UNIVERSITA' DI FIRENZE – CDL IN INFORMATICA – A. A. 2019-2020
Prova scritta "in presenza" di "Matematica Discreta e Logica" del giorno 3 settembre 2020

Soluzione degli esercizi

Esercizio 1

Sia n il numero che in base *quindici* si scrive

$$9\,\mathrm{C}30\,.$$

Si scriva n in base *quattordici*.

Soluzione – In base *dieci*, si ha

$$n = 3 \cdot 15 + 12 \cdot 15^2 + 9 \cdot 15^3 = 3 \cdot 15 + 12 \cdot 225 + 9 \cdot 3375 =$$
$$= 45 + 2\,700 + 30\,375 = 33\,120\,.$$

Per scrivere n in base *quattordici*, effettuiamo divisioni successive per *quattordici* come segue (la notazione è in base *dieci*):

$33\,120 = 2\,365 \cdot 14 + 10\,;$ $\quad 2\,365 = 168 \cdot 14 + 13\,;$

$168 = 12 \cdot 14 + 0\,;$ $\quad 12 = 0 \cdot 14 + 12$

e prendiamo (in ordine inverso) le "cifre" che rappresentano i resti ottenuti. Si ottiene dunque che

$$n = \mathrm{C0DA}_{\textit{quattordici}}\,.$$

Esercizio 2

Siano α, β le permutazioni sull'insieme {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12} così definite:

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 7 & 2 & 5 & 9 & 12 & 8 & 4 & 3 & 10 & 1 & 11 \end{pmatrix},$$

$$\beta := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 10 & 9 & 7 & 3 & 2 & 4 & 6 & 5 & 1 & 12 & 11 \end{pmatrix}$$

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

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 4 & 10 & 3 & 5 & 11 & 6 & 7 & 9 & 1 & 8 & 12 \end{pmatrix}$$

dunque

$$\sigma = (1\ \ 2\ \ 4\ \ 3\ \ 10)\,(6\ \ 11\ \ 8\ \ 7) = (1\ \ 2)\,(1\ \ 4)\,(1\ \ 3)\,(1\ \ 10)\,(6\ \ 11)\,(6\ \ 8)\,(6\ \ 7)\,.$$

Poiché σ si scrive come prodotto di 7 trasposizioni, σ è una permutazione dispari.

Esercizio 3

Sia $\mathbb{Z}_{847}$ l'anello delle classi di resto modulo 847. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{847}$ a cui z appartiene. Per ciascuno dei seguenti elementi di $\mathbb{Z}_{847}$ si stabilisca, motivando la risposta, se è invertibile in $\mathbb{Z}_{847}$ e nel caso che la risposta sia affermativa si dica quanti inversi ha e si determini esplicitamente ogni suo inverso:

$$[56], \quad [256], \quad [319].$$

Soluzione — Si ha

$$847 = 7 \cdot 11^2, \quad 56 = 2^3 \cdot 7, \quad 256 = 2^8, \quad 319 = 11 \cdot 29$$

e dunque

$$\text{MCD}(847, 56) = 7 \neq 1, \quad \text{MCD}(847, 256) = 1, \quad \text{MCD}(847, 319) = 11 \neq 1.$$

Pertanto fra gli elementi di $\mathbb{Z}_{847}$ proposti dall'esercizio l'unico invertibile è $[256]$. In un qualsiasi anello se un elemento è invertibile esso ha un solo inverso; per trovare l'inverso di $[256]$ in $\mathbb{Z}_{847}$ dobbiamo risolvere l'equazione

$$[256] \cdot [x] = [1]$$

in $\mathbb{Z}_{847}$, che ci riconduce all'equazione diofantina

$$256\, x + 847\, y = 1$$

della quale vogliamo trovare una soluzione nella x. A tale scopo basta scrivere l'identità di Bezout, che si ricava dall'algoritmo di Euclide applicato alla coppia $(847,\ 256)$. Si ha

$$847 = 256 \cdot 3 + 79\,; \qquad 256 = 79 \cdot 3 + 19\,;$$

$$79 = 19 \cdot 4 + 3\,; \qquad 19 = 3 \cdot 6 + 1\,;$$

$$3 = 1 \cdot 3 + 0\,.$$

Pertanto

$$1 = 19 - 3 \cdot 6 = 19 - (79 - 19 \cdot 4) \cdot 6 = 19 \cdot 25 - 79 \cdot 6 = (256 - 79 \cdot 3) \cdot 25 - 79 \cdot 6 =$$

$$= 256 \cdot 25 - 79 \cdot 81 = 256 \cdot 25 - (847 - 256 \cdot 3) \cdot 81 = 256 \cdot 268 - 847 \cdot 81$$

e dunque l'inverso di $[256]$ in $\mathbb{Z}_{847}$ è $[268]$.

Esercizio 4

Sia $\mathbb{Z}_{6413}$ l'anello delle classi di resto modulo $6\,413$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{6413}$ a cui z appartiene.
Si dica, motivando la risposta, quanti sono i numeri interi positivi $x \in \mathbb{Z}^+$ per i quali

$$[52]^x = [1]$$

e, se ne esistono, se ne trovino almeno due.

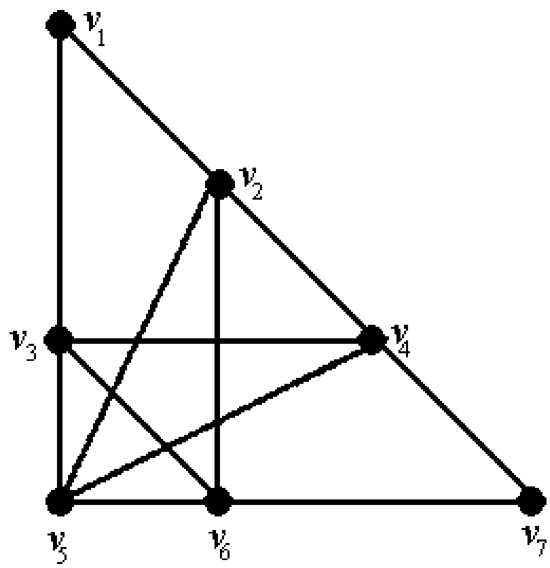
Soluzione — Per affrontare questo tipo di problemi conviene utilizzare il teorema di Euler-Fermat, in base al quale se sono dati $[a]$ e $[1]$ in $\mathbb{Z}_n$ l'equazione $[a]^x = [1]$ ha soluzione in $\mathbb{Z}^+$ se e soltanto se $\text{MCD}(a, n) = 1$. In tal caso, l'equazione ha infinite soluzioni e ogni numero intero positivo della forma $k \cdot \varphi(n)$, con $k \in \mathbb{Z}^+$, è soluzione.

Dobbiamo dunque calcolare il massimo comun divisore fra $6\,413$ e 52. In questo caso conviene fattorizzare i due numeri, perché se ci sono soluzioni vorremo calcolare $\varphi(6\,413)$.

Si ha $6\,413 = 11^2 \cdot 53$, $52 = 2^2 \cdot 13$, quindi è chiaro che $\mathrm{MCD}(6\,413, 52) = 1$. Una soluzione dell'equazione proposta è dunque $\varphi(6\,413) = \varphi(11^2 \cdot 53) = \varphi(11^2) \cdot \varphi(53) = 110 \cdot 52 = 5\,720$. Un'altra soluzione è, ad esempio, $2 \cdot 5\,720 = 11\,440$.

Esercizio 5

Sia $\mathcal{G}$ il grafo senza orientamento con 7 vertici ($v_1, v_2, v_3, v_4, v_5, v_6$ e v_7), qui disegnato:



Si dica, motivando ciascuna risposta:

(i) se $\mathcal{G}$ è semplice;

(ii) che grado ha ciascun vertice di $\mathcal{G}$, e che legame c'è fra la somma di tutti i gradi dei vertici di $\mathcal{G}$ e il numero dei lati di $\mathcal{G}$;

(iii) se $\mathcal{G}$ è piano;

(iv) se $\mathcal{G}$ è euleriano;

(v) se $\mathcal{G}$ è hamiltoniano.

Nelle risposte, qualora si voglia far riferimento a cammini di $\mathcal{G}$, si indichi con ℓ_{ij} il lato di estremi v_i e v_j .

Soluzione $-$ $\mathcal{G}$ è semplice perché non ci sono lati fra loro paralleli.

I vertici v_2, v_3, v_4, v_5 e v_6 hanno (ciascuno) grado 4; i vertici v_1 e v_7 hanno (ciascuno) grado 2. La somma di tutti i gradi dei vertici di $\mathcal{G}$ è 24, cioè esattamente il doppio del numero dei lati di $\mathcal{G}$.

Il grafo $\mathcal{G}$ non è piano perché è (isomorfo a) una suddivisione del grafo completo $\mathcal{K}_5$ (che si ottiene da $\mathcal{G}$ sopprimendo i vertici v_1 e v_7, sostituendo un unico lato ℓ_{23} ai lati ℓ_{21} e ℓ_{13}, e infine sostituendo un unico lato ℓ_{46} ai lati ℓ_{47} e ℓ_{76}).

Il grafo $\mathcal{G}$ è euleriano, perché è connesso e ogni suo vertice ha grado pari.

Infine, il grafo $\mathcal{G}$ è hamiltoniano perché possiede il seguente ciclo hamiltoniano:

$$v_1,\ \ell_{12},\ v_2,\ \ell_{24},\ v_4,\ \ell_{47},\ v_7,\ \ell_{76},\ v_6,\ \ell_{65},\ v_5,\ \ell_{53},\ v_3,\ \ell_{31},\ v_1\ .$$

Esercizio 6

Siano x, y, z, t, u, w variabili proposizionali. Si stabilisca, motivando la risposta, se il seguente insieme ***K*** di clausole è soddisfacibile; e, nel caso che la risposta sia affermativa, si determini una valutazione di verità che lo soddisfa:

$$\boldsymbol{K} := \{\{x,y\}, \{\neg x,y\}, \{x,\neg z\}, \{\neg x,t\}, \{\neg y,t\}, \{t,z\}, \{\neg t,\neg w\}, \{y,\neg t,u\}, \\ \{u,w,z\}, \{\neg u,w,\neg z\}, \{\neg u,\neg w,z\}, \{w,t,\neg z\}\}\,.$$

Soluzione – Applichiamo l'algoritmo di Davis-Putnam.

Pivot x:

clausole non contenenti né x né $\neg x$:

$$\{\neg y,t\}, \{t,z\}, \{\neg t,\neg w\}, \{y,\neg t,u\}, \{u,w,z\}, \{\neg u,w,\neg z\}, \{\neg u,\neg w,z\}, \{w,t,\neg z\}\,;$$

Ris$_x(\{x,y\}, \{\neg x,y\}) = \{y\}$;
Ris$_x(\{x,y\}, \{\neg x,t\}) = \{y,t\}$ (si sopprime perché contiene il precedente risolvente) ;
Ris$_x(\{x,\neg z\}, \{\neg x,y\}) = \{\neg z,y\}$ (si sopprime perché contiene il primo risolvente ottenuto) ;
Ris$_x(\{x,\neg z\}, \{\neg x,t\}) = \{\neg z,t\}$;

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

La clausola $\{y,\neg t,u\}$ può essere soppressa perché contiene la clausola $\{y\}$ (cfr. oss. 2.9.7 negli appunti di logica), cosicché siamo ricondotti a considerare il seguente insieme di clausole:

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

Pivot y:

clausole non contenenti né y né $\neg y$:

$$\{t,z\}, \{\neg t,\neg w\}, \{u,w,z\}, \{\neg u,w,\neg z\}, \{\neg u,\neg w,z\}, \{w,t,\neg z\}, \{\neg z,t\};$$

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

$$\{\{t,z\}, \{\neg t,\neg w\}, \{u,w,z\}, \{\neg u,w,\neg z\}, \{\neg u,\neg w,z\}, \{w,t,\neg z\}, \{\neg z,t\}, \{t\}\}$$

Le clausole $\{t,z\}$, $\{w,t,\neg z\}$ e $\{\neg z,t\}$ possono essere soppresse perché contengono la clausola $\{t\}$. Siamo dunque ricondotti a considerare il seguente insieme di clausole:

$$\{\{\neg t,\neg w\}, \{u,w,z\}, \{\neg u,w,\neg z\}, \{\neg u,\neg w,z\}, \{t\}\}$$

Pivot z:

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

Ris$_z(\{u,w,z\}, \{\neg u,w,\neg z\}) = \{u,w,\neg u\}$ (si sopprime perché tautologia) ;

Ris$_z(\{\neg u,\neg w,z\}, \{\neg u,w,\neg z\}) = \{\neg u,\neg w,w\}$ (si sopprime perché tautologia) ;

$$\{\{\neg t,\neg w\}, \{t\}\}$$

Pivot t:

Ris$_t(\{\neg t,\neg w\}, \{t\}) = \{\neg w\}$;

$$\{\{t\}\}$$

Pivot t:

non ci sono risolventi da calcolare!

$$\{\}$$

Avendo ottenuto l'insieme vuoto di clausole, possiamo concludere che ***K*** è soddisfacibile. Una valutazione di verità v che soddisfa ***K*** si costruisce (procedendo "a ritroso" nell'assegnazione del valore di v sulle variabili proposizionali) ponendo

$$v(t) := 1\,; \quad v(w) := 0\,; \quad v(u) := 0\,; \quad v(z) := 1\,; \quad v(y) := 1\,; \quad v(x) := 1\,.$$

Esercizio 7

Sia $\mathcal{L}$ un linguaggio della logica dei predicati con un simbolo di costante (c) e due simboli di predicato unari (P, Q). Sia x una variabile individuale di $\mathcal{L}$.

Si stabilisca, motivando la risposta, se in $\mathcal{L}$

$$(\forall x)\neg \mathrm{P}(x) \wedge (\exists x)\mathrm{P}(x) \vDash \mathrm{Q}(c) \wedge \neg \mathrm{Q}(c)\,.$$

Soluzione – La formula $\mathrm{Q}(c) \wedge \neg \mathrm{Q}(c)$ è conseguenza logica della formula $(\forall x)\neg \mathrm{P}(x) \wedge (\exists x)\mathrm{P}(x)$ se e soltanto se la formula

$$\varphi := (\forall x)\neg \mathrm{P}(x) \wedge (\exists x)\mathrm{P}(x) \wedge \neg\big(\mathrm{Q}(c) \wedge \neg \mathrm{Q}(c)\big)$$

è insoddisfacibile. Trasformiamo φ in una formula logicamente equivalente in forma normale prenessa:

$$\varphi \equiv (\forall x)\neg \mathrm{P}(x) \wedge (\exists y)\mathrm{P}(y) \wedge \big(\neg \mathrm{Q}(c) \vee \mathrm{Q}(c)\big) \equiv (\exists y)(\forall x)\big(\neg \mathrm{P}(x) \wedge \mathrm{P}(y) \wedge \big(\neg \mathrm{Q}(c) \vee \mathrm{Q}(c)\big)\big)$$

La formula così ottenuta si può skolemizzare introducendo nel linguaggio un simbolo di costante k, sopprimendo il quantificatore esistenziale $\exists y$ e sostituendo ovunque il simbolo di costante k alla variabile individuale y. Si ottiene la formula

$$(\forall x)\big(\neg \mathrm{P}(x) \wedge \mathrm{P}(k) \wedge \big(\neg \mathrm{Q}(c) \vee \mathrm{Q}(c)\big)\big)$$

che dà luogo allo schema di clausole

$$\big\{\{\neg \mathrm{P}(x)\},\, \{\mathrm{P}(k)\},\, \{\neg \mathrm{Q}(c), \mathrm{Q}(c)\}\big\}\,.$$

Poiché l'universo di Herbrand consiste dei soli simboli di costante c e k, si ottiene lo schema di clausole

$$\big\{\{\neg \mathrm{P}(c)\},\, \{\neg \mathrm{P}(k)\},\, \{\mathrm{P}(k)\},\, \{\neg \mathrm{Q}(c), \mathrm{Q}(c)\}\big\}$$

che è soddisfacibile se e soltanto se lo è la φ. Poiché abbiamo un numero finito di clausole, possiamo applicare l'algoritmo di Davis e Putnam!

Sopprimiamo la clausola $\{\neg \mathrm{Q}(c), \mathrm{Q}(c)\}$ che è una tautologia, e consideriamo l'insieme

$$\big\{\{\neg \mathrm{P}(c)\},\, \{\neg \mathrm{P}(k)\},\, \{\mathrm{P}(k)\}\big\}$$

Pivot $\mathrm{P}(k)$:

clausole non contenenti né $\mathrm{P}(k)$ né $\neg \mathrm{P}(k)$: $\neg \mathrm{P}(c)$.

$\mathrm{Ris}_{\mathrm{P}(k)}(\{\neg \mathrm{P}(k)\}, \{\mathrm{P}(k)\}) = []$;

$$\big\{\{\neg \mathrm{P}(c)\},\, []\big\}$$

Poiché abbiamo ottenuto la clausola vuota, la formula da cui siamo partiti non è soddisfacibile e quindi $\mathrm{Q}(c) \wedge \neg \mathrm{Q}(c)$ è effettivamente conseguenza logica di $(\forall x)\neg \mathrm{P}(x) \wedge (\exists x)\mathrm{P}(x)$.