Rigurgiti di Unicorno

di Valentino Bocchino

Esercizi svolti

Parte II
Esercizi

9 Esercizi sugli insiemi (sezione 2)

9.1 Appartenenza, insiemi, sottoinsiemi, insieme vuoto

Per risolvere questo esercizio, leggere nella teoria dal punto 2.1 fino al punto 2.2.2
Sia $A = \{a, b, c\}$. Dire quali delle seguenti affermazioni sono **vere** e quali **false**:

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

1. $b \in A$ è **vera** poiché l'elemento b è effettivamente nell'insieme A.
2. $\emptyset \subset A$ è **vera** per il punto 2.2, ovvero: ogni insieme ha come sottoinsieme $\emptyset$. Questo è un sottoinsieme banale.
3. $\{\emptyset\} \subset A$ è **falsa** perché nonostante sia vero che A ha come sottoinsieme l'insieme vuoto, *non è corretto affermare* che contiene un insieme che a sua volta contiene l'insieme vuoto.
4. $\{c, d\} \not\subset A$ è **vera** perché è vero che A *non* contiene l'oggetto d.
5. $\{a, \{c\}\} \subset A$ è **falsa** perché A contiene l'oggetto a ma non contiene il sottoinsieme che a sua volta contiene l'oggetto c.

Per i punti 2,3,4,5 è utile ricordare che gli unici sottoinsiemi di A sono:

$$A = \{\emptyset, A, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}\}$$

Quello che ho appena descritto è l'insieme delle parti di A: $P(A)$

9.2 Insieme delle parti di A (Punto 2.2.2)

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

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

Per vedere un esempio di $P(A)$ vedi il punto 9.1

1. $\emptyset \in P(A)$ è **vera.** *Guarda i punti: 2.2.1 e 2.2.2*
2. $a \in P(A)$ è **falsa.** Perché $\{a\}$ è un elemento di $P(A)$ ma a non lo è.
3. $\{i, u\} \subset P(A)$ è **falsa.** Perché $\{i, u\}$ non è un sottoinsieme di $P(A)$. *Da non confondere con un sottoinsieme di A.*
4. $\{e, o\} \in P(A)$ è **vera.** Perché $\{e, o\}$ è un sottoinsieme di A.
5. $\{\{e\}, \{o\}\} \subset P(A)$ è **vera.** Perché $\{\{e\}, \{o\}\}$ è un sottoinsieme di $P(A)$. *Da non confondere con un sottoinsieme di A.*

Nei punti 3 e 5 il trucco è quello di capire che stiamo considerando i sottoinsiemi dell'insieme delle parti di A, ovvero: $P(P(A))$.
Prestare *estrema attenzione* al simbolo utilizzato dal quesito. $\in$ e $\subset$ sono facilmente confondibili quando si legge velocemente, quindi è opportuno leggere con assoluta lentezza e svolgere l'esercizio per poi ricontrollarlo bene più tardi.

9.3 Intersezione, unione, prodotto cartesiano e complementare.

Si considerino gli insiemi:

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

Dire quali delle seguenti affermazioni sono vere e quali sono false:

1. $A \cap B \subset C$
2. $(v, v) \in A \times B \setminus B \times C$
3. $\{d, e\} \in P(C \cap D)$
4. $(e, p) \in A \times D$
5. $(A \times B) \cap (C \times D) = \emptyset$
6. $\{b, l, u\} \subset P(B \cup D)$

Per i punti 1,3,5 vedere nella teoria il punto 2.4.1
Per il punto 6 vedere nella teoria il punto 2.4.2
Per i punti 2,4,5 vedere nella teoria il punto 2.6.1
Per il punto 2 vedere nella teoria il punto 2.4.4

1. **Falsa**, perché $A \cap B = \{g, v\}$, ma $\{g, v\}$ non può essere un sottoinsieme di C perché g non è un elemento di C.

2. **Falsa**:
Possiamo anche calcolare $A \times B$ e $B \times C$ per poi calcolare la differenza, ma sarebbe un'operazione estremamente dispendiosa.
Ragionando, possiamo dedurre che la coppia (v, v) può solo esistere nel prodotto $A \times B$ se sia A che B contengono v.
Con una rapida verifica, possiamo affermare che $(v, v) \in A \times B$.
Ora però, dobbiamo ricordare che la differenza *rimuove* tutti gli elementi di $B \times C$ presenti in $A \times B$.
Quindi dobbiamo verificare se la coppia (v, v) esiste in $B \times C$.
Con una rapida verifica, possiamo affermare che $(v, v) \in B \times C$.
Siccome (v, v) appare in entrambi i prodotti cartesiani, il complementare la rimuove e pertanto possiamo concludere che l'affermazione è **FALSA.**

3. **Vera**, perché $C \cap D = \{d, e, r\}$, quindi il suo insieme delle parti $P = \{\emptyset, \{d\}, \{e\}, \{r\}, \{d, e\}, \{d, r\}, \{e, r\}, \{d, e, r\}\}$, contiene $\{d, e\}$

4. **Falsa**, perché e non è un oggetto presente in A, e quindi per il prodotto non può esistere nessuna coppia che abbia come primo elemento e. Anche qui, non serve calcolare $A \times D$.

5. **Falsa**:
Anche qui non serve calcolare alcun prodotto.
Dobbiamo semplicemente trovare almeno una coppia che sia in comune ai due prodotti.
Ragionando, per avere due coppie in comune ai due prodotti, serve che A e C abbiano almeno un elemento in comune e che anche B e D abbiano almeno un elemento in comune.
Notiamo che A e C hanno in comune un solo elemento v.
Quindi un'eventuale coppia in comune ai due prodotti deve per forza essere del tipo $(v, ?)$.
Notiamo che B e D hanno in comune un solo elemento z.
Quindi la coppia in comune è proprio (v, z) e pertanto è **falso** dire che i due prodotti non hanno nessuna coppia in comune, e che quindi la loro intersezione è vuota.

6. **Falsa**: perché l'unione di B e D è l'insieme composto da tutti gli elementi di B e di D, e gli elementi b, l, u compaiono in B e D. L'insieme delle parti P ha come oggetto $\{b, l, u\}$, ma non ha certamente come sottoinsieme $\{b, l, u\}$.

10 Esercizi sulle funzioni (sezione 3)

10.1 Immagine e controimmagine

Per risolvere questo esercizio, vedere nella teoria il punto 3.2.3
Sia $f : \mathbb{Z} \to \mathbb{Z}$ la funzione definita da $f(n) = n^2 - 1$.
Calcolare: $f^{-1}(-5), f^{-1}(-1), f^{-1}(8), f^{-1}(12)$.
Qui notiamo subito che la notazione può essere confusa con la definizione di funzione inversa. Tuttavia, qui non ci è stato chiesto di trovare o definire una funzione inversa. Inoltre, l'esercizio non specifica tale funzione. Pertanto f^{-1}è da intendersi come il simbolo per indicare la controimmagine.
L'esercizio è molto banale e consiste nel trovare n per ognuno dei valori proposti. Quindi:

1. Per $f^{-1}(-5)$:
   $n^2 - 1 = -5$
   $n^2 = -4$
   La soluzione di questa equazione non esiste in $\mathbb{Z}$, pertanto per $f^{-1}(-5)$ non esistono controimmagini ($f^{-1}(-5) = \emptyset$).

2. Per $f^{-1}(-1)$:
   $n^2 - 1 = -1$
   $n^2 = 0$
   L'equazione è risolta per $n = 0$, pertanto $f^{-1}(-1) = \{0\}$

3. Per $f^{-1}(8)$:
   $n^2 - 1 = 8$
   $n^2 = 9$
   L'equazione è risolta per $n = \pm 3$ (2 soluzioni), pertanto $f^{-1}(8) = \{-3, 3\}$.

4. Per $f^{-1}(12)$:
   $n^2 - 1 = 12$
   $n^2 = 13$
   La soluzione di questa equazione non esiste in $\mathbb{Z}$, pertanto per $f^{-1}(12)$ non esistono controimmagini ($f^{-1}(12) = \emptyset$).

10.2 Funzioni iniettive e suriettive

Per risolvere questo esercizio, vedere nella teoria i punti 3.2.2 e 3.2.5

10.2.1 Verifica di una funzione

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 $f^{-1}(0) \cap \{(m, n) \in \mathbb{Z} \times \mathbb{Z} | n = 4 \cdot m\}$
4. Calcolare l'immagine $f(S)$ del sottoinsieme $S = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} | n = 2m - 1\}$

Risolviamo:

1. Notiamo subito che non è iniettiva, perché per le coppie $(0, 0)$ e $(1, 1)$ abbiamo:
   $f((0, 0)) = 0^2 - 0 = 0$ e $f((1, 1)) = 1^2 - 1 = 1 - 1 = 0$
   Per verificare l'iniettività, possiamo anche imporre che se $f((m, n)) = f((a, b))$, allora $(m, n) = (a, b)$ e vedere se funziona:
   Quindi se $m^2 - n = a^2 - b$, allora $(m, n) = (a, b)$, ovvero $m = a$ e $n = b$
   Partendo da $m^2 - n = a^2 - b$ proviamo ad arrivare alla forma $m = a$:
   $m = \pm\sqrt{a^2 - b + n}$
   è palese che, avendo 2 soluzioni, questo risultato non garantisce mai che $m = a$. Perché sia iniettiva, $m = a$ deve valere per ogni coppia $\mathbb{Z} \times \mathbb{Z}$.
   Nell'ipotetico caso in cui fossimo riusciti ad arrivare ad $m = a$, serve comunque che anche $n = b$.
   Possiamo quindi concludere che **non** è iniettiva.

2. Si verifica banalmente che la funzione è *suriettiva* poiché non esistono elementi in $\mathbb{Z}$ che $m^2 - n$ non può rappresentare.
   In maniera più formale, si può dire che, per ogni $x \in \mathbb{Z}$ arbitrario, se consideriamo tutte le coppie del dominio del tipo:
   $(0, n)$ allora $m^2 - n = x$ diventa:
   $-n = x$
   Siccome $n, x \in \mathbb{Z}$ possiamo tranquillamente imporre $n = -x$
   e quindi ottenere: $-(-x) = x$ e quindi $x = x$ il che conferma che per ogni $x \in \mathbb{Z}$ arbitrario esiste una *controimmagine*.

3. Possiamo calcolare $f^{-1}(0)$, oppure possiamo direttamente impostare l'equazione:
   $m^2 - 4m = 0$
   che con $= 0$ impone la condizione di $f^{-1}(0)$ e con $-4m$ impone la condizione dell'insieme.
   Otteniamo quindi:
   $m^2 = 4 \cdot m$
   $m^2 - 4 \cdot m = 0$
   $\Delta = (-4)^2 - 4 \cdot 1 \cdot 0 = 16$
   $m = \dfrac{-(-4) \pm \sqrt{16}}{2 \cdot 1} = \dfrac{4 \pm 4}{2}$
   $m_1 = 0, m_2 = 4$
   Con i valori ottenuti, sostituendo nella coppia $(m, 4 \cdot m)$ i valori ottenuti, abbiamo le coppie che formano l'insieme cercato:
   $\{(0, 0), (4, 16)\}$

4. Per ogni $m \in \mathbb{Z}$, l'immagine è data da:
   $m^2 - (2 \cdot m - 1) = m^2 - 2 \cdot m + 1$, ovvero: $(m - 1)^2$, quindi:
   $f(S) = \{(m - 1)^2 | m \in \mathbb{Z}\}$

10.2.2 Iniettività/suriettività di una funzione - caso particolare

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE
(è troppo grande per una sola pagina)
Sia $f : \mathbb{N} \to \mathbb{N}$ la funzione definita come:

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

Dimostrare o confutare le affermazioni seguenti:

1. f è iniettiva
2. f è suriettiva
3. L'immagine $f(2\mathbb{N})$ dell'insieme dei numeri pari è contenuta nell'insieme dei numeri dispari.
4. La controimmagine $f^{-1}(3\mathbb{N})$ dell'insieme dei numeri divisibili per 3 è contenuta nell'insieme dei numeri pari.

Dopodiché, calcolare esplicitamente:

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

1. Usiamo la tecnica vista nel punto 10.2.1:
   Ricordiamo che la funzione è iniettiva se $f(a) = f(b)$, solo quando $a = b$, per ogni a, b nel dominio.
   Analizziamo tutti i casi possibili:

   1.1 Primo caso: a e b sono uguali e sono entrambi pari: allora $\frac{a}{2} = \frac{b}{2}$, quindi $a = b$

   1.2 Secondo caso: a e b sono uguali e sono entrambi dispari: allora $3 \cdot a + 1 = 3 \cdot b + 1$, quindi $a = b$

   1.3 Terzo caso: a e b sono diversi ma sono anche pari e dispari rispettivamente. In questo caso non devono avere la stessa immagine. Quindi deve valere:
   $\frac{a}{2} \neq 3 \cdot b + 1$
   Notiamo tuttavia, che l'equazione $\frac{a}{2} = 3 \cdot b + 1$ ha soluzione sia per a che per b e che tali soluzioni sono distinte ($a \neq b$). Questo significa che, scelti valori opportuni di a e b, possiamo ottenere la stessa immagine con entrambi.
   Pertanto la funzione *non* è iniettiva.
   Non serve verificare il caso in cui a e b siano diversi ma entrambi con la stessa parità, poiché il primo e il secondo caso dimostrano che due numeri con la stessa parità non possono produrre la stessa immagine.

2. Dobbiamo capire se l'immagine di f copre tutto $\mathbb{N}$: Prendiamo un $a \in \mathbb{N}$ qualunque e iniziamo a vedere cosa succede quando n è pari:
   Dobbiamo partire da $\frac{n}{2} = a$ ed arrivare a: $a = a$.
   Se a è pari, allora con $n = 2 \cdot a$, otteniamo:
   $\frac{\cancel{2} \cdot a}{\cancel{2}} = a.$
   Se a è dispari, con $n = 2 \cdot a$, abbiamo comunque n pari e pertanto riotteniamo:
   $\frac{\cancel{2} \cdot a}{\cancel{2}} = a$
   Questo funziona perché $2\mathbb{N}$ è l'insieme dei numeri pari, quindi $2 \cdot a$ è sempre pari.
   Quindi f è suriettiva.

3. Falso perché come abbiamo visto nel punto 2, l'immagine dei numeri pari è mappata su tutto $\mathbb{N}$. Inoltre, non è vero che siccome un numero del tipo $2 \cdot a$ è sempre pari, allora un numero a sia sempre dispari. A titolo esemplificativo:
   Prendiamo $2 \in \mathbb{N}$, e valutiamo $f(2\mathbb{N})$:
   $f(4) = \frac{4}{2} = 2$ ma 2 è pari.

4. Vero. Iniziamo dicendo che tutti i numeri pari sono mappati in $\mathbb{N}$, quindi sicuramente $f^{-1}(3\mathbb{N})$ è contenuta nei numeri pari, tuttavia, viene da chiedersi se un n dispari sia in grado di generare $f^{-1}(3\mathbb{N})$, perché in tal caso sarebbe mappata sia nei pari che nei dispari. Tuttavia, notiamo che se n è dispari, allora:
   $f(n) = 3 \cdot n + 1$, quindi con n dispari non si avrà mai un divisore di 3 ma semmai un successore di un divisore di 3.
   Quindi $f^{-1}(3\mathbb{N})$ è contenuta solo nei numeri pari.

Calcoliamo le immagini
$f(1) = 3 \cdot 1 + 1 = 4, f(2) = \dfrac{2}{2} = 1, f(3) = 3 \cdot 3 + 1 = 10, f(4) = \dfrac{4}{2} = 2, f(5) = 3 \cdot 5 + 1 = 16$
$f(6) = \dfrac{6}{2} = 3, f(7) = 3 \cdot 7 + 1 = 22, f(8) = \dfrac{8}{2} = 4, f(9) = 3 \cdot 9 + 1 = 28, f(10) = \dfrac{10}{2} = 5$
Per le controimmagini, verifichiamo entrambe le condizioni:

1. $f^{-1}(1)$:
   $3 \cdot n + 1 = 1 \rightarrow n = 0$ quindi è impossibile perché n dovrebbe essere dispari.
   $\dfrac{n}{2} = 1 \rightarrow n = 2$ quindi $\{2\}$ è l'insieme delle controimmagini per $f^{-1}(1)$.

2. $f^{-1}(2)$:
   $3 \cdot n + 1 = 2 \rightarrow n \notin \mathbb{N}$ quindi è impossibile
   $\dfrac{n}{2} = 2 \rightarrow n = 4$ quindi $\{4\}$ è l'insieme delle controimmagini per $f^{-1}(2)$.

3. $f^{-1}(7)$:
   $3 \cdot n + 1 = 7 \rightarrow n = 2$ quindi è impossibile perché n dovrebbe essere dispari.
   $\dfrac{n}{2} = 7 \rightarrow n = 14$ quindi $\{14\}$ è l'insieme delle controimmagini per $f^{-1}(7)$.

4. $f^{-1}(9)$:
   $3 \cdot n + 1 = 9 \rightarrow n \notin \mathbb{N}$ quindi è impossibile
   $\dfrac{n}{2} = 9 \rightarrow n = 18$ quindi $\{18\}$ è l'insieme delle controimmagini per $f^{-1}(9)$.

5. $f^{-1}(10)$:
   $3 \cdot n + 1 = 10 \rightarrow n = 3$ quindi 3 è una controimmagine.
   $\dfrac{n}{2} = 10 \rightarrow n = 20$ quindi 20 è una controimmagine. L'insieme delle controimmagini è $\{3, 20\}$ per $f^{-1}(10)$

6. $f^{-1}(13)$:
   $3 \cdot n + 1 = 13 \rightarrow n = 4$ quindi è impossibile perché n dovrebbe essere dispari.
   $\dfrac{n}{2} = 13 \rightarrow n = 26$ quindi $\{26\}$ è l'insieme delle controimmagini per $f^{-1}(13)$.

Per risolvere questo esercizio è molto utile svolgere prima l'ultima parte dove è necessario calcolare esplicitamente i valori di f e f^{-1}.
Infatti, nelle immagini, si notava subito che $f(1) = f(8)$ e quindi si aveva già la risposta al primo quesito.
Inoltre, il calcolo di $f^{-1}(10)$ avrebbe anche risolto immediatamente il primo quesito.

11 Esercizi sulla combinatorica (sezione 4)

11.1 Principio di inclusione-esclusione

Per risolvere questi esercizi, vedere i punti 4.4.2 e 4.4.3

11.1.1 Numero di multipli

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE
(è troppo grande per una sola pagina)
Calcolare quanti sono i numeri interi

1. Da 1 a 1.680 che sono divisibili per almeno uno tra 2, 6 e 7.
2. Da 1 a 2.160 che sono divisibili né per 5, né per 9, né per 12.

Soluzione:

1. Analizzando bene la richiesta, possiamo impostare il problema in questo modo:
   Definiamo 3 insiemi A, B, C che contengono i multipli di 2, 6 e 7 rispettivamente. Ovviamente consideriamo solo i multipli tra 1 e 1680 come da richiesta.
   Notiamo immediatamente che questi insiemi non sono disgiunti e che l'esercizio richiede di contare un qualunque numero tra 1 e 1680 che sia almeno multiplo di 2,6 e 7. Infatti ad esempio 6 è multiplo di 2 e di 6
   Per risolvere questo quesito dobbiamo quindi fare riferimento al principio di inclusione-esclusione, ed in particolare usare la formula per più di due insiemi (in alternativa si può applicare ricorsivamente la formula del punto 4.4.2).
   La formula $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$ richiede la conoscenza di $|A|, |B|, |C|$ e inoltre richiede la conoscenza delle varie intersezioni.
   Nonostante queste conoscenze non vengano fornite esplicitamente, è comunque possibile ricavarle attraverso il ragionamento:
   Ad esempio, facciamo finta di dover trovare il numero di multipli di 5 tra 1 e 50.
   Quindi abbiamo 5, 10, 15, 20,...
   Quindi i multipli si ottengono come $5 \cdot 1, 5 \cdot 2, ..., 5 \cdot k$. Quindi per ottenere il valore di k basta prendere un multiplo e dividerlo per 5.
   Siccome k cresce di $+1$ per ogni nuovo multiplo, per ottenere il numero di multipli tra 1 e 50, è sufficiente calcolare $\frac{50}{5} = 10$. Infatti i multipli tra 1 e 50 di 5 sono proprio la tabellina del 5: 5,10,15,20,25,30,35,40,45,50.
   Ovviamente se avessimo dovuto trovare i multipli di 3 avremmo avuto $\frac{50}{3} = 16,\overline{6}$. In questo caso si troncano i decimali (NON si approssima) e si conserva 16. Infatti i multipli di 3 tra 1 e 50 sono 16.
   Quindi abbiamo per $|A| = \frac{1.680}{2} = 840$ per $|B| = \frac{1.680}{6} = 280$ e per $|C| = \frac{1.680}{7} = 240$.
   Ora dobbiamo trovare le cardinalità delle intersezioni tra due insiemi.
   Per trovare i multipli in comune tra due insiemi, possiamo usare l'mcm (vedi il punto 5.4.1). Il minimo comune multiplo infatti ci dà il numero più piccolo che è il multiplo di tutti i numeri per cui stiamo calcolando l'mcm. Dopodiché se dividiamo 1680 per questo numero, otteniamo il numero di multipli di questo multiplo, e quindi otteniamo il numero di elementi che sono multipli di entrambi gli insiemi.
   Quindi abbiamo per $|A \cap B| = \frac{1.680}{\mathrm{mcm}(2,6)}$, per $|A \cap C| = \frac{1.680}{\mathrm{mcm}(2,7)}$, per $|B \cap C| = \frac{1.680}{\mathrm{mcm}(6,7)}$.
   Calcoliamo gli mcm:
   $\mathrm{mcm}(2,6)$: abbiamo $2 = 2$ e $6 = 2 \cdot 3$, quindi $\mathrm{mcm}(2,6) = 2 \cdot 3 = 6$
   $\mathrm{mcm}(2,7)$: abbiamo $2 = 2$ e $7 = 7$, quindi $\mathrm{mcm}(2,7) = 2 \cdot 7 = 14$
   $\mathrm{mcm}(6,7)$: abbiamo $6 = 2 \cdot 3$ e $7 = 7$, quindi $\mathrm{mcm}(2,7) = 2 \cdot 3 \cdot 7 = 42$
   Quindi per $|A \cap B| = \frac{1.680}{6} = 280$, per $|A \cap C| = \frac{1.680}{14} = 120$, per $|B \cap C| = \frac{1.680}{42} = 40$.
   Con lo stesso metodo calcoliamo $|A \cap B \cap C| = \frac{1.680}{\mathrm{mcm}(2,6,7)}$
   $\mathrm{mcm}(2,6,7)$: abbiamo $2 = 2$, $6 = 2 \cdot 3$ e $7 = 7$, quindi $\mathrm{mcm}(2,6,7) = 2 \cdot 3 \cdot 7 = 42$
   Quindi $|A \cap B \cap C| = \frac{1.680}{42} = 40$
   Quindi la soluzione è data da: $|A \cup B \cup C| = 840 + 280 + 240 - 280 - 120 - 40 + 40 = 960$
2. Qui il ragionamento è il medesimo ma con un "tocco finale". Dobbiamo contare tutti i numeri tra 1 e 2160 che sono multipli di 5, 9 oppure 12. Una volta trovato questo numero, dobbiamo sottrarlo a

2160, che rappresenta il totale di tutti i numeri, ovvero, quelli che rispettano il criterio e quelli che non lo rispettano.Definiamo quindi gli insiemi A, B, C come contenenti i multipli (da 1 a 2160) di 5,9 e 12 rispettivamente. Quindi dobbiamo risolvere:
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$
Abbiamo quindi:
$|A| = \dfrac{2.160}{5} = 432, |B| = \dfrac{2.160}{9} = 240, |C| = \dfrac{2.160}{12} = 180$
$|A \cap B| = \dfrac{2.160}{\text{mcm}(5,9)} = \dfrac{2.160}{45} = 48, |A \cap C| = \dfrac{2.160}{\text{mcm}(5,12)} = \dfrac{2.160}{60} = 36, |B \cap C| = \dfrac{2.160}{\text{mcm}(9,12)} = \dfrac{2.160}{36} = 60$
inoltre:
$|A \cap B \cap C| = \dfrac{2.160}{\text{mcm}(5,9,12)} = \dfrac{2.160}{180} = 12$
quindi:
$|A \cup B \cup C| = 432 + 240 + 180 - 48 - 36 - 60 + 12 = 720$
L'esercizio è quindi risolto con: $2.160 - 720 = 1.440$

11.1.2 Numero di monete

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?
Anche qui per risolvere l'esercizio si usa il principio di esclusione-inclusione. In particolare, se definiamo tre insiemi A, B, C dove A contiene le monete di argento, B contiene le monete europee e C contiene le monete di formato rotondo, allora l'esercizio si risolve cercando: $|A \cup B \cup C|$.
Quindi: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$
$|A|, |B|, |C|, |A \cap C|, |B \cap C|$ sono già noti. Infatti:$|A| = 25, |B| = 170, |C| = 415, |A \cap C| = 22, |B \cap C| = 152$.
Sappiamo anche che $A \cap B \subset C$ il che significa che $|A \cap B \cap C| = |A \cap B|$
Riscriviamo la formula:
$|A \cup B \cup C| = 25 + 170 + 415 - |A \cap B| - 22 - 152 + |A \cap B|$
Abbiamo quindi:
$|A \cup B \cup C| = 25 + 170 + 415 \cancel{- |A \cap B|} - 22 - 152 \cancel{+ |A \cap B|}$
$|A \cup B \cup C| = 25 + 170 + 415 - 22 - 152 = 436$

11.1.3 Numero di presenti alla festa

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 gli occhi azzurri e 4 gli occhi verdi mentre tra coloro che avevano i capelli neri 1 aveva gli occhi azzurri e 7 gli occhi verdi. Quante persone erano presenti alla festa?
Definiamo gli insiemi A, B, C, D per le persone con i capelli biondi,neri e gli occhi azzurri,verdi rispettivamente.
Stiamo cercando $|A \cup B \cup C \cup D|$. Usando quanto detto al punto 4.4.3 otteniamo:
$|A \cup B \cup C \cup D| = |A| + |B| + |C| + |D| - |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D| + |A \cap B \cap C \cap D|$
Sostituiamo con quello che conosciamo:
$|A \cup B \cup C \cup D| = 20 + 18 + 15 + 12 - |A \cap B| - 12 - 4 - 1 - 7 - |C \cap D| + |A \cap B \cap C \cap D|$
Inoltre, vale per forza la seguente:
$|A \cap B| = |C \cap D| = |A \cap B \cap C \cap D| = 0$, ovvero:
Nessuna persona ha i capelli biondi e neri allo stesso tempo, nessuna persona ha gli occhi azzurri e verdi e nessuno ha i capelli biondi e neri e gli occhi azzurri e verdi.
Abbiamo quindi:
$|A \cup B \cup C \cup D| = 20 + 18 + 15 + 12 - 0 - 12 - 4 - 1 - 7 - 0 + 0 = 41$

11.2 Ordinamenti

Per risolvere questo esercizio, vedere il punto 4.6.3

11.2.1 Ordinare gli elementi di un insieme rispettando particolari vincoli

Sia $S = \{a, b, c, d, e, f, 1, 2, 3, 4\}$. Calcolare il numero degli ordinamenti di S tali che:

1. Il primo e l'ultimo simbolo siano una lettera ed una cifra
2. Il primo e l'ultimo simbolo siano due lettere oppure due cifre

Ci sta chiedendo di calcolare un ordinamento, quindi sappiamo già cosa fare:

1. Abbiamo 10 scelte per 10 posizioni da popolare e non possiamo considerare ripetizioni. Quindi per ogni scelta che facciamo, abbiamo 10 - 1 scelte rimanenti. Se non avessimo vincoli, per le 10 scelte potremmo usare 10! per calcolare tutte le scelte possibili. Tuttavia il vincolo ci impone un massimo di 6 scelte per la prima posizione e un massimo di 4 scelte per l'ultima posizione. Quindi, per i restanti 8 elementi abbiamo solo più 8! scelte restanti. Pertanto abbiamo:
   $6 \cdot 8! \cdot 4 = 967.680$
   Dobbiamo ancora considerare il caso dove si inizia con una cifra e si finisce con una lettera: il caso è identico al precedente:
   $4 \cdot 8! \cdot 6 = 967.680$
   Tuttavia queste scelte vanno sommate tra loro, quindi abbiamo:
   $967.680 + 967.680 = 1.935.360$
   possibili scelte.
   Nota: il testo è poco chiaro perché può anche essere interpretato pensando di dover considerare solo il caso in cui si inizi con una lettera e si finisca con una cifra. In questo caso, potrebbe essere opportuno chiedere chiarimenti, oppure svolgerlo considerando tutti i casi possibili, ovvero tutti i casi non esplicitamente vietati, per poi magari aggiungere un commento, spiegando la situazione e motivando il proprio ragionamento.

2. Qui facciamo lo stesso ragionamento. Dividiamo lo studio in 2 casi:

   2.1 Iniziamo e terminiamo con una lettera:
   Qui dobbiamo fare particolarmente attenzione perché siccome il primo e l'ultimo elemento sono della stessa tipologia, una volta scelto uno di loro, abbiamo esaurito una scelta nel sottoinsieme delle lettere. Quindi per l'ultima posizione, possiamo solo più considerare 5 lettere, in quanto una di queste è già stata usata. Pertanto abbiamo
   Abbiamo in questo caso: $6 \cdot 8! \cdot 5$ possibili scelte.

   2.2 Iniziamo e terminiamo con una cifra:
   Anche qui, dobbiamo considerare il discorso per il caso precedente e quindi ricordarci che per l'ultima posizione possiamo solo più scegliere tra 3 cifre, poiché una è già stata utilizzata:
   Abbiamo in questo caso: $4 \cdot 8! \cdot 3$ possibili scelte.

   Anche qui eseguiamo la somma dei casi per ottenere il totale delle scelte possibili quando sono imposti i vincoli della richiesta:
   $6 \cdot 8! \cdot 5 + 4 \cdot 8! \cdot 3 = 1.693.440$

11.3 Esercizi misti

Per risolvere questi esercizi, vedere i punti 4.5.2, 4.7.4, 4.8.2, 4.8.6, 4.8.8

11.3.1 6 amici e 6 sedie (Ordinamenti, disposizioni semplici)

6 amici, Alessandro, Bruno, Carlo, Daniele, Enrico e Franco prendono posto su una fila di 6 sedie. Calcolare in quanti modi i 6 possono sedersi:

1. Senza restrizioni
2. In modo che Carlo e Franco siedano sulle 2 sedie centrali
3. In modo che Bruno e Carlo siedano vicini

Soluzione:
Indichiamo Alessandro, Bruno, Carlo, Daniele, Enrico e Franco con le lettere a, b, c, d, e ed f rispettivamente. Inoltre chiamiamo M l'insieme degli amici

1. Per sedersi senza restrizione, sicuramente dobbiamo considerare un metodo di calcolo che escluda le ripetizioni. Siccome a noi interessa che ad esempio le coppie (a, b, c, d, e, f) e (a, b, d, c, f, e) vengano contate entrambe, l'ordine conta. Quindi scegliamo la disposizione semplice:

$$\mathcal{O}_M = D_{6,6} = \frac{6!}{(6-6)!} = \frac{6!}{1} = 6! = 720$$

   Ricordando la convenzione che $0! = 1$ Vedere 4.6.2
   Inoltre, per chi si ricorda, in questo caso si poteva applicare: $\mathcal{O}_M = 6!$ *Per chi non si ricorda, la disposizione fa lo stesso lavoro, niente panico!*

2. Per questo caso, c ed f si possono sedere sulle due sedie centrali, ma non abbiamo nessun vincolo in merito al loro ordine, quindi possiamo considerare $??cf??$ e $??fc??$ come 2 ordinamenti possibili.
   Dopodiché, gli altri possono sedersi nei restanti sedili, quindi dobbiamo chiederci in quanti modi possiamo ordinare 4 persone distinte sulle restanti 4 sedie. Anche qui possiamo scrivere una disposizione semplice che alla fine non sarà niente meno che un ordinamento del sottoinsieme di M che chiameremo $S = \{a, b, d, e\}$:

$$\mathcal{O}_S = 4! = 24$$

   Per considerare tutte le scelte possibili tra loro, consideriamo 24 possibili scelte per $??cf??$ e altre 24 per $??fc??$, in altre parole, le due scelte sono indipendenti. Abbiamo quindi:

$$2 \cdot 24 = 48$$

   modi diversi di sedersi.

3. Qui si applica un discorso simile, ma non uguale al punto precedente. Infatti b e d possono sedersi in posti diversi, che non sono per forza al centro. Per questo problema, non esistono formule nella teoria, quindi serve ragionare. Se consideriamo un *array* di 6 sedie, possiamo prendere la coppia dei 2 e vedere in quanti modi distinti possiamo farli sedere. Otteniamo 5 modi possibili.
   In realtà la formula per queste situazioni esiste: chiamiamo il numero di sedie (dim. array) con la variabile d. Chiamiamo la dimensione della coppia c.
   La formula è: $d - c + 1$. Infatti $6 - 2 + 1 = 5$. (non confondere d e c con Daniele e Carlo del problema!)
   Questo problema capita spesso in programmazione quando abbiamo a che fare con pattern matching, sottosequenze, ecc.ecc.... Per ricordare questo concetto si può pensare al concetto delle "sliding windows".
   Dopodiché consideriamo come nel punto precedente che la coppia b e c può anche configurarsi come c e b.
   Infine, considera nell'esercizio precedente come gli altri possono disporsi, ovvero in 24 modi possibili.
   Siccome questi tre casi sono completamente indipendenti tra loro, abbiamo:

$$5 \cdot 2 \cdot 24 = 240$$

   modi possibili di sedersi.

11.3.2 Gli outfit di Anna (Scelte successive, disposizioni semplici, combinazioni semplici)

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE

(è troppo grande per una sola pagina)

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 1 weekend al mare e decide di portare con sé 4 magliette, 2 paia di pantaloni, 2 paia di scarpe e 1 borsetta. Quante sono le possibili scelte di questi capi?

Soluzione:

1. Dobbiamo escludere le ripetizioni, assumendo che Anna non indossi 2 scarpe contemporaneamente, oppure ad esempio, che non si metta più di una borsetta per compensare il fatto che non si è messa una maglietta. Per ogni outfit, abbiamo 4 oggetti e per ciascuno di questi oggetti abbiamo 11, 5, 6 e 2 scelte possibili. Possiamo usare il metodo delle scelte successive:

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

poiché ogni scelta è indipendente dalle altre.

2. Dobbiamo anche qui escludere le ripetizioni per quanto riguarda le scarpe poiché un ordine che conta due volte lo stesso paio non è valido. Tuttavia, siccome stiamo contando i modi di ordinare le scarpe, dobbiamo avvalerci di una disposizione, per la quale appunto, conta l'ordine. Per questo dobbiamo usare le disposizioni semplici (ovvero senza elementi ripetuti). Infatti ci stiamo chiedendo quanti modi esistono, per disporre 6 paia di scarpe in 14 scomparti, ovvero, stiamo considerando la disposizione semplice di ordine 6 nell'insieme dei 14 scomparti. Consideriamo quindi la formula:

$$D_{n,k} = \frac{n!}{(n-k)!}$$

dove n rappresenta la cardinalità dell'insieme degli scomparti, ovvero: $n = 14$ e k rappresenta l'ordine, ovvero $k = 6$.
Abbiamo quindi:

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

possibili ordinamenti. Anna può scegliere tra 2.162.160 modi diversi di riordinare le sue scarpe nella scarpiera.
Quindi, nessun oggetto si ripete (non prendiamo in considerazione una singola disposizione che abbia in 2 scomparti lo stesso paio), ma prendiamo certamente in considerazione tutte le disposizioni che considerano le 6 paia (che infatti saranno sempre le stesse paia di scarpe tra una disposizione e l'altra).

3. Concentriamoci sul primo oggetto: le magliette. Anche qui dobbiamo calcolare quanti modi esistono di scegliere 4 magliette da un insieme più grande di 11 magliette (senza ripetizioni), tuttavia, non possiamo considerare le disposizioni, perché per questo problema, ad esempio, gli insiemi delle magliette (gialla, verde, blu, rosa) e (verde, blu, rosa, gialla) andrebbero conteggiati una sola volta perché sono lo stesso insieme, mentre con una disposizione, questi verrebbero entrambi conteggiati! Per questa ragione ci avvaliamo delle combinazioni semplici, che denotiamo col coefficiente binomiale.
Quindi per le magliette abbiamo:

$$\binom{11}{4} = \frac{11!}{4! \cdot (11-4)!} = \frac{\cancel{11!}}{4! \cdot \cancel{7!}} = \frac{\cancel{8} \cdot \cancel{9} \cdot \cancel{10} \cdot 11}{\cancel{4!}} = 2 \cdot 3 \cdot 5 \cdot 11 = 330$$

Per i pantaloni abbiamo:

$$\binom{5}{2} = \frac{5!}{2! \cdot (5-2)!} = \frac{\cancel{5!}}{2! \cdot \cancel{3!}} = \frac{\cancel{4} \cdot 5}{\cancel{2!}} = 2 \cdot 5 = 10$$

Per le scarpe:

$$\binom{6}{2} = \frac{6!}{2! \cdot (6-2)!} = \frac{\cancel{6!}}{2! \cdot \cancel{4!}} = \frac{5 \cdot \cancel{6}}{\cancel{2!}} = 5 \cdot 3 = 15$$

Per le borsette:

$$\binom{2}{1} = \frac{2!}{1! \cdot (2-1)!} = \frac{2}{1} = 2$$

Il quesito ci chiede essenzialmente in quanti modi diversi possiamo comporre la nostra valigia. Quindi anche qui si tratta di escludere le ripetizioni, perché una valigia con le stesse scelte non costituisce una nuova scelta. Inoltre, anche qui notiamo che basta anche solo che un singolo oggetto (ad esempio una maglietta) sia diversa tra una valigia e un'altra per poter dire che si tratta di due modi diversi di comporre la valigia. Le scelte sono quindi indipendenti tra loro, e pertanto Anna ha:

$$330 \cdot 10 \cdot 15 \cdot 2 = 99.000$$

modi diversi di comporre la sua valigia.
Attenzione: Anche qui, la domanda "*Quante sono le possibili scelte di questi capi?*" è estremamente ambigua perché ammette più risposte, ad esempio si potrebbe pensare che vengano richieste solo le singole disposizioni, oppure che venga richiesto il totale delle scelte possibili, oppure (come nel caso specifico) che chieda quanti modi ci sono di scegliere un set completo composto da 4 magliette, 2 paia di pantaloni, 2 paia di scarpe ed 1 borsetta. Se capitasse una roba del genere in sede d'esame, suggerisco di argomentare la risposta ed eventualmente di chiedere chiarimenti.

11.3.3 PIN degli impiegati (Disposizioni e combinazioni semplici)

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE

(è troppo grande per una sola pagina)

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

1. Un codice deve alternare cifre pari a cifre dispari e non può contenere cifre ripetute.
2. Un codice non può cominciare con la cifra 0 ed inoltre la somma delle cifre che lo compongono deve essere pari.
3. Un codice non può contenere la cifra 0 più di due volte.

Soluzione:

1. Per alternare le cifre pari con quelle dispari esistono 2 modi (indichiamo con P le cifre pari e con D le cifre dispari):

   1.1 $PDPDPD$:
   Qui possiamo usare il metodo delle scelte successive, considerando che per 10 cifre, 5 sono pari e 5 sono dispari. Dobbiamo capire quanti modi possibili ci sono di scegliere 6 cifre da un insieme di 10 cifre, considerando anche il fatto che non possono esserci ripetizioni. Abbiamo quindi:

   $$5 \cdot 5 \cdot 4 \cdot 4 \cdot 3 \cdot 3 = 3.600$$

   Se invece vogliamo usare una disposizione semplice, possiamo considerare che un numero a 6 cifre con ogni cifra che si alterna tra pari e dispari, avrà sempre 3 cifre pari e 3 cifre dispari. Possiamo quindi considerare quanti modi ci sono di scegliere 3 cifre pari da un insieme di 5 cifre pari:

   $$D_{5,3} = \frac{5!}{(5-3)!} = \frac{\cancel{5!}}{\cancel{2!}} = 3 \cdot 4 \cdot 5 = 60$$

   Qui usiamo una disposizione e non una combinazione perché ad esempio le coppie (3,5,7) e (3,7,5) andrebbero contate entrambe, ma la combinazione semplice ne conterebbe solo una.
   Per le cifre dispari vale lo stesso ragionamento, ovvero $D_{5,3} = 60$. Siccome la scelta delle cifre pari è indipendente dalla scelta delle cifre dispari abbiamo:

   $$D_{5,3} \cdot D_{5,3} = 60 \cdot 60 = 3.600$$

   1.2 $DPDPDP$:
   è identico al primo.

   Abbiamo quindi la somma dei due casi: $3.600 + 3.600 = 7.200$ casi possibili.

2. Il trucco qui è notare che la richiesta non impone vincoli sugli elementi ripetuti, e quindi dà per scontato che in un codice le cifre possono ripetersi:
   Intanto ragioniamo sul fatto che una somma di numeri pari è sempre pari, mentre una somma di numeri dispari è pari solo se il numero degli addendi dispari è pari. Quindi una somma con numeri pari e dispari è pari solo se il numero di elementi dispari è pari.
   Questo ci permette di arrivare ad un vincolo implicito, ovvero che l'ultima cifra (o comunque una delle 6 cifre) dovrà essere pari oppure dispari, per permettere di avere una somma pari. Quindi per l'ultima cifra possiamo solo avere 5 scelte possibili.
   Inoltre per la prima cifra, non possiamo scegliere lo 0, quindi abbiamo solo 9 scelte possibili.
   Per le altre cifre invece, non abbiamo il vincolo dello 0, quindi abbiamo 10 scelte possibili, visto che consideriamo anche le ripetizioni: Quindi abbiamo:

   $$9 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 5 = 450.000$$

   codici possibili.

3. Anche qui consideriamo i codici con ripetizione. Per trovare tutti i codici, dobbiamo prima considerare tutti i codici che non contengono lo 0. Abbiamo quindi:

   $$9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 = 9^6 = 531.441$$

Dobbiamo poi considerare tutti i codici che hanno un solo 0. Quindi dobbiamo innanzitutto chiederci, quanti modi ci sono per mettere una cifra nulla in un insieme di 6 cifre. Anche qui usiamo una combinazione semplice perché in realtà l'ordine in cui viene messa la cifra non conta.

$$\binom{6}{1} = \frac{6!}{1! \cdot (6-1)!} = \frac{\cancel{6!}}{\cancel{5!}} = 6$$

Dopodiché calcoliamo:

$$9^5 = 59.049$$

Moltiplichiamo il risultato per tutti i modi possibili:

$$59.049 \cdot 6 = 354.294$$

Consideriamo anche il caso con 2 cifre che hanno uno 0. Anche qui, proprio perché l'ordine delle due cifre non conta, la combinazione semplice è il metodo adatto:

$$\binom{6}{2} = \frac{6!}{2! \cdot (6-2)!} = \frac{\cancel{6!}}{2! \cdot \cancel{4!}} = \frac{5 \cdot 6}{2!} = \frac{30}{2} = 15$$

Infatti non ci interessa contare ad esempio le disposizioni distinte 001234 e 001234 perché sono equivalenti ma una disposizione semplice le conterebbe entrambi. Quindi vanno considerate appunto le combinazioni e non le disposizioni.
Dopodiché calcoliamo:

$$9^4 = 6.561$$

Moltiplichiamo il risultato per tutti i modi possibili:

$$15 \cdot 6.561 = 98.415$$

Per ottenere il risultato sommiamo i tre casi:

$$531.441 + 354.294 + 98.415 = 984.150$$

11.3.4 Scuola di ballo (interessante per il principio di inclusione-esclusione)

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE

(è troppo grande per una sola pagina)

Ad un corso di ballo sono iscritti 11 uomini e 9 donne. Si tengono 2 lezioni a settimana, il lunedì ed 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. Dobbiamo fare estremamente attenzione perché con coppie possibili, l'esercizio ci chiede quante coppie si possono formare, e non quante coppie possono coesistere, andando quindi a discutere il fatto che se tutti ballano in coppia, 2 uomini rimarranno senza una donna. Quindi in questo caso la risposta corretta sarebbe:
$$11 \cdot 9 = 99$$
ovvero, *ogni ballerina può ballare con ogni ballerino* quindi le coppie sono 99.

2. La scelta dei 10 studenti è in realtà composta da 2 scelte indipendenti. Per ciascuna di queste scelte, l'ordine non conta e vale sempre il vincolo sulle ripetizioni. Quindi per gli uomini consideriamo la combinazione semplice:
$$\binom{11}{5} = \frac{11!}{5! \cdot (11-5)!} = \frac{\cancel{11!}}{5! \cdot \cancel{6!}} = \frac{7 \cdot \cancel{8} \cdot \cancel{9} \cdot \cancel{10} \cdot 11}{2 \cdot \cancel{3} \cdot \cancel{4} \cdot \cancel{5}} = \frac{7 \cdot 2 \cdot 3 \cdot \cancel{2} \cdot 11}{\cancel{2}} = 7 \cdot 2 \cdot 3 \cdot 11 = 462$$
Per le donne:
$$\binom{9}{5} = \frac{9!}{5! \cdot (9-5)!} = \frac{\cancel{9!}}{\cancel{5!} \cdot 4!} = \frac{\cancel{6} \cdot 7 \cdot \cancel{8} \cdot \cancel{9}}{\cancel{2} \cdot \cancel{3} \cdot \cancel{4}} = 3 \cdot 7 \cdot 2 \cdot 3 = 126$$
Quindi ci sono $462 \cdot 126 = 58.212$ modi di scegliere i 10 studenti.

3. Qui dobbiamo fare un ragionamento profondo per sfruttare la formula di unione tra insiemi. Innanzitutto, consideriamo gli uomini e le donne separatamente. Consideriamo ora il principio di inclusione-esclusione:
$$|A \cup B| = |A| + |B| - |A \cap B|$$
Quando l'esercizio dice: "ogni studente era presente ad almeno una lezione" ci sta essenzialmente rivelando $|A \cup B|$, il che ci permette di ricavare $|A \cap B|$ dalla formula, ovvero il numero di coloro che hanno partecipato *ad entrambe* le lezioni.
Impostiamo il problema per gli uomini:
definiamo con M_ℓ l'insieme gli uomini presenti il lunedì e con M_g gli uomini presenti il giovedì. Abbiamo quindi:
$|M_\ell| = 7$ e $|M_g| = 9$. Inoltre sappiamo che gli uomini nel corso sono 11 e che tutti erano presenti almeno una volta nella settimana, pertanto: $|M_\ell \cup M_g| = 11$. Possiamo quindi trovare la soluzione:
$11 = 7 + 9 - |M_\ell \cap M_g|$
$11 + |M_\ell \cap M_g| = 7 + 9$
$|M_\ell \cap M_g| = 7 + 9 - 11 = 5$
Per le donne definiamo con D_ℓ e D_g gli insiemi delle donne presenti il lunedì e il giovedì rispettivamente. Abbiamo quindi: $|D_\ell| = 8, |D_g| = 7$ e $|D_\ell \cup D_g| = 9$. Pertanto abbiamo come soluzione:
$$|D_\ell \cap D_g| = 8 + 7 - 9 = 6$$
Pertanto gli studenti presenti ad entrambe le lezioni sono $5 + 6 = 11$.

11.3.5 Match di tennis (combinazioni semplici, ordinamenti)

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

1. Il circolo “Laver” ha 8 tennisti e 5 tenniste di buon livello tra cui selezionare la squadra. Quante sono le squadre possibili che il “Laver” può scegliere?
2. Formate le squadre, i partecipanti verranno accoppiati casualmente (tennisti con tennisti e tenniste con tenniste) per i 6 singolari ed un tennista ed una tennista per squadra verranno sorteggiati per il doppio misto. Quanti sono teoricamente i possibili accoppiamenti fra le squadre?
3. I 7 incontri vengono disputati consecutivamente: prima i 4 singoli singoli maschili, poi i 2 singoli femminili, poi il doppio. Quanti sono i possibili ordinamenti dei 7 incontri?

Soluzione:
Non conosco il tennis, ma per fortuna esiste Google!

1. Per giocare agli incontri è necessaria una squadra composta da 4 tennisti e 2 tenniste (1 giocatore per ogni singolo). Come già detto nel testo, per il doppio misto vengono utilizzati giocatori già presenti nella squadra. La scelta della squadra si scompone in 2 scelte indipendenti, una riguarda la scelta dei tennisti e l’altra riguarda la scelta delle tenniste. Per ognuna di queste scelte, non possiamo avere ripetizioni (i giocatori non si clonano) e non ci interessa l’ordine. Pertanto, per i tennisti, calcoliamo la disposizione semplice:
$$\binom{8}{4} = \frac{8!}{4! \cdot (8-4)!} = \frac{\cancel{8!}}{\cancel{4!} \cdot 4!} = \frac{5 \cdot \cancel{6} \cdot 7 \cdot \cancel{8}}{2 \cdot \cancel{3} \cdot \cancel{4}} = \frac{5 \cdot 2 \cdot 7 \cdot \cancel{2}}{\cancel{2}} = 5 \cdot 2 \cdot 7 = 70$$
Per le tenniste:
$$\binom{5}{2} = \frac{5!}{2! \cdot (5-2)!} = \frac{\cancel{5!}}{2 \cdot \cancel{3!}} = \frac{\cancel{4} \cdot 5}{\cancel{2}} = 2 \cdot 5 = 10$$
Abbiamo quindi: $70 \cdot 10 = 700$ possibili squadre.
2. Qui chiede essenzialmente di calcolare tutti i possibili accoppiamenti tra squadre, che sono a loro volta composti da scelte indipendenti (i singoli accoppiamenti per ogni match).
Tenendo a mente che le 2 squadre sono composte da 4 tennisti e 2 tenniste, *Google ci conferma* che un giocatore può essere scelto per un solo singolare, quindi non sono ammesse ripetizioni.
Per i tennisti: abbiamo per i singolari 4! possibili scelte. L’altra squadra ha a sua volta 4! possibili scelte, quindi abbiamo: $4! \cdot 4!$ possibili accoppiamenti
Per le tenniste: abbiamo 2! possibili accoppiamenti per i singolari, così come l’altra squadra. Abbiamo quindi $2! \cdot 2!$ possibili accoppiamenti:
Per il doppio misto: abbiamo $4 \cdot 2$ possibili scelte nella prima squadra per sorteggiare i due giocatori per il doppio misto, e l’altra squadra avrà a sua volta $4 \cdot 2$ possibili scelte. Quindi ci sono $4 \cdot 2 \cdot 4 \cdot 2$ possibili accoppiamenti.
Per il totale di tutti gli accoppiamenti:
$$4! \cdot 4! \cdot 2! \cdot 2! \cdot 4 \cdot 2 \cdot 4 \cdot 2 = (4!)^2 \cdot 4^2 \cdot 2^4 = (4!)^2 \cdot 4^2 \cdot 2^2 \cdot 2^2 = (4! \cdot 4 \cdot 4)^2 = (4! \cdot 4^2)^2 = 147.456$$
3. Qui viene richiesto di calcolare quanti modi possibili ci sono di giocare le dispute dei singolari maschili, femminili e i doppi misti. Per calcolare i modi possibili è necessario considerare come scelte indipendenti i singolari maschili, i singolari femminili e i doppi misti. Dobbiamo innanzitutto imporre che non ci siano ripetizioni, perché non si gioca 2 volte lo stesso match, tuttavia qui conta l’ordine. Pertanto, abbiamo per i singolari maschili, il numero di disposizioni semplici:$D_{4,4} = 4! = 24$ possibili modi di organizzare le dispute.
Per i singolari femminili abbiamo $2! = 2$ possibili modi.
Il caso del doppio misto è banale perché ammette 1 solo modo possibile.
Il totale dei modi possibili è quindi: $4! \cdot 2! = 24 \cdot 2 = 48$.

11.3.6 I 16 informatici (combinazioni semplici e con ripetizioni)

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

1. Il gruppo di lavoro sarà denominato con una sigla formata dalle 4 iniziali I, F, B, S delle nazioni coinvolte. Quante sono le possibili sigle?
2. Quante diverse distribuzioni per nazionalità può avere un tale gruppo se si richiede che sia presente almeno 1 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, ed i 3 rimanenti ricopriranno il ruolo di coordinatore tra i 2 progetti, responsabile del budget e responsabile della presentazione dei risultati. In quanti modi in totale si possono attribuire i compiti?

Soluzione:

1. Le possibili sigle, date dall'ordinamento dell'insieme delle lettere I, F, B, S è: $4! = 24$
2. Siccome deve essere presente almeno 1 membro per ognuna delle 4 nazioni partecipanti, per le diverse distribuzioni dobbiamo solo considerare solo 12 persone, perché 4 sono già vincolate. Siccome stiamo cercando le possibili distribuzioni in riferimento alla nazione, l'ordine in cui queste persone compaiono nelle distribuzioni non conta, ma conta soltanto il numero di persone per nazioni. Inoltre, siccome dobbiamo occupare tutte e 12 le posizioni nel gruppo, dobbiamo avere anche più di un informatico per ogni nazione, pertanto il calcolo corretto è quello di una combinazione con ripetizione, ovvero:

$$C'_{n,k} = C_{k+n-1,n-1} = \frac{(k+n-1)!}{(n-1)! \cdot k!}$$

dove $k = 12$ sono le persone da scegliere, da un insieme $n = 4$ di 4 nazioni. Quindi abbiamo:

$$C'_{4,12} = C_{12+4-1,4-1} = C_{15,3} = \frac{\cancel{15!}}{3! \cdot \cancel{12!}} = \frac{13 \cdot \cancel{14} \cdot \cancel{15}}{\cancel{3!}} = 13 \cdot 7 \cdot 5 = 455$$

distribuzioni possibili.

3. Il problema chiede di calcolare il prodotto tra più scelte indipendenti tra loro. Calcoliamo ciascuna di queste scelte:
Per decidere in quanti modi possiamo scegliere il gruppo per il sottoprogetto 1, facciamo attenzione a non ragionare come prima, perché qui non possiamo considerare un caso con ripetizioni, perché nessuna persona è clone di un'altra persona. Inoltre, non consideriamo l'ordine con cui vengono disposte le persone, ovvero, un gruppo con 7 persone del tipo $\{1, 2, 3, 4, 5, 6, 7\}$ e un gruppo del tipo $\{1, 2, 4, 5, 7, 6, 3\}$ sono lo stesso gruppo. Quindi applichiamo la formula della combinazione semplice:

$$C_{16,7} = \frac{16!}{7! \cdot (16-7)!} = \frac{\cancel{16!}}{7! \cdot \cancel{9!}} = \frac{\cancel{10} \cdot 11 \cdot \cancel{12} \cdot 13 \cdot \cancel{14} \cdot \cancel{15} \cdot \cancel{16}}{\cancel{2} \cdot 3 \cdot \cancel{4} \cdot \cancel{5} \cdot \cancel{6} \cdot \cancel{7}} = \frac{5 \cdot 11 \cdot 2 \cdot 13 \cdot 2 \cdot \cancel{3} \cdot 4}{\cancel{3}} = 5{\cdot}11{\cdot}2{\cdot}13{\cdot}2{\cdot}4 = 11.440$$

Siccome non ammettiamo ripetizioni, per il prossimo caso dobbiamo considerare solo più $16 - 7 = 9$ persone. Consideriamo i modi possibili di formare il gruppo del sottoprogetto 2 composto da 6 persone. Applichiamo lo stesso metodo per il sottoprogetto 1:

$$C_{9,6} = \frac{9!}{6! \cdot (9-6)!} = \frac{\cancel{9!}}{\cancel{6!} \cdot 3!} = \frac{7 \cdot \cancel{8} \cdot \cancel{9}}{\cancel{2} \cdot \cancel{3}} = 7 \cdot 4 \cdot 3 = 84$$

Per il coordinatore tra i 2 progetti abbiamo solo più $9 - 6 = 3$ persone rimanenti da cui scegliere:

$$C_{3,1} = \frac{3!}{1! \cdot (3-1)!} = \frac{3!}{2!} = 3$$

Per il responsabile del budget possiamo solo più scegliere tra 2 persone, quindi ci restano 2 scelte possibili.
Per il responsabile della presentazione dei risultati ci resta solamente una scelta.
Abbiamo quindi:

$$11.440 \cdot 84 \cdot 3 \cdot 2 \cdot 1 = 5.765.760$$

modi possibili di organizzare i 16 informatici nei gruppi descritti.

11.3.7 Il chimico profumiere (combinazioni semplici e con ripetizioni)

Un chimico vuole preparare un profumo miscelando in parti uguali, 8 essenze base a sua disposizione.

1. Quante sono in totale le miscele possibili usando 2, 3 o 4 essenze?
2. 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. Quante invece sono le confezioni possibili se ogni scatola contiene 3 coppie di boccette dello stesso colore?

Soluzione:

1. Non dobbiamo considerare l'ordine, e inoltre, non possiamo considerare le ripetizioni. Il motivo per cui si scartano le ripetizioni è molto sottile, ma se riflettiamo sulla parte in cui dice "*in parti uguali*" e poi consideriamo una combinazione con ripetizione, allora potremmo avere ad esempio 2 parti di lavanda e 1 di bergamotto, il che violerebbe la richiesta "*in parti uguali*". Quindi se uno considera il quesito come "...2, 3 o 4 essenze *in parti uguali*" in realtà risulta chiara l'esigenza di evitare ripetizioni. Impostiamo quindi una combinazione semplice per le 2 essenze:

   $$\binom{8}{2} = \frac{8!}{2! \cdot (8-2)!} = \frac{\cancel{8!}}{2 \cdot \cancel{6!}} = \frac{7 \cdot \cancel{8}}{\cancel{2}} = 7 \cdot 4 = 28$$

   per 3 essenze abbiamo:

   $$\binom{8}{3} = \frac{8!}{3! \cdot (8-3)!} = \frac{\cancel{8!}}{3! \cdot \cancel{5!}} = \frac{\cancel{6} \cdot 7 \cdot \cancel{8}}{\cancel{2} \cdot \cancel{3}} = 2 \cdot 7 \cdot 4 = 56$$

   per 4 essenze:

   $$\binom{8}{4} = \frac{8!}{4! \cdot (8-4)!} = \frac{\cancel{8!}}{\cancel{4!} \cdot 4!} = \frac{5 \cdot \cancel{6} \cdot 7 \cdot \cancel{8}}{2 \cdot \cancel{3} \cdot \cancel{4}} = \frac{5 \cdot 2 \cdot 7 \cdot \cancel{2}}{\cancel{2}} = 5 \cdot 2 \cdot 7 = 70$$

   Notiamo inoltre che il quesito non chiede quante miscele possiamo preparare usando 2, 3 e 4 essenze. Ma piuttosto chiede la somma delle singole casistiche. Quindi nonostante siano scelte indipendenti, anziché calcolare il prodotto calcoleremo la somma:

   $$28 + 56 + 70 = 154$$

2. Ci stiamo chiedendo quanti modi possibili ci sono di scegliere 6 boccette di 4 colori diversi. Ovviamente dobbiamo considerare le ripetizioni. L'ordine in questo caso non conta perché 2 scatole aventi le stesse boccette sono considerate identiche, a prescindere da come queste boccette sono disposte al suo interno. Consideriamo quindi la combinazione con ripetizione:

   $$C'_{4,6} = C_{6+4-1,4-1} = \frac{(6+4-1)!}{(4-1)! \cdot 6!} = \frac{\cancel{9!}}{3! \cdot \cancel{6!}} = \frac{7 \cdot 8 \cdot 9}{3!} = \frac{7 \cdot \cancel{8} \cdot \cancel{9}}{\cancel{2} \cdot \cancel{3}} = 7 \cdot 4 \cdot 3 = 84$$

   Possiamo quindi produrre fino ad 84 scatole distinte con boccette prese a caso.

3. *Anche qui la consegna è* ***ambigua****: nonostante la soluzione di questo esercizio si aspetti il calcolo di una combinazione senza ripetizioni, nulla nella consegna vieta di considerare scatole che abbiano più coppie dello stesso colore. D'altronde il vincolo è imposto sulle boccette nelle coppie e non sulle coppie nella scatola. Inoltre, non è nemmeno un ragionamento assurdo, visto che nel mondo reale, dei prodotti simili sono ampiamente commercializzati. All'esame, di fronte ad un quesito del genere, è bene chiedere chiarimenti.*
   Ci stiamo chiedendo quante scatole distinte da 3 coppie ciascuna possiamo generare, se abbiamo a disposizione 4 coppie (4 colori) da cui scegliere. Come al punto precedente, l'ordine non conta. Calcoliamo quindi il numero di combinazioni senza ripetizioni:

   $$\binom{4}{3} = \frac{4!}{3! \cdot (4-3)!} = \frac{4!}{3!} = 4$$

   Possiamo quindi comporre solamente 4 scatole distinte, senza ripetizioni, con i vincoli imposti dal quesito.

11.3.8 Semifinali olimpiche (casi particolari di combinazioni semplici)

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE

(è troppo grande per una sola pagina)

Alle semifinali olimpiche della gara dei 100 metri piani sono ammessi i 16 tempi migliori delle qualificazioni. I 16 atleti sono poi distribuiti in 2 semifinali di 8 atleti ciascuna. Determinare il numero delle possibili distribuzioni dei 16 atleti nelle 2 semifinali nei casi seguenti:

1. Non si richiede nessuna condizione: tutte le possibilità sono ammesse.
2. I 4 atleti con i tempi migliori devono essere distribuiti equamente nelle 2 semifinali (2 per ciascuna)
3. 9 atleti in semifinale sono europei ed in ciascuna semifinale devono essere presenti non più di 6 atleti europei.

Soluzione:

1. Per calcolare il numero delle possibili distribuzioni dei 16 atleti dobbiamo valutare due scelte. Ognuna di queste scelte rappresenta una semifinale da 8 atleti ciascuna. Per ognuna di queste scelte l'ordine non conta, tuttavia non possiamo ammettere ripetizioni, perché gli umani non sono ancora clonabili. Tenendo conto del metodo delle scelte successive, per la prima semifinale abbiamo 16 atleti da cui scegliere mentre per la seconda ne avremo $16 - 8 = 8$. Per la prima scelta:

$$\binom{16}{8} = \frac{16!}{8! \cdot (16-8)!} = \frac{\cancel{16!}}{\cancel{8!} \cdot 8!} = \frac{9 \cdot \cancel{10} \cdot 11 \cdot \cancel{12} \cdot 13 \cdot \cancel{14} \cdot \cancel{15} \cdot \cancel{16}}{\cancel{2} \cdot 3 \cdot 4 \cdot \cancel{5} \cdot \cancel{6} \cdot \cancel{7} \cdot \cancel{8}} = \frac{9 \cdot 5 \cdot 11 \cdot 2 \cdot 13 \cdot \cancel{2} \cdot \cancel{3} \cdot \cancel{2}}{\cancel{3} \cdot \cancel{4}} = 9 \cdot 5 \cdot 11 \cdot 2 \cdot 13 = 12.870$$

   Per la seconda scelta abbiamo: $\binom{8}{8} = 1$

   Abbiamo quindi 12.870 possibili distribuzioni.

2. Per tutte le casistiche consideriamo sempre delle combinazioni semplici.
   Attenzione a non fare l'errore di scegliere i 4 migliori. Quelli sono già fissati dal quesito, che infatti non ci chiede i modi possibili per individuarli.
   Per questi 4 atleti, consideriamo tutti i modi possibili per scegliere una coppia:

$$\binom{4}{2} = \frac{4!}{2! \cdot (4-2)!} = \frac{4!}{2! \cdot 2!} = \frac{2 \cdot 3 \cdot \cancel{4}}{\cancel{4}} = 6$$

   Quindi per la prima semifinale, consideriamo tutti i modi possibili per scegliere $8 - 2 = 6$ atleti dai $16 - 4 = 12$ concorrenti:

$$\binom{12}{6} = \frac{12!}{6! \cdot (12-6)!} = \frac{12!}{6! \cdot 6!} = 924$$

   Come per il primo punto, alla seconda semifinale rimangono $\binom{6}{6} = 1$ scelte per gli atleti e $\binom{2}{2} = 1$ scelte per la coppia di atleti coi tempi migliori.
   Abbiamo quindi 6 modi per accoppiarli tra di loro e 924 modi per scegliere i restanti 6. Pertanto:

$$6 \cdot 924 = 5.544$$

3. Consideriamo la prima semifinale:
   Visto il vincolo, deve avere almeno 3 europei, e al massimo 6. Studiamo i vari casi:
   Ricordo che $16 - 9 = 7$
   Quando ha 3 europei, allora ha:

$$\binom{9}{3} = \frac{9!}{3! \cdot (9-3)!} = 84$$

   scelte possibili tra gli europei e

$$\binom{7}{5} = \frac{7!}{5! \cdot (7-5)!} = 21$$

   scelte possibili tra i non europei.
   La seconda semifinale raccoglie tutti gli altri quindi non ha scelte.
   Quando ha 4 europei, allora ha:

$$\binom{9}{4} = \frac{9!}{4! \cdot (9-4)!} = 126$$

scelte possibili tra gli europei e

$$\binom{7}{4} = \frac{7!}{4! \cdot (7-4)!} = 35$$

scelte possibili tra i non europei.
Quando ha 5 europei, allora ha:

$$\binom{9}{5} = \frac{9!}{5! \cdot (9-5)!} = 126$$

scelte possibili tra gli europei e

$$\binom{7}{3} = \frac{7!}{3! \cdot (7-3)!} = 35$$

scelte possibili tra i non europei.
Quando ha 6 europei, allora ha:

$$\binom{9}{6} = \frac{9!}{6! \cdot (9-6)!} = 84$$

scelte possibili tra gli europei e

$$\binom{7}{2} = \frac{7!}{2! \cdot (7-2)!} = 21$$

scelte possibili tra i non europei.
Quindi abbiamo in realtà

$$2 \cdot (84 \cdot 21) + 2 \cdot (126 \cdot 35) = 12.348$$

Sommiamo i casi perché appunto abbiamo 4 casi distinti, ma non è applicabile il metodo delle scelte successive poiché il numero di scelte possibili per ogni singolo evento è legato all'evento stesso, in particolare, è in funzione del numero di europei. Insomma, non sono scelte collegate l'una con l'altra. A questo punto diventa chiara la richiesta del quesito, ovvero: calcolare la sommatoria di tutte le possibili scelte per ogni caso possibile.

11.4 Principio delle gabbie e dei piccioni

Per risolvere questo esercizio, vedere il punto 4.3.7

11.4.1 Fioraio (principio delle gabbie e dei piccioni, combinazioni semplici e con ripetizioni)

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 il 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. Vogliamo calcolare quanti modi possibili abbiamo per abbinare 2 colori diversi tra loro. Quindi non ammettiamo ripetizioni e non ci interessa l'ordine perché ad esempio un mazzo "rosso-rosa" è uguale ad un mazzo "rosa-rosso". I colori da cui possiamo scegliere sono 5. Calcoliamo quindi la combinazione semplice:

$$\binom{5}{2} = \frac{5!}{2! \cdot (5-2)!} = \frac{\cancel{5!}}{2! \cdot \cancel{3!}} = \frac{\cancel{4} \cdot 5}{\cancel{2}} = 2 \cdot 5 = 10$$

   Si sottintende un mazzo formato da 2 rose. Se avessimo un mazzo formato da un numero pari di rose, il calcolo cambierebbe.

2. Qui possiamo usare il principio delle gabbie e dei piccioni. Assumendo il caso peggiore in cui il fioraio faccia di tutto per darci tutte le rose di un colore diverso, sappiamo per certo che dalla 6° rosa in poi sarà costretto a darcene una che abbia un colore uguale a una di quelle che ci ha già dato. Usando la formula $n \cdot (k-1) + 1$ abbiamo:

$$5 \cdot (5-1) + 1 = 21$$

   Qualunque mazzo con un numero di rose ≥ 21 ha almeno 5 rose dello stesso colore.

3. Qui non conta l'ordine, ma possono esserci ripetizioni. Infatti non possiamo avere mazzi con tutte le rose dello stesso colore, ma dobbiamo avere più rose dello stesso colore nello stesso mazzo.
   Dalle 12 rose su cui dobbiamo operare una scelta, dobbiamo sottrarre 5, perché su ognuna di queste 5 rose sarà assegnato un colore diverso così che queste 5 rappresentino tutti e 5 i colori, rispettando così il vincolo della richiesta. Sulle restanti 7 rose, dobbiamo trascurare l'ordine ma imporre ripetizioni. Calcoliamo quindi una combinazione con ripetizione:

$$C'_{5,7} = C_{7+5-1,5-1} = \frac{(7+5-1)!}{(5-1)! \cdot 7!} = \frac{\cancel{11!}}{4! \cdot \cancel{7!}} = \frac{\cancel{8} \cdot \cancel{9} \cdot \cancel{10} \cdot 11}{\cancel{2} \cdot \cancel{3} \cdot \cancel{4}} = 2 \cdot 3 \cdot 5 \cdot 11 = 330$$

   Possiamo quindi comporre 330 mazzi diversi.

11.5 Anagrammi

Per risolvere questo esercizio vedere il punto 4.6.5

11.5.1 Anagrammi con lettere ripetute.

Calcolare il numero degli anagrammi delle parole seguenti:

1. ALGORITMO
2. INFORMATICA
3. TORINO
4. DISPOSIZIONI
5. COROLLARIO

Soluzione:
Questi sono tutti anagrammi con parole ripetute.

1. Per ALGORITMO abbiamo:
$$\frac{9!}{2!} = \frac{9!}{2} = 181.440$$
dove 9 è il numero di lettere e 2 rappresenta la lettera O, ripetuta 2 volte.

2. $\dfrac{11!}{2! \cdot 2!} = 9.979.200$ 3. $\dfrac{6!}{2!} = 360$ 4. $\dfrac{12!}{4! \cdot 2! \cdot 2!} = 4.989.600$ 5. $\dfrac{10!}{3! \cdot 2! \cdot 2!} = 151.200$

12 Esercizi sui numeri interi (sezione 5)

12.1 Divisione euclidea

Per risolvere questo esercizio vai ai punti 5.2 e 5.2.4

12.1.1 Divisione euclidea

Calcolare la divisione euclidea per le seguenti coppie di dividendo a e divisore b:

1. $a = 26.754, b = -307$
2. $a = -29.244, b = 289$
3. $a = 781.116, b = 1.101$

Soluzione (*q è il quoziente ed r è il resto*) :

1. $q = -87, r = 45$ 2. $q = -102, r = 234$ 3. $q = 709, r = 507$

12.2 MCD e Identità di Bézout

Per risolvere questi esercizi, guarda i punti 5.2.7 e 5.2.8

12.2.1 MCD e identità di Bézout

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE

(è troppo grande per una sola pagina)

Calcolare i seguenti massimi comuni denominatori (*anche detti massimi comuni divisori o più semplicemente MCD*) e realizzare l'identità di Bézout:

1. MCD(1.156, 75)
2. MCD(1.377, 1.071)
3. MCD, (3.973, 1.853)
4. MCD(26.125, 17.043)
5. MCD(40.257, 5.439)
6. MCD(153.664, 24.321)

1. MCD(1.156,75):

$1.156 = 15 \cdot 75 + 31$
$75 = 2 \cdot 31 + 13$
$31 = 2 \cdot 13 + 5$
$13 = 2 \cdot 5 + 3$
$5 = 1 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

$$
\begin{aligned}
1 &= 3-1\cdot 2= \\
&= (13-2\cdot 5) - 1\cdot(5-1\cdot 3) = \\
&= (75-2\cdot 31) - 2\cdot 5 - 1\cdot 5 + 1\cdot(13-2\cdot 5) = \\
&= 75-2\cdot 31-2\cdot 5-1\cdot 5+13-2\cdot 5= \\
&= 75-2\cdot 31-2\cdot(31-2\cdot 13) - 1\cdot(31-2\cdot 13)+13-2\cdot 5= \\
&= 75-2\cdot 31-2\cdot 31+4\cdot 13-1\cdot 31+2\cdot 13+13-2\cdot 5= \\
&= 75-5\cdot 31+7\cdot 13-2\cdot 5= \\
&= 75-5\cdot 31+7\cdot 13-2\cdot(31-2\cdot 13) = \\
&= 75-5\cdot 31+7\cdot 13-2\cdot 31+4\cdot 13= \\
&= 75-7\cdot 31+11\cdot 13= \\
&= 75-7\cdot 31+11\cdot(75-2\cdot 31) = \\
&= 75-7\cdot 31+11\cdot 75-22\cdot 31= \\
&= 75-29\cdot 31+11\cdot 75= \\
&= 75-29\cdot(1.156-15\cdot 75) + 11\cdot 75= \\
&= 75-29\cdot 1.156+435\cdot 75+11\cdot 75= \\
&= 447\cdot 75-29\cdot 1.156=1
\end{aligned}
$$

---

2. MCD(1.377,1.071):

$1.377 = 1 \cdot 1.071 + 306$
$1071 = 3 \cdot 306 + 153$
$306 = 2 \cdot 153 + 0$

$$
\begin{aligned}
153 &= 1071-3\cdot 306= \\
&= 1071-3\cdot(1.377-1\cdot 1.071) = \\
&= 1071-3\cdot 1.377+3\cdot 1.071= \\
&= 4\cdot 1.071-3\cdot 1.377=153
\end{aligned}
$$

---

3. MCD(3.973,1.853): 3.973= 2·1.853+267 1.853= 6·267+251 267= 1·251+16 251= 15·16+11 16= 1·11+5 11= 2·5+1 5= 5·1+0	1=11−2·5= = (251−15·16) − 2 · (16−1·11) = =251−15·16−2·16+2·11= =251−17·16+2·11= =251−17·16+2 · (251−15·16) = =251−17·16+2·251−30·16= =3·251−47·16= =3·251−47 · (267−1·251) = =3·251−47·267+47·251= =50·251−47·267= =50·251−47 · (3.973−2·1.853) = =50·251−47·3.973+94·1.853= =50 · (1.853−6·267) − 47·3.973+94·1.853= =50·1.853−300·267−47·3.973+94·1.853= =144·1.853−300·267−47·3.973= =144·1.853−300 · (3.973−2·1.853) − 47·3.973= =144·1.853−300·3.973+600·1.853−47·3.973= =744·1.853−347·3.973=1
4. MCD(26.125,17.043): 26.125= 1·17.043+9.082 17.043= 1·9.082+7.961 9.082= 1·7.961+1.121 7.961= 7·1.121+114 1.121= 9·114+95 114= 1·95+19 95= 5·19+0	19=114−1·95= = (7.961−7·1.121) − 1 · (1.121−9·114) = =7.961−7·1.121−1·1.121+9·114= =7.961−8·1.121+9·114= =7.961−8·1.121+9 · (7.961−7·1.121) = =7.961−8·1.121+9·7.961−63·1.121= =10·7.961−71·1.121= =10 · (17.043−1·9.082) − 71 · (9.082−1·7.961) = =10·17.043−10·9.082−71·9.082+71·7.961= =10·17.043−81·9.082+71·7.961= =10·17.043−81·9.082+71 · (17.043−1·9.082) = =10·17.043−81·9.082+71·17.043−71·9.082= =81·17.043−152·9.082= =81·17.043−152 · (26.125−1·17.043) = =81·17.043−152·26.125+152·17.043= =233·17.043−152·26.125=19
5. MCD(40.257,5.439): 40.257= 7·5.439+2.184 5.439= 2·2.184+1.071 2.184= 2·1.071+42 1.071= 25·42+21 42= 2·21+0	21=1.071−25·42= = (5.439−2·2.184) − 25 · (2.184−2·1.071) = =5.439−2·2.184−25·2.184+50·1.071= =5.439−27·2.184+50·1.071= =5.439−27·2.184+50 · (5.439−2·2.184) = =5.439−27·2.184+50·5.439−100·2.184= =51·5.439−127·2.184= =51·5.439−127 · (40.257−7·5.439) = =51·5.439−127·40.257+889·5.439= =940·5.439−127·40.257=21

6. MCD(153.664,24.321):

$153.664 = 6 \cdot 24.321 + 7.738$
$24.321 = 3 \cdot 7.738 + 1.107$
$7.738 = 6 \cdot 1.107 + 1.096$
$1.107 = 1 \cdot 1.096 + 11$
$1.096 = 99 \cdot 11 + 7$
$11 = 1 \cdot 7 + 4$
$7 = 1 \cdot 4 + 3$
$4 = 1 \cdot 3 + 1$
$3 = 3 \cdot 1 + 0$

$1 = 4 - 1 \cdot 3 =$
$= (11 - 1 \cdot 7) - 1 \cdot (7 - 1 \cdot 4) =$
$= 11 - 1 \cdot 7 - 1 \cdot 7 + 1 \cdot 4 =$
$= 11 - 2 \cdot 7 + 1 \cdot 4 =$
$= 11 - 2 \cdot 7 + 1 \cdot (11 - 1 \cdot 7) =$
$= 11 - 2 \cdot 7 + 1 \cdot 11 - 1 \cdot 7 =$
$= 2 \cdot 11 - 3 \cdot 7 =$
$= 2 \cdot (1.107 - 1 \cdot 1.096) - 3 \cdot (1.096 - 99 \cdot 11) =$
$= 2 \cdot 1.107 - 2 \cdot 1.096 - 3 \cdot 1.096 + 297 \cdot 11 =$
$= 2 \cdot 1.107 - 5 \cdot 1.096 + 297 \cdot 11 =$
$= 2 \cdot 1.107 - 5 \cdot 1.096 + 297 \cdot (1.107 - 1 \cdot 1.096) =$
$= 2 \cdot 1.107 - 5 \cdot 1.096 + 297 \cdot 1.107 - 297 \cdot 1.096 =$
$= 299 \cdot 1.107 - 302 \cdot 1.096 =$
$= 299 \cdot (24.321 - 3 \cdot 7.738) - 302 \cdot (7.738 - 6 \cdot 1.107) =$
$= 299 \cdot 24.321 - 897 \cdot 7.738 - 302 \cdot 7.738 + 1.812 \cdot 1.107 =$
$= 299 \cdot 24.321 - 1.199 \cdot 7.738 + 1.812 \cdot 1.107 =$
$= 299 \cdot 24.321 - 1.199 \cdot 7.738 + 1.812 \cdot (24.321 - 3 \cdot 7.738) =$
$= 299 \cdot 24.321 - 1.199 \cdot 7.738 + 1.812 \cdot 24.321 - 5.436 \cdot 7.738 =$
$= 2.111 \cdot 24.321 - 6.635 \cdot 7.738 =$
$= 2.111 \cdot 24.321 - 6.635 \cdot (153.664 - 6 \cdot 24.321) =$
$= 2.111 \cdot 24.321 - 6.635 \cdot 153.664 + 39.810 \cdot 24.321 =$
$= 41.921 \cdot 24.321 - 6.635 \cdot 153.664 = 1$

12.2.2 Identità di Bézout

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

1. $8X - 11Y = 6$
2. $15X - 6Y = 42$
3. $9X - 12 = 22$
4. $28X + 49Y = 91$

Per risolvere questo esercizio, è sufficiente calcolare l'MCD. Se l'MCD divide il termine noto, allora l'equazione ammette soluzioni.

1. MCD(11,8): $11 = 1 \cdot 8 + 3$ $8 = 2 \cdot 3 + 2$ $3 = 1 \cdot 2 + 1$ $2 = 2 \cdot 1 + 0$ $6 : 1 = 6$ *l'equazione ammette soluzioni.*	2. MCD(15,6): $15 = 2 \cdot 6 + 3$ $6 = 2 \cdot 3 + 0$ $42 : 3 = 14$ *l'equazione ammette soluzioni.*
3. MCD(12,9): $12 = 1 \cdot 9 + 3$ $9 = 3 \cdot 3 + 0$ $22 : 3 = 7,\overline{3}$ *l'equazione **non** ammette soluzioni.*	4. MCD(49,28): $49 = 1 \cdot 28 + 21$ $28 = 1 \cdot 21 + 7$ $21 = 3 \cdot 7 + 0$ $91 : 7 = 13$ *l'equazione ammette soluzioni.*

12.3 Basi numeriche

Per risolvere questi esercizi vedere nella teoria i punti 5.2.2, 5.2.3 e 5.2.5

12.3.1 Da una base n alla base 10

Convertire in base 10 i seguenti numeri scritti nelle basi indicate:
Per gli ultimi 2 possiamo usare la tabella nel punto 5.2.2
Quindi abbiamo $A = 10$, $B = 11$, $C = 12$ *ed* $E = 14$.

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

$11001_{[2]} = 1_0 \cdot 2^0 + 0_1 \cdot 2^1 + 0_2 \cdot 2^2 + 1_3 \cdot 2^3 + 1_4 \cdot 2^4 =$ $= 1 + 2^3 + 2^4 = 25_{[10]}$	$20110_{[3]} = 0_0 \cdot 3^0 + 1_1 \cdot 3^1 + 1_2 \cdot 3^2 + 0_3 \cdot 3^3 + 2_4 \cdot 3^4 =$ $= 3 + 3^2 + 2 \cdot 3^4 = 174_{[10]}$
$13203_{[4]} = 3_0 \cdot 4^0 + 0_1 \cdot 4^1 + 2_2 \cdot 4^2 + 3_3 \cdot 4^3 + 1_4 \cdot 4^4 =$ $= 3 + 2 \cdot 4^2 + 3 \cdot 4^3 + 4^4 = 483_{[10]}$	$14403_{[5]} = 3_0 \cdot 5^0 + 0_1 \cdot 5^1 + 4_2 \cdot 5^2 + 4_3 \cdot 5^3 + 1_4 \cdot 5^4 =$ $= 3 \cdot 1 + 4 \cdot 5^2 + 4 \cdot 5^3 + 5^4 = 1.228_{[10]}$
$25034_{[6]} = 4_0 \cdot 6^0 + 3_1 \cdot 6^1 + 0_2 \cdot 6^2 + 5_3 \cdot 6^3 + 2_4 \cdot 6^4 =$ $= 4 + 3 \cdot 6 + 5 \cdot 6^3 + 2 \cdot 6^4 = 3.694_{[10]}$	$57704_{[8]} = 4_0 \cdot 8^0 + 0_1 \cdot 8^1 + 7_2 \cdot 8^2 + 7_3 \cdot 8^3 + 5_4 \cdot 8^4 =$ $= 4 + 7 \cdot 8^2 + 7 \cdot 8^3 + 5 \cdot 8^4 = 24.516_{[10]}$
$1BA8_{[12]} = 8_0 \cdot 12^0 + 10_1 \cdot 12^1 + 11_2 \cdot 12^2 + 1_3 \cdot 12^3 =$ $= 8 + 10 \cdot 12 + 11 \cdot 12^2 + 12^3 = 3.440_{[10]}$	
$E1C45_{[16]} = 5_0 \cdot 16^0 + 4_1 \cdot 16^1 + 12_2 \cdot 16^2 + 1_3 \cdot 16^3 + 14_4 \cdot 16^4 =$ $= 5 + 4 \cdot 16 + 12 \cdot 16^2 + 1 \cdot 16^3 + 14 \cdot 16^4 = 924.741_{[10]}$	

12.3.2 Dalla base 10 ad una base n

Convertire nelle basi indicate, i numeri scritti in base 10
ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE
(è troppo grande per una sola pagina)

1. Base 2: 570, 2.095, 11.003
2. Base 3: 198, 1.532, 10.707
3. Base 4: 221, 3.037, 17.627
4. Base 8: 617, 4.038, 21.639
5. Base 12: 455, 6.169, 37.093
6. Base 16: 331, 4.773, 35

1. $570=285\cdot 2+0_0$
$285=142\cdot 2+1_1$
$142=71\cdot 2+0_2$
$71=35\cdot 2+1_3$
$35=17\cdot 2+1_4$
$17=8\cdot 2+1_5$
$8=4\cdot 2+0_6$
$4=2\cdot 2+0_7$
$2=1\cdot 2+0_8$
$1=0\cdot 2+1_9$
1000111010

$2.095=1.047\cdot 2+1_0$
$1.047=523\cdot 2+1_1$
$523=261\cdot 2+1_2$
$261=130\cdot 2+1_3$
$130=65\cdot 2+0_4$
$65=32\cdot 2+1_5$
$32=16\cdot 2+0_6$
$16=8\cdot 2+0_7$
$8=4\cdot 2+0_8$
$4=2\cdot 2+0_9$
$2=1\cdot 2+0_{10}$
$1=0\cdot 2+1_{11}$
100000101111

$11.003=5.501\cdot 2+1_0$
$5.501=2.750\cdot 2+1_1$
$2.750=1.375\cdot 2+0_2$
$1.375=687\cdot 2+1_3$
$687=343\cdot 2+1_4$
$343=171\cdot 2+1_5$
$171=85\cdot 2+1_6$
$85=42\cdot 2+1_7$
$42=21\cdot 2+0_8$
$21=10\cdot 2+1_9$
$10=5\cdot 2+0_{10}$
$5=2\cdot 2+1_{11}$
$2=1\cdot 2+0_{12}$
$1=0\cdot 2+1_{13}$
10101011111011

---

2. $198=66\cdot 3+0_0$
$66=22\cdot 3+0_1$
$22=7\cdot 3+1_2$
$7=2\cdot 3+1_3$
$2=0\cdot 3+2_4$
21100

$1.532=510\cdot 3+2_0$
$510=170\cdot 3+0_1$
$170=56\cdot 3+2_2$
$56=18\cdot 3+2_3$
$18=6\cdot 3+0_4$
$6=2\cdot 3+0_5$
$2=0\cdot 3+2_6$
2002202

$10.707=3.569\cdot 3+0_0$
$3.569=1.189\cdot 3+2_1$
$1.189=396\cdot 3+1_2$
$396=132\cdot 3+0_3$
$132=44\cdot 3+0_4$
$44=14\cdot 3+2_5$
$14=4\cdot 3+2_6$
$4=1\cdot 3+1_7$
$1=0\cdot 3+1_8$
112200120

---

3. $221=55\cdot 4+1_0$
$55=13\cdot 4+3_1$
$13=3\cdot 4+1_2$
$3=0\cdot 4+3_3$
3131

$3.037=759\cdot 4+1_0$
$759=189\cdot 4+3_1$
$189=47\cdot 4+1_2$
$47=11\cdot 4+3_3$
$11=2\cdot 4+3_4$
$2=0\cdot 4+2_5$
233131

$17.627=4.406\cdot 4+3_0$
$4.406=1.101\cdot 4+2_1$
$1.101=275\cdot 4+1_2$
$275=68\cdot 4+3_3$
$68=17\cdot 4+0_4$
$17=4\cdot 4+1_5$
$4=1\cdot 4+0_6$
$1=0\cdot 4+1_7$
10103123

---

4. $617=77\cdot 8+1_0$
$77=9\cdot 8+5_1$
$9=1\cdot 8+1_2$
$1=0\cdot 8+1_3$
1151

$4.038=504\cdot 8+6_0$
$504=63\cdot 8+0_1$
$63=7\cdot 8+7_2$
$7=0\cdot 8+7_3$
7706

$21.639=2.704\cdot 8+7_0$
$2.704=338\cdot 8+0_1$
$338=42\cdot 8+2_2$
$42=5\cdot 8+2_3$
$5=0\cdot 8+5_4$
52207

---

5. $455=37\cdot12+11_0 \rightarrow B_0$
$37=3\cdot12+1_1$
$3=0\cdot12+3_2$
31B

$6.169=514\cdot12+1_0$
$514=42\cdot12+10_1 \rightarrow A_1$
$42=3\cdot12+6_2$
$3=0\cdot12+3_3$
36A1

$37.093=3.091\cdot12+1_0$
$3.091=257\cdot12+7_1$
$257=21\cdot12+5_2$
$21=1\cdot12+9_3$
$1=0\cdot12+1_4$
19571

---

6. $331=20\cdot16+11_0 \rightarrow B_0$
$20=1\cdot16+4_1$
$1=0\cdot16+1_2$
14B

$4.773=298\cdot16+5_0$
$298=18\cdot16+10_1 \rightarrow A_1$
$18=1\cdot16+2_2$
$1=0\cdot16+1_3$
12A5

$35.916=2.244\cdot16+12_0 \rightarrow C_0$
$2.244=140\cdot16+4_1$
$140=8\cdot16+12_2 \rightarrow C_2$
$8=0\cdot16+8_3$
8C4C

12.4 Numeri primi

Per risolvere questo esercizio, utilizza la tabella al punto: 5.4.2

12.4.1 Scomposizione in fattori primi

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

224, 1.584, 6.125, 11.343, 17.901, 37.422, 40.033, 69.629, 81.191

224	2	1.584	2	6.125	5	11.343	3	17.901	3
111	2	792	2	1.225	5	3.781	19	5.967	3
56	2	396	2	245	5	199	199	1.989	3
28	2	198	2	49	7	1		663	3
14	2	99	3	7	7			221	13
7	7	33	3	1				17	17
1		11	11					1	
		1							

37.422	2	40.033	7	69.629	7	81.191	11
18.711	3	5.719	7	9.947	7	7.381	11
6.237	3	817	19	1.421	7	671	11
2.079	3	43	43	203	7	61	61
693	3	1		29	29	1	
231	3			1			
77	7						
11	11						
1							

13 Esercizi sulle permutazioni (sezione 6)

13.1 Composizioni e cicli

13.1.1 Composizione di permutazioni

Per risolvere questo esercizio vedere il punto 6.1.5 nella teoria.
Siano date le seguenti permutazioni in $\mathcal{S}_7$:

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

Calcolare $\sigma^2, \sigma\tau, \tau\sigma, \tau^2, \sigma\tau\sigma, \tau\sigma\tau$
Ricordiamoci che con $\sigma\tau$ si intende $\sigma \circ \tau$ e con σ^2 si intende $\sigma \circ \sigma$.

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

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

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

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

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

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

13.1.2 Da tabella a cicli disgiunti

Per risolvere questo esercizio, vedere il punto 6.2.5 *nella teoria.*
Determinare la decomposizione in cicli disgiunti delle seguenti permutazioni in $\mathcal{S}_8$:

$$\pi_1 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 5 & 7 & 2 & 6 & 4 & 1 \end{pmatrix} \pi_2 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 2 & 8 & 3 & 5 & 1 & 7 \end{pmatrix}$$

$$\pi_3 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 7 & 1 & 8 & 4 & 6 \end{pmatrix} \pi_4 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 7 & 8 & 2 & 5 & 1 & 4 \end{pmatrix}$$

Per π_1 notiamo che 6 va in se stesso. Per tutti gli altri, scriviamo il loro percorso. Iniziamo per comodità da 1:

$$(1\ 3\ 5\ 2\ 8)$$

Notiamo che ci mancano ancora dei numeri. Ricominciamo da 4 (*anche qui si può ripartire da un qualunque numero mancante*):

$$(4\ 7)$$

Abbiamo finito. Abbiamo quindi:

$$(1\ 3\ 5\ 2\ 8)(4\ 7)$$

Per le altre permutazioni abbiamo π_2: $(1\ 4\ 8\ 7)(2\ 6\ 5\ 3)$, π_3: $(1\ 5)(2\ 3)(4\ 7)(6\ 8)$, π_4: $(1\ 3\ 7)(2\ 6\ 5)(4\ 8)$

13.2 Scrittura in cicli disgiunti, tipo, parità e periodo

13.2.1 Convertire cicli non disgiunti in cicli disgiunti, tipo e parità

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE

(è troppo grande per una sola pagina)

Per risolvere questo esercizio, vedere i punti 6.2.6, 6.3.5, 6.3.6, 6.3.7

Per ciascuna coppia σ, τ di permutazioni in $\mathcal{S}_n$, calcolare la decomposizione in cicli disgiunti, il tipo e la parità di $\sigma, \tau, \sigma\tau, \tau\sigma$

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:

1. Scriviamo σ e τ in cicli disgiunti e calcoliamo $\sigma\tau$ e $\tau\sigma$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix} = (1\ 5\ 2\ 4\ 3)$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} = (1\ 3\ 5\ 2)$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix} = (2\ 5\ 4\ 3)$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = (1\ 2\ 4\ 5)$$

   I tipi di $\sigma, \tau, \sigma\tau, \tau\sigma$ sono $(5), (4), (4), (4)$ rispettivamente.
   σ è pari mentre $\tau, \sigma\tau, \tau\sigma$ sono dispari.

2. Scriviamo σ e τ in cicli disgiunti e calcoliamo $\sigma\tau$ e $\tau\sigma$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 6 & 3 & 5 \\ 6 & 4 & 1 & 2 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 2 & 3 & 5 \end{pmatrix} = (1\ 6\ 5\ 3)(2\ 4)$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \\ 5 & 4 & 3 & 6 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 2 & 1 \end{pmatrix} = (1\ 5\ 2\ 4\ 6)$$

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

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

   I tipi di $\sigma, \tau, \sigma\tau, \tau\sigma$ sono $(4, 2), (5), (2, 2), (2, 2)$ rispettivamente.
   σ è composto da due cicli con stessa parità, quindi è pari.
   Per lo stesso motivo sono pari anche $\sigma\tau$ e $\tau\sigma$.
   Inoltre τ ha *lunghezza* 5 quindi è pari.

3. Scriviamo σ e τ in cicli disgiunti e calcoliamo $\sigma\tau$ e $\tau\sigma$:
σ è già espresso come composizione di cicli disgiunti. Scriviamo comunque la tabella di σ per facilitare i calcoli.

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

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

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

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

I tipi di $\sigma, \tau, \sigma\tau, \tau\sigma$ sono $(6), (4,3), (2,4), (4,2)$ rispettivamente.
Quindi $\sigma\tau, \tau\sigma$ sono pari, mentre σ, τ sono dispari.

4. Scriviamo σ e τ in cicli disgiunti e calcoliamo $\sigma\tau$ e $\tau\sigma$:

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

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

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

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

I tipi di $\sigma, \tau, \sigma\tau, \tau\sigma$ sono $(9), (8), (2,4,2), (4,2,2)$ rispettivamente.
σ è pari, mentre τ è dispari.
Per $\sigma\tau$ calcoliamo: $P = (2-1) + (4-1) + (2-1) = 5$ quindi $\sigma\tau$ è dispari perché 5 è dispari.
Per $\tau\sigma$ P è sempre uguale a 5, quindi $\tau\sigma$ è dispari.

13.2.2 Parità e periodo di permutazioni

Per risolvere questo esercizio vedere i punti 6.3.7 e 6.4.4
Determinare la parità ed il periodo delle permutazioni in $\mathcal{S}_n$ attraverso il loro tipo:

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:

1. Le permutazioni con tipo $(2, 3, 4)$ hanno $P = (2-1) + (3-1) + (4-1) = 6$ e quindi sono pari.
   Il loro periodo è: $\text{mcm}(2, 3, 4) = 12$
   Le permutazioni con tipo $(3, 3, 3)$ hanno $P = (3-1) + (3-1) + (3-1) = 6$ e quindi sono pari.
   Il loro periodo è: $\text{mcm}(3, 3, 3) = 3$

2. Le permutazioni con tipo $(3, 7)$ sono pari perché 3 e 7 hanno la stessa parità.
   Il loro periodo è: $\text{mcm}(3, 7) = 21$
   Le permutazioni con tipo $(2, 2, 2, 3)$ hanno $P = (2-1) + (2-1) + (2-1) + (3-1) = 5$ e quindi sono dispari.
   Il loro periodo è: $\text{mcm}(2, 2, 2, 3) = 6$

3. Le permutazioni con tipo $(3, 11)$ sono pari perché 3 e 11 hanno la stessa parità.
   Il loro periodo è: $\text{mcm}(3, 11) = 33$
   Le permutazioni con tipo $(2, 4, 7)$ hanno $P = (2-1) + (4-1) + (7-1) = 10$ quindi sono pari.
   Il loro periodo è: $\text{mcm}(2, 4, 7) = 28$
   Le permutazioni con tipo $(4, 4, 6)$ hanno $P = (4-1) + (4-1) + (6-1) = 11$ quindi sono dispari.
   Il loro periodo è: $\text{mcm}(4, 4, 6) = 12$

4. Le permutazioni con tipo $(3, 5, 6, 6)$ hanno $P = (3-1) + (5-1) + (6-1) + (6-1) = 16$ quindi sono pari.
   Il loro periodo è: $\text{mcm}(3, 5, 6, 6) = 30$
   Le permutazioni con tipo $(8, 12)$ sono pari perché 8 e 12 hanno la stessa parità.
   Il loro periodo è: $\text{mcm}(8, 12) = 24$
   Le permutazioni con tipo $(2, 2, 2, 2, 2, 2, 3, 4)$ hanno $P = 6 \cdot (2-1) + (3-1) + (4-1) = 11$ quindi sono dispari.
   Il loro periodo è: $\text{mcm}(2, 2, 2, 2, 2, 2, 3, 4) = 12$

13.3 Numero di cicli, numero di permutazioni (cardinalità)

13.3.1 Numero di cicli nell'insieme delle permutazioni

Per risolvere questo esercizio, vedere nella teoria il punto 6.2.8
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:

1. Abbiamo:
   $$\frac{1}{4} D_{7,4} = \frac{1}{4} \cdot \frac{7!}{(7-4)!} = \frac{\cancel{7!}}{\cancel{4 \cdot 3!}} = 5 \cdot 6 \cdot 7 = 210$$
   cicli di lunghezza 4 in $\mathcal{S}_7$.

2. Abbiamo:
   $$\frac{1}{6} D_{8,6} = \frac{1}{6} \cdot \frac{8!}{(8-6)!} = \frac{\cancel{8!}}{\cancel{6 \cdot 2}} = 3 \cdot 4 \cdot 5 \cdot 7 \cdot 8 = 3.360$$
   cicli di lunghezza 6 in $\mathcal{S}_8$.

3. Abbiamo:
   $$\frac{1}{10} D_{13,10} = \frac{1}{10} \cdot \frac{13!}{(13-10)!} = \frac{13!}{10 \cdot 3!} = 103.783.680$$
   cicli di lunghezza 10 in $\mathcal{S}_{13}$.

13.3.2 Numero di permutazioni in base al tipo

Per risolvere questo esercizio, vedere il punto 6.2.9
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:

1. Per calcolare il numero di permutazioni di tipo $(2,3)$ in $\mathcal{S}_6$, riscriviamo il tipo come $(2,3,1)$ per ottenere $2+3+1=6$.
   Dopodiché applichiamo la formula:
   $$\frac{\cancel{6!}}{\cancel{2\cdot 3\cdot 1}} = 4\cdot 5\cdot 6 = 120$$
2. Il numero di permutazioni di tipo $(2,2,4)$ in $\mathcal{S}_8$ è:
   $$\frac{\cancel{8!}}{\cancel{2^2\cdot 4\cdot 2!}} = 2\cdot 3\cdot 5\cdot 6\cdot 7 = 1.260$$
3. Per calcolare il numero di permutazioni di tipo $(3,3)$ in $\mathcal{S}_9$, riscriviamo il tipo come $(3,3,1,1,1)$.
   Applichiamo la formula:
   $$\frac{\cancel{9!}}{\cancel{3^2\cdot 2!\cdot 1^3\cdot 3!}} = 2\cdot 5\cdot 6\cdot 7\cdot 8 = 3.360$$
4. Per calcolare il numero di permutazioni di tipo $(2,4,5)$ in $\mathcal{S}_{12}$, riscriviamo il tipo come $(2,4,5,1)$:
   $$\frac{12!}{2\cdot 4\cdot 5\cdot 1} = 11.975.040$$
5. Il numero di permutazioni di tipo $(3,3,4,4)$ in $\mathcal{S}_{14}$ è:
   $$\frac{14!}{3^2\cdot 4^2\cdot 2!\cdot 2!} = 151.351.200$$

14 Esercizi sui gruppi (sezione 7)

14.1 Verifica di sottogruppi

14.1.1 Verifica dei sottogruppi del gruppo prodotto

Per risolvere questo esercizio, vedi i punti 3.5.4, 7.1.6 e 7.2.2
Nel gruppo prodotto $\mathbb{R} \times \mathbb{R}$ dire quali dei seguenti sottoinsiemi sono sottogruppi e quali no.

1. $A = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = 2 \cdot x\}$
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:
Innanzitutto, per quanto detto nella teoria, il gruppo prodotto $\mathbb{R} \times \mathbb{R}$ opera tra i gruppi $(\mathbb{R}, +)$ e $(\mathbb{R}, +)$.
Indico con $(\mathbb{R} \times \mathbb{R}, \bullet)$ il gruppo prodotto, con H invece indico un sottogruppo qualunque.
L'elemento neutro in $(\mathbb{R}, +)$ è 0, abbiamo quindi $(0, 0)$ come elemento neutro in $\mathbb{R} \times \mathbb{R}$.
Per ogni $(x, y) \in H$ deve esistere un $(x', y') \in H$ tale che:

$$(x, y) \bullet (x', y') = (0, 0) \in H$$

La condizione impone quindi di verificare che $(0, 0)$ sia presente in H.
Inoltre, controlliamo che per ogni $(x, y), (x', y') \in H$, $(x, y) \bullet (x', y')$ rimanga sempre in H.

1. Verifichiamo che $(0, 0) \in A$:
   Ci stiamo chiedendo se $(x, 2 \cdot x) = (0, 0)$, ovvero, se fissato $x = 0$, vale $2 \cdot x = 0$.
   La condizione è soddisfatta.
   Dopodiché, per ogni $(x, 2 \cdot x) \in A$ deve esistere un $(x', 2 \cdot x') \in A$ tale che:

   $$(x, 2 \cdot x) \bullet (x', 2 \cdot x') = (0, 0)$$

   La condizione è rispettata per ogni coppia, perché siccome $2 \cdot x$ conserva il segno di x, per ogni x positivo, esiste un x negativo sempre nell'insieme A, ovvero:

   $$(x, 2 \cdot x) \bullet (-x, -2 \cdot x) = (0, 0)$$

   vale per ogni x. Quindi per ogni x esiste un $-x \in A$.
   Inoltre, prese 2 coppie qualunque $(x, 2 \cdot x), (x', 2 \cdot x') \in A$ abbiamo:

   $$(x, 2 \cdot x) \bullet (x', 2 \cdot x') = (x + x', 2 \cdot (x + x'))$$

   $(x + x', 2 \cdot (x + x')) \in A$ vale sempre poiché $(x + x', 2 \cdot (x + x'))$ rispetta il vincolo imposto.
   A è quindi un sottogruppo di $\mathbb{R} \times \mathbb{R}$.

2. $(0, 0)$ esiste in B, poiché la coppia (x, x^2) con $x = 0$ soddisfa la nostra richiesta.
   Tuttavia, x^2 restituisce solo valori positivi o nulli, quindi non possiamo soddisfare:
   $(x, x^2) \bullet (-x, (-x)^2) = (0, 0)$ per ogni $x \in B$ (infatti funziona solo con $x = 0$)
   Quindi B *non* è un sottogruppo.

3. Verifichiamo che $(0, 0)$ esiste in C:
   Siccome dobbiamo ottenere una coppia $(x, x + 1) = (0, 0)$ ci stiamo essenzialmente chiedendo se, fissato $x = 0$ sia vero che:
   $x + 1 = 0$, ovvero $0 + 1 = 0$ che è ovviamente impossibile.
   Siccome in C non esiste $(0, 0)$, C non è un sottogruppo.

14.1.2 Verifica dei sottogruppi dei gruppi delle permutazioni

Per risolvere questo esercizio vedi i punti 7.1.7 e 6.1.1
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. $C = \{\pi \in \mathcal{S}_7 | \pi^2 = \text{id}\}$

Soluzione:
Sappiamo che tutti gli S_n sono gruppi con l'operazione di *composizione*. Inoltre, siccome nei 3 quesiti, $n = 7$, sappiamo che il gruppo $(S_7, \circ)$ *non* è commutativo.
Per l'operazione di composizione $\circ$ in S_7 l'elemento neutro è la funzione identità id_7.
La funzione identità è quella permutazione che manda tutto in se stesso.
Puoi pensarla come un ciclo vuoto ( ) oppure, se vuoi esagerare, come ad una roba del genere:
$\text{id}_7 = (1)(2)(3)(4)(5)(6)(7)$
Indichiamo con H un sottogruppo di $(S_7, \circ)$.
Inoltre, sappiamo sempre che per ogni permutazione in S_n esiste sempre una sua inversa nello stesso insieme S_n, quindi non dobbiamo preoccuparci di capire se per una qualunque permutazione π l'inversa esiste, ma dobbiamo solo cercare di capire se questa appartiene all'insieme H.
Per ogni permutazione $\pi \in H$ deve esistere un'altra permutazione $\pi^{-1} \in H$, tale che: $\pi \circ \pi^{-1} = \text{id}_7$
Questo implica che id_7 deve esistere in H ($\text{id}_7 \in H$). In altre parole, per ogni:

$$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \pi(1) & \pi(2) & \pi(3) & \pi(4) & \pi(5) & \pi(6) & \pi(7) \end{pmatrix}$$

deve esistere in H un π^{-1} tale che:

$$\pi^{-1} \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \pi(1) & \pi(2) & \pi(3) & \pi(4) & \pi(5) & \pi(6) & \pi(7) \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \text{id}_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

Se non hai capito quanto appena detto vai a vedere i punti 6.1.3 e 6.1.5
Inoltre, controlliamo che per ogni $\pi, \sigma \in H$, $\pi \circ \sigma$ rimanga sempre in H.

1. Il sottoinsieme A non è un sottogruppo perché non contiene id_7 in quanto id_7 non rispetta il criterio $\pi(4) = 5$.

2. In B esiste id_7 poiché id_7 rispetta il criterio $\pi(6) = 6$. Riflettiamo sull'esistenza della permutazione inversa:
   L'unico vincolo è che tutte le permutazioni in B mandino 6 in se stesso, pertanto una qualunque permutazione inversa (*pensala come la permutazione che rimette tutto al suo posto*) non ha bisogno di *rimettere a posto* anche il 6 perché non è mai stato *toccato*.
   Quindi possiamo dedurre che una qualunque inversa di una permutazione che manda un elemento in se stesso deve a sua volta mandare quell'elemento sempre in se stesso.
   Concludiamo quindi che il vincolo $\pi(6) = 6$ *non* impedisce ad una qualunque inversa π^{-1} di far parte del sottoinsieme.
   Inoltre, presi π_1 e π_2 qualunque, siccome né π_1 né π_2 *toccano* il 6, abbiamo la garanzia che:
   $\pi_1 \circ \pi_2 \in B$ sia sempre vero.
   B è quindi un sottogruppo.

3. In C esiste per forza id_7 poiché in C sono soltanto ammesse le permutazioni per cui vale $\pi \circ \pi = \text{id}_7$.
   Inoltre, sempre per questo fatto, l'inversa di una qualunque permutazione in C è la permutazione stessa, ovvero: $\pi^{-1} = \pi$, quindi l'operazione $\pi \circ \pi^{-1}$ è sempre definita in C.
   Tuttavia, se consideriamo due permutazioni π e σ in C con $\pi \neq \sigma$, notiamo che:
   in generale $\pi \circ \sigma \notin C$ poiché non abbiamo alcuna garanzia del fatto che per la permutazione $\pi \circ \sigma$ valga: $(\pi \circ \sigma)^2 = \text{id}$
   C non e un sottogruppo.

14.1.3 Verifica di sottogruppi astratti

Per risolvere questo esercizio, vedi il punto 3.5.4
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. $C = \{(g, e_G) \in G \times G | g \in G\}$

Soluzione:
Innanzitutto, per quanto detto nella teoria, il gruppo prodotto $G \times G$ opera tra i gruppi $(G, *)$ e $(G, *)$.
Indico con $(G \times G, \bullet)$ il gruppo prodotto. Con H invece indico un sottogruppo qualunque.
L'elemento neutro di $(G \times G, \bullet)$ è (e_G, e_G).
Per ogni $(x, y) \in H$ deve esistere un $(x', y') \in H$ tale che: $(x, y) \bullet (x', y') = e_G \in H$.
La condizione impone quindi di verificare che (e_G, e_G) sia presente in H.
Inoltre, controlliamo che per ogni $(x, y), (x', y') \in H$, $(x, y) \bullet (x', y')$ rimanga sempre in H.
Ricordiamoci che $(G, *)$ è un gruppo e che quindi per definizione, ogni $g \in G$ ha un inverso $g^{-1} \in G$ rispetto all'operazione $*$.

1. $e_G \in G$ e quindi la coppia $(g, g) = (e_G, e_G)$ soddisfa il criterio $g \in G$, pertanto l'elemento neutro esiste in A.
   L'operazione $(g, g) \bullet (g^{-1}, g^{-1}) = (g * g^{-1}, g * g^{-1}) = (e_G, e_G)$ è sempre definita,
   poiché la coppia (g^{-1}, g^{-1}) rispetta i criteri per A.
   Inoltre, presi $(x, x), (y, y) \in A$ qualunque, abbiamo la garanzia che:
   $$(g, g) \bullet (g', g') = (g * g', g * g') = (x, x)$$
   con $x \in G$, quindi (x, x) rispetta i criteri per l'insieme A.
   A è un sottogruppo.

2. $e_G \in G$ inoltre, e_G ha come inverso se stesso, quindi (e_G, e_G) appartiene ad B in quanto soddisfa i criteri.
   Nonostante non ci siano garanzie per il fatto che $(G, *)$ sia o meno abeliano, la definizione di elemento inverso ci rassicura sul fatto che se g ha come inverso g^{-1}, allora g^{-1} è unico e g^{-1} ha a sua volta come inverso g e g è unico. Vale quindi: $g * g^{-1} = g^{-1} * g$.
   Pertanto l'identità: $(g, g^{-1}) \bullet (g^{-1}, g) = (e_G, e_G)$ è sempre definita in B in quanto (g^{-1}, g) rispetta il vincolo per l'insieme B in quanto g è l'inverso di g^{-1}.
   Tuttavia, presi $a, b \in G$ qualunque, l'operazione:
   $$(a, a^{-1}) \bullet (b, b^{-1}) = (a * b, a^{-1} * b^{-1})$$
   non è definita in B, questo perché: $a * b * a^{-1} * b^{-1} \neq e_G$ in quanto non ci sono garanzie che $*$ sia commutativa. In generale:
   $$a * b * a^{-1} * b^{-1} \neq a * a^{-1} * b * b^{-1}$$
   Quindi B non è un sottogruppo.

3. Nulla vieta $g = e_G$, pertanto $(e_G, e_G) \in C$.
   (g^{-1}, e_G) rispetta i criteri per C, pertanto l'operazione $(g, e_G) \bullet (g^{-1}, e_G) = (e_G, e_G)$ è definita in C.
   Inoltre, presi $(g, e_G), (g', e_G) \in C$, allora: $(g, e_G) \bullet (g', e_G) = (g * g', e_G)$ e siccome $g * g' \in G$, risulta una chiusura di C rispetto all'operazione $\bullet$.
   C è un sottogruppo.

Se G fosse stato abeliano, allora B sarebbe stato un sottogruppo, in quanto $a^{-1} + b^{-1}$ sarebbe stato un inverso di $a + b$.

14.2 Dimostrazione sui sottogruppi delle permutazioni.

14.2.1 Proprietà dei gruppi e sottogruppi delle permutazioni

Fissiamo $k \in I_{n+1} = \{1, ..., n+1\}$ e sia $H_k = \{\pi \in \mathcal{S}_{n+1} | \pi(k) = k\}$

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

Soluzione:

1. Dato l'insieme I_{n+1}, vogliamo studiare il suo insieme delle permutazioni S_{n+1}.
   In particolare ci stiamo chiedendo se l'insieme H_k delle permutazioni, che raccoglie tutte le permutazioni di I_{n+1}, eccetto quelle che operano su k sia un sottogruppo dell'insieme di tutte le permutazioni di I_{n+1}.
   Siccome non consideriamo la cardinalità dell'insieme di tutte quelle permutazioni che operano su k, possiamo considerare H_k come l'insieme di tutte le permutazioni dell'insieme $I_{n+1} \setminus \{k\}$. La cardinalità di $I_{n+1} \setminus \{k\}$ è quindi:
   $|I_{n+1} \setminus \{k\}| = n + 1 - 1 = n$, pertanto H_k è a tutti gli effetti l'insieme delle permutazioni S_n, poiché per definizione, possiamo studiare le permutazioni di un insieme attraverso la sua cardinalità. In particolare, H_k e S_n sono legati da una biezione, e siccome H_k e S_n sono entrambi (per definizione) dotati dell'operazione associativa della composizione, tale biezione è a tutti gli effetti un isomorfismo.
   S_n è un sottogruppo di S_{n+1} perché condivide lo stesso elemento neutro (*funzione identità*), è chiuso rispetto all'operazione $\circ$ e per ogni permutazione, esiste la sua inversa.

2. I_{n+1} è composto da elementi distinti, pertanto, così come possiamo definire il sottogruppo H_k di tutte le permutazioni, eccetto per quelle che operano su k, possiamo definire altri sottogruppi con la stessa logica, che però anziché escludere k escludono un altro elemento distinto. Ci sono $n+1$ elementi distinti in I_{n+1} e per ciascuno di loro possiamo definire un sottogruppo H_k.

3. Per definizione ogni insieme delle permutazioni non è vuoto perché contiene la funzione identità, quindi l'intersezione tra tutti gli insiemi H, dove ciascuno di questi esclude le permutazioni che operano su un particolare oggetto di I hanno in comune (per definizione di permutazione e di sottogruppo) la funzione identità.

14.3 Verifica di omomorfismi

14.3.1 Verifica di monomorfismi, epimorfismi e isomorfismi I

Dire quali delle seguenti funzioni $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ sono omomorfismi e quali non lo sono.
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:
Il gruppo $(\mathbb{Z}, +)$ è commutativo e ha come elemento neutro 0.
Il gruppo prodotto $(\mathbb{Z} \times \mathbb{Z}, \bullet)$ ha come elemento neutro $(0, 0)$.
Verifichiamo se $f((m, n) \bullet (a, b)) = f((m, n)) + f((a, b))$
Ricordiamoci che $(m, n) \bullet (a, b) = (m+a, n+b)$, quindi dobbiamo verificare $f((m+a, n+b)) = f((m, n)) + f((a, b))$

1. Abbiamo:
   $f((m + a, n + b)) = m + a + n + b - 1$
   $f((m, n)) + f((a, b)) = m + n - 1 + a + b - 1 = m + a + n + b - 2$
   $f((m + a, n + b)) \neq f((m, n)) + f((a, b))$ quindi f non è un isomorfismo.

2. Abbiamo:
   $f((m + a, n + b)) = (m + a)^2 - (n + b)^2$
   $f((m, n)) + f((a, b)) = m^2 - n^2 - a^2 - b^2$
   $m^2 + 2ma + a^2 - (n^2 + 2nb + b^2) = m^2 + 2ma + a^2 - n^2 - 2nb - b^2$
   $m^2 + 2ma + a^2 - n^2 - 2nb - b^2 \neq m^2 - n^2 - a^2 - b^2$ quindi f non è un isomorfismo.

3. Abbiamo:
   $f((m + a, n + b)) = 2(m + a) - 3(n + b) = 2m + 2a - 3n + 3b$
   $f((m, n)) + f((a, b)) = 2m - 3n + 2a - 3b$
   $\cancel{2m} + \cancel{2a} - \cancel{3n} + \cancel{3b} = \cancel{2m} - \cancel{3n} + \cancel{2a} - \cancel{3b}$
   $0 = 0$
   f è un isomorfismo. Verifichiamo se è iniettivo: Calcoliamo il nucleo:
   Dobbiamo trovare quando $2m - 3n = 0$:
   $2m = 3n$
   Quindi, ogniqualvolta la coppia (m, n) è tale per cui il doppio di m è uguale al triplo di n, allora $f((m, n)) = 0$
   Pertanto, siccome 0 non è l'unica soluzione possibile, allora f non è iniettiva.
   Verifichiamo se è suriettivo:
   Ci stiamo chiedendo se un qualunque numero $a \in \mathbb{Z}$ può essere rappresentato come $2m - 3n$
   $\mathrm{MCD}(2, 3) = 1$ quindi tutti i multipli di 1 possono essere scritti come $2m - 3n$, pertanto f è suriettiva.

14.3.2 Verifica di monomorfismi, epimorfismi e isomorfismi II

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:
Il gruppo $(\mathbb{Z}, +)$ è commutativo e ha come elemento neutro 0.
Il gruppo prodotto $(\mathbb{Z} \times \mathbb{Z}, \bullet)$ ha come elemento neutro $(0, 0)$.
Verifichiamo se $f(n+m) = f(n) \bullet f(m)$

1. Abbiamo:
   $f(n+m) = (n+m-1, n+m+1)$
   $f(n) \bullet f(m) = (n-1, n+1) \bullet (m-1, m+1) = (n+m-2, n+m+2)$
   $(n+m-1, n+m+1) \neq (n+m-2, n+m+2)$ pertanto f non è un omomorfismo.

2. Abbiamo:
   $f(n+m) = (3(n+m), 0) = (3n+3m, 0)$
   $f(n) \bullet f(m) = (3n, 0) \bullet (3m, 0) = (3n+3m, 0)$
   pertanto f è un omomorfismo. Vediamo se è iniettivo. Calcoliamo $\ker(f)$:
   Dobbiamo trovare quando $f(n) = (0, 0)$. Per il secondo elemento della coppia questo è sempre soddisfatto.
   Dobbiamo quindi vedere quando $3n = 0$. Otteniamo $n = 0$ come unica soluzione, pertanto $0 \in \mathbb{Z}$ è l'unica soluzione.
   Quindi f è iniettiva. Verifichiamo se è suriettiva:
   Ci stiamo chiedendo se con $(3n, 0)$ possiamo rappresentare una qualunque coppia in $\mathbb{Z} \times \mathbb{Z}$.
   f non è iniettiva poiché è palese che qualunque coppia $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ con $b \neq 0$ non sia rappresentabile.

3. Abbiamo:
   $f(n+m) = (1, 5(n+m)) = (1, 5n+5m)$
   $f(n) \bullet f(m) = (1, 5n) \bullet (1, 5m) = (2, 5n+5m)$ quindi f non è un omomorfismo.

4. Abbiamo:
   $f(n+m) = (2(n+m), -(n+m))$
   $f(n) \bullet f(m) = (2n, -n) \bullet (2m, -m) = (2n+2m, -n-m) = (2(n+m), -(n+m))$ quindi f è un omomorfismo.
   Vediamo se è iniettivo. Calcoliamo $\ker(f)$: dobbiamo trovare quando $f(n) = (0, 0)$:
   Ci stiamo chiedendo quante (*e quali*) soluzioni ha il sistema:

   $$\begin{cases} 2n = 0 \\ -n = 0 \end{cases}$$

   $2n = 0$ solo quando $n = 0$, vale lo stesso per $-n$. Quindi f è iniettiva perché 0 è l'unica soluzione.
   Vediamo se è suriettivo:
   Ci stiamo chiedendo se con $(2n, -n)$ possiamo rappresentare una qualunque coppia in $\mathbb{Z} \times \mathbb{Z}$.
   Anche qui ci accorgiamo subito che non è possibile, infatti:
   una qualunque coppia $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ con a dispari non è rappresentabile.

14.3.3 Verifica di gruppi e isomorfismi

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 $\omega : (G, *) \to (G, \circ)$ definita da $\omega(g) = g^{-1}$ è un isomorfismo di gruppi.

Soluzione:

1. Dobbiamo verificare se $\circ$ è associativa, ovvero, se

$$(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$$

Sostituiamo $(g_1 \circ g_2)$ con $(g_2 * g_1)$ e $(g_2 \circ g_3)$ con $(g_3 * g_2)$ come da definizione di $\circ$:

$$(g_2 * g_1) \circ g_3 = g_1 \circ (g_3 * g_2)$$

Sostituiamo nuovamente, ovvero scriviamo $(g_2 * g_1) \circ g_3$ come $g_3 * (g_2 * g_1)$ e $g_1 \circ (g_3 * g_2)$ come $(g_3 * g_2) * g_1$:

$$g_3 * (g_2 * g_1) = (g_3 * g_2) * g_1$$

Sappiamo già che $(G, *)$ è un gruppo pertanto sappiamo che qui la proprietà associativa vale, e che quindi conta soltanto l'ordine degli elementi, in quanto fino a prova contraria, $*$ non è commutativa. L'ordine è preservato su entrambi i lati dell'uguaglianza, quindi $\circ$ è associativa.
Dobbiamo inoltre verificare l'esistenza dell'elemento neutro e per $\circ$, ovvero,
preso un $a \in (G, \circ)$ qualunque deve valere:

$$a \circ e = e \circ a = a$$

Siccome per definizione $*$ ha l'elemento neutro, anche se $*$ non è commutativa, per quanto appena visto, la posizione dell'elemento neutro non cambia l'esito dell'operazione.
Quindi di fatto, anche se $\circ$ inverte la posizione degli elementi in $*$, $\circ$ ha come elemento neutro, l'elemento neutro di $*$, ovvero:

$$e_* = e_\circ$$

A questo punto dobbiamo solo assicurarci che ogni elemento in G abbia un inverso rispetto all'operazione $\circ$, ovvero:
preso un $a \in G$ qualunque deve valere:

$$a^{-1} \circ a = a^{-1} \circ b = e \text{ (con } a^{-1} \in G)$$

Anche qui notiamo che l'ordine degli elementi non conta, pertanto ogni elemento di G ha lo stesso elemento neutro, sia per l'operazione $*$ che per l'operazione $\circ$.

2. Per ogni $g \in (G, *)$, ω deve restituire $g^{-1} \in (G, \circ)$. Come visto nella dimostrazione di $(G, \circ)$ non solo $g_*^{-1} = g_\circ^{-1}$, ma l'ordine dell'inverso non conta, infatti: $g^{-1} * g = g * g^{-1} = g \circ g^{-1} = g^{-1} \circ g = e_G$
Perché ω sia un isomorfismo dev'essere sia iniettivo che suriettivo: calcoliamo il nucleo:
Ci stiamo chiedendo quale $g \in (G, *)$ abbia come inverso $g^{-1} = e_G$
Siccome devono valere:

$$g \circ e = e \circ g = g$$
$$g^{-1} \circ g = g \circ g^{-1} = e \text{ (con } g^{-1} \in G)$$

L'unico $g \in (G, *)$ che può soddisfare tali condizioni è $g = e_G$.
Quindi $\ker(\omega) = \{e_G\}$, pertanto ω è iniettivo.
Vogliamo ora verificare se ogniqualvolta $\omega(g) = \omega(a)$, con $g, a \in (G, *)$ allora $g = a$.
Questo fatto si verifica banalmente, dal momento in cui per la definizione di gruppo e più in generale, per la definizione di elemento inverso, se un inverso esiste allora è unico, pertanto due elementi non possono avere la stessa immagine in ω.
Pertanto, ω è un isomorfismo.

15 Esercizi sull'aritmetica modulare (sezione 8)

15.1 Inverso di una classe di resto

Per risolvere questo esercizio, vai al punto 8.2.3

15.1.1 Inverso della classe di resto

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE
(è troppo grande per una sola pagina)
Delle seguenti classi resto dire quali sono invertibili e di quelle invertibili calcolare l'inversa.

1. $[4]_9$
2. $[7]_{15}$
3. $[15]_{24}$
4. $[13]_{36}$
5. $[6]_9$
6. $[9]_{15}$
7. $[9]_{29}$
8. $[23]_{40}$
9. $[7]_{10}$
10. $[9]_{20}$
11. $[18]_{30}$
12. $[35]_{42}$
13. $[8]_{10}$
14. $[9]_{21}$
15. $[19]_{30}$
16. $[17]_{55}$
17. $[2]_{11}$
18. $[7]_{22}$
19. $[11]_{32}$
20. $[39]_{80}$
21. $[7]_{12}$
22. $[10]_{23}$
23. $[3]_{34}$
24. $[10]_{95}$
25. $[6]_{14}$
26. $[5]_{24}$
27. $[10]_{36}$
28. $[71]_{100}$

Soluzione:

1. Per $[4]_9$ abbiamo MCD(9,4)=1
quindi è invertibile:
L'identità di Bézout è: $1= 1\cdot 9-2\cdot 4$
Calcoliamo $-2 : 9 = 9\cdot(-1)+7$
Abbiamo quindi: $[4]_9^{-1}=[7]_9$

2. Per $[7]_{15}$ abbiamo: MCD(15,7):
$15= 2\cdot 7+1$
$7= 7\cdot 1+0$
MCD(15,7)=1 quindi è invertibile:
L'identità di Bézout è: $1= 1\cdot 15-2\cdot 7$
Calcoliamo $-2 : 15 = 15\cdot(-1)+13$
Abbiamo quindi $[7]_{15}^{-1}=[13]_{15}$

3. Per $[15]_{24}$ abbiamo MCD(24,15):
$24= 1\cdot 15+9$
$15= 1\cdot 9+6$
$9= 1\cdot 6+3$
$6= 2\cdot 3+0$
MCD(24,15)=3
quindi $[15]_{24}$ è uno 0-divisiore,
pertanto non è invertibile.

4. Per $[13]_{36}$ abbiamo MCD(36,13):
$36= 2\cdot 13+10$
$13= 1\cdot 10+3$
$10= 3\cdot 3+1$
$3= 3\cdot 1+0$
MCD(36,13)=1 quindi è invertibile:
L'identità di Bézout è:
$1=10-3\cdot 3=$
$=36-2\cdot 13-3\cdot(13-1\cdot 10)=$
$=36-2\cdot 13-3\cdot 13+3\cdot 10=$
$=36-5\cdot 13+3\cdot(36-2\cdot 13)=$
$=36-5\cdot 13+3\cdot 36-6\cdot 13=$
$=4\cdot 36-11\cdot 13=1$
Calcoliamo $-11 : 36 = 36\cdot(-1)+25$
Abbiamo quindi $[13]_{36}^{-1}=[25]_{36}$

5. Per $[6]_9$ abbiamo MCD(9,6):
$9= 1\cdot 6+3$
$6= 2\cdot 3+0$
MCD(9,6)=3
quindi $[6]_9$ è uno 0-divisiore,
pertanto non è invertibile.

6. Per $[9]_{15}$ abbiamo MCD(15,9):
$15= 1\cdot 9+6$
$9= 1\cdot 6+3$
$6= 2\cdot 3+0$
MCD(15,9)=3
quindi $[9]_{15}$ è uno 0-divisiore,
pertanto non è invertibile.

7. Per $[9]_{29}$ abbiamo MCD(29,9):
$29 = 3 \cdot 9 + 2$
$9 = 4 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$
MCD(29,9)=1 quindi è invertibile:
L'identità di Bézout è:
$1 = 9 - 4 \cdot 2 =$
$= 9 - 4 \cdot (29 - 3 \cdot 9) =$
$= 9 - 4 \cdot 29 + 12 \cdot 9 =$
$= -4 \cdot 29 + 13 \cdot 9 = 1$
Abbiamo quindi $[9]_{29}^{-1} = [13]_{29}$

8. Per $[23]_{40}$ abbiamo MCD(40,23):
$40 = 1 \cdot 23 + 17$
$23 = 1 \cdot 17 + 6$
$17 = 2 \cdot 6 + 5$
$6 = 1 \cdot 5 + 1$
$5 = 5 \cdot 1 + 0$
MCD(40,23)=1 quindi è invertibile:
L'identità di Bézout è:
$1 = 6 - 1 \cdot 5 =$
$= (23 - 1 \cdot 17) - 1 \cdot (17 - 2 \cdot 6) =$
$= (23 - 1 \cdot 17) - 1 \cdot 17 + 2 \cdot 6 =$
$= 23 - 1 \cdot 17 - 1 \cdot 17 + 2 \cdot (23 - 1 \cdot 17) =$
$= 23 - 1 \cdot 17 - 1 \cdot 17 + 2 \cdot 23 - 2 \cdot 17 =$
$= 3 \cdot 23 - 4 \cdot 17 =$
$= 3 \cdot 23 - 4 \cdot (40 - 1 \cdot 23) =$
$= 3 \cdot 23 - 4 \cdot 40 + 4 \cdot 23 =$
$= 7 \cdot 23 - 4 \cdot 40 =$
Abbiamo quindi $[23]_{40}^{-1} = [7]_{40}$

9. Per $[7]_{10}$ abbiamo MCD(10,7):
$10 = 1 \cdot 7 + 3$
$7 = 2 \cdot 3 + 1$
$3 = 3 \cdot 1 + 0$
MCD(10,7)=1 quindi è invertibile:
L'identità di Bézout è:
$1 = 7 - 2 \cdot 3 =$
$= 7 - 2 \cdot (10 - 1 \cdot 7) =$
$= 7 - 2 \cdot 10 + 2 \cdot 7 =$
$= 3 \cdot 7 - 2 \cdot 10 = 1$
Abbiamo quindi $[7]_{10}^{-1} = [3]_{10}$

10. Per $[9]_{20}$ abbiamo MCD(20,9):
$20 = 2 \cdot 9 + 2$
$9 = 4 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$
MCD(20,9)=1 quindi è invertibile:
L'identità di Bézout è:
$1 = 9 - 4 \cdot 2 =$
$= 9 - 4 \cdot (20 - 2 \cdot 9) =$
$= 9 - 4 \cdot 20 + 8 \cdot 9 =$
$= +9 \cdot 9 - 4 \cdot 20 = 1$
Abbiamo quindi $[9]_{20}^{-1} = [9]_{20}$

11. Per $[18]_{30}$ abbiamo MCD(30,18):
$30 = 2 \cdot 18 + 12$
$18 = 1 \cdot 12 + 6$
$12 = 2 \cdot 6 + 0$
MCD(30,18)=6
quindi $[18]_{30}$ è uno 0-divisiore,
pertanto non è invertibile.

12. Per $[35]_{42}$ abbiamo MCD(42,35):
$42 = 1 \cdot 35 + 7$
$35 = 5 \cdot 7 + 0$
MCD(42,35)=7
quindi $[35]_{42}$ è uno 0-divisiore,
pertanto non è invertibile.

13. Per $[8]_{10}$ abbiamo MCD(10,8):
$10 = 1 \cdot 8 + 2$
$8 = 4 \cdot 2 + 0$
MCD(10,8)=2
quindi $[8]_{10}$ è uno 0-divisiore,
pertanto non è invertibile.

14. Per $[9]_{21}$ abbiamo MCD(21,9):
$21 = 2 \cdot 9 + 3$
$9 = 3 \cdot 3 + 0$
MCD(21,9)=3
quindi $[9]_{21}$ è uno 0-divisiore,
pertanto non è invertibile.

15. Per $[19]_{30}$ abbiamo MCD(30,19):
$30= 1{\cdot}19+11$
$19= 1{\cdot}11+8$
$11= 1{\cdot}8+3$
$8= 2{\cdot}3+2$
$3= 1{\cdot}2+1$
$2= 2{\cdot}1+0$
MCD(30,19)=1 quindi è invertibile:
L'identità di Bézout è:
$1=3-1{\cdot}2=$
$=11-1{\cdot}8-1{\cdot}2=$
$=11-1\cdot(19-1{\cdot}11)-1{\cdot}2=$
$=11-1{\cdot}19+1{\cdot}11-1{\cdot}2=$
$=2{\cdot}11-1{\cdot}19-1{\cdot}2=$
$=2\cdot(30-1{\cdot}19)-1{\cdot}19-1{\cdot}2=$
$=2{\cdot}30-2{\cdot}19-1{\cdot}19-1{\cdot}2=$
$=2{\cdot}30-3{\cdot}19-1\cdot(8-2{\cdot}3)=$
$=2{\cdot}30-3{\cdot}19-1{\cdot}8+2{\cdot}3=$
$=2{\cdot}30-3{\cdot}19-1\cdot(19-1{\cdot}11)+2{\cdot}3=$
$=2{\cdot}30-3{\cdot}19-1{\cdot}19+1{\cdot}11+2{\cdot}3=$
$=2{\cdot}30-4{\cdot}19+1{\cdot}11+2\cdot(11-1{\cdot}8)=$
$=2{\cdot}30-4{\cdot}19+1{\cdot}11+2{\cdot}11-2{\cdot}8=$
$=2{\cdot}30-4{\cdot}19+3{\cdot}11-2\cdot(19-1{\cdot}11)=$
$=2{\cdot}30-4{\cdot}19+3{\cdot}11-2{\cdot}19+2{\cdot}11=$
$=2{\cdot}30-6{\cdot}19+5{\cdot}11=$
$=2{\cdot}30-6{\cdot}19+5\cdot(30-1{\cdot}19)=$
$=2{\cdot}30-6{\cdot}19+5{\cdot}30-5{\cdot}19=$
$=7{\cdot}30-11{\cdot}19=1$
Calcoliamo $-11 : 30 = 30\cdot(-1)+19$
Abbiamo quindi $[19]_{30}^{-1}=[19]_{30}$

16. Per $[17]_{55}$ abbiamo MCD(55,17):
$55= 3{\cdot}17+4$
$17= 4{\cdot}4+1$
$4= 1{\cdot}1+0$
MCD(55,17)=1 quindi è invertibile:
L'identità di Bézout è:
$1=17-4{\cdot}4=$
$=17-4\cdot(55-3{\cdot}17)=$
$=17-4{\cdot}55+12{\cdot}17=$
$=-4{\cdot}55+13{\cdot}17=1$
Abbiamo quindi $[17]_{55}^{-1}=[13]_{55}$

17. Per $[2]_{11}$ abbiamo MCD(11,2):
$11= 5{\cdot}2+1$
$2= 2{\cdot}1+0$
MCD(11,2)=1 quindi è invertibile:
L'identità di Bézout è:
$1=11-5{\cdot}2$
Calcoliamo $-5 : 11 = 11\cdot(-1)+6$
Abbiamo quindi $[2]_{11}^{-1}=[6]_{11}$

18. Per $[7]_{22}$ abbiamo MCD(22,7):
$22= 3{\cdot}7+1$
$7= 7{\cdot}1+0$
MCD(22,7)=1 quindi è invertibile:
L'identità di Bézout è:
$1=22-3{\cdot}7$
Calcoliamo $-3 : 22 = 22\cdot(-1)+19$
Abbiamo quindi $[7]_{22}^{-1}=[19]_{22}$

19. Per $[11]_{32}$ abbiamo MCD(32,11):
$32= 2{\cdot}11+10$
$11= 1{\cdot}10+1$
$10= 1{\cdot}1+0$
MCD(32,11)=1 quindi è invertibile:
L'identità di Bézout è:
$1=11-1{\cdot}10=$
$=11-1\cdot(32-2{\cdot}11)=$
$=11-1{\cdot}32+2{\cdot}11=$
$=-1{\cdot}32+3{\cdot}11=$
Abbiamo quindi $[11]_{32}^{-1}=[3]_{32}$

20. Per $[39]_{80}$ abbiamo MCD(80,39):
$80= 2{\cdot}39+2$
$39= 19{\cdot}2+1$
$2= 2{\cdot}1+0$
MCD(80,39)=1 quindi è invertibile:
L'identità di Bézout è:
$1=39-19{\cdot}2=$
$=39-19\cdot(80-2{\cdot}39)=$
$=39-19{\cdot}80+38{\cdot}39=$
$=-19{\cdot}80+39{\cdot}39=1$
Abbiamo quindi $[39]_{80}^{-1}=[39]_{80}$

21. Per $[7]_{12}$ abbiamo MCD(12,7):
$12= 1\cdot7+5$
$7= 1\cdot5+2$
$5= 2\cdot2+1$
$2= 2\cdot1+0$
MCD(12,7)=1 quindi è invertibile:
L'identità di Bézout è:
$1=5-2\cdot2=$
$= (12-1\cdot7) - 2\cdot(7-1\cdot5) =$
$=12-1\cdot7-2\cdot7+2\cdot5=$
$=12-3\cdot7+2\cdot5=$
$=12-3\cdot7+2\cdot(12-1\cdot7) =$
$=12-3\cdot7+2\cdot12-2\cdot7=$
$=+3\cdot12-5\cdot7=1$
Calcoliamo $-5 : 12 = 12\cdot(-1) + 7$
Abbiamo quindi $[7]_{12}^{-1} = [7]_{12}$

22. Per $[10]_{23}$ abbiamo MCD(23,10):
$23= 2\cdot10+3$
$10= 3\cdot3+1$
$3= 3\cdot1+0$
MCD(23,10)=1 quindi è invertibile:
L'identità di Bézout è:
$1=10-3\cdot3=$
$=10-3\cdot(23-2\cdot10) =$
$=10-3\cdot23+6\cdot10=$
$=-3\cdot23+7\cdot10=$
Abbiamo quindi $[10]_{23}^{-1} = [7]_{23}$

23. Per $[3]_{34}$ abbiamo MCD(34,3):
$34= 11\cdot3+1$
$3= 3\cdot1+0$
MCD(34,3)=1 quindi è invertibile:
L'identità di Bézout è:
$1=34-11\cdot3$
Calcoliamo $-11 : 34 = 34\cdot(-1) + 23$
Abbiamo quindi $[3]_{34}^{-1} = [23]_{34}$

24. Per $[10]_{95}$ abbiamo MCD(95,10):
$95= 9\cdot10+5$
$10= 2\cdot5+0$
MCD(95,10)=5
quindi $[10]_{95}$ è uno 0-divisiore, pertanto non è invertibile.

25. Per $[6]_{14}$ abbiamo MCD(14,6):
$14= 2\cdot6+2$
$6= 3\cdot2+0$
MCD(14,6)=5
quindi $[6]_{14}$ è uno 0-divisiore, pertanto non è invertibile.

26. Per $[5]_{24}$ abbiamo MCD(24,5):
$24= 4\cdot5+4$
$5= 1\cdot4+1$
$4= 4\cdot1+0$
MCD(24,5)=1 quindi è invertibile:
L'identità di Bézout è:
$1=5-1\cdot4=$
$=5-1\cdot(24-4\cdot5) =$
$=5-1\cdot24+4\cdot5=$
$=-1\cdot24+5\cdot5=$
Abbiamo quindi $[5]_{24}^{-1} = [5]_{24}$

27. Per $[10]_{36}$ abbiamo MCD(36,10):
$36= 3\cdot10+6$
$10= 1\cdot6+4$
$6= 1\cdot4+2$
$4= 2\cdot2+0$
MCD(36,10)=2
quindi $[10]_{36}$ è uno 0-divisiore, pertanto non è invertibile.

28. Per $[71]_{100}$ abbiamo MCD(100,71):
$100= 1\cdot71+29$
$71= 2\cdot29+13$
$29= 2\cdot13+3$
$13= 4\cdot3+1$
$3= 3\cdot1+0$
MCD(100,71)=1 quindi è invertibile:
L'identità di Bézout è:
$1=13-4\cdot3=$
$= (71-2\cdot29) - 4\cdot(29-2\cdot13) =$
$=71-2\cdot29-4\cdot29+8\cdot13=$
$=71-6\cdot29+8\cdot13=$
$=71-6\cdot29+8\cdot(71-16\cdot29) =$
$=-22\cdot29+9\cdot71=$
$=-22\cdot(100-1\cdot71) + 9\cdot71=$
$=-22\cdot100+22\cdot71+9\cdot71=$
$=-22\cdot100+31\cdot71=$
Abbiamo quindi $[71]_{100}^{-1} = [31]_{100}$

15.2 Funzione φ di Eulero

Per risolvere questo esercizio vedere i punti 8.2.5, 8.2.7 e 8.2.8
Utilizza la tabella dei numeri primi al punto 5.4.2 per risolvere più velocemente alcuni punti.

15.2.1 Calcolare $\varphi(n)$

Calcolare il valore $\varphi(n)$ della funzione di Eulero per i seguenti valori di n:
124, 245, 300, 320, 408, 667, 820, 837, 1.350, 1.375, 3.969
Soluzione:
Scomponiamo tutti i numeri:

124	2	245	5	300	5	320	5	408	2	3.969	3
62	2	49	7	60	5	64	2	204	2	1.323	3
31	31	7	7	12	3	32	2	102	2	441	3
1		1		4	2	16	2	51	3	147	3
				2	2	8	2	17	17	49	7
				1		4	2	1		7	7
						2	2			1	
						1					

667	23	820	2	837	3	1.350	5	1.375	5
29	29	410	2	279	3	270	5	275	5
1		205	5	93	3	54	3	55	5
		41	41	31	31	18	3	11	11
		1		1		6	3	1	
						2	2		
						1			

Quindi calcoliamo:
$\varphi(124) = \varphi(2^2 \cdot 31) = \varphi(2^2) \cdot 30 = 2 \cdot 30 = 60$
$\varphi(245) = \varphi(7^2 \cdot 5) = \varphi(7^2) \cdot 4 = 7 \cdot 6 \cdot 4 = 168$
$\varphi(300) = \varphi(5^2 \cdot 3 \cdot 2^2) = \varphi(5^2) \cdot \varphi(2^2) \cdot 2 = 5 \cdot 4 \cdot 2 \cdot 2 = 80$
$\varphi(320) = \varphi(5 \cdot 2^6) = 4 \cdot \varphi(2^6) = 4 \cdot 2^5 = 128$
$\varphi(408) = \varphi(17 \cdot 3 \cdot 2^3) = 16 \cdot 2 \cdot 2^2 = 128$
$\varphi(3.969) = \varphi(7^2 \cdot 3^4) = 7 \cdot 6 \cdot 3^3 \cdot 2 = 2.268$
$\varphi(667) = \varphi(23 \cdot 29) = 22 \cdot 28 = 616$
$\varphi(820) = \varphi(41 \cdot 5 \cdot 2^2) = 40 \cdot 4 \cdot 2 = 320$
$\varphi(837) = \varphi(31 \cdot 3^3) = 30 \cdot 3^2 \cdot 2 = 540$
$\varphi(1.350) = \varphi(5^2 \cdot 3^3 \cdot 2) = 5 \cdot 4 \cdot 3^2 \cdot 2 = 360$
$\varphi(1.375) = \varphi(11 \cdot 5^3) = 10 \cdot 5^2 \cdot 4 = 1.000$

15.3 Congruenze lineari

15.3.1 Risoluzione di congruenze lineari

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE

(è troppo grande per una sola pagina)

Per risolvere questo esercizio, vedere i punti 8.2.3 e 8.3.2

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

1. $3X \equiv 5 \bmod 10$
2. $3X \equiv 8 \bmod 20$
3. $6X \equiv 9 \bmod 30$
4. $6X \equiv 7 \bmod 12$
5. $7X \equiv 2 \bmod 21$
6. $7X \equiv 8 \bmod 40$
7. $8X \equiv 6 \bmod 14$
8. $10X \equiv 6 \bmod 24$
9. $9X \equiv 11 \bmod 54$
10. $2X \equiv 10 \bmod 15$
11. $15X \equiv 5 \bmod 25$
12. $12X \equiv 16 \bmod 64$

1. $3X \equiv 5 \bmod 10$:
   Calcoliamo MCD(10,3):
   $10 = 1 \cdot 3 + 1$
   $3 = 3 \cdot 1 + 0$
   MCD(10,3) $=1$ quindi possiamo procedere:
   L'identità di Bézout è: $1 = 10 - 1 \cdot 3$
   Calcoliamo $-1 : 10 = 10 \cdot (-1) + 9$
   Abbiamo quindi $[3]_{10}^{-1} = [9]_{10}$
   Calcoliamo: $9 \cdot 5 = 45$
   $45 : 10 = 10 \cdot 4 + 5$
   $X \equiv 5 \bmod 10$

2. $3X \equiv 8 \bmod 20$:
   Calcoliamo MCD(20,3):
   $20 = 6 \cdot 3 + 2$
   $3 = 1 \cdot 2 + 1$
   $2 = 1 \cdot 2 + 0$
   MCD(20,3) $=1$
   quindi possiamo procedere:
   L'identità di Bézout è:
   $1 = 3 - 1 \cdot 2 =$
   $= 3 - 1 \cdot (20 - 6 \cdot 3) =$
   $= 3 - 1 \cdot 20 + 6 \cdot 3 =$
   $= -1 \cdot 20 + 7 \cdot 3 = 1$
   Abbiamo quindi $[3]_{20}^{-1} = [7]_{20}$
   Calcoliamo: $7 \cdot 8 = 56$
   $56 : 20 = 20 \cdot 2 + 16$
   $X \equiv 16 \bmod 20$

3. $6X \equiv 9 \bmod 30$:
   Calcoliamo MCD(30,6):
   $30 = 5 \cdot 6 + 0$
   MCD(30,6) $=6$
   6 non divide 9,
   Non esistono soluzioni per X

4. $6X \equiv 7 \bmod 12$:
   Calcoliamo MCD(12,6):
   $12 = 2 \cdot 6 + 0$
   MCD(12,6) $=6$
   6 non divide 7.
   Non esistono soluzioni per X

5. $7X \equiv 2 \bmod 21$:
Calcoliamo MCD(21,7):
$21 = 3 \cdot 7 + 0$
MCD(21,7) $= 7$
7 non divide 2
Non esistono soluzioni per X

6. $7X \equiv 8 \bmod 40$:
Calcoliamo MCD(40,7):
$40 = 5 \cdot 7 + 5$
$7 = 1 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$
MCD(40,7) $= 1$
quindi possiamo procedere:
$1 = 5 - 2 \cdot 2 =$
$= (40 - 5 \cdot 7) - 2 \cdot (7 - 1 \cdot 5) =$
$= 40 - 5 \cdot 7 - 2 \cdot 7 + 2 \cdot 5 =$
$= 40 - 7 \cdot 7 + 2 \cdot 5 =$
$= 40 - 7 \cdot 7 + 2 \cdot (40 - 5 \cdot 7) =$
$= 40 - 7 \cdot 7 + 2 \cdot 40 - 10 \cdot 7 =$
$= -17 \cdot 7 + 3 \cdot 40 = 1$
Calcoliamo:
$-17 : 40 = 40 \cdot (-1) + 23$
$23 \cdot 8 = 184$
$184 : 40 = 40 \cdot 4 + 24$
$X \equiv 24 \bmod 40$

7. $8X \equiv 6 \bmod 14$:
Calcoliamo MCD(14,8):
$14 = 1 \cdot 8 + 6$
$8 = 1 \cdot 6 + 2$
$6 = 3 \cdot 2 + 0$
MCD(14,8) $= 2$
2 divide 6 quindi possiamo procedere:
Dividiamo tutti i termini noti per 2.
Risolviamo: $4X \equiv 3 \bmod 7$:
Calcoliamo MCD(7,4):
$7 = 1 \cdot 4 + 3$
$4 = 1 \cdot 3 + 1$
$3 = 3 \cdot 1 + 0$
MCD(7,4) $= 1$
$1 = 4 - 1 \cdot 3 =$
$= 4 - 1 \cdot (7 - 1 \cdot 4) =$
$= 4 - 1 \cdot 7 + 1 \cdot 4 =$
$= -1 \cdot 7 + 2 \cdot 4 = 1$
Otteniamo quindi la classe di resto $[6]_7$
X ha esattamente 2 soluzioni:
Calcoliamo la seconda soluzione: $6 + 7 = 13$
Le soluzioni sono:
$X \equiv 6 \bmod 14$ e $X \equiv 13 \bmod 14$

8. $10X \equiv 6 \bmod 24$:
Calcoliamo MCD(24,10):
$24 = 2 \cdot 10 + 4$
$10 = 2 \cdot 4 + 2$
$4 = 2 \cdot 2 + 0$
MCD(24,10) $= 2$
2 divide 6 quindi possiamo procedere:
Dividiamo tutti i termini noti per 2.
Risolviamo: $5X \equiv 3 \bmod 12$
Calcoliamo MCD(12,5):
$12 = 2 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$
MCD(12,5) $= 1$
$1 = 5 - 2 \cdot 2 =$
$= 5 - 2 \cdot (12 - 2 \cdot 5) =$
$= 5 - 2 \cdot 12 + 4 \cdot 5 =$
$= -2 \cdot 12 + 5 \cdot 5 = 1$
Calcoliamo $5 \cdot 3 = 15$ quindi: $[15]_{24}$
X ha esattamente 2 soluzioni:
Calcoliamo la seconda soluzione:
$15 + 12 = 27$
Riduciamo la soluzione:
$27 : 24 = 24 \cdot 1 + 3$
Le soluzioni sono:
$X \equiv 15 \bmod 24$ e $X \equiv 3 \bmod 24$

9. $9X \equiv 11 \bmod 54$:
Calcoliamo MCD(54,9):
54= 6·9+0
MCD(54,9) =9
9 non divide 11,
Non esistono soluzioni per X

10. $2X \equiv 10 \bmod 15$:
Calcoliamo MCD(15,2):
15= 7·2+1
2= 2·1+0
MCD(15,2) =1
quindi possiamo procedere:
L'identità di Bézout è: 1=15−7·2
Calcoliamo: $-7 : 15 = 15 \cdot (-1) + 8$
Calcoliamo: $8 \cdot 10 = 80$
Adattiamo la soluzione:
$80 : 15 = 15 \cdot 5 + 5$
$X \equiv 5 \bmod 15$

11. $15X \equiv 5 \bmod 25$:
Calcoliamo MCD(25,15):
25= 1·15+10
15= 1·10+5
10= 2·5+0
MCD(25,15) =5
5 divide 15 quindi possiamo procedere:
Dividiamo tutti i termini noti per 5.
Risolviamo: $3X \equiv 1 \bmod 5$:
Calcoliamo MCD(5,3):
5= 1·3+2
3= 1·2+1
2= 2·1+0
MCD(5,3) =1
1=3−1·2=
=3−1 · (5−1·3) =
=3−1·5+1·3=
=−1·5+2·3=1
Otteniamo quindi la classe di resto $[2]_5$
X ha esattamente 5 soluzioni:
Calcoliamo la seconda soluzione: $2 + 5 = 7$
Calcoliamo la terza soluzione: $7 + 5 = 12$
Calcoliamo la quarta soluzione: $12 + 5 = 17$
Calcoliamo la quinta soluzione: $17 + 5 = 22$
Le soluzioni sono:
$X \equiv 2 \bmod 25$, $X \equiv 7 \bmod 25$,
$X \equiv 12 \bmod 25$,
$X \equiv 17 \bmod 25$ e $X \equiv 22 \bmod 25$

12. $12X \equiv 16 \bmod 64$:
Calcoliamo MCD(64,12):
64= 5·12+4
12= 3·4+0
MCD(64,12) =4
4 divide 16 quindi possiamo procedere:
Dividiamo tutti i termini noti per 4.
Risolviamo: $3X \equiv 4 \bmod 16$:
Calcoliamo MCD(16,3):
16= 5·3+1
3= 3·1+0
MCD(16,3) =1
L'identità di Bézout è: 1=16−5·3
Calcoliamo: $-5 : 16 = 16 \cdot (-1) + 11$
Calcoliamo: $11 \cdot 4 = 44$
Adattiamo la soluzione:
$44 : 16 = 16 \cdot 2 + 12$
X ha esattamente 4 soluzioni:
Calcoliamo la seconda soluzione:
$12 + 16 = 28$
Calcoliamo la terza soluzione:
$28 + 16 = 44$
Calcoliamo la quarta soluzione:
$44 + 16 = 60$
Le soluzioni sono:
$X \equiv 12 \bmod 64$, $X \equiv 28 \bmod 64$,
$X \equiv 44 \bmod 64$ e $X \equiv 60 \bmod 64$

15.4 Applicazioni pratiche

15.4.1 Criteri di divisibilità

Per risolvere questo esercizio, vedere il punto 8.4.1
Dei seguenti numeri, dire quali sono divisibili per $2, 3, 5, 9$ e 11.

1. 372.405.912.042
2. 2.517.090.248.794
3. 74.100.761.224.335
4. 9.113.703.764.402

Soluzione:

1. È divisibile per 2 perché la sua ultima cifra è pari.
   La somma delle sue cifre è:
   $3+7+2+4+0+5+9+1+2+0+4+2=39$
   È divisibile per 3 perché 39 è divisibile per 3.
   non è divisibile per 5 perché
   la sua ultima cifra non è né 5 né 0.
   non è divisibile per 9 perché
   la somma delle sue cifre non è divisibile per 9.
   La somma delle cifre in posizione pari è:
   $2+0+1+5+4+7=19$
   La somma delle cifre in posizione dispari è:
   $4+2+9+0+2+3=20$
   non è divisibile per 11 perché:
   $20-19=1$ e 1 *non* è divisibile per 11.

2. È divisibile per 2.
   la somma delle sue cifre è 58.
   non è divisibile per 3.
   non è divisibile per 5.
   non è divisibile per 9.
   La somma delle cifre in posizioni pari è:
   $4+7+4+0+0+1+2=18$
   La somma delle cifre in posizioni dispari è:
   $9+8+2+9+7+5=40$
   è divisibile per 11 perché $40-18=22$

3. Non è divisibile per 2.
   la somma delle sue cifre è 45.
   è divisibile per 3 .
   è divisibile per 5 perché termina con 5.
   è divisibile per 9.
   La somma delle cifre in posizione pari è:
   $5+3+2+1+7+0+4=22$
   La somma delle cifre in posizione dispari è:
   $3+4+2+6+0+1+7=22$
   non è divisibile per 11.

4. È divisibile per 2.
   la somma delle sue cifre è 47.
   non è divisibile per 3.
   non è divisibile per 5.
   non è divisibile per 9.
   La somma delle cifre in posizione pari è:
   $2+4+6+3+7+1+9=32$
   La somma delle cifre in posizione dispari è:
   $0+4+7+0+3+1=15$
   non è divisibile per 11.

15.4.2 Determinare l'ultima cifra di un numero (classi di resto modulo 10^n)

Per risolvere questo esercizio vedere il punto 8.4.2
Determinare la cifra finale dei seguenti numeri:

$$3^{755.042}, \qquad 3^{905.041} + 7^{448.065}, \qquad 13^{899.243} - 3^{577.097}, \qquad 7^{299.047} - 4^{377.001}$$

Soluzione:
Calcoliamo $\varphi(10) = \varphi(5 \cdot 2) = \varphi(5) \cdot \varphi(2) = (5-1) \cdot (2-1) = 4$

1. Per $3^{755.042}$ calcoliamo
$$3^{755.042 \bmod \varphi(10)} \equiv r \bmod 10$$
Calcoliamo quindi 755.042 mod 4:
$755.042 : 4 = 4 \cdot 188.760 + 2$. Per trovare l'ultima cifra è quindi sufficiente calcolare:
$$3^2 \equiv r \bmod 10$$
$9 : 10 = 10 \cdot 0 + 9$. L'ultima cifra di $3^{755.042}$ è 9.

2. Per $3^{905.041} + 7^{448.065}$ calcoliamo prima le singole cifre e successivamente le sommiamo:
Per $3^{905.041}$ calcoliamo: $905.041 : 4 = 4 \cdot 226.260 + 1$. Quindi risolviamo:
$$3 \equiv r \bmod 10$$
L'ultima cifra di $3^{905.041}$ è 3. Per $7^{448.065}$ calcoliamo:
$448.065 : 4 = 4 \cdot 112.016 + 1$. Quindi risolviamo:
$$7 \equiv r \bmod 10$$
L'ultima cifra di $7^{448.065}$ è 7. La somma è quindi $3 + 7 = 10$, ma siccome a noi interessa solo l'ultima cifra:
L'ultima cifra di $3^{905.041} + 7^{448.065}$ è 0.

3. Usiamo lo stesso approccio del punto precedente. Per $13^{899.243}$ calcoliamo:
$899.243 : 4 = 4 \cdot 224.810 + 3$. Quindi risolviamo:
$$13^3 \equiv r \bmod 10$$
$13^3 : 10 = 10 \cdot 219 + 7$. L'ultima cifra di $13^{899.243}$ è 7.
Per $3^{577.097}$ calcoliamo:
$577.097 : 4 = 4 \cdot 144.274 + 1$. Quindi risolviamo:
$$3 \equiv r \bmod 10$$
L'ultima cifra di $3^{577.097}$ è 3. L'ultima cifra dell'operazione: $13^{899.243} - 3^{577.097}$ è $7 - 3 = 4$

4. Per $7^{299.047}$:
$299.047 : 4 = 4 \cdot 74.761 + 3$. Quindi risolviamo:
$$7^3 \equiv r \bmod 10$$
$7^3 : 10 = 10 \cdot 34 + 3$. L'ultima cifra di $7^{299.047}$ è 3.
Per $4^{377.001}$ calcoliamo:
$377.001 : 4 = 4 \cdot 94.250 + 1$. Quindi risolviamo:
$$4 \equiv r \bmod 10$$
L'ultima cifra di $4^{377.001}$ è 4. L'ultima cifra dell'operazione: $7^{299.047} - 4^{377.001}$ è $7 - 4 = -1$, tuttavia, in quel caso si scalerebbe dell'unità successiva, ripartendo essenzialmente da 9, quindi l'ultima cifra dell'operazione: $7^{299.047} - 4^{377.001}$ è 0.

15.4.3 Determinare le ultime cifre di un numero (classi di resto modulo 10^n)

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE

(è troppo grande per una sola pagina)

Per risolvere questo esercizio, vedere i punti 8.4.2 e 8.3.1

Determinare le due cifre finali dei seguenti numeri:

$$17^{894.283}, \qquad 11^{437.241} + 29^{722.602}, \qquad 35^{396.689}, \qquad 41^{488.936} - 37^{472.288}$$

Soluzione:

Ragionando, possiamo notare che ottenere le ultime cifre di un numero n qualunque, significa il resto r della divisione $n : 10^c$ dove c rappresenta il numero di cifre che vogliamo ottenere. Quindi per le ultime 2 cifre $c = 2$.

1. Per $17^{894.283}$ stiamo cercando $17^{894.283} \equiv r \bmod 10^2$. Questo equivale a:

   $$17^{894.283 \bmod \varphi(10^2)} \equiv r \bmod 10^2$$

   $\varphi(10^2) = \varphi(10 \cdot 10) = \varphi(5^2 \cdot 2^2) = \varphi(5^2) \cdot \varphi(2^2) = [5^{2-1} \cdot (5-1)] \cdot [2^{2-1} \cdot (2-1)] = 5 \cdot 4 \cdot 2 \cdot 1 = 40$
   894.283 mod 40:
   $894.283 : 40 = 40 \cdot 22.357 + 3$
   $894.283 \bmod 40 = 3$. Abbiamo quindi:

   $$17^3 \equiv r \bmod 10^2$$

   Per le proprietà delle congruenze abbiamo che $17^3 \equiv r \bmod 10^2$ se e solo se $r \equiv 17^3 \bmod 10^2$.
   Quindi abbiamo $r = 17^3 \bmod 10^2$:
   $17^3 : 10^2 = 10^2 \cdot 49 + 13$
   $r = 13$
   $17^{894.283}$ termina con le cifre 13.

2. Per $11^{437.241} + 29^{722.602}$ possiamo scomporre il problema trovando prima le ultime 2 cifre di $11^{437.241}$, per poi trovare le ultime 2 cifre di $29^{722.602}$ e sommare insieme i risultati.
   Stiamo cercando $11^{437.241} \equiv r \bmod 10^2$, quindi utilizziamo il valore calcolato precedentemente di $\varphi(10^2) = 40$ e calcoliamo:
   $437.241 : 40 = 40 \cdot 10.931 + 1$. Abbiamo quindi:

   $$11^1 \equiv r \bmod 10^2$$

   Troviamo r:
   $11 : 10^2 = 10^2 \cdot 0 + 11$
   Quindi $11^{437.241}$ termina con il numero 11.
   Per $29^{722.602}$, calcoliamo: $722.602 : 40 = 40 \cdot 18.065 + 2$. Abbiamo quindi

   $$29^2 \equiv r \bmod 10^2$$

   Troviamo r: $29^2 : 10^2 = 10^2 \cdot 8 + 41$
   Quindi $29^{722.602}$ termina con il numero 41.
   Sommiamo: $41 + 11 = 52$. Il numero $11^{437.241} + 29^{722.602}$ termina con le cifre 52.

3. Per $35^{396.689}$, esattamente come per gli altri calcoliamo il nuovo esponente:
   $396.689 : 40 = 40 \cdot 9.917 + 9$. Stiamo quindi cercando:

   $$35^9 \equiv r \bmod 10^2$$

   La calcolatrice non risolve questo tipo di quesito. Pertanto possiamo usare una delle proprietà delle congruenze:
   In particolare, se: $35^9 \equiv r \bmod 10^2$ allora anche $35^8 \cdot 35 \equiv n^8 \cdot n \bmod 10^2$ (se fissiamo $n^9 = r$)
   Abbiamo:
   $35^2 \equiv r \bmod 10^2$
   Abbiamo quindi: $35^2 : 10^2 = 10^2 \cdot 12 = 25$
   Perciò possiamo scrivere $35^7 \cdot 25 \equiv r \bmod 10^2$
   Quindi vale anche $25^2 \equiv r \bmod 10^2$:
   Calcoliamo: $25^2 : 10^2 = 10^2 \cdot 6 + 25$
   Quindi le potenze pari ritornano a 25.
   Pertanto il problema è ridotto a $35 \cdot 25 \equiv r \bmod 10^2$
   Calcoliamo $875 : 10^2 = 10^2 \cdot 8 + 75$
   $35^{396.689}$ termina con le cifre 75.

4. Usiamo lo stesso metodo del punto 2. Iniziamo con $37^{472.288}$:
Calcoliamo $472.288 : 40 = 40 \cdot 11.807 + 8$. Stiamo quindi cercando $37^8 \equiv r \mod 10^2$.
Anche qui la calcolatrice non può gestire numeri così grandi, pertanto, procediamo calcolando:
Per $37^2 \equiv r \mod 10^2$
Abbiamo quindi: $37^2 : 10^2 = 10^2 \cdot 13 + 69$
Per $37^3 \equiv r \mod 10^2$
Abbiamo: $37^3 : 10^2 = 10^2 \cdot 506 + 53$
Per $37^4 \equiv r \mod 10^2$
Abbiamo: $37^4 : 10^2 = 10^2 \cdot 18.741 + 61$
Per $37^6 \equiv r \mod 10^2$
Abbiamo: $37^6 : 10^2 = 10^2 \cdot 25.657.264 + 9$
Lo scopo era quello di identificare un ciclo. Non ci sono riuscito, tuttavia, questo è un buon risultato.
Possiamo quindi scrivere: $69 \cdot 9 \equiv r \mod 10^2$
Calcoliamo $69 \cdot 9 = 621$
$621 : 10^2 = 10^2 \cdot 6 + 21$
$37^{472.288}$ termina con le cifre 21.
Calcoliamo ora le ultime due cifre di $41^{488.936}$:
$488.936 : 40 = 40 \cdot 12.223 + 16$
Stiamo cercando $41^{16} \equiv r \mod 10^2$.
Proviamo a cercare $41^4 \equiv r \mod 10^2$:
$41^4 : 10^2 = 10^2 \cdot 28.257 + 61$
61^4 è già gestibile dalla calcolatrice. Calcoliamo quindi: $61^4 \equiv r \mod 10^2$:
$61^4 : 10^2 = 10^2 \cdot 138.458 + 41$
$41^{488.936}$ termina con le cifre 41.
Abbiamo quindi che la sottrazione $41^{488.936} - 37^{472.288}$ termina con le cifre: $41 - 21 = 20$.

15.4.4 Classi di resto con esponenti grandi

Per risolvere questo esercizio, vedere il punto 8.4.2
Calcolare le seguenti classi resto:

$$\left[3^{207.859}\right]_5, \qquad \left[7^{240.974}\right]_{11}, \qquad \left[6^{66.095}\right]_{14}, \qquad \left[15^{96.603}\right]_{24}, \qquad \left[9^{391.203}+13^{286.341}\right]_{25}$$

Soluzione:

1. Per $3^{207.859} \equiv r \bmod 5$ abbiamo: $3^{207.859 \bmod \varphi(5)} \equiv r \bmod 5$
   $\varphi(5) = 4$, quindi 207.849 mod 4:
   $207.859 : 4 = 4 \cdot 51.964 + 3$
   Abbiamo quindi $3^3 \equiv r \bmod 5$. Adattiamo la soluzione al modulo:
   $3^3 : 5 = 5 \cdot 5 + 2$, pertanto: $3^{207.859} \equiv 2 \bmod 5$

2. Per $7^{240.974} \equiv r \bmod 11$ abbiamo: $7^{240.974 \bmod \varphi(11)} \equiv r \bmod 11$
   $\varphi(11) = 10$, quindi 240.974 mod 10:
   $240.974 : 10 = 10 \cdot 24.097 + 4$
   Abbiamo quindi $7^4 \equiv r \bmod 11$. Adattiamo la soluzione al modulo:
   $7^4 : 11 = 11 \cdot 218 + 3$, pertanto: $7^{240.974} \equiv 3 \bmod 11$

3. Per $6^{66.095} \equiv r \bmod 14$ abbiamo: $6^{66.095 \bmod \varphi(14)} \equiv r \bmod 11$
   $$\begin{array}{r|l} 14 & 2 \\ 7 & 7 \\ 1 & \end{array}$$
   $\varphi(14) = \varphi(2 \cdot 7) = \varphi(2) \cdot \varphi(7) = 1 \cdot 6 = 6$, quindi 66.095 mod 6:
   $66.095 : 6 = 6 \cdot 11.015 + 5$
   Abbiamo quindi $6^5 \equiv r \bmod 14$. Adattiamo la soluzione al modulo:
   $6^5 : 14 = 14 \cdot 555 + 6$, pertanto: $6^{66.095} \equiv 6 \bmod 14$

4. Per $15^{96.603} \equiv r \bmod 24$ abbiamo: $15^{96.603 \bmod \varphi(24)} \equiv r \bmod 24$
   $$\begin{array}{r|l} 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}$$
   $\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3) \cdot \varphi(3) = 2^2 \cdot 2 = 8$, quindi 96.603 mod 8:
   $96.603 : 8 = 8 \cdot 12.075 + 3$
   Abbiamo quindi $15^3 \equiv r \bmod 24$. Adattiamo la soluzione al modulo:
   $15^3 : 24 = 24 \cdot 140 + 15$, pertanto: $15^{96.603} \equiv 15 \bmod 24$

5. Per $\left[9^{391.203}+13^{286.341}\right]$ vale $\left[9^{391.203}+13^{286.341}\right]_{25} = \left[9^{391.203}\right]_{25} + \left[13^{286.341}\right]_{25}$.
   Calcoliamo $\varphi(25) = \varphi(5^2) = 5^{2-1} \cdot (5-1) = 20$
   Per $9^{391.203} \equiv r \bmod 25$ abbiamo: $9^{931.203 \bmod \varphi(25)} \equiv r \bmod 25$
   $931.203 : 25 = 25 \cdot 37.248 + 3$
   Abbiamo quindi $9^3 \equiv r \bmod 25$. Adattiamo la soluzione al modulo:
   $9^3 : 25 = 25 \cdot 29 + 4$, pertanto: $9^{391.203} \equiv 4 \bmod 25$
   Per $13^{286.341} \equiv r \bmod 25$ abbiamo: $13^{286.341 \bmod \varphi(25)} \equiv r \bmod 25$
   $286.341 : 25 = 25 \cdot 11.453 + 16$
   Abbiamo quindi $13^{16} \equiv r \bmod 25$. Calcoliamo:
   $13^8 \equiv r \bmod 25$:
   $13^8 : 25 = 25 \cdot 32.629.228 + 21$, quindi $13^{16} \equiv 21^2 \equiv r \bmod 25$
   Calcoliamo: $21^2 : 25 = 25 \cdot 17 + 16$ pertanto: $13^{286.341} \equiv 16 \bmod 25$
   Il risultato è: $\left[9^{391.203}+13^{286.341}\right]_{25} = [4+16]_{25} = [20]_{25}$