CdS Informatica – Torino
Corso di Matematica Discreta

Esercizi dal Libro di Testo–Soluzioni
Capitolo 1

Esercizio 1. *Sia $A = \{a, b, c\}$. Dire quali delle seguenti affermazioni sono vere e quali false:*

$$b \in A, \quad \emptyset \subset A, \quad \{\emptyset\} \subset A, \quad \{c, d\} \not\subset A, \quad \{a, \{c\}\} \subset A.$$

Soluzione: vera, vera, falsa, vera, falsa.

Esercizio 2. *Sia $A = \{x \in \mathbb{R} \,|\, x^2 > 25\} \cap \{x \in \mathbb{R} \,|\, 2x \in \mathbb{Z}\}$. Dire quali delle seguenti affermazioni sono vere e quali false:*

$$5 \in A, \quad -\frac{11}{2} \in A, \quad \frac{100}{3} \in A, \quad \mathbb{N} \subset A, \quad \left\{\frac{7}{2}, 6\right\} \subset A.$$

Soluzione: falsa, vera, falsa, falsa, falsa.

Esercizio 3. *Sia $A = \{a, e, i, o, u\}$. Dire quali delle seguenti affermazioni sono vere e quali false:*

$$\emptyset \in P(A), \quad a \in P(A), \quad \{i, u\} \subset P(A), \quad \{e, o\} \in P(A), \quad \{\{e\}, \{o\}\} \subset P(A).$$

Soluzione: vera, falsa, falsa, vera, vera.

Esercizio 4. *Siano $P(x)$ e $Q(x)$ due espressioni contenenti numeri reali ed un'incognita x e siano A e B l'insieme delle soluzioni dell'equazione $P(x) = 0$ e l'insieme delle soluzioni dell'equazione $Q(x) = 0$ rispettivamente.*

1. *L'equazione $P(x)Q(x) = 0$ ha come insieme di soluzioni $A \cap B$ o $A \cup B$?*
2. *Il sistema $\begin{cases} P(x) = 0 \\ Q(x) = 0 \end{cases}$ ha come insieme di soluzioni $A \cap B$ o $A \cup B$?*

Soluzione:

1. Fra numeri reali si ha $P(x)Q(x) = 0$ solo se $P(x) = 0$ oppure $Q(x) = 0$. Quindi $A \cup B$.
2. La soluzione di un sistema è soluzione di entrambe le equazioni, quindi $A \cap B$.

Esercizio 5. *Dimostrare che $A \cap B = \emptyset$ se e soltanto se $P(A) \cap P(B) = \{\emptyset\}$.*

Soluzione: Se $A \cap B = \emptyset$ un sottoinsieme proprio di $X \subset A$ non può essere un sottoinsieme di B, altrimenti si avrebbe $X \subset A \cap B$ contraddicendo l'ipotesi. Dunque $\emptyset$ è l'unico sottoinsieme comune ad A e B e questo vuol dire che $P(A) \cap P(B) = \{\emptyset\}$.

Viceversa supponiamo $P(A) \cap P(B) = \{\emptyset\}$. Se esistesse un elemento $x \in A \cap B$, l'insieme $\{x\}$ sarebbe un sottoinsieme sia di A che di B e quindi un elemento di $P(A) \cap P(B)$, ma ciò è impossibile per ipotesi.

Esercizio 6. *Dire se le seguenti affermazioni sono vere o false:*

$$P(A \cap B) = P(A) \cap P(B), \qquad P(A \cup B) = P(A) \cup P(B).$$

Soluzione: La prima affermazione è vera. Infatti se $X \in P(A \cap B$, cioè $X \subset A \cap B$, allora $X \subset A$ e $X \subset B$. Quindi $X \in P(A) \cap P(B)$. Viceversa, se $X \in P(A) \cap P(B)$ allora X è sia un sottoinsieme di A che di B, ovvero $X \subset A \cap B$.

La seconda affermazione falsa. Ad esempio consideriamo la situazione seguente: $A = \{a, b\}$, $B = \{b, c\}$. L'insieme $X = \{a, c\}$ è sicuramente un sottoinsieme di $A \cup B = \{a, b, c\}$ e quindi $X \in P(A \cup B)$, ma X non è un sottoinsieme di A, ne' di B e quindi $X \notin P(A) \cup P(B)$.

Esercizio 7. *Dimostrare l'uguaglianza* $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Soluzione: Sia $x \in (A \cap B) \cup C$. Per definizione $x \in A \cap B$ oppure $x \in C$. Se $x \in A \cap B$, allora x è sia in A che in B. Ma allora x è sia in $A \cup C$, sia in $B \cup C$ e quindi in $(A \cup C) \cap (B \cup C)$.

Viceversa se $x \in (A \cup C) \cap (B \cup C)$ allora, per definizione, x è in $A \cup C$ e in $B \cup C$. Se $x \in C$ allora certamente $x \in (A \cap B) \cup C$. Altrimenti x deve essere in A e in B, quindi in $A \cap B$ e certamente in $(A \cap B) \cup C$.

Esercizio 8. *Enunciare e dimostrare proprietà distributive analoghe a quelle dell'esercizio precedente per intersezioni ed unioni di famiglie arbitrarie di insiemi*

Soluzione: Le propriet distributive per una famiglia arbitraia $\{A_i\}_{i \in I}$ di insiemi hanno la forma

$$\left(\bigcap_{i \in I} A_i \right) \cup C = \bigcap_{i \in I} (A_i \cup C), \qquad \left(\bigcup_{i \in I} A_i \right) \cap C = \bigcup_{i \in I} (A_i \cap C).$$

Si dimostrano esattamente come nel caso dell'intersezione o unione di due insiemi (vedi libro di testo e la soluzione dell'esercizio precedente).

Esercizio 9. *Dimostrare la seconda la legge di De Morgan:* $\mathcal{C}_X(A \cup B) = \mathcal{C}_X(A) \cap \mathcal{C}_X(B)$

Soluzione: Sia $x \in \mathcal{C}_X(A \cup B)$: Allora, per definizione, $x \in X$ ma $x \notin A \cup B$. Questo significa che x non è in A, ne' in B. Quindi x è in $\mathcal{C}_X(A)$ e in $\mathcal{C}_X(B)$ e quindi in $\mathcal{C}_X(A) \cap \mathcal{C}_X(B)$.

Viceversa, se $x \in \mathcal{C}_X(A) \cap \mathcal{C}_X(B)$ allora x è un elemento di X che non è ne' in A ne' in B e quindi non è in $A \cup B$. Ma questo vuol dire che $x \in \mathcal{C}_X(A \cup B)$.

Esercizio 10. *Dimostrare le Leggi di de Morgan generalizzate a intersezione ed unione di una famiglia arbitraria di sottoinsiemi.*

Soluzione: La dimostrazione è di fatto identica a quella del caso di due insiemi.

Esercizio 11. *Dimostrare che vale una versione delle Leggi di de Morgan per l'insieme differenza. Precisamente, dati insiemi X, A e B dimostrare che*

$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B) \quad e \quad X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B).$$

Soluzione: La dimostrazione è di fatto identica a quella del caso in cui A e B sono sottoinsiemi di X.

Soluzione: Diamo una dimostrazione della prima uguaglianza (l'altra è del tutto analoga).

Se $x \in X \setminus (A \cap B)$, l'elemento x è un elemento di x che non è comune ad A e B, quindi o non è in A, o non è in B. In formule questo vuol dire che $x \in (X \setminus A) \cup (X \setminus B)$.

Viceversa, se $x \in (X \setminus A) \cup (X \setminus B)$, l'elemento x è sicuramente in X ma o non sta in A oppure non sta in B e quindi non può essere contemporaneamente in A e B, cioè non può stare in $A \cap B$. Ma questo, in formule, vuol dire che $x \in X \setminus (A \cap B)$.

Esercizio 12. *Dimostrare che dati insiemi A e B si ha*

$$A \cup B \setminus A = \mathcal{C}_B(A \cap B).$$

Soluzione: Sia $x \in A \cup B \setminus A$. Siccome $x \notin A$ deve succedere che $x \in B$ (altrimenti non potrebbe stare in $A \cup B$). Ma allora $x \in \mathcal{C}_B(A \cap B)$ perché questo insieme è formato dagli elementi in B non in A.

Viceversa se $x \in \mathcal{C}_B(A \cap B)$, x è un elemento di B non in A. Ma se $x \in B$ sicuramente è anche $x \in A \cup B$ e dunque $x \in A \cup B \setminus A$.

Esercizio 13. *Si considerino gli insiemi*

$$\begin{array}{ll} A = \{a, g, h, i, p, u, v\} & B = \{b, g, l, m, n, q, v, z\} \\ C = \{d, e, f, m, n, o, q, r, s, v\} & D = \{c, d, e, h, i, p, r, t, u, z\} \end{array}$$

Dire quali delle seguenti affermazioni sono vere e quali false.

$$A \cap B \subset C \qquad \{d, e\} \in P(C \cap D) \quad (A \times B) \cap (C \times D) = \emptyset$$

$$(v, v) \in A \times B \setminus B \times C \qquad (e, p) \in A \times D \qquad \{b, l, u\} \subset P(B \cup D)$$

Soluzione: falsa, vera, falsa, falsa, vera, falsa

Esercizio 14. *Determinare tutte le partizioni possibili dell'insieme $A = \{a, b, c, d\}$.*

Soluzione: Possiamo elencare sistematicamente le partizioni di A come segue.

- C'è la partizione di A formata dal solo sottoinsieme A.

- Ci sono le partizioni formate da un sottoinsieme con 3 elementi e un sottoinsieme con un solo elemento:

$$\{a,b,c\}\cup\{d\},\ \{a,b,d\}\cup\{c\},\ \{a,c,d\}\cup\{b\},\ \{b,c,d\}\cup\{a\}.$$

- Ci sono le partizioni formate da due sottoinsiemi con 2 elementi:

$$\{a,b\}\cup\{c,d\},\ \{a,c\}\cup\{b,d\},\ \{a,d\}\cup\{b,c\}.$$

- Ci sono le partizioni formate da un sottoinsieme con 2 elementi e due e sottoinsiemi con un solo elemento

$$\begin{array}{lll}\{a,b\}\cup\{c\}\cup\{d\}, & \{a,c\}\cup\{b\}\cup\{d\}, & \{a,d\}\cup\{b\}\cup\{c\},\\ \{b,c\}\cup\{a\}\cup\{d\}, & \{b,d\}\cup\{a\}\cup\{c\}, & \{c,d\}\cup\{a\}\cup\{b\}.\end{array}$$

- C'è la partizione formata da 4 sottoinsiemi con un singolo elemento:

$$\{a\}\cup\{b\}\cup\{c\}\cup\{d\}.$$

Esercizio 15. *Sia $\mathcal{R}$ l'insieme delle rette per l'origine O in un piano cartesiano Oxy. È vero che $\mathcal{R}$ è un ricoprimento del piano? Una partizione?*

Soluzione: Le rette per l'origine formano un ricoprimento perché la loro unione è tutto il piano: dato un qualunque punto P del piano certamente esiste una retta per l'origine che contiene P.

Però non sono una partizione del piano perché due rette per l'origine non sono mai ad intersezione vuota, entrambe contenendo–per definizione–l'origine.

Esercizio 16. *Sia X un insieme con un numero finito n di elementi, $|X| = n$. Per ogni $k = 0, 1, \ldots, n$ sia*

$$P_k = \{A \subset X \text{ tali che } |A| = k\}.$$

Dimostrare che $\mathcal{P} = \{P_k\}$ è una partizione di $P(X)$. Quanti elementi ha l'insieme quoziente?

Soluzione: I sottoinsiemi assegnati formano un ricoprimento di $P(X)$ perché ogni sottoinsieme di X deve avere un numero di elementi compresi fra 0 e n e quindi appartiene ad uno dei P_k.

Inoltre è chiaro che se $k \neq \ell$ si ha $P_k \cap P_\ell = \emptyset$ in quanto il numero degli elementi di un sottoinsieme di X è ben determinato.

Infine, l'insieme quoziente consiste di $n+1$ elementi in quanto ci sono proprio $n+1$ possibilità per $|S|$ per un sottoinsieme $S \subset X$.

Esercizio 17. *Siano $A = A_1 \cup A_2$ e $B = B_1 \cup B_2$ due insiemi con partizioni assegnate. Dimostrare che*

$$A \times B = (A_1 \times B_1) \cup (A_1 \times B_2) \cup (A_2 \times B_1) \cup (A_2 \times B_2)$$

è una partizione di $A \times B$.

Esercizio 18. *Sia* $S = \mathbb{R} \times \mathbb{R} \setminus [0,1] \times [0,1]$. *Determinare una partizione di* A *formata da sottoinsiemi della forma* $A \times B$.

Soluzione: Le soluzioni sono molteplici. Una possibile soluzione è la seguente. Poniamo

$$X = \{r \in \mathbb{R} \text{ tali che } r < 0\} \quad \text{e} \quad Y = \{r \in \mathbb{R} \text{ tali che } r > 1\}.$$

Allora

$$S = (X \times \mathbb{R}) \cup ([0,1] \times X) \cup ([0,1] \times Y) \cup (Y \times \mathbb{R})$$

è una partizione del tipo voluto (fare un disegno per sincerarsene).

Esercizio 19. *Dimostrare per induzione le formule seguenti.*

1. $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1)$ *per ogni* $n \geq 1$.
2. $1 + 3 + 5 + \cdots + (2n-1) = n^2$ *per ogni* $n \geq 1$.
3. $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$ *per ogni* $n \geq 1$.
4. $n^2 > 2n + 1$ *per ogni* $n \geq 3$.
5. $2^n > n^2$ *per ogni* $n \geq 5$.

Soluzione

1. La formula è vera per $n = 1$ perché $1 = \frac{1}{2}1 \cdot 2$. Supponiamo (ipotesi induttiva) la formula vera per n. Per $n+1$ si ha

$$\begin{aligned} 1 + 2 + 3 + \cdots + (n+1) &= (1 + 2 + 3 + \cdots + n) + (n+1) \\ &= \frac{1}{2}n(n+1) + (n+1) \\ &= (\frac{1}{2}n + 1)(n+1) = \frac{1}{2}(n+1)(n+2) \end{aligned}$$

   Poiché l'espressione finale è quella che si ottiene da $\frac{1}{2}n(n+1)$ sostituendo n con $n+1$ la formula enunciata è vera per ogni $n \geq 1$.

2. La formula è vera per $n = 1$ perché $1 = 1^2$. Supponiamo (ipotesi induttiva) la formula vera per n. Per $n+1$ si ha

$$\begin{aligned} 1 + 3 + \cdots + (2n+1) &= (1 + 3 + \cdots + (2n-1)) + (2n+1) \\ &= n^2 + (2n+1) \\ &= (n+1)^2 \end{aligned}$$

   Poiché l'espressione finale è quella che si ottiene da n^2 sostituendo n con $n+1$ la formula enunciata è vera per ogni $n \geq 1$.

3. La formula è vera per $n = 1$ perché $1 = \frac{1}{4}1^2 \cdot 2^2$. Supponiamo (ipotesi induttiva) la formula vera per n. Per $n+1$ si ha

$$\begin{aligned} 1^3 + 2^3 + \cdots + n^3 + (n+1)^3 &= (1^3 + 2^3 + \cdots + n^3) + (n+1)^3 \\ &= \frac{1}{4}n^2(n+1)^2 + (n+1)^3 \\ &= (n+1)^2\left(\frac{1}{4}n^2 + (n+1)\right) \\ &= \frac{1}{4}(n+1)^2(n^2+4n+4) \\ &= \frac{1}{4}(n+1)^2(n+2)^2 \end{aligned}$$

Poiché l'espressione finale è quella che si ottiene da $\frac{1}{4}n^2(n+1)^2$ sostituendo n con $n+1$ la formula enunciata è vera per ogni $n \geq 1$.

4. La disuguaglianza è vera per $n = 3$ perché $3^2 = 9 \geq 2 \cdot 3 + 1 = 7$ (si noti che è falsa per $n = 0$, 1 o 2). Supponiamo (ipotesi induttiva) la disuguaglianza vera per n. Poiché $n \geq 3$ si ha sicuramente $2n + 1 \geq 2$ e quindi per $n+1$ si ha

$$\begin{aligned} (n+1)^2 &= n^2 + 2n + 1 \\ &\geq (2n+1) + 2 \\ &= 2(n+1) + 1 \end{aligned}$$

Poiché l'espressione finale è quella che si ottiene da $2n + 1$ sostituendo n con $n+1$ la disuguaglianza enunciata è vera per ogni $n \geq 3$.

5. La disuguaglianza è vera per $n = 5$ perché $2^5 = 32 \geq 5^2 = 25$ (si noti che è falsa per $n = 0$, 1, 2, 3 e 4). Supponiamo (ipotesi induttiva) la disuguaglianza vera per n. Poiché $n^2 \geq 2n + 1$, come dimostrato nel punto precedente, per $n+1$ si ha

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &\geq 2n^2 = n^2 + n^2 \\ &\geq n^2 + 2n + 1 = (n+1)^2 \end{aligned}$$

Poiché l'espressione finale è quella che si ottiene da n^2 sostituendo n con $n+1$ la disuguaglianza enunciata è vera per ogni $n \geq 5$.

CdS Informatica – Torino
Corso di Matematica Discreta

Esercizi dal Libro di Testo–Soluzioni
Capitolo 2

Esercizio 1. Sia $f : \mathbb{Z} \to \mathbb{Z}$ la funzione definita da $f(n) = n^2 - 1$. Calcolare $f^{-1}(-5)$, $f^{-1}(-1)$, $f^{-1}(8)$, $f^{-1}(12)$.

Soluzione: Per trovare $f^{-1}(k)$ occorre risolvere l'equazione $f(n) = n^2 - 1 = k$. Quindi:

- $f^{-1}(-5) = \emptyset$;
- $f^{-1}(-1) = \{0\}$;
- $f^{-1}(8) = \{-3, 3\}$;
- $f^{-1}(12) = \emptyset$ (in quanto $\pm\sqrt{13} \notin \mathbb{Z}$).

Esercizio 2. Sia $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ la funzione definita come $f((m, n)) = m^2 - n$.

1. Dire se f è iniettiva.
2. Dire se f è suriettiva.
3. Calcolare l'insieme $f^{-1}(0) \cap \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \,|\, n = 4m\}$.
4. Calcolare l'immagine $f(S)$ del sottoinsieme $S = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \,|\, n = 2m - 1\}$.

Soluzione:

- f non è iniettiva, ad esempio $f((-m, 0)) = f((m, 0)) = m^2$ per ogni $m \in \mathbb{Z}$;
- f è suriettiva, ad esempio $f((0, n)) = n$ per ogni $n \in \mathbb{Z}$;
- Ci stiamo chiedendo chi sono i valori $m \in \mathbb{Z}$ per cui $f((m, 4m)) = m^2 - 4m = 0$, quindi $\{0, 4\}$;
- Si ha $f((m, 2m - 1)) = m^2 - (2m - 1) = (m - 1)^2$ per cui $f(S) = \{0, 1, 4, 9, ...\}$ (insieme dei quadrati in $\mathbb{Z}$).

Esercizio 3. Sia $f : \mathbb{N} \to \mathbb{N}$ la funzione definita come

$$f(n) = \begin{cases} n/2 & \text{se } n \text{ è pari,} \\ 3n + 1 & \text{se } n \text{ è dispari.} \end{cases}$$

Dimostrare o confutare le affermazioni seguenti:

a) f è iniettiva;

b) f è suriettiva;

c) l'immagine $f(2\mathbb{N})$ dell'insieme dei numeri pari è contenuta nell'insieme dei numeri dispari;

d) la controimmagine $f^{-1}(3\mathbb{N})$ dell'insieme dei numeri divisibili per 3 è contenuta nell'insieme dei numeri pari.

Dopodiché, calcolare esplicitamente

$$f(\{1,2,3,4,5,6,7,8,9,10\}) \quad \text{e} \quad f^{-1}(\{1,2,7,9,10,13\}).$$

Soluzione:

- f non è iniettiva, ad esempio $f(1) = f(8) = 4$;
- f è suriettiva, ad esempio $f(2n) = n$ per ogni $n \in \mathbb{N}$;
- l'affermazione è falsa, ad esempio 4 è pari ma $f(4) = 2$ è ancora pari;
- l'affermazione è vera perché se n è dispari allora $f(n) = 3n + 1$ non è mai un multiplo di 3.

Infine $f(\{1,2,3,4,5,6,7,8,9,10\}) = \{1,2,3,4,5,10,16,22,28\}$ e $f^{-1}(\{1,2,7,9,10,13\}) = \{2,3,4,14,18,20,26\}$.

Esercizio 4. Descrivere il grafico delle proiezioni $p_1 : A \times B \to A$ e $p_2 : A \times B \to B$.

Soluzione: Il grafico della proiezione p_1 è costituito dalle terne in $A \times B \times A$ della forma

$$(a, b, a) \qquad a \in A, b \in B.$$

Quello della proiezione p_2 è analogo.

Esercizio 5. Sia $f : A \to B$ una funzione con grafico Γ e sia $S \subset A$ un sottoinsieme. Denotiamo Γ_S il grafico della restrizione $f_{|S}$ di f ad S. Si dimostri che $\Gamma_S = \Gamma \cap (S \times B)$.

Soluzione: Per definizione si ha $f_{|S}(s) = f(s)$ per ogni $s \in S$, quindi:

- $(s, b) \in \Gamma_S \Rightarrow f_{|S}(s) = f(s) = b \Rightarrow (s, b)\Gamma$. Ma è anche $(s, b) \in S \times B$, dunque $(s, b) \in \Gamma_S \cap S \times B$.
- $(s, b) \in \Gamma_S \cap S \times B \Rightarrow s \in S$ e $f_{|S}(s) = b = f(s)$. Dunque $(s, b) \in \Gamma$.

Esercizio 6. Sia $f : A \to B$ una funzione, $S \subset A$ un sottoinsieme del dominio e $T \subset B$ un sottoinsieme del codominio. Si dimostri che $f(S) = \bigcup_{s \in S} \{f(s)\}$ e che $f^{-1}(T) = \bigcup_{t \in T} f^{-1}(t)$.

Soluzione: Le identità seguono immediatamente per definizione.

Esercizio 7. Sia Γ il grafico della funzione $f : A \to B$. Dimostrare che f è iniettiva se e soltanto se per ogni $b \in B$ l'intersezione $\Gamma \cap (A \times \{b\})$ contiene al più un elemento.

Soluzione: Equivalentemente dimostriamo che f non è iniettiva se e soltanto se esiste un $b \in B$ tale che l'intersezione $\Gamma \cap (A \times \{b\})$ contiene al più un elemento:

- f non iniettiva vuol dire che esistono $a_1 \neq a_2$ in A tali che $f(a_1) = f_(a_2)$. Posto $b = f(a_1) = f_(a_2)$, allora (a_1, b) e (a_1, b) sono due elementi distinti in $\Gamma \cap (A \times \{b\})$.
- Se (a_1, b) e (a_1, b) sono due elementi distinti in $\Gamma \cap (A \times \{b\})$ si ha $b = f(a_1) = f(a_2)$ per definizione di Γ, cioè f non è iniettiva.

Esercizio 8. Ciascuna delle seguenti funzioni non è biettiva (spiegare perché). Modificare in modo opportuno dominio e/o codominio in modo da ottenere una funzione biettiva e scrivere quindi la funzione inversa di quella così trovata.

1. $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = 3n$;
2. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 2x$.
3. $f : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x, y) = (x^2, x^2 + y^2)$.

Soluzione:

1. f non è suriettiva, ad esempio $1 \notin \mathrm{im}(f)$, f diventa biettiva come funzione $\mathbb{Z} \to 3\mathbb{Z}$;
2. f non è ne' iniettiva ($f(-2) = f(0) = 0$) ne' suriettiva ($-2 \notin \mathrm{im}(f)$), f diventa biettiva ad esempio come funzione $\mathbb{R}^{>0} \to \mathbb{R}^{>0}$;
3. f non è ne' iniettiva ($f((-1, 0)) = f((1, 0)) = (1, 1)$) ne' suriettiva ($\mathrm{im}(f) \subset \mathbb{R}^{>0} \times \mathbb{R}^{>0}$), ci sono molti modi per ottenere una mappa biettiva restringendo dominio e codominio, ad esempio come mappa $\mathbb{R}^{>0} \times \{0\} \to \{(r, r) \mid r > 0\}$.

Esercizio 9. Sia $f : A \to B$ una funzione con grafico Γ. Si dimostri che la funzione $(p_1)_{|\Gamma} : \Gamma \to A$, restrizione a $\Gamma \subset A \times B$ della prima proiezione, è una biezione.

Soluzione: La funzione $(p_1)_{|\Gamma} : \Gamma \to A$ è biettiva perché:

- è iniettiva in quanto per ogni $a \in A$ esiste un solo $b \in B$ con $(a, b) \in \Gamma$;
- è suriettiva in quanto per ogni $a \in A$ un $b \in B$ con $(a, b) \in \Gamma$ esiste.

Esercizio 10. Supponiamo di avere funzioni $f : \mathbb{N} \to \mathbb{Z}$, $g : \mathbb{Z} \to \mathbb{Z}$, $h : \mathbb{Z} \to \mathbb{N}$. Dire quali delle seguenti composizioni sono legittime e quali no specificandone, in caso affermativo, dominio e codominio:

$$g \circ h, \quad h \circ f, \quad g \circ f, \quad f \circ g, \quad g \circ f \circ h, \quad g \circ g \circ f, \quad f \circ h \circ h.$$

Soluzione:

$$NO, \quad \mathbb{N} \to \mathbb{N}, \quad \mathbb{N} \to \mathbb{Z}, \quad NO, \quad \mathbb{Z} \to \mathbb{Z}, \quad NO, \quad NO.$$

Esercizio 11. Siano $f, g : \mathbb{Z} \to \mathbb{Z}$ due funzioni così definite:

$$f(n) = \begin{cases} 2n+1 & \text{se } n \text{ è pari,} \\ 5-n & \text{se } n \text{ è dispari,} \end{cases}, \qquad g(n) = \begin{cases} 0 & \text{se } n \geq 0, \\ 2-n^2 & \text{se } n < 0. \end{cases}$$

Calcolare $f \circ g(1)$, $g \circ f(-1)$, $f \circ g \circ f(0)$, $g \circ g \circ f(3)$, $f \circ g \circ g(-2)$, $g \circ f \circ g(2)$.

Soluzione:

$$\begin{array}{lll} f \circ g(1) = 1 & g \circ f(-1) = 0 & f \circ g \circ f(0) = 1 \\ g \circ g \circ f(3) = 0 & f \circ g \circ g(-2) = -7 & g \circ f \circ g(2) = 0 \end{array}$$

Esercizio 12. Costruire un esempio esplicito di funzione $f : A \to B$ e funzioni $g_1, g_2 : B \to Y$ e $h_1, h_2 : X \to A$ con $g_1 \neq g_2$ e $h_1 \neq h_2$ tali che $g_1 \circ f = g_2 \circ f$ e $f \circ h_1 = f \circ h_2$.

Soluzione: Si possono fare molti esempi.

Esercizio 13. Mostrare che la funzione id_X è l'unico elemento neutro per l'operazione di composizione $\circ$ in $\mathcal{F}_X$

Soluzione: Sia $e : X \to X$ una funzione neutra per la composizione. Consideriamo la composizione

$$h = \mathrm{id}_X \circ e.$$

Poiché id_X è neutra $h = e$. Poiché e è neutra $h = \mathrm{id}_X$. Dunque $\mathrm{id}_X = e$.

Esercizio 14. Una funzione $f : \mathbb{R} \to \mathbb{R}$ della forma $f(x) = ax + b$ dove a e $b \in \mathbb{R}$ sono costanti e $a \neq 0$ si dice *lineare*. Si dimostri che:

a) ogni funzione lineare è invertibile con inversa una funzione lineare;

b) la composizione di funzioni lineari è lineare.

Soluzione:

- L'inversa della funzione $f(x) = ax + b$ è la funzione $g(x) = \frac{1}{a}x - \frac{b}{a}$, lineare anch'essa.
- Date funzioni lineari $f(x) = ax + b$ e $g(x) = cx + d$ la composizione

  $$g \circ f(x) = g(f(x)) = g(ax + b) = c(ax + b) + d = acx + bc + d$$

  è ancora lineare.

Esercizio 15. Prendendo spunto dalla proposizione 2.24 e dalla sua dimostrazione, enunciare e dimostrare una formula per l'inverso di una composizione di più di due funzioni biettive.

Soluzione: La formula è $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Per dimostrarla basta comporre $f^{-1} \circ g^{-1}$ con $g \circ f$ nei due modi possibili e verificare che si ottiene la funzione identità in ciascun caso.

Esercizio 16. In ciascuno dei casi seguenti di insieme X con operazione $*$ dire se le proprietà associativa e commutativa sono soddisfatte o no. Dire anche se un elemento neutro esiste e se, in tal caso, quali elementi di X ammettono inverso.

1. $X = \mathbb{N}$ e $m * n = m^n$ (assumiamo $0^0 = 1$).
2. $X = \mathbb{N}$ e $m * n = m + n + 1$
3. $X = \mathbb{Z}$ e $m * n = mn + m + n$.
4. $X = \mathbb{Z}$ e
$$m * n = \begin{cases} m + n & \text{se almeno uno tra } m \text{ ed } n \text{ è pari,} \\ 0 & \text{se } m \text{ ed } n \text{ sono entrambi dispari.} \end{cases}$$
5. $X = \mathbb{Z}$ e $m * n = 2m + 3n$.
6. $X = \mathbb{Z} \times \mathbb{Z}$ e $(a, b) * (c, d) = (a + c, bd)$.
7. $X = \mathbb{R}^\times \times \mathbb{R}$ e $(a, b) * (c, d) = (ac, bc + d)$.
8. $X \neq \emptyset$ qualunque e $x * y = x$.
9. X il piano della geometria euclidea,
$$P * Q = \begin{cases} M & \text{punto medio del segmento } PQ \text{ se } P \neq Q, \\ P & \text{se } P = Q. \end{cases}$$

Soluzione:

1. Ne' commutativa, ne' associativa. Non c'è elemento neutro.
2. Commutativa ed associativa. Non c'è elemento neutro.
3. Commutativa ed associativa con elemento neutro $e = 0$. L'unico elemento ad avere inverso è 0 stesso.
4. Commutativa, non associativa (ad esempio $(1*1)*2 = 2$ ma $1*(1*2) = 0$), con elemento neutro $e = 0$. Se m è pari l'inverso di m è $-m$, se m è dispari ogni numero dispari è inverso di m.
5. Ne' commutativa, ne' associativa. Non c'è elemento neutro.
6. Commutativa ed associativa con elemento neutro $(0, 1)$. Gli elementi invertibili sono tutti e soli quelli della forma $(m, \pm 1)$.

7. Associativa ma non commutativa con elemento neutro $(1, 0)$. L'elemento (a, b) ha inverso $(\frac{1}{a}, -\frac{b}{a})$.

8. Associativa ma non commutativa. Non c'è elemento neutro.

9. Commutativa ma non associativa. Non c'è elemento neutro.

CdS Informatica – Torino
Corso di Matematica Discreta

Esercizi dal Libro di Testo–Soluzioni
Capitolo 3

Esercizio 1. Siano A e B due insiemi non vuoti, Dimostrare che:

1. se esiste una funzione iniettiva $f : A \to B$ allora esiste una funzione suriettiva $g : B \to A$;
2. se esiste una funzione suriettiva $f : A \to B$ allora esiste una funzione iniettiva $g : B \to A$.

Soluzione:

1. Per ogni $b \in \mathrm{Im}(f)$ si ha che $f^{-1}(b) = \{a\}$ (un solo elemento) in quanto f è iniettiva. Poniamo dunque $g(b) = a$. Infine se $b \notin \mathrm{Im}(f)$ poniamo come $g(b)$ un elemento di A arbitrariamente scelto. La funzione g è suriettiva perché per ogni $a \in A$ si ha $a = g(f(a))$.
2. Per ogni $b \in B$ si ha $f^{-1}(b) \neq \emptyset$. Definiamo g ponendo $g(b) =$ un qualunque elemento in $f^{-1}(b)$. La funzione g è iniettiva in quanto se $b \neq b' \in B$ si ha $f^{-1}(b) \cap f^{-1}(b') = \emptyset$ e quindi $g(b) \neq g(b')$.

Esercizio 3. Scrivere la formula del principio di inclusione-esclusione per 4 insiemi A, B, C, D nell'ipotesi che ogni intersezione di 3 di essi è vuota.

Soluzione: Per $X = A \cup B \cup C \cup D$ si ha

$$|X| = |A|+|B|+|C|+|D|-|A\cap B|-|A\cap C|-|A\cap D|-|B\cap C|-|B\cap D|-|C\cap D|.$$

Esercizio 4. Calcolare quanti sono i numeri interi

1. da 1 e 1680 che sono divisibili per almeno uno tra 2, 6 e 7;
2. da 1 e 2160 che non sono divisibili né per 5, ne' per 9 né per 12.

Soluzione: Indichiamo $I_n(d)$ l'insieme dei numeri interi da 1 a n che sono multipli di d. Osservato che per ogni d e d' si ha

$$I_n(d) \cap I_n(d') = I_n(m)$$

dove m è il minimo comune multiplo di d e d' e che $|I_n(d)| = \frac{n}{d}$ quando d divide n, si ha quanto segue.

1. Vogliamo calcolare $N = |I_{1680}(2) \cup I_{1680}(6) \cup I_{1680}(7)|$. Poiché $I_{1680}(6) \subset I_{1680}(2)$ l'insieme $I_{1680}(6)$ puó essere ignorato. Dunque

$$N = |I_{1680}(2)| + |I_{1680}(7)| - |I_{1680}(14)| = 840 + 240 - 120 = 960.$$

2. Vogliamo calcolare $N = 2160 - |I_{2160}(5) \cup I_{2160}(9) \cup I_{2160}(12)|$. Detta X l'unione dei tre insiemi,

   $$|X| = |I_{2160}(5)|+|I_{2160}(9)|+|I_{2160}(12)|-|I_{2160}(45)|-|I_{2160}(60)|-|I_{2160}(36)|+|I_{2160}(180)|$$

   calcolando i singoli addendi $|X| = 432+240+180-48-36-18+12 = 762$. Dunque $N = 1398$.

Esercizio 5. Un numismatico possiede una collezione che include 25 monete d'argento, 170 monete europee e 415 monete di formato rotondo. Sappiamo che ogni sua moneta possiede almeno una delle caratteristiche suddette. Sappiamo anche che: le monete d'argento tonde sono 22, le monete europee tonde sono 152 e le monete europee d'argento sono tutte tonde. Quante monete ci sono nella collezione?

Soluzione: Indichiamo con A l'insieme delle monete d'argento, E l'insieme delle monete europee e R l'insieme delle monete rotonde presenti nella collezione. Le informazioni contenute nel testo del problema sono che:

- $C = A \cup E \cup R$ esaurisce l'intera collezione e pertanto $|A \cup E \cup R|$ è il numero che dobbiamo calcolare;
- $|A| = 25$, $|E| = 170$, $|R| = 415$, $|A \cap R| = 22$, $|E \cap R| = 152$;
- $A \cap E \subset R$,

In particolare, l'ultima informazione comporta che $A \cap E = A \cap E \cap R$ e quindi nella formula di inclusione applicata a questa situazione i termini $+|A \cap E \cap R|$ e $-|A \cap E|$ si cancellano l'un l'altro. Dunque la formula fornisce

$$|C| = 25 + 170 + 415 - 22 - 152 = 436.$$

Esercizio 6. Ad una festa c'erano 20 persone con i capelli biondi, 18 con i capelli neri, 15 con gli occhi azzurri e 12 con gli occhi verdi e ogni invitato aveva almeno una di queste caratteristiche. Sappiamo che delle persone bionde 12 avevano occhi azzurri e 4 occhi verdi mentre tra coloro che avevano capelli neri 1 aveva occhi azzurri e 7 occhi verdi. Quante persone erano presenti alla festa?

Soluzione: Denotiamo F l'insieme delle persone presenti alla festa, B ed N gli insiemi delle persone con i capelli biondi e neri rispettivamente, A e V gli insiemi delle persone con gli occhi azzurri e verdi rispettivamente. Le informazioni che possiediamo sono:

- $F = B \cup N \cup A \cup V$;
- $|B| = 20$, $|N| = 18$, $|A| = 15$, $|V| = 12$;
- $|B \cap A| = 12$, $|B \cap V| = 4$, $|N \cap A| = 1$, $|N \cap V| = 7$.

Inoltre sappiamo che certamente

$$B \cap N = \emptyset, \qquad A \cap V = \emptyset$$

in quanto le condizioni di colore sui capelli e sugli occhi sono mutualmente esclusive. Inoltre ogni intersezione fra tre o quattro dei suddetti insiemi deve essere vuota, in quanto presi comunque tre tra B, N, A e V la loro intersezione è contenuta in $B \cap N$ o in $A \cap V$.

Quindi abbiamo tutte le informazioni necessarie per applicare il principio di inclusione-esclusione per il calcolo di F e la formula fornisce

$$|F| = 20 + 18 + 15 + 12 - 12 - 4 - 1 - 7 = 41.$$

Esercizio 8. Anna possiede 11 magliette, 5 paia di pantaloni, 6 paia di scarpe e 2 borsette.

1. In quanti modi diversi Anna può scegliere maglietta, pantaloni, scarpe e borsetta per vestirsi?
2. 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?
3. 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:

1. Le scelte sono indipendenti quindi il totale è il prodotto:

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

2. Si vogliono contare le disposizioni di 6 oggetti tra 14 per cui possiamo applicare direttamente la formula

$$D_{6,14} = \frac{14!}{8!} = 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 = 2.162.160$$

3. Anna può scegliere le magliette in $\binom{11}{4}$ modi, i pantaloni in $\binom{5}{2}$ modi, le scarpe in $\binom{6}{2}$ modi e la borsetta in 2 modi. Poiché le scelte sono indipendenti il loro totale è

$$\binom{11}{4} \cdot \binom{5}{2} \cdot \binom{6}{2} \cdot 2 = 99.000$$

Esercizio 9. Sei amici, Alessandro, Bruno, Carlo, Daniele, Enrico e Franco prendono posto su una fila di sei sedie. Calcolare in quanti modi i sei possono sedersi

1. senza restrizioni;

2. oppure in modo che Carlo e Franco siedano sulle due sedie centrali;

3. oppure in modo che Bruno e Daniele siedano vicini.

Soluzione:

1. Stiamo considerando funzioni biettive tra l'insieme dei 6 amici e l'insieme delle 6 sedie. Sono 6!.

2. Ci sono 2 modi di far sedere Carlo e Franco nelle sedie centrali: Carlo a sinistra e Franco a destra, oppure Carlo a destra e Franco a sinistra. Ciascuna di queste scelte può essere completata con un'unica disposizione dei restanti 4 amici sulle 4 sedie esterne. Poichè ci sono 4! modi di fare ciò, per il metodo delle scelte successive il numero totale delle sistemazioni è

$$2 \cdot 4! = 2 \cdot 24 = 48.$$

3. Ci sono 10 modi per assegnare un posto a Bruno e Daniele: Bruno sulla sedia 1 e Daniele sulla sedia 2, Bruno sulla sedia 2 e Daniele sulla sedia 1, Bruno sulla sedia 2 e Daniele sulla sedia 3, eccetera. Ciascuna di queste scelte può essere completata con un'unica disposizione dei restanti 4 amici sulle 4 sedie rimanenti. Poichè ci sono 4! modi di fare questo secondo passo, per il metodo delle scelte successive il numero totale delle sistemazioni è

$$10 \cdot 4! = 10 \cdot 24 = 240.$$

Soluzione alternativa. Un altro modo di arrivare al totale è quello di pensare alla coppia (Bruno, *Daniele*) come un unico "elemento" e quindi il problema si riconduce a quello di far sedere 5 elementi in 5 posti, cosa che si può fare in 5! modi. Ciascuna di queste sistemazioni va però contata 2 volte: una volta quando Bruno siede a sinistra di Daniele, l'altra quando Bruno siede a destra di Daniele. pertanto il totale è

$$2 \cdot 5! = 2 \cdot 120 = 240.$$

Esercizio 10. Ad un corso di ballo sono iscritti 11 uomini ed 9 donne. Si tengono due lezioni la settimana, il lunedì e il giovedì.

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

2. Per uno spettacolo alla fine del corso i maestri scelgono fra gli studenti 5 uomini e 5 donne per una certa coreografia. Quante sono le scelte possibili di quei 10 studenti?

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

Soluzione:

1. Ogni ballerina può ballare con ogni ballerino, quindi il totale delle coppie possibili è $11 \cdot 9 = 99$.

2. Le scelte di 5 uomini su 11 sono $\binom{11}{5}$ e le scelte di 5 donne su 9 sono $\binom{9}{5}$. Poiché le scelta di un gruppo di uomini è indipendente da quella di un gruppo di donne il numero totale delle scelte dei 10 ballerini è

$$\binom{11}{5} \cdot \binom{9}{5} = \frac{11!}{5! \cdot 6!} \cdot \frac{9!}{5! \cdot 4!} = 58464$$

3. Complessivamente, lunedì erano presenti 15 studenti e giovedì erano presenti 16 studenti. Detto n il numero degli studenti presenti ad entrambi le lezioni il principio di inclusione-esclusione fornisce la relazione

$$20 = 15 + 16 - n$$

da cui $n = 11$.

Esercizio 11. Viene formato un gruppo di lavoro costituito da 16 informatici per un progetto europeo a cui partecipano Italia, Francia, Belgio, Spagna.

1. Il gruppo di lavoro sarà denominato con una sigla formata dalle 4 iniziali I, F, B, S delle nazioni coinvolte. Quanti sono le possibili sigle?

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

3. Una volta scelto il gruppo dei 16 informatici, si provvede ad attribuire i compiti: 7 di loro lavoreranno al sottoprogetto 1, 6 al sottoprogetto 2, i tre rimanenti ricopriranno il ruolo di coordinatore tra i due progetti, di responsabile del budget e di responsabile della presentazione dei risultati. In quanti modi in totale si possono attribuire i compiti?

Soluzione:

1. Poiché le iniziali sono tutte distinte, dobbiamo contare gli ordinamenti di 4 elementi che dunque sono $4! = 24$.

2. Sottolineiamo che nel calcolare questo tipo di scelte stiamo considerando solo le nazionalit delle persone e non gli individui. Per contare il numero delle scelte possibili di 16 persone in modo che ognuna delle 4 nazionalità sia rappresentata seguiamo la strategia seguente. Come primo passo scegliamo una persona di ciascuna nazionalità. Questa scelta è unica.

   A questo punto completiamo la scelta dei 16 scegliendo in modo arbitrario le 12 persone: comunque ciò si faccia alla fine tutte e quattro le nazionalità saranno rappresentate perché di ciò si è occupato il primo passo. Ma scegliere 12 persone di 4 nazionalità in modo arbitrario è considerare le combinazioni con ripetizione di ordine $n = 12$ su un insieme con $k = 4$ elementi e quindi il loro numero è

$$\binom{n+k-1}{k-1} = \binom{15}{3} = \frac{15 \cdot 14 \cdot 13}{3 \cdot 2 \cdot 1} = 455.$$

3. Per il sottoprogetto 1 bisogna scegliere 7 persone su 16 e questo si può fare in $\binom{16}{7}$ modi. Per il sottoprogetto 2 bisogna scegliere 6 persone tra le rimanenti 9 e questo si può fare in $\binom{9}{6}$ modi. Infine le 3 persone rimanenti vanno ordinate nelle 3 posizioni rimanenti e questo si può fare in 3! modi.

   Poiché ad ogni passo la scelta è indipendente dalle precedenti, per il metodo delle scelte consecutive il totale delle possibili scelte di attribuzione di compiti è

$$\binom{16}{7} \cdot \binom{9}{6} \cdot 3! = \frac{16!}{7! \cdot 9!} \cdot \frac{9!}{6! \cdot 3!} \cdot 3! = \frac{16!}{7! \cdot 6!} = 5.765.760$$

Esercizio 12. Un fiorista vende rose di 5 colori diversi (rosa, rosse, gialle, bianche e azzurre).

1. Volendo acquistare un mazzo bicolore, quanti sono i possibili abbinamenti di colore?
2. Di quante rose deve essere costituito un mazzo per essere sicuri che ve ne siano almeno 5 dello stesso colore?
3. Quanti mazzi distinti di 12 rose si possono formare se si vuole che tutti i colori siano presenti?

Soluzione:

1. Scegliere due colori su 5 si può fare in $\binom{5}{2} = 10$ modi diversi.
2. Con 5 colori a disposizione un mazzo con $\leq 20 = 4 \cdot 5$ rose pu avere ogni colore rappresentato 4 volte o meno. Ma se le rose sono ≥ 21 almeno un colore deve essere presente almeno 5 volte.
3. Per formare un mazzo in cui ogni colore sia rappresentato iniziamo col scegliere una rosa per ogni colore. Fatto ciò, possiamo scegliere le rimanenti 7 rose in modo arbitrario. Quindi il problema equivale a calcolare il numero delle combinazioni con ripetizione di $n = 7$ rose con $k = 5$ colori, ed esse sono

$$\binom{7+5-1}{5-1} = \binom{11}{4} = \frac{11!}{7! \cdot 4!} = \frac{11 \cdot 10 \cdot 9 \cdot 8}{4 \cdot 3 \cdot 2 \cdot 1} = 330.$$

Esercizio 13. Alle semifinali olimpiche della gara dei 100 metri piani sono ammessi i 16 tempi migliori delle qualificazioni. I 16 atleti sono poi distribuiti in due semifinali da 8 atleti ciascuna. Determinare il numero delle possibili distribuzioni dei 16 atleti nelle due semifinali nei casi seguenti:

1. non si richiede nessuna condizione, tutte le possibilità sono ammesse;
2. i quattro atleti coi tempi migliori devono essere distribuiti equamente nelle due semifinali (due per ciascuna);

3. 9 atleti in semifinale sono europei e in ciascuna semifinale devono essere presenti non più di 6 atleti europei.

Soluzione: L'enunciato del problema contiene un'ambiguità che è lasciata al lettore da risolvere: conta solo la suddivisione dei 16 atleti in due gruppi di 8 oppure conta anche in quale precisa semifinale gli atleti vanno collocati? In altre parole: scambiando fra loro i due gruppi di semifinalisti conta come una sola distribuzione o come 2? Risolviamo il problema in entrambe le situazioni.

Assumiamo quindi che le **semifinali sono distinte**, abbiamo cioè una semifinale 1 ed una semifinale 2.

1. Per formare la semifinale 1 dobbiamo scegliere 8 dei 16 qualificati. Questo si può fare in
$$\binom{16}{8} = \frac{16!}{8! \cdot 8!} = 12.970$$
modi. Una volta scelti gli 8 primi semifinalisti la scelta dei secondi semifinalisti è obbligata e quindi il totale delle possibili distribuzioni è 12970.

2. Per formare la semifinale 1 prima scegliamo 2 dei 4 qualificati con i tempi migliori: questo si può fare in $\binom{4}{2}$ modi. Poi completiamo la semifinale 1 scegliendo 6 dal gruppo di 12 qualificati meno veloci: questo si può fare in $\binom{12}{6}$ modi. Una volta completata la semifinale 1 la scelta degli 8 partecipanti alla semifinale 2 è obbligata. Quindi il totale delle distribuzioni è
$$\binom{4}{2} \cdot \binom{12}{6} = \frac{4!}{2! \cdot 2!} \cdot \frac{12!}{6! \cdot 6!} = 6 \cdot 924 = 5.544$$

3. Per rispettare la condizione gli atleti europei possono suddividersi tra le due semifinali solo 6+3 o 5+4. Quindi alla semifinale 1 possono partecipare 3, 4, 5 o 6 atleti europei. Queste varie possibilità sono in alternativa e quindi dobbiamo calcolare in quanti modi si possono ottenere ognuna di esse e poi sommare i risultati parziali. Osserviamo che se inseriamo k atleti europei nella semifinale 1, la semifinale va poi completata con $8-k$ atleti scelti fra i 7 non europei. Quindi abbiamo
   - $\binom{9}{3} \cdot \binom{7}{5}$ modi di formare la semifinale 1 con 3 atleti europei;
   - $\binom{9}{4} \cdot \binom{7}{4}$ modi di formare la semifinale 1 con 4 atleti europei;
   - $\binom{9}{5} \cdot \binom{7}{3}$ modi di formare la semifinale 1 con 5 atleti europei;
   - $\binom{9}{6} \cdot \binom{7}{2}$ modi di formare la semifinale 1 con 6 atleti europei;

   In totale (ricordando che $\binom{9}{3} = \binom{9}{6}$, $\binom{7}{5} = \binom{7}{2}$, eccetera:
$$2 \cdot \binom{9}{3} \cdot \binom{7}{5} + 2 \cdot \binom{9}{4} \cdot \binom{7}{4} = 2 \cdot 84 \cdot 21 + 2 \cdot 126 \cdot 35 = 12748$$

Assumiamo invece ora che le **semifinali siano indistinguibili**, cioè guardiamo solo alla suddivisione dei 16 semifinalisti in due gruppi di 8 senza curarci di quale gruppo va nella semifinale 1 e quale nella semifinale 2. Per ogni ripartizione dei 16 in due gruppi di 8 ci sono due possibilità di compilare le semifinale, inserendo uno dei due gruppi di 8 una volta nella semifinale 1 ed una seconda volta nella semifinale 2. Pertanto in questa situazione possiamo semplicemente ripetere i calcoli fatti sopra ma alla fine dividere i risultati per 2. Quindi:

1. Le distribuzioni distinte in due semifinali sono $\frac{1}{2} \cdot \binom{16}{8} = 6.485$

2. Le distribuzioni distinte in due semifinali con i 4 tempi più veloci ripsrtiti $2+2$ sono $\frac{1}{2}\binom{4}{2} \cdot \binom{12}{6} = 2.772$

3. Le distribuzioni distinte in due semifinali con non più di 6 europei in una singola semifinale sono $\frac{1}{2}\left(2 \cdot \binom{9}{3} \cdot \binom{7}{5} + 2 \cdot \binom{9}{4}\binom{7}{4}\right) = 6.374$

Esercizio 14. Calcolare il numero degli anagrammi delle parole seguenti,

ALGORITMO, INFORMATICA, TORINO, DISPOSIZIONI, COROLLARIO.

Soluzione:

1. ALGORITMO ha 9 lettere di cui 2 O. Per cui gli anagrammi sono $\frac{9!}{2!} = 181.440$.

2. INFORMATICA ha 11 lettere di cui 2 A e 2 I. Per cui gli anagrammi sono $\frac{9!}{2!\cdot 2!} = 9.979.200$

3. TORINO ha 6 lettere di cui 2 O. Per cui gli anagrammi sono $\frac{6!}{2!} = 360$

4. DISPOSIZIONI ha 12 lettere di cui 4 I, 2 O e 2 S. Per cui gli anagrammi sono $\frac{12!}{4!\cdot 2!\cdot 2!} = 4.989.600$.

5. COROLLARIO ha 10 lettere di cui 3 O, 2 L e 2 R. Per cui gli anagrammi sono $\frac{10!}{3!\cdot 2!\cdot 2!} = 151.200$.

Esercizio 18. Se $n \geq 2$ e $2 \leq k \leq n-2$ dimostrare che

$$\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-1}{k-1} + \binom{n-2}{k}.$$

Poi dimostrare che la formula vale anche senza restrizione su k se poniamo $\binom{n}{k} = 0$ per $k \notin \{0, 1, ..., n\}$.

Soluzione: Se $2 \leq k \leq n-2$ usiamo una prima volta la formula di Stiefel per scrivere

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

e poi riapplichiamo una seconda volta la formula di Stiefel ai singoli addendi dell'ultima espressione per ottenere

$$\left(\binom{n-2}{k} + \binom{n-2}{k-1}\right) + \left(\binom{n-2}{k-1} + \binom{n-2}{k-2}\right) = \binom{n-2}{k-2} + 2\binom{n-1}{k-1} + \binom{n-2}{k}.$$

Dopodiché:

- Se $k = 0$ la formula da dimostrare diventa $\binom{n}{0} = 0 + 0 + 1$ ed è vera.
- Se $k = 1$ la formula da dimostrare diventa $\binom{n}{1} = 0 + 2 + (n-2)$ ed è vera.

I casi $k = n - 1$ e $k = n$ i trattano per simmetria.

Esercizio 19. Sia n dispari. Dimostrare che

$$\sum_{k \text{ pari}} \binom{n}{k} = \sum_{k \text{ dispari}} \binom{n}{k}.$$

L'uguaglianza è vera anche se n è pari?

Soluzione: Iniziamo col supporre n dispari. Ricordando che $\binom{n}{k} = \binom{n}{n-k}$ osserviamo che

$$k \text{ è pari} \iff n - k \text{ è dispari}.$$

Pertanto per ogni coefficiente binomiale $\binom{n}{k}$ con k pari ce ne è un secondo uguale con "denominatore" dispari. Dunque deve aversi

$$\sum_{k \text{ pari}} \binom{n}{k} = \sum_{k \text{ dispari}} \binom{n}{k}.$$

perché stiamo sommando esattamente gli stessi addendi a sinistra e a destra.

Supponiamo ora n pari. Scriviamo la formula di Newton per $(a + b)^n$ dove peró prendiamo $a = 1$ e $b = -1$. Poiché in questo caso $a + b = 0$ la formula diventa

$$0 = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot (-1)^k = \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k.$$

Nella sommatoria i coefficienti binomiali $\binom{n}{k}$ entrano con un segno $+$ per k pari e con un segno $-$ per k dispari. Pertanto separandoli otteniamo anche in questo caso l'uguaglianza

$$\sum_{k \text{ pari}} \binom{n}{k} = \sum_{k \text{ dispari}} \binom{n}{k}.$$

CdS Informatica – Torino
Corso di Matematica Discreta

Esercizi dal Libro di Testo–Soluzioni
Capitolo 4

Esercizio 1. Calcolare la divisione euclidea per le seguenti coppie di dividendo a e divisore b.

1. $a = 26754$, $b = -307$
2. $a = -29244$, $b = 289$
3. $a = 781116$, $b = 1101$

Soluzione:

1. Si ha $26754 = 87 \cdot 307 + 45$ e quindi
$$26754 = (-87) \cdot (-307) + 45.$$
2. Si ha $29244 = 101 \cdot 289 + 55$ e quindi
$$-29244 = (-102) \cdot 289 + 234.$$
3. Si ha $781116 = 709 \cdot 1101 + 507$.

Esercizio 2. Calcolare i seguenti massimi comuni denominatori e realizzare l'identità di Bezout.

1. MCD$(1156, 75)$.
2. MCD$(1377, 1071)$.
3. MCD$(3973, 1853)$.
4. MCD$(26125, 17043)$.
5. MCD$(40257, 5439)$.
6. MCD$(153664, 24321)$

Soluzione: Diamo la soluzione solo per le prime tre coppie di numeri.

1.
$$\begin{aligned} 1156 &= 15 \cdot 75 + 31 \\ 75 &= 2 \cdot 31 + 13 \\ 31 &= 2 \cdot 13 + 5 \\ 13 &= 2 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + \boxed{1} \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Dunque MCD$(1156, 75) = 1$, Per l'identità di Bezout:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \cdot 3 - 5 \\ &= 2(13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 5 \cdot 5 \\ &= 2 \cdot 13 - 5(31 - 2 \cdot 13) = 12 \cdot 13 - 5 \cdot 31 \\ &= 12(75 - 2 \cdot 31) - 5 \cdot 31 = 12 \cdot 75 - 29 \cdot 31 \\ &= 12 \cdot 75 - 29(1156 - 15 \cdot 75) = \boxed{447 \cdot 75 - 29 \cdot 1156}. \end{aligned}$$

2.

$$\begin{aligned} 1377 &= 1 \cdot 1071 + 306 \\ 1071 &= 3 \cdot 306 + \boxed{153} \\ 306 &= 2 \cdot 153 + 0 \end{aligned}$$

Dunque MCD$(1377, 1071) = 153$, Per l'identità di Bezout:

$$\begin{aligned} 153 &= 1071 - 3 \cdot 306 \\ &= 1071 - 3(1377 - 1071) = \boxed{4 \cdot 1071 - 3 \cdot 1377} \end{aligned}$$

3.

$$\begin{aligned} 3973 &= 2 \cdot 1853 + 267 \\ 1853 &= 6 \cdot 267 + 251 \\ 267 &= 1 \cdot 251 + 16 \\ 251 &= 15 \cdot 16 + 11 \\ 16 &= 1 \cdot 11 + 5 \\ 11 &= 2 \cdot 5 + \boxed{1} \\ 5 &= 5 \cdot 1 + 0. \end{aligned}$$

Dunque MCD$(3973, 1853) = 1$, Per l'identità di Bezout:

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 11 - 2(16 - 11) = 3 \cdot 11 - 2 \cdot 16 \\ &= 3(251 - 15 \cdot 16) - 2 \cdot 16 = 3 \cdot 251 - 47 \cdot 16 \\ &= 3 \cdot 251 - 47(267 - 251) = 50 \cdot 251 - 47 \cdot 267 \\ &= 50(1853 - 6 \cdot 267) - 47 \cdot 267 = 50 \cdot 1853 - 347 \cdot 267 \\ &= 50 \cdot 1853 - 347(3973 - 2 \cdot 1853) = \boxed{447 \cdot 75 - 29 \cdot 1156}. \end{aligned}$$

Esercizio 3. Dire se le seguenti equazioni lineari in 2 variabili ammettono soluzioni in $\mathbb{Z} \times \mathbb{Z}$:

$$8X - 11Y = 6, \quad 15X - 6Y = 42, \quad 9X - 12Y = 22, \quad 28X + 49Y = 91.$$

Soluzione: L'equazione $aX + bY = n$ è risolubile in $\mathbb{Z} \times \mathbb{Z}$ esattamente quando n è un multiplo di MCD(a, b). Quindi:

1. $8X - 11Y = 6$ è risolubile perché MCD$(8, -11) = 1 \mid 6$.
2. $15X - 6Y = 42$ è risolubile perché MCD$(15, -6) = 3 \mid 42$.
3. $9X - 12Y = 22$ non è risolubile perché MCD$(9, -12) = 3$ non divide 6.

4. $28X + 49Y$ è risolubile perché $\text{MCD}(28, 49) = 7 \mid 91$.

Esercizio 4. Convertire in base 10 i seguenti numeri scritti nelle basi indicate.

$11001_{[2]},\ 20110_{[3]},\ 13203_{[4]},\ 14403_{[5]},\ 25034_{[6]},\ 57704_{[8]},\ 1BA8_{[12]},\ E1C45_{[16]}$.

Soluzione:

1. $11001_{[2]} = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 = 25$.
2. $20110_{[3]} = 0 + 1 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 = 174$.
3. $13203_{[4]} = 3 + 0 \cdot 4 + 2 \cdot 4^2 + 3 \cdot 4^3 + 1 \cdot 4^4 = 467$.
4. $14403_{[5]} = 3 + 0 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4 = 1228$.
5. $25034_{[6]} = 4 + 3 \cdot 6 + 0 \cdot 6^2 + 5 \cdot 6^3 + 2 \cdot 6^4 = 3694$.
6. $57704_{[8]} = 4 + 0 \cdot 8 + 7 \cdot 8^2 + 7 \cdot 8^3 + 5 \cdot 8^4 = 24916$.
7. $1BA8_{[12]} = 8 + 10 \cdot 12 + 11 \cdot 12^2 + 1 \cdot 12^3 = 3440$.
8. $E1C45_{[16]} = 5 + 4 \cdot 16 + 12 \cdot 16^2 + 1 \cdot 16^3 + 14 \cdot 16^4 = 924741$.

Esercizio 5. Convertire nelle basi b indicate di volta in volta i seguenti numeri scritti in base 10.

1. Base 2: 570, 2095, 11003.
2. Base 3: 198, 1532, 10707.
3. Base 4: 221, 3037, 17627.
4. Base 8: 617, 4038, 21639.
5. Base 12: 455, 6169, 37093.
6. Base 16: 331, 4773, 35916.

Soluzione: Mostriamo la conversione di un numero per ogni base.

1. $2095 = 100000101111_{[2]}$.
2. $198 = 21100_{[3]}$.
3. $221 = 3131_{[4]}$.
4. $21639 = 52207_{[8]}$.
5. $37093 = 19571_{[12]}$.
6. $4773 = 12A5_{[16]}$.

Esercizio 6. Trovare la fattorizzazione come prodotto di primi dei seguenti numeri interi:

$$224, \quad 1584, \quad 6125, \quad 17901, \quad 37422, \quad 69629, \quad 81191.$$

Soluzione:

1. $224 = 2^5 \cdot 7$.
2. $1584 = 2^4 \cdot 3^2 \cdot 11$.
3. $6125 = 5^3 \cdot 7^2$.
4. $17901 = 3^4 \cdot 13 \cdot 17$.
5. $37422 = 2 \cdot 3^5 \cdot 7 \cdot 11$.
6. $69629 = 7^4 \cdot 29$.
7. $81191 = 11^3 \cdot 61$.

CdS Informatica – Torino
Corso di Matematica Discreta

Esercizi dal Libro di Testo–Soluzioni
Capitolo 5

Esercizio 1. Siano date le seguenti permutazioni in $\mathcal{S}_7$:

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

Calcolare σ^2, $\sigma\tau$, $\tau\sigma$, τ^2, $\sigma\tau\sigma$, $\tau\sigma\tau$.

Soluzione: Riportiamo il risultato solo per alcune delle composizioni richieste:

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

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

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

Esercizio 2. Determinare la decomposizione in cicli disgiunti delle seguenti permutazioni in $\mathcal{S}_8$:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 5 & 7 & 2 & 6 & 4 & 1 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 2 & 8 & 3 & 5 & 1 & 7 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 7 & 1 & 8 & 4 & 6 \end{pmatrix} \quad \delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 7 & 8 & 2 & 5 & 1 & 4 \end{pmatrix}$$

Soluzione:

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

$$\gamma = (1\ 5)(2\ 3)(4\ 7)(6\ 8), \qquad \delta = (1\ 3\ 7)(2\ 6\ 5)(4\ 8).$$

Esercizio 3. Per ciascuna coppia σ, τ di permutazioni in $\mathcal{S}_n$ data nei punti seguenti, calcolare la decomposizione in cicli disgiunti il tipo e la parità di σ, τ, $\sigma\tau$, $\tau\sigma$.

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

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

Soluzione: Risolviamo esplicitamente solo i primi 2 esercizi

1. Si ha
$$\sigma = (1\ 5\ 2\ 4\ 3), \qquad \tau = (1\ 3\ 5\ 2)$$
e allora σ è un ciclo di lunghezza 5, dunque una permutazione pari e τ è un ciclo di lunghezza 4 dunque una permutazione dispari. Abbiamo poi
$$\sigma\tau = (2\ 5\ 4\ 3), \qquad \tau\sigma = (1\ 2\ 4\ 5)$$
e allora $\sigma\tau$ e $\sigma\tau$ sono entrambe cicli di lunghezza 4 quindi permutazioni dispari.

2. Si ha
$$\sigma = (1\ 6\ 5\ 3)(2\ 4), \qquad \tau = (1\ 5\ 2\ 4\ 6)$$
e allora σ ha tipo $(4, 2)$ dunque una permutazione pari e τ è un ciclo di lunghezza 5 dunque una permutazione pari. Abbiamo poi
$$\sigma\tau = (1\ 3)(4\ 5), \qquad \tau\sigma = (2\ 6)(3\ 5)$$
e allora $\sigma\tau$ e $\sigma\tau$ hanno entrambe tipo $(2, 2)$ quindi permutazioni pari.

Esercizio 4. Siano π e σ permutazioni in $\mathcal{S}_n$.

1. Dimostrare che le permutazioni π e π^{-1} hanno la stessa parità.
2. Dimostrare che π, $\sigma \circ \pi \circ \sigma$, $\sigma \circ \pi \circ \sigma^{-1}$ hanno la stessa parità.

Soluzione:

1. Sia
$$\pi = s_1 \circ \cdots \circ s_k$$
una scrittura di π come composizione di scambi. Poiché per ogni scambio s si ha $s^{-1} = s$ si ha dalla scrittura precedente che
$$\pi^{-1} = (s_1 \circ \cdots \circ s_k)^{-1} = s_k^{-1} \circ \cdots s_1^{-1} = s_k \circ \cdots \circ s_1.$$
Quindi π e π^{-1} si scrivono utilizzando lo stesso numero di scambi e quindi hanno la stessa parità.

2. Siano
$$\pi = s_1 \circ \cdots \circ s_k, \qquad \sigma = t_1 \circ \cdots \circ s_k,$$
scritture di π e σ come composizione di scambi. Ragionando come nel punto precedente abbiamo
$$\sigma \circ \pi \circ \sigma = t_1 \circ \cdots \circ t_\ell \circ s_1 \circ \cdots \circ s_k \circ t_1 \circ \cdots \circ t_\ell$$
e
$$\sigma \circ \pi \circ \sigma^{-1} = t_1 \circ \cdots \circ t_\ell \circ s_1 \circ \cdots \circ s_k \circ t_\ell \circ \cdots \circ t_1.$$
Quindi $\sigma \circ \pi \circ \sigma$ e $\sigma \circ \pi \circ \sigma^{-1}$ ammettono entrambe una scrittura come composizione di $k + 2\ell$ scambi e quindi basta osservare che i numeri k e $k + 2\ell$ sono entrambi pari o entrambi dispari.

Esercizio 5. Determinare la parità ed il periodo di una permutazione in $\mathcal{S}_n$ di tipo assegnato come segue:

1. $n = 9$: tipo $(2, 3, 4)$, tipo $(3, 3, 3)$.
2. $n = 10$: tipo $(3, 7)$, tipo $(2, 2, 2, 3)$.
3. $n = 14$: tipo $(3, 11)$, tipo $(2, 4, 7)$, tipo $(4, 4, 6)$.
4. $n = 20$: tipo $(3, 5, 6, 6)$, tipo $(8, 12)$, tipo $(2, 2, 2, 2, 2, 2, 3, 4)$.

Soluzione: risolviamo esplicitamente solo alcuni degli esempi richiesti

1. $n = 9$ tipo $(2, 3, 4)$. Parità $D \cdot P \cdot D = P$, periodo $\text{mcm}(2, 3, 4) = 12$.
3. $n = 14$: tipo $(4, 4, 6)$. Parità $D \cdot D \cdot D = D$, periodo $\text{mcm}(4, 4, 6) = 12$.
4. $n = 20$: tipo $(3, 5, 6, 6)$. Parità $P \cdot P \cdot D\dot{D} = P$, periodo $\text{mcm}(3, 5, 6, 6) = 30$.

Esercizio 6. Calcolare il numero dei cicli

1. di lunghezza 4 in $\mathcal{S}_7$;
2. di lunghezza 6 in $\mathcal{S}_8$;
3. di lunghezza 10 in $\mathcal{S}_{13}$.

Soluzione: Questi esercizi si risolvono applicando direttamente la formula.

1. I cicli di lunghezza 4 in $\mathcal{S}_7$ sono $\frac{1}{4}D_{7,4} = \frac{1}{4}\frac{7!}{3!} = 210$.
2. I cicli di lunghezza 6 in $\mathcal{S}_8$ sono $\frac{1}{6}D_{8,6} = \frac{1}{6}\frac{8!}{2!} = 3360$.
3. I cicli di lunghezza 10 in $\mathcal{S}_{13}$ sono $\frac{1}{10}D_{13,10} = \frac{1}{10}\frac{13!}{3!} = 103783680$.

Esercizio 7. Calcolare il numero delle permutazioni

1. di tipo $(2, 3)$ in $\mathcal{S}_6$;
2. di tipo $(2, 2, 4)$ in $\mathcal{S}_8$;
3. di tipo $(3, 3)$ in $\mathcal{S}_9$;
4. di tipo $(2, 4, 5)$ in $\mathcal{S}_{12}$;
5. di tipo $(3, 3, 4, 4)$ in $\mathcal{S}_{14}$.

Soluzione: Risolviamo esplicitamente solo alcuni degli esercizi proposti.

1. Scegliamo prima un ciclo di lunghezza 2 tra 6 elementi e poi un ciclo di lunghezza 3 tra i 4 elementi rimanenti. Le scelte possibili sono

$$\frac{1}{2}\frac{6!}{4!} \cdot \frac{1}{3}\frac{4!}{1!} = 5! = 120.$$

3. Scegliamo prima un ciclo di lunghezza 3 tra 9 elementi e poi un altro ciclo di lunghezza 3 tra i 6 elementi rimanenti. Poiché pero ci sono 2 cicli da scegliere di lunghezza uguale il numero totale di scelte è

$$\frac{1}{2}\cdot\frac{1}{3}\frac{9!}{6!}\cdot\frac{1}{3}\frac{6!}{3!}=\frac{8!}{2\cdot 3!}=3360.$$

5. Scegliamo prima un ciclo di lunghezza 3 tra 14 elementi, poi un altro ciclo di lunghezza 3 tra glii 11 elementi rimanenti, poi un ciclo di lunghezza 4 tra 8 elementi rimanenti e finalmente usiamo gli ultimi 4 elementi per formare un altro ciclo di lunghezza 4. Poiché pero ci sono 2 cicli da scegliere di lunghezza uguale a 3 e altri due cicli di lunghezza uguale a 4 il numero totale di scelte è

$$\left(\frac{1}{2}\right)^2\cdot\frac{1}{3}\frac{14!}{11!}\cdot\frac{1}{3}\frac{11!}{8!}\cdot\frac{1}{4}\frac{8!}{4!}\cdot\frac{1}{4}\frac{4!}{0!}=\frac{14!}{2^2\cdot 3^2\cdot 4^2}=151351200.$$

Esercizio 8. Sia $\sigma\in\mathcal{S}_n$ una permutazione qualunque.

1. Dimostrare che se $c\in\mathcal{S}_n$ è un ciclo di lunghezza ℓ, allora anche $\sigma c\sigma^{-1}$ è un ciclo di lunghezza ℓ.
2. Dimostrare che se $\pi\in\mathcal{S}_n$ è una permutazione qualunque, allora π e $\sigma\pi\sigma^{-1}$ hanno lo stesso tipo.

Suggerimento: per il punto b) usare il punto a) insieme al fatto che una permutazione si scrive come prodotto di cicli disgiunti.

Soluzione:

1. Poniamo $c=(n_1\ n_2\ ...\ n_\ell)$. Allora vale la formula

$$\sigma c\sigma^{-1}=(\sigma(n_1)\ \sigma(n_2)\ ...\ \sigma(n_\ell))$$

che rende evidente quanto si chiede di dimostrare. Per verificare la correttezza della formula calcoliamo i due membri dell'uguaglianza per $t\in I_n$.

Se $t=\sigma(n_i)$ per un qualche $i=1,...,\ell$ si ha

$$\sigma c\sigma^{-1}(t)=\sigma c\sigma^{-1}(\sigma(n_i))=\sigma c(\sigma^{-1}\sigma(n_i))=\sigma c(n_i)=\sigma(n_{i+1})$$

a sinistra e $\sigma(n_i)$ è trasformato in $si(n_{i+1})$ anche col ciclo di destra.

Se $t=\sigma(k)$ per qualche $k\notin\{n_1,...,n_\ell\}$ si ha

$$\sigma c\sigma^{-1}(t)=\sigma c\sigma^{-1}(\sigma(k))=\sigma c(\sigma^{-1}\sigma(k))=\sigma c(k)=\sigma(k)=t$$

a sinistra e anche il ciclo di destra non sposta t. La formula è così verificata

2. Scriviamo $\pi=c_1\cdots c_k$ come prodotto di cicli disgiunti e osserviamo che

$$\sigma\pi\sigma^{-1}=\sigma c_1\cdots c_k\sigma^{-1}=\sigma c_1\sigma^{-1}\sigma c_2\sigma^{-1}\cdots\sigma c_k\sigma^{-1}.$$

Per il punto precedente l'ultima espressione è uguale a $c_1'\cdots c_k'$ dove ogni c_i' è un ciclo della stessa lunghezza di c_i. Dunque le due permutazioni π e $\sigma\pi\sigma^{-1}$ hanno lo stesso tipo.

Esercizio 9. Elencare tutti i possibili tipi che può avere una permutazione $\pi \in \mathcal{S}_7$ con la proprietà che $\pi(k) \neq k$ per ogni $k \in I_7$.

Soluzione: Se $\pi(k) = k$ il numero k non compare nei cicli disgiunti della decomposizione di π. Pertanto stiamo cercando tipi $(n_1, ..., n_k)$ tali che $n_1 + \cdots + n_k = 7$ (e non semplicemente ≤ 7). I tipi sono

$$(7), \quad (5,2), \quad (4,3), \quad (3,2,2).$$

CdS Informatica – Torino
Corso di Matematica Discreta

Esercizi dal Libro di Testo–Soluzioni
Capitolo 6

Esercizio 1. Nell'insieme $\mathbb{Q} \times \mathbb{Q}$ delle coppie di numeri razionali si consideri l'operazione $*$ definita da

$$(a, b) * (c, d) = (ac + 3bd, ad + bc).$$

1. Si verifichi che l'operazione $*$ è associativa, commutativa e ammette un elemento neutro.
2. Si verifichi che ogni elemento $(a, b) \neq (0, 0)$ ammette inverso.
3. È vero che $\mathbb{Q} \times \mathbb{Q} \setminus \{(0, 0)\}$ con l'operazione $*$ è un gruppo?

Soluzione:

1. Per verificare la proprietà associativa osserviamo che le espressioni

   $$((a,b)*(c,d))*(e,f) = (ac+3bd, ad+bc)*(e,f) = (ace+3bde+3(ad+be)f, acf+ade+bce+3bdf)$$

   e

   $$(a,b)*((c,d))*(e,f) = (a,b)*(ce+3df, de+cf) = (ace+3(ad+be)f+3bde, acf+ade+bce+3bdf)$$

   coincidono. La proprietà commutativa è chiara dall'espressione che definisce l'operazione $*$ ed infine la coppia $(1, 0)$ è neutra in quanto

   $$(a, b) * (1, 0) = (a \cdot 1 + 3b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b)$$

   per ogni $(a, b) \in \mathbb{Q} \times \mathbb{Q}$.

2. Dato $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ poniamo $\Delta = a^2 - 3b^2$. Osserviamo che se $(a, b) \neq 0$ allora $\Delta \neq 0$ (perché?). Allora si ha

   $$(a, b) * (a/\Delta, -b/\Delta) = (a^2/\Delta - 3b^2/\Delta, -ab/\Delta + ab/\Delta) = (1, 0)$$

   e dunque abbiamo determinato l'inverso di (a, b).

3. Per concludere che $\mathbb{Q} \times \mathbb{Q} \setminus \{(0, 0)\}$ è un gruppo basta verificare che è chiuso rispetto all'operazione $*$. D'altra parte se fosse

   $$(a, b) * (c, d) = (0, 0)$$

   con $(a, b) \neq (0, 0)$ moltiplicando entrambi i termini per l'inverso di (a, b) si ottiene $(c, d) = (0, 0)$ e quindi il prodotto di elementi in $\mathbb{Q} \times \mathbb{Q} \setminus \{(0, 0)\}$ è ancora in $\mathbb{Q} \times \mathbb{Q} \setminus \{(0, 0)\}$.

Esercizio 2. Siano G_1 e G_2 due gruppi. Si dimostri che il gruppo prodotto $G_1 \times G_2$ è abeliano se e soltanto se G_1 e G_2 sono entrambi abeliani.

Soluzione: Dire che

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$$

e

$$(g_1', g_2')(g_1, g_2) = (g_1' g_1, g_2' g_2)$$

sono uguali per ogni $g_1, g_1' \in G_1$ e per ogni $g_2, g_2' \in G_2$ (cioè $G_1 \times G_2$ è commutativo) se e soltanto se $g_1 g_1' = g_1' g_1$ e $g_2 g_2' = g_2' g_2$ (cioè G_1 e G_2 sono entrambi commutativi.

Esercizio 3. Nel gruppo prodotto $\mathbb{R} \times \mathbb{R}$ dire quali dei seguenti sottoinsiemi sono sottogruppi e quali no.

1. $A = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, y = 2x\}$;
2. $B = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, y = x^2\}$;
3. $C = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, y = x + 1\}$.

Soluzione:

1. Date due coppie $(a, 2a)$ e $(b, 2b)$ in A si ha

   $$(a, 2a) + (b, 2b) = (a + b, 2a + 2b) = (a + b, 2(a + b))$$

   che è ancora una coppia in A, quindi A è chiuso rispetto all'operazione. Inoltre l'elemento neutro $(0, 0) \in A$ e se $(a, 2a) \in A$ si ha $-(a, 2a) = (-a, 2(-a)) \in A$ cosicché A contiene gli opposti dei suoi elementi. Dunque A è un sottogruppo.

2. B non è chiuso rispetto all'operazione. Ad esempio $(1, 1) \in B$ perché $1^2 = 1$ ma

   $$(1, 1) + (1, 1) = (2, 2) \notin B$$

   perché $2^2 = 4 \neq 2$.

3. C non è un sottogruppo perché , per esempio, $(0, 0) \notin C$.

Esercizio 4. Nel gruppo $\mathcal{S}_7$ delle permutazioni su 7 elementi dire quali dei seguenti sottoinsiemi sono sottogruppi e quali no.

1. $A = \{\pi \in \mathcal{S}_7 \,|\, \pi(4) = 5\}$;
2. $B = \{\pi \in \mathcal{S}_7 \,|\, \pi(6) = 6\}$;
3. $C = \{\pi \in \mathcal{S}_7 \,|\, \pi^2 = \mathrm{id}\}$.

Soluzione:

1. A non è un sottogruppo. Una ragione è che $\mathrm{id} \notin A$.
2. B è un sottogruppo. Un modo di rendersene conto è notare che B è l'insieme di tutte le permutazioni dell'insieme $\{1, 2, 3, 4, 5, 7\}$ e l'insieme di tutte le permutazioni di un insieme forma un gruppo.

3. C non è un sottogruppo. Una ragione è che C non è chiuso rispetto alla composizione. Infatti gli scambi (1 2) e (2 3) sono in C ma la composizione $\pi = (1\ 2)(2\ 3) = (1\ 2\ 3) \notin C$ in quanto $\pi^2 = (1\ 3\ 2) \neq \mathrm{id}$.

Esercizio 5. Sia G un gruppo. Dire quali dei seguenti sottoinsiemi del gruppo prodotto $G \times G$ sono sottogruppi e quali no:

1. $A = \{(g, g) \in G \times G \,|\, g \in G\}$;
2. $B = \{(g, g^{-1}) \in G \times G \,|\, g \in G\}$;
3. $C = \{(g, e_G) \in G \times G \,|\, g \in G\}$.

Le risposte sarebbero le stesse se G fosse abeliano?

Soluzione:

1. A è un sottogruppo. Infatti se (g, g) e $(h, h) \in A$ si ha

$$(g, g)(h, h) = (gh, gh) \in A,$$

ovvero A è chiuso rispetto al prodotto. Inoltre $e_{G\times G} = (e_G, e_G) \in A$ e dato $(g, g) \in A$ anche $(g, g)^{-1} = (g^{-1}, g^{-1}) \in A$.

2. B non è un sottogruppo. Una ragione è che B non è chiuso rispetto al prodotto. Infatti se (g, g^{-1}) e $(h, h^{-1}) \in B$ non è detto che il prodotto

$$(g, g^{-1})(h, h^{-1}) = (gh, g^{-1}h^{-1})$$

sia in B in quanto in generale $g^{-1}h^{-1} \neq (gh)^{-1}$.

3. C è un sottogruppo. Infatti se (g, e_G) e $(h, e_G) \in C$ si ha

$$(g, e_G)(h, e_G) = (gh, e_G) \in C,$$

ovvero C è chiuso rispetto al prodotto. Inoltre $e_{G\times G} = (e_G, e_G) \in C$ e dato $(g, e_G) \in C$ anche $(g, e_G)^{-1} = (g^{-1}, e_G) \in C$.

Nel caso in cui G è abeliano anche B è un sottogruppo perché in questo caso $g^{-1}h^{-1} = (gh)^{-1}$ e le altre proprietà di sottogruppo risultano verificate.

Esercizio 6. Fissiamo $k \in I_{n+1} = \{1, ..., n + 1\}$ e sia

$$H_k = \{\pi \in \mathcal{S}_{n+1} \text{ tali che } \pi(k) = k\}.$$

1. Dimostrare che H_k è un sottogruppo di $\mathcal{S}_{n+1}$ ed è isomorfo a S_n.
2. Dimostare che $\mathcal{S}_{n+1}$ possiede almeno $n + 1$ sottogruppi distinti ciascuno dei quali è isomorfo a $\mathcal{S}_n$.
3. Calcolare $H_1 \cap \cdots \cap H_{n+1}$.

Soluzione:

1. Ogni $\pi \in H_k$ può essere pensata come una permutazione dell'insieme $J_k = I_{n+1} \setminus \{k\}$. Viceversa una permutazione σ dell'insieme J_k può essere pensata come una permutazione di I_{n+1} tale che $\sigma(k) = k$, cioè come un elemento di H_k.

   Dunque H_k è l'insieme delle permutazioni dell'insieme J_k e quindi H_k è certamente un gruppo, quindi un sottogruppo di $\mathcal{S}_{n+1}$, ed è isomorfo a $\mathcal{S}_n$ perché $|J_k| = n$.

2. Dal punto precedente sappiamo che ciascun sottogruppo $H_k < \mathcal{S}_{n+1}$ è isomorfoa $\mathcal{S}_n$. Se $k \neq \ell$ dobbiamo avere $H_k \neq H_\ell$ in quanto, ad esempio H_ℓ contiene permutazioni π tali che $\pi(k) \neq k$.

   Dunque i sottogruppi $H_1, ..., H_{n+1}$ sono i sottogruppi cercati.

3. Sia $\pi \in H_1 \cap \cdots \cap H_{n+1}$. Allora per ogni $k = 1, ..., n+1$ si ha $\pi \in H_k$, ovvero $\pi(k) = k$ e quindi $\pi = \mathrm{id}$. Dunque

$$H_1 \cap \cdots \cap H_{n+1} = \{\mathrm{id}\}.$$

Esercizio 7. Dimostrare che in un gruppo G l'elemento neutro e_G è l'unico elemento x tale che $x^2 = x$.

Soluzione: Applicando la legge di cancellazione a

$$x^2 = x * x = x$$

si ha immediatamente $x = e_G$.

Esercizio 8. Siano G_1 e G_2 due gruppi e siano H_1 un sottogruppo di G_1 e H_2 un sottogruppo di G_2. Dimostrare che $H_1 \times H_2$ è un sottogruppo di $G_1 \times G_2$.

Soluzione: Se (h_1, h_2) e (h_1', h_2') sono due elementi in $H_1 \times H_2$ si ha

$$(h_1, h_2) * (h_1', h_2') = (h_1 h_1', h_2 h_2') \in H_1 \times H_2$$

perché $H_1 < G_1$ e $H_2 < G_2$. Dunque $H_1 \times H_2$ è chiuso rispetto al prodotto componente per componente.

Indicato con e_i, $i = 1, 2$, l'elemento neutro di G_i si ha $(e_1, e_2) \in H_1 \times H_2$ in quanto $e_i \in H_i < G_i$. D'altra parte è chiaro che (e_1, e_2) è l'elemento neutro di $G_1 \times G_2$.

Infine dato $(h_1, h_2) \in H_1 \times H_2$ si verifica subito che $(h_1, h_2)^{-1} = (h_1^{-1}, h_2^{-1}) \in H_1 \times H_2$ di nuovo perché $H_1 < G_1$ e $H_2 < G_2$ contengono gli inversi dei loro elementi.

Questo termina la verifica che $H_1 \times H_2$ è un sottogruppo.

Esercizio 9. Sia $\{H_i\}_{i \in \mathcal{I}}$ una famiglia arbitraria di sottogruppi del gruppo G. Si dimostri che $\bigcap_{i \in \mathcal{I}} H_i$ è un sottogruppo di G.

Soluzione: La dimostrazione procede identica alla dimostrazione della proprietà analoga per l'intersezione di due gruppi una volta che si osserva che dire $h, h', ... \in \bigcap_{i \in \mathcal{I}} H_i$ equivale a dire che $h, h', ... \in H_i$ per ogni $i \in \mathcal{I}$.

Esercizio 11. Calcolare esplicitamente le partizioni di $\mathcal{S}_4$ nei laterali destri e sinistri del sottogruppo $H = \langle(1\ 3\ 2\ 4)\rangle$.

Soluzione: Elenchiamo solo i laterali sinistri, per i destri la procedura sar analoga. Procediamo come segue: iniziamo elencando gli elementi di H (che è esso stesso il laterale sinistro $H\mathrm{id}$) e nei passi successivi elenchiamo gli elementi in Hg per un g arbitrario non elencato fino a quel punto calcolando esplicitamente i prodotti hg al variare di $h \in H$.

- $H = \{\mathrm{id}, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\}$;
- $H(1\ 2) = \{(1\ 2), (1\ 4)(2\ 3), (3\ 4), (1\ 3)(2\ 4)\}$;
- $H(1\ 3) = \{(1\ 3), (1\ 2\ 4), (1\ 4\ 3\ 2), (2\ 3\ 4)\}$;
- $H(1\ 4) = \{(1\ 4), (2\ 4\ 3), (1\ 3\ 4\ 2), (1\ 2\ 3)\}$;
- $H(2\ 3) = \{(2\ 3), (1\ 3\ 4), (1\ 2\ 4\ 3), (1\ 4\ 2)\}$;
- $H(2\ 4) = \{(2\ 4), (1\ 3\ 2), (1\ 2\ 3\ 4), (1\ 4\ 3)\}$.

Esercizio 12. Dimostrare che per ogni $n \geq 2$ la funzione $\phi : \mathbb{R} \to \mathbb{R}$ definita da $\phi(x) = x^n$ non è un omomorfismo.

Soluzione: Se fosse un omomorfismo dovrebbe valere $\phi(x + y) = \phi(x) + \phi(y)$ per ogni $x, y \in R$. Ma basta prendere $x = y = 1$ per avere

$$\phi(1 + 1) = 2^n \neq 2 = 1^n + 1^n = \phi(1) + \phi(1)$$

se $n \geq 2$.

Esercizio 13. Dimostrare che per ogni $n \geq 2$ la funzione $\phi : \mathbb{R}^\times \to \mathbb{R}^\times$ definita da $\phi(x) = x^n$ è un omomorfismo e se ne calcoli il nucleo.

Soluzione: Poiché la moltiplicazione in $\mathbb{R}$ è commutativa si ha

$$\phi(xy) = (xy)^n = x^n y^n = \phi(x)\phi(y)$$

per ogni x, $y \in \mathbb{R}^\times$. Dunque ϕ è un omomorfismo e

$$\ker(\phi) = \{x \in \mathbb{R}^\times \text{ tali che } \phi(x) = x^n = 1\} = \begin{cases} \{1, -1\} & \text{se } n \text{ è pari,} \\ \{1\} & \text{se } n \text{ è dispari.} \end{cases}$$

Esercizio 14. Dire quali delle seguenti funzioni $f : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ sono omomorfismi e quali no. Nei casi affermativi discuterne l'iniettività e la suriettività.

1. $f((m, n)) = m + n - 1$;
2. $f((m, n)) = m^2 - n^2$;
3. $f((m, n)) = 2m - 3n$.

Soluzione: Diamo solo le risposte senza giustificazione.

1. Non è un omomorfismo.
2. Non è un omomorfismo.
3. È un omomomorfismo suriettivo ma non iniettivo.

Esercizio 15. Dire quali delle seguenti funzioni $f : \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ sono omomorfismi e quali no. Nei casi affermativi discuterne l'iniettività e la suriettività.

1. $f(n) = (n-1, n+1)$;
2. $f(n) = (3n, 0)$;
3. $f(n) = (1, 5n)$;
4. $f(n) = (2n, -n)$.

Soluzione: Anche qui diamo solo le risposte senza giustificazione.

1. Non è un omomorfismo.
2. È un omomorfismo iniettivo ma non suriettivo.
3. Non è un omomorfismo.
4. È un omomomorfismo iniettivo ma non suriettivo.

Esercizio 16. Dato $x \in \mathbb{R}$, $x \neq 0$ definiamo il **segno** di x come

$$s(x) = \frac{x}{|x|} = \begin{cases} 1 & \text{se } x > 0, \\ -1 & \text{se } x < 0. \end{cases}$$

1. Dimostrare che $s : \mathbb{R}^\times \to \{1, -1\}$ è un epimorfismo.
2. Dimostrare che la funzione

$$f : \mathbb{R}^\times \longrightarrow \mathbb{R}^{>0} \times \{1, -1\}, \qquad f(x) = (|x|, s(x))$$

è un isomorfismo (ricordiamo che $\mathbb{R}^{>0}$ denota il sottogruppo del gruppo moltiplicativo di $\mathbb{R}$ dei numeri reali positivi).

Soluzione:

1. La funzione segno è sicuramente suriettiva perché vale 1 sui numeri positivi e vale -1 sui numeri negativi. Ricordando la proprietà $|xy| = |x| \cdot |y|$ del valore assoluto si ha

$$s(xy) = \frac{xy}{|xy|} = \frac{x}{|x|} \cdot \frac{y}{|y|} = s(x) \cdot s(y)$$

per ogni x, $y \in \mathbb{R}^\times$, dimostrando così che la funzione segno è un omomorfismo.

2. Il fatto che f sia un omomorfismo è anche qui una conseguenza della proprietà $|xy| = |x| \cdot |y|$ del valore assoluto (omettiamo i dettagli).

   La suriettività segue immediatamente dall'osservazione che per $r \in \mathbb{R}^{>0}$ si ha
   $$s(\pm r) = (r, \pm 1).$$
   Infine l'inisttività segue dal fatto che
   $$\ker(f) = \{r \in \mathbb{R}^{\times} \text{ tali che } |r| = 1 \text{ e } s(r) = 1\} = \{1\}.$$

Esercizio 17. Sia $(G, *)$ un gruppo. Nell'insieme G si definisca una seconda operazione $\circ$ definita da
$$x \circ y = y * x \qquad \text{per ogni } x,\, y \in G.$$

1. Dimostrare che $(G, \circ)$ è un gruppo.
2. Verificare che la funzione $\iota : (G, *) \to (G, \circ)$ definita da $\iota(g) = g^{-1}$ è un isomorfismo di gruppi.

Soluzione:

1. In $(G, \circ)$ vale la proprietà associativa in quanto
   $$(x \circ y) \circ z = (y * x) \circ z = z * (y * x) = (z * y) * x = x \circ (z * y) = z \circ (y \circ z)$$
   per ogni x, y, $z \in G$ poiché la proprietà associativa vale nel gruppo $(G, *)$.

   Inoltre si verifica subito che e_G è neutro per entrambe le operazioni e l'inverso g^{-1} per l'operazione $*$ è inverso anche per l'operazione $\circ$.
2. La funzione ι è sicuramente una biezione dell'insieme G in sè. Per vedere che è un omomorfismo osserviamo che per ogni x, $y \in G$ si ha
   $$\iota(x * y) = (x * y)^{-1} = y^{-1} * x^{-1} = x^{-1} \circ y^{-1} = \iota(x) \circ \iota(y).$$

Esercizio 18. Siano $\phi_1 : G \to H_1$ e $\phi_2 : G \to H_2$ omomorfismi di gruppi. Dimostrare che la funzione
$$\phi : G \longrightarrow H_1 \times H_2, \qquad \phi(g) = (\phi_1(g), \phi_2(g)), \forall g \in G$$
è un omomorfismo. Dire poi se le seguenti affermazioni sono vere o false.

- Se ϕ_1 e ϕ_2 sono iniettivi anche ϕ è iniettivo.
- Se ϕ_1 e ϕ_2 sono suriettivi anche ϕ è suriettivo.

Soluzione: La funzione ϕ è un omomorfismo perché
$$\phi(xy) = (\phi_1(xy), \phi_2(xy)) = (\phi_1(x)\phi_1(y), \phi_2(x)\phi_2(y)) = \phi(x)\phi(y)$$
per ogni x, $y \in G$.

- Se ϕ_1 e ϕ_2 sono iniettivi anche ϕ lo è perché

  $\ker(\phi) = \{g \in G \text{ tali che } phi_1(g) = e_{H_1} \text{ e } phi_2(g) = e_{H_2}\} = \ker(\phi_1) \cap \ker(\phi_2) = \{e_G\}$

- Anche se ϕ_1 e ϕ_2 sono suriettivi non è detto che ϕ lo sia. Ad esempio se $H_1 = H_2 = G$ e $\phi_1 = \phi_2 = \mathrm{id}_G$ l'immagine è il sottoinsieme

  $$\Delta = \{(g, g) \in G \times G \text{ tali che } g \in G\}$$

  che è un sottoinsieme proprio di $G \times G$.

Esercizio 19. Elencare gli elementi di periodo finito nei gruppi seguenti.

1. $\mathbb{R} \times \{\pm 1\}$;
2. $\mathbb{R}^\times \times \mathbb{R}^\times$;
3. $\mathbb{R}^\times \times \mathcal{S}_3$.

Soluzione:

1. $\{0\} \times \{\pm 1\}$.
2. $\{\pm 1\} \times \{\pm 1\}$.
3. $\{\pm 1\} \times \mathcal{S}_3$.

Esercizio 20. Sia $q = \frac{a}{b} \in \mathbb{Q}$ un numero razionale non nullo.

1. Dimostrare che tutti i multipli non nulli di q hanno come denominatore b o un suo divisore.
2. Concludere che il gruppo $(\mathbb{Q}, +)$ non è ciclico.

Soluzione:

1. Un multiplo non nullo del numero razionale $q\frac{a}{b}$ è della forma $nq = n\frac{a}{b}$ con $n \in \mathbb{Z}$, $n \neq 0$. Ma allora le uniche semplificazioni possono aversi se n e b hanno divisori interi comuni. In tal caso il denominatore b è sostituito da un divisore.
2. Sia $q = \frac{a}{b}$ e sia p un numero primo che non divide b. Allora per quanto detto nel punto precedente la frazione $\frac{1}{p}$ non è un multiplo intero di q, cioè $\frac{1}{p} \notin \langle q \rangle$.

   Poiché questo è vero qualunque sia q, il gruppo $\mathbb{Q}$ non può essere ciclico.

Esercizio 21. *Sia G un gruppo di ordine n. Dimostrare che esistono esattamente n omomorfismi $\phi : \mathbb{Z} \to G$.*

Soluzione: Poiché $\mathbb{Z}$ è ciclico un omomorfismo $f : \mathbb{Z} \to G$ è completamente determinato dall'immagine $f(1) \in G$.

Viceversa, dato un elemento $g \in G$ possiamo definire un omomorfismo $f : \mathbb{Z} \to G$ ponendo

$$f(n) = g^n, \qquad \forall n \in \mathbb{Z}.$$

Dunque ci sono tanti omomorfismi $\mathbb{Z} \to G$ quanti sono gli elementi di G.

CdS Informatica – Torino
Corso di Matematica Discreta

Esercizi dal Libro di Testo–Soluzioni
Capitolo 7

Esercizio 1. Dire quali delle seguenti funzioni sono ben definite e tra queste quali sono omomorfismi e calcolarne il nucleo.

1. $f_1 : \mathbb{Z}_8 \to \mathbb{Z}_{12}$ data da $f_1([k]_8) = [3k]_{12}$.
2. $f_2 : \mathbb{Z}_{14} \to \mathbb{Z}_{15}$ data da $f_2([k]_{15}) = [5k]_{15}$.
3. $f_3 : \mathbb{Z}_{30} \to \mathbb{Z}_{36}$ data da $f_3([k]_{30}) = [k^2]_{36}$.
4. $f_4 : \mathbb{Z}_{12} \to \mathbb{Z}_{16}$ data da $f_4([k]_{12}) = [4k]_{16}$.
5. $f_5 : \mathbb{Z}_{21} \to \mathbb{Z}_{42}$ data da $f_5([k]_{21}) = [2k+3]_{42}$.
6. $f_6 : \mathbb{Z}_{14} \to \mathbb{Z}_{10}$ data da $f_6([k]_{14}) = [3k-1]_{10}$.
7. $f_7 : \mathbb{Z}_9 \to \mathbb{Z}_{54}$ data da $f_7([k]_9) = [2k^3]_{54}$.

Soluzione:

1. Siccome $[k]_8 = [\ell]_8$ significa che $k-\ell = 8r$ con $r \in \mathbb{Z}$ (8 divide $k-\ell$), allora $3k - 3\ell = 24r = 12(2r)$, cioè $[3k]_{12} = [3\ell]_{12}$ e quindi f_1 è ben definita.

   Poiché $f_1([k]_8 + [\ell]_8) = f_1([k+\ell]_8) = [3(k+\ell)]_{12} = [3k]_{12} + [3\ell]_{12} = f_1([3k]_8) + f_1([3\ell]_8)$ la funzione f_1 è un omomorfismo e

   $$\ker(f_1) = \{[k]_8 \text{ tali che } [3k]_{12} = [0]_{12}\} = \{[0]_8, [4]_8\}.$$

2. Si ha, ad esempio, $[1]_{14} = [15]_{14}$ ma $[5 \cdot 1]_{15} = [5]_{15} \neq [5 \cdot 15]_{15} = [0]_{15}$ e quindi f_2 non è ben definita.

3. Si ha, ad esempio, $[10]_{30} = [40]_{30}$ ma $[10^2]_{36} = [100]_{36} \neq [40^2]_{36} = [1600]_{36}$ e quindi f_3 non è ben definita.

4. Siccome $[k]_{12} = [\ell]_{12}$ significa che $k - \ell = 12r$ con $r \in \mathbb{Z}$ (12 divide $k-\ell$), allora $4k - 4\ell = 48r = 16(3r)$, cioè $[4k]_{16} = [4\ell]_{16}$ e quindi f_4 è ben definita.

   Poiché $f_4([k]_{12} + [\ell]_{12}) = f_1([k+\ell]_{12}) = [4(k+\ell)]_{16} = [4k]_{16} + [4\ell]_{16} = f_4([4k]_{12}) + f_4([4\ell]_{16})$ la funzione f_4 è un omomorfismo e

   $$\ker(f_4) = \{[k]_{12} \text{ tali che } [4k]_{16} = [0]_{16}\} = \{[0]_{12}, [4]_{12}, [8]_{12}\}.$$

5. Siccome $[k]_{21} = [\ell]_{21}$ significa che $k - \ell = 21r$ con $r \in \mathbb{Z}$ (21 divide $k-\ell$), allora $(2k+3) - (2\ell+3) = 42r$, cioè $[2k+3]_{42} = [2\ell+3]_{42}$ e quindi f_5 è ben definita.

   Però f_5 non è un omomorfismo in quanto, ad esempio, $f_5([0]_{21}) = [3]_{42} \neq [0]_{42}$.

6. Si ha, ad esempio, $[0]_{14} = [14]_{14}$ ma $[3 \cdot 0 - 1]_{10} = [-1]_{10} \neq [3 \cdot 14 - 1]_{10} = [51]_{10}$ e quindi f_6 non è ben definita.

7. Siccome $[k]_9 = [\ell]_9$ significa che $k - \ell = 9r$ con $r \in \mathbb{Z}$ (9 divide $k - \ell$), allora da $k = \ell + 9r$ otteniamo

$$2k^3 = 2(\ell + 9r)^3 = 2\ell^3 + 2 \cdot 3^3 \ell^2 r + 2 \cdot 3^5 \ell r^2 + 2 \cdot 3^6 r^3.$$

Da questa espressione risulta che $54 = 2 \cdot 3^3$ divide $2k^3 - 2\ell^3$ e quindi f_7 è ben definita.

Però f_7 non è un omomorfismo. Ad esempio $[3]_9 = [1]_9 + [2]_9$ e $f_7([3]_9) = [2 \cdot 3^3]_{54} = [0]_{54}$ mentre $f_7([1]_9) + f_7([2]_9) = [2 \cdot 1^3]_{54} + [2 \cdot 2^3]_{54} = [2]_{54} + [16]_{54} = [18]_{54}$.

Esercizio 2. Verificare che le seguenti funzioni sono omomorfismi ben definiti e calcolarne il nucleo.

1. $f_1 : \mathbb{Z}_{10} \to \mathbb{Z}_6$ data da $f_1([k]_{10}) = [3k]_6$.
2. $f_2 : \mathbb{Z}_{42} \to \mathbb{Z}_{36}$ data da $f_2([k]_{42}) = [6k]_{36}$.
3. $f_3 : \mathbb{Z}_{80} \to \mathbb{Z}_{50}$ data da $f_3([k]_{80}) = [5k]_{50}$.

Soluzione:

1. Siccome $[k]_{10} = [\ell]_{10}$ significa che $k - \ell = 10r$ con $r \in \mathbb{Z}$ (10 divide $k - \ell$), allora $3k - 3\ell = 30r = 6(5r)$, cioè $[3k]_6 = [3\ell]_6$ e quindi f_1 è ben definita.

   Poiché $f_1([k]_{10} + [\ell]_{10}) = f_1([k + \ell]_{10}) = [3(k + \ell)]_6 = [3k]_6 + [3\ell]_6 = f_1([3k]_{10}) + f_1([3\ell]_{10})$ la funzione f_1 è un omomorfismo e

$$\ker(f_1) = \{[k]_{10} \text{ tali che } [3k]_6 = [0]_6\} = \{[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}.$$

2. Siccome $[k]_{42} = [\ell]_{42}$ significa che $k - \ell = 42r$ con $r \in \mathbb{Z}$ (42 divide $k - \ell$), allora $6k - 6\ell = 6 \cdot 42r = 36(7r)$, cioè $[6k]_{36} = [6\ell]_{36}$ e quindi f_2 è ben definita.

   Poiché $f_2([k]_{42} + [\ell]_{42}) = f_2([k + \ell]_{42}) = [6(k + \ell)]_{36} = [6k]_{36} + [6\ell]_{36} = f_2([6k]_{36}) + f_2([6\ell]_{36})$ la funzione f_2 è un omomorfismo e

$$\ker(f_2) = \{[k]_{42} \text{ tali che } [6k]_{36} = [0]_{36}\} = \{[6m]_{42}\}_{m=0,1,\ldots,6}.$$

3. Siccome $[k]_{80} = [\ell]_{80}$ significa che $k - \ell = 80r$ con $r \in \mathbb{Z}$ (80 divide $k - \ell$), allora $5k - 5\ell = 5 \cdot 80r = 50(8r)$, cioè $[5k]_{50} = [5\ell]_{50}$ e quindi f_3 è ben definita.

   Poiché $f_3([k]_{80} + [\ell]_{80}) = f_3([k + \ell]_{80}) = [5(k + \ell)]_{50} = [5k]_{50} + [5\ell]_{50} = f_3([5k]_{50}) + f_3([5\ell]_{50})$ la funzione f_3 è un omomorfismo e

$$\ker(f_3) = \{[k]_{80} \text{ tali che } [5k]_{50} = [0]_{50}\} = \{[10m]_{42}\}_{m=0,1,\ldots,7}.$$

Esercizio 3. Dire quali delle seguenti funzioni sono ben definite e tra queste quali sono gli omeomorfismi.

1. $f : \mathbb{Z}_{10} \to \mathcal{S}_4$ data da $f([k]_{10}) = \pi^{2k}$ dove $\pi = (1\ 3\ 4\ 2)$.
2. $f : \mathbb{Z}_{16} \to \mathcal{S}_5$ data da $f([k]_{16}) = \pi^{5k}$ dove $\pi = (1\ 2\ 4)(3\ 5)$.
3. $f : \mathbb{Z}_{20} \to \mathcal{S}_7$ data da $f([k]_{20}) = \pi^{9k}$ dove $\pi = (1\ 2\ 7)(3\ 6\ 5\ 4)$.
4. $f : \mathbb{Z}_{22} \to \mathcal{S}_8$ data da $f([k]_{10}) = \pi^{3k}$ dove $\pi = (1\ 7)(2\ 4\ 6\ 3\ 8)$.

Soluzione:

1. L'uguaglianza di classi $[k]_{10} = [\ell]_{10}$ significa che $k = \ell + 10r$ con $r \in \mathbb{Z}$ (10 divide $k - \ell$). Allora $2k = 2\ell + 20r$ e l'uguaglianza $\pi^{2k} = \pi^{2\ell}\pi^{20r}$ risulta vera perché π ha periodo 4 e 4 divide 20. Dunque f è ben definita ed è un omomorfismo per la legge delle potenze.
2. L'uguaglianza di classi $[k]_{16} = [\ell]_{16}$ significa che $k = \ell + 16r$ con $r \in \mathbb{Z}$ (16 divide $k - \ell$). Allora $5k = 5\ell + 80r$ e l'uguaglianza $\pi^{5k} = \pi^{5\ell}\pi^{80r}$ risulta falsa in generale perché π ha periodo 6 e 6 non divide $80r$ (ad esempio se $r = 1$). Dunque f non è ben definita.
3. L'uguaglianza di classi $[k]_{20} = [\ell]_{20}$ significa che $k = \ell + 20r$ con $r \in \mathbb{Z}$ (20 divide $k - \ell$). Allora $9k = 9\ell + 180r$ e l'uguaglianza $\pi^{9k} = \pi^{9\ell}\pi^{180r}$ risulta vera perché π ha periodo 12 e 12 divide 180. Dunque f è ben definita ed è un omomorfismo per la legge delle potenze.
4. L'uguaglianza di classi $[k]_{22} = [\ell]_{22}$ significa che $k = \ell + 22r$ con $r \in \mathbb{Z}$ (22 divide $k - \ell$). Allora $3k = 3\ell + 66r$ e l'uguaglianza $\pi^{3k} = \pi^{3\ell}\pi^{66r}$ risulta falsa in generale perché π ha periodo 10 e 10 non divide $66r$ (ad esempio se $r = 1$). Dunque f non è ben definita.

Esercizio 4. Delle seguenti classi resto dire quali sono invertibili e di quelle invertibili calcolare l'inversa.

$[4]_9$	$[6]_9$	$[7]_{10}$	$[8]_{10}$	$[2]_{11}$	$[7]_{12}$	$[6]_{14}$
$[7]_{15}$	$[9]_{15}$	$[9]_{20}$	$[9]_{21}$	$[7]_{22}$	$[10]_{23}$	$[5]_{24}$
$[15]_{24}$	$[9]_{29}$	$[18]_{30}$	$[19]_{30}$	$[11]_{32}$	$[3]_{34}$	$[10]_{36}$
$[13]_{36}$	$[23]_{40}$	$[35]_{42}$	$[17]_{55}$	$[39]_{80}$	$[10]_{95}$	$[71]_{100}$

Soluzione: Le classi $[6]_9$, $[8]_{10}$, $[6]_{14}$, $[9]_{15}$, $[9]_{21}$, $[15]_{24}$, $[18]_{30}$, $[10]_{36}$, $[35]_{42}$, $[10]_{95}$ sono non invertibili perché tutte della forma $[k]_N$ con $\mathrm{MCD}(k, N) > 1$. Le altre sono tutte invertibili. Di qualcuna ne mostriamo esplicitamente l'inversa omettendo però i dettagli del calcolo dell'identità di Bezout.

- $[7]_{10}^{-1} = [3]_{10}$ dall'identità $3 \cdot 7 - 2 \cdot 10 = 1$.
- $[9]_{20}^{-1} = [9]_{20}$ dall'identità $9 \cdot 9 - 4 \cdot 20 = 1$.
- $[10]_{23}^{-1} = [7]_{23}$ dall'identità $7 \cdot 10 - 3 \cdot 23 = 1$.
- $[9]_{29}^{-1} = [13]_{29}$ dall'identità $13 \cdot 9 - 4 \cdot 29 = 1$.

- $[3]_{34}^{-1} = [-11]_{34} = [23]_{34}$ dall'identità $(-11) \cdot 3 + 1 \cdot 34 = 1$.
- $[71]_{100}^{-1} = [31]_{100}$ dall'identità $9 \cdot 71 - 22 \cdot 100 = 1$.

Esercizio 5. Dimostrare che assegnato $n \in \mathbb{Z}$ con $n \neq 0, \pm 1$ è possibile trovare un $N > 0$ tale che $[n]_N$ è un divisore dello zero in $\mathbb{Z}_N$.

Soluzione: Basta prendere come N un qualunque multiplo positivo $N = kn$, con $k \neq 0, \pm 1$. Ad esempio, se $n \geq 2$ si ha

$$[2]_{2n} \cdot [n]_{2n} = [2n]_{2n} = [0]_{2n}$$

ma $[2]_{2n}$ e $[n]_{2n}$ sono entrambe diverse da $[0]_{2n}$.

Esercizio 6. Dimostrare che i seguenti gruppi moltiplicativi sono ciclici trovando un generatore esplicito:

$$\mathbb{Z}_7^\times, \qquad \mathbb{Z}_9^\times, \qquad \mathbb{Z}_{11}^\times, \qquad \mathbb{Z}_{17}^\times.$$

Soluzione: Di ciascun esempio forniamo un generatore omettendo però la verifica:

$$\mathbb{Z}_7^\times = \langle \bar{3} \rangle, \qquad \mathbb{Z}_9^\times = \langle \bar{2} \rangle, \qquad \mathbb{Z}_{11}^\times = \langle \bar{2} \rangle, \qquad \mathbb{Z}_{17}^\times = \langle \bar{3} \rangle.$$

Esercizio 7. Dimostrare che i seguenti gruppi moltiplicativi non sono ciclici:

$$\mathbb{Z}_8^\times, \qquad \mathbb{Z}_{15}^\times, \qquad \mathbb{Z}_{24}^\times.$$

Soluzione:

1. $\mathbb{Z}_8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ ha ordine 4. Però
$$\bar{3}^2 = \bar{5}^2 = \bar{7}^2 = \bar{1}$$
e quindi non ci sono classi di periodo 4.
2. $\mathbb{Z}_{15}^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$ ha ordine 8. Però
$$\bar{2}^4 = \bar{7}^4 = \bar{8}^4 = \bar{13}^4 = \bar{1} \quad \text{e} \quad \bar{4}^2 = \bar{11}^2 = \bar{14}^2 = \bar{1}$$
e quindi non ci sono classi di periodo 8.
3. $\mathbb{Z}_{24}^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}, \bar{19}, \bar{23}\}$ ha ordine 8. Però si ha
$$\bar{k}^2 = \bar{1}, \qquad \forall \bar{k} \in \mathbb{Z}_{24}^\times$$
e quindi non ci sono elementi di periodo 8.

Esercizio 8. Calcolare il valore $\varphi(n)$ della funzione di Eulero per i seguenti valori di n:

124, 245, 300, 320, 408, 667, 820, 837, 1350, 1375, 3969.

Soluzione: Calcoliamo qualche esempio.

- $\varphi(320) = \varphi(2^6 \cdot 5) = \varphi(2^6) \cdot \varphi(5) = 2^5(2-1) \cdot (5-1) = 32 \cdot 4 = 128$.
- $\varphi(667) = \varphi(23 \cdot 29) = \varphi(23) \cdot \varphi(29) = (23-1)(29-1) = 616$.
- $\varphi(837) = \varphi(3^3 \cdot 31) = \varphi(3^3) \cdot \varphi(31) = 3^2(3-1) \cdot (31-1) = 18 \cdot 30 = 540$.
- $\varphi(1350) = \varphi(2 \cdot 3^3 \cdot 5^2) = \varphi(2) \cdot \varphi(3^3) \cdot \varphi(5^2) = (2-1) \cdot 3^2(3-1) \cdot 5(5-1) = 1 \cdot 18 \cdot 20 = 360$.

Esercizio 9. Dire quali dei seguenti gruppi della forma $\mathbb{Z}_m \times \mathbb{Z}_n$ è ciclico e per quelli che lo sono trovare almeno un generatore diverso da $([1]_m, [1]_n)$:

$$\mathbb{Z}_6 \times \mathbb{Z}_{11}, \quad \mathbb{Z}_8 \times \mathbb{Z}_{15}, \quad \mathbb{Z}_{12} \times \mathbb{Z}_{35}, \quad \mathbb{Z}_{14} \times \mathbb{Z}_{35}, \quad \mathbb{Z}_{30} \times \mathbb{Z}_{105}, \quad \mathbb{Z}_{49} \times \mathbb{Z}_{99}.$$

Soluzione: Elenchiamo solo quelli che sono ciclici indicando un generatore come richiesto.

- $\mathbb{Z}_6 \times \mathbb{Z}_{11} = \langle([1]_6, [2]_{11})\rangle$.
- $\mathbb{Z}_8 \times \mathbb{Z}_{15} = \langle([3]_8, [2]_{15})\rangle$.
- $\mathbb{Z}_{12} \times \mathbb{Z}_{35} = \langle([5]_{12}, [1]_{35})\rangle$.
- $\mathbb{Z}_{49} \times \mathbb{Z}_{99} = \langle([3]_{49}, [7]_{99})\rangle$.

Esercizio 10. Dire quali delle seguenti congruenze lineari sono risolvibili e in caso in cui lo siano elencare tutte le soluzioni.

$3X \equiv 5 \bmod 10$	$6X \equiv 7 \bmod 12$	$8X \equiv 6 \bmod 14$	$2X \equiv 10 \bmod 15$
$3X \equiv 8 \bmod 20$	$7X \equiv 2 \bmod 21$	$10X \equiv 6 \bmod 24$	$15X \equiv 5 \bmod 25$
$6X \equiv 9 \bmod 30$	$7X \equiv 8 \bmod 40$	$9X \equiv 11 \bmod 54$	$12X \equiv 16 \bmod 64$

Soluzione: Risolviamo solo alcune congruenze in modo da esaurire la casistica.

- $6X \equiv 7 \bmod 12$. Siccome $\mathrm{MCD}(6, 12) = 6$ non divide 7 la congruenza non ha soluzioni.
- $2X \equiv 10 \bmod 15$. Siccome $\mathrm{MCD}(2, 15) = 1$ e $[2]_{15}^{-1} = [8]_{15}$ l'unica soluzione della congruenza è $X = 8 \cdot 10 = 5 \bmod 15$.
- $15X \equiv 5 \bmod 25$. Siccome $\mathrm{MCD}(15, 25) = 5$ divide 5 la congruenza assegnata equivale a $3X \equiv 1 \bmod 5$ che ha come unica soluzione $X = 2 \bmod 5$ e quindi le soluzioni dellla congruenza originale sono

$$X = 2, 7, 12, 17, 22 \bmod 25.$$

- $12X \equiv 16 \bmod 64$. Sicome $\mathrm{MCD}(12, 64) = 4$ divide 16 la congruenza assegnata equivale a $3X \equiv 4 \bmod 16$ che ha come unica soluzione $X = 11 \cdot 4 = 12 \bmod 16$ e quindi le soluzioni della congruenza originale sono

$$X = 12, 28, 44, 60 \bmod 64.$$

Esercizio 11. Dei seguenti numeri dire quali sono divisibili per 2, per 3, per 5, per 9, per 11:

372405912042, 2517090248794 74100761224335, 9113703764402.

Soluzione: Analizziamo solo il numero $N = 74100761224335$.

- La cifra finale è 5 quindi il numero è divisibile per 5 ma non per 2.
- Si ha $7+4+1+0+0+7+6+1+2+2+4+3+3+5 = 45$ che è divisibile per 3 e quindi N è divisibile per 3.
- Si ha $7-4+1-0+0-7+6-1+2-2+4-3+3-5 = 7$ che non è divisibile per 11 e quindi N non è divisibile per 11.

Esercizio 12. Determinare la cifra finale dei seguenti numeri:

$$3^{755042}, \qquad 3^{905041} + 7^{448065}, \qquad 13^{899243} - 3^{577097}, \qquad 7^{299047} - 4^{377001}.$$

Soluzione: Ricordiamo che calcolare la cifra finale di un numero vuol dire calcolare la sua classe resto modulo 10. Svolgiamo il conto in due casi. Usiamo sempre il fatto che $\varphi(10) = 4$ per applicare il teorema di Eulero

- Poiché $755042 = 188760 \cdot 4 + 2$ e per il teorema di Eulero $[3]_{10}^4 = [1]_{10}$ abbiamo $[3^{755042}]_{10} = [3]_{10}^{755042} = [3]_{10}^2 = [9]_{10}$.
- Poiché $299047 = 74761 \cdot 4 + 3$ e per il teorema di Eulero $[7]_{10}^4 = [1]_{10}$ abbiamo $[7^{299047}]_{10} = [7]_{10}^{299047} = [7]_{10}^3 = [3]_{10}$.

  Non è però possibile applicare il teorema di Eulero alle potenze di 4 ma in questo caso possiamo osservare che $[4]_{10}^2 = [6]_{10}$ e $[4]_{10}^3 = [4]_{10}$ per cui $[4]_{10}^n = [4]_{10}$ se n è dispari e $= [6]_{10}$ se n è pari. Mettendo insieme i due calcoli

$$[7^{299047} - 4^{377001}]_{10} = [7]_{10}^{299047} - [4]_{10}^{377001} = [3]_{10} - [4]_{10} = [9]_{10}.$$

Esercizio 13. Determinare le due cifre finali dei seguenti numeri

$$17^{894283}, \qquad 11^{437241} + 29^{722602}, \qquad 35^{396689}, \qquad 41^{488936} - 37^{472288}.$$

Soluzione: Ricordiamo che calcolare la cifra finale di un numero vuol dire calcolare la sua classe resto modulo 100. Svolgiamo il conto in due casi. Usiamo sempre il fatto che $\varphi(100) = 40$ per applicare il teorema di Eulero

- Poiché $437241 = 10931 \cdot 40 + 1$ e $722602 = 18065 \cdot 40 + 2$ otteniamo per il teorema di Eulero $[11^{437241}]_{100} = [11]_{100}^{437241} = [11]_{100}$ e $[29^{722602}]_{100} = [29]_{100}^{722602} = [29]_{100}^2 = [41]_{100}$. Dunque

$$[11^{437241} + 29^{722602}]_{100} = [11]_{100} + [41]_{100} = [52]_{100}.$$

- Poiché $\mathrm{MCD}(35, 100) = 5 \neq 1$ il teorema di Eulero non si applica alle potenze di 35. Allora scriviamo $35^{396689} = 5^{396689} \cdot 7^{396689}$ e trattiamo separatamente i due fattori.

  Poiché $396689 = 9917 \cdot 40 + 9$ dal teorema di Eulero otteniamo $[7^{396689}]_{100} = [7]_{100}^{396689} = [7]_{100}^{9} = [7]_{100}$ (l'ultima uguaglianza segue subito se si osserva che un calcolo esplicito fornisce $[7]_{100}^{4} = [1]_{100}$).

  Per l'altro fattore osserviamo che siccome $[5]_{100}^{3} = [5]_{100}^{2} = [25]_{100}$ si ha $[5]_{100}^{n} = [25]_{100}$ per ogni $n \geq 2$. Dunque

$$[35^{396689}]_{100} = [7]_{100} \cdot [25]_{100} = [75]_{100}.$$

Esercizio 14. Calcolare le seguenti classi resto

$$[3^{207859}]_5, \qquad [7^{240974}]_{11}, \quad [6^{66095}]_{14}, \quad [15^{96603}]_{24}, \quad [9^{391203} + 13^{286341}]_{25}$$

Soluzione: Calcoliamo la soluzione in due situazioni che esauriscono la casistica.

- Per calcolare $[7^{240974}]_{11} = [7]_{11}^{240974}$ possiamo applicare direttamente il teorema di Eulero giacchè $\mathrm{MCD}(7, 11) = 1$. Poiché $\varphi(11) = 10$ si ha $[7]_{11}^{10} = [1]_{10}$ e dunque

$$[7^{240974}]_{11} = [7]_{11}^{240974} = [7]_{11}^{4} = [3]_{11}$$

  in quanto $240974 = 24097 \cdot 10 + 4$.

- Per calcolare $[15^{96603}]_{24} = [15]_{24}^{96603}$ non possiamo applicare direttamente il teirema di Eulero in quanto $\mathrm{MCD}(15, 24) = 3 \neq 1$. Allora scriviamo $[15]_{24}^{96603} = [3]_{24}^{96603} \cdot [5]_{24}^{96603}$ e trattiamo separatamente i due fattori.

  Per calcolare le potenze di $[5]_{24}$ possiamo applicare il teorema di Eulero, ma in realtà è immediato osservare che $[5]_{24}^{2} = [1]_{24}$ e quindi si ottiene subito $[5]_{24}^{n} = [1]_{24}$ se n è pari e $[5]_{24}^{n} = [5]_{24}$ se n è dispari.

  Per quanto riguarda le potenze di $[3]_{24}$ si calcola immediatamente $[3]_{24}^{2} = [9]_{24}$ e $[3]_{24}^{3} = [3]_{24}$ da cui si ottiene $[3]_{24}^{n} = [9]_{24}$ se $n \geq 2$ è pari e $[3]_{24}^{n} = [3]_{24}$ se n è dispari. In definitiva

$$[15^{96603}]_{24} = [15]_{24}^{96603} = [3]_{24}^{96603} \cdot [5]_{24}^{96603} = [3]_{24} \cdot [5]_{24} = [15]_{24}.$$