

Prova “*in itinere*” per “Matematica Discreta e Logica” – primo appello**31.1.2020****FILA “A”**Esercizio 1

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

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

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

Soluzione – Esaminiamo separatamente le due affermazioni proposte.

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

(ii) Poiché la formula $q \vee \neg q$ è una tautologia, essa è certamente soddisfatta da qualsiasi valutazione di verità soddisfi la formula $(p \rightarrow s) \wedge (\neg q \rightarrow r)$; 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:

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

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 h .

Pivot h :

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

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

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

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

Pivot t :

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

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

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

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

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

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

Pivot w :

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

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

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

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

Pivot y :

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

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

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

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

La clausola $\{\neg k, \neg x, z\}$ si può sopprimere perché contiene l'altra clausola $\{\neg k, \neg x\}$, quindi si considera l'insieme di clausole

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

Pivot x :

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

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

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

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

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

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

Pivot k :

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

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

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

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

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

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

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:

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

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

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

dunque

$$\sigma = (2\ 4)(3\ 6\ 8)(5\ 9) = (2\ 4)(3\ 6)(3\ 8)(5\ 9).$$

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

Esercizio 4

Sia \mathbb{Z}_{12901} l'anello delle classi di resto modulo 12901. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di \mathbb{Z}_{12901} a cui z appartiene.

Per ciascuna delle seguenti equazioni nell'incognita x si dica quante soluzioni ha in \mathbb{Z}_{12901} :

$$[291] \cdot x = [489]; \quad [399] \cdot x = [931].$$

Soluzione – Consideriamo in primo luogo l'equazione

$$[291] \cdot x = [489].$$

Sappiamo dalla teoria che essa ha soluzione in \mathbb{Z}_{12901} se e soltanto se il massimo comun divisore δ fra 12901 e 291 divide 489; e in tal caso essa ha esattamente δ soluzioni.

Calcoliamo con l'algoritmo di Euclide il MCD fra 12901 e 291:

$$\begin{aligned} 12901 &= 291 \cdot 44 + 97; \\ 291 &= 97 \cdot 3 + 0. \end{aligned}$$

Il massimo comun divisore fra 12901 e 291 è dunque 97; poiché non si tratta di un divisore di 489 (infatti $489 = 97 \cdot 5 + 4$), l'equazione considerata non ha soluzione (quindi il numero delle soluzioni è zero).

Consideriamo poi l'equazione

$$[399] \cdot x = [931].$$

Sappiamo dalla teoria che essa ha soluzione in \mathbb{Z}_{12901} se e soltanto se il massimo comun divisore δ fra 12901 e 399 divide 931; e in tal caso essa ha esattamente δ soluzioni.

Calcoliamo con l'algoritmo di Euclide il MCD fra 12901 e 399:

$$\begin{aligned} 12901 &= 399 \cdot 32 + 133; \\ 399 &= 133 \cdot 3 + 0. \end{aligned}$$

Il massimo comun divisore fra 12901 e 399 è dunque 133; poiché si tratta di un divisore di 931 ($= 133 \cdot 7$), l'equazione considerata ha 133 soluzioni.

Esercizio 5

Sia \mathbb{Z}_{329} l'anello delle classi di resto modulo 329. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di \mathbb{Z}_{329} a cui z appartiene.

Per ciascuno dei seguenti elementi di \mathbb{Z}_{329} si stabilisca, motivando la risposta, se è invertibile in \mathbb{Z}_{329} e, se è invertibile, se ne trovi l'inverso:

$$[94]; \quad [100].$$

Soluzione – Sappiamo che l'elemento $[a]$ è invertibile in \mathbb{Z}_{329} se e soltanto se

$$\text{MCD}(329, a) = 1.$$

Poiché

$$\begin{aligned} 329 &= 94 \cdot 3 + 47; & 94 &= 47 \cdot 2 + 0; \\ 329 &= 100 \cdot 3 + 29; & 100 &= 29 \cdot 3 + 13; & 29 &= 13 \cdot 2 + 3; \\ & & 13 &= 3 \cdot 4 + 1; & 3 &= 1 \cdot 3 + 0 \end{aligned}$$

si ha che

$$\text{MCD}(329, 94) = 47 \neq 1, \quad \text{MCD}(329, 100) = 1$$

e pertanto fra i due elementi di \mathbb{Z}_{329} proposti dall'esercizio l'unico invertibile è $[100]$.

Per trovare l'inverso di $[100]$ in \mathbb{Z}_{329} dobbiamo risolvere l'equazione

$$[100] \cdot [x] = [1]$$

in \mathbb{Z}_{329} , che ci riconduce all'equazione diofantina

$$100x - 329y = 1$$

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 $\text{MCD}(329, 100)$. Si ha dunque

$$\begin{aligned} 1 &= 13 - 3 \cdot 4 = 13 - (29 - 13 \cdot 2) \cdot 4 = 13 \cdot 9 + 29 \cdot (-4) = \\ &= (100 - 29 \cdot 3) \cdot 9 + 29 \cdot (-4) = 100 \cdot 9 + 29 \cdot (-31) = \\ &= 100 \cdot 9 + (329 - 100 \cdot 3) \cdot (-31) = 329 \cdot (-31) + 100 \cdot 102 \end{aligned}$$

cosicché l'inverso di $[100]$ in \mathbb{Z}_{329} è $[102]$.

Esercizio 6

Con riferimento all'anello \mathbb{Z}_{23125} delle classi di resto modulo 23125, 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}_{23125} è invertibile se e soltanto se

$$\text{MCD}(a, 23125) = 1$$

e quindi il numero degli elementi invertibili di \mathbb{Z}_{23125} è

$$\varphi(23125) = \varphi(5^4 \cdot 37) = \varphi(5^4) \cdot \varphi(37) = 5^3 \cdot (5 - 1) \cdot (37 - 1) = 18000.$$

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

$$18\,000 = 15 \cdot 1\,200 + 0;$$

$$1\,200 = 15 \cdot 80 + 0;$$

$$80 = 15 \cdot 5 + 5;$$

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

Pertanto, *diciottomila* in base quindici si scrive 5500.

I divisori dello zero di $\mathbb{Z}_{23\,125}$ sono quegli elementi che sono diversi da zero e non sono invertibili; dunque il loro numero è $23\,125 - 1 - 18\,000 = 5\,124$.

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

$$5\,124 = 15 \cdot 341 + 9;$$

$$341 = 15 \cdot 22 + 11;$$

$$22 = 15 \cdot 1 + 7;$$

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

Pertanto, *cinquemilacentoveventiquattro* in base quindici si scrive 17B9.

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 12 allora $n^2 - 1$ è multiplo di 7;

(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 12 è pari, e quindi non è dispari; dunque la condizione “ n è un numero dispari multiplo di 12” 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 sette lettere dell’alfabeto italiano (21 caratteri) che soddisfa tutte le seguenti condizioni:

– le consonanti sono tre o quattro, 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 – Convieni distinguere tra il caso in cui le consonanti sono tre e il caso in cui le consonanti sono quattro: 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 tre. Il loro posto si può scegliere in $\binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 35$ modi diversi (e determina automaticamente il posto delle quattro vocali); le tre consonanti (il cui ordine è determinato dalle condizioni del problema) possono essere scelte in $\binom{16}{3} = \frac{16 \cdot 15 \cdot 14}{3 \cdot 2} = 8 \cdot 5 \cdot 14 = 560$ modi diversi; le quattro vocali (il cui ordine è anch'esso determinato dalle condizioni del problema) possono essere scelte in $\binom{5+4-1}{4} = \frac{8 \cdot 7 \cdot 6 \cdot 5}{4 \cdot 3 \cdot 2} = 7 \cdot 2 \cdot 5 = 70$ modi diversi. Applicando il principio di moltiplicazione, si trova che le password che rientrano nel primo caso sono

$$35 \cdot 560 \cdot 70 = 1\,372\,000.$$

Consideriamo poi il caso in cui le consonanti sono quattro. Il loro posto si può scegliere in $\binom{7}{4} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 35$ modi diversi (e determina automaticamente il posto delle tre 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 tre vocali (il cui ordine è anch'esso determinato dalle condizioni del problema) possono essere scelte in $\binom{5+3-1}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 7 \cdot 5 = 35$ modi diversi. Applicando il principio di moltiplicazione, si trova che le password che rientrano nel secondo caso sono

$$35 \cdot 1\,820 \cdot 35 = 2\,295\,500.$$

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

$$1\,372\,000 + 2\,295\,500 = 3\,667\,500.$$