv 0 & \pmod 5 \\ -55 \equiv -1 & \pmod 3 & , & 11 \equiv -1 & \pmod 3 \\ 23 \equiv 2 & \pmod 7 & , & 36 \equiv 1 & \pmod 7 \end{array}$$

il nostro sistema si trasforma così

$$\circledast : \begin{cases} 17\,x \;\equiv\; -105 \pmod 5 \\ -55\,x \;\equiv\; 11 \pmod 3 \\ 23\,x \;\equiv\; 36 \pmod 7 \end{cases} \iff \begin{cases} 2\,x \;\equiv\; 0 \pmod 5 \\ -x \;\equiv\; -1 \pmod 3 \\ 2\,x \;\equiv\; 1 \pmod 7 \end{cases}$$

e l'ultimo sistema a sua volta è equivalente a

$$\odot : \begin{cases} x \;\equiv\; 0 \pmod 5 \\ x \;\equiv\; 1 \pmod 3 \\ x \;\equiv\; 4 \pmod 7 \end{cases} \tag{1}$$

In particolare, l'ultima equazione congruenziale del secondo sistema ha effettivamente come soluzione $x \equiv 4 \pmod 7$; infatti, una soluzione particolare è $x_0 = 4$ dato che abbiamo $2\cdot 4 = 8 \equiv 1 \pmod 7$, e tutte le altre soluzioni sono della forma $x = x_0 + 7\cdot z$ $(\forall\, z \in \mathbb{Z})$ in quanto M.C.D.$(2,7) = 1$, dunque $x \equiv x_0 = 4 \pmod 7$.

Per trovare una soluzione particolare dell'equazione congruenziale

$$2\,x \;\equiv\; 1 \pmod 7 \tag{2}$$

— se non si trova ad occhio la soluzione $x_0 = 4$ — si può procedere mediante la risoluzione dell'equazione diofantea associata

$$2\,x + 7\,y \;=\; 1 \tag{3}$$

la quale ammette certamente soluzioni, perché il M.C.D. tra i due coefficienti delle incognite (che sono 2 e 7) è 1, e pertanto divide il termine noto 1. Ciò premesso, una soluzione della (3) corrisponde ad una identità di Bézout per il suddetto $\text{M.C.D.}(2,7) = 1$, che possiamo trovare tramite l'algoritmo euclideo delle divisioni successive. In dettaglio, tale algoritmo si sviluppa come segue:

$$\begin{aligned} 2 \;&=\; 7\cdot 0 + 2 \quad &\Longrightarrow \quad 2 \;&=\; 2 + 7\cdot(-0) \\ 7 \;&=\; 2\cdot 3 + 1 \quad &\Longrightarrow \quad 1 \;&=\; 7 + 2\cdot(-3) \\ 2 \;&=\; 1\cdot 2 + 0 \quad &\Longrightarrow \quad &\text{STOP!} \end{aligned}$$

e così per sostituzioni succcessive (molto pignole) troviamo

$$1 \;=\; 7 + 2\cdot(-3) \;=\; 7 + \big(2 + 7\cdot(-0)\big)\cdot(-3) \;=\; 2\cdot(-3) + 7\cdot\big(1 + (-0)(-3)\big) \;=\; 2\cdot\underline{(-3)} + 7\cdot\underline{1}$$

che ci dice che la coppia $\big(x_0' \,, y_0'\big) := (-3\,, 1)$ è soluzione dell'equazione diofantea in (3). Da questo segue che la prima componente di tale coppia, cioè $x_0' = -3$, è soluzione dell'equazione congruenziale in (2). Si noti che questa *non* è la soluzione particolare $x_0 = 4$ considerata in precedenza! Tuttavia, se utilizziamo questa nuova soluzione particolare per descrivere l'insieme di tutte le soluzioni dell'equazione congruenziale (2), troviamo che queste sono date da $x \equiv x_0' = -3 \pmod 7$, cioè dalla classe di congruenza di $x_0' = -3$ modulo 7; ma siccome $x_0' = -3 \equiv 4 = x_0 \pmod 7$, l'insieme di soluzioni così individuato è lo stesso nei due casi, cioè sia che si parta da $x_0 = 4$ sia che si parta da $x_0' = -3$, perché la classe di congruenza (modulo 7) individuata è la stessa.

Resta ora da risolvere il sistema $\odot$ in (1), equivalente a quello iniziale per cui l'insieme delle soluzioni sarà lo stesso per l'uno e per l'altro sistema. A tal fine, possiamo adottare due diversi metodi:

*Primo metodo: Risoluzione per Sostituzioni Successive:* Risolviamo la prima equazione congruenziale in (1) — che in realtà è già risolta... — e sostituiamo i valori trovati nella seconda e nella terza: questo dà un nuovo sottosistema di due equazioni congruenziali, che risolviamo a sua volta; iterando il procedimento, dopo un numero finito di passi troviamo il risultato finale. In dettaglio si ha:

$$\odot : \begin{cases} x \equiv 0 \pmod 5 \\ x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 7 \end{cases} \Longrightarrow \begin{cases} x = 5h \quad (h \in \mathbb{Z}) \\ 5h \equiv 1 \pmod 3 \\ 5h \equiv 4 \pmod 7 \end{cases} \Longrightarrow \begin{cases} x = 5h \quad (h \in \mathbb{Z}) \\ h \equiv 2 \pmod 3 \\ 5h \equiv 4 \pmod 7 \end{cases} \Longrightarrow$$

$$\Longrightarrow \begin{cases} x = 5h \quad (h \in \mathbb{Z}) \\ h = 2 + 3k \quad (k \in \mathbb{Z}) \\ 5(2 + 3k) \equiv 4 \pmod 7 \end{cases} \Longrightarrow \begin{cases} x = 5h \quad (h \in \mathbb{Z}) \\ h = 2 + 3k \quad (k \in \mathbb{Z}) \\ 15k \equiv -6 \pmod 7 \end{cases} \Longrightarrow$$

$$\Longrightarrow \begin{cases} x = 5h \quad (h \in \mathbb{Z}) \\ h = 2 + 3k \quad (k \in \mathbb{Z}) \\ k \equiv 1 \pmod 7 \end{cases} \Longrightarrow \begin{cases} x = 5h \quad (h \in \mathbb{Z}) \\ h = 2 + 3k \quad (k \in \mathbb{Z}) \\ k = 1 + 7z \quad (z \in \mathbb{Z}) \end{cases}$$

da cui in definitiva ricaviamo

$$x \,=\, 5\,h \,=\, 5\,(2+3\,k) \,=\, 10+15\,k \,=\, 10+15\,(1+7\,z) \,=\, 25+105\,z \qquad \forall\ z\in\mathbb{Z}$$

cioè $x \,=\, 25+105\,z\ \big(\forall\ z\in\mathbb{Z}\big)$ oppure — descrivendo lo stesso insieme di soluzioni in un altro modo — $x \,\equiv\, 25\ \big(\mathrm{mod}\ 105\big)$ . In altre parole, l'insieme di tutte le soluzioni del sistema $\odot$ in (1) — e quindi del sistema originale $\circledast$ — è il sottoinsieme di $\mathbb{Z}$ costituito dall'intera classe di congruenza $[25]_{\equiv_{105}}$ .

*Secondo metodo: Applicazione del Teorema Cinese del Resto:* Il sistema (1) è del tipo *in forma cinese*, cioè in cui le singole equazioni congruenziali sono già (separatamente) risolte e i diversi moduli (delle varie equazioni congruenziali: in questo caso 5, 3 e 7) sono a due a due coprimi. In tal caso, l'insieme di tutte le soluzioni del sistema si ottiene sommando multipli interi del prodotto di tutti i moduli del sistema — nel nostro caso, il prodotto $R := r_1\,r_2\,r_3 = 5\cdot 3\cdot 7 = 105$ — ad una soluzione particolare $x_0$ del sistema. In sintesi, il suddetto insieme delle soluzioni è

$$\mathcal{S} \,:=\, \big\{\, x = x_0 + R\,z \;\big|\; z\in\mathbb{Z}\,\big\} \,=\, [x_0]_{\equiv_R} \tag{4}$$

cioè l'intera classe di congruenza modulo $R$ della soluzione particolare $x_0$ .

Per calcolare una soluzione particolare $x_0$ del sistema in (1), procediamo come segue. Siano $R := r_1\,r_2\,r_3 = 5\cdot 3\cdot 7 = 105$ , $R_1 := r_2\,r_3 = 3\cdot 7 = 21$ , $R_2 := r_1\,r_3 = 5\cdot 7 = 35$ , e $R_3 := r_1\,r_2 = 5\cdot 3 = 15$ . Consideriamo le tre equazioni congruenziali (nelle tre incognite $x_1$ , $x_2$ e $x_3$ ) che si ottengono da quelle che figurano in $\odot$ moltiplicando l'incognita rispettivamente per $R_1$ , $R_2$ e $R_3$ : esplicitamente queste sono

$$R_1\,x_1 \,\equiv\, 0 \ \ \big(\mathrm{mod}\ 5\big) \quad , \qquad R_2\,x_2 \,\equiv\, 1 \ \ \big(\mathrm{mod}\ 3\big) \quad , \qquad R_3\,x_3 \,\equiv\, 4 \ \ \big(\mathrm{mod}\ 7\big)$$

cioè

$$21\,x_1 \,\equiv\, 0 \ \ \big(\mathrm{mod}\ 5\big) \quad , \qquad 35\,x_2 \,\equiv\, 1 \ \ \big(\mathrm{mod}\ 3\big) \quad , \qquad 15\,x_3 \,\equiv\, 4 \ \ \big(\mathrm{mod}\ 7\big) \tag{5}$$

In ciascuna di queste semplifichiamo i coefficienti sostituendoli con altri numeri ad essi congruenti (modulo 5 nel primo caso, modulo 3 nel secondo e modulo 7 nel terzo) e più semplici: otteniamo così

$$1\,x_1 \,\equiv\, 0 \ \ \big(\mathrm{mod}\ 5\big) \quad , \qquad -1\,x_2 \,\equiv\, 1 \ \ \big(\mathrm{mod}\ 3\big) \quad , \qquad 1\,x_3 \,\equiv\, 4 \ \ \big(\mathrm{mod}\ 7\big)$$

da cui otteniamo

$$x_1 \,\equiv\, 0 \ \ \big(\mathrm{mod}\ 5\big) \quad , \qquad x_2 \,\equiv\, -1 \ \ \big(\mathrm{mod}\ 3\big) \quad , \qquad x_3 \,\equiv\, 4 \ \ \big(\mathrm{mod}\ 7\big)$$

Ne segue che una soluzione della prima, della seconda o della terza equazione è data rispettivamente da

$$x'_1 \,=\, 0 \quad , \qquad x'_2 \,=\, -1 \quad , \qquad x'_3 \,=\, 4 \quad . \tag{6}$$

A partire dalle soluzioni particolari in (6) delle equazioni congruenziali in (5) costruiamo una soluzione particolare $x_0$ del sistema $\odot$ in (1) mediante la formula

$$x_0 \,:=\, R_1\,x'_1 + R_2\,x'_2 + R_3\,x'_3$$

la quale esplicitamente ci dà

$$x_0 \,:=\, R_1\, x'_1 + R_2\, x'_2 + R_3\, x'_3 \,=\, 21\,0 + 35\,(-1) + 15\,4 \,=\, 0 - 35 + 60 \,=\, 25$$

cioè $x_0 = 25$ che è la soluzione particolare già trovata col primo metodo (per sostituzioni successive). Da questo e da (4) troviamo l'insieme di tutte le soluzioni del sistema in esame, precisamente

$$\mathcal{S} \,:=\, \big\{\, x = 25 + 105\, z \;\big|\; z \in \mathbb{Z} \,\big\} \,=\, [25]_{\equiv_{105}}$$

come già trovato col primo metodo.

<u>*Attenzione*</u>: si noti che le cose possono andare in modo diverso (ma equivalente!), nei passi intermedi. Ad esempio, nella (6) possiamo considerare le soluzioni

$$x''_1 \,=\, 5 \quad , \qquad x''_2 \,=\, 2 \quad , \qquad x'_3 \,=\, 4 \quad . \tag{$6_+$}$$

e quindi a partire da queste passiamo a costruire la soluzione particolare

$$x''_0 \,:=\, R_1\, x''_1 + R_2\, x''_2 + R_3\, x''_3 \,=\, 21 \cdot 5 + 35 \cdot 2 + 15 \cdot 4 \,=\, 105 + 70 + 60 \,=\, 235$$

cioè $x''_0 = 235$. Da questa soluzione particolare e dalla (4) segue che l'insieme di tutte le soluzioni del sistema in esame è

$$\mathcal{S}'' \,:=\, \big\{\, x = 235 + 105\, z \;\big|\; z \in \mathbb{Z} \,\big\} \,=\, [235]_{\equiv_{105}}$$

che è *lo stesso insieme già trovato in precedenza* in quanto $[235]_{\equiv_{105}} = [25]_{\equiv_{105}}$, poiché si ha $235 \equiv 25 \,\big(\mathrm{mod}\ 105\big)$ dato che $235 - 25 = 210 = 105 \cdot 2$ .

**[2]** — Ricordiamo che una partizione di un insieme è una *famiglia di sottoinsiemi* dell'insieme dato (detti "blocchi" della partizione) che siano *non vuoti*, a due a due *disgiunti o coincidenti*, e tali che *la loro unione sia tutto l'insieme di partenza*.

*(a)* Un esempio di partizione dell'insieme $\mathbb{E}$ in cinque blocchi di cardinalità rispettivamente 5, 3, 3, 2, 1 è dato da $\pi' := \big\{\mathbb{E}'_i\big\}_{i\in\{1,2,3,4,5\}}$ con blocchi

$$\mathbb{E}'_1 := \{0,1,2,3,4\}\ , \quad \mathbb{E}'_2 := \{5,6,7\}\ , \quad \mathbb{E}'_3 := \{8,9,\heartsuit\}\ , \quad \mathbb{E}'_4 := \{\spadesuit,\clubsuit\}\ , \quad \mathbb{E}'_5 := \{\diamondsuit\}$$

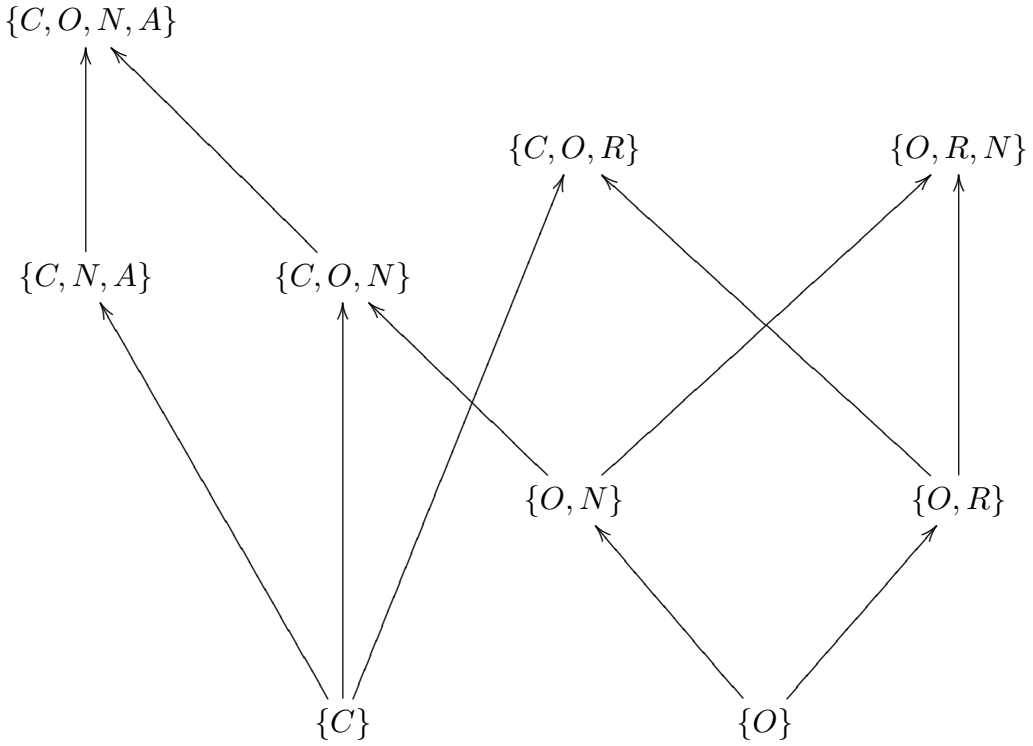
(ovviamente esistono molti altri esempi).

*(b)* Un esempio di partizione dell'insieme $\mathbb{E}$ in quattro blocchi di cardinalità rispettivamente 7, 5, 1, 1 è dato da $\pi'' := \big\{\mathbb{E}''_i\big\}_{i\in\{1,2,3,4\}}$ con blocchi

$$\mathbb{E}''_1 := \{0,1,2,3,4,5,6\}\ , \quad \mathbb{E}''_2 := \{7,8,9,\heartsuit,\spadesuit\}\ , \quad \mathbb{E}''_3 := \{\clubsuit\}\ , \quad \mathbb{E}''_4 := \{\diamondsuit\}$$

(ovviamente esistono molti altri esempi).

**[3]** — *(a)* Il *diagramma di Hasse* dell'insieme ordinato $\big(\mathcal{E}\,;\subseteq\big)$ è il seguente:




*N.B.:* ovviamente, lo stesso diagramma può essere disegnato anche in modi diversi...

*(b)* Direttamente dall'analisi del diagramma di Hasse vediamo che nell'insieme ordinato $\big(\mathcal{E}\,;\subseteq\big)$ esistono *tre* diversi elementi massimali — cioè tali che non siano inclusi strettamente in nessun elemento di $\mathcal{E}$ — che sono $\{C,O,N,A\}$ , $\{C,O,R\}$ , $\{O,R,N\}$ ; ne segue pertanto che *non esiste invece* $\max(\mathcal{E})$ .

*(c)* Direttamente dall'analisi del diagramma di Hasse vediamo che nell'insieme ordinato $\big(\mathcal{E}\,;\subseteq\big)$ esistono due diversi *elementi minimali*, precisamente $\{C\}$ e $\{O\}$ : infatti per entrambi gli elementi non esiste nessun elemento in $\mathcal{E}$ che sia strettamente incluso in nessuno di essi, e questi sono gli unici elementi per cui valga tale proprietà — *N.B.:* come conseguenza, dall'esistenza di *due* diversi elementi minimali segue anche che *non esiste* $\min(\mathcal{E})$ .

*(d)* Ricordiamo che l'elemento $\inf\big(\{C,O,N\},\{C,N,A\}\big)$ , se esiste, è il massimo dei minoranti dell'insieme $\big\{\{C,O,N\},\{C,N,A\}\big\}$ . Ora, l'insieme dei minoranti di $\{C,O,N\}$ è $\mathrm{minor}\big(\{C,O,N\}\big) = \big\{\{C,O,N\},\{C\},\{O,N\},\{O\}\}\big\}$ , e l'insieme dei minoranti di $\{C,N,A\}$ è $\mathrm{minor}\big(\{C,N,A\}\big) = \big\{\{C,N,A\},\{C\}\big\}$ : quindi l'insieme che stiamo cercando dei minoranti di $\big\{\{C,O,N\},\{C,N,A\}\big\}$ è

$$\mathrm{minor}\big(\big\{\{C,O,N\},\{C,N,A\}\big\}\big) \;=\; \mathrm{minor}\big(\{C,O,N\}\big)\bigcap \mathrm{minor}\big(\{C,N,A\}\big) \;=$$
$$= \big\{\{C,O,N\},\{C\},\{O,N\},\{O\}\}\big\}\bigcap\big\{\{C,N,A\},\{C\}\big\} \;=\; \big\{\{C\}\big\}$$

e in particolare ha minimo, pari a $\{C\}$ . In definitiva otteniamo

$$\exists \quad \inf\big(\{C,O,N\},\{C,N,A\}\big) \;=\; \mathrm{minor}\big(\big\{\{C,O,N\},\{C,N,A\}\big\}\big) \;=$$
$$= \min\big(\big\{\{C\}\big\}\big) \;=\; \{C\}$$

cioè *esiste* $\inf\big(\{C,O,N\},\{C,N,A\}\big) = \{C\}$ .

*(e)* L'insieme $\text{minor}\big(\big\{\{C,N,A\},\{O,R,N\}\big\}\big)$ formato da tutti i minoranti dell'insieme $\big\{\{C,N,A\},\{O,R,N\}\big\}$ è vuoto — perché non ci sono elementi *dell'insieme* $\mathcal{E}$ che siano simultaneamente contenuti in $\{C,N,A\}$ e in $\{O,R,N\}$ — *N.B.:* questo è dovuto al fatto che il sottoinsieme $\{C,N,A\}\cap\{O,R,N\}=\{N\}$ e l'insieme vuoto $\emptyset$ *non sono elementi di* $\mathcal{E}$ . Pertanto l'insieme $\text{minor}\big(\big\{\{C,N,A\},\{O,R,N\}\big\}\big)$ , essendo vuoto, non ha massimo, e quindi non esiste $\max\big(\text{minor}\big(\big\{\{C,N,A\},\{O,R,N\}\big\}\big)\big)$ , cioè *non esiste* $\inf\big(\big\{\{C,N,A\},\{O,R,N\}\big\}\big)$ .

*(f)* Ricordiamo che l'estremo superiore $\sup(X)$ di un sottoinsieme $X$ in un insieme ordinato $E$ è, *se esiste*, il minimo dell'insieme $\text{maggior}(X)$ dei maggioranti di $X$ . Ora, l'insieme dei maggioranti di $\{C\}$ è

$$\text{maggior}\big(\{C\}\big) \;=\; \big\{\{C\},\{C,N,A\},\{C,O,N\},\{C,O,R\},\{C,O,N,A\}\big\}$$

e l'insieme dei maggioranti di $\{O\}$ è

$$\text{maggior}\big(\{O\}\big) \;=\; \big\{\{O\},\{O,N\},\{O,R\},\{C,O,N\},\{C,O,R\},\{O,R,N\},\{C,O,N,A\}\big\}$$

Quindi l'insieme $\text{maggior}\big(\big\{\{C\},\{O\}\big\}\big)$ dei maggioranti di $\big\{\{C\},\{O\}\big\}$ è

$$\text{maggior}\big(\big\{\{C\},\{O\}\big\}\big) \;=\; \text{maggior}\big(\{C\}\big)\bigcap\text{maggior}\big(\{O\}\big) \;= \\ = \;\big\{\{C,O,N\},\{C,O,R\},\{C,O,N,A\}\big\}$$

e tale sottoinsieme *non ha minimo* (ha invece *due* diversi elementi minimali, precisamente $\{C,O,N\}$ e $\{C,O,R\}$ ). Pertanto, da questa analisi otteniamo in definitiva che non esiste $\min\big(\text{maggior}\big(\big\{\{C\},\{O\}\big\}\big)\big)$ , e quindi *non esiste* $\sup\big(\big\{\{C\},\{O\}\big\}\big)$ .

**[4]** — La tesi da dimostrare è che per ogni $n\in\mathbb{N}$ il numero $A(n):=3^{2\,n+1}+2^{n+2}$ sia divisibile per 7, cioè esista un $k_n\in\mathbb{N}$ tale che $A(n)=7\,k_n$ . Vogliamo dimostrarla per induzione debole, che procede in due passi: *Base dell'Induzione* e *Passo Induttivo*.

Base dell'Induzione: Dobbiamo dimostrare che *"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 $n_0=0$ , dunque la base dell'induzione consiste nel dimostrare che

$$A(0) \text{ è divisibile per } 7, \quad \text{cioè} \qquad \exists\; k_0\in\mathbb{N} \;:\; A(0) \;=\; 7\,k_0$$

Ora, per definizione $A(0):=3^{2\cdot0+1}+2^{0+2}=3^1+2^2=3+4=7=7\cdot1$ , quindi vale effettivamente la (7) con $k_0=1$ .

Passo Induttivo (in forma debole): Dobbiamo dimostrare che *"Per ogni valore utile di n , SE è vera la tesi per n , ALLORA è vero anche la tesi per* $n+1$ *"*.

Nel caso in esame, il suddetto passo induttivo assume la forma seguente:

*Per ogni* $n\in\mathbb{N}$ *, SE (Ipotesi Induttiva) esiste un* $k_n\in\mathbb{N}$ *tale che* $A(n)=7\,k_n$ *,*
*ALLORA (Tesi Induttiva) esiste anche un* $k_{n+1}\in\mathbb{N}$ *tale che* $A(n+1)=7\,k_{n+1}$ *.*

Per dimostrare il passo induttivo, riscriviamo $A(n+1)$ collegandolo a $A(n)$ come segue:

$$\begin{aligned} A(n+1) &:= 3^{2\,(n+1)+1} + 2^{(n+1)+2} = 3^{2\,n+2+1} + 2^{n+1+2} = 3^{2\,n+1}\cdot 3^2 + 2^{n+2}\cdot 2^1 = \\ &= 3^{2\,n+1}\cdot 9 + 2^{n+2}\cdot 2 = 3^{2\,n+1}\cdot (7+2) + 2^{n+2}\cdot 2 = 3^{2\,n+1}\cdot 7 + 3^{2\,n+1}\cdot 2 + 2^{n+2}\cdot 2 = \\ &= 3^{2\,n+1}\cdot 7 + \left(3^{2\,n+1} + 2^{n+2}\right)\cdot 2 = 3^{2\,n+1}\cdot 7 + A(n)\cdot 2 = 7\cdot 3^{2\,n+1} + 7\,k_n\,2 = \\ &= 7\left(3^{2\,n+1} + 2\,k_n\right) = 7\,k_{n+1} \end{aligned}$$

cioè esiste $k_{n+1} := 3^{2\,n+1} + 2\,k_n \in \mathbb{N}$ tale che $A(n+1) = 7\,k_{n+1}$ , q.e.d.

**[5]** — *(a)* Ricordiamo che una classe $\overline{X} = [X]_{20}$ in $\mathbb{Z}_{20}$ è invertibile se e soltanto se si ha M.C.D.$(X, 20) = \pm 1$ , cioè $X$ è coprimo con $20$ . Poiché $9$ e $7$ sono entrambi coprimi con $20$ , possiamo concludere che in $\mathbb{Z}_{20}$ esistono una classe inversa di $\overline{9}$ e una classe inversa di $\overline{7}$ ; inoltre, anche $9\cdot 7$ è coprimo con $20$ — perché lo sono i due fattori $9$ e $7$ — quindi in $\mathbb{Z}_{20}$ esiste pure una classe inversa di $\overline{9}\cdot\overline{7} = \overline{9\cdot 7}$ . D'altra parte, tale classe esiste anche perché da un risultato generale sappiamo che

$$\exists\ a^{-1}\,,\ \exists\ b^{-1} \quad\Longrightarrow\quad \exists\ (a\,b)^{-1} = b^{-1}a^{-1}$$

e quindi per $a = \overline{9}$ e $b := \overline{7}$ dall'esistenza di $\overline{9}^{-1}$ e di $\overline{7}^{-1}$ deduciamo l'esistenza di $\left(\overline{9}\cdot\overline{7}\right)^{-1}$ .

Per lo stesso criterio, poiché M.C.D.$(5, 20) = \pm 5 \neq \pm 1$ e M.C.D.$(5\cdot 7, 20) = \pm 5 \neq \pm 1$ abbiamo che non esistono in $\mathbb{Z}_{20}$ una classe inversa di $\overline{5}$ né una classe inversa di $\overline{5\cdot 7}$ .

Per calcolare le classi inverse $\overline{9}^{-1}$, $\overline{7}^{-1}$ e $\left(\overline{9}\cdot\overline{7}\right)^{-1}$ — di cui già abbiamo appurato l'esistenza — osserviamo che esse sono le soluzioni (uniche) di certe equazioni modulari in $\mathbb{Z}_{20}$ , precisamente (e rispettivamente)

$$\overline{9}\,\overline{x} = \overline{1} \quad , \qquad \overline{7}\,\overline{x} = \overline{1} \quad , \qquad \left(\overline{9}\cdot\overline{7}\right)\overline{x} = \overline{1}$$

Nei primi due casi è facile vedere che le soluzioni richieste sono rispettivamente $\overline{9}^{-1} = \overline{9}$ , perché $\overline{9}\cdot\overline{9} = \overline{9\cdot 9} = \overline{81} = \overline{1}$ , e $\overline{7}^{-1} = \overline{3}$ , perché $\overline{7}\cdot\overline{3} = \overline{7\cdot 3} = \overline{21} = \overline{1}$ .

Per la terza equazione, cominciamo riscrivendola come $\overline{3}\,\overline{x} = \overline{1}$ — in quanto $\overline{9}\cdot\overline{7} = \overline{9\cdot 7} = \overline{63} = \overline{3}$ — e osserviamo poi che essa ha soluzione $\overline{3}^{-1} = \overline{7}$ in quanto $\overline{3}\cdot\overline{7} = \overline{3\cdot 7} = \overline{21} = \overline{1}$ . In alternativa, nel terzo caso possiamo ottenere il risultato osservando che

$$\left(\overline{9}\cdot\overline{7}\right)^{-1} = \left(\overline{9\cdot 7}\right)^{-1} = \overline{63}^{-1} = \overline{3}^{-1} = \left(\overline{7}^{-1}\right)^{-1} = \overline{7}$$

oppure tramite la serie di passaggi (motivati qui sopra)

$$\left(\overline{9}\cdot\overline{7}\right)^{-1} = \overline{7}^{-1}\cdot\overline{9}^{-1} = \overline{3}\cdot\overline{9} = \overline{3\cdot 9} = \overline{27} = \overline{7}$$

*(b)* Riscriviamo l'equazione modulare $\overline{647}\,\overline{x} = \overline{-516}$ in $\mathbb{Z}_{20}$ utilizzando rappresentanti diversi per le classi di congruenza $\overline{647}$ e $\overline{-516}$ . Precisamente, poiché $647 \equiv 7 \pmod{20}$ e $-516 \equiv 4 \pmod{20}$ abbiamo $\overline{647} = \overline{7}$ e $\overline{-516} = \overline{4}$ , quindi la nostra equazione modulare può essere riscritta nella forma $\circledast : \overline{7}\,\overline{x} = \overline{4}$ . Dato che in $\circledast$ il coefficiente $\overline{7}$ dell'incognita è invertibile, l'equazione ha una e una sola soluzione, data da $\overline{x} = \overline{7}^{-1}\cdot\overline{4}$ , e grazie a quanto già visto in *(a)* questo ci dà $\overline{x} = \overline{7}^{-1}\cdot\overline{4} = \overline{3}\cdot\overline{4} = \overline{3\cdot 4} = \overline{12}$ , cioè $\overline{x} = \overline{12}$ .

In alternativa, l'equazione modulare $\circledast : \overline{7}\,\overline{x} = \overline{4}$ in $\mathbb{Z}_{20}$ può essere risolta tramite la risoluzione di un'equazione diofantea in $\mathbb{Z}$, precisamente

$$\circledast_{\text{E.D.}} : \; 7\,x + 20\,y = 4 \tag{7}$$

la quale certamente ha soluzioni perché $\text{M.C.D.}(7,20) = 1 \,\Big|\, 4 \;\big(= 1 \cdot 4\big)$ .

Per calcolare una soluzione, calcoliamo una identità di Bezóut per $\text{M.C.D.}(7,20) = 1$ tramite l'algoritmo euclideo delle divisioni successive. I calcoli espliciti ci danno

$$\begin{aligned} 7 &= 20 \cdot 0 + 7 \quad \Longrightarrow \quad 7 = 7 + 20 \cdot (-0) \\ 20 &= 7 \cdot 2 + 6 \quad \Longrightarrow \quad 6 = 20 + 7 \cdot (-2) \\ 7 &= 6 \cdot 1 + 1 \quad \Longrightarrow \quad 1 = 7 + 6 \cdot (-1) \\ 6 &= 1 \cdot 6 + 0 \quad \Longrightarrow \quad \text{STOP!} \end{aligned}$$

e quindi risalendo all'indietro

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

così che l'identità di Bézout trovata è $7 \cdot 3 + 20 \cdot (-1) = 1$ . Moltiplicando i coefficienti di 7 e di 20 per 4 tale identità ci dà

$$7 \cdot 12 + 20 \cdot (-4) = 4$$

che ci dice che la coppia $\big(x', y'\big) := (12\,, -4)$ è una soluzione dell'equazione diofantea in (7). Per concludere, la prima componente di tale soluzione della (7), cioè $x' = 12$, ci dà una soluzione — che, per quanto già visto, è *l'unica* possibile — dell'equazione modulare $\overline{7}\,\overline{x} = \overline{4}$ in $\mathbb{Z}_{20}$, precisamente $\overline{x'} = \overline{12}$.

*(c)* Riscriviamo l'equazione congruenziale $436\,x \equiv 92 \pmod{20}$ sostituendo al coefficiente e al termine noto altri numeri ad essi congruenti modulo 20 e più semplici (ai fini dei nostri calcoli). Ad esempio, dato che $436 \equiv -4 \pmod{20}$ e $92 \equiv -8 \pmod{20}$, la nostra equazione congruenziale è equivalente a $-4\,x \equiv -8 \pmod{20}$ . Dividendo *tutto* (coefficiente, termine noto e modulo) per $-4$, quest'ultima equazione a sua volta è equivalente a $x \equiv 2 \pmod{5}$ — osservando che $20/-4 = -5$ , e che la congruenza modulo $-5$ è uguale a quella modulo 5 ... — che è un'equazione *già risolta!* In conclusione, le soluzioni della nostra equazione congruenziale di partenza sono tutti e soli i numeri interi della forma

$$x = 2 + 5\,z \;, \qquad \forall \; z \in \mathbb{Z}$$

o, in altre parole, tutti e soli i numeri interi che costituiscono $[2]_{\equiv_5}$ , cioè la classe di congruenza di 2 modulo 5.

**[6]** — *(a)* Osserviamo che per ogni $E \in \mathcal{P}(B \setminus C)$ si ha $E \subseteq (B \setminus C)$, ma è anche $(B \setminus C) \subseteq B$ e quindi — per la tranisitività della relazione di inclusione $\subseteq$ — si ha pure $E \subseteq B$, cioè $E \in \mathcal{P}(B)$. Allora per ogni $E \in \mathcal{P}(B \setminus C)$ si può considerare $f(E)$, e si ha $f(E) := E \setminus C = E \setminus \big(E \cap C\big) = E \setminus \emptyset = E$ perché $E \subseteq (B \setminus C)$ e quindi $E \cap C = \emptyset$. La conclusione è che per ogni $E \in \mathcal{P}(B \setminus C)$ esiste $E \in \mathcal{P}(B)$ tale che $f(E) = E$, e quindi in particolare $f$ è suriettiva, q.e.d.

*(b)* Dovendo dimostrare una doppia implicazione "$\iff$", procediamo a dimostrare prima l'implicazione "$\implies$" e poi l'implicazione "$\impliedby$".

$\big(\implies\big)$: Supponiamo che $f$ sia iniettiva. Poiché $B \cap C \subseteq C$ dalle definizioni si ha ovviamente $f\big(B \cap C\big) := \big(B \cap C\big) \setminus C = \emptyset$ ; d'altra parte è anche $f(\emptyset) := \emptyset \setminus C = \emptyset$ . Dunque $f\big(B \cap C\big) = f(\emptyset)\ \big(= \emptyset\big)$ e siccome $f$ è iniettiva concludiamo che $B \cap C = \emptyset$, q.e.d.

*In alternativa*, possiamo procedere con una *dimostrazione per assurdo*, come segue. Supponiamo che $f$ sia iniettiva, e supponiamo anche, *per assurdo*, che sia $B \cap C \neq \emptyset$ . Ora, come già visto si ha $f\big(B \cap C\big) = \emptyset$ e $f(\emptyset) = \emptyset$ . Dunque $f\big(B \cap C\big) = f(\emptyset)\ \big(= \emptyset\big)$ con $B \cap C \neq \emptyset$, *contro* l'ipotesi che $f$ sia iniettiva. La contraddizione implica che l'ipotesi $B \cap C \neq \emptyset$ è assurda, e quindi dev'essere necessariamente $B \cap C = \emptyset$, q.e.d.

$\big(\impliedby\big)$: Supponiamo che sia $B \cap C = \emptyset$ . Allora per ogni $E \in \mathcal{P}(B)$ si ha $E \cap C \subseteq B \cap C = \emptyset$ e quindi $E \cap C = \emptyset$ ; ma allora $f(E) := E \setminus C = E \setminus \big(E \cap C\big) = E \setminus \emptyset = E$ . Dunque abbiamo $f(E) = E$ per ogni $E \in \mathcal{P}(B)$, e quindi se per $E', E'' \in \mathcal{P}(B)$ si ha $f\big(E'\big) = f\big(E''\big)$ se ne deduce che $E' = f\big(E'\big) = f\big(E''\big) = E''$, cioè $E' = E''$: pertanto concludiamo che $f$ è iniettiva, q.e.d.

**[7]** — Ricordiamo che l'espressione di un numero $N \in \mathbb{N}$ con notazione posizionale in una qualsiasi base $B\ (> 1)$ è la scrittura $N = (c_k \cdots c_1 c_0)_{B} := \sum_{s=0}^{k} c_s B^s$ con $0 \leq c_s \leq B-1$ $(\forall\, s = 0, 1, \ldots, k)$ e $c_k \neq 0$ quando $N \neq 0$ , e $N = (0)_{B} := 0$ quando invece $N = 0$. La suddetta espressione di $N$ in base $B$ si trova operando in successione diverse divisioni per $B$ — cominciando col divididere $N$ stesso — i cui resti saranno le cifre $c_s$ che formano la scrittura posizionale di $N$. Si noti che nel fare i calcoli per una divisione con resto i numeri coinvolti si possono scrivere in una base o in un'altra, ma l'operazione stessa (di "divisione con resto") è indipendente da come si rappresentino tali numeri.

Procediamo ora ad trattare i singoli punti dell'esercizio.

*(a)* Sia $n$ il numero naturale che in base dieci è espresso dalla notazione posizionale $n := (9873)_{\text{DIECI}}$. Dobbiamo scrivere tale $n$ in base $b' := \text{OTTO}$ e in base $b'' := \text{SETTE}$.

Operiamo ora l'algoritmo delle divisioni successive — scrivendo i calcoli espliciti in base dieci — che ci dà

$$\begin{aligned}
9873 &= 8 \cdot 1234 + 1 \quad &\Longrightarrow \quad c_0 &= 1\,, \quad q_0 = 1234 \\
1234 &= 8 \cdot 154 + 2 \quad &\Longrightarrow \quad c_1 &= 2\,, \quad q_1 = 154 \\
154 &= 8 \cdot 19 + 2 \quad &\Longrightarrow \quad c_2 &= 2\,, \quad q_2 = 19 \\
19 &= 8 \cdot 2 + 3 \quad &\Longrightarrow \quad c_3 &= 3\,, \quad q_3 = 2 \\
2 &= 8 \cdot 0 + 2 \quad &\Longrightarrow \quad c_4 &= 2\,, \quad q_4 = 0 \ \rightarrowtail \text{ STOP!}
\end{aligned}$$

da cui, leggendo la colonna delle cifre $c_0\,,\ c_1\,,\ \ldots\,,\ c_4$, troviamo che

*la scrittura di $n$ in base $b' := OTTO$ è* $n = (23221)_{b'}$ .

Come controprova, convertiamo adesso in base $b := \text{DIECI}$ la scrittura $n = (23221)_{b'}$ , sapendo che dobbiamo ottenere $n = (9873)_{b}$ . I calcoli espliciti (scritti in base dieci) ci danno

$$n \;=\; (23221)_{b':=\text{OTTO}} \;=\; 2\cdot 8^4 + 3\cdot 8^3 + 2\cdot 8^2 + 2\cdot 8^1 + 1\cdot 8^0 \;=$$
$$=\; 2\cdot 4096 + 3\cdot 512 + 2\cdot 64 + 2\cdot 8 + 1\cdot 1 \;=\; 8192 + 1536 + 128 + 16 + 1 \;=\; 9873$$
così che ritroviamo $n = (9873)_b$ , q.e.d.

Cerchiamo ora la scrittura di $n$ in base $b'' :=$ SETTE . Operiamo nuovamente l'algoritmo delle divisioni successive — scrivendo i calcoli espliciti in base dieci — e troviamo

$$\begin{array}{rcl} 9873 \;=\; 7\cdot 1410 + 3 & \Longrightarrow & c_0 \;=\; 3\,, \quad q_0 \;=\; 1410 \\ 1410 \;=\; 7\cdot 201 + 3 & \Longrightarrow & c_1 \;=\; 3\,, \quad q_1 \;=\; 201 \\ 201 \;=\; 7\cdot 28 + 5 & \Longrightarrow & c_2 \;=\; 5\,, \quad q_2 \;=\; 28 \\ 28 \;=\; 7\cdot 4 + 0 & \Longrightarrow & c_3 \;=\; 0\,, \quad q_3 \;=\; 4 \\ 4 \;=\; 7\cdot 0 + 4 & \Longrightarrow & c_4 \;=\; 4\,, \quad q_4 \;=\; 0 \;\rightarrowtail \text{STOP!} \end{array}$$
da cui, leggendo la colonna delle cifre $c_0\,,\; c_1\,,\; \ldots\,,\; c_4$ , otteniamo che
$$\textit{la scrittura di } n \textit{ in base } b'' := \textit{SETTE } \textit{è } \; n = (40533)_{b''}\,.$$

Come controprova (per avere una conferma) andiamo a convertire in base $b :=$ DIECI la scrittura $n = (40533)_{b''}$ , sapendo che dobbiamo necessariamente trovare $n = (9873)_b$ . I calcoli espliciti — scritti ancora in base dieci — ci danno
$$n \;=\; (40533)_{b'':=\text{SETTE}} \;=\; 4\cdot 7^4 + 0\cdot 7^3 + 5\cdot 7^2 + 3\cdot 7^1 + 3\cdot 7^0 \;=$$
$$=\; 4\cdot 2401 + 0\cdot 343 + 5\cdot 49 + 3\cdot 7 + 3\cdot 1 \;=\; 9604 + 0 + 245 + 21 + 3 \;=\; 9873$$
così troviamo nuovamente $n = (9873)_b$ , q.e.d.

*In alternativa*, possiamo ottenere la scrittura di $n$ in base $b'' :=$ SETTE a partire da quella in base $b' :=$ OTTO , sviluppando quest'ultima e calcolando la formula corrispondente (sviluppandone i calcoli direttamente in base $b'' :=$ SETTE , in particolare sfruttando il fatto che $b' :=$ OTTO in base $b'' :=$ SETTE si scrive, dato che $b' = b'' + 1$ , semplicemente come $b' = (11)_{b'':=\text{SETTE}}$ ). Ciò premesso, i calcoli espliciti (scritti in base $b'' :=$ SETTE ) ci danno
$$n \;=\; (23221)_{b':=\text{OTTO}} \;=\; 2\cdot 8^4 + 3\cdot 8^3 + 2\cdot 8^2 + 2\cdot 8^1 + 1\cdot 8^0 \;=$$
$$=\; (2)_{b''}\cdot (11)_{b''}^{\,4} + (3)_{b''}\cdot (11)_{b''}^{\,3} + (2)_{b''}\cdot (11)_{b''}^{\,2} + (2)_{b''}\cdot (11)_{b''}^{\,1} + (1)_{b''}\cdot (11)_{b''}^{\,0} \;=$$
$$=\; (2)_{b''}\cdot (14641)_{b''} + (3)_{b''}\cdot (1331)_{b''} + (2)_{b''}\cdot (121)_{b''} + (2)_{b''}\cdot (11)_{b''} + (1)_{b''}\cdot (1)_{b''} \;=$$
$$=\; (32612)_{b''} + (4323)_{b''} + (242)_{b''} + (22)_{b''} + (1)_{b''} \;=\; (40533)_{b'':=\text{SETTE}}$$
cioè in conclusione $n = (40533)_{b'':=\text{SETTE}}$ come già trovato in precedenza.

*(b)* Dobbiamo scrivere in base $b' :=$ DIECI il numero $S := \big(41032\big)_{b:=\text{CINQUE}}$ . Esplicitando quest'ultima espressione, e scrivendo i relativi calcoli in base $b' :=$ DIECI , otteniamo
$$S \;=\; (41032)_{b:=\text{CINQUE}} \;=\; 4\cdot 5^4 + 1\cdot 5^3 + 0\cdot 5^2 + 3\cdot 5^1 + 2\cdot 5^0 \;=$$
$$=\; 4\cdot 625 + 1\cdot 125 + 0\cdot 25 + 3\cdot 5 + 2\cdot 1 \;=\; 2500 + 125 + 0 + 15 + 2 \;=\; (2642)_{b':=\text{DIECI}}$$
dunque $S = (2642)_{b':=\text{DIECI}}$ *è la scrittura di* $S$ *in base* $b' :=$ *DIECI cercata.*

Come controprova (tanto per fare una verifica), calcoliamo l'espressione in base $b :=$ CINQUE di $S = (2642)_{b':=\text{DIECI}}$ . L'algoritmo usuale (che scriviamo in base dieci) ci dà

$$\begin{array}{rcl} 2642 \;=\; 5\cdot 528 + 2 & \Longrightarrow & c_0 \;=\; 2\,, \quad q_0 \;=\; 528 \\ 528 \;=\; 5\cdot 105 + 3 & \Longrightarrow & c_1 \;=\; 3\,, \quad q_1 \;=\; 105 \\ 105 \;=\; 5\cdot 21 + 0 & \Longrightarrow & c_2 \;=\; 0\,, \quad q_2 \;=\; 21 \\ 21 \;=\; 5\cdot 4 + 1 & \Longrightarrow & c_3 \;=\; 1\,, \quad q_3 \;=\; 4 \\ 4 \;=\; 5\cdot 0 + 4 & \Longrightarrow & c_4 \;=\; 4\,, \quad q_4 \;=\; 0 \;\rightarrowtail \text{STOP!} \end{array}$$
e quindi dalla colonna delle cifre $c_0\,,\; c_1\,,\; \ldots\,,\; c_4$ , otteniamo $S = (41032)_{b=\text{CINQUE}}$ , q.e.d.

*(c)* Dobbiamo scrivere in base $b' := \text{QUATTRO}$ e in base $b'' := \text{DUE}$ il numero $L$ che in base $b := \text{OTTO}$ si scrive come $L := \big(3471\big)_b$ . In questo caso sfruttiamo il fatto notevole che tra le basi in esame c'è questo tipo di relazione: $b'' := 2$ è radice di $b := 8$, perché $2^3 = 8$, e $b' := 4$ è potenza di $b'' := 2$, perché $4 = 2^2$.

Poiché $8 = 2^3$, ogni cifra in base 8 si scrive come numero di (al più) tre cifre in base 2, precisamente

$$\begin{gathered} (0)_8 = (000)_2 \quad , \qquad (1)_8 = (001)_2 \quad , \qquad (2)_8 = (010)_2 \quad , \qquad (3)_8 = (011)_2 \\ (4)_8 = (100)_2 \quad , \qquad (5)_8 = (101)_2 \quad , \qquad (6)_8 = (110)_2 \quad , \quad (7)_8 = (111)_2 \end{gathered} \tag{8}$$

In conseguenza, data la scrittura $L := \big(3471\big)_8$ di $L$ in base 8, sviluppando ogni sua cifra come terna di cifre in base 2 secondo la (8), otteniamo $L := \big(011.100.111.001\big)_2$ — dove abbiamo messo dei punti in basso per marcare la suddivisione in terne di cifre (in base 2) provenienti da singole cifre in base 8. Da questo, scartando i suddetti punti e lo 0 iniziale, *otteniamo la scrittura di L in base 2, che è* $L := \big(11100111001\big)_{b'':=2}$ .

Poiché $4 = 2^2$, ogni cifra in base 4 si scrive come numero di (al più) due cifre in base 2, e viceversa ogni numero di (al più) due cifre in base 2 si scrive come numero a una sola cifra in base 4; precisamente, la corrispondenza tra le due scritture è la seguente (analoga della (8) qui sopra):

$$(0)_4 = (00)_2 \quad , \qquad (1)_4 = (01)_2 \quad , \qquad (2)_4 = (10)_2 \quad , \qquad (3)_8 = (11)_2 \tag{9}$$

A questo punto, a partire dalla scrittura $L := \big(11100111001\big)_2 = \big(01.11.00.11.10.01\big)_2$ di $L$ in base 2 — in cui abbiamo raccolto le cifre a coppie, partendo dall'ultima a destra (e aggiungendo uno 0 a sinistra per "completare" la coppia più a sinistra) — sostituiamo ogni coppia di cifre in base 2 con una singola cifra in base 4, secondo la (9): così facendo otteniamo $L := \big(1.3.0.3.2.1\big)_2$ e infine — scartando i punti di suddivisione — *ricaviamo la scrittura di L in base 4, precisamente* $L := \big(130321\big)_{b':=4}$ .

*(d)* Dati i due numeri $N := \big(12021\big)_{\beta:=3}$ e $M := \big(20102\big)_{\beta:=3}$ , dobbiamo calcolare la loro somma $N + M$ svolgendo i calcoli con la notazione in base $\beta := 3$, e dobbiamo poi esprimere il risultato sia in base $\beta := 3$ che in base $\beta' := \text{DIECI}$.

Facendo il calcolo direttamente in base $\beta := 3$ — e indicando nella linea aggiuntiva superiore i "riporti" — otteniamo l'espressione di $N + M$ in base 3, precisamente

$$\left( \begin{array}{r} 1 \quad 1\,1 \\ 1\,2\,0\,2\,1 + \\ \underline{2\,0\,1\,0\,2} = \\ 1\,0\,2\,2\,0\,0 \end{array} \right)_{\beta:=3} \quad \Longrightarrow \quad N + M \;=\; \big(102200\big)_{\beta:=3} \tag{10}$$

A partire da tale espressione possiamo ottenere quella in base $\beta' := \text{DIECI}$ sviluppando l'espressione precedente e calcolandone la formula corrispondente (con calcoli scritti in base dieci) come segue:

$$\begin{aligned} N + M \;&=\; \big(102200\big)_{\beta:=3} \;=\; 1 \cdot 3^5 + 0 \cdot 3^4 + 2 \cdot 3^3 + 2 \cdot 3^2 + 0 \cdot 3^1 + 0 \cdot 3^0 \;= \\ &= 1 \cdot 243 + 0 \cdot 81 + 2 \cdot 27 + 2 \cdot 9 + 0 \cdot 3 + 0 \cdot 1 \;=\; 243 + 0 + 54 + 18 + 0 + 0 \;=\; (315)_{\beta':=\text{DIECI}} \end{aligned}$$

per cui $N + M = (315)_{\beta':=\text{DIECI}}$ è la scrittura di $N + M$ in base $\beta' := \text{DIECI}$ richiesta.

Come controprova, possiamo convertire entrambi i numeri $N$ ed $M$ in base $\beta' := \text{DIECI}$, calcolarne la somma $N+M$ direttamente in base $\beta' := \text{DIECI}$ e poi convertire il risultato in base $\beta := 3$. Per il primo passo abbiamo

$$\begin{aligned} N \;&=\; \big(12021\big)_{\beta:=3} \;=\; 1\cdot 3^4 + 2\cdot 3^3 + 0\cdot 3^2 + 2\cdot 3^1 + 1\cdot 3^0 \;= \\ &= 1\cdot 81 + 2\cdot 27 + 0\cdot 9 + 2\cdot 3 + 1\cdot 1 \;=\; 81+54+0+6+1 \;=\; (142)_{\beta':=\text{DIECI}} \\ M \;&=\; \big(20102\big)_{\beta:=3} \;=\; 2\cdot 3^4 + 0\cdot 3^3 + 1\cdot 3^2 + 0\cdot 3^1 + 2\cdot 3^0 \;= \\ &= 2\cdot 81 + 0\cdot 27 + 1\cdot 9 + 0\cdot 3 + 2\cdot 1 \;=\; 162+0+9+0+2 \;=\; (173)_{\beta':=\text{DIECI}} \end{aligned}$$

e quindi per il secondo passo troviamo

$$N+M \;=\; (142)_{\beta':=\text{DIECI}} + (173)_{\beta':=\text{DIECI}} \;=\; (315)_{\beta':=\text{DIECI}}$$

così che ritroviamo la scrittura in base $\beta' = \text{DIECI}$ come $N+M = (315)_{\beta':=\text{DIECI}}$ come in precedenza. Infine, possiamo verificare la correttezza dell'espressione in (10) andando a riscrivere in base $\beta := 3$ il numero $N+M$ espresso come $N+M = (315)_{\beta':=\text{DIECI}}$. Con l'algoritmo standard delle divisioni per $\beta$ in successione (scrivendo i calcoli espliciti in base dieci) otteniamo

$$\begin{array}{rcl} 315 \;=\; 3\cdot 105 + 0 & \Longrightarrow & c_0 \;=\; 0\,, \quad q_0 \;=\; 105 \\ 105 \;=\; 3\cdot 35 + 0 & \Longrightarrow & c_1 \;=\; 0\,, \quad q_1 \;=\; 35 \\ 35 \;=\; 3\cdot 11 + 2 & \Longrightarrow & c_2 \;=\; 2\,, \quad q_2 \;=\; 11 \\ 11 \;=\; 3\cdot 3 + 2 & \Longrightarrow & c_3 \;=\; 2\,, \quad q_3 \;=\; 3 \\ 3 \;=\; 3\cdot 1 + 0 & \Longrightarrow & c_4 \;=\; 0\,, \quad q_4 \;=\; 1 \\ 1 \;=\; 3\cdot 0 + 1 & \Longrightarrow & c_5 \;=\; 1\,, \quad q_5 \;=\; 0 \;\rightarrowtail \text{STOP!} \end{array}$$

e quindi dalla colonna delle cifre $c_0\,,\; c_1\,,\; \ldots\,,\; c_4$, otteniamo $(315)_{\beta':=\text{DIECI}} = (102200)_{\beta:=3}$, cioè $N+M = (102200)_{\beta:=3}$, che è effettivamente l'espressione già trovata in (10).

**[8]** — Ricordiamo che $\psi : \mathbb{N}_+ \longrightarrow \mathcal{P}(\mathbb{N})$ è data da $\psi(\ell) := \big\{\, p \in \mathbb{N}_+ \big|\, p \text{ primo}, p \text{ divide } \ell \,\big\}$ (per $\ell \in \mathbb{N}_+$), e la relazione $\lhd$ è definita da $\ell_1 \lhd \ell_2 \iff \psi\big(\ell_1\big) \subseteq \psi\big(\ell_2\big)$ (per $\ell_1, \ell_2 \in \mathbb{N}_+$).

*(a)* Per ogni $\ell \in \mathbb{N}_+$ si ha $\psi(\ell) = \psi(\ell)$, quindi in particolare $\psi(\ell) \subseteq \psi(\ell)$ e dunque $\ell \lhd \ell$; perciò la relazione $\lhd$ è riflessiva e transitiva, q.e.d.

Inoltre, per ogni $\ell_1, \ell_2, \ell_3 \in \mathbb{N}_+$ tali che $\ell_1 \lhd \ell_2$ e $\ell_2 \lhd \ell_3$ si ha $\psi(\ell_1) \subseteq \psi(\ell_2)$ e $\psi(\ell_2) \subseteq \psi(\ell_3)$, quindi — per la transitività della relazione di inclusione $\subseteq$ — anche $\psi(\ell_1) \subseteq \psi(\ell_3)$, che significa $\ell_1 \lhd \ell_3$; perciò la relazione $\lhd$ è transitiva, q.e.d.

*(b)* Siano $\ell_1, \ell_2 \in \mathbb{N}_+$ tali che $\ell_1 \lhd \ell_2$ e $\ell_2 \lhd \ell_1$: questo significa che $\psi(\ell_1) \subseteq \psi(\ell_2)$ e $\psi(\ell_2) \subseteq \psi(\ell_1)$, il che equivale a $\psi(\ell_1) = \psi(\ell_2)$. Così troviamo che $(\ell_1 \lhd \ell_2)$ & $(\ell_2 \lhd \ell_1)$ equivale a $\psi(\ell_1) = \psi(\ell_2)$, *ma questo non significa che sia* $\ell_1 = \ell_2$, perché la funzione $\psi$ *non è iniettiva*. Ad esempio, per $\ell_1 := 4$ e $\ell_2 := 8$ abbiamo $\psi(4) = \psi(8)$ $\big(= \{2\}\big)$ e quindi $4 \lhd 8$ e $8 \lhd 4$, *ma* $4 \neq 8$. Questo dimostra che la relazione $\lhd$ non è antisimmetrica, q.e.d.

*N.B.:* volendo generalizzare l'ultimo passo, osserviamo che dati $\ell_1, \ell_2 \in \mathbb{N}_+$ si ha

$$(\ell_1 \lhd \ell_2) \;\&\; (\ell_2 \lhd \ell_1) \iff \psi(\ell_1) = \psi(\ell_2) \tag{11}$$

dove l'ultima condizione significa semplicemente che nella fattorizzazione (unica) in primi di $\ell_1$ e $\ell_2$ compaiono (in modo esplicito cioè con esponenti positivi) esattamente gli stessi primi.

*(c)* Cerchiamo — se esiste... — un $\ell_\downarrow \in \mathbb{N}_+$ tale che $\ell_\downarrow \lhd \ell$ per ogni $\ell \in \mathbb{N}_+$. Questa richiesta equivale a $\psi(\ell_\downarrow) \subseteq \psi(\ell)$ per ogni $\ell \in \mathbb{N}_+$; ora, già per i casi particolari $\ell := 2$ e $\ell := 3$ abbiamo $\psi(2) = \{2\}$ e $\psi(3) = \{3\}$, quindi dovremmo avere $\psi(\ell_\downarrow) \subseteq \{2\}$ e $\psi(\ell_\downarrow) \subseteq \{3\}$, dunque $\psi(\ell_\downarrow) \subseteq \{2\} \cap \{3\} = \emptyset$ che implicherebbe necessariamente $\psi(\ell_\downarrow) = \emptyset$. Viceversa, se $\psi(\ell_\downarrow) = \emptyset$ allora ovviamente $\psi(\ell_\downarrow) = \emptyset \subseteq \psi(\ell)$ e quindi $\ell_\downarrow \lhd \ell$ per ogni $\ell \in \mathbb{N}_+$ come richiesto. Dunque l'elemento $\ell_\downarrow$ cerato deve soddisfare la *condizione necessaria e sufficiente* $\psi(\ell_\downarrow) = \emptyset$, che significa che non esiste nessun primo che divida $\ell_\downarrow$: ma questo è vero se e soltanto se $\ell_\downarrow = 1$, perciò in conclusione si ha che

$$\textit{esiste uno (e un solo!) elemento } \ell_\downarrow \in \mathbb{N}_+ \textit{ tale che } \ell_\downarrow \lhd \ell\,, \textit{ precisamente } \ell_\downarrow = 1\,.$$

*(d)* Cerchiamo — se esiste... — un $\ell^\uparrow \in \mathbb{N}_+$ tale che $\ell \lhd \ell^\uparrow$ per ogni $\ell \in \mathbb{N}_+$. Questa richiesta equivale a $\psi(\ell) \subseteq \psi(\ell^\uparrow)$ per ogni $\ell \in \mathbb{N}_+$; ora, per tutti i casi particolari $\ell := p$ numero *primo* in $\mathbb{N}_+$ abbiamo $\psi(p) = \{p\}$, quindi dovremmo avere $\{p\} \subseteq \psi(\ell^\uparrow)$ per ogni primo $p$ in $\mathbb{N}_+$: questo implicherebbe che $\ell^\uparrow$ fosse un numero naturale divisibile da *tutti* i numeri primi, il che è impossibile. Pertanto si conclude che

$$\textit{non esiste un elemento } \ell^\uparrow \in \mathbb{N}_+ \textit{ tale che } \ell \lhd \ell^\uparrow\,.$$

*(e)* Ricordiamo che la relazione $\asymp$ in $\mathbb{N}_+$ è definita da $\ell_1 \asymp \ell_2 \iff \big(\ell_1 \lhd \ell_2\big) \wedge \big(\ell_2 \lhd \ell_1\big)$.

Dobbiamo dimostrare che tale relazione è una equivalenza, cioè gode delle proprietà *riflessiva (R)*, *transitiva (T)* e *simmetrica (S)*. Verifichiamo separatamente queste tre proprietà.

$\big(\underline{\mathrm{R}}\big)$: Per ogni $\ell \in \mathbb{N}_+$ si ha $\ell \lhd \ell$, quindi $\big(\ell \lhd \ell\big) \wedge \big(\ell \lhd \ell\big)$ cioè $\ell \asymp \ell$. Questo prova che $\ell \asymp \ell$ per ogni $\ell \in \mathbb{N}_+$, cioè che la relazione $\asymp$ è riflessiva, q.e.d.

$\big(\underline{\mathrm{T}}\big)$: Siano $\ell_1, \ell_2, \ell_3 \in \mathbb{N}_+$ tali che $\ell_1 \asymp \ell_2$ e $\ell_2 \asymp \ell_3$; dobbiamo allora dimostrare che si ha anche $\ell_1 \asymp \ell_3$. Dalle definizioni abbiamo

$$\ell_1 \asymp \ell_2 \implies \big(\ell_1 \lhd \ell_2\big) \wedge \big(\ell_2 \lhd \ell_1\big) \qquad \text{e} \qquad \ell_2 \asymp \ell_3 \implies \big(\ell_2 \lhd \ell_3\big) \wedge \big(\ell_3 \lhd \ell_2\big)$$

quindi complessivamente abbiamo

$$\ell_1 \lhd \ell_2 \quad , \qquad \ell_2 \lhd \ell_1 \quad , \qquad \ell_2 \lhd \ell_3 \quad , \qquad \ell_3 \lhd \ell_2$$

Da queste relazioni, sfruttando il fatto che la relazione $\lhd$ è transitiva — per la parte *(a)* qui sopra — deduciamo

$$\big(\ell_1 \lhd \ell_2\big) \wedge \big(\ell_2 \lhd \ell_3\big) \implies \ell_1 \lhd \ell_3 \qquad \text{e} \qquad \big(\ell_3 \lhd \ell_2\big) \wedge \big(\ell_2 \lhd \ell_1\big) \implies \ell_3 \lhd \ell_1$$

dunque otteniamo $\big(\ell_1 \lhd \ell_3\big) \wedge \big(\ell_3 \lhd \ell_1\big)$, cioè $\ell_1 \asymp \ell_3$, q.e.d.

$\big(\underline{\mathrm{S}}\big)$: Siano $\ell_1, \ell_2 \in \mathbb{N}_+$ tali che $\ell_1 \asymp \ell_2$; dobbiamo allora dimostrare che $\ell_2 \asymp \ell_1$.

La dimostrazione è pressoché tautologica: infati, direttamente dalle definizioni abbiamo

$$\ell_1 \asymp \ell_2 \implies \big(\ell_1 \lhd \ell_2\big) \wedge \big(\ell_2 \lhd \ell_1\big) \implies \big(\ell_2 \lhd \ell_1\big) \wedge \big(\ell_1 \lhd \ell_2\big) \implies \ell_2 \asymp \ell_1$$

e dunque possiamo concludere che $\ell_2 \asymp \ell_1$, q.e.d.

*In alternativa*, possiamo dimostrare che $\asymp$ è una equivalenza in modo molto più rapido (ancorché indiretto), come segue. Dalla definizione stessa di $\asymp$ e dalla (11) segue che $\asymp$ è *la relazione $\rho_\psi$ canonicamente associata alla funzione $\psi$*: ora, per un risultato generale, ogni tale relazione è *sempre* un'equivalenza, quindi anche $\asymp$ stessa è un'equivalenza, q.e.d.

**[9]** — In ciascuno dei casi in esame abbiamo un numero della forma $N = B^E$ (con $N, B, E \in \mathbb{N}$): trovarne il resto nella divisione per 20 significa trovare quell'unico numero naturale $r \in \{0, 1, 2, \ldots, 18, 19\}$ tale che $N = 20 \cdot q + r$ per un certo $q \in \mathbb{N}$ (che qui non ci interessa conoscere). Dunque $r$ è l'unico numero intero nell'intervallo $\{0, 1, \ldots, 19\}$ tale che $N = 20 \cdot q + r \equiv r \pmod{20}$, cioè $\overline{N} = \overline{r}$ in $\mathbb{Z}_{20}$ con $r \in \{0, 1, \ldots, 19\}$.

Ora, da $N = B^E$ segue che $\overline{N} = \overline{B^E} = \overline{B}^{\,E}$ in $\mathbb{Z}_{20}$, quindi una prima semplificazione si ottiene semplificando la rappresentazione della classe $\overline{B}$, cioè scegliendo un rappresentante "piccolo" — ad esempio, compreso tra 0 e 19, oppure tra -10 e +10 — per la classe di congruenza $\overline{B}$. Una ulteriore semplificazione può riguardare eventualmente l'"esponente" $E$, ma questa dipende dalla relazione tra $B$ — o un qualsiasi rappresentante più semplice della sua classe di congruenza $\overline{B}$ — e il modulo 20, quindi dipenderà da un'analisi caso per caso.

*(a)* Per $N = a := 457^{\,35062867}$ abbiamo $N = B^E$ con $B := 457$ e $E := 35062867$. In tal caso $\overline{B} = \overline{457} = \overline{-3}$, quindi

$$\overline{a} \;=\; \overline{457^{\,35062867}} \;=\; \overline{457}^{\,35062867} \;=\; \overline{-3}^{\,35062867}$$

Osserviamo adesso che $\text{M.C.D.}(-3\,,20) = 1$, quindi per la classe $\overline{-3} = -\overline{3}$ si può applicare il Teorema di Eulero, che ci dice in questo caso che $\overline{-3}^{\,\varphi(20)} = \overline{1}$ in $\mathbb{Z}_{20}$, dove $\varphi(20)$ è il valore della funzione di Eulero $\varphi$ su 20; come conseguenza, se $35062867 = \varphi(20)\,\kappa + \rho$ è la divisione di 35062867 per $\varphi(20)$ — dunque con resto $\rho < \varphi(20)$ — si ha subito

$$\overline{a} \;=\; \overline{-3}^{\,35062867} \;=\; \overline{-3}^{\,\varphi(20)\,\kappa+\rho} \;=\; \left(\overline{-3}^{\,\varphi(20)}\right)^{\kappa} \cdot \overline{-3}^{\,\rho} \;=\; \overline{1} \cdot \overline{-3}^{\,\rho} \;=\; \overline{-3}^{\,\rho}$$

Si noti quindi che riguardo all'esponente 35062867 conta soltanto il resto $\rho$ nella divisione per $\varphi(20)$, cioè quell'unico $\rho \in \{0, 1, \ldots, \varphi(20) - 1\}$ tale che $35062867 \equiv \rho \pmod{\varphi(20)}$, o in altre parole tale che $\overline{35062867} = \overline{\rho}$ in $\mathbb{Z}_{\varphi(20)}$.

Ora, per $\varphi(20)$ abbiamo $\varphi(20) = \varphi\big(5 \cdot 2^2\big) = (5-1) \cdot 2^{2-1}\,(2-1) = 4 \cdot 2 = 8$, cioè $\varphi(20) = 8$, così che $\overline{-3}^{\,20} = \overline{1}$; inoltre $\overline{35062867} = \overline{867} = \overline{67} = \overline{3}$ in $\mathbb{Z}_{\varphi(20)} = \mathbb{Z}_8$ così che $\rho = 3$. Allora l'analisi precedente ci dà

$$\overline{a} \;=\; \overline{-3}^{\,\rho} \;=\; \overline{-3}^{\,3} \;=\; \overline{(-3)^3} \;=\; \overline{-27} \;=\; \overline{-7} \;=\; \overline{13}$$

per cui in conclusione *il resto cercato è* $r = 13$ .

*(b)* Per $N = b := 2384^{\,16}$ abbiamo $N = B^E$ con $B := 2384$ e $E := 16$. In questo caso $\overline{B} = \overline{2384} = \overline{4}$, quindi

$$\overline{b} \;=\; \overline{2384^{\,16}} \;=\; \overline{2384}^{\,16} \;=\; \overline{4}^{\,16}$$

Osserviamo ora che $\text{M.C.D.}(4\,,20) = 4 \neq 1$, quindi per la classe $\overline{4}$ *non si può applicare il Teorema di Eulero*: non è dunque possibile sfruttare una semplificazione "diretta" della forma $\overline{4}^{\,\varphi(20)} = \overline{1}$, bisogna invece ricorrere ad un'analisi diversa, specifica per questa situazione — sapendo che *comunque* una qualche forma di semplificazione sarà certamente possibile.

Dovendo calcolare potenze di $\overline{4}$ in $\mathbb{Z}_{20}$, osserviamo che $\overline{4}^{\,2} = \overline{16} = \overline{-4} = -\overline{4}$, cioè $\overline{4}^{\,2} = -\overline{4}$; da questo segue immediatamente che $\overline{4}^{\,3} = +\overline{4}$, $\overline{4}^{\,4} = -\overline{4}$, ecc. ecc.: precisamente, dimostriamo per induzione che

$$\overline{4}^{\,n} \;=\; \begin{cases} +\overline{4} & \forall\ n \text{ dispari} \\ -\overline{4} & \forall\ n \text{ pari} \end{cases} \qquad \big(n \in \mathbb{N}_+\big)$$

In particolare per $n = 16$ questo ci dà $\overline{4}^{16} = -\overline{4} = \overline{16}$, e quindi

$$\overline{b} \,=\, \overline{2384}^{16} \,=\, \overline{4}^{16} \,=\, \overline{16}$$

per cui in conclusione *il resto cercato è* $r = 16$ .

*(c)* Per $N = c := 645^{5607290843}$ abbiamo $N = B^E$ con $B := 645$ e $E := 5607290843$. In questo caso $\overline{B} = \overline{645} = \overline{5}$, quindi

$$\overline{c} \,=\, \overline{645^{\,5607290843}} \,=\, \overline{645}^{\,5607290843} \,=\, \overline{5}^{\,5607290843}$$

Notiamo adesso che $\text{M.C.D.}(5\,,20) = 5 \neq 1$, perciò per la classe $\overline{5}$ *non si può applicare il Teorema di Eulero*: quindi non è possibile sfruttare una semplificazione "diretta" della forma $\overline{5}^{\,\varphi(20)} = \overline{1}$, bisogna invece ricorrere ad un'analisi diversa, specifica per questa situazione — sapendo che *comunque* una qualche forma di semplificazione sarà certamente possibile.

Dato che dobbiamo calcolare potenze di $\overline{5}$ in $\mathbb{Z}_{20}$, osserviamo che $\overline{5}^{\,2} = \overline{25} = \overline{5}$, cioè $\overline{5}^{\,2} = \overline{5}$: ma da questo segue subito (per induzione) che $\overline{5}^{\,n} = \overline{5}$ per ogni $n \in \mathbb{N}_+$. Quindi

$$\overline{c} \,=\, \overline{645^{\,5607290843}} \,=\, \overline{645}^{\,5607290843} \,=\, \overline{5}^{\,5607290843} \,=\, \overline{5}$$

così che in definitiva *il resto cercato è* $r = 5$ .

**[10]** — Ricordiamo che una famiglia $\big\{X_s\big\}_{s\in S}$ di sottoinsiemi di un insieme $X$ si dice *partizione* di $X$ se valgono le seguenti proprietà:

*(N)* $X_s \neq \emptyset$, per ogni $s \in S$;

*(D)* $X_s \cap X_r \neq \emptyset \implies X_r = X_s$, per ogni $s, r \in S$;

*(R)* $\bigcup\limits_{s\in S} X_s = X$ .

Per ipotesi valgono le proprietà *(N)*, *(D)* e *(R)* per entrambe le famiglie $\big\{X_s\big\}_{s\in S} = \big\{E'_i\big\}_{i\in I}$ e $\big\{X_s\big\}_{s\in S} = \big\{E''_j\big\}_{j\in J}$ di sottoinsiemi di $X := E$, e dobbiamo dimostrare che lo stesso vale per la famiglia $\big\{E'_i \cap E''_j\big\}_{(i,j)\in K}$ con $K := \big\{\,(i,j) \in I \times J \,\big|\, E'_i \cap E''_j \neq \emptyset\,\big\}$ .

Per cominciare, la proprietà *(N)* è valida per la famiglia $\big\{E'_i \cap E''_j\big\}_{(i,j)\in K}$ direttamente per come è stato definito l'insieme $K$ che indicizza la famiglia stessa.

Per la proprietà *(D)*, siano $(i_1, j_1), (i_2, j_2) \in K$ tali che $\big(E'_{i_1} \cap E''_{j_1}\big) \cap \big(E'_{i_2} \cap E''_{j_2}\big) \neq \emptyset$ . Allora si ha anche

$$\emptyset \;\neq\; \big(E'_{i_1} \cap E''_{j_1}\big) \cap \big(E'_{i_2} \cap E''_{j_2}\big) \;=\; \big(E'_{i_1} \cap E'_{i_2}\big) \cap \big(E''_{j_1} \cap E''_{j_2}\big) \implies$$

$$\implies \begin{cases} \big(E'_{i_1} \cap E'_{i_2}\big) \neq \emptyset \\ \big(E''_{j_1} \cap E''_{j_2}\big) \neq \emptyset \end{cases} \implies \begin{cases} E'_{i_1} = E'_{i_2} \\ E''_{j_1} = E''_{j_2} \end{cases} \implies \big(E'_{i_1} \cap E''_{j_1}\big) = \big(E'_{i_2} \cap E''_{j_2}\big)$$

dove abbiamo sfruttato la proprietà *(D)* di entrambe le famiglie $\big\{E'_i\big\}_{i\in I}$ e $\big\{E''_j\big\}_{j\in J}$. Dunque abbiamo $\big(E'_{i_1} \cap E''_{j_1}\big) \cap \big(E'_{i_2} \cap E''_{j_2}\big) \neq \emptyset \implies \big(E'_{i_1} \cap E''_{j_1}\big) = \big(E'_{i_2} \cap E''_{j_2}\big)$, cioè vale la proprietà *(D)* anche per la famiglia $\big\{E'_i \cap E''_j\big\}_{(i,j)\in K}$ .

Infine, per la proprietà *(R)* il calcolo diretto ci dà

$$\bigcup_{(i,j)\in K}\left(E'_i\cap E''_j\right)=\bigcup_{(i,j)\in I\times J}\left(E'_i\cap E''_j\right)=\bigcup_{i\in I}\bigcup_{j\in J}\left(E'_i\cap E''_j\right)=\bigcup_{i\in I}\left(\bigcup_{j\in J}\left(E'_i\cap E''_j\right)\right)=$$
$$=\bigcup_{i\in I}\left(E'_i\cap\left(\bigcup_{j\in J}E''_j\right)\right)=\left(\bigcup_{i\in I}E'_i\right)\bigcap\left(\bigcup_{j\in J}E''_j\right)=E\bigcap E=E$$

dove abbiamo utilizzato (a rovescio) la proprietà distributiva dell'intersezione rispetto all'unione (a destra e sinistra) e il fatto che vale la proprietà *(R)* per le famiglie $\left\{E'_i\right\}_{i\in I}$ e $\left\{E''_j\right\}_{j\in J}$, per cui $\bigcup_{i\in I}E'_i=E$ e $\bigcup_{j\in J}E''_j=E$. La conclusione è che $\bigcup_{(i,j)\in K}\left(E'_i\cap E''_j\right)=E$, dunque vale la proprietà *(R)* anche per le famiglia $\left\{\left(E'_i\cap E''_j\right)\right\}_{(i,j)\in K}$, q.e.d.