Corso di Studi in Informatica
Matematica Discreta

Prova scritta 19 gennaio 2017 – Versione B

COGNOME ..... **NOME** .....

MATRICOLA .....

Rispondere a ciascuna domanda, motivando adeguatamente le risposte. Per essere sufficiente un compito deve raggiungere almeno 18 punti.

Esercizio 1 (11 punti)**.** Viene formato un gruppo di lavoro costituito da 15 informatici per un progetto europeo a cui partecipano Albania, Danimarca, Grecia, Olanda e Spagna.

a) Il gruppo di lavoro sarà indicato con una sigla formata dalle 5 iniziali A,D,G,O,S delle nazioni coinvolte. Quante sono le possibili sigle?

b) Quante diverse distribuzioni per nazionalità può avere un tale gruppo se si richiede che sia presente almeno un membro per ciascuna nazione partecipante?

c) Una volta scelto il gruppo dei 15 informatici, si provvede ad attribuire i compiti: 7 di loro lavoreranno al sottoprogetto 1, 5 al sottoprogetto 2, i tre rimanenti ricopriranno il ruolo di coordinatore tra i due progetti, di responsabile del budget e di responsabile della presentazione dei risultati. In quanti modi si possono attribuire i compiti?

Soluzione.

a) Le sigle possibili sono tante quante le permutazioni delle lettere, quindi $5! = 120$.

b) Dovendo esservi almeno un rappresentante di ciascuna delle 5 nazioni, la scelta si riduce ai rappresentanti per $10 = 15 - 5$ membri. Potendosi prendere, su questi 10, un numero arbitrario di rappresentanti di ciascuna nazionalità il numero totale delle distribuzioni è

$$\binom{10+5-1}{5-1} = \binom{14}{4} = \frac{1}{4!}14 \cdot 13 \cdot 12 \cdot 11 = 1001.$$

c) Ci sono da scegliere 7 membri su 15 per il sottoprogetto 1, 5 membri sui restanti 8 per il sottoprogetto 2, mentre gli ultimi 3 si possono permutare a piacere nelle restanti posizioni. Quindi il numero totale delle attribuzioni compiti è

$$\binom{15}{7}\binom{8}{5}3! = \frac{15!}{8! \cdot 7!}\frac{8!}{5! \cdot 3!}3! = \frac{15!}{5! \cdot 7!} = 2162160.$$

Esercizio 2 (11 punti)**.** Si considerino la permutazioni di S_7:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 3 & 4 & 5 & 6 & 2 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 6 & 3 & 5 & 7 \end{pmatrix}$$

a) Determinare tipo e parità di σ e τ.

b) Determinare le composizioni $\tau \circ \sigma$ e $\sigma \circ \tau$.

c) Verificare che l'insieme $H = \{\sigma^h \tau^k \mid h, k \in \mathbb{Z}\}$ è un sottogruppo di S_7 e che si tratta di un gruppo ciclico.

Soluzione.

a) Si ha che $\sigma = (1\ 7\ 2)$ è un 3-ciclo, quindi pari, e $\tau = (3\ 4\ 6\ 5)$ è un 4-ciclo quindi dispari.

b) Poichè σ e τ sono cicli disgiunti si ha

$$\tau \circ \sigma = \sigma \circ \tau = (1\ 7\ 2)(3\ 4\ 6\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 4 & 6 & 3 & 5 & 2 \end{pmatrix}$$

c) Poichè σ e τ commutano, per qualunque $h, h', k, k' \in \mathbb{Z}$ si ha

$$\sigma^h \tau^k (\sigma^{h'} \tau^{k'})^{-1} = \sigma^h \tau^k \sigma^{-h'} \tau^{-k'} = \sigma^{h-h'} \tau^{k-k'} \in H$$

e quindi H è un sottogruppo perchè soddisfa il criterio.

Osserviamo che siccome σ ha periodo 3 e τ ha periodo 4, vale l'uguaglianza $\sigma^h \tau^k = \sigma^{h'} \tau^{k'}$ esattamente quando $h \equiv h' \bmod 3$ e $k \equiv k' \bmod 4$ per un totale di 12 elementi in H. Ora l'elemento $\sigma\tau$ è in H e ha periodo $12 = \mathrm{mcm}(3, 4)$, quindi tutte le sue potenze esauriscono gli elementi di H ovvero $\langle \sigma\tau \rangle = H$.

Esercizio 3 (11 punti)**.**

a) Determinare MCD e identità di Bézout dei numeri $m = 3973$ e $n = 1853$.

b) Determinare le ultime due cifre decimali del numero 41803^{1003}.

c) Determinare il numero di elementi invertibili dei due anelli prodotto $A = \mathbb{Z}_8 \times \mathbb{Z}_{15}$ e $R = \mathbb{Z}_{12} \times \mathbb{Z}_{10}$. Stabilire se $g\colon A \to R$ data da $g([h]_8, [k]_{15}) = ([3h]_{12}, [2k]_{10})$ è un omomorfismo di anelli e in caso affermativo determinare $\ker(g)$ e $\mathrm{Im}(g)$.

Soluzione.

a) Si ha

$$\begin{aligned} 3973 &= 2 \cdot 1853 + 267 \\ 1853 &= 6 \cdot 267 + 16 \\ 267 &= 1 \cdot 251 + 16 \\ 251 &= 15 \cdot 16 + 11 \\ 16 &= 1 \cdot 11 + 5 \\ 11 &= 2 \cdot 5 + 1. \end{aligned}$$

Quindi $\mathrm{MCD}(3973, 1853) = 1$. Risalendo dal basso e sostituendo i valori precedenti

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 3 \cdot 11 - 2 \cdot 16 \\ &= 3 \cdot 251 - 47 \cdot 16 \\ &= 50 \cdot 251 - 47 \cdot 267 \\ &= 50 \cdot 1853 - 347 \cdot 267 \\ &= 744 \cdot 1853 - 347 \cdot 3973. \end{aligned}$$

dove l'ultima uguaglianza realizza l'identità di Bezout.

b) Siccome $\mathrm{MCD}(41803, 100) = \mathrm{MCD}(3, 100) = 1$ e $\varphi(100) = \varphi(4)\varphi(25) = 2 \cdot 20 = 40$ possiamo applicare il teorema di Lagrange per cui $41803^{40} \equiv 3^{40} \equiv 1 \bmod 100$. Osservato che $1003 = 25 \cdot 40 + 3$ si ottiene

$$41803^{1003} \equiv 3^{1003} \equiv (3^{40})^{25} 3^3 \equiv 27 \bmod 100.$$

c) Ricordando che per anelli A e B si ha sempre $(A \times B)^\times = A^\times \times B^\times$ si ha subito $|(\mathbb{Z}_8 \times \mathbb{Z}_{15})^\times| = \varphi(8)\varphi(15) = 4 \cdot 8 = 32$ e $|(\mathbb{Z}_{12} \times \mathbb{Z}_{10})^\times| = \varphi(12)\varphi(10) = 4 \cdot 4 = 16$.

La funzione g è ben definita perchè $[3(h+8n)]_{12} = [3h+24n]_{12} = [3h]_{12}$ e $[2(h+15n)]_{10} = [2h + 30n]_{10} = [32h]_{10}$. La verifica della relazione

$$([3(h + h')]_{12}, [2(k + k')]_{10}) = ([3h]_{12}, [2k]_{10}) + ([3h']_{12}, [2k']_{10})$$

è immediata, ma in generale

$$([3hh']_{12}, [2kk']_{10}) \neq ([3h]_{12}, [2k]_{10})([3h']_{12}, [2k']_{10}) = ([9hh']_{12}, [4kk']_{10})$$

e quindi g è un omomorfismo di gruppi abeliani ma non di anelli.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 10 febbraio 2017 – Versione A

COGNOME ..... **NOME** .....

MATRICOLA .....

Rispondere a ciascuna domanda, motivando adeguatamente le risposte. Per essere sufficiente un compito deve raggiungere almeno 18 punti.

Esercizio 1 ($11 = 4 + 4 + 3$ punti)**.**

a) Una certa sigla alfanumerica è formata da tre lettere (di un alfabeto di 21 lettere) seguite da tre cifre. Le cifre possono essere ripetute, le lettere no. Quante sono le possibli sigle in tutto?

b) Calcolare il numero degli anagrammi della parola SILLOGISMO.

c) Dire quanti sono i numeri tra 1 e 4200 non divisibili né per 2, né per 3 né per 7.

Soluzione.

a) Avendo a disposizione 21 lettere non ripetibili e 10 cifre ripetibili il numero delle possibili combinazioni è $\frac{21!}{18!}10^3 = 21 \cdot 20 \cdot 19 \cdot 10^3 = 7980000$.

b) La parola contiene 10 lettere di cui 4 compaiono due volte. Quindi il numero totale degli anagrammi è $10!/(2!)^4 = 216800$.

c) Indicato con A_n l'insieme dei numeri tra 1 e 4200 divisibili per n, se n divide 4200 allora $|A_n| = \frac{4200}{n}$. Quindi

$$|A_2| = 2100, \qquad |A_3| = 1400, \qquad |A_7| = 600.$$

Se inoltre n_1 e n_2 dividono 4200 e sono coprimi, allora $A_{n_1} \cap A_{n_2} = A_{n_1 n_2}$. Quindi

$$A_2 \cap A_3 = A_6, \qquad A_2 \cap A_7 = A_{14}, \qquad A_3 \cap A_7 = A_{21}, \qquad A_2 \cap A_3 \cap A_7 = A_6 \cap A_7 = A_{42}$$

ossia

$$|A_2 \cap A_3| = 700, \quad |A_2 \cap A_7| = 300, \quad |A_3 \cap A_7| = 200, \quad |A_2 \cap A_3 \cap A_7| = 100.$$

Allora applicando il principio di inclusione-esclusione otteniamo

$$|A_2 \cup A_3 \cup A_7| = 2100 + 1400 + 600 - 700 - 300 - 200 + 100 = 3000.$$

Pertanto la quantità voluta è $4200 - 3000 = 1200$.

Esercizio 2 ($11 = 4 + 4 + 3$ punti)**.** Si considerino i seguenti cicli in S_7:

$$\sigma_1 = (2\ 6\ 1\ 7\ 5) \qquad \sigma_2 = (1\ 3\ 6\ 4)\,.$$

a) Calcolare la decomposizione in cicli disgiunti della composizione $\tau = \sigma_1 \circ \sigma_2$

b) Determinare tipo, parità e periodo di τ

c) Verificare che la funzione $f : \mathbb{Z}_{20} \to \mathcal{S}_7$ con $f([k]) = \tau^k$ è ben definita, è un omomorfismo di gruppi da $(\mathbb{Z}_{20}, +)$ a $(S_7, \circ)$ e determinarne esplicitamente il nucleo.

Soluzione.

a) Si ha $\tau = (1\ 3)(2\ 6\ 4\ 7\ 5)$.

b) τ ha tipo $(2, 5)$, parità dispari e periodo $\mathrm{mcm}(2, 5) = 10$.

c) Se $[k] = [\ell]$ in $\mathbb{Z}_{20}$ possiamo scrivere $\ell = k + 20n$ per un qualche intero n. Ma allora $\tau^\ell = \tau^k(\tau^{20})^n = \tau^k$ perché $\tau^{20} = 1$ in quanto τ ha periodo 10.

La catena di uguaglianze

$$f([k + k']) = \tau^{k+k'} = \tau^k \tau^{k'} = f([k])f([k'])$$

implica che f è un omomorfismo.

Infine $\ker f = \{[0], [10]\}$ perché 0 e 10 sono gli unici multipli del periodo di τ compresi tra 0 e 19.

Esercizio 3 ($11 = 4 + 4 + 3$ punti)**.**

a) Dopo aver verificato che $\mathrm{MCD}(75, 1156) = 1$, calcolare l'inverso di 75 in $\mathbb{Z}_{1156}$.

b) Calcolare il numero degli elementi invertibili nell'anello $\mathbb{Z} \times \mathbb{Z}_{20}$.

c) Calcolare il resto della divisione di 1387^{34} per 60.

Soluzione.

a) Si ha

$$\begin{aligned} 1156 &= 15 \cdot 75 + 31 \\ 75 &= 2 \cdot 31 + 13 \\ 31 &= 2 \cdot 13 + 5 \\ 13 &= 2 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Ciò conferma che $\mathrm{MCD}(75, 1853) = 1$. Risalendo dal basso e sostituendo i valori precedenti

$$\begin{aligned} 1 &= 3 - 2 \\ &= 2 \cdot 3 - 5 \\ &= 2 \cdot 13 - 5 \cdot 5 \\ &= 12 \cdot 13 - 5 \cdot 31 \\ &= 12 \cdot 75 - 29 \cdot 31 \\ &= 447 \cdot 75 - 29 \cdot 1156. \end{aligned}$$

L'ultima uguaglianza realizza l'identità di Bezout e quindi l'inverso di 75 in $\mathbb{Z}_{1156}$ è 447.

b) Ricordando che per anelli A e B si ha sempre $(A \times B)^\times = A^\times \times B^\times$ e che $\mathbb{Z}^\times = \{\pm 1\}$ si ha

$$|(\mathbb{Z} \times \mathbb{Z}_{20})^\times| = 2 \cdot \varphi(20) = 2 \cdot 8 = 16.$$

c) Siccome $1387 = 23 \cdot 60 + 7$ si ha $\mathrm{MCD}(1387, 60) = \mathrm{MCD}(7, 60) = 1$ e siccome $\varphi(60) = \varphi(3)\varphi(4)\varphi(5) = 2 \cdot 2 \cdot 4 = 16$ possiamo applicare il teorema di Lagrange per cui $1387^{16} \equiv 7^{16} \equiv 1 \bmod 60$. Osservato che $34 = 2 \cdot 16 + 2$ si ottiene

$$1387^{34} \equiv (7^{16})^2 \cdot 7^2 \equiv 49 \bmod 60.$$

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 19 giugno 2017 – Versione B

COGNOME ..... **NOME** .....

MATRICOLA .....

Rispondere a ciascuna domanda, motivando adeguatamente le risposte. Per essere sufficiente un compito deve raggiungere almeno 18 punti.

Esercizio 1. Alle semifinali olimpiche degli 800 metri piani sono ammessi i 24 atleti con i tempi migliori delle qualificazioni. Gli atleti sono poi distribuiti in tre semifinali da 8. Determinare il numero di modi in cui possono essere scelti gli atleti per la prima semifinale nei casi seguenti:

a) non si richiede nessuna condizione, tutte le possibilità sono ammesse;

b) i ciascuna semifinale devono essere presenti 2 dei 6 atleti coi tempi migliori;

c) 8 atleti in semifinale sono europei (e 16 non europei) e in ciascuna semifinale devono essere presenti non più di 3 atleti europei.

Esercizio 2. Si considerino i seguenti cicli in S_8:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 8 & 4 & 2 & 1 & 5 & 3 \end{pmatrix} \qquad \tau = (1\ 7\ 5\ 2\ 6)\,.$$

a) Calcolare la decomposizione in cicli disgiunti di σ, σ^2 e $\sigma \circ \tau$

b) Fornire esempi di elementi di S_8 con periodo 6, 10, 13, oppure spiegare perchè tali elementi non esistono.

c) Verificare che la funzione $f : \mathbb{Z}_{10} \to \mathcal{S}_8$ con $f([k]) = \tau^{3k}$ è ben definita ed è un omomorfismo di gruppi da $(\mathbb{Z}_{10}, +)$ a $(S_8, \circ)$. Elencare tutti gli elementi nucleo.

Esercizio 3. a) Calcolare la cifra finale del numero $7^{777} + 3^{333}$.

b) Risolvere la congruenza $40x \equiv 3 \bmod 1183$.

c) Determinare il numero degli elementi invertibili nell'anello $\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 13 settembre 2017

COGNOME ..... **NOME** .....

MATRICOLA .....

Rispondere a ciascuna domanda, motivando adeguatamente le risposte. Per essere sufficiente un compito deve raggiungere almeno 18 punti.

Esercizio 1 $(3+3+4)$**.** Un fiorista vende rose di 5 colori diversi (rosa, rosse, gialle, bianche e azzurre).

a) Volendo acquistare un mazzo bicolore, quanti sono i possibili abbinamenti di colore?

b) Di quante rose deve essere costituito un mazzo per essere sicuri che ve ne siano almeno 5 dello stesso colore?

c) Quanti mazzi distinti di 12 rose si possono formare se si vuole che tutti i colori siano presenti?

Soluzione.

a) Scegliere 2 colori fra 5 per formare un mazzo di rose si può fare in $\binom{5}{2} = \frac{5!}{2!3!} = 10$ modi.

b) Scegliendo 4 rose per ogni colore se ne ha un totale di $4 \cdot 5 = 20$. Aggiungendone una 21esima almeno un colore raggiunge 5 esemplari. Quindi ogni mazzo che contiene almeno 21 rose ne deve contenere 5 dello stesso colore.

c) Per formare una mazzo di 12 rose in cui compaia almeno una rosa per ogni colore procediamo in due passi. Prima di tutto prendiamo una rosa di ciascun colore (sono 5). Poi scegliamo in modo totalmente arbitrario le restanti 7 rose. Scegliere arbitrariamente 7 rose di 5 colori si può fare in

$$\binom{7+5-1}{5-1} = \binom{11}{4} = \frac{11!}{4! \cdot 7!} = 330$$

modi diversi, che è il totale dei mazzi possibili.

Esercizio 2 (3+3+4)**.** a) Determinare mediante l'algoritmo euclideo il massimo comune divisore d e il minimo comune multiplo D dei due numeri $a = 1377$ e $b = 1071$.

b) Determinare le ultime due cifre decimali (decine e unità) del numero 4597^{1603}.

c) Determinare tutte le soluzioni di ciascuna delle due congruenze lineari

- $38x \equiv 25 \bmod 42$
- $25x \equiv 38 \bmod 42$.

Soluzione.

a) Eseguendo l'algoritmo euclideo troviamo:

- $1377 = 1071 \cdot 1 + 306$
- $1071 = 306 \cdot 3 + 153$
- $306 = 153 \cdot 2 + 0$

Quindi $d = 153$ e $D = \frac{1377 \cdot 1071}{153} = 9639$.

b) Cerchiamo il rappresentante speciale di $[4597^{1603}]$ in $\mathbb{Z}_{100}$. Osserviamo intanto che in tale anello $[4597^{1603}] = [4597]^{1603} = [97]^{1603}]$. Poichè 97 è coprimo con 100, la sua classe è invertibile in $\mathbb{Z}_{100}$, ossia è un elemento del gruppo moltiplicativo $\mathbb{Z}_{100}^*$, che ha $\varphi(100) = 40$ elementi. Quindi $[97]^{40} = [1]$. Poichè $1603 = 40 \cdot 40 + 3$ avremo $[97]^{1603} = [97]^{40 \cdot 40} \cdot [97]^3 = [1] \cdot [-3]^3 = [-27] = [73]$. Quindi le ultime cifre sono 7 e 3.

c) La prima congruenza non ha soluzioni perchè $2 = MCD(38, 42)$ non divide 25.

La seconda congruenza ha invece soluzioni. Per trovarle dobbiamo determinare l'inverso di $[25]$ in $\mathbb{Z}_{42}$. Eseguendo l'algoritmo euclideo troviamo

- $42 = 25 \cdot 1 + 17$
- $25 = 17 \cdot 1 + 8$
- $17 = 8 \cdot 2 + 1$

e quindi ricavando 1 dal basso verso l'alto:

$1 = 42 \cdot 3 + 25 \cdot (-5)$.

Passando alle classi in $\mathbb{Z}_{42}$ abbiamo quindi $[1] = [25] \cdot [-5] \in \mathbb{Z}_{42}$e dunque l'inverso di $[25] \in \mathbb{Z}_{42}$ è $[-5] = [37]$. Possiamo allora riscrivere la congruenza come

$$x \equiv 38 \cdot (-5) \bmod 42$$

e quindi le sue soluzioni sono gli elementi dell'insieme

$$\{-190 + 42 \cdot k \mid \forall k \in \mathbb{Z}\}.$$

Esercizio 3 (3+3+4)**.** Sia σ la seguentte permutazione di S_9:

$$\sigma = (1\ 6\ 7\ 2)\,(3\ 5\ 9\ 4)\,(8\ 6)\,.$$

a) Scrivere la decomposizione in cicli disgiunti di σ, σ^2 e di σ^3.

b) Determinare il numero di elementi del sottogruppo ciclico $H :=< \sigma >$ di S_9.

c) Si consideri l'applicazione $f : H \ \to S_9$ data da $f(\sigma^k) = \sigma^{3k}$. Si dimostri che f è un omomorfismo dei gruppi $(H, \circ)$ e $(S_9, \circ)$ e si determini il suo nucleo. Si verifiche che $Im(f)$ coincide con H stesso.

Soluzione.

a) La decomposizione di σ in cicli disgiunti è (1 6 8 7 2)(3 5 9 4).

La decomposizione di σ^2 è (1 8 2 6 2)(3 9)(5 4) e quella di di σ^3 è (1 7 6 2 8)(3 4 9 5)

b) Guardando alla decomposizione in cicli disgiunti vediamo che il periodo di σ è 20, il minimo comune multiplo delle loro lunghezze. Quindi H ha 20 elementi.

Per quanto detto prima, il gruppo $< \sigma >$ ha 3 elementi, che sono σ, σ^2 e l'identitàdi S_9.

c) Dobbiamo verificare che f è compatibile con le operazioni, ossia che per ogni $\sigma^h, \sigma^k \in H$ si ha $f(\sigma^h \circ \sigma^k) = f(\sigma^h) \circ f(\sigma^k)$. Per le proprietÃ proprietà delle potenze che valgono nei gruppi, il primo membro è $f(\sigma^{h+k}) = \sigma^{3(h+k)}$. Il secondo è $\sigma^{3h} \circ \sigma^{3k}$ e quindi, sempre per le proprietà delle potenze è σ^{3h+3k}. I due membri sono quindi uguali perchè sono potenze di σ con lo stesso esponente $3(h + k) = 3h + 3k$.

Il nucleo di f è il sottogruppo del dominio dato da $f^{-1}(1_{S_9})$. Quindi $Ker(f)$ ècostituito da tutte le potenze di σ il cui cubo è l'identità. Dato che σ ha periodo 20 coprimo con 3, si ha $\sigma^{3m} = 1_{S_9}$ se e solo se $3m$ è multiplo di 20 e quindi se e solo se $m = 20t$. Dunque gli elementi del nucleo sono del tipo $(\sigma^{20})^{3t} = (1_{S_9})^{3t} = 1_{S_9}$. Pertanto f è iniettiva.

Una conseguenza dell'iniettività è il fatto che l'immagine contiene tanti elementi quanti il dominio, ossia 20. Gli elementi dell'immagine sono potenze di σ, quindi sono elementi di H, e sono 20 quanti gli elementi di H. Per il principio dei cassetti, $Im(f) = H$.