

1. Sia $n \in \mathbf{Z}$ un numero pari.
 - (a) Fattorizzare $n^2 + 1$ per $n = 8$ e per $n = 12$.
 - (b) Sia $m = n^2 + 1$. Dimostrare che $\bar{n} \in \mathbf{Z}_m^*$ ha ordine 4.
 - (c) Dimostrare che ogni divisore primo q di $n^2 + 1$ soddisfa $q \equiv 1 \pmod{4}$.
2. Sia p un numero primo e sia $M_p = 2^p - 1$ il p -esimo numero di Mersenne. Sia q un divisore primo di M_p .
 - (a) Dimostrare che $\bar{2} \in \mathbf{Z}_q^*$ ha ordine p .
 - (b) Dimostrare che $q \equiv 1 \pmod{p}$.
 - (c) Dimostrare che M_p è primo per ogni primo $p < 11$, ma che $M_{11} = 2047$ non è primo.
3. Sia $k \in \mathbf{Z}_{\geq 0}$ e sia $F_k = 2^{2^k} + 1$ il k -esimo numero di Fermat. Sia q un divisore primo di F_k .
 - (a) Dimostrare che $\bar{2} \in \mathbf{Z}_q^*$ ha ordine 2^{k+1} .
 - (b) Dimostrare che $q \equiv 1 \pmod{2^{k+1}}$.
 - (c) Dimostrare che F_k è primo per ogni $k < 5$, ma che $F_5 = 4294967297$ non è primo.
4. Sia G un gruppo. Sia $e \in G$ l'elemento neutro.
 - (a) Sia $H = G$. Dimostrare che G/H è il gruppo banale.
 - (b) Sia $H = \{e\}$. Dimostrare che G/H è isomorfo a G .
5. Dimostrare che per ogni sottogruppo H di $\mathbf{Z}$ esiste $n \in \mathbf{Z}$ tale che $H = \{kn : k \in \mathbf{Z}\}$. Dimostrare che per $n \neq 0$ si ha che $\mathbf{Z}/H = \mathbf{Z}_n$. Determinare la struttura di $\mathbf{Z}/H$ quando $n = 0$.
6. Sia $m \in \mathbf{Z}_{>0}$. Dimostrare che per ogni sottogruppo H di $\mathbf{Z}_m$ esiste un divisore d di m tale che $H = \{\bar{a} \in \mathbf{Z}_m : d \text{ divide } a\}$. Enumerare i sottogruppi di $\mathbf{Z}_{12}$.
7. Dimostrare che un sottogruppo di un gruppo ciclico è ciclico. Dimostrare che un quoziente di un gruppo ciclico è ciclico.
8. Sia $G = \mathbf{Z}_{20}^*$.
 - (a) Sia H il sottogruppo generato da $\bar{9}$. Stabilire se il gruppo quoziente G/H è ciclico o meno.
 - (b) Sia H il sottogruppo generato da $\bar{19}$. Stabilire se il gruppo quoziente G/H è ciclico o meno.
9. Sia $G = \mathbf{Z}_{32}^*$.
 - (a) Sia H il sottogruppo generato da $\bar{25}$ e $\bar{31}$. Stabilire se il gruppo quoziente G/H è ciclico o meno.
 - (b) Sia H il sottogruppo generato da $\bar{5}$ e $\bar{9}$. Stabilire se il gruppo quoziente G/H è ciclico o meno.
10. Sia G il gruppo $\mathbf{Z}_2 \times \mathbf{Z}_8$ e sia H il sottogruppo generato dall'elemento v . Nei seguenti casi determinare l'ordine di v e determinare la struttura del gruppo quoziente G/H .
 - (a) $v = (\bar{0}, \bar{2})$; (b) $v = (\bar{1}, \bar{0})$; (c) $v = (\bar{1}, \bar{2})$.