

Prova “*in itinere*” per “Matematica Discreta e Logica” – primo appello

31.1.2020

FILA “C”

Esercizio 1

Siano p, q, r, s variabili proposizionali. Per ciascuna delle seguenti affermazioni si dica, motivando la risposta, se è vera o falsa:

$$(i) \quad s \wedge \neg s \wedge (p \rightarrow s) \models (p \rightarrow q) \wedge (\neg q \rightarrow p);$$

$$(ii) \quad (p \rightarrow r) \wedge (\neg q \rightarrow r) \models r \vee \neg r.$$

Soluzione – Esaminiamo separatamente le due affermazioni proposte.

(i) Poiché la formula $s \wedge \neg s$ è insoddisfacibile, anche la formula $s \wedge \neg s \wedge (p \rightarrow s)$ è insoddisfacibile; pertanto qualsiasi valutazione di verità che la soddisfa (non ce ne sono!) soddisfa anche la formula $(p \rightarrow q) \wedge (\neg q \rightarrow p)$, e quindi la (i) è vera.

(ii) Poiché la formula $r \vee \neg r$ è una tautologia, essa è certamente soddisfatta da qualsiasi valutazione di verità soddisfa la formula $(p \rightarrow r) \wedge (\neg q \rightarrow r)$; pertanto, anche la (ii) è vera.

Esercizio 2

Siano h, k, t, w, x, y, z variabili proposizionali. Si stabilisca, motivando la risposta, se il seguente insieme di clausole è soddisfacibile; e nel caso che la risposta sia affermativa si trovi un'interpretazione che lo soddisfa:

$$\{\{x, y\}, \{h, t\}, \{\neg h, k, t, z\}, \{\neg w, \neg z\}, \{k, w\}, \{\neg h, \neg y\}, \{h, \neg k, \neg t, \neg z\}, \\ \{\neg k, \neg x\}, \{\neg t, z\}, \{w, x, \neg y\}\}.$$

Soluzione – Applichiamo l'algoritmo di Davis e Putnam, scegliendo come primo *pivot* una variabile proposizionale che compare in una clausola di lunghezza 2, ad esempio la x .

Pivot x :

$$\text{clausole non contenenti né } x \text{ né } \neg x: \{h, t\}, \{\neg h, k, t, z\}, \{\neg w, \neg z\}, \{k, w\}, \{\neg h, \neg y\}, \{h, \neg k, \neg t, \neg z\}, \{\neg t, z\};$$

$$\text{Ris}_x(\{x, y\}, \{\neg k, \neg x\}) = \{\neg k, y\};$$

$$\text{Ris}_x(\{w, x, \neg y\}, \{\neg k, \neg x\}) = \{\neg k, w, \neg y\};$$

$$\{\{h, t\}, \{\neg h, k, t, z\}, \{\neg w, \neg z\}, \{k, w\}, \{\neg h, \neg y\}, \{h, \neg k, \neg t, \neg z\}, \{\neg t, z\}, \{\neg k, y\}, \{\neg k, w, \neg y\}\}.$$

Pivot h :

clausole non contenenti né h né $\neg h$: $\{\neg w, \neg z\}, \{k, w\}, \{\neg t, z\}, \{\neg k, y\}, \{\neg k, w, \neg y\}$;

$\text{Ris}_h(\{h, t\}, \{\neg h, k, t, z\}) = \{k, t, z\}$;

$\text{Ris}_h(\{h, t\}, \{\neg h, \neg y\}) = \{t, \neg y\}$;

$\text{Ris}_h(\{h, \neg k, \neg t, \neg z\}, \{\neg h, k, t, z\}) = \{k, \neg k, t, \neg t, z, \neg z\}$ (si sopprime perché tautologia);

$\text{Ris}_h(\{h, \neg k, \neg t, \neg z\}, \{\neg h, \neg y\}) = \{\neg k, \neg t, \neg y, \neg z\}$;

$\{\{\neg w, \neg z\}, \{k, w\}, \{\neg t, z\}, \{\neg k, y\}, \{\neg k, w, \neg y\}, \{k, t, z\}, \{t, \neg y\}, \{\neg k, \neg t, \neg y, \neg z\}\}$

Pivot w :

clausole non contenenti né w né $\neg w$: $\{\neg t, z\}, \{\neg k, y\}, \{k, t, z\}, \{t, \neg y\}, \{\neg k, \neg t, \neg y, \neg z\}$;

$\text{Ris}_w(\{\neg w, \neg z\}, \{k, w\}) = \{k, \neg z\}$;

$\text{Ris}_w(\{\neg w, \neg z\}, \{\neg k, w, \neg y\}) = \{\neg k, \neg y, \neg z\}$;

$\{\{\neg t, z\}, \{\neg k, y\}, \{k, t, z\}, \{t, \neg y\}, \{\neg k, \neg t, \neg y, \neg z\}, \{k, \neg z\}, \{\neg k, \neg y, \neg z\}\}$.

La clausola $\{\neg k, \neg t, \neg y, \neg z\}$ si può sopprimere perché contiene l'altra clausola $\{\neg k, \neg y, \neg z\}$, quindi si considera l'insieme di clausole

$\{\{\neg t, z\}, \{\neg k, y\}, \{k, t, z\}, \{t, \neg y\}, \{k, \neg z\}, \{\neg k, \neg y, \neg z\}\}$.

Pivot t :

clausole non contenenti né t né $\neg t$: $\{\neg k, y\}, \{k, \neg z\}, \{\neg k, \neg y, \neg z\}$;

$\text{Ris}_t(\{\neg t, z\}, \{k, t, z\}) = \{k, z\}$;

$\text{Ris}_t(\{\neg t, z\}, \{t, \neg y\}) = \{\neg y, z\}$;

$\{\{\neg k, y\}, \{k, \neg z\}, \{\neg k, \neg y, \neg z\}, \{k, z\}, \{\neg y, z\}\}$.

Pivot k :

clausole non contenenti né k né $\neg k$: $\{\neg y, z\}$;

$\text{Ris}_k(\{\neg k, y\}, \{k, \neg z\}) = \{y, \neg z\}$;

$\text{Ris}_k(\{\neg k, y\}, \{k, z\}) = \{y, z\}$;

$\text{Ris}_k(\{\neg k, \neg y, \neg z\}, \{k, \neg z\}) = \{\neg y, \neg z\}$;

$\text{Ris}_k(\{\neg k, \neg y, \neg z\}, \{k, z\}) = \{\neg y, z, \neg z\}$ (si sopprime perché tautologia);

$\{\{\neg y, z\}, \{y, \neg z\}, \{y, z\}, \{\neg y, \neg z\}\}$

Pivot y :

clausole non contenenti né y né $\neg y$: non ce ne sono!

$\text{Ris}_k(\{\neg y, z\}, \{y, \neg z\}) = \{z, \neg z\}$ (si sopprime perché tautologia);

$\text{Ris}_k(\{\neg y, z\}, \{y, z\}) = \{z\}$;

$\text{Ris}_y(\{\neg y, \neg z\}, \{y, \neg z\}) = \{\neg z\}$;

$\text{Ris}_y(\{\neg y, \neg z\}, \{y, z\}) = \{\neg z, z\}$ (si sopprime perché tautologia);

$\{\{z\}, \{\neg z\}\}$

Pivot z :

clausole non contenenti né z né $\neg z$: non ce ne sono!

$\text{Ris}_z(\{z\}, \{\neg z\}) = []$;

$\{[]\}$

Avendo ottenuto la clausola vuota, possiamo concludere che \mathcal{K} non è soddisfacibile.

Esercizio 3

Siano α, β le permutazioni sull'insieme $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ così definite:

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 9 & 4 & 8 & 3 & 1 & 6 & 5 \end{pmatrix}, \quad \beta := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 6 & 9 & 1 & 7 & 8 & 3 \end{pmatrix}.$$

e sia σ la permutazione ottenuta applicando prima α e poi β .

Si scriva σ come prodotto di cicli disgiunti e si dica, motivando la risposta, se σ è una permutazione pari oppure una permutazione dispari.

Soluzione – Si ha

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 3 & 6 & 8 & 4 & 2 & 1 & 9 \end{pmatrix}$$

dunque

$$\sigma = (1\ 5\ 8)(2\ 7)(4\ 6) = (1\ 5)(1\ 8)(2\ 7)(4\ 6).$$

Poiché σ si scrive come prodotto di quattro trasposizioni, σ è una permutazione pari.

Esercizio 4

Sia $\mathbb{Z}_{11\,039}$ l'anello delle classi di resto modulo 11 039. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{11\,039}$ a cui z appartiene.

Per ciascuna delle seguenti equazioni nell'incognita x si dica quante soluzioni ha in $\mathbb{Z}_{11\,039}$:

$$[249] \cdot x = [419]; \quad [399] \cdot x = [798].$$

Soluzione – Consideriamo in primo luogo l'equazione

$$[249] \cdot x = [419].$$

Sappiamo dalla teoria che essa ha soluzione in $\mathbb{Z}_{11\,039}$ se e soltanto se il massimo comun divisore δ fra 11 039 e 249 divide 419; e in tal caso essa ha esattamente δ soluzioni.

Calcoliamo con l'algoritmo di Euclide il MCD fra 11 039 e 249:

$$\begin{aligned} 11\,039 &= 249 \cdot 44 + 83; \\ 249 &= 83 \cdot 3 + 0. \end{aligned}$$

Il massimo comun divisore fra 11 039 e 249 è dunque 83; poiché non si tratta di un divisore di 419 (infatti $419 = 83 \cdot 5 + 4$), l'equazione considerata non ha soluzione (quindi il numero delle soluzioni è zero).

Consideriamo poi l'equazione

$$[399] \cdot x = [798].$$

Sappiamo dalla teoria che essa ha soluzione in $\mathbb{Z}_{11\,039}$ se e soltanto se il massimo comun divisore δ fra 11 039 e 399 divide 798; e in tal caso essa ha esattamente δ soluzioni.

Calcoliamo con l'algoritmo di Euclide il MCD fra 11 039 e 399:

$$\begin{aligned} 11\,039 &= 399 \cdot 27 + 266; \\ 399 &= 266 \cdot 1 + 133; \\ 266 &= 133 \cdot 2 + 0. \end{aligned}$$

Il massimo comun divisore fra 11 039 e 399 è dunque 133; poiché si tratta di un divisore di 798 ($= 133 \cdot 6$), l'equazione considerata ha 133 soluzioni.

Esercizio 5

Sia \mathbb{Z}_{259} l'anello delle classi di resto modulo 259. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di \mathbb{Z}_{259} a cui z appartiene.

Per ciascuno dei seguenti elementi di \mathbb{Z}_{259} si stabilisca, motivando la risposta, se è invertibile in \mathbb{Z}_{259} e, se è invertibile, se ne trovi l'inverso:

$$[74]; \quad [102].$$

Soluzione – Sappiamo che l'elemento $[a]$ è invertibile in \mathbb{Z}_{259} se e soltanto se

$$\text{MCD}(259, a) = 1.$$

Poiché

$$\begin{aligned} 259 &= 74 \cdot 3 + 37; & 74 &= 37 \cdot 2 + 0; \\ 259 &= 102 \cdot 2 + 55; & 102 &= 55 \cdot 1 + 47; & 55 &= 47 \cdot 1 + 8; \\ & & 47 &= 8 \cdot 5 + 7; & 8 &= 7 \cdot 1 + 1; \\ & & & & 7 &= 1 \cdot 7 + 0 \end{aligned}$$

si ha che

$$\text{MCD}(259, 74) = 37 \neq 1, \quad \text{MCD}(259, 102) = 1$$

e pertanto fra i due elementi di \mathbb{Z}_{259} proposti dall'esercizio l'unico invertibile è $[102]$.

Per trovare l'inverso di $[102]$ in \mathbb{Z}_{259} dobbiamo risolvere l'equazione

$$[102] \cdot [x] = [1]$$

in \mathbb{Z}_{259} , che ci riconduce all'equazione diofantina

$$102x - 259y = 1$$

della quale vogliamo trovare una soluzione nella x . A tale scopo basta scrivere l'identità di Bezout, che si ricava dai calcoli già fatti per trovare il $\text{MCD}(259, 102)$. Si ha dunque

$$\begin{aligned} 1 &= 8 - 7 = 8 - (47 - 8 \cdot 5) = 8 \cdot 6 + 47 \cdot (-1) = (55 - 47) \cdot 6 + 47 \cdot (-1) = \\ &= 55 \cdot 6 + 47 \cdot (-7) = 55 \cdot 6 + (102 - 55) \cdot (-7) = 55 \cdot 13 + 102 \cdot (-7) = \\ &= (259 - 102 \cdot 2) \cdot 13 + 102 \cdot (-7) = 259 \cdot 13 + 102 \cdot (-33) \end{aligned}$$

cosicché l'inverso di $[102]$ in \mathbb{Z}_{259} è $[-33]$ ($= [226]$).

Esercizio 6

Con riferimento all'anello $\mathbb{Z}_{25\,625}$ delle classi di resto modulo 25 625, si dica, esprimendo ogni risposta in base *quindici*:

- quanti sono gli elementi invertibili;
- quanti sono i divisori dello zero.

Soluzione – Un elemento $[a]$ di $\mathbb{Z}_{25\,625}$ è invertibile se e soltanto se

$$\text{MCD}(a, 25\,625) = 1$$

e quindi il numero degli elementi invertibili di $\mathbb{Z}_{25\,625}$ è

$$\varphi(25\,625) = \varphi(5^4 \cdot 41) = \varphi(5^4) \cdot \varphi(41) = 5^3 \cdot (5 - 1) \cdot (41 - 1) = 20\,000.$$

Scriviamo questo numero in base *quindici*, eseguendo successive divisioni per 15:

$$20\,000 = 15 \cdot 1\,333 + 5;$$

$$1\,333 = 15 \cdot 88 + 13;$$

$$88 = 15 \cdot 5 + 13;$$

$$5 = 15 \cdot 0 + 5.$$

Pertanto, *ventimila* in base *quindici* si scrive 5DD5.

I divisori dello zero di $\mathbb{Z}_{25\,625}$ sono quegli elementi che sono diversi da zero e non sono invertibili; dunque il loro numero è $25\,625 - 1 - 20\,000 = 5\,624$.

Scriviamo questo numero in base *quindici*, eseguendo successive divisioni per 15:

$$5\,624 = 15 \cdot 374 + 14;$$

$$374 = 15 \cdot 24 + 14;$$

$$24 = 15 \cdot 1 + 9;$$

$$1 = 15 \cdot 0 + 1.$$

Pertanto, *cinquemilaseicentoventiquattro* in base *quindici* si scrive 19EE.

Esercizio 7

Per ciascuna delle due seguenti affermazioni si dica se è vera per ogni $n \in \mathbb{N}$ (richiamando esplicitamente il motivo per cui lo è) oppure è falsa per qualche $n \in \mathbb{N}$ (presentando in questo caso un controesempio):

(i) se n è un numero dispari multiplo di 14 allora $n^2 - 1$ è multiplo di 13;

(ii) se n divide un prodotto ab (con $a, b \in \mathbb{N}$), allora n divide a oppure n divide b .

Soluzione –

(i) Ogni multiplo di 14 è pari, e quindi non è dispari; dunque la condizione “ n è un numero dispari multiplo di 14” è certamente falsa, qualunque sia $n \in \mathbb{N}$. Pertanto l’implicazione considerata è certamente vera, qualunque sia $n \in \mathbb{N}$.

(ii) L’affermazione è falsa, come si vede considerando $n := 6$, $a := 4$ e $b := 9$.

Esercizio 8

La password di accesso a una banca dati è una sequenza ordinata di nove lettere dell’alfabeto italiano (21 caratteri) che soddisfa tutte le seguenti condizioni:

– le consonanti sono quattro o cinque, tutte diverse fra loro e disposte, da sinistra a destra, in ordine alfabetico;

– le vocali possono essere anche ripetute ma anch’esse devono essere disposte, da sinistra a destra, in ordine alfabetico.

Si dica, motivando la risposta, quante sono in tutto le possibili password.

Soluzione – Conviene distinguere tra il caso in cui le consonanti sono quattro e il caso in cui le consonanti sono cinque: essi si escludono a vicenda, quindi possiamo contare separatamente le password che rientrano nel primo caso e quelle che rientrano nel secondo caso e poi applicare il principio di addizione.

Consideriamo il caso in cui le consonanti sono quattro. Il loro posto si può scegliere in $\binom{9}{4} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2} = 9 \cdot 7 \cdot 2 = 126$ modi diversi (e determina automaticamente il posto delle cinque vocali); le quattro consonanti (il cui ordine è determinato dalle condizioni del problema) possono essere scelte in $\binom{16}{4} = \frac{16 \cdot 15 \cdot 14 \cdot 13}{4 \cdot 3 \cdot 2} = 2 \cdot 5 \cdot 14 \cdot 13 = 1\,820$ modi diversi; le cinque vocali (il cui ordine è anch'esso determinato dalle condizioni del problema) possono essere scelte in $\binom{5+5-1}{5} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2} = 9 \cdot 2 \cdot 7 = 126$ modi diversi. Applicando il principio di moltiplicazione, si trova che le password che rientrano nel primo caso sono

$$126 \cdot 1\,820 \cdot 126 = 28\,894\,320.$$

Consideriamo poi il caso in cui le consonanti sono cinque. Il loro posto si può scegliere in $\binom{9}{5} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2} = 9 \cdot 2 \cdot 7 = 126$ modi diversi (e determina automaticamente il posto delle quattro vocali); le cinque consonanti (il cui ordine è determinato dalle condizioni del problema) possono essere scelte in $\binom{16}{5} = \frac{16 \cdot 15 \cdot 14 \cdot 13 \cdot 12}{5 \cdot 4 \cdot 3 \cdot 2} = 2 \cdot 14 \cdot 13 \cdot 12 = 4\,368$ modi diversi; le quattro vocali (il cui ordine è anch'esso determinato dalle condizioni del problema) possono essere scelte in $\binom{5+4-1}{4} = \frac{8 \cdot 7 \cdot 6 \cdot 5}{4 \cdot 3 \cdot 2} = 2 \cdot 7 \cdot 5 = 70$ modi diversi. Applicando il principio di moltiplicazione, si trova che le password che rientrano nel secondo caso sono

$$126 \cdot 4\,368 \cdot 70 = 38\,525\,760.$$

Applicando infine il principio di addizione, si ottiene che il numero totale delle possibili password è

$$28\,894\,320 + 38\,525\,760 = 67\,420\,080.$$