Corso di Studi in Informatica
Matematica Discreta

Prova scritta 23 Gennaio 2018 – 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. Serena ha comprato anche quest'anno 6 regali diversi per i suoi 6 nipotini.

a) Per incartarli ha comprato 6 fogli di carta di colori diversi. In quanti modi può abbinare la carta ai regali?

b) Lo scorso anno aveva comprato per i nipotini 3 modellini di auto (uguali) e 3 giochi da tavolo (tutti diversi). In quanti modi diversi poteva distribuire i regali ai nipoti?

c) Due anni fa ognuno dei 6 regali aveva almeno uno delle seguenti caratteristiche: era stato incartato, aveva un fiocco oppure era grande. Più esattamente: 3 erano incartati, 3erano grandi e 3 avevano sopra un fiocco, 2 erano incartati e grandi, 1 era incartato e con fiocco, e 1 era grande con fiocco. Quanti nipotini hanno ricevuto un pacco grande, incartato e con fiocco?

Soluzione.

a) Una volta numerati i regali, il problema equivale a contare gli ordinamenti dei fogli, che quindi sono 6!.

b) Ci sono $\binom{6}{3}$ modi di scegliere i bambini che che riceveranno le automobiline, mentre ci sono 3! modi di distribuire i giochi ai restanti 3. Pertanto il numero delle possibili distribuzioni è $\binom{6}{3} \cdot 3! = 120$.

c) Dalla formula di inclusione esclusione, detto x il numero dei pacchi che sono contemporaneamente grandi, incartati e con fiocco si trova

$$6 = 3 + 3 + 3 - 2 - 1 - 1 + x$$

da cui $x = 1$.

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

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

a) Determinare la decomposizione in cicli disgiunti di σ e τ.

b) Calcolare il periodo di σ, τ e $\sigma\tau$.

c) Dire perché la funzione $f : \mathbb{Z}_{10} \to \mathcal{S}_7$, $f(\bar{k}) = \sigma^k$ è ben definita, perché è un omomorfismo non suriettivo e determinarne il nucleo.

Soluzione.

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

b) Il periodo di σ è 5, quello di τ è $6 = \mathrm{mcm}(2,3)$. La decomposizione in cicli disgiunti di $\sigma\tau$ è $(2\ 5\ 6)$ per cui il suo periodo è 3.

c) Se $\bar{k} = \bar{\ell}$ si ha $\ell = k + 10n$ per qualche $n \in \mathbb{Z}$. Ma allora $\sigma^k = \sigma^\ell$ perché il periodo di σ divide 10. Dunque f è ben definita.

È un omomorfismo perché $\sigma^{r+s} = \sigma^r\sigma^s$ e non può essere suriettivo perché le potenze di σ (che costituiscono l'immagine di f) sono 5 e non esauriscono l'intero gruppo $\mathcal{S}_8$ che conta molti più elementi. Infine il nucleo $\ker(f)$ è costituito dalle classi $\bar{k} \in \mathbb{Z}_{10}$ tali che $\sigma^k = \mathrm{id}$. Quindi

$$\ker(f) = \{\bar{0}, \bar{5}\}$$

in quanto il periodo di σ è 5.

Esercizio 3. a) Calcolare $\mathrm{MCD}(3575, 654)$ e realizzare l'identità di Bezout.

b) Calcolare il resto della divisione per 27 del numero $3^{12007} + 5^{36184}$.

c) Dire se il gruppo $\mathbb{Z} \times \mathbb{Z}_4$ è ciclico o no.

Soluzione.

a) Applichiamo l'algoritmo di divisione euclideo:

$$\begin{aligned} 3575 &= 5 \cdot 654 + 305 \\ 654 &= 2 \cdot 305 + 44 \\ 305 &= 6 \cdot 44 + 41 \\ 44 &= 1 \cdot 41 + 3 \\ 41 &= 13 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Quindi $\mathrm{MCD}(3575, 654) = 1$. Invertendo la procedura

$$\begin{aligned} 1 &= 3 - 2 \\ &= 14 \cdot 3 - 41 \\ &= 14 \cdot 44 - 15 \cdot 41 \\ &= 104 \cdot 44 - 15 \cdot 305 \\ &= 104 \cdot 654 - 223 \cdot 305 \\ &= 1219 \cdot 654 - 223 \cdot 3575. \end{aligned}$$

b) Calcoliamo $[3^{12007} + 5^{36184}]_{27} = [3^{12007}]_{27} + [5^{36184}]_{27} = [3]_{27}^{12007} + [5]_{27}^{36184}$. Poiché $27 = 3^3$ si ha che $[3]_{27}^k = [0]_{27}$ per ogni $k \geq 3$. Siccome poi $\mathrm{MCD}(5, 27) = 1$ e $\varphi(27) = 18$ si ha $5^{18} \equiv 1 \bmod 27$ per il teorema di Eulero e osservando che $36184 \equiv 4 \bmod 18$ otteniamo alla fine

$$[3^{12007} + 5^{36184}]_{27} = [5]_{27}^4 = [4]_{27}.$$

c) Il gruppo non è ciclico. Se lo fosse, sarebbe il gruppo ciclico con infiniti elementi. Ma il gruppo ciclico con infiniti elementi non possiede elementi di ordine finito mentre in $\mathbb{Z} \times \mathbb{Z}_4$ l'elemento $(0, \bar{1})$ ha periodo 4.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 8 Febbraio 2018 – Versione D

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

MATRICOLA .....

Rispondere a ciascuna domanda, motivando adeguatamente le risposte. Ogni esercizio vale 11 punti. Per essere sufficiente un compito deve raggiungere almeno 18 punti.

Esercizio 1. Ad un corso di tango sono iscritti 8 donne e 12 uomini. Si tengono due lezioni la settimana, il lunedì e il giovedì.

a) Se ad una lezione tutti gli studenti sono presenti, quante sono le possibili coppie (uomo-donna) che si possono formare durante la lezione?

b) Per uno spettacolo alla fine del corso i maestri scelgono fra gli studenti 4 uomini e 4 donne per una certa coreografia. Quante sono le scelte possibili di quei 8 studenti?

c) La scorsa settimana ogni studente era presente ad almeno una lezione: al lunedì erano presenti 8 uomini e 6 donne mentre al giovedì erano presenti 9 uomini e 7 donne. Quanti dei 20 studenti erano presenti ad entrambe le lezioni?

Soluzione.

a) Se D denota l'insieme delle donne e U l'insieme degli uomini, l'insieme delle coppie è l'insieme $D \times U$. Dunque sono possibili $|D \times U| = |D| \cdot |U| = 8 \cdot 12 = 96$ coppie.

b) Si possono scegliere i 5 uomini in $\binom{12}{4}$ modi e le donne in $\binom{8}{4}$ modi. Complessivamente le scelte sono

$$\binom{12}{4} \cdot \binom{8}{4} = \frac{12!}{4!8!} \cdot \frac{8!}{4!4!} = 34350.$$

c) Sia L l'insieme degli studenti presenti il lunedì e G l'insieme degli studenti presenti il giovedì. I dati del problema indicano che $|L \cup G| = 20$, $|L| = 14$ e $|G| = 16$, quindi dal principio di inclusone-esclusione si ottiene che

$$|L \cap G| = |L| + |G| - |L \cap G| = 14 + 16 - 20 = 10.$$

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

Esercizio 2. Consideriamo le seguenti due permutazioni di $\mathcal{S}_9$ date come prodotto di cicli:

$$\alpha = (3\ 7\ 6\ 9\ 5)(2\ 8\ 4), \qquad \beta = (1\ 3\ 7\ 9\ 8\ 4)^2.$$

a) Determinare il periodo di α e β.

b) Calcolare la parità di α, di β e di $\alpha^3 \circ \beta^{-1}$.

c) Dire (motivando la risposta) quali dei seguenti gruppi sono isomorfi a $(\mathbb{Z}_{15}, +)$:

$$H = (\langle\alpha\rangle, \circ), \qquad L = (\mathbb{Z}_3 \times \mathbb{Z}_5, +), \qquad M = (\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5\ , +).$$

Soluzione.

a) α è dato come prodotto di cicli disgiunti ed il suo periodo è $\text{mcm}(3,5) = 15$, mentre la decomposizione in cicli disgiunti di β è $(1\ 7\ 8)(3\ 9\ 4)$ e quindi ha periodo 3.

b) α e β sono pari perché entrambe prodotto di cicli pari. Inoltre anche $\alpha^3 \circ \beta^{-1}$ è pari in quanto prodotto di permutazioni pari.

c) M ha ordine 25 mentre $\mathbb{Z}_{15}$ ha 15 elementi e quindi non possono essere isomorfi.

Invece H e L sono entrambi isomorfi a $\mathbb{Z}_{15}$ perchè sono tutti gruppi ciclici di ordine 15: H lo è per definizione e L lo è in quanto $\text{mcm}(3,5) = 15 = 3 \cdot 5$.

Esercizio 3. Sia $f\colon \mathbb{Z}_{18} \to \mathbb{Z}_9$ data da $f([a]_{18}) = [4a]_9$.

a) Verificare che f è ben definita ed è un omomorfismo tra i gruppi $(\mathbb{Z}_{18}, +)$ e $(\mathbb{Z}_9, +)$.

b) Determinare l'immagine di f è stabilire se f è suriettivo.

c) Determinare tutti i numeri interi x tali che $0 \leq x < 18$ e $[x]_{18} = [7^{344}]_{18}$.

Soluzione.

a) f è ben definita perchè $f([a + 18k]_{18}) = [4a + 108k]_9 = [4a]_9 = f([a]_{18})$. Si tratta di un omomorfismo perchè

$$f([a]_{18} + [b]_{18}) = [6a + 6b]_9 = [4a]_{10} + [4b]_9 = f([a]_{18}) + f([b]_{18}).$$

b) L'immagine di f è costituita da tutti i multipli di 4 in $\mathbb{Z}_9$. Ma poiché $\text{MCD}(4,9) = 1$ la classe $[4]_9$ genera $\mathbb{Z}_9$, cioè $\text{Im}(f) = \mathbb{Z}_9$ ed f è suriettiva.

c) Si può usare direttamente il teorema di Eulero in quanto $MCD(7,18) = 1$. Si ha $\varphi(18) = 6$ e $344 = 6 \cdot 57 + 2$. Quindi

$$[x]_{18} = [7^{344}]_{18} = [7^2]_{18} = [13]_{18},$$

cioè $x = 13$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 13 Giugno 2018 – 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. Anna possiede 11 magliette, 5 paia di pantaloni, 6 paia di scarpe e 2 borsette.

a) In quanti modi diversi Anna può scegliere maglietta, pantaloni, scarpe e borsetta per vestirsi?

b) Anna ha comprato una scarpiera che ha 14 scomparti. In quanti modi diversi Anna può riporre le sue scarpe mettendo ogni paio di scarpe in un diverso scomparto nella scarpiera?

c) Anna parte per un weekend al mare e decide di portare con sè 4 magliette, 2 paia di pantaloni, 2 paia di scarpe e 1 borsetta. Quante sono le possibili scelte di questi capi?

Soluzione.

a) Anna deve scegliere una maglietta, un paio di pantaloni, un paio di scarpe e una borsetta. Questo si può fare in

$$11 \cdot 5 \cdot 6 \cdot 2 = 660$$

modi.

b) Anna deve selezionare ordinatamente 6 scomparti su 14: il numero totale è il numero delle disposizioni semplici

$$D_{14,6} = \frac{14!}{8!} = 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 = 2162160.$$

c) Anna ha $\binom{11}{4} = \frac{11!}{4!7!} = 330$ modi di scegliere 4 magliette, $\binom{5}{2} = \frac{5!}{2!3!} = 10$ modi di scegliere 2 paia di pantaloni, $\binom{6}{2} = \frac{6!}{2!4!} = 15$ modi di scegliere 2 paia di scarpe e $\binom{2}{1} = 2$ modi di scegliere 1 borsetta. Quindi il totale delle possibili scelte è

$$\binom{11}{4} \cdot \binom{5}{2} \cdot \binom{6}{2} \cdot \binom{2}{1} = 330 \cdot 10 \cdot 15 \cdot 2 = 99000.$$

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

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

$$\alpha = (3\ 5)(1\ 2\ 4)(2\ 7\ 4\ 5), \qquad \beta = (1\ 2\ 4\ 7\ 6)(1\ 3\ 5\ 7).$$

a) Determinare la decomposizione in cicli disgiunti di α e di α^2.

b) Calcolare il periodo di α, il periodo di β e il periodo di $\beta \circ \alpha$.

c) Dire perchè la funzione $f : \mathbb{Z}_9 \to \mathcal{S}_7$ data da $f(\bar{k}) = \alpha^k$ è ben definita, perchè é un omomorfismo di gruppi e perchè non é nè iniettiva nè suriettiva.

Soluzione.

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

b) Il periodo di α è $3 = \text{mcm}(3, 3)$. Il periodo di β è $12 = \text{mcm}(4, 3)$. La decomposizione in cicli disgiunti di $\beta \circ \alpha$ è $(1\ 4\ 5\ 7\ 3\ 6)$ per cui il suo periodo è 6.

c) Se $\bar{k} = \bar{\ell}$ in $\mathbb{Z}_9$ si ha $\ell = k + 9n$ per qualche $n \in \mathbb{Z}$. Ma allora $\alpha^k = \alpha^\ell$ perché il periodo 3 di α divide $9n$. Dunque f è ben definita.

È un omomorfismo perché $\alpha^{r+s} = \alpha^r \alpha^s$ e non può essere suriettivo perché le potenze di α (che costituiscono l'immagine di f) sono solo 3 e quindi non esauriscono l'intero gruppo $\mathcal{S}_8$. Infine il nucleo $\ker(f)$ è costituito dalle classi $\bar{k} \in \mathbb{Z}_9$ tali che $\alpha^k = \text{id}$, ossia tali che k è multiplo del periodo di α. Quindi

$$\ker(f) = \{\bar{0}, \bar{3}, \bar{6}\}$$

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

Esercizio 3.

a) Calcolare MCD$(5355, 651)$ e realizzare l'identità di Bezout.

b) Determinare le ultime 2 cifre del numero $17^{20922} + 25^{15775}$.

c) Trovare tutte le soluzioni della congruenza $12x \equiv 16 \bmod 140$.

Soluzione.

a) Applicando l'algoritmo di divisione:

$$\begin{aligned} 5355 &= 8 \cdot 651 + 147 \\ 651 &= 4 \cdot 147 + 63 \\ 147 &= 2 \cdot 63 + 21 \\ 63 &= 3 \cdot 21 \end{aligned}$$

Dunque MCD$(5355, 651) = 21$.

Utilizzando in ordine invertito i calcoli precedenti otteniamo poi:

$$\begin{aligned} 21 &= 147 - 2 \cdot 63 \\ &= 147 - 2(651 - 4 \cdot 147) = -2 \cdot 651 + 9 \cdot 147 \\ &= -2 \cdot 651 + 9(5355 - 8 \cdot 651) = 9 \cdot 5355 - 74 \cdot 651 \end{aligned}$$

b) Siccome $\varphi(100) = \varphi(4)\varphi(25) = 2 \cdot 20$ e MCD$(17, 100) = 1$ si ha $17^{40} \equiv 1 \bmod 100$ per il teorema di Eulero. Dunque

$$17^{20922} = 17^{523 \cdot 40 + 2} \equiv 17^2 \equiv 289 \equiv 89 \bmod 100.$$

Invece MCD$(25, 100) \neq 1$ e quindi non possiamo applicare il teorema di Eulero. Però osserviamo che $25^2 = 625 \equiv 25 \bmod 100$ e quindi, induttivamente, $25^k \equiv 25 \bmod 100$ per qualsiasi esponente $k \geq 1$. Mettendo insieme gli ingredienti,

$$17^{20922} + 25^{15775} \equiv 89 + 25 \equiv 114 \equiv 14 \bmod 100.$$

c) Poiché MCD$(12, 140) = 4$ e 4 divide 16 la congruenza ha soluzioni e queste si ottengono dalla conguenza

$$3x \equiv 4 \bmod 35$$

ottenuta dalla precedente dividendo coefficienti e modulo per 4. Poiché MCD$(3, 35) = 1$ l'ultima congruenza si risolve determinando l'inverso moltiplicativo di 3 modulo 35 e siccome $3 \cdot 12 = 36 = 35 + 1$ tale inverso è 12. Per cui la soluzione dell'ultima conguenza è $x = 12 \cdot 4 = 48 \equiv 13 \bmod 35$. Qundi le soluzioni della congruenza originale modulo 140 sono

$$x_1 = 13, \quad x_2 = 13 + 35 = 48, \quad x_3 = 13 + 2 \cdot 35 = 83, \quad x_4 = 13 + 3 \cdot 35 = 118.$$

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 4 Luglio 2018

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

MATRICOLA .....

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

Esercizio 1. a) Calcolare il numero di anagrammi diversi della parola ALMENO e quelli della parola ADEGUATAMENTE.

b) Ad una gara partecipano 10 squadre ed in palio ci sono 4 premi uguali. Quante possono essere le possibili quaterne di squadre vincitrici?

c) La squadra A ha totalizzato 12 punti. Carlo, Viola e Giovanna, che costituiscono la squadra A, hanno ottenuto rispettivamente c, v e g punti nelle vari prove. Quante sono le possibili terne (c, v, g)?

Soluzione.

a) La parola ALMENO è formata da 6 lettere tutte diverse per cui i suoi anagrammi sono $6! = 720$.

Invece la parola ADEGUATAMENTE è formata da 13 lettere, due delle quali sono presenti 3 volte ed una terza 2 volte e dunque i suoi anagrammi sono $\frac{13|}{2!3!3!} = 86486400$.

b) Poiché i premi sono uguali l'ordine di arrivo non conta e quindi il numero di quaterne possibili sono $\binom{10}{4} = 210$.

c) Il problema consiste nel ripartire 12 punti tra c, g e v. Si tratta quindi di combinazioni con ripetizione e il numero cercato è $\binom{12+3-1}{3-1} = \binom{14}{2} = 91$.

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

Esercizio 2. a) Calcolare il periodo della permutazione

$$\pi = (3\ 4\ 1\ 6)(1\ 6\ 5\ 2) \in \mathcal{S}_6$$

b) Qual è il periodo massimo di una permutazione in $\mathcal{S}_{10}$?

c) Sia $\sigma = (1\ 4)(2\ 5\ 3) \in \mathcal{S}_5$. Dimostrare che $f([k]) = \sigma^{2k}$ definisce un omomorfismo $f : \mathbb{Z}_{18} \to \mathcal{S}_5$ e se ne calcolino nucleo e immagine.

Soluzione.

a) La scrittura di π in cicli disgiunti è $(1\ 3\ 4)(2\ 6\ 5)$. Quindi π ha tipo $(3, 3)$ e periodo $\mathrm{mcm}(3, 3) = 3$.

b) Il periodo di una permutazione è il mcm delle lunghezze del suo tipo, per cui bisogna massimizzare il mcm degli addendi di una somma che totalizza al massimo 10. Un'analisi delle possibilità mostra che il massimo periodo è 30, per una permutazione di tipo $(5, 3, 2)$.

c) La scrittura di σ è già una composizione di cicli disgiunti, quindi il suo periodo è 6. A questo punto:

1. La funzione f è ben definita perché se $[k] = [l]$ allora $l = k + 18n$ per qualche $n \in \mathbb{Z}$ e dunque $f([l]) = \sigma^{2l} = \sigma^{2k}\sigma^{36n} = \sigma^{2k} = f([k])$.
2. Una volta che f è ben definita il fatto che sia un omomorfismo segue subito dalla regola delle potenze: $\sigma^{2k}\sigma^{2l} = \sigma^{2(k+l)}$.
3. L'immagine di f è costituita da tutte le potenze di σ con esponente pari. Siccome σ ha periodo 6 queste potenze sono $\{1, \sigma^2, \sigma^4\}$.
4. Il nucleo di f è formato da tutte quelle classi $[k] \in \mathbb{Z}_{18}$ tali che $2k$ è un multiplo del periodo di σ (cioè 6). Dunque

$$\ker(f) = \{[0], [3], [6], [9], [12], [15]\}.$$

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

Esercizio 3.

a) Scrivere il numero 15497 in base 8.

b) Calcolare il resto della divisione di 11^{95774} per 28.

c) Dei seguenti gruppi additivi uno solo è ciclico. Dire quale ed esibirne 2 generatori espliciti:

$$\mathbb{Z}_{10} \times \mathbb{Z}_{22}, \qquad \mathbb{Z}_{15} \times \mathbb{Z}_{26}, \qquad \mathbb{Z}_{18} \times \mathbb{Z}_{21}.$$

Soluzione.

a) Dividiamo ripetutamente per 8 mettendo da parte il resto fino ad ottenere quoziente 0. Si ha

$$\begin{aligned} 15497 &= 1937 \cdot 8 + 1 \\ 1937 &= 242 \cdot 8 + 1 \\ 242 &= 30 \cdot 8 + 2 \\ 30 &= 3 \cdot 8 + 6 \\ 3 &= 0 \cdot 8 + 3 \end{aligned}$$

Dunque $15497 = [36211]_8$.

b) Poiché $\mathrm{MCD}(11, 28) = 1$ e $\varphi(28) = \varphi(4)\varphi(7) = 2 \cdot 6 = 12$ il teorema di Eulero dice che $11^{12k} \equiv 1 \bmod 28$ per ogni $k \in \mathbb{Z}$.

Allora basta dividere $95774 = 7981 \cdot 12 + 2$ per ottenere

$$[11^{95774}]_{28} = [11]_{28}^{7981 \cdot 12}[11]_{28}^{2} = [121]_{28} = [9]_{28}.$$

c) Il gruppo additivo $\mathbb{Z}_m \times \mathbb{Z}_n$ è ciclico se e soltanto se $\mathrm{MCD}(m, n) = 1$, pertanto fra quelli elencati l'unico ciclico è $\mathbb{Z}_{15} \times \mathbb{Z}_{26}$.

Per scrivere generatori espliciti basta tener presente che $([a]_{15}, [b]_{26})$ genera $\mathbb{Z}_{15} \times \mathbb{Z}_{26}$ se e soltanto se $[a]_{15}$ genera $\mathbb{Z}_{15}$ e $[b]_{26}$ genera $\mathbb{Z}_{26}$, ovvero

$$([a]_{15}, [b]_{26}) \text{ genera } \mathbb{Z}_{15} \times \mathbb{Z}_{26} \text{ se e soltanto se } \mathrm{MCD}(a, 15) = \mathrm{MCD}(b, 26) = 1.$$

Corso di Studi in Informatica
Matematica Discreta

Prova scritta del 21 settembre 2018

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

MATRICOLA .....

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

Esercizio 1. Un certo corso di studi universitario comporta il superamento di 15 esami. Di questi 15 esami, sette sono obbligatori. Degli altri otto, 4 o 5 vanno scelti in un gruppo A di 9 esami, mentre i rimanenti 3 o 4 vanno scelti in un gruppo B di 6 esami (B disgiunto da A, ossia $A \cap B = \emptyset$).

a) Quanti sono i piani di studio possibili per quel corso di studi?

b) Alberto ha scelto 4 esami dal gruppo A e 4 dal gruppo B. In quanti modi può sostenere questi otto esami se quelli del gruppo A vanno sostenuti prima di quelli del gruppo B?

c) Elena aveva scelto un piano di studi con 5 esami del gruppo A e 3 del gruppo B e aveva già sostenuto 2 esami del gruppo A. Ora però vuole cambiare piano sostituendo 2 qualsiasi degli esami rimanenti del gruppo A con 1 (non già scelto) del gruppo A e uno (non già scelto) del gruppo B. Quanti modi ha di farlo?

Soluzione.

a) Ci sono 2 casi.

- Se si scelgono 4 esami del gruppo A (su 9 disponibili) e quindi 4 dal gruppo B (su 6 disponibili) il numero totale delle scelte per gli esami facoltativi è $\binom{9}{4} \cdot \binom{6}{4}$.
- Se si scelgono 5 esami del gruppo A (su 9 disponibili) e quindi 3 dal gruppo B (su 6 disponibili) il numero totale delle scelte per gli esami facoltativi è $\binom{9}{5} \cdot \binom{6}{3}$.

Poiché c'è una sola scelta per gli esami obbligatori il totale delle scelte possibili dei 15 esami è

$$\binom{9}{4} \cdot \binom{6}{4} + \binom{9}{5} \cdot \binom{6}{3} = \frac{9!}{4! \cdot 5!} \frac{6!}{4! \cdot 2!} + \frac{9!}{5! \cdot 4!} \frac{6!}{3! \cdot 3!} = 126 \cdot 15 + 126 \cdot 20 = 4410.$$

b) Ogni gruppo di 4 esami può essere ordinato in $4! = 24$ modi. Poiché gli esami del gruppo A devono precedere quelli del gruppo B e l'ordinamento di un tipo non influenza quello dell'altro, gli ordinamenti possibili degli 8 esami facoltativi sono

$$4! \cdot 4! = 24^2 = 576.$$

c) Avendo sostenuto 2 dei sue esami del gruppo A sui 5 scelti, Elena deve sceglierne 2 da scartare sui 3 rimanenti e questo può farlo in $\binom{3}{2} = 3$ modi. Ognuno di questi scarti deve essere sostituito con 1 esame del gruppo A, quindi tante possibiltà quanti sono gli esami non scelti inizialmente, cioè $4 = 9 - 5$ e 1 dal gruppo B, quindi tante possibiltà quanti sono gli esami non scelti inizialmente, cioè$3 = 6 - 3$. Il totale dei modi di cambiare piano è dunque

$$3 \cdot 4 \cdot 3 = 36.$$

Esercizio 2.
Si consideri il gruppo S_{10} delle permutazioni degli elementi dell'insieme $\{1, 2, \ldots, 10\}$ con l'operazione di composizione e la permutazione

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

a) Determinare la decomposizione in cicli disgiunti di σ e stabilire se σ è una permutazione pari oppure dispari.

b) Calcolare σ^2 e σ^{-1}.

c) Determinare tutti gli elementi del sottogruppo $\langle\sigma\rangle = \{\sigma^k \mid k \in \mathbb{Z}\} \subset S_{10}$.

d) Verificare che la funzione $f : (\langle\sigma\rangle, \circ) \to (\mathbb{Z}_3, +)$ data da $f(\sigma^k) = [k]_3$ è un omomorfismo di gruppi e determinare il nucleo di f.

Soluzione.

a) La decomposizione in cicli disgiunti è $(1\ 6)(2\ 5\ 10)(3\ 9\ 8)$. Poiché σ è composizione di uno scambio e due cicli di lunghezza 3 è una permutazione dispari.

b) Lavorando con la decomposizione in cicli disgiunti si ha

$$\sigma^2 = (1\ 6)^2(2\ 5\ 10)^2(3\ 9\ 8)^2 = (2\ 10\ 5)(3\ 8\ 9)$$

e

$$\sigma^{-1} = (1\ 6)^{-1}(2\ 5\ 10)^{-1}(3\ 9\ 8)^{-1} = (1\ 6)(2\ 10\ 5)(3\ 8\ 9) = (1\ 6)\sigma^2.$$

c) Poiché il periodo di σ è $\mathrm{mcm}(2, 3) = 6$ si ha

$$\langle\sigma\rangle = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}.$$

d) La funzione f è ben definita perchè il periodo di σ è 6 (calcolato prima) e $[6]_3 = [0]_3$. La funzione f è allora un omomorfismo in conseguenza della legge delle potenze $\sigma^k \circ \sigma^l = \sigma^{k+l}$:

$$f(\sigma^k \circ \sigma^l) = f(\sigma^{k+l}) = [k + l]_3 = [k]_3 + [l]_3 = f(\sigma^k) + f(\sigma^l).$$

Infine

$$\ker(f) = \{\sigma^k \in \langle\sigma\rangle \mid [k]_3 = [0]_3\} = \{\mathrm{id}, \sigma^3\}.$$

Esercizio 3.
Sia $U = \mathbb{Z}_{10}^*$ il gruppo delle classi resto invertibili di $\mathbb{Z}_{10}$.

a) Trovare due elementi non nulli in $\mathbb{Z}_{10}$ il cui prodotto è nullo.

b) Provare che $a = [3^{303}]_{10}$ appartiene a U e che U coincide col gruppo ciclico $\langle a \rangle$.

c) Risolvere la congruenza $6x \equiv 8 \bmod 20$.

Soluzione.

a) Ad esempio $[2]_{10} \cdot [5]_{10} = [0]_{10}$.

b) Osservato che $[3]_{10}$ è invertibile, $[3^{303}]_{10} = [3]_{10}^{303}$ risulta invertibile in quanto potenza di un invertibile. Poiché $\varphi(10) = 4$ il teorema di Eulero dice che

$$a = [3]_{10}^{303} = [3]_{10}^{3} = [7]_{10}.$$

Ma allora le potenze di a (omettendo per brevità il segno di classe) sono:

$$a^0 = 1, \quad a^1 = 7, \quad a^2 = 9, \quad a^3 = 3$$

e questo elenco esaurisce i 4 elementi di U, quindi $U = \langle a \rangle$.

c) Sia ha $\mathrm{MCD}(6, 20) = 2$ e $2 \mid 8$, dunque la congruenza può essere riscritta come

$$3x \equiv 4 \bmod 10$$

Poichè 7 è l'inverso moltiplicativo modulo 10 di 3 l'ultima congruenza ha come unica soluzione (modulo 10)

$$x = 7 \cdot 4 \equiv 8 \bmod 10.$$

Dunque le soluzioni della congruenza originale (modulo 20) sono:

$$x \equiv 8 \bmod 20 \qquad \text{e} \qquad x \equiv 18 \bmod 20.$$