1. Sia φ la funzione phi di Euler. Calcolare $\varphi(23)$, $\varphi(24)$, $\varphi(25)$, $\varphi(60)$, $\varphi(101)$.

2. (a) Stabilire se esistono $s, t \in \mathbf{Z}$ tali che $24s + 18t = 20$;
   (b) Stabilire se esistono $s, t \in \mathbf{Z}$ tali che $24s + 18t = -12$;
   (c) Stabilire se esistono $s, t \in \mathbf{Z}$ tali che $24s + 18t = 3$.

3. Determinare tutte le soluzioni $x \in \mathbf{Z}$ delle seguenti congruenze
   (a) $x \equiv 3 \pmod{11}$; (b) $3x \equiv 1 \pmod{5}$; (c) $9x \equiv 0 \pmod{30}$.

4. Stabilire se per le seguenti congruenze esistono soluzioni $x \in \mathbf{Z}$. In caso affermativo, determinarle tutte. (a) $5x \equiv 8 \pmod{17}$ (b) $9x \equiv 26 \pmod{30}$.

5. Determinare tutte le soluzioni $x \in \mathbf{Z}$ dei seguenti sistemi di congruenze
   (a) $\begin{cases} x \equiv 3 \pmod{7}, \\ x \equiv 7 \pmod{11}; \end{cases}$ (b) $\begin{cases} x \equiv 4 \pmod{8}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 4 \pmod{9}; \end{cases}$ (c) $\begin{cases} 5x \equiv 4 \pmod{8}, \\ 3x \equiv 3 \pmod{5}, \\ 2x \equiv 4 \pmod{9}; \end{cases}$

6. Sia G un gruppo e sia $g \in G$. Sia $f : \mathbf{Z} \longrightarrow G$ l'applicazione definita da $f(n) = g^n$. Dimostrare che f è un omomorfismo e descrivere il nucleo e l'immagine in termini dell'ordine dell'elemento g.

7. Siano $d, n \in \mathbf{Z}_{\geq 1}$ e supponiamo che d sia un divisore di n.
   (a) Dimostrare che l'applicazione $r : \mathbf{Z}_n \longrightarrow \mathbf{Z}_d$ data da $r(a \pmod{n}) = (a \pmod{d})$ è un omomorfismo ben definito. Far vedere che è suriettivo.
   (b) Dimostrare che l'applicazione $s : \mathbf{Z}_n^* \longrightarrow \mathbf{Z}_d^*$ data da $s(a \pmod{n}) = (a \pmod{d})$ è un omomorfismo ben definito. Far vedere che è suriettivo.

8. (*Numeri di Fermat*) Sia $n \geq 1$ un numero intero.
   (a) Dimostrare che $2^n + 1$ non è primo se n non è una potenza di 2.
   Sia $k \geq 0$, sia $F_k = 2^{2^k} + 1$ e sia q un divisore primo di F_k.
   (b) Dimostrare che $\overline{2} \in \mathbf{Z}_q^*$ ha ordine 2^{k+1}.
   (c) Dimostrare che $q \equiv 1 \pmod{2^{k+1}}$.
   (d) Dimostrare che F_k è primo per $k = 0, 1, 2, 3$ e 4 (Euler: ma non per $k = 5$).

9. Sia $n \in \mathbf{Z}_{>1}$.
   (a) Per $n = 2, 3, 4, 5$ fattorizzare $n^4 + 1$ in fattori primi.
   (b) Sia $m = n^4 + 1$. Dimostrare che $\overline{n} \in \mathbf{Z}_m^*$ ha ordine 8.
   (c) Dimostrare che ogni divisore primo $q > 2$ di $n^4 + 1$ soddisfa $q \equiv 1 \pmod{8}$.

10. (a) Determinare tutti gli interi $n > 0$ per cui il gruppo $\mathbf{Z}_n^*$ ha cardinalità 1.
    (b) Determinare tutti gli interi $n > 0$ per cui il gruppo $\mathbf{Z}_n^*$ ha cardinalità 2.
    (c) Determinare tutti gli interi $n > 0$ per cui il gruppo $\mathbf{Z}_n^*$ ha la proprietà che $\overline{x} \cdot \overline{x} = \overline{1}$ per ogni $\overline{x} = \mathbf{Z}_n^*$. (Sugg. distinguere due casi: 5 divide n o meno)