1. Dato un gruppo G con 4 elementi $\{e, a, b, c\}$ verificare che esistono a priori solo due tabelle distinte per G.

   Soluzione.

   Questo esercizio è equivalente a verificare che un gruppo G di ordine 4 deve essere necessariamente isomorfo a $\mathbb{Z}_4$ o al gruppo di Klein, V, che definiamo qui di seguito. L'elemento a può avere ordine 2 o 4. Supponiamo che i tre elementi a, b, c abbiano tutti ordine 2: $a^2 = b^2 = c^2 = e$. Deve allora essere $ab = c$, perché se fosse $ab = a$ allora, per cancellazione, $b = e$, impossibile. Se $ab = e$ allora b sarebbe l'inverso di a mentre per ipotesi a è inverso di se stesso. Infine, se $ab = b$ allora $a = e$, impossibile.

   Abbiamo allora la tabella moltiplicativa del gruppo V di Klein seguente:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

   Se invece almeno un elemento, diciamo b ha ordine 4, allora chiaramente $G \sim \mathbb{Z}_4$ in quanto $G = \langle b \rangle$.

2. Dimostrare che il gruppo D_3 delle simmetrie di un triangolo equilatero è isomorfo al gruppo S_3 delle permutazioni su tre elementi.

3. Dimostrare che l'unico omomorfismo possibile tra $\mathbb{Z}_3$ e $\mathbb{Z}_4$ è quello banale.

   Soluzione.

   Infatti, se $f : \mathbb{Z}_3 \to \mathbb{Z}_4$ allora $o(Im(f))$ deve dividere sia 3 che 4 e dunque è uguale a 1.

4. Sia G il gruppo degli interi di Gauss, cioè dei numeri complessi con parte reale e parte immaginaria intera, $G = \mathbb{Z} + i\mathbb{Z}$ e sia G' l'insieme dei numeri razionali della forma $2^n 3^m$ al variare di $m, n \in \mathbb{Z}$. Dimostrare che $G \simeq G'$. (Verificare che $f : G \to G'$ definita da $f(m+in) = 2^n 3^m$ è un isomorfismo.)

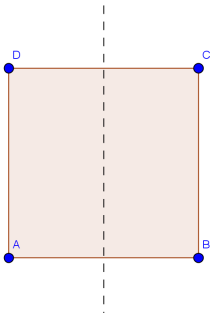
5. Costruire un omomorfismo, se possibile, tra $\mathbb{Z}_6$ e D_4.

   Soluzione.

   Se $f : \mathbb{Z}_6 \to D_4$ è un omomorfismo allora $o(Imf)$ divide sia $o(\mathbb{Z}_6) = 6$ che $o(D_4) = 8$ e dunque $o(ImF)$ può solo essere 1 o 2. Il caso $o(Imf) = 1$ corrisponde all'omomorfismo banale in cui ogni elemento di $\mathbb{Z}_6$ si trasforma nell'elemento neutro I di D_4.

   Se $o(Imf) = 2$ allora domandiamoci quali sottogruppi di D_4 hanno ordine 2. Essi sono quelli generati dalle 4 riflessioni del quadrato e quello generato dalla rotazione di 180 gradi.

   Prendendo ad esempio la riflessione T del quadrato rispetto all'asse verticale



il sottogruppo di D_4 di ordine 2 è $\{I, T\}$. Possiamo stabilire allora la seguente corrispondenza

$$\begin{array}{ccc} 0 & \mapsto & I \\ 1 & \mapsto & T \\ 2 & \mapsto & I \\ 3 & \mapsto & T \\ 4 & \mapsto & I \\ 5 & \mapsto & T \end{array}$$

Si può verificare che questa corrispondenza è in effetti un omomorfismo. Per esempio $1 + 3 = 4$ corrisponde a $T \circ T = I$ etc.

6. Costruire un campo con 25 elementi.

7. Stabilire se esistono soluzioni del sistema di equazioni lineari

$$\begin{cases} x + 2y = 4 \\ 4x + 3y = 4 \end{cases}$$

dove i coefficienti sono in $\mathbb{Z}_7$ o in $\mathbb{Z}_5$.

8. Per quali dei seguenti numeri primi p possiamo costruire un campo di ordine p^2 usando il polinomio $x^2 + 1$? $p = 3, 5, 7, 11, 13, 19, 23$

9. Sia p un numero primo. Dimostrare che il numero di matrici invertibili di ordine due a coefficienti in $\mathbb{Z}_p$ è $(p^2 - 1)(p^2 - p_)$.

   Soluzione. Una matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ è invertibile se le sue colonne sono linearmente indipendenti. La prima colonna può dunque essere scelta in $p^2 - 1$ maniere (tutti i vettori tranne quello nullo). La seconda colonna deve essere scelta in modo da non essere un multiplo della prima. I multipli della prima sono della forma $k\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$ e sono in numero di p . In totale ci sono dunque $(p^2 - 1)(p^2 - p)$ matrici.

10. Se p è primo e m un intero maggiore o uguale a 2, trovare una formula per il numero di matrici di ordine m invertibili in $\mathbb{Z}_p$.