Corso di Studi in Informatica
Matematica Discreta

Prova scritta 29 Gennaio 2019 – Versione C

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

MATRICOLA .....

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

Esercizio 1. Un negoziante vende 22 tipi diversi di capsule di caffè, distinguibili per colore.

1. (3 p.) Per allestire una vetrina il negoziante posiziona in fila una capsula di ciascun colore disponibile. Quanti modi ha di farlo?

2. (4 p.) Un cliente vuole acquistare 4 capsule di colori diversi. Quante sono le scelte possibili?

3. (4 p.) Per promozione i primi 8 clienti ricevono una capsula in regalo a loro scelta. Quante sono le possibili successioni di scelte di queste capsule regalo?

Soluzione.

1. Si tratta di scegliere un ordinamento di un insieme di 22 elementi. Le possibilità sono 22!.

2. Il cliente deve scegliere un sottoinsieme di 4 colori tra i 22 disponibili. Le possibilità sono
$$\binom{22}{4} = \frac{22!}{4! \cdot 18!} = \frac{22 \cdot 21 \cdot 20 \cdot 19}{4 \cdot 3 \cdot 2 \cdot 1} = 7315$$

3. Le scelte dei clienti sono ovviamente indipendenti, per cui ogni successione di 8 colori è possibile, incluse le ripetizioni. Le successioni sono 22^8.

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

Esercizio 2. Consideriamo le seguenti due permutazioni di $\mathcal{S}_7$ date come prodotto di cicli:

$$\sigma = (7\ 4\ 3)(6\ 7)(1\ 2\ 6), \qquad \tau = (2\ 6\ 4)(3\ 4\ 5\ 6)(1\ 2).$$

1. (p. 4) Determinare la decomposizione in cicli disgiunti di σ e τ.
2. (p. 3) Calcolare il periodo di σ, τ e $\sigma\tau$.
3. (p. 4) Stabilire se la funzione $f : \langle\sigma\rangle \to \mathbb{Z}_{18}$ definita pomendo $f(\sigma^k) = \overline{3k}$ per ogni $k \in \mathbb{Z}$ è ben definita, se è un omomorfismo, se è iniettiva e se è suriettiva.

Soluzione.

1. Si ha $\sigma = (2\ 4\ 3\ 7\ 6\ 1)(5)$ e $\tau = (3\ 2\ 1\ 6)(4\ 5)(7)$.
2. Il periodo di σ è $o(\sigma) = \text{mcm}(6,1) = 6$, quello di τ è $\text{mcm}(4,2,1) = 4$. La decomposizione in cicli disgiunti di $\sigma\tau$ è $(2)(3\ 4\ 5)(6\ 7)(1)$ per cui il suo periodo è $\text{mcm}(3,2,1,1) = 6$.
3. Per vedere che è ben definita dobbiamo dimostrare che $\sigma^a = \sigma^b \Rightarrow f(\sigma^a) = f(\sigma^b)$ per ogni $a, b \in \mathbb{Z}$. Ora $\sigma^a = \sigma^b \Rightarrow \sigma^{a-b} = \text{Id} \Rightarrow o(\sigma) \mid (a-b) \Rightarrow 6 \mid (a-b) \Rightarrow 18 \mid (3a-3b)$. Pertanto $\overline{3a} = \overline{3b}$ che era quello che dovevamo dimostrare. È un omomorfismo perché

$$f(\sigma^a \circ \sigma^b) = f(\sigma^{a+b}) = \overline{2(a+b)} = \overline{2a+2b} = \overline{2a} + \overline{2b} = f(\sigma^a) + f(\sigma^b).$$

Per vedere se è iniettiva calcoliamo il nucleo

$$\ker(f) = \{\sigma^k \mid f(\sigma^k) = \overline{0}\} = \{\sigma^k \mid \overline{3k} = \overline{0}\} = \{\sigma^k \text{ tale che } 18 \mid 3k\} = \{\sigma^k \text{ tale che } 6 \mid k\}.$$

Visto che $6 = o(\sigma)$ otteniamo $\ker(f) = \{\text{Id}\}$ e quindi f è iniettiva.
Infine, poiché $o(\sigma) = 6$ abbiamo $\langle\sigma\rangle = \{\text{Id}, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$ e quindi

$$\text{Im}(f) = \{f(\text{Id}), f(\sigma), f(\sigma^2), f(\sigma^3), f(\sigma^4), f(\sigma^5)\}$$

contiene non più di 6 elementi. Siccome $\mathbb{Z}_{18}$ ha 18 elementi è chiaro che $\text{Im}(f) \neq \mathbb{Z}_{18}$, cioè f non è suriettiva.

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

Esercizio 3. 1. (p. 4) Applicando l'algoritmo euclideo determinare MCD$(57, 25)$ e realizzare l'identità di Bezout.

2. (p. 4) Calcolare il resto della divisione per 38 del numero 5^{561}.

3. (p. 3) Stabilire se il gruppo $\mathbb{Z}_9 \times \mathbb{Z}$ è ciclico o no.

Soluzione.

1. Applichiamo l'algoritmo di divisione euclideo:

$$\begin{aligned} \underline{57} &= 2 \cdot \underline{25} + \underline{7} \\ \underline{25} &= 3 \cdot \underline{7} + \underline{4} \\ \underline{7} &= 1 \cdot \underline{4} + \underline{3} \\ \underline{4} &= 1 \cdot \underline{3} + \boxed{\underline{1}} \\ \underline{3} &= 3 \cdot \underline{1} + \underline{0} \end{aligned}$$

Quindi MCD$(13, 8) = 1$. Invertendo la procedura

$$\begin{aligned} \underline{1} &= \underline{4} - \underline{3} \\ &= \underline{4} - (\underline{7} - \underline{4}) = 2 \cdot \underline{4} - \underline{7} \\ &= 2 \cdot (\underline{25} - 3 \cdot \underline{7}) - \underline{7} = 2 \cdot \underline{25} - 7 \cdot \underline{7} \\ &= 2 \cdot \underline{25} - 7 \cdot (\underline{57} - 2 \cdot \underline{25}) = 16 \cdot \underline{25} - 7 \cdot \underline{57}. \end{aligned}$$

2. Poiché MCD$(5, 38) = 1$ sappiamo che $5^{\varphi(38)} \equiv 1 \mod 38$. Calcoliamo

$$\varphi(38) = \varphi(2 \cdot 19) = (2 - 1) \cdot (19 - 1) = 18.$$

Quindi $5^{18} \equiv 1 \mod 38$. Dividendo 561 per 18 otteniamo $561 = 31 \cdot 18 + 3$ da cui $5^{561} \equiv 5^{31 \cdot 13 + 3} \equiv 5^3 \equiv 125 \equiv \boxed{11} \mod 38$.

3. Il gruppo $\mathbb{Z}_9 \times \mathbb{Z}$ non è ciclico. Perché lo sia dovrebbe avere un generatore $g = (\overline{a}, b)$. Dovendo ottenere $(\overline{0}, 1) \in \mathbb{Z}_9 \times \mathbb{Z}$ da g deve essere $\overline{a} = \overline{0}$ e $b = \pm 1$. Ma anche $(\overline{1}, 0) \in \mathbb{Z}_9 \times \mathbb{Z}$ e questo non appartiene al gruppo generati da g se $\bar{a} = \bar{0}$. Quindi un generatore non esiste.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 14 febbraio 2019 – 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. Un giardiniere ha a disposizione 12 tipi diversi di piante per adornare un giardino

1. (3 p.) Per una piccola aiuola deve scegliere 5 piante di tipo diverso. Quante possibili scelte ha dei 5 tipi?
2. (4 p.) In un'aiuola grande deve piantare 15 piante, peró mettendo almeno una pianta per tipo. Quante sono le possibili scelte delle 15 piante?
3. (4 p.) Lungo uno dei muri di cinta deve mettere 24 piante, 2 per tipo. Quanti modi ha di farlo?

Soluzione.

1. Si scelgono 5 elementi in un insieme di 12, per cui le scelte sono $\binom{12}{5} = \frac{12!}{5!\cdot 7!} = 792$.
2. Scelta una pianta per tipo restano da scegliere 3 piante di 12 tipi per completare il gruppo di 15. Questo si può fare in $\binom{3+12-1}{12-1} = \binom{14}{11} = \frac{14!}{10!\cdot 4!} = 364$ modi.
3. Il problema è equivalente a contare il numero degli anagrammi di una parola di lunghezza 24 in cui ogni lettera è ripetuta 2 volte. Quindi il totale è $\frac{24!}{2^{12}}$.

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

Esercizio 2. Consideriamo la seguente permutazioni di $\mathcal{S}_9$:

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

1. (p. 4) Determinare la decomposizione in cicli disgiunti di σ, σ^{-1} e σ^2.
2. (p. 3) Determinare tipo e parità di σ, σ^{-1} e σ^2.
3. (p. 4) Stabilire se la funzione $f : \mathbb{Z}_{10} \to \mathcal{S}_9$ definita ponendo $f(\overline{k}) = \sigma^{3k}$ per ogni $k \in \mathbb{Z}$ è ben definita, se è un omomorfismo, se è iniettiva e se è suriettiva.

Soluzione.

1. Si ha $\sigma = (1\ 9)(2\ 3\ 8)(4\ 7\ 5)$, $\sigma^{-1} = (4\ 7\ 5)^{-1}(2\ 3\ 8)^{-1}(1\ 9)^{-1} = (4\ 5\ 7)(2\ 8\ 3)(1\ 9)$ e
$$\sigma^2 = (1\ 4)^2(2\ 3\ 8)^2(4\ 7\ 5)^2 = (2\ 8\ 3)(4\ 5\ 7).$$
2. σ e σ^{-1} hanno tipo $(3, 3, 2)$ e periodo $\mathrm{mcm}(3, 2) = 6$ mentre σ^2 ha tipo $(3, 3)$ e periodo 3.
3. Per vedere che è ben definita dobbiamo dimostrare che $\overline{a} = \overline{b} \Rightarrow f(\overline{a}) = f(\overline{b})$ per ogni $a, b \in \mathbb{Z}$. Ora $\overline{a} = \overline{b} \Rightarrow 10 \mid (a - b) \Rightarrow \exists t \in \mathbb{Z}, a = b + 10t$. Pertanto
$$f(\overline{a}) = \sigma^{3a} = \sigma^{3b+30t} = \sigma^{3b} \circ \sigma^{30t} = \sigma^{3b} = f(\overline{b})$$
perché σ ha periodo 6 e dunque $\sigma^{30t} = \mathrm{id}$. Quindi f è ben definita.
È un omomorfismo perché
$$f(\overline{a} + \overline{b}) = f(\overline{a + b}) = \sigma^{3(a+b)} = \sigma^{3a+3b} = \sigma^{3a} \circ \sigma^{3b} = f(\overline{a}) \circ f(\overline{b}).$$
Per vedere se è iniettiva calcoliamo il nucleo
$$\ker(f) = \{\overline{a} \mid f(\overline{a}) = \mathrm{Id}\} = \{\overline{a} \mid \sigma^{3a} = \mathrm{id}\} = \{\overline{a} \text{ tale che } 6 \mid 3a\} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}.$$
Pertanto f non è iniettiva. Infine il dominio di f ha 10 elementi mentre il codominio ne ha $9! > 10$ e quindi f non è essere suriettiva.

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

Esercizio 3. 1. (p. 4) Scivere il numero $224_{[6]}$ (scritto in base 6) in notazione binaria.

2. (p. 3) Tra i seguenti gruppi uno è ciclico. Dire quale e trovarne i generatori:

$$\mathbb{Z}_2 \times \mathbb{Z}_5, \qquad \mathbb{Z}_2 \times \mathbb{Z}_6, \qquad \mathbb{Z}_2 \times \mathbb{Z}_{10}.$$

3. (p. 4) Calcolare tutte le soluzioni della congruenza $14x \equiv 6 \bmod 20$.

Soluzione.

1. Prima sciviamo $224_{[6]}$ in base 10:

$$224_{[6]} = 2 \cdot 6^2 + 2 \cdot 6^1 + 4 \cdot 6^0 = 72 + 12 + 4 = 88.$$

Ora dividiamo ripetutamente per la nuova base, cioè 2:

$$\begin{aligned} 88 &= 44 \cdot 2 + \mathbf{0} \\ 44 &= 22 \cdot 2 + \mathbf{0} \\ 22 &= 11 \cdot 2 + \mathbf{0} \\ 11 &= 5 \cdot 2 + \mathbf{1} \\ 5 &= 2 \cdot 2 + \mathbf{1} \\ 2 &= 1 \cdot 2 + \mathbf{0} \\ 1 &= 0 \cdot 2 + \mathbf{1} \end{aligned}$$

In conclusione $224_{[7]} = 88_{[10]} = 1011000_{[2]}$.

2. Sappiamo che $\mathbb{Z}_a \times \mathbb{Z}_b$ è ciclico soltanto se $\mathrm{MCD}(a, b) = 1$. Pertanto l'unico ciclico dei tre è $\mathbb{Z}_2 \times \mathbb{Z}_5$. I suoi generatori sono le coppie di generatori:

$$([1]_2, [1]_5) \qquad ([1]_2, [2]_5) \qquad ([1]_2, [3]_5) \qquad ([1]_2, [4]_5).$$

3. Siccome $\mathrm{MCD}(14, 20) = 2$ divide 8, la congruenza ha soluzioni. Per ottenerle semplifichiamo la congruenza iniziale dividendone i coefficienti per 2:

$$7x \equiv 3 \bmod 10.$$

Ora $\mathrm{MCD}(7, 10) = 1$, con identità di Bezout $3 \cdot 7 + (-2)10 = 1$ da cui $[7]_{10}^{-1} = [3]_{10}$. Quindi, moltiplicando per 3, otteniamo

$$x = 3 \cdot 3 = 9 \bmod 10$$

come unica soluzione modulo 10 della congruenza iniziale. Siccome però la congruenza richiede soluzioni modulo 20 le soluzioni sono $x = 9, 19 \bmod 20$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 17 giugno 2019 – 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. 1. (4 p.) Contare gli interi compresi tra 1 e 4000 divisibili per 4 o per 10.

2. (4 p.) Contare gli anagrammi, anche privi di senso, della parola POLPETTONE.

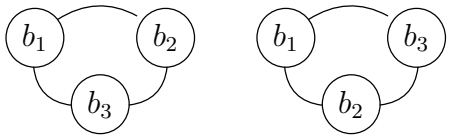
3. (3 p.) Durante un gioco, 15 bambini devono mettersi in cerchio tenendosi per mano a gruppetti di 3 persone. In quanti modi lo possono fare?

Soluzione.

1. Sia D_n l'insieme dei numeri naturali compresi tra 1 e 4000 divisibili per n. Allora $|D_n| = \lfloor \frac{4000}{n} \rfloor$, la parte intera di $\frac{4000}{n}$. Il testo ci chiede $|D_4 \cup D_{10}|$. Per il Principio di Inclusione-Esclusione, $|D_4 \cup D_{10}| = |D_4| + |D_{10}| - |D_4 \cap D_{10}| = |D_4| + |D_{10}| - |D_{20}| = \lfloor \frac{4000}{4} \rfloor + \lfloor \frac{4000}{10} \rfloor - \lfloor \frac{4000}{20} \rfloor = 1000 + 400 - 200 = 1200$.

2. In POLPETTONE le lettere ripetute sono P ($\times 2$), O ($\times 2$), E ($\times 2$) e T ($\times 2$). Il numero di anagrammi è dunque $\frac{10!}{2!\cdot 2!\cdot 2!\cdot 2!} = \frac{10!}{16} = 226800$.

3. Il primo cerchio è ottenuto contando prima i sottoinsiemi $\{b_1, b_2, b_3\}$ di tre bambini scelti tra i 15 presenti (sono in tutto $\binom{15}{3}$ perché sono combinazioni semplici) e osservando che ognuno di questi sottoinsiemi individua due possibili cerchi



Otteniamo così $2 \cdot \binom{15}{3}$ modi diversi di formare il primo cerchio. Per il secondo cerchio il ragionamento è analogo ma coi $15-3 = 12$ bambini rimasti, cioé $2 \cdot \binom{12}{3}$ modi diversi. Proseguendo così otteniamo apparentemente $2 \cdot \binom{15}{3} \cdot 2 \cdot \binom{12}{3} \cdot 2 \cdot \binom{9}{3} \cdot 2 \cdot \binom{6}{3} \cdot 2 \cdot \binom{3}{3}$ accorpamenti. Poiché però la posizione reciproca dei 5 cerchi non conta, dobbiamo dividere ulteriormente per 5! ottenedo così $2\cdot\binom{15}{3}\cdot 2\cdot\binom{12}{3}\cdot 2\cdot\binom{9}{3}\cdot 2\cdot\binom{6}{3}\cdot 2\cdot\binom{3}{3}\cdot\frac{1}{5!} = 44844800$.

Più rapidamente, si poteva notare che il problema equivale a contare le permutazioni fatte così: $(*\ *\ *)(*\ *\ *)(*\ *\ *)(*\ *\ *)(*\ *\ *)$. Il loro numero è $\frac{15!}{3^5\cdot 15!} = 44844800$.

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

Esercizio 2. Consideriamo la seguente permutazioni di $\mathcal{S}_7$:

$$\sigma = (1\ 2\ 3)(3\ 4\ 5\ 6), \qquad \tau = (6\ 7) \circ \sigma \circ (6\ 7).$$

1. (p. 4) Determinare la decomposizione in cicli disgiunti di σ, τ, τ^2, τ^3 e $\sigma\tau$.
2. (p. 4) Determinare il periodo di σ, τ^2, τ^3 e $\sigma\tau$.
3. (p. 3) Stabilire se la funzione $f : \mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathcal{S}_9$ definita ponendo $f(\overline{a}, \overline{b}) = \sigma^{3a-2b}$ per ogni $a, b \in \mathbb{Z}$ è ben definita, se è un omomorfismo e se è suriettiva.

Soluzione.

1. Si ha $\sigma = (1\ 2\ 3\ 4\ 5\ 6)$, $\tau = (1\ 2\ 3\ 4\ 5\ 7)$, $\tau^2 = (1\ 3\ 5)(2\ 4\ 7)$, $\tau^3 = (1\ 4)(2\ 5)(3\ 7)$ e $\sigma\tau = (1\ 3\ 5\ 7\ 2\ 4\ 6)$.
2. $\mathrm{per}(\sigma) = 6$, $\mathrm{per}(\tau^2) = \mathrm{mcm}(3,3) = 3$, $\mathrm{per}(\tau^3) = \mathrm{mcm}(2,2,2) = 2$ e $\mathrm{per}(\sigma\tau) = 7$.
3. Per vedere che è ben definita dobbiamo dimostrare che

   $$(\overline{a_1}, \overline{b_1}) = (\overline{a_2}, \overline{b_2}) \Rightarrow f(\overline{a_1}, \overline{b_1}) = f(\overline{a_2}, \overline{b_2})$$

   per ogni $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Ora $(\overline{a_1}, \overline{b_1}) = (\overline{a_2}, \overline{b_2})$ vuol dire $2 \mid (a_1 - a_2)$ e $3 \mid (b_1 - b_2)$ cioè esistono $t_1, t_2 \in \mathbb{Z}$ tali che $a_1 = a_2 + 2t_1$ e $b_1 = b_2 + 3t_2$. Pertanto

   $$f(\overline{a_1}, \overline{b_1}) = \sigma^{3a_1-2b_1} = \sigma^{3(a_2+2t_1)-2(b_2+3t_2)} = \sigma^{3a_2-2b_2} \circ \sigma^{6(t_1-t_2)} = \sigma^{3a_2-2b_2} = f(\overline{a_2}, \overline{b_2})$$

   perché $\mathrm{per}(\sigma) = 6$ e dunque $\sigma^{6(t_1-t_2)} = \mathrm{Id}$. Quindi f è ben definita.

   È un omomorfismo perché

   $$\begin{aligned} f((\overline{a_1}, \overline{b_1}) + (\overline{a_2}, \overline{b_2})) &= f(\overline{a_1 + a_2}, \overline{b_1 + b_2}) = \sigma^{3(a_1+a_2)-2(b_1+b_2)} \\ &= \sigma^{3a_1-2b_1} \circ \sigma^{3a_2-2b_2} = f(\overline{a_1}, \overline{b_1}) \circ f(\overline{a_2}, \overline{b_2}). \end{aligned}$$

   Infine, siccome $|\mathbb{Z}_2 \times \mathbb{Z}_3| = |\mathbb{Z}_2| \cdot |\mathbb{Z}_3| = 2 \cdot 3 = 6 < 9! = |\mathcal{S}_9|$, la f non è suriettiva.

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

Esercizio 3. 1. (p. 4) Calcolare il resto della divisione per 20 di $7^{401} + 3^{402}$.

2. (p. 3) Calcolare gli elementi invertibili in $\mathbb{Z} \times \mathbb{Z}_{12}$ rispetto al prodotto componente per componente.

3. (p. 4) Risolvere l'equazione $\overline{21}x = \overline{15}$ in $\mathbb{Z}_{12}$.

Soluzione.

1. Poiché $\mathrm{MCD}(7, 20) = 1 = \mathrm{MCD}(3, 20)$, sappiamo che $7^{\varphi(20)} \equiv 1 \bmod 20$ e che $3^{\varphi(20)} \equiv 1 \bmod 20$. Ora $\varphi(20) = \varphi(2^2)\varphi(5) = (2^2 - 2) \cdot 4 = 8$. Quindi

$$7^{401} + 3^{402} \equiv 7^{400+1} + 3^{400+2} \equiv 7 + 3^2 \equiv 16 \bmod 20.$$

2. Sappiamo che l'insieme degli elementi invertibili in $\mathbb{Z} \times \mathbb{Z}_{12}$ è $(\mathbb{Z} \times \mathbb{Z}_{12})^\times = \mathbb{Z}^\times \times \mathbb{Z}_{12}^\times$. Ora $\mathbb{Z}^\times = \{\pm 1\}$ mentre $\mathbb{Z}_{12}^\times = \{\overline{n} \mid 0 \leq n \leq 12, \mathrm{MCD}(n, 12) = 1\} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ Pertanto
$$(\mathbb{Z} \times \mathbb{Z}_{12})^\times = \{(\pm 1, \overline{1}), (\pm 1, \overline{5}), (\pm 1, \overline{7}), (\pm 1, \overline{11})\}.$$

3. Sappiamo che l'equazione ha soluzione $\overline{u} \in \mathbb{Z}_{12}$ se e solo se la congruenza $21x \equiv 15 \bmod 12$ ha soluzione $u \in \mathbb{Z}$. Questa è risolubile perché $\mathrm{MCD}(21, 12) = 3$ divide 15. Per risolverla, semplifichiamola dividendo per 3 ottenendo $7x \equiv 5 \bmod 4$. Visto che $\mathrm{MCD}(7, 4) = 1$ vale l'identità di Bezout che risulta essere $7 \cdot (-1) + 4 \cdot (2) = 1$. Moltiplicandola per 5 otteniamo $7 \cdot (-5) + 4 \cdot (10) = 5$. Dunque $x_0 = -5$ è una soluzione particolare di $7x \equiv 5 \bmod 4$. Tutte le altre sono del tipo $x = -5 + 4k$ con $k \in \mathbb{Z}$. Per scriverle modulo 12 (come la congruenza di partenza) basta considerare $x = -5 + 4k$ con $0 \leq k < \mathrm{MCD}(21, 12) = 3$. Quindi $x \equiv -5 \equiv 7 \bmod 12$, $x \equiv -5 + 4 \equiv -1 \equiv 11 \bmod 12$ e $x \equiv -5 + 8 \equiv 3 \bmod 12$. Pertanto $\overline{21}x = \overline{15}$ ha per soluzioni $\overline{7}$, $\overline{11}$ e $\overline{3}$ in $\mathbb{Z}_{12}$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 7 luglio 2019

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

MATRICOLA .....

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

Esercizio 1. 1. (4 p.) In una classe di una scuola materna ci sono 10 maschi ed 8 femmine. Per un gioco la maestra vuole scegliere un gruppetto di 4 facendo in modo che ci siano 2 maschi e 2 femmine. Quanti modi ha di farlo?

2. (3 p.) Un'azienda produce palline da ping-pong bianche, gialle, arancioni e rosse. Le distribuisce in confezioni da 8 in cui i colori sono mischiati a caso. Quante confezioni diverse per distribuzione di colori possono esistere?

3. (4 p.) Un hacker scopre che una password d'accesso ad un sito è un anagramma di

AACEHHHPRRZ

che non inizia per E. Quante sono le possibili password che deve tentare?

Soluzione.

1. Le scelte dei maschi e delle femmine sono indipendenti per cui il totale dei gruppetti di 4 con le condizioni volute è
$$\binom{10}{2} \cdot \binom{8}{2} = \frac{10 \cdot 9}{2} \cdot \frac{8 \cdot 7}{2} = 1260.$$

2. Guardando ai colori stiamo calcolando al numero delle combinazioni con ripetizione di 8 oggetti di 4 tipi. Il numero è
$$\binom{8+4-1}{4-1} = \binom{11}{3} = \frac{11 \cdot 10 \cdot 9}{3 \cdot 2 \cdot 1} = 165.$$

3. Il numero totale di anagrammi di AACEHHHPRRZ è
$$\frac{11!}{2 \cdot 2 \cdot 3!} = 1663200$$
in quanto delle 11 lettere due sono ripetute 2 volte ed una tre volte. Di questi quelli che iniziano per E sono
$$\frac{10!}{2 \cdot 2 \cdot 3!} = 151200$$
perché tanti quanti gli anagrammi delle 10 lettere restanti una volta assegnata la prima posizione ad E (che non era fra le lettere ripetute). Otteniamo quindi il numero cercato per differenza:
$$1663200 - 151200 = 1512000.$$

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

Esercizio 2. 1. (p. 4) Sia

$$\sigma = (3\ 8\ 1)(2\ 4\ 8\ 5)(3\ 5\ 6\ 7)(2\ 1\ 6\ 4\ 3) \in \mathcal{S}_8.$$

Calcolare la decomposizione in cicli disgiunti ed il periodo di σ e σ^{-1}.

2. (p. 4) Sia σ la permutazione del punto precedente. Dire per quali $k > 0$ la permutazione σ^k è un ciclo

3. (p. 3) Di una permutazione $\tau \in \mathcal{S}_{11}$ sappiamo che ha periodo 10. Quali potranno essere i tipi di τ?

Soluzione.

1. La consueta proceduta fornisce

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

per cui $\sigma^{-1} = (1\ 6\ 5\ 8\ 7)(2\ 4\ 3)$ ed entrambe hanno periodo $\mathrm{mcm}(3, 5) = 15$.

2. Abbiamo visto che la decomposizione di σ è della forma $c_5 c_3$ con c_ℓ un ciclo di lunghezza ℓ. Poiché i cicli sono disgiunti avremo

$$\sigma^k = c_3^k c_5^k$$

per ogni $k > 0$ e questo sarà un ciclo quando $c_3^k = \mathrm{id}$ oppure quando $c_5^k = \mathrm{id}$, ovvero quando k è un multiplo di 3 oppure un multiplo di 5.

3. Dovrà risultare 10 uguale al minimo comune di multiplo di numeri la cui somma totale è al più 11. Le possibilità sono quindi

$$(10), \quad (2, 5), \quad (2, 2, 5), \quad (2, 2, 2, 5).$$

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

Esercizio 3. 1. (p. 4) Determinare le due cifre finali del numero $49^{67681} - 3^{53483}$.

2. (p. 3) Convertire in base 8 il numero $4021_{[6]}$ scritto in base 6.

3. (p. 4) Dimostrare che la funzione

$$f : \mathbb{Z}_{15} \longrightarrow \mathbb{Z}_{18}, \qquad f([x]_{15}) = [6x]_{18}$$

è ben definita ed è un omomorfismo. Dire poi se f è iniettiva o suriettiva.

Soluzione.

1. Determinare le due cifre finali di un numero equivale a calcolarne la classe modulo 100. Poiché $\mathrm{MCD}(3, 100) = \mathrm{MCD}(49, 100) = 1$ possiamo applicare il teorema di Eulero. Siccome $\varphi(100) = 40$ abbiamo

$$[49^{67681} - 3^{53483}]_{100} = [49]_{100}^{40\cdot 1692+1} - [3]_{100}^{40\cdot 1337+3} = [49]_{100} - [3]_{100}^{3} = [22]_{100}.$$

2. Passando per la base 10 si ha

$$4021_{[6]} = 1 + 2 \cdot 6 + 0 \cdot 6^2 + 4 \cdot 6^3 = 877$$

e poi la successione di divisioni col resto $877 = 109{\cdot}8{+}\boxed{5}$, $109 = 13{\cdot}8{+}\boxed{5}$, $13 = 1{\cdot}8{+}\boxed{5}$ e $1 = 0 \cdot 8 + \boxed{1}$ permette di concludere che

$$4027_{[6]} = 1555_{[8]}.$$

3. Si ha $[x]_{15} = [y]_{15}$ quando $15 \mid x - y$. In tal caso si ha $6 \cdot 15 = 90 \mid 6x - 6y$ e siccome $18 \mid 90$ possiamo concludere che $[6x]_{18} = [6y]_{18}$, cioè f è ben definita. La funzione è un omomorfismo perché

$$f([x]_{15} + [y]_{15}) = f([x + y]_{15}) = [6(x + y)]_{18} = [6x]_{18} + [6y]_{18} = f([x]_{15}) + f([y]_{15}).$$

Infine, l'immagine di f è costituita dai multipli di 6 in $\mathbb{Z}_{18}$ che sono solo $\{\overline{0}, \overline{6}, \overline{12}\}$ e quindi f non può essere suriettiva e neanche iniettiva in quanto il dominio ha più elementi dell'immagine.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 9 settembre 2019

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

MATRICOLA .....

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

Esercizio 1. 1. (4 p.) Su 180 iscritti all'appello unificato di MDL sappiamo che 106 hanno sostenuto il parziale di MD e 138 il parziale di L. Quanti studenti hanno sostenuto solo MD? Quanti solo L?

2. (3 p.) Quante sono permutazioni di tipo $(4, 3, 3, 2)$ in S_{12}? Quante in S_{14}?

3. (4 p.) In un barattolo ci sono 12 caramelle di colore diverso. Sapendo che Alessia, Beatrice e Carla ne hanno prese rispettivamente a, b e c svuotando il barattolo, quante sono le possibili terne (a, b, c), includendo anche il caso che qualche ragazza non abbia preso alcuna caramella?

Soluzione.

1. Sia A l'insieme degli studenti che hanno sostenuto MD e sia B l'insieme degli studenti che hanno sostenuto L. Allora $|A| = 106$, $|B| = 138$ e $|A \cup B| = 180$. Per il Principio di Inclusione-Esclusione, abbiamo

$$|A \cup B| = |A| + |B| - |A \cap B|$$

da cui $|A \cap B| = |A| + |B| - |A \cup B| = 106 + 138 - 180 = 64$. Gli studenti che hanno sostenuto solo MD sono $|A \setminus (A \cap B)| = 106 - 64 = 42$ e quelli che hanno sostenuto solo L sono $|B \setminus (A \cap B)| = 138 - 64 = 74$.

2. Dalla teoria sappiamo che in S_{12} sono $\frac{12!}{(4\cdot 3\cdot 3\cdot 2)\cdot 2!}$ mentre in S_{14} sono $\frac{14!}{(4\cdot 3\cdot 3\cdot 2)\cdot 2!}$.

3. Si tratta di contare le terne del tipo (a, b, c) con $a + b + c = 12$. Il loro numero è quello delle combinazioni con ripetizione di elementi di un insieme di 3 elementi presi 12 alla volta cioè $\binom{3+12-1}{3-1} = \binom{14}{2} = 7 \cdot 13 = 91$.

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

Esercizio 2. 1. (p. 4) Sia

$$\sigma = (1\ 3)(7\ 5\ 1)(4\ 7)(1\ 5\ 7)(3\ 1\ 2\ 9)(1\ 3)(6\ 7\ 8) \in \mathcal{S}_9.$$

Calcolarne la decomposizione in cicli disgiunti, il tipo, la parità ed il periodo.

2. (p. 3) Sia σ la permutazione del punto precedente. Individuare un numero $k > 0$ per cui la permutazione σ^k abbia periodo 4. Individuare un $s > 0$ per cui σ^s abbia periodo 3.

3. (p. 4) Stabilire se la funzione $f : \langle \sigma^2 \rangle \to \mathbb{Z}_{12} : \sigma^{2k} \mapsto \overline{3k}$ è ben definita, un omorfismo, iniettiva e suriettiva.

Soluzione.

1. La consueta procedura fornisce

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

per cui il tipo è $(4, 3, 2)$, la permutazione è pari edl suo periodo è $\mathrm{mcm}(4, 3, 2) = 12$.

2. Notiamo che $\sigma^3 = (1\ 3\ 2\ 9)^3(4\ 5)^3(6\ 7\ 8)^3 = (1\ 3\ 2\ 9)^3(4\ 5)^3 = (1\ 9\ 2\ 3)(4\ 5)$ ha periodo $\mathrm{mcm}(4, 2) = 4$. Similmente $\sigma^4 = (1\ 3\ 2\ 9)^4(4\ 5)^4(6\ 7\ 8)^4 = (6\ 7\ 8)^4 = (6\ 7\ 8)$ ha periodo 3.

3. È ben definita se, per ogni a, b, si ha che $\sigma^{2a} = \sigma^{2b} \Rightarrow f(\sigma^{2a}) = f(\sigma^{2b})$. Da una parte

$$\sigma^{2a} = \sigma^{2b} \Leftrightarrow \sigma^{2a-2b} = \mathrm{Id} \Leftrightarrow 12 \mid 2a - 2b \Leftrightarrow 6 \mid a - b.$$

Dall'altra parte

$$f(\sigma^{2a}) = f(\sigma^{2b}) \Leftrightarrow \overline{3a} = \overline{3b} \Leftrightarrow 12 \mid 3a - 3b \Leftrightarrow 4 \mid a - b.$$

Pertanto f NON è ben definita. Le altre domande perdono dunque significato.

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

Esercizio 3. 1. (p. 4) Verificare che $\mathrm{MCD}(11907, 1625) = 1$ e determinare la corrispondente identità di Bezout.

2. (p. 3) Dire quali delle seguenti funzioni che hanno $\mathbb{Z}$ come dominio e codominio (pensato come gruppo additivo) sono omomorfismi:

$$f(n) = n^2 - n, \qquad g(n) = -4n, \qquad h(n) = |n|.$$

3. (p. 4) Calcolare il resto della divisione per 13 del numero 3^{780338}.

Soluzione.

1. Applichiamo l'algoritmo di divisione euclideo:

$$\begin{aligned} \underline{11907} &= 7 \cdot \underline{1625} + \underline{532} \\ \underline{1625} &= 3 \cdot \underline{532} + \underline{29} \\ \underline{532} &= 18 \cdot \underline{29} + \underline{10} \\ \underline{29} &= 2 \cdot \underline{10} + \underline{9} \\ \underline{10} &= 1 \cdot \underline{9} + \boxed{\underline{1}} \\ \underline{9} &= 9 \cdot \underline{1} + 0 \end{aligned}$$

Quindi $\mathrm{MCD}(11907, 1625) = 1$. Invertendo la procedura

$$\begin{aligned} \underline{1} &= \underline{10} - \underline{9} \\ &= \underline{10} - (\underline{29} - 2 \cdot \underline{10}) = -\underline{29} + 3 \cdot \underline{10} \\ &= -\underline{29} + 3 \cdot (\underline{532} - 18 \cdot \underline{29}) = 3 \cdot \underline{532} - 55 \cdot \underline{29} \\ &= 3 \cdot \underline{532} - 55 \cdot (\underline{1625} - 3 \cdot \underline{532}) = 168 \cdot \underline{532} - 55 \cdot \underline{1625} \\ &= 168 \cdot (\underline{11907} - 7 \cdot \underline{1625}) - 55\underline{1625} = \boxed{168 \cdot \underline{11907} - 1231 \cdot \underline{1625}}. \end{aligned}$$

2. Si ha $f(1) = 1^2 - 1 = 0$ e $f(2) = 2^2 - 2 = 2$ per cui $f(1+1) = f(2) \neq f(1) + f(1)$ e f non è un omomorfismo.

   Si ha $g(m+n) = -4(m+n) = -4m - 4n = g(m) + g(n)$ per ogni m, $n \in \mathbb{Z}$ e quindi g è un omomorfismo.

   Si ha $h(1) = |1| = 1 = |-1| = h(-1)$ e quindi $2 = h(1) + h(-1) \neq h(1-1) = h(0) = 0$. Perciò h non è un omomorfismo.

3. Poichè 13 è un numero primo risulta $\varphi(13) = 12$ e $3^{12} \equiv 1 \bmod 13$ per il teorema di Eulero-Fermat. Dunque

$$3^{780338} = 3^{12 \cdot 65028 + 2} \equiv 3^2 = 9 \bmod 13.$$