1. Determinare la tabella additiva e la tabella moltiplicativa di $\mathbf{Z}_6$.
   (a) Verificare dalla tabella moltiplicativa di $\mathbf{Z}_6$ che esistono $\bar{x}$ e $\bar{y}$ non nulli in $\mathbf{Z}_6$ tali che $\bar{x} \cdot \bar{y} = \bar{0}$.
   (b) Verificare dalla tabella moltiplicativa di $\mathbf{Z}_6$ che esiste $\bar{x} \in \mathbf{Z}_6$ che non ammette inverso moltiplicativo.

Sol. La tabella additiva e la tabella moltiplicativa di $\mathbf{Z}_6$ sono date rispettivamente da

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

(a) Dalla tabella si vede che $\bar{2} \cdot \bar{3} = \bar{0}$ ed anche $\bar{3} \cdot \bar{4} = \bar{0}$.
(b) Nella tabella moltiplicativa guardiamo la riga o la colonna di $\bar{2}$. Poiché non c'è nessun elemento che moltiplicato per $\bar{2}$ dà $\bar{1}$, possiamo concludere che $\bar{2}$ non ha inverso moltiplicativo. Lo stesso vale per $\bar{3}$ e per $\bar{4}$.

2. Sia $\mathbf{Z}_8$ l'insieme delle classi resto modulo 8.
   (a) Scrivere la tabella dell'addizione e della moltiplicazione in $\mathbf{Z}_8$.
   (b) Determinare $\mathbf{Z}_8^*$, il sottoinsieme degli elementi invertibili rispetto alla moltiplicazione in $\mathbf{Z}_8$.
   (c) Scrivere la tabella della moltiplicazione in $\mathbf{Z}_8^*$.
   (d) Determinare le soluzioni in $\mathbf{Z}_8$ dell'equazione $\overline{x}^2 \equiv \overline{0}$.
   (e) Determinare tutte le soluzioni intere della congruenza $4x \equiv 0 \pmod 8$ e le soluzioni in $\mathbf{Z}_8$ dell'equazione $\overline{4}\overline{x} \equiv \overline{0}$.
   (f) Determinare tutte le soluzioni intere della congruenza $2x \equiv 6 \pmod 8$ e le soluzioni in $\mathbf{Z}_8$ dell'equazione $\overline{2}\overline{x} \equiv \overline{6}$.
   (g) Determinare tutte le soluzioni intere della congruenza $3x \equiv 1 \pmod 8$. Quante soluzioni in $\mathbf{Z}_8$ ha l'equazione $\overline{3}\overline{x} \equiv \overline{1}$?

Sol. (a) La tabella additiva e la tabella moltiplicativa di $\mathbf{Z}_8$ sono date rispettivamente da

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

(b) $\mathbf{Z}_8^* = \{\bar{x} \in \mathbf{Z}_8 \mid mcd(\bar{x}, 8) = 1\} = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

(c) La tabella moltiplicativa di $\mathbf{Z}_8^*$ è data da

	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

(d) Esaminando la tabella in (a) vediamo che le soluzioni dell'equazione $\bar{x}^2 = \bar{0}$ in $\mathbf{Z}_8$ sono $\bar{0}$ e $\bar{4}$: infatti $\bar{0}^2 = \bar{4}^2 = \bar{0}$.
(e) Abbiamo che $4x \equiv 0 \bmod 8$ se e solo se $x \equiv 0 \bmod 2$. Le soluzioni intere della congruenza sono dunque $x = 2k$, al variare di $k \in \mathbf{Z}$. In parole povere, ogni numero pari moltiplicato per quattro è un multiplo di 8. Fra esse le soluzioni $0 \leq x \leq 7$ sono $x = 0, 2, 4, 6$. Guardando la riga o la colonna di $\bar{4}$ nella tabella moltiplicativa di $\mathbf{Z}_8$ vediamo infatti che

$$\bar{4} \cdot \bar{0} = \bar{4} \cdot \bar{2} = \bar{4} \cdot \bar{4} = \bar{4} \cdot \bar{6} = \bar{0}.$$

(f) Abbiamo che $2x \equiv 6 \bmod 8$ se e solo se $x \equiv 3 \bmod 4$. Le soluzioni intere della congruenza sono dunque $x = 3 + 4k$, al variare di $k \in \mathbf{Z}$. Fra esse le soluzioni $0 \leq x \leq 7$ sono $x = 3, 7$. Guardando la riga o la colonna di $\bar{2}$ nella tabella moltiplicativa di $\mathbf{Z}_8$ vediamo infatti che

$$\bar{2} \cdot \bar{3} = \bar{2} \cdot \bar{7} = \bar{6}.$$

(g) Le soluzioni intere della congruenza $3x \equiv 1 \bmod 8$ sono date da $x = 3 + 8k$, al variare di $k \in \mathbf{Z}$. Poiché tutte queste soluzioni differiscono per multipli interi di 8, potremmo dire che "la soluzione è unica modulo 8". Guardando la riga o la colonna di $\bar{3}$ nella tabella moltiplicativa di $\mathbf{Z}_8$ vediamo infatti che che l'equazione $\bar{3} \cdot \bar{x} = \bar{1}$ ha un'unica soluzione in $\mathbf{Z}_8$, data da $\bar{3}$. Infatti

$$\bar{3} \cdot \bar{3} = \bar{1}.$$

Osserviamo che per definizione $\bar{3}$ è l'inverso moltiplicativo di $\bar{3}$ in $\mathbf{Z}_8$.

3. Determinare le tabelle moltiplicative di $\mathbf{Z}_5^*$ e di $\mathbf{Z}_{12}^*$ e confrontarle.
   (a) Per ognuno degli elementi in $\mathbf{Z}_5^*$ identificare il suo inverso.
   (b) Determinare tutti gli $\bar{x} \in \mathbf{Z}_5^*$ tali che $\bar{x}^2 = \bar{1}$.
   (c) Per ognuno degli elementi in $\mathbf{Z}_{12}^*$ identificare il suo inverso.
   (d) Determinare tutti gli $\bar{x} \in \mathbf{Z}_{12}^*$ tali che $\bar{x}^2 = \bar{1}$.

Sol. Poiché 5 è primo $\mathbf{Z}_5^*$ consiste di tutte le classi non nulle: $\mathbf{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. La tabella moltiplicativa di $\mathbf{Z}_5^*$ è data da

	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\mathbf{Z}_{12} = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$ e la sua tabella moltiplicativa è data da

	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\overline{11}$
$\bar{1}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\overline{11}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\overline{11}$	$\bar{7}$
$\bar{7}$	$\bar{7}$	$\overline{11}$	$\bar{1}$	$\bar{5}$
$\overline{11}$	$\overline{11}$	$\bar{7}$	$\bar{5}$	$\bar{1}$

(a) Guardando la tabella vediamo che in $\mathbf{Z}_5^*$

$$\bar{1}^{-1} = \bar{1}, \quad \bar{2}^{-1} = \bar{3}, \quad \bar{3}^{-1} = \bar{2}, \quad \bar{4}^{-1} = \bar{4}.$$

(b) Guardando la tabella vediamo che in $\mathbf{Z}_5^*$ le soluzioni dell'equazione $\bar{x}^2 = \bar{1}$ sono $\bar{x} = \bar{1}, \bar{4}$ (ossia gli elementi che coincidono col proprio inverso moltiplicativo).
(c)(d) Guardando la tabella vediamo che in $\mathbf{Z}_{12}^*$ tutti gli elementi coincidono col proprio inverso moltiplicativo e quindi soddisfano l'equazione $\bar{x}^2 = \bar{1}$. Osserviamo che in $\mathbf{Z}_{12}^*$ l'equazione di secondo grado $\bar{x}^2 = \bar{1}$ ha quattro soluzioni!

4. Sia dato l'insieme $A = \{1, -1, i, -i\}$ con l'operazione data dalla moltiplicazione fra numeri complessi.
   (a) Verificare che A è un gruppo abeliano.
   (b) Determinare i^{-1} e $(-i)^{-1}$.
   (c) Scrivere la tabella della moltiplicazione su A. Confrontarla con quelle dell'esercizio precedente.

Sol. Per verificare che A è un gruppo conviene osservare che è un sottoinsieme del gruppo moltiplicativo abeliano dei numeri complessi non nulli $\mathbf{C}^*$. Inoltre A è chiuso rispetto al prodotto fra numeri complessi (il prodotto di due qualsiasi elementi di A appartiene ad A) e l'inverso di ogni elemento di A rispetto a tale prodotto appartiene ad A. Scriviamo la tabella moltiplicativa di A:

	1	i	$-i$	-1
1	1	i	$-i$	-1
i	i	-1	1	$-i$
$-i$	$-i$	1	-1	i
-1	-1	$-i$	i	1

Il fatto che la tabella sia simmetrica rispetto alla diagonale principlae conferma che il gruppo A è abeliano.
(b) Abbiamo $i^{-1} = -i$ e $(-i)^{-1} = i$. Infatti $i(-i) = (-i)i = 1$.
(c) Confrontando le tabelle possiamo vedere che "mutatis mutandis", ossia associando

$$1 \mapsto \bar{1}, \quad i \mapsto \bar{2}, \quad -i \mapsto \bar{3}, \quad -1 \mapsto \bar{4},$$

la tabella di A funziona come quella di Z_5^*. In questo caso si dice che i due gruppi A e Z_5^* sono isomorfi. Invece è sostanzialmente diversa da quella di Z_{12}^*: mentre in Z_{12}^* ogni elemento al quadrato dà $\bar{1}$, questo non vale in A né in Z_5^*. In questo caso si dice che i due gruppi A e Z_{12}^* non sono isomorfi.

5. La *funzione φ di Eulero* è definita da $\varphi(n) = \#\mathbf{Z}_n^*$ (per $n \in \mathbf{N}$).
   (a) Calcolare $\varphi(n)$ per ogni $n \leq 10$.
   (b) In ognuno di tali casi enunciare il corrispondente Teorema di Lagrange per $\mathbf{Z}_n^*$.

Sol. (a) Abbiamo che $\varphi(n) = \#\mathbf{Z}_n^* = \#\{\bar{x} \in \mathbf{Z}_n \mid mcd(\bar{x}, n) = 1\}$. Si verifica direttamente che

$$\varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(5) = 4, \quad \varphi(6) = 2, \quad \varphi(7) = 6, \quad \varphi(8) = 4, \quad \varphi(9) = 6, \quad \varphi(10) = 4.$$

(b) $Z_3^* = \{\bar{1}, \bar{2}\}$: $\quad \bar{x}^2 = \bar{1}, \quad \forall \bar{x} \in Z_3^*$;
$Z_4^* = \{\bar{1}, \bar{3}\}$: $\quad \bar{x}^2 = \bar{1}, \quad \forall \bar{x} \in Z_4^*$;
$Z_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$: $\quad \bar{x}^4 = \bar{1}, \quad \forall \bar{x} \in Z_5^*$;
$Z_6^* = \{\bar{1}, \bar{5}\}$: $\quad \bar{x}^2 = \bar{1}, \quad \forall \bar{x} \in Z_6^*$;
$Z_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$: $\quad \bar{x}^6 = \bar{1}, \quad \forall \bar{x} \in Z_7^*$;
$Z_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$: $\quad \bar{x}^4 = \bar{1}, \quad \forall \bar{x} \in Z_8^*$;
$Z_9^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$: $\quad \bar{x}^6 = \bar{1}, \quad \forall \bar{x} \in Z_9^*$;
$Z_{10}^* = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$: $\quad \bar{x}^4 = \bar{1}, \quad \forall \bar{x} \in Z_{10}^*$;

6. Sia $n = 13$. Enunciare il Piccolo Teorema di Fermat per $G = \mathbf{Z}_{13}^*$. Usare tale risultato per calcolare

$$\overline{4^{24}}, \quad \overline{4^{59}}, \quad \overline{4^{26}}, \quad \overline{4^{24001}} \quad \in \mathbf{Z}_{13}.$$

Sol. Poiché 13 è primo, Z_{13}^* consiste di tutte le classi resto non nulle in $\mathbf{Z}_{13}$. In particolare $\varphi(13) = 12$. Il terorema di Lagrange, che in questo caso si chiama il Piccolo Teorema di Fermat, dice che

$$\bar{x}^{12} = \bar{1} \bmod 13, \quad \forall \bar{x} \in \mathbf{Z}_{13}^*.$$

7. Siano dati $\bar{x} = \overline{13^{35}}$ e $\bar{y} = \overline{41^{35}}$ in $\mathbf{Z}_{37}$.
   (a) Determinare $\bar{x}^{-1}$.
   (b) Determinare $\bar{y}^{-1}$.

Sol. Osserviamo innanzitutto che 37 è primo e dunque $\varphi(37) = 36$. In questo caso il Piccolo Teorema di Fermat, dice che

$$\bar{x}^{36} = \bar{1} \bmod 37, \quad \forall \bar{x} \in \mathbf{Z}_{37}^* = \{\bar{x} \in \mathbf{Z}_{37}, \ \bar{x} \neq \bar{0}\}.$$

(a) Poiché $\overline{13^{35}} \cdot \overline{13} = \overline{13}^{35} \cdot \overline{13} = \overline{13}^{36} = \bar{1}$, ne segue che $\bar{x}^{-1} = \overline{13}$.
(b) Poiché $\bar{y} = \overline{41^{35}} = \overline{41}^{35} = \bar{4}^{35}$ ed inoltre $\bar{4}^{35} \cdot \bar{4} = \bar{4}^{36} = \bar{1}$, ne segue che $\bar{y}^{-1} = \bar{4}$.

8. Calcolare $\bar{2}^{300}$ in $\mathbf{Z}_6$. Possiamo usare il Teorema di Lagrange?

Sol. Osserviamo che $mcd(2, 6) = 2 \neq 1$. Quindi $\bar{2} \notin \mathbf{Z}_6^*$ ed in questo caso *non* possiamo usare il Teorema di Lagrange. Calcolando direttamente qualche potenza di $\bar{2}$ in $\mathbf{Z}_6$, troviamo

$$\bar{2}^2 = \bar{4}, \quad \bar{2}^3 = \bar{2}, \quad \bar{2}^4 = \bar{4}, \quad \ldots \begin{cases} \bar{2}^n = \bar{2} & n \text{ dispari} \\ \bar{2}^n = \bar{4} & n \text{ pari.} \end{cases}$$

Ne segue che $\bar{2}^{300} = \bar{4}$ in $\mathbf{Z}_6$.

9. Calcolare

$$2^{1000} \bmod 5, \qquad 2^{1000} \bmod 7, \qquad 10^{1000} \bmod 3, \qquad 10^{1000} \bmod 5.$$

Sol. Poiché $\bar{2} \in \mathbf{Z}_5^*$ e $\varphi(5) = 4$ abbiamo che modulo 5

$$\bar{2}^{1000} = \bar{2}^{4 \cdot 250} = (\bar{2}^4)^{250} = \bar{1}^{250} = \bar{1}.$$

Poiché $\bar{2} \in \mathbf{Z}_7^*$ e $\varphi(7) = 6$ abbiamo che modulo 7

$$\bar{2}^{1000} = \bar{2}^{6 \cdot 166 + 4} = (\bar{2}^6)^{166} \cdot \bar{2}^4 = \bar{1} \cdot \bar{2}^4 = \bar{2}.$$

Poiché $\overline{10} = \bar{1} \mod 3$, abbiamo che modulo 3

$$\overline{10}^{1000} = \bar{1}^{1000} = \bar{1}.$$

Poiché $\overline{10} = \bar{0} \mod 5$, abbiamo che modulo 5

$$\overline{10}^{1000} = \bar{0}^{1000} = \bar{0}.$$

10. Determinare l'ultima cifra decimale dei seguenti numeri

$$37^{37}, \qquad 16^{16}, \qquad 19^{19}.$$

Sol. Determinare l'ultima cifra decimale di un numero equivale a calcolare la sua classe resto modulo 10:
innanzitutto $\overline{37}^{37} = \bar{7}^{37}$ modulo 10; inoltre $7 \in \mathbf{Z}_{10}^*$ e $\varphi(10) = 4$. Ne segue che

$$\bar{7}^{37} = \bar{7}^{4 \cdot 9 + 1} = \bar{7}^{4 \cdot 9} \cdot \bar{7} = \bar{7}.$$

Con argomenti simili si trova che modulo 10

$$\overline{19}^{19} = \bar{9}^{19} = \bar{9}^{4 \cdot 4 + 3} = \bar{9}^3 = \bar{9}^2 \cdot \bar{9} = \bar{9}.$$

Infine $\overline{16}^{16} = \bar{6}^{16}$ modulo 10; osserviamo però che $\bar{6} \notin \mathbf{Z}_{10}^*$, quindi in questo caso non possiamo usare il teorema di Lagrange come nei casi precedenti. Calcolando direttamente qualche potenza di $\bar{6}$ in $\mathbf{Z}_{10}$ troviamo

$$\bar{6}^2 = \bar{6}, \quad \bar{6}^3 = \bar{6}, \quad \ldots, \quad \bar{6}^n = \bar{6}, \ \forall n.$$

Ne segue che $\overline{16}^{16} = \bar{6}$ modulo 10.

11. Calcolare

$$5^{95} \mod 70, \qquad 2^{1000} \mod 110.$$

Sol. Abbiamo $70 = 2 \cdot 5 \cdot 7$, da cui

$$x \equiv 5^{95} \mod 70 \quad \Leftrightarrow \quad \begin{cases} x \equiv 5^{95} \mod 2 \\ x \equiv 5^{95} \mod 5 \\ x \equiv 5^{95} \mod 7 \end{cases} \quad \Leftrightarrow \quad \begin{cases} x \equiv 1^{95} \mod 2 \\ x \equiv 0^{95} \mod 5 \\ x \equiv 5^{95} \mod 7 \end{cases}$$

$$\Leftrightarrow \quad \begin{cases} x \equiv 1 \mod 2 \\ x \equiv 0 \mod 5 \\ x \equiv 3 \mod 7. \end{cases}$$

N.B. Per semplificare la terza congruenza del sistema abbiamo usato il fatto che per il Piccolo Teorema di Fermat $5^6 \equiv 1 \mod 7$, da cui $5^{6\cdot 15+5} \equiv 5^5 \equiv 3 \mod 7$.
Le soluzioni intere del sistema sono date da $x = 45 + k70$, al variare di $k \in \mathbf{Z}$. La classe resto di $5^{95} \mod 70$ è l'unica soluzione del sistema compresa fra 0 e 70, cioè $x = 45$.

Abbiamo $110 = 2 \cdot 5 \cdot 11$, da cui

$$x \equiv 2^{1000} \mod 110 \quad \Leftrightarrow \quad \begin{cases} x \equiv 2^{1000} \mod 2 \\ x \equiv 2^{1000} \mod 5 \\ x \equiv 2^{1000} \mod 11 \end{cases} \quad \Leftrightarrow \quad \begin{cases} x \equiv 0^{1000} \mod 2 \\ x \equiv 2^{1000} \mod 5 \\ x \equiv 2^{1000} \mod 11 \end{cases}$$

$$\Leftrightarrow \quad \begin{cases} x \equiv 0 \mod 2 \\ x \equiv 1 \mod 5 \\ x \equiv 1 \mod 11. \end{cases}$$

Anche in questo caso abbiamo usato il Piccolo Teorema di Fermat:

$$2^4 \equiv 1 \mod 5, \qquad 2^{10} \equiv 1 \mod 11,$$

da cui

$$2^{1000} \equiv 1 \mod 5, \qquad 2^{1000} \equiv 1 \mod 11.$$

La classe resto di $2^{1000} \mod 110$ è l'unica soluzione del sistema compresa fra 0 e 110, cioè $x = 56$.

12. (a) Determinare il resto delle divisioni per 5, per 7 e per 11 di 3^{302}; determinare il resto della divisione per 385 di 3^{302} (si noti che $385 = 5 \cdot 7 \cdot 11$).
    (b) Determinare il resto delle divisioni per 7, per 11 e per 13 di 5^{2003}; determinare il resto della divisione per 1001 di 5^{2003} (si noti che $1001 = 7 \cdot 11 \cdot 13$).

Sol. (a) Il resto della divisione per 5 di 3^{302} è per definizione la sua classe resto modulo 5. Poiché 5 è primo e $\varphi(5) = 4$, per il Teorema di Lagrange (o Piccolo Teorema di Fermat), vale

$$\overline{3^{302}} \equiv \bar{3}^{302} \equiv \bar{3}^{4\cdot 75+2} \equiv \bar{3}^2 \equiv \bar{4} \mod 5.$$

Con ragionamenti simili si trova che i resti delle divisioni di 3^{302} per 7 e per 11 sono dati rispettivamente da

$$\overline{3^{302}} \equiv \bar{3}^{302} \equiv \bar{3}^{6\cdot 50+2} \equiv \bar{3}^2 \equiv \bar{2} \mod 7 \qquad \varphi(7) = 6;$$

$$\overline{3^{302}} \equiv \bar{3}^{302} \equiv \bar{3}^{10\cdot 30+2} \equiv \bar{3}^2 \equiv \bar{9} \mod 11 \qquad \varphi(11) = 10.$$

Per il Teorema Cinese del Resto, il resto della divisione di 3^{302} per $385 = 5 \cdot 7 \cdot 11$ è l'unica soluzione x_0 del sistema di congruenze

$$\begin{cases} x \equiv 4 \mod 5 \\ x \equiv 2 \mod 7 \\ x \equiv 9 \mod 11 \end{cases}$$

che soddisfa $0 \leq x_0 \leq 385$. Risolvendo il sistema troviamo $x_0 = 9$.

(b) Con uno svolgimento analogo, troviamo che

$$\overline{5^{2003}} \equiv \bar{3} \mod 7, \quad \overline{5^{2003}} \equiv \bar{4} \mod 11, \quad \overline{5^{2003}} \equiv \bar{8} \mod 13,$$

da cui

$$\overline{5^{2003}} \equiv \overline{983} \mod 1001.$$

13. Determinare il resto della divisione per 5 di $33213454^{27221447}$. Determinare il resto della divisione per 7 di $19^{19^{19}}$.

Sol. Dobbiamo calcolare $33213454^{27221447}$ modulo 5:

$$33213454^{27221447} \equiv 4^{27221447} \equiv (-1)^{27221447} \equiv -1 \equiv 4 \mod 5.$$

Dobbiamo calcolare $19^{19^{19}}$ modulo 7:

$$19^{19^{19}} \equiv 5^{19^{19}} \mod 7.$$

Poiché $\varphi(7) = 6$, per il Piccolo Teorema di Fermat $5^6 \equiv 1 \bmod 7$. A questo punto osserviamo che $19^{19} \equiv 1^{19} \equiv 1 \bmod 6$, ossia $19^{19} = 1 + 6M$, per qualche intero M. Ne segue che

$$19^{19^{19}} \equiv 5^{19^{19}} \equiv 5^{6M+1} \equiv 5^{6M}5 \equiv 5 \mod 7.$$

14. Calcolare il resto della divisione per 70 di 3^{302}.

Sol. Poiché $70 = 2 \cdot 5 \cdot 7$, con uno svolgimento analogo a quello dell'esercizio 12, troviamo

$$\overline{3^{302}} \equiv \bar{1} \bmod 2, \quad \overline{3^{302}} \equiv \bar{4} \bmod 5, \quad \overline{3^{302}} \equiv \bar{2} \bmod 7, \qquad \overline{3^{302}} \equiv \bar{9} \bmod 70.$$

15. Sia $n \in \mathbf{N}$. L'ordine $\mathrm{ord}_n(x)$ di $x \in \mathbf{Z}_n^*$ è il più piccolo $r > 0$ tale che $x^r \equiv 1 \pmod n$.
    (a) Sia $n = 7$. Calcolare $\mathrm{ord}_n(x)$ per ogni $x \in \mathbf{Z}_n^*$.
    (b) Sia n primo. Dimostrare che $\mathrm{ord}_n(x)$ divide $n - 1$ per ogni $x \in \mathbf{Z}_n^*$.
    (c) Sia $n \in \mathbf{N}$. Calcolare l'ordine di $-1 \pmod n$.

Sol. (a) $\bar{1} \cdot \bar{1} = \bar{1}$, $\bar{6} \cdot \bar{6} = \overline{-1} \cdot \overline{-1} = \bar{1}$. Gli elementi $\overline{-1}$ e $\bar{1}$ hanno ordine 2.
$\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{1}$, per cui l'ordine di $\bar{2}$ è 3.
$\bar{3}^2 = \bar{2}$, $\bar{3}^3 = \bar{6}$, $\bar{3}^4 = \bar{4}$, $\bar{3}^5 = \bar{5}$, $\bar{3}^6 = \bar{1}$, per cui l'ordine di $\bar{3}$ è 6.
$\bar{4}^2 = \bar{2}$, $\bar{4}^3 = \bar{1}$, per cui l'ordine di $\bar{4}$ è 3.
$\bar{5}^2 = \bar{4}$, $\bar{5}^3 = \bar{6}$, $\bar{5}^4 = \bar{2}$, $\bar{5}^5 = \bar{3}$, $\bar{5}^6 = \bar{1}$, per cui l'ordine di $\bar{5}$ è 6.
(b) Sia $n = p$ primo. Il gruppo $\mathbf{Z}_p^* = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ ha ordine $p - 1$ e dal Teorema di Lagrange segue che $\bar{x}^{p-1} \equiv \bar{1} \mod p$. Sia $k > 0$ il più piccolo intero tale che $x^k \equiv \bar{1} \mod p$. Chiaramente $k \leq p - 1$. Facendo il quoziente di $p - 1$ per k possiamo scrivere $p - 1 = km + r$, con $0 \leq r < k$. Vogliamo dimostrare che $r = 0$, cioè che k divide $p - 1$. Abbiamo

$$\bar{x}^{p-1} = \bar{x}^{mk+r} = \bar{x}^{km}\bar{x}^r \equiv \bar{x}^r \mod p.$$

Se $r > 0$, questo contraddice il fatto che $k > 0$ è il più piccolo intero per cui $x^k \equiv \bar{1} \mod p$. Conclusione: $r = 0$ e k divide $p - 1$.
(c) $\overline{-1} \cdot \overline{-1} = \bar{1} \mod n$, per cui l'ordine di $\overline{-1}$ è sempre 2.

16. (a) Sia $p > 2$ un primo. Dimostrare che $\{x \in \mathbf{Z}_p : x^2 = 1\} = \{\pm 1\}$.
    (b) Determinare tutti gli $x \in \mathbf{Z}_{15}^*$ per cui $x^2 = 1$. Stessa domanda per $\mathbf{Z}_{21}^*$.
    (c) Sia $n = pq$ prodotto di due primi dispari. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?
    (d) Determinare tutti gli $x \in \mathbf{Z}_9^*$ per cui $x^2 = 1$. Stessa domanda per $\mathbf{Z}_{25}^*$.
    (e) Sia $n = p^2$ quadrato di un numero primo $p > 2$. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?

Sol. (a) Si ha che

$$x^2 \equiv 1 \bmod p \quad \Leftrightarrow \quad x^2 - 1 \equiv 0 \bmod p \quad \Leftrightarrow \quad (x+1)(x-1) \equiv 0 \bmod p.$$

Poiché p è primo, questo implica che p divide $x+1$ oppure p divide $x-1$, da cui

$$x \equiv 1 \bmod p \quad \text{oppure} \quad \text{x} \equiv -1 \bmod \text{p}.$$

(c) Sia $n = pq$ prodotto di due primi dispari. Si ha che

$$x^2 \equiv 1 \bmod pq \quad \Leftrightarrow \quad x^2 - 1 \equiv 0 \bmod pq \quad \Leftrightarrow \quad (x+1)(x-1) \equiv 0 \bmod pq$$

$$\Leftrightarrow \quad \begin{cases} (x+1)(x-1) \equiv 0 \bmod p \\ (x+1)(x-1) \equiv 0 \bmod q, \end{cases}$$

da cui

$$\begin{cases} (x+1) \equiv 0 \bmod p \\ (x+1) \equiv 0 \bmod q \end{cases} \bigcup \begin{cases} (x+1) \equiv 0 \bmod p \\ (x-1) \equiv 0 \bmod q \end{cases} \bigcup \begin{cases} (x-1) \equiv 0 \bmod p \\ (x-1) \equiv 0 \bmod q \end{cases} \bigcup \begin{cases} (x-1) \equiv 0 \bmod p \\ (x+1) \equiv 0 \bmod q \end{cases}$$

$$\begin{cases} x \equiv -1 \bmod p \\ x \equiv -1 \bmod q \end{cases} \bigcup \begin{cases} x \equiv -1 \bmod p \\ x \equiv 1 \bmod q \end{cases} \bigcup \begin{cases} x \equiv 1 \bmod p \\ x \equiv 1 \bmod q \end{cases} \bigcup \begin{cases} x \equiv 1 \bmod p \\ x \equiv -1 \bmod q. \end{cases}$$

In conclusione, ci sono *quattro classi resto modulo pq* che soddisfano l'equazione di secondo grado $x^2 = 1$ in $\mathbf{Z}^*_{pq}$. Si ottengono risolvendo i quattro sistemi qui sopra.

(b) Nel primo caso $p = 3$ e $q = 5$. I sistemi da risolvere sono

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 4 \bmod 5 \end{cases} \bigcup \begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 1 \bmod 5 \end{cases} \bigcup \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 1 \bmod 5 \end{cases} \bigcup \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 4 \bmod 5. \end{cases}$$

Le quattro classi resto di $\mathbf{Z}^*_{15}$ che soddisfano l'equazione di secondo grado $x^2 = 1$ sono date da $\bar{x} = 14$, $\bar{x} = 11$, $\bar{x} = 1$, $\bar{x} = 4$.

Nel secondo caso $p = 3$ e $q = 7$. Le quattro classi resto di $\mathbf{Z}^*_{21}$ che soddisfano l'equazione di secondo grado $x^2 = 1$ si ottengono risolvendo i sistemi

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 6 \bmod 7 \end{cases} \bigcup \begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 1 \bmod 7 \end{cases} \bigcup \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 1 \bmod 7 \end{cases} \bigcup \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 6 \bmod 7. \end{cases}$$

e sono date da $\bar{x} = etc....$

(e) Sia $n = p^2$ quadrato di un numero primo $p > 2$. Si ha che

$$x^2 \equiv 1 \bmod p^2 \quad \Leftrightarrow \quad x^2 - 1 \equiv 0 \bmod p^2 \quad \Leftrightarrow \quad (x+1)(x-1) \equiv 0 \bmod p^2.$$

Poiché p è primo, questo implica che p divide $x+1$ oppure p divide $x-1$; in effetti anche p^2 divide $x+1$ oppure divide $x-1$ (questo segue dal fatto che la differenza fra $x+1$ e $x-1$ è solo due: se fosse $x+1 = mp$ e $x-1 = np$, avremmo $(m-n)p = 2$...impossibile), da cui

$$\bar{x} \equiv 1 \bmod p^2 \quad \text{oppure} \quad \bar{\text{x}} \equiv -1 \bmod \text{p}^2.$$

(d) Nel primo caso $p = 3$ e $p^2 = 9$. Le classi resto di $\mathbf{Z}^*_9$ che soddisfano l'equazione di secondo grado $x^2 = 1$ sono date da $\bar{x} = 1$ e $\bar{x} = -1 \equiv 8$. Si verifica che $8^2 = 64 \equiv 1 \bmod 9$.

Nel secondo caso $p = 5$ e $p^2 = 25$. Le classi resto di $\mathbf{Z}_{25}^*$ che soddisfano l'equazione di secondo grado $x^2 = 1$ sono date da $\bar{x} = 1$ e $\bar{x} = -1 \equiv 24$. Si verifica che $24^2 = 576 \equiv 1 \bmod 25$.

N.B.: In $\mathbf{Z}_p^*$ e in $\mathbf{Z}_{p^k}^*$ con k primo l'equazione di secondo grado $x^2 - 1$ ha due soluzioni, come ci aspettiamo. Ma in $\mathbf{Z}_{pq}^*$ ne ha $2^2 = 4$. In generale in $\mathbf{Z}_{p_1 p_2 \dots p_k}^*$, con p_i primi distinti, ne ha 2^k.

17. Dimostrare che $4^{2n+1} + 3^{n+2}$ è divisibile per 13, per ogni $n \in \mathbf{N}$ (suggerimento: calcolare in $\mathbf{Z}_{13}$).

Sol. Scriviamo $4^{2n+1} + 3^{n+2} = (4 \cdot 4)^n \cdot 4 + 3^n \cdot 3^2 = 4 \cdot 16^n + 9 \cdot 3^n$. Modulo 13, l'espressione diventa $4 \cdot 3^n + 9 \cdot 3^n \equiv 13 \cdot 3^n \equiv 0$. Ne segue che $4^{2n+1} + 3^{n+2}$ è divisibile per 13.

18. Sia $p \in \mathbf{N}$ un numero primo. Verificare che in $\mathbf{Z}_p$ vale l'uguaglianza $(\bar{x} + \bar{y})^p = \bar{x}^p + \bar{y}^p$, per ogni $\bar{x},\ \bar{y} \in \mathbf{Z}_p$ (suggerimento: usare la formula di Newton).
Verificare che per $n = 4$, tale uguaglianza non vale.

Sol. Per la formula di Newton abbiamo

$$(\bar{x} + \bar{y})^p = \bar{x}^p + \binom{p}{1}\bar{x}^{p-1}\bar{y} + \binom{p}{2}\bar{x}^{p-2}\bar{y}^2 + \ldots + \bar{y}^p.$$

Per ottenere la tesi, verifichiamo che per ogni $k = 1, \ldots, p-1$ il coefficiente binomiale $\binom{p}{k}$ è divisibile per p, e dunque è 0 modulo p. Scriviamo

$$\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!} \in \mathbf{Z}.$$

Poiché p è primo non può essere diviso per nessuno dei fattori di $k!$. Ne segue che $\binom{p}{k}$ è un multiplo intero di p, come richiesto.

Per $n = 4$, i coefficienti binomiali sono $1, 4, 6, 4, 1$. Il coefficiente centrale 6 non è zero modulo 4. In questo caso infatti l'uguaglianza $(\bar{x} + \bar{y})^4 = \bar{x}^4 + \bar{y}^4$ non vale.

19. Dimostrare che $\sum_{\bar{x} \in \mathbf{Z}_n} \bar{x} = \bar{0}$ in $\mathbf{Z}_n$, per ogni n dispari.

Sol. Poiché $\mathbf{Z}_n$ è un gruppo, ogni $\bar{x} \in \mathbf{Z}_n$ ammette opposto dato da $\overline{-x} = \overline{n - x} \in \mathbf{Z}_n$. Osserviamo che l'elemento neutro $\bar{0}$ coicide col suo opposto: infatti $\bar{0} + \bar{0} = \bar{0}$. Osserviamo inoltre che se n è dispari, l'opposto di ogni classe resto $\bar{x} \not\equiv \bar{0}$ è necessariamente diverso da $\bar{x}$ (infatti se per qualche $\bar{x} \not\equiv \bar{0}$ vale $\bar{x} \equiv \overline{n - x}$ allora $n = 2x$, ossia n è pari). Dunque per n dispari ogni $\bar{x} \not\equiv \bar{0}$ risulta accoppiato col suo opposto e per ogni coppia vale $\bar{x} + \overline{n - x} = \bar{0}$. Ne segue che $\sum_{\bar{x} \in \mathbf{Z}_n} \bar{x} = \bar{0}$, come richiesto.

ESEMPIO: in $\mathbf{Z}_7$ abbiamo $\bar{0} + (\bar{1} + \bar{6}) + (\bar{2} + \bar{5}) + (\bar{3} + \bar{4}) = \bar{0}$.
Invece in $\mathbf{Z}_6$ abbiamo $\bar{3} = \overline{-3}$ e vale $\bar{0} + (\bar{1} + \bar{5}) + (\bar{2} + \bar{4}) + \bar{3} = \bar{3} \neq \bar{0}$.

20. Calcolare $(p-1)!$ in $\mathbf{Z}_p$, per p primo.

Sol. Osserviamo che $(p-1)! = (p-1)\ldots 3 \cdot 2 \cdot 1$ può essere visto come il prodotto di tutte le classi resto di $\mathbf{Z}_p^*$, che sono $p - 1$. Se p è primo, ogni classe resto $\bar{x} \neq \bar{1}, \overline{-1}$ è accoppiata col suo inverso $\bar{x}^{-1}$, che è distinto da $\bar{x}$ (nota che $\overline{-1} = \overline{p-1}$). Chiaramente per ognuna di tali coppie vale $\bar{x} \cdot \bar{x}^{-1} = \bar{1}$. In totale abbiamo quindi

$$(p-1)! = (p-1) \cdot 1.$$

ESEMPIO: in $\mathbf{Z}_7^*$ abbiamo

$$\bar{1} \cdot \bar{6} \cdot (\bar{2} \cdot \bar{4}) \cdot (\bar{3} \cdot \bar{5}) \equiv \bar{6}.$$

21. Siano $(G_1, e_1, \circ)$ e $(G_2, e_2, *)$ due gruppi. Sul prodotto cartesiano $G_1 \times G_2$ definiamo una operazione mediante

$$(g_1, g_2) \cdot (h_1, h_2) := (g_1 \circ h_1, g_2 * h_2).$$

(a) Dimostare che con questa operazione $G_1 \times G_2$ è un gruppo.
(b) Siano $(G_1, e_1, \circ) = (G_2, e_2, *) = (\mathbf{Z}_2, \bar{0}, +)$, con la somma $\overline{x} + \overline{y} := \overline{x+y}$. Scrivere la tabella dell'operazione indotta su $\mathbf{Z}_2 \times \mathbf{Z}_2$.
(c) Siano $(G_1, e_1, \circ) = (\mathbf{Z}_2, \bar{0}, +)$ e $(G_2, e_2,) = (\mathbf{Z}_3, \bar{0}, +)$. Scrivere la tabella dell'operazione indotta su $\mathbf{Z}_2 \times \mathbf{Z}_3$.

Sol. (a) L'operazione $(g_1, g_2) \cdot (h_1, h_2) := (g_1 \circ h_1, g_2 * h_2)$ è associativa, perché è definita componenete per componenete e le due operazioni singolarmente lo sono.... Si verifica facilmente che l'elemento neutro è (e_1, e_2) e che l'inverso di un elemento (g_1, g_2) è (g_1^{-1}, g_2^{-1}).

(b)

	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{1})$
$(\bar{0},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$
$(\bar{1},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{0})$

(c)

	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$
$(\bar{0},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$	$(\bar{1},\bar{0})$
$(\bar{0},\bar{2})$	$(\bar{0},\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$
$(\bar{1},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{0},\bar{0})$
$(\bar{1},\bar{2})$	$(\bar{1},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$

22. Sia G un gruppo tale che $g^2 = e$, per ogni $g \in G$. Dimostrare che G è abeliano.

Sol. Siano x, y elementi di G e sia $xy \in G$ il loro prodotto. Dall'ipotesi segue che

$$(xy)^2 = xyxy = e \quad \Leftrightarrow \quad y^{-1}x^{-1}xyxy = y^{-1}x^{-1} \quad \Leftrightarrow \quad xy = y^{-1}x^{-1}.$$

Osserviamo che $x^2 = e$ equivale a $x = x^{-1}$. Dunque $xy = yx$, per ogni $x, y \in G$, come richiesto.

23. Sia $G = \{M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{R},\ \det M \neq 0\}$. Dimostrare che G col prodotto fra matrici usuale è un gruppo non commutativo.

Sol. Vedi Geometria 1.

24. Sia $A = \{M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{R}\}$.
(a) Dimostrare che A con la somma fra matrici usuale è un gruppo abeliano.

(b) Dimostrare che A con la somma e il prodotto fra matrici usuali è un anello non commutativo.
(c) Far vedere che esistono matrici non nulle $M, N \in A$ il cui prodotto è la matrice nulla.
(d) Chi sono le unità in A?

Sol. Vedi Geometria 1.

25. Sia X un insieme e sia $P(X)$ l'insieme dei sottoinsiemi di X. Definiamo su $P(X)$ una "somma" ed un "prodotto" mediante

$$A \oplus B := (A \cup B) - (A \cap B), \qquad A \otimes B := A \cap B.$$

(a) Verificare che $A \oplus B = (A - B) \cup (B - A)$.
(b) Dimostrare che $P(X)$ con l'operazione $\oplus$ è un gruppo abeliano.
(c) Scrivere la tabella di composizione per un insieme X di due elementi. Confrontare con il gruppo di Klein V_4.
(d) Dimostrare che $P(X)$ con le operazioni "$\oplus$" e "$\otimes$" è un anello commutativo.
(d) Chi sono le unità in $P(X)$?