Corso di Studi in Informatica
Matematica Discreta

Prova scritta 14 Luglio 2020

Esercizio 1. I circoli di tennis "Laver" e "Rosewall" si sfidano su un match di 7 incontri: 4 singolari maschili, 2 singolari femminili ed un doppio misto. Il doppio misto è giocato da tennisti e tenniste già selezionate per i singoli.

1. Il circolo "Laver" ha 8 tennisti e 5 tenniste di buon livello tra cui selezionare la squadra. Quante sono le squadre possibili tra cui il "Laver" deve sceglierne una?

2. Formate le squadre, i partecipanti verranno accoppiati casualmente (tennisti con tennisti e tenniste con tenniste) per i 6 singolari e un tennista ed una tennista per squadra verranno sorteggiati per il doppio misto. Quanti sono teoricamente i possibili accoppiamenti fra le due squadre?

3. I sette incontri vengono disputati consecutivamente: prima i 4 singoli maschili, poi i 2 singoli femminili, poi il doppio. Quanti sono i possibili ordinamenti dei sette incontri?

Soluzione.

1. Il "Laver" deve scegliere 4 tennisti fra 8 e 2 tenniste fra 5. Poiché le scelte sono indipendenti il numero totale è

$$\binom{8}{4} \cdot \binom{5}{2} = \frac{8!}{4! \cdot 4!} \cdot \frac{5!}{3! \cdot 2!} = 700.$$

2. Ci sono $4! = 24$ modi di accoppiare i tennisti fra di loro e $2! = 2$ modi per le tenniste. Inoltre ogni squadra può scegliere $4 \cdot 2 = 8$ diverse coppie miste che quindi daranno luogo ad $8^2 = 64$ possibili accoppiamenti per il doppio. Poichè tutte queste scelte sono fra loro indipendenti il totale dei possibili abbinamenti è

$$24 \cdot 2 \cdot 64 = 3072.$$

3. Ci sono $4! = 24$ per ordinare i singolari maschili e $2! = 2$ per ordinare i singolari femminili. Siccome l'unico incontro di doppio verrà giocato per ultimo il totale degli ordinamenti è $24 \cdot 2 \cdot 1 = 48$.

Esercizio 2. 1. Risolvere la congruenza $15X \equiv 6 \bmod 33$ In $\mathbb{Z}_{33}$.

2. Verificare che il gruppo moltiplicativo $\mathbb{Z}_{11}^{\times}$ delle classi invertibili modulo 11 è ciclico e generato da $[2]_{11}$. Determinare tutti gli altri generatori.

3. Dimostrare che la funzione $f : \mathbb{Z}_{11}^{\times} \to \mathbb{Z}_{20}$, $f([2]_{11}^k) = [2k]_{20}$ è un omomorfismo iniettivo.

Soluzione.

1. Poiché $3 = \text{MCD}(15, 33)$ divide 6 la congruenza si riduce a $5X \equiv 2 \bmod 11$ che ha $\overline{7}$ come unica soluzione modulo 11. Quindi le soluzioni in $\mathbb{Z}_{33}$ sono $\{[7]_{33}, [18]_{33}, [29]_{33}\}$.

2. Il calcolo diretto delle potenze $[2]_{11}^k$ mostra che $[2]_{11}$ genera $\mathbb{Z}_{11}^\times$. Dunque i generatori sono le potenze $[2]_{11}^k$ con $\mathrm{MCD}(k, 10) = 1$, ovvero

$$[2]_{11}, \quad [2]_{11}^3 = [8]_{11}, \quad [2]_{11}^7 = [7]_{11}, \quad [2]_{11}^9 = [6]_{11}.$$

3. Siccome il periodo di $[2]_{11}$ è 10 per controllare che f è ben definita basta osservare che se 10 divide $r - s$ allora 20 divide $2r - 2s = 2(r - s)$. È un omomorfismo perché

$$f([2]_{11}^r \cdot [2]_{11}^s) = f([2]_{11}^{r+s}) = \overline{2(r+s)} = \overline{2r} + \overline{2s} = f([2]_{11}^r) + f([2]_{11}^s).$$

ed è iniettivo perché 20 divide $2k$ se e soltanto se 10 divide k, cosicché $\ker(f) = \{[1]_{11}\}$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 15 Giugno 2020

Esercizio 1. 1. (Punti 4) Verificare che $\mathrm{MCD}(142, 112) = 2$ e determinare la corrispondente identità di Bezout.

2. (Punti 4) Determinare l'inversa moltiplicativa di $\overline{56}$ in $\mathbb{Z}_{71}$.

3. (Punti 4) Elencare esplicitamente i generatori del gruppo additivo $(\mathbb{Z}_{18}, +)$.

Soluzione.

1. L'algoritmo di divisione euclidea fornisce

$$\begin{aligned} 142 &= 112 + 30 \\ 112 &= 3 \cdot 30 + 22 \\ 30 &= 22 + 8 \\ 22 &= 2 \cdot 8 + 6 \\ 8 &= 6 + 2 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

confermando che $\mathrm{MCD}(142, 112) = 2$. Invertendo la procedura si ottiene l'identità di Bezout

$$2 = 15 \cdot 142 - 19 \cdot 56.$$

2. Dividendo per 2 l'identità del punto precedente si ottiene subito

$$1 = 15 \cdot 71 - 19 \cdot 112$$

da cui $[56]_{71}^{-1} = [-19]_{71} = [52]_{71}$.

3. I generatori di $\mathbb{Z}_{18}$ sono $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\}$.

Esercizio 2. Consideriamo la permutazione $\pi = (3\ 7\ 8)(2\ 3\ 5)(1\ 4\ 5\ 6\ 9)(7\ 9) \in \mathcal{S}_9$

1. (Punti 4) Determinare tipo, periodo e parità di π.

2. (Punti 4) Qual è il più piccolo $k > 0$ tale che π^k è un ciclo?

3. (Punti 4) Dimostrare che la funzione $f : \langle \pi \rangle \to \mathbb{Z}_8$, $f(\pi^t) = \overline{2t}$ è un omomorfismo ben definito. È iniettiva? È suriettiva?

Soluzione.

1. La decomposizione in cicli disgiunti di π è

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

Dunque il tipo è $(5, 4)$, il periodo 20 e la permutazione è dispari.

2. Si ha che $\pi^k = (1\ 4\ 2\ 7)^k(3\ 5\ 6\ 9\ 8)^k$ è un ciclo quando uno dei due fattori è l'identità e l'altro è un ciclo. Il più piccolo valore per cui questo accade è $k = 4$.

3. Ricordando che il periodo di π è 20 per verificare che f è ben definita basta osservare che se 20 divide $s - t$ allora 8 divide $2s - 2t = 2(s - t)$ ed è un omomorfismo perché

$$f(\pi^s \circ \pi^t) = f(\pi^{s+t}) = \overline{2(s+t)} = \overline{2s} + \overline{2t} = f(\pi^s) + f(\pi^t).$$

   Non è iniettivo perché il dominio ha più elementi del codominio e non è suriettivo perchè le classi $\overline{n}$ con n dispari non sono nell'immagine di f.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 12 Febbraio 2020 – 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. (Punti 3) In quanti modi diversi 4 persone possono sedersi in una fila di 10 sedie?
2. (Punti 4) Un allenatore di calcio ha nella sua squadra 3 portieri, 8 difensori, 8 centrocampisti e 6 attaccanti. In quanti modi diversi può scegliere 1 portiere, 4 difensori, 4 centrocampisti e 2 attaccanti?
3. (Punti 4) Ho 15 monete da 1 euro e 4 salvadanai. In quanti modi diversi posso mettere tutte le monete nei 4 salvadanai in modo che nessun salvadanaio sia vuoto?

Soluzione.

1. Sono dati dalle disposizioni semplici $D_{10,4} = 10 \cdot 9 \cdot 8 \cdot 7$
2. I modi in cui scegliere 1 portiere tra 3 è dato da $\binom{3}{1}$; i modi in cui scegliere 4 difensori tra 8 è dato da $\binom{8}{4}$; i modi in cui scegliere 4 centrocampisti tra 8 è dato da $\binom{8}{4}$; i modi in cui scegliere 2 attaccanti tra 6 è dato da $\binom{6}{2}$. In totale, l'allenatore può effettuare $\binom{3}{1} \cdot \binom{8}{4} \cdot \binom{8}{4} \cdot \binom{6}{2}$ scelte.
3. Siccome ogni salvadanaio deve contenere almeno una moneta, rimangono 11 monete da distribuire nei 4 salvadanai. I modi in cui farlo sono dati dalle combinazioni con ripetizione $C^r_{4,11} = \binom{11+4-1}{4-1} = \binom{14}{3}$

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

Esercizio 2. 1. (Punti 3) Calcolare la decomposizione in cicli disgiunti della permutazione

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

2. (Punti 4) Determinare tipo, periodo e parità della permutazione σ^2 (con σ del punto precedente).

3. (Punti 4) Si considerino le permutazioni $\alpha = (1\ 3\ 5\ 6)(2\ 4)$ e $\beta = (1\ 5)(3\ 6)(2\ 7\ 4)$ in $\mathcal{S}_8$. Calcolare $\langle\alpha\rangle \cap \langle\beta\rangle$.

Soluzione.

1. Il calcolo fornisce $\sigma = (1\ 7\ 6\ 8\ 3)(2\ 4\ 5)$.

2. Si ha $\sigma^2 = (1\ 6\ 3\ 7\ 8)(2\ 5\ 4)$ che ha tipo $(3, 5)$, periodo $\mathrm{mcm}(3, 5) = 15$ ed è pari.

3. Poiché α e β sono già dati come composizione di cicli disgiunti i loro periodi sono rispettivamente $\mathrm{mcm}(2, 4) = 4$ e $\mathrm{mcm}(2, 2, 3) = 6$. Quindi si ha

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

Il calcolo esplicito mostra che l'unica uguaglianza non banale è $\alpha^2 = \beta^3 = (1\ 5)(3\ 6)$ e quindi

$$\langle\alpha\rangle \cap \langle\beta\rangle = \{\mathrm{id}, (1\ 5)(3\ 6)\}.$$

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

Esercizio 3. 1. (Punti 3) Si consideri il gruppo $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$, determinare l'ordine di $\langle(6,5)\rangle$ e $\langle(5,6)\rangle$.

2. (Punti 4) Determinare le soluzioni della congruenza $12x \equiv 16 \pmod{40}$ in $\mathbb{Z}_{40}$.

3. (Punti 4) Sia $(G, *)$ un gruppo ciclico di ordine 30 con generatore g, dimostrare che la seguente funzione è ben definita ed è un omomorfismo di gruppi

$$\varphi : G \longrightarrow \mathbb{Z}_{18}, \quad \varphi(g^k) = \overline{6k}.$$

Dire se si tratta di un omomorfismo iniettivo e/o suriettivo.

Soluzione.

1. Il più piccolo intero k tale per cui $6k \equiv 0 \pmod{24}$ è 4, ovvero l'ordine del sottogruppo ciclico $\langle 6\rangle$ di $\mathbb{Z}_{24}$ è 4. Analogamente il più piccolo intero k tale per cui $5k \equiv 0 \pmod{30}$ è 6, ovvero l'ordine del sottogruppo ciclico $\langle 5\rangle$ di $\mathbb{Z}_{30}$ è 6. Dunque l'ordine del sottogruppo ciclico $\langle(6,5)\rangle$ è $\text{mcm}(4,6) = 12$.
Analogamente si osserva che l'ordine di $\langle 5\rangle$ in $\mathbb{Z}_{24}$ è 24 e l'ordine di $\langle 6\rangle$ in $\mathbb{Z}_{30}$ è 5. Quindi $|\langle(5,6)\rangle| = \text{mcm}(24,5) = 120$.

2. Siccome $\text{MCD}(12,40) = 4$ divide 16, la congruenza ha soluzioni che si ottengono risolvendo la congruenza $3x \equiv 4 \pmod{10}$. Tale congruenza si risolve facilmente calcolando l'inverso di 3 in $\mathbb{Z}_{10}$ che è 7, da cui $x \equiv 8 \pmod{10}$. Quindi le soluzioni della congruenza in $\mathbb{Z}_{40}$ sono $\overline{8}, \overline{18}, \overline{28}, \overline{38}$.

3. Siccome G è un gruppo ciclico di ordine 30 e generatore g un suo generico elemento sarà della forma g^k con k intero compreso tra 0 e 29. Inoltre, siccome G ha ordine 30, per ogni intero h si ha $g^k = g^{k+30h}$. Per verificare che φ sia ben definita occorre che $\varphi(g^k) = \varphi(g^{k+30h})$ e in effetti:

$$\varphi(g^{k+30h}) = \overline{6(k+30h)} = \overline{6k+180h} = \overline{6k} = \varphi(g^k)$$

in quanto $180 = 6 \cdot 3 \cdot 10 \equiv 0 \pmod{18}$.
Per ogni $g^a, g^b \in G$ si ha

$$\varphi(g^a * g^b) = \varphi(g^{a+b}) = \overline{6(a+b)} = \overline{6a} + \overline{6b} = \varphi(g^a) + \varphi(g^b),$$

ovvero φ è un omomorfismo.
Siccome $|G| > |\mathbb{Z}_{18}|$, φ non può essere iniettiva e non è suriettiva poiché $Im\varphi = \{\overline{0}, \overline{6}, \overline{12}\}$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 23 Gennaio 2020 – 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. (Punti 3) Calcolare il numero degli anagrammi della parola

PARALLELEPIPEDO.

2. (Punti 4) Si consideri l'insieme $\mathcal{A} = \{A, B, C, D, E, F, 1, 2, 3, 4\}$ i cui elementi sono lettere e cifre. Calcolare il numero degli ordinamenti di $\mathcal{A}$ in cui compaiono solo cifre nei due posti centrali.

3. (Punti 4) Sia $\mathcal{A}$ l'insieme del punto precedente. Calcolare il numero dei sottoinsiemi di A costituiti da 2 lettere e 3 cifre.

Soluzione.

1. La parola PARALLELEPIPEDO è costituita da 15 lettere di cui la A ripetuta 2 volte, la E 3 volte, la L 3 volte e la P 3 volte. Dunque applicando la formula si ottiene immediatamente
$$\frac{15!}{(3!)^3 \cdot 2!} = 3,027,024,000.$$

2. Poiché le cifre a disposizione sono 4 ci sono $4 \cdot 3 = 12$ modi di piazzare 2 cifre nei posti centrali. Gli altri 8 simboli possono essere ordinati a piacere nei posti restanti per cui il totale degli ordinamenti voluti è
$$12 \cdot 8! = 483,840.$$

3. Ci sono $\binom{6}{2}$ scelte di 2 lettere fra le 6 a disposizione e $\binom{4}{3}$ modi di scegliere 3 lettere fra 4. Quindi il totale dei sottoinsiemi come da richiesta è
$$\binom{6}{2} \cdot \binom{4}{3} = \frac{6!}{2! \cdot 4!} \cdot \frac{4!}{3! \cdot 1!} = 15 \cdot 4 = 60.$$

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

Esercizio 2. Si considerino le seguenti permutazioni in S_8:

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

1. (Punti 3) Scrivere σ, τ, $(\sigma \circ \tau)^{-1}$ come prodotto di cicli disgiunti e determinarne il periodo.
2. (Punti 4) Scrivere $(\sigma \circ \tau)^{9074}$ come prodotto di cicli disgiunti.
3. (Punti 4) Dimostrare che $H = \{\alpha \in S_8 : \alpha \circ \sigma = \sigma \circ \alpha\}$ è un sottogruppo di S_8. Esibire un elemento in H diverso dall'identità e un elemento che non appartiene ad H.

Soluzione.

1. Si ha
$$\sigma = (1428)(35)(67), \quad \tau = (256)(378), \quad (\sigma \circ \tau)^{-1} = (17586324).$$
Dunque σ ha periodo 4, τ ha periodo 3, $(\sigma \circ \tau)^{-1}$ ha periodo 8
2. Siccome $\sigma \circ \tau = (14236857)$ ha periodo 8, si ha
$$(\sigma \circ \tau)^{9074} = (\sigma \circ \tau)^{8 \cdot 1134 + 2} = (\sigma \circ \tau)^2 = (1265)(3874).$$
3. Si osservi che $\beta \in H$ implica $\beta^{-1} \in H$, infatti
$$\beta \circ \sigma = \sigma \circ \beta \Rightarrow (\beta^{-1} \circ \beta) \circ (\sigma \circ \beta^{-1}) = (\beta^{-1} \circ \sigma) \circ (\beta \circ \beta^{-1}) \Rightarrow \sigma \circ \beta^{-1} = \beta^{-1} \circ \sigma,$$
avendo moltiplicato ambo i membri della prima ugualianza per β^{-1} sia a sinistra che a destra e avendo usato la proprietà associativa dell'operazione. Ora, per ogni $\alpha, \beta \in H$ dimostriamo che $\alpha \circ \beta^{-1} \in H$:
$$(\alpha \circ \beta^{-1}) \circ \sigma = \alpha \circ (\beta^{-1} \circ \sigma) = \alpha \circ (\sigma \circ \beta^{-1}) = (\alpha \circ \sigma) \circ \beta^{-1} = (\sigma \circ \alpha) \circ \beta^{-1} = \sigma \circ (\alpha \circ \beta^{-1}).$$
Un elemento diverso dall'identità in H è la permutazione σ^2, infatti $\sigma^2 \circ \sigma = \sigma^3$ e $\sigma \circ \sigma^2 = \sigma^3$. Un elemento che non appartiene ad H è τ, infatti $\sigma \circ \tau \neq \tau \circ \sigma$.

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

Esercizio 3. 1. (Punti 4) Solo una tra le classi $\overline{5}$, $\overline{6}$ e $\overline{14}$ è invertibile in $\mathbb{Z}_{28}$. Dire quale e calcolarne l'inversa.

2. (Punti 4) Calcolare il resto della divisione di 7^{530} per 32.

3. (Punti 3) Si considerino le seguenti funzioni $\mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ e si dica quali sono omomorfismi di gruppo e quali no.

$$f(a,b) = 5a - 2b, \qquad g(a,b) = 2a + 3b - 1, \qquad h(a,b) = a^2 - 5b.$$

Soluzione.

1. La classe invertibile è $\overline{5}$ perché $\mathrm{MCD}(5,28) = 1$ mentre $\mathrm{MCD}(6,28) = 2$ e $\mathrm{MCD}(14,28) = 14$. Il calcolo dell'identità di Bezout mediante l'algoritmo di divisione fornisce

$$1 = 2 \cdot 28 - 11 \cdot 5$$

per cui $\overline{5}^{-1} = \overline{-11} = \overline{17}$.

2. Poiché $\mathrm{MCD}(7,32) = 1$ possiamo applicare il teorema di Eulero. Siccome $\varphi(32) = \varphi(2^5) = (2-1)\cdot 2^4 = 16$ e $530 = 33 \cdot 16 + 2$ si ottiene

$$[7^{530}]_{32} = [7]_{32}^{530} = [7]_{32}^{2} = [49]_{32} = [17]_{32}.$$

Quindi i resto è 17.

3. L'unico omomorfismo è f in quanto

$$f(a,b) + f(a',b') = (5a - 2b) + (5a' - 2b') = 5(a+a') - 2(b+b') = f(a+a', b+b')$$

per ogni a, b, a', $b' \in \mathbb{Z}$. La funzione g non è un omomorfismo perché $g(0,0) = -1 \neq 0$ e h neppure perchè, ad esempio, $h(2,0) = 4$ mentre $h(1,0) + h(1,0) = 1 + 1 = 2$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 3 Febbraio 2021

Turno 1, Problema 1: Una ditta associa ad ogni impiegato un codice numerico di 6 cifre. Calcolare il numero dei codici possibili in ciascuno dei casi seguenti.

1. (Punti 3) Un codice deve alternare cifre pari a cifre dispari e non può contenere cifre ripetute.

2. (Punti 4) Un codice non può cominciare con la cifra 0 ed inoltre la somma delle cifre che lo compongono deve essere pari.

3. (Punti 4) Un codice non può contenere la cifra 0 più di due volte.

Soluzione:

1. La prima cifra può essere qualunque. La seconda anche può essere qualunque purché di parità diversa dalla prima. La terza deve avere la stessa parità della prima ma non essere uguale, e così via. Poiché ci sono in tutto 5 cifre pari e 5 dispari, il totale delle possibilità è
$$10 \cdot 5 \cdot 4 \cdot 4 \cdot 3 \cdot 3 = 7200.$$

2. Ci sono 9 scelte per la prima cifra e 10 per ogni scelta dalla seconda alla quinta. L'ultima deve essere scelta in modo da rendere pari la somma delle cifre e quindi andrà scelta (a seconda dei casi) solo tra le cifre pari o quelle dispari limitando a 5 il numero delle scelte. Quindi il totale delle possibilità è
$$9 \cdot 10^4 \cdot 5 = 450000.$$

3. Ci sono
   - 9^6 codici che non contengono la cifra 0 (9 scelte arbitrarie per ogni cifra);
   - $6 \cdot 9^5$ codici che contengono esattamente una volta la cifra 0 (5 scelte arbitrarie di una cifra fra 9 e 6 scelte per dove collocare lo 0);
   - $\binom{6}{2} \cdot 9^4$ codici che contengono 0 esattamente 2 volte (4 scelte arbitrarie di una cifra fra 9 e $\binom{6}{2}$ scelte per dove collocare gli 0)-

   . Dunque il totale è $9^6 + 6 \cdot 9^5 + \binom{6}{2} \cdot 9^4 = 984150$.

Turno 1, Problema 2: Si consideri in S_9 la permutazione $\sigma = (15782)(2496)$.

1. (Punti 3) Si scriva σ come prodotto di cicli disgiunti e si calcoli σ^{-1}.
2. (Punti 4) Si calcoli il periodo di σ^{98}.
3. (Punti 4) Dimostrare che la funzione

$$f : \langle\sigma\rangle \to \mathbb{Z}_{12}, \quad \sigma^t \mapsto \overline{3t}$$

è ben definita. f è iniettiva? f è suriettiva?

Soluzione:

1. $\sigma = (1\ 5\ 7\ 8\ 2\ 4\ 9\ 6)$ e quindi $\sigma^{-1} = (1\ 6\ 9\ 4\ 2\ 8\ 7\ 5)$.
2. Siccome σ è un ciclo di lunghezza, e quindi di periodo, 8 si ha

$$\sigma^{98} = \sigma^2 = (1\ 7\ 2\ 9)(5\ 8\ 4\ 6)$$

che ha tipo $(4, 4)$ e quindi periodo 4.

3. Sempre perché σ ha periodo 8 si ha $\sigma^s = \sigma^t$ se e soltanto se $8 \mid s - t$. Ma allora $12 \mid 3s - 3t$ e $\overline{s} = \overline{t}$ in $\mathbb{Z}_{12}$.

   La funzione f non è iniettiva in quanto, ad esempio, $f(\sigma^0) = f(\sigma^4) = \overline{0}$ ma $\sigma^0 \neq \sigma^4$.

   La funzione f non è suriettiva in quanto le classi della forma $\overline{3t}$ non esauriscono le classi in $\mathbb{Z}_{12}$, ad esempio $\overline{3t} \neq \overline{1}$ per ogni t.

Turno 2, Problema 1: Svolgere i punti seguenti.

1. (Punti 3) Determinare l'inverso di $\overline{72}$ in $\mathbb{Z}_{125}$.
2. (Punti 4) Elencare le soluzioni in $\mathbb{Z}_{68}$ della congruenza $12X \equiv 8 \bmod 68$.
3. (Punti 4) Dire quante sono le classi $\overline{x} \in \mathbb{Z}_{11}$ tali che $\overline{5}^k = \overline{x}$ per qualche $k \in \mathbb{N}$.

Soluzione:

1. L'applicazione ripetuta dell'algoritmo di divisione euclidea applicata inizialmente alla coppia $(125, 72)$ conduce all'identità di Bezout

$$33 \cdot 72 - 15 \cdot 125 = 1$$

da cui $\overline{72}^{-1} = \overline{33} \in \mathbb{Z}_{125}$.

2. Si ha che $4 = \mathrm{MCD}(12, 68)$ divide 8 e quindi la congruenza assegnata si riduce a

$$3X \equiv 2 \bmod 17$$

che ha come unica soluzione $X \equiv 12 \bmod 17$. Allora le soluzioni in $\mathbb{Z}_{68}$ sono

$$\{\overline{12}, \overline{29}, \overline{46}, \overline{63}\}.$$

3. Le classi della forma $\overline{5}^k$ sono esattamente quelle nel sottogruppo di $\mathbb{Z}_{11}^\times$ generato da $\overline{5}$ e quindi sono le 5 classi

$$\overline{5}^0 = \overline{1}, \quad \overline{5}^2 = \overline{3}, \quad \overline{5}^3 = \overline{4}, \quad \overline{5}^4 = \overline{9}$$

in quanto $\overline{5}^5 = \overline{1}$.

Turno 2, Problema 2: Sia G un gruppo ciclico di ordine 30 con generatore g.

1. (Punti 3) Dire se le seguenti funzioni sono ben definite e sono omomorfismi di gruppi:

   $$f : G \to \mathbb{Z}_{20}, \quad h : G \to \mathbb{Z}_{20}$$

   definite da $f(g^k) = \overline{3k}$ e $h(g^k) = \overline{4k}$ per ogni $k \in \mathbb{Z}$

2. (Punti 4) Determinare nucleo e immagine di h.

3. (Punti 4) Determinare i generatori di un sottogruppo ciclico di G di ordine 10.

Soluzione:

1. La funzione f non è ben definita. Per esempio, $g^0 = g^3 0$ ma $\overline{0} \neq \overline{90}$ in $\mathbb{Z}_{20}$.

   La funzione h invece è ben definita perchè se $g^r = g^s$ deve risultare $30 \mid s - t$ da cui $20 \mid 4s - 4t$, cioè $\overline{s} = \overline{t} \in \mathbb{Z}_{20}$. Inoltre h è un omomorfismo in quanto

   $$h(g^{r+s}) = \overline{4(s+t)} = \overline{4s} + \overline{4t} = h(g^r) + h(g^s)$$

   qualunque siano r ed s.

2. Il nucleo di h è

   $$\ker(h) = \{g^r \in G \,|\, \overline{4r} = \overline{0} \in \mathbb{Z}_{20}\} = \{g^0, g^5, g^{10}, g^{15}, g^{20}.g^{25}\}.$$

   L'immagine di h è costituita dalle classi in $\mathbb{Z}_{20}$ della forma $\overline{4t}$, quindi

   $$\{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}\}.$$

3. Poiché $G = \langle g \rangle$ ha ordine 30 l'elemento $\gamma = g^3$ ha ordine 10. Dunque il sottogruppo $\langle \gamma \rangle$ ha ordine 10 ed i suoi generatori sono gli elementi della forma γ^k con $\mathrm{MCD}(k, 10) = 1$, cioè

   $$\gamma = g^3, \quad \gamma^3 = g^9, \quad \gamma^7 = g^{21}, \quad \gamma^9 = g^{27}.$$

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 22/23 Febbraio 2021

Problema 1: Sia $C = \langle g \rangle$ un gruppo ciclico con 48 elementi.

1. (Punti 4) Dimostrare che la funzione $f : C \to \mathbb{Z}_{60}$, $f(g^k) = \overline{5k}$, è un omomorfismo ben definito e decidere se è iniettivo e/o suriettivo.
2. (Punti 3) Sia $H < \mathbb{Z}_{60}$ l'immagine di f. Dire quanti generatori ha H.
3. (Punti 4) Calcolare il rappresentante tra 0 e 59 di $(f(g^7))^{18}$.

Soluzione:

1. Si ha che $g^k = g^\ell$ quando 48 divide $k-\ell$ ma allora 60 divide $5 \cdot 48 = 240$ che divide $5k-5\ell$ e quindi $\overline{5k} = \overline{5\ell}$ in $\mathbb{Z}_{60}$, cioè f è ben definita. Inoltre $f(g^r \cdot g^s) = f(g^{r+s}) = \overline{5(r+s)} = \overline{5r} + \overline{5s}$ e dunque f è un omomorfismo.

   Infine:

   - f non è iniettiva. Ad esempio perché $e_C \neq g^{10} \in \ker(f)$;
   - f non è suriettiva. Ad esempio perché C ha meno elementi di $\mathbb{Z}_{60}$.

2. Siccome C è generato da g, $H = \mathrm{Im}(f)$ è generato da $f(g) = \overline{5}$ che ha ordine 12. Dunque H è ciclico di ordine 12 e come tale possiede $\varphi(12) = 4$ generatori.

3. Si ha $(f(g^7))^{18} = \overline{35}^{18} = \overline{5}^{18} \cdot \overline{7}^{18} \in \mathbb{Z}_{60}$. Ora

   - $MCD(7, 60) = 1$ e siccome $\varphi(60) = 16$ otteniamo $\overline{7}^{18} = \overline{7}^2 = \overline{49}$;
   - dal calcolo diretto si vede subito che $\overline{5}^k = \overline{5}$ se k è dispari e $\overline{5}^k = \overline{25}$ se k è pari.

   Riassumendo: $(f(g^7))^{18} = \overline{5}^{18} \cdot \overline{7}^{18} = \overline{49} \cdot \overline{25} = \overline{25}$.

Problema 2: Adriana, Berto e Camilla giocano con un mazzo di 40 carte, 10 di ciascun seme.

1. (Punti 4) Scelte 12 carte coperte dal mazzo, quanti modi ci sono per distribuirle fra i tre giocatori?

2. (Punti 3) Adriana ha ricevuto 2 carte e sono entrambe di cuori. Quante sono le possibili mani di Adriana?

3. (Punti 4) Berto ha ricevuto 3 carte e Camilla 7. Quante possono essere complessivamente le loro mani se entrambi hanno ricevuto lo stesso numero di carte di cuori?

Soluzione:

1. Si tratta di suddividere 12 oggetti indistinguibili tra 3 persone, quindi la formula delle combinazioni con ripetizione fornisce subito $\binom{14}{2} = 14 \cdot 13/2 = 91$.

2. Le possibilità sono tante quante le scelte di 2 carte di cuori su 10 e quindi sono $\binom{10}{2} = 10 \cdot 9/2 = 45$.

3. (**Nota Bene:** risolviamo questo punto supponendolo **indipendente** dal punto precedente, cioè a prescindere dalle carte ottenute da Adriana. Ci sono altre interpretazioni possibili e valide che si trattano in maniera analoga)

   Il numero di carte di cuori assegnate a Berto e Camilla può essere $k = 0$, 1, 2 o 3.

   Per le k carte di cuori di Berto ci sono $\binom{10}{k}$ possibilità e quindi per le k carte di cuori di Camilla ci sono $\binom{10-k}{k}$ possibilità. Per completare le 3 carte di Berto serve una scelta di $3-k$ carte tra 30 (le "non-cuori"), quindi $\binom{30}{3-k}$, e per completare le 7 carte di Camilla serve una scelta di $7-k$ carte tra le $30-(3-k)$ rimanenti, ovvero $\binom{27+k}{7-k}$. Questo porta ad un totale parziale di

   $$t_k = \binom{10}{k}\binom{30}{3-k}\binom{10-k}{k}\binom{27+k}{7-k}$$

   mani tra Berto e Camilla con esattamente k carte di cuori ciascuna. Poiché queste situazioni sono in alternativa il totale generale si ottiene

sommando i totali parziali per tutti i valori possibili di k, ovvero

$$t_0 + t_1 + t_2 + t_3 = \binom{30}{3}\binom{27}{7} + \binom{10}{1}\binom{30}{2}\binom{9}{1}\binom{28}{6} + \binom{10}{2}\binom{30}{1}\binom{8}{2}\binom{29}{5} + \binom{10}{3}\binom{7}{3}\binom{30}{4}.$$

Corso di Studi in Informatica
Matematica Discreta
Prova scritta 22/23 Febbraio 2021

Problema 1: Si consideri il gruppo $\mathbb{Z}_{14} \times \mathbb{Z}_{21}$ con la consueta operazione di somma componente per componente e sia data la funzione

$$f : \mathbb{Z} \to \mathbb{Z}_{14} \times \mathbb{Z}_{21}$$

definita da $f(n) = ([2n]_{14}, [3n]_{21})$, per ogni $n \in \mathbb{Z}$.

1. (punti 4) Dimostrare che f è un omomorfismo di gruppi e determinarne il nucleo.
2. (punti 4) Determinare la cardinalità di $\mathrm{Im}(f)$ e le controimmagini di $([3]_{14}, [3]_{21})$.
3. (Punti 3) Calcolare il resto della divisione di $2^{141232} + 7^{6536779}$ per 30.

Soluzione

1. Si ha per ogni $n, m \in \mathbb{Z}$

$$\begin{aligned} f(n+m) &= ([2(n+m)]_{14}, [3(n+m)]_{21}) \\ &= ([2n+2m]_{14}, [3n+3m]_{21}) \\ &= ([2n]_{14}, [3n]_{21}) + ([2m]_{14}, [3m]_{21}) \end{aligned}$$

(dove l'ultimo segno di addizione è l'operazione di gruppo nel codominio)

$$= f(n) + f(m).$$

Quindi f è un omomorfismo. Inoltre

$$\begin{aligned} \ker(f) &= \{n \in \mathbb{Z} \mid ([2n]_{14}, [3n]_{21}) = ([0]_{14}, [0]_{21})\} \\ &= \{n \in \mathbb{Z} \mid 2n \equiv 0 \pmod{14} \text{ e } 3n \equiv 0 \pmod{21}\} \\ &= \{n \in \mathbb{Z} \mid n \equiv 0 \pmod{7}\} = [0]_7. \end{aligned}$$

2. Si ha

$$\begin{aligned} \mathrm{Im}(f) =& \{([2n]_{14}, [3n]_{21}) \mid n \in \mathbb{Z}\} \\ =& \{([0]_{14}, [0]_{21}), ([2]_{14}, [3]_{21}), ([4]_{14}, [6]_{21}), \\ & ([6]_{14}, [9]_{21}), ([8]_{14}, [12]_{21}), ([10]_{14}, [15]_{21}), ([12]_{14}, [18]_{21})\} \end{aligned}$$

da cui $|\mathrm{Im}(f)| = 7$.
Una controimmagine di $([3]_{14}, [3]_{21})$ sarebbe un intero $n \in \mathbb{Z}$ soddisfacente simultaneamente

$$\begin{cases} 2n \equiv 3 \pmod{14} \\ 3n \equiv 3 \pmod{21} \end{cases}$$

La seconda congruenza è soddisfatta per $n \equiv 1 \pmod 7$, ovvero $n = 1+7k$ con $k \in \mathbb{Z}$. Sostituendo nella prima congruenza troviamo $2n = 2+14k \equiv 3 \pmod{14}$ cioè $2 \equiv 3 \pmod{14}$, che è una contraddizione. Ne segue che l'insieme delle controimmagini cercate è vuoto.

Problema 2: Si considerino in S_9 le permutazioni

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 4 & 3 & 7 & 9 & 8 & 2 & 6 \end{pmatrix}, \quad \tau = (34)(69)$$

1. (Punti 4) Si scrivano come prodotto di cicli disgiunti σ, σ^{-1}, $(\sigma \circ \tau)^{-1}$.
2. (Punti 3) Esibire esplicitamente un sottogruppo di S_9 di ordine 10. Spiegare perchè non esiste in S_9 un sottogruppo di ordine 13.
3. (Punti 4) Verificare che la funzione

   $$f : \mathbb{Z}_{10} \to S_9, \quad \bar{t} \mapsto \sigma^t$$

   è ben definita. Scrivere esplicitamente quali elementi di $\mathbb{Z}_{10}$ appartengono a $\ker(f)$.

Soluzione

1. Si ha

   $$\begin{aligned} \sigma &= (1\ 5\ 7\ 8\ 2)(3\ 4)(6\ 9) \\ \sigma^{-1} &= (1\ 2\ 8\ 7\ 5)(3\ 4)(6\ 9) \\ (\sigma \circ \tau)^{-1} &= \tau^{-1} \circ \sigma^{-1} = (1\ 2\ 8\ 7\ 5). \end{aligned}$$

2. L'elemento $(1\ 2\ 3\ 4\ 5)(6\ 7)$ ha periodo 10, e quindi genera un sottogruppo di ordine 10.
   Poiché 13 è primo, un gruppo di ordine 13 è necessariamente ciclico. Quindi un sottogruppo di S_9 di ordine 13 dovrebbe essere generato da un elemento di periodo 13 e, sempre per la primalità di 13, tale elemento deve essere la composizione di cicli disgiunti di lunghezza 13. Ma S_9 non contiene cicli di lunghezza 13.

3. Dalla scrittura di σ come prodotto di cicli disgiunti vediamo che σ ha periodo 10. Se $t_1, t_2 \in \mathbb{Z}$ sono tali che $t_1 \equiv t_2 \pmod{10}$ allora $t_2 = t_1 + 10k$ per qualche $k \in \mathbb{Z}$, da cui

   $$\sigma^{t_2} = \sigma^{t_1+10k} = \sigma^{t_1} \circ (\sigma^{10})^k = \sigma^{t_1}.$$

   Questo prova la buona definizione. Inoltre

   $$f(\bar{t}_1 + \bar{t}_2) = \sigma^{t_1+t_2} = \sigma^{t_1} \circ \sigma^{t_2} = f(\bar{t}_1) + f(\bar{t}_2),$$

   da cui vediamo che σ è un omomorfismo. Si ha

   $$\ker(f) = \{\bar{t} \in \mathbb{Z}_{10} \mid \sigma^t = (1)\},$$

   e poiché σ ha periodo 10 si ha $\sigma^t = (1)$ se e solo se 10 divide t. Quindi $\ker(f) = \{\overline{0}\}$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 16 Giugno 2021

Problema 1: Il gioco degli scacchi si svolge tra due schieramenti (Bianco e Nero) formati da 8 "pezzi" (Re, Regina, 2 Torri, 2 Alfieri, 2 Cavalli) e 8 "pedoni" ciascuno su una scacchiera di 64 caselle colorate alternativamente bianche e nere.

1. (Punti 3) Quanti modi ci sono per piazzare in modo casuale i 16 pedoni totali su una scacchiera? (Ogni casella può essere occupata ma non può contenere più di un pedone)

2. (Punti 4) Quanti sono i modi per piazzare in modo casuale gli 8 pezzi bianchi sulla prima riga della scacchiera?

3. (Punti 4) Come nel punto precedente, ma con la richiesta che pezzi dello stesso tipo vengano piazzati su caselle di colore diverso.

Problema 2 Nel gruppo delle permutazioni S_7 si considerino le seguenti permutazioni

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

1. (Punti 3) Scrivere $\sigma, \tau, \sigma \circ \tau, \tau \circ \sigma, \sigma^{-1}$ come prodotto di cicli disgiunti.

2. (Punti 4) Calcolare il periodo di σ e scrivere σ^{999} come prodotto di cicli disgiunti;

3. (Punti 4) Determinare una permutazione $\mu \in S_7$ tale che $\mu \circ \sigma = \tau^2$.

SOLUZIONI:

Problema 1:

1. Poiché pedoni dello stesso colore sono indistinguibili, ci sono $\binom{64}{8}$ modi per sistemare 8 pedoni bianchi e $\binom{56}{8}$ modi per sistemare 8 pedoni neri nelle caselle libere rimanenti. Il totale dei modi per piazzare tutti i pedoni quindi è

$$\binom{64}{8} \cdot \binom{56}{8} = \frac{64!}{8! \cdot 56!} \cdot \frac{56!}{8! \cdot 48!} = \frac{64!}{(8!)^2 \cdot 48!} \simeq 6.2 \cdot 10^{18}.$$

2. Poiché una riga è formata da 8 caselle, piazzarci 8 pezzi in tutti i modi possibili è come considerare tutti gli anagrammi della "parola" AACCTTDR (D=Regina). Poichè tra le 8 lettere ve ne sono 3 ciascuna ripetuta due volte il totale è

$$\frac{8!}{2! \cdot 2! \cdot 2|} = 7! = 5040.$$

3. Iniziamo col disporre alfiere, cavallo e torre sulle 4 caselle bianche. Si tratta di disposizioni semplici di 3 oggetti su 4 posti e il totale delle possibilità è $D_{4,3} = 4!/1! = 4! = 24$. Stesso discorso (e stesso totale) per alfiere, cavallo e torre sulle caselle nere. Infine vi sono 2 possibilità per sistemare re e regina nelle 2 caselle rimanenti. Poiché le scelte sono indipendenti il numero totale delle configurazioni volute è

$$4! \cdot 4! \cdot 2 = 1152.$$

Problema 2:

1. Si ha

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

e di conseguenza $\sigma \circ \tau = (2\ 4\ 7)(3\ 5\ 6)$, $\tau \circ \sigma = (2\ 7\ 4)(3\ 5\ 6)$ e $\sigma^{-1} = (2\ 4)(3\ 6\ 5)$.

2. Dal punto precedente si ottiene che il periodo di σ è $\mathrm{mcm}(2,3) = 6$. Siccome $999 = 6 \cdot 166 + 3$ si ha

$$\sigma^{999} = \sigma^3 = (2\ 4)^3(3\ 5\ 6)^3 = (2\ 4).$$

3. Siccome $\tau^2 = \mathrm{id}$ basta prendere $\mu = \sigma^{-1}$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 13 luglio 2021

Problema 1:
Si consideri l'insieme $G = [0,1) = \{x \in \mathbb{R} | 0 \leq x < 1\} \subset \mathbb{R}$, e la seguente funzione $*$:

$$* : \mathbb{R} \times \mathbb{R} \to \mathbb{R},$$

$$\forall t_1, t_2 \in \mathbb{R}, \quad t_1 * t_2 = \begin{cases} t_1 + t_2, & \text{se } t_1 + t_2 < 1, \\ t_1 + t_2 - 1, & \text{se } t_1 + t_2 \geq 1. \end{cases}$$

1. (Punti 3) Verificare che $*$ ristretta a $G \times G$ è un'operazione su G
2. (Punti 4) Dando per verificato che $*$ come operazione su G è associativa, dimostrare che G con l'operazione $*$ é un gruppo abeliano.
3. (Punti 4) Calcolare il periodo di $\frac{2}{7} \in G$, cioè il più piccolo intero positivo n tale che
$$\underbrace{\frac{2}{7} * \cdots * \frac{2}{7}}_{n \text{ volte}} = 0.$$

1 RISOLUZIONE:

1. Bisogna verificare che $\forall g_1, g_2 \in G$, $g_1 * g_2 \in G$.

   Se $g_1 + g_2 < 1$, allora $g_1 * g_2 = g_1 + g_2 < 1$ quindi $g_1 * g_2 \in G$.

   Se invece $g_1 + g_2 \geq 1$, allora $g_1 * g_2 = g_1 + g_2 - 1$. Essendo g_1 e g_2 elementi di G, quindi numeri reali entrambi strettamente minori di 1, si ha che $g_1 + g_2 < 2$. Questo implica che $0 \leq g_1 + g_2 - 1 < 1$ e quindi $g_1 * g_2 \in G$.

2. Osserviamo innanzitutto che l'operazione $*$ è commutativa, perchè è definita mediante la somma su $\mathbb{R}$, che è commutativa.

   Nell'insieme G rispetto all'operazione $*$ esiste un elemento neutro, 0. Infatti $\forall g \in G$, $g * 0 = g + 0 = g$.

   Inoltre, $\forall g \in G$, si osservi che l'inverso di g rispetto ad $*$ è $1 - g$, che appartiene a G.

3. Calcolando esplicitamente otteniamo che

   $$\frac{2}{7} * \frac{2}{7} = \frac{4}{7}; \quad \frac{4}{7} * \frac{2}{7} = \frac{6}{7}; \quad \frac{6}{7} * \frac{2}{7} = \frac{1}{7}; \quad \frac{1}{7} * \frac{2}{7} = \frac{3}{7}; \quad \frac{3}{7} * \frac{2}{7} = \frac{5}{7}; \quad \frac{5}{7} * \frac{2}{7} = 0.$$

   Quindi, il periodo di $\frac{2}{7}$ è $n = 7$.

Problema 2:

1. (Punti 3) Trovare le soluzioni in $\mathbb{Z}$ della congruenza lineare

$$6x \equiv 14 \mod 40.$$

2. (Punti 4) Calcolare MCD$(208, 743)$ e determinare la corrispondente identità di Bezout.

3. (Punti 4) Calcolare il resto della divisione di $3^{5354} + 5^{4358}$ per 14.

1 RISOLUZIONE:

1. La congruenza lineare ha soluzioni poichè $MCD(6, 40) = 2$ divide 14. Le soluzioni della congruenza assegnata coincidono quindi con le soluzioni della congruenza $3x \equiv 7 \mod 20$.

   Per trovare le soluzioni di quest'ultima è sufficiente osservare che $3 \cdot 7 = 21 \equiv 1 \mod 20$. Quindi le soluzioni dell'equazione, sono le soluzioni di $x \equiv 9 \mod 20$.

   L'insieme delle soluzioni dell'equazione di partenza in $\mathbb{Z}$ è quindi

$$\{9 + 20 \cdot k | k \in \mathbb{Z}\}.$$

2. Per calcolare il massimo comun divisore richiesto, procediamo con l'algortimo euclideo:

$$\begin{aligned} 743 &= 3 \cdot 208 + 119; \\ 208 &= 1 \cdot 119 + 89; \\ 119 &= 1 \cdot 89 + 30; \\ 89 &= 2 \cdot 30 + 29; \\ 30 &= 1 \cdot 29 + 1; \\ 29 &= 29 \cdot 1 + 0. \end{aligned}$$

   Concludiamo quindi che $MCD(208, 743) = 1$. Ripercorrendo i passaggi sopra, otteniamo la seguente identità di Bézout:

$$-25 \cdot 208 + 7 \cdot 743 = 1.$$

3. Il resto richiesto è $0 \leq x < 14$ tale che $x \equiv 3^{5354} + 5^{4358} \mod 14$. Sia per la potenza con base 3, sia per la potenza con base 5, possiamo usare il teorema di Eulero-Fermat, poichè in entrambi i casi abbiamo due interi coprimi con 14:

$$3^{\varphi(14)} \equiv 1 \mod 14, \quad 5^{\varphi(14)} \equiv 1 \mod 14.$$

   Osserviamo che

$$\varphi(14) = 6, \quad 5354 = 892 \cdot 6 + 2, \quad 4358 = 726 \cdot 6 + 2.$$

   Allora otteniamo

$$3^{5354} + 5^{4358} = 3^{6^{892}} \cdot 3^2 + 5^{6^{726}} \cdot 5^2 \equiv 3^2 + 5^2 \mod 14.$$

   Concludiamo quindi che il resto della divisione di $3^{5354} + 5^{4358}$ per 14 è $6 (\equiv 3^2 + 5^2 \mod 14)$.

CORSO DI STUDI IN INFORMATICA
MATEMATICA DISCRETA
PROVA SCRITTA 7 SETTEMBRE 2021

Problema 1 Sia G il sottogruppo di S_6 definito da

$$G = \{(12)^i(3456)^j \mid 0 \leq i \leq 1, 0 \leq j \leq 3\}.$$

a) [3 punti] Si scrivano gli elementi di G come prodotti di cicli disgiunti e per ogni elemento di G si determini il periodo
b) [4 punti] Dire se G è un gruppo commutativo e se è ciclico.
c) [4 punti] Sia

$$H = \{\sigma \in G \mid \sigma(1) = 1\}.$$

Elencare gli elementi di H e dire se H è un sottogruppo ciclico di G.

Soluzione

a) Gli elementi di G sono
   - (1), periodo 1
   - (12), periodo 2
   - (3456), periodo 4
   - $(12)(3456)$, periodo 4
   - $(3456)^2 = (35)(46)$, periodo 2
   - $(12)(3456)^2 = (12)(35)(46)$, periodo 2
   - $(3456)^3 = (3654)$, periodo 4
   - $(12)(3456)^3 = (12)(3654)$, periodo 4

b) Utilizzando il fatto che cicli disgiunti commutano vediamo che

$$(12)^i(3456)^j(12)^a(3456)^b = (12)^{i+a}(3456)^{j+b} = (12)^a(3456)^b(12)^i(3456)^j$$

quindi G è commutativo. Non è ciclico, perché $|G| = 8$ e nessun elemento ha periodo 8.

c) $H = \{(1), (3456), (35)(46), (3645)\} = \langle 3456 \rangle$ è un sottogruppo ciclico di G.

Problema 2

a) (3 punti) In quanti modi diversi 8 persone possono sedersi in fila su una panchina?

b) (4 punti) In quanti modi diversi 8 persone possono sedersi in fila su una panchina se ci sono 4 uomini, 4 donne e gli uomini sono tutti seduti vicini?

c) (4 punti) In quanti modi diversi 8 persone possono sedersi su una panchina se due di esse (A e B) non vogliono stare vicine?

Soluzione

a) Sono $8! = 40320$, il numero di permutazioni di 8 elementi.

b) Si scelgono prima 4 posti adiacenti in cui collocare i 4 uomini: questo può essere fatto in 5 modi diversi. Una volta scelto l'insieme dei posti per gli uomini, ci sono $4!$ modi per sistemare gli uomini, e $4!$ modi per sistemare le donne nei posti rimanenti. Quindi il risultato è

$$5 \cdot 4! \cdot 4! = 2880.$$

c) Conviene contare l'insieme complementare, ovvero i modi diversi in cui le persone possono sedersi con A e B vicini. Come sopra queste sono

$$7 \cdot 2! \cdot 6! = 10080.$$

Quindi il risultato richiesto è

$$8! - 10080 = 30240.$$