Corso di Studi in Informatica
Matematica Discreta

Prova scritta 25/26 gennaio 2022

Prova in presenza

Alla prova in presenza sono state proposte 4 varianti dei problemi riportati sotto. Le varianti differivano l'una dall'altra per i soli dati numerici e si risolvevano tutte allo stesso modo. Si presenta qui testo e soluzione di una sola delle varianti.

Problema 1:
Consideriamo una classe di una scuola elementare di Torino, in cui ci sono 25 bambini.

1. (Punti 3) La scuola propone come attività pomeridiane facoltative un laboratorio di teatro al lunedí e un corso di minibasket al mercoledí. Nella classe 13 bambini partecipano al laboratorio di teatro, 15 al corso di minibasket, e 3 bambini non aderiscono a nessuna delle due iniziative. Quanti sono i bambini che partecipano sia al laboratorio di teatro, sia al corso di basket?

2. (Punti 4) Nella classe ci sono 10 bambini e 15 bambine. Il maestro per premiarli a fine quadrimestre per i loro buoni voti, decide di regalare a ognuno una penna. Per i maschi, compra 5 penne rosse e 5 nere, per le femmine compra 8 penne verdi e 7 blu. In quanti modi il maestro può distribuire le penne ai suoi scolari?

3. (Punti 4) I bambini della classe, all'uscita da scuola, si mettono in fila per due. Ovviamente un bambino rimane senza compagno di fila, e sta primo nella fila con il maestro. Se non conta quale bimbo sta a destra e quale a sinistra in ogni coppia della fila, in quanti modi diversi i bimbi possono sistemarsi in fila?

SOLUZIONE:

1. Poniamo A l'insieme dei bambini che partecipano al laboratorio di teatro, e B l'insieme dei bambini che partecipano al corso di minibasket. Il problema chiede d determinare $|A \cap B|$ fornendo come dati

$$|A \cup B| = 22, \quad |A| = 13, \quad |B| = 15$$

avendo già preso in considerazione il fatto che 3 bambini non partecipano ad alcuna attività. Usando il principio di inclusione-esclusione otteniamo:

$$|A \cap B| = |A| + |B| - |A \cup B| = 13 + 15 - 22 = 6.$$

2. Considerando le penne distinguibili solo per il colore, il maestro ha $\binom{10}{5}$ modi di distribuire le penne rosse tra i 10 maschi e $\binom{15}{8}$ modi di distribuire le penne verdi tra le femmine. Fatto ciò le altre penne saranno distribuite agli altri alunni univocamente. Dunque il totale delle possibili distribuzioni è

$$\binom{10}{5} \cdot \binom{15}{8} = \frac{10!}{5! \cdot 5!} \cdot \frac{15!}{8! \cdot 7!} = 13 \cdot 11 \cdot 7 \cdot 5 \cdot 3^4 \cdot 2^2.$$

3. Per comporre la fila scegliamo il primo alunno, quello che sta con il maestro, con 25 modi possibili. Per ogni fila successiva, in cui non importa chi sta a destra e chi a sinistra, dobbiamo scegliere due bambini fra quelli ancora non scelti e quindi per il metodo delle scelte il totale delle file possibili è

$$25 \cdot \binom{24}{2} \cdot \binom{22}{2} \cdot \dots \cdot \binom{2}{2} = \frac{25!}{2^{12}}.$$

Alternativamente si può considerare un ordinamento totale degli alunni (ci sono 25! ordinamenti) e scambiare a piacere gli alunni nei posti 2 e 3, 4 e 5, 6 e 7, eccetera senza cambiare la fila risultante. Ci sono 12 tali possibili scambi.

Problema 2:
Si risolvano i seguenti problemi:

1. (Punti 3) Per quali classi $\bar{a} \in \mathbb{Z}_{12}$ la congruenza $ax \equiv 3 \bmod 12$ ammette almeno una soluzione?

2. (Punti 4) Se $\bar{y}$ è inversa di $\bar{x}$ in $\mathbb{Z}_7$, qual'è l'inversa di $\overline{2x}$?

3. (Punti 4) Sia $n > 0$ un numero intero. Spiegare perchè $\mathrm{MCD(n, n+3)}$ può essere solo 1 o 3.

SOLUZIONE:

1. La congruenza proposta ammette almeno una soluzione se a è invertibile modulo 12 oppure, più generalmente, se $\mathrm{MCD}(a, 12)$ divide 3. Dunque si ha almeno una soluzione se
$$\bar{a} \in \{\bar{1}, \bar{3}, \bar{5}, \bar{6}, \bar{7}, \bar{9}, \overline{11}\} \subset \mathbb{Z}_{12}.$$

2. Osservato che in $\mathbb{Z}_7$ l'inversa di $\bar{2}$ è $\bar{4}$ in quanto $2 \cdot 4 = 8 \equiv 1 \bmod 7$ possiamo scrivere
$$\overline{2x}^{-1} = \bar{2}^{-1}\bar{x}^{-1} = \bar{4}\bar{y} = \overline{4y}.$$

3. In generale, se $d = \mathrm{MCD}(a, b)$ allora d divide $b-a$. Dunque posto $d = \mathrm{MCD(n, n+3)}$, deve aversi che d divide $(n+3) - n = 3$. Dunque $d = 1$ oppure 3.

   Alternativamente, la divisione euclidea di $n+3$ per n si scrive
$$n + 3 = 1 \cdot n + 3$$
   (a rigor di termini questo è vero per $n > 3$ ma i casi $n \in \{1, 2, 3\}$ possono essere controllati singolarmente molto facilmente). Ne segue che $\mathrm{MCD}(n+3, n) = \mathrm{MCD}(n, 3)$ e quest'ultimo può essere solo 1 o 3.

Prova a distanza

Problema 1:
Un chimico vuole preparare un profumo miscelando in parti uguali 12 essenze base a sua disposizione.

1. (Punti 4) Quante sono in totale le miscele possibili usando 2, 3 o 4 essenze?

2. (Punti 4) Una volta scelta la miscela questa viene commercializzata in scatolette contenenti 6 boccette ciascuna, ognuna delle quali può essere di 4 colori diversi. Quante sono le confezioni possibili se le 6 boccette sono prese a caso?

3. (Punti 3) Quante invece sono le confezioni possibili se ogni scatola contiene 3 coppie di boccette dello stesso colore?

RISOLUZIONE:

1. Scegliere 2, 3 o 4 essenze tra 12 da miscelare si può fare in $\binom{12}{2}$, $\binom{12}{3}$ e $\binom{12}{4}$ modi rispettivamente. Poichè le scelte di quante essenze miscelare sono mutualmente esclusive e poichè in ciascun caso si tratta di combinazioni semplici il totale delle possibilità è
$$\binom{12}{2} + \binom{12}{3} + \binom{12}{4} = 66 + 220 + 495 = 781.$$

2. In questo caso si tratta di combinazioni con ripetizione e quindi i modi di scegliere 6 boccette di 4 colori diversi sono
$$\binom{6+4-1}{4-1} = \binom{9}{3} = 84.$$

3. La composizione della scatola è determinata una volta scelti 3 colori fra 4 e questo si può fare in $\binom{4}{3} = 4$ modi diversi.

Problema 2: Si considerino le seguenti permutazioni di S_9:

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

1. (Punti 3) Si scriva la decomposizione di σ, τ e $\sigma \circ \tau^{-1}$ in cicli disgiunti

2. (Punti 4) Calcolare periodo e parità di σ^2, σ^5, τ^2.

3. (Punti 4) Si considerino i seguenti sottoinsiemi di S_9, considerato come gruppo con l'operazione di composizione:
$$H_1 = \{\sigma^t | t \in \mathbb{Z}\}, \quad H_2 = \{\sigma^t | t \in \mathbb{Z}, \sigma^t(1) = 1\}.$$
Stabilire se H_1 e H_2 sono sottogruppi di S_9, motivando adeguatamente la risposta.

SOLUZIONE:

1. Il calcolo diretto fornisce
$$\sigma = (1\ 5)(2\ 8\ 9\ 6\ 4) \qquad e \qquad \tau = (3\ 5)(4\ 6).$$
Osservato che $\tau^{-1} = \tau$, si ha $\sigma \circ \tau^{-1} = \sigma \circ \tau = (1\ 3\ 5)(2\ 8\ 9\ 4)$.

2. Dalla struttura in cicli disgiunti calcolata al punto precedente, otteniamo:
   - $\sigma^2 = (1\ 5)^2(2\ 8\ 9\ 6\ 4)^2 = (2\ 9\ 4\ 8\ 6)$, quindi di periodo 5 e pari;
   - $\sigma^5 = (1\ 5)^5(2\ 8\ 9\ 6\ 4)^5 = (1\ 5)$, quindi di periodo 2 e dispari;
   - $\tau^2 = \mathrm{id}$, quindi di periodo 1 e pari.

3. Per definizione H_1 è l'insieme delle potenze di σ e quindi è il sottogruppo ciclico $\langle\sigma\rangle$ generato da σ in S_9.

   Per quanto riguarda H_2 basta osservare che $\mathrm{id} \in H_2$ e che se σ^r e σ^s sono potenze di σ tali che $\sigma^r(1) = \sigma^s(1) = 1$ allora anche $\sigma^{r+s}(1) = 1$ e $\sigma^{-r}(1) = 1$.

   Alternativamente si può notare dalla decomposizione in cicli disgiunti di σ che $\sigma^t(1) = 1$ esattamente quando t è pari. Ma allora, analogamente a quanto sopra,

$$H_2 = \{\sigma^t \mid t \in 2\mathbb{Z}\} = \{\sigma^{2s} = (\sigma^2)^s \mid s \in \mathbb{Z}\} = \langle\sigma^2\rangle.$$

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 25/26 gennaio 2022

Prova in presenza

Problema 1: Si consideri la permutazione

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

1. (Punti 3) Calcolare il periodo e determinare la parità di π.

2. (Punti 4) Dire quante sono le permutazioni di $\mathcal{S}_9$ dello stesso tipo di π.

3. (Punti 4) Verificare che la funzione

$$f\colon \mathbb{Z}_8 \longrightarrow \mathcal{S}_9, \qquad f(\bar{k}) \mapsto \pi^{5k}$$

è ben definita ed è un omomorfismo. Determinarne poi il nucleo.

SOLUZIONE:

1. Il calcolo della scrittura in cicli disgiunti fornisce $\pi = (1\ 8\ 2\ 9)(3\ 7\ 4\ 5\ 6)$ e quindi π ha tipo $(5, 4)$. Ne segue che π ha periodo $\mathrm{mcm}(5, 4) = 20$ ed è dispari.

2. Poiché un ciclo di lunghezza ℓ ammette ℓ scritture differenti i cicli di lunghezza $\ell \geq 2$ costruibili con n elementi a disposizione sono $\frac{1}{\ell}\frac{n!}{(n-\ell)!}$. Poiché i due cicli di lunghezza 5 e 4 rispettivamente devono essere disgiunti il loro numero è

$$\frac{1}{5}\cdot\frac{9!}{4!}\cdot\frac{1}{4}\cdot\frac{4!}{0!} = \frac{1}{20}9!.$$

3. Se $m \equiv n \bmod 8$ allora $5m \equiv 5n \bmod 40$ e quindi f è ben definita perché 40 è un multiplo del periodo di π.

   La funzione f é un omomorfismo perché per ogni m ed n si ha $f(\bar{m}+\bar{n}) = \pi^{5(m+n)} = f(\bar{m}) \circ f(\bar{n})$.

   Infine il nucleo di f è costituito da quelle classi $\bar{k}$ modulo 8 tale che $5\bar{k}$ è multiplo del periodo di π. Dunque

$$\ker(f) = \{\bar{0}, \bar{4}\} \subset \mathbb{Z}_8.$$

Problema 2:
In questo problema consideriamo classi resto in $\mathbb{Z}_{20}$.

1. (Punti 3) Quanti modi si hanno di scegliere 3 classi invertibili?

2. (Punti 4) Dire se il gruppo moltiplicativo $\mathbb{Z}_{20}^{\times}$ è ciclico o no.

3. (Punti 4) Determinare tutti gli $n \in \mathbb{Z}$ tale che $\bar{3}^n = \bar{9}$.

SOLUZIONE:

1. Le classi invertibili sono $|\mathbb{Z}_{20}^{\times}| = \varphi(20) = 8$. Sceglierne 3 può essere fatto in $\binom{8}{3} = 56$ modi

2. Gli 8 elementi di $\mathbb{Z}_{20}^{\times}$ sono $\{\pm\bar{1}, \pm\bar{3}, \pm\bar{7}, \pm\bar{9}\}$. Il calcolo diretto mostra che

$$(\pm\bar{1})^2 = (\pm\bar{3})^4 = (\pm\bar{7})^4 = (\pm\bar{9})^2 = \bar{1}.$$

   Pertanto il gruppo non è ciclico in quanto ogni elemento ha periodo al più 4.

3. Dal punto precedente si vede che il periodo moltiplicativo di $\bar{3}$ è esattamente 4. Siccome $\bar{3}^2 = \bar{9}$ concludiamo subito che

$$\{n \in \mathbb{Z} \,|\, \bar{3}^n = \bar{9}\} = \{n \in \mathbb{Z} \,|\, n \equiv 2 \bmod 4\} = \{\cdots, -6, -2, 2, 6, 10, \cdots\}.$$

Prova a distanza

Problema 1:

Alle elezioni a Freedonia partecipano 3 liste, A, B e C, ciascuna con 10 candidati e vi sono 2556 cittadini con diritto di voto.

1. (Punti 4) Ogni votante deve scegliere esattamente 2 liste, altrimenti il voto è nullo. In 910 hanno votato per A e B, in 795 per A e C, e B ha ricevuto 1658 voti validi. Quanti sono i voti nulli? Quale lista ha ottenuto più voti?

2. (Punti 3) Viene formato un comitato scegliendo a caso 4, 3 e 2 candidati dalle liste secondo l'ordine del risultato elettorale. Quanti sono i possibili comitati?

3. (Punti 4) Al voto è associato un referendum per la scelta della bandiera. La bandiera deve contenere il rosso, il nero e il blu e può avere tre strisce verticali oppure quattro strisce orizzontali senza colori uguali adiacenti. Quante sono le bandiere possibili?

SOLUZIONE:

1. I votanti che non hanno scelto la lista B hanno scelto necessariamente le liste A e C, quindi il numero totale di voti validi è $1658 + 795 = 2453$. Di conseguenza $2556 - 2453 = 103$ cittadini non hanno votato o hanno consegnato scheda bianca o nulla.
   I voti attribuiti alla lista A si ottengono facilmente sommando $910 + 795 = 1705$. I restanti voti validi sono quindi $2453 - 1705 = 748$ e sono da attribuire alle liste B e C. Di conseguenza la lista C ha ottenuto $795 + 748 = 1543$ voti. Pertanto la lista più votata è la A con 1705 voti.

2. Per costituire il Consiglio, si devono fare tre scelte successive di combinazioni di 4, 3 e 2 candidati rispettivamente, scelti ogni volta da un insieme di 10 elementi. Pertanto i risultati possibili sono

$$\binom{10}{4} \cdot \binom{10}{3} \cdot \binom{10}{2}$$

3. Le bandiere con tre strisce verticali si ottengono con tutte le permutazioni possibili dei tre colori, quindi sono $3! = 6$.
   Quelle con quattro strisce orizzontali si possono ottenere in diversi modi. Fissato il colore che si ripete, basta scegliere in quale posizione collocare gli altri due: questo si può fare in $4 \cdot 3 = 12$ modi, ma 6 tra questi non sono accettabili perché lascerebbero libere due strisce adiacenti. Pertanto ci sono 6 scelte possibili. Ripetendo il ragionamento cambiando la scelta del colore che si ripete, otteniamo 18 bandiere a strisce orizzontali.
   Trattandosi di opzioni disgiunte tra loro, il numero di bandiere con strisce verticali va sommato al numero di bandiere con strisce orizzontali. In conclusione, i cittadini dovranno scegliere tra 24 modelli di bandiera.

Problema 2:
Rispondere ai punti seguenti

1. (Punti 3) Calcolare il resto della divisione di 5^{2139} per 84.

2. (Punti 4) Dimostrare che per ogni intero $n \geq 1$ si ha $\mathrm{MCD}(n, n^2 + 1) = 1$.

3. (Punti 4) Dire per quali $b \in \mathbb{Z}$ la congruenza

$$165 \cdot x \equiv 22 \cdot b \bmod 336$$

ammette almeno una soluzione.

SOLUZIONE:

1. Verifichiamo che valgono le ipotesi del teorema di Eulero: $MCD(5, 84) = 1$. Possiamo quindi applicare il teorema di Eulero, ottenendo $5^{\phi(84)} \equiv 1 \mod 84$. Poichè $\phi(84) = \phi(2^2) \cdot \phi(3) \cdot \phi(7) = 24$, calcoliamo la divisione di 2139 rispetto a 24, ottenendo $2139 = 89 \cdot 24 + 3$. Quindi il resto della divisione di 5^{2139} per 84 è 41, come si vede dal calcolo seguente:

$$5^{2139} = (5^{24})^{89} \cdot 5^3 \equiv 5^3 \mod 84 \equiv 41 \mod 84.$$

2. Se $n = 1$, $MCD(1, 2) = 1$. Per ogni $n \geq 2$, è sufficiente usare l'algoritmo di Euclide. Come primo passo, si calcla la divisione con resto di $n^2 + 1$ rispetto a n:

$$n^2 + 1 = q \cdot n + r, \text{ con } r < n.$$

Otteniamo quoziente $q = n$ e resto $r = 1$. All'iterazione successiva, otteniamo resto 0, quindi $MCD(n^2 + 1, n) = 1$.

3. La congruenza ammette almeno una soluzione se e solo se $MCD(165, 336)$ divide $22 \cdot b$. Calcolando esplicitamente, otteniamo $MCD(165, 336) = 3$: allora la congruenza ammette almeno una soluzione se e solo se 3 divide $22 \cdot b$, ovvero se e solo se 3 divide b.
Quindi la congruenza ammette almeno una soluzione per $b = 3n$, con $n \in \mathbb{Z}$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 14 giugno 2022

Problema 1:
Si considerino le seguenti permutazioni in $\mathcal{S}_8$:

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

1. (Punti 3) Calcolare $\pi \circ \sigma$ e $\sigma \circ \pi$.
2. (Punti 4) Si consideri il sottogruppo ciclico $H = \langle \pi \rangle$ di $\mathcal{S}_8$. Stabilire se σ appartiene a H.
3. (Punti 4) Si esibisca esplicitamente un sottogruppo di $\mathcal{S}_8$ di ordine 12 oppure si spieghi perché un tale sottogruppo di $\mathcal{S}_8$ non esiste.

Soluzione:

1. Le scritture in cicli disgiunti sono $\pi = (2\ 5\ 7)(3\ 6\ 8\ 4)$ e $\sigma = (2\ 7\ 5)(3\ 8)(6\ 4)$ da cui risulta chiaro che $\sigma = \pi^2$. Per cui
$$\pi \circ \sigma = \sigma \circ \pi = \pi^3 = (4\ 8\ 6\ 3).$$
2. Per quanto detto nel punto precedente σ certamente è un elemento di H in quanto qust'ultimo è costituito, per definizione, dalle permutazioni che sono potenze di π.
3. Dalla decomposizione in cicli disgiunti scritta nel punto 1 si vede che l'ordine di π è $\mathrm{mcm}(3, 4) = 12$. Pertanto un esempio di sottogruppo con 12 elementi è proprio H,

Problema 2: Una scuola di ballo deve organizzare il saggio di fine anno, che coinvolgerà in totale 32 partecipanti.

1. (Punti 3) Lo spettacolo prevede 2 protagonisti principali. In quanti modi si possono scegliere i 2 protagonisti tra i 32 partecipanti?

2. (Punti 4) I costumi dei partecipanti al saggio (protagonisti esclusi!) prevedono che 12 ballerini/e indossino una calzamaglia bianca, 20 un cappello e 14 una maglietta blu. Ci sono 6 ballerini che indossano sia la calzamaglia bianca sia il cappello, 6 che indossano sia il cappello sia la maglietta blu e 6 che indossano sia la calzamaglia bianca sia la maglietta blu. Quanti ballerini/e indosseranno cappello e maglietta blu, ma non una calzamaglia bianca?

3. (Punti 4) Una volta scelti i 2 protagonisti principali, gli altri partecipanti al saggio devono formare due file da 15 persone ciascuna. In quanti modi diversi possono essere formate le due file?

Soluzione:

1. Scegliere 2 persone tra 32 si può fare in $\binom{32}{2} = \frac{32 \cdot 31}{2} = 496$ modi.

2. Denotati A, B e C gli insiemi delle persone che indossano la calzamaglia, il cappello e la maglietta rispettivamente applichiamo il principio di inclusione-esclusione. Allora

$$30 = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| = \\ 12 + 20 + 14 - 6 - 6 - 6 + |A \cap B \cap C|,$$

   da cui $|A \cap B \cap C| = 2$.

   Il numero di persone cercato è $|B \cap C| - |A \cap B \cap C| = 6 - 2 = 4$.

3. Per formare 2 righe di 15 basta formare una riga di 30 e spezzarla a metà. Ciò si può fare in 30! modi.

   Si può argomentare che le due file di 15 possano essere scambiate liberamente. Secondo tale interpretazione il numero di possibilità è $\frac{1}{2}30!$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 11luglio 2022

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

MATRICOLA .... **Versione A**

Rispondere a ciascuna domanda, motivando adeguatamente le risposte.

Problema 1:
In questo problema consideriamo il gruppo $\mathcal{S}_7$ delle permutazioni su 7 elementi.

1. (Punti 3) Calcolare periodo e parità della permutazione

$$\pi = (5\ 6\ 3\ 1\ 2)(7\ 4)(1\ 7\ 3)(2\ 5\ 4) \in \mathcal{S}_7.$$

2. (Punti 4) Sia $f : \mathbb{Z}_5 \to \mathcal{S}_7$ un omomorfismo iniettivo. Dire quali delle seguenti permutazioni sicuramente **non** sono nell'immagine di f:

$$\sigma_1 = (1\ 6)(2\ 7\ 3), \qquad \sigma_2 = (2\ 5\ 4\ 6)$$
$$\sigma_3 = (2\ 4\ 1\ 7\ 6), \qquad \sigma_4 = (2\ 5)(1\ 6)(3\ 4).$$

3. (Punti 4) Esiste in $\mathcal{S}_7$ un sottogruppo con 10 elementi?

Soluzione:

1. La scrittura in cicli disgiunti è

$$\pi = (1\ 4\ 5\ 7)(2\ 6\ 3)$$

per cui il periodo è $\mathrm{mcm}(4, 3) = 12$ e π è dispari.

2. Poiché $\bar{5} = \bar{0}$ in $\mathbb{Z}_5$ una permutazione σ nell'immagine di f deve essere tale che $\sigma^5 = \mathrm{id}$. Delle permutazioni assegnate σ_1, σ_2 e σ_4 non hanno questa proprietà avendo periodo 6, 4 e 2 rispettivamente.

3. Per ottenere un sottogruppo con 10 elementi basta considerare il sottogruppo ciclico generato da una permutazione di tipo $(5, 2)$ che ha, per l'appunto, periodo $\mathrm{mcm}(5, 2) = 10$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 11 luglio 2022

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

MATRICOLA ....

Versione A

Rispondere a ciascuna domanda, motivando adeguatamente le risposte.

Problema 2:

1. (punti 4) Dire se esiste l'inverso moltiplicativo di 35 modulo 143 ed in caso affermativo calcolarlo.
2. (punti 4) Calcolare il resto della divisione di $7^{1362} - 11^{449}$ per 60.
3. (Punti 3) Determinare tutte le soluzioni della congruenza

$$15X + 9 \equiv 0 \bmod 36.$$

Soluzione:

1. Applichiamo l'algoritmo di divisione euclidea:

$$\begin{aligned} 143 &= 4 \cdot 35 + 3 \\ 35 &= 11 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

Dunque $\mathrm{MCD}(143, 35) = 1$ e quindi 35 è invertibile modulo 143. Per calcolarne l'inverso procediamo a ritroso per determinare l'identità di Bezout:

$$\begin{aligned} 1 &= 3 - 2 = 3 - (35 - 11 \cdot 3) \\ &= -35 + 12 \cdot 3 = -35 + 12(143 - 35 \cdot 4) \\ &= -49 \cdot 35 + 12 \cdot 143. \end{aligned}$$

Dunque l'inverso di 35 modulo 143 è $-49 \equiv 94$.

2. Si ha $\varphi(60) = \varphi(4) \cdot \varphi(3) \cdot \varphi(5) = 2 \cdot 2 \cdot 4 = 16$. Poiché $\mathrm{MCD}(7, 60) = \mathrm{MCD}(11, 60) = 1$ usando il teorema di Eulero otteniamo

$$\begin{cases} 7^{1362} \equiv (7^{16})^{85} \cdot 7^2 \equiv 49 \bmod 60 \\ 11^{449} \equiv (11^{16})^{28} \cdot 11 \equiv 11 \bmod 60. \end{cases}$$

In definitiva $7^{1362} - 11^{449} \equiv 49 - 11 = 38 \bmod 60$.

3. Dividendo per 3 ci si riconduce a $5X + 3 \equiv 0 \bmod 12$. Poiché l'inverso di 5 modulo 12 è 5 stesso la soluzione modulo 12 è $X = 5 \cdot (-3) \equiv 9 \bmod 12$. Dunque le soluzioni modulo 36 sono $\{9, 21, 33\}$.

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 12 Settembre 2022

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

MATRICOLA .... **Versione A**

Rispondere a ciascuna domanda, motivando adeguatamente le risposte.

Problema 1:
Ricordato che un numero in base 8 si scrive utilizzando le cifre $\{0, 1, 2, 3, 4, 5, 6, 7\}$ rispondere alle domande seguenti.

1. (Punti 3) Quanti sono in base 8 i numeri di tre cifre (quindi da 100 a 777 inclusi) che non includono la cifra 4?
2. (Punti 4) Quanti sono in base 8 i numeri di tre cifre (quindi da 100 a 777 inclusi) che includono la cifra 6 esattamente una volta?
3. (Punti 4) Quanti sono in base 8 i numeri di tre cifre (quindi da 100 a 777 inclusi) formati da tre cifre consecutive anche non ordinatamente? (ad esempio: 201, 453, eccetera)

Soluzione:

1. Un numero in base 8, di tre cifre, che non includa la cifra 4, si ottiene scegliendo una cifra da 1 a 7 diversa da 4 (quindi 6 opzioni possibili) e due cifre da 0 a 7 diverse da 4 (quindi 7 opzioni possibili per ciascuna scelta). Per il principio delle scelte successive, il numero di combinazioni possibili si ottiene moltiplicando:
$$6 \cdot 7 \cdot 7 = 294.$$
2. Un numero in base 8, di tre cifre, che includa la cifra 6 esattamente una volta, si può ottenere in tre modi:
   - Scegliendo come prima cifra il 6, seguito da due cifre diverse da 6. In questo caso le combinazioni possibili sono
   $$7 \cdot 7 = 49.$$
   - Scegliendo come seconda cifra il 6 e come prima e terza due cifre diverse da 6. In questo caso le combinazioni possibili sono
   $$6 \cdot 7 = 42$$
   poiché la prima cifra deve anche essere diversa da 0.
   - Scegliendo come terza cifra il 6. Come nel caso precedente abbiamo 42 opzioni possibili.

I tre casi sono disgiunti tra loro, quindi il totale delle combinazioni possibili si ottiene sommando:
$$49 + 42 + 42 = 133.$$

3. Per rispondere alla terza domanda occorre innanzitutto scegliere una terna di cifre consecutive tra 0 e 7. Le terne possibili sono 6:
$$012, \quad 123, \quad 234, \quad 345, \quad 456, \quad 567.$$
Con ciascuna terna possiamo costruire $P_3 = 3! = 6$ numeri di tre cifre, corrispondenti a tutte le permutazioni della terna.
Dobbiamo però escludere dal computo le permutazioni che iniziano per 0, ovvero 012 e 021. In totale si avranno quindi $6 \cdot 6 - 2 = 34$ combinazioni possibili.

Problema 2: Si consideri la permutazione in $\mathcal{S}_8$ data da
$$\sigma = (5\ 2\ 3\ 8\ 7\ 1\ 6)(2\ 5)(1\ 4\ 8).$$

1. (punti 4) Calcolare periodo e parità di σ.
2. (punti 3) Trovare una permutazione $\tau \in \mathcal{S}_8$ tale che
$$\sigma \circ \tau = (2\ 5\ 8).$$
3. (Punti 4) Denotato $G = \langle\sigma\rangle$ il sottogruppo di $\mathcal{S}_8$ generato da σ si verifichi che la funzione
$$f : G \longrightarrow \mathbb{Z}_8, \qquad f(\sigma^k) = \overline{2k}$$
è un omomorfismo e dire se è iniettivo o suriettivo.

Soluzione:

1. Innanzitutto scriviamo σ come prodotto di cicli disgiunti:
$$\sigma = (1\ 4\ 7)(3\ 8\ 6\ 5).$$
Pertanto σ è una permutazione di tipo $(3, 4)$, da cui deduciamo che $\text{per}(\sigma) = \text{mcm}(3, 4) = 12$. Infine σ è una permutazione dispari in quanto composta di un ciclo pari (di lunghezza 3) con un ciclo dispari (di lunghezza 4).

2. Dalla relazione
$$\sigma \circ \tau = (2\ 5\ 8),$$
ricordando che qualunque permutazione è invertibile e componendo a sinistra con σ^{-1}, si ricava facilmente che
$$\tau = \sigma^{-1} \circ (2\ 5\ 8).$$
L'inversa σ^{-1} si può ottenere invertendo l'ordine dei termini nei cicli che compongono σ, ovvero $\sigma^{-1} = (1\ 7\ 4)(3\ 5\ 6\ 8)$ (non è necessario invertire l'ordine dei cicli, essendo essi disgiunti, quindi permutabili tra loro). Pertanto
$$\tau = (1\ 7\ 4)(3\ 5\ 6\ 8)(2\ 5\ 8) = (1\ 7\ 4)(2\ 6\ 8)(3\ 5).$$

3. Per verificare che f è un omomorfismo di gruppi, occorre verificare che per ogni coppia di valori h e k in $\mathbb{Z}$ vale l'uguaglianza

$$f(\sigma^h \circ \sigma^k) = f(\sigma^h) + f(\sigma^k).$$

È sufficiente sviluppare ciascun membro dell'uguaglianza:

$$\begin{aligned} f(\sigma^h \circ \sigma^k) &= f(\sigma^{h+k}) = \overline{h+k} \\ f(\sigma^h) + f(\sigma^k) &= \overline{h} + \overline{k} = \overline{h+k}. \end{aligned}$$

Essendo f un omomorfismo di gruppi, per stabilire se è iniettivo è sufficiente valutarne il nucleo. Ora

$$\sigma^k \in \mathrm{Ker}(f) \quad \Longleftrightarrow \quad f(\sigma^k) = \overline{0} \quad \Longleftrightarrow \quad \overline{2k} = \overline{0} \text{ in } \mathbb{Z}_8,$$

cioè σ^k sta nel nucleo di f se e solo se $2k$ è multiplo di 8, ovvero k è multiplo di 4. Poiché σ ha periodo 12, G è formato da 12 potenze distinte di σ, di cui tre con esponente multiplo di 4: $\sigma^0 = id$, σ^4 e σ^8. Pertanto $\mathrm{Ker}(f) = \{id, \sigma^4, \sigma^8\}$ non è banale e l'omomorfismo non è iniettivo.
f non è nemmeno suriettivo perché, per esempio, la classe $\overline{1}$ non ha controimmagini. Infatti, se esistesse k in $\mathbb{Z}$ tale che $f(\sigma^k) = \overline{1}$, avremmo che $\overline{2k} = \overline{1}$ in $\mathbb{Z}_8$. Ciò è assurdo poiché la classe $\overline{2}$ non è invertibile in $\mathbb{Z}_8$, essendo $\mathrm{MCD}(2,8) = 2$.