

1. (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 $24s + 18t = 3$.
2. Determinare tutte le soluzioni $x \in \mathbf{Z}$ delle seguenti congruenze
(a) $x \equiv 3 \pmod{11}$; (b) $3x \equiv 1 \pmod{5}$; (c) $9x \equiv 0 \pmod{30}$.
3. Stabilire se per le seguenti congruenze esistono soluzioni $x \in \mathbf{Z}$. In caso affermativo, determinarle tutte. (a) $5x \equiv 8 \pmod{17}$ (b) $9x \equiv 26 \pmod{30}$.
4. 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) $\begin{cases} 5x \equiv 4 \pmod{8}, \\ 3x \equiv 3 \pmod{5}, \\ 2x \equiv 4 \pmod{9}; \end{cases}$
5. Sia G un gruppo e sia $g \in G$. Sia $f : \mathbf{Z} \rightarrow G$ 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 .
6. Siano $d, n \in \mathbf{Z}_{\geq 1}$ e supponiamo che d sia un divisore di n .
(a) Dimostrare che l'applicazione $r : \mathbf{Z}_n \rightarrow \mathbf{Z}_d$ data da $r(a \pmod{n}) = (a \pmod{d})$ è un omomorfismo ben definito. Far vedere che è suriettivo.
(b) Dimostrare che l'applicazione $s : \mathbf{Z}_n^* \rightarrow \mathbf{Z}_d^*$ data da $s(a \pmod{n}) = (a \pmod{d})$ è un omomorfismo ben definito. Far vedere che è suriettivo.
7. Sia $p > 2$ un numero primo e sia $T_p = \frac{1}{2}(3^p - 1)$.
(a) Dimostrare che T_p non è primo se p non è primo.
Supponiamo che p sia primo. Sia q un divisore primo di T_p .
(b) Dimostrare che $\bar{3} \in \mathbf{Z}_q^*$ ha ordine p .
(c) Dimostrare che $q \equiv 1 \pmod{p}$.
(d) Dimostrare che T_p è primo per $p = 3$ e $p = 7$, ma non per $p = 5$ e $p = 11$.
8. 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 $\bar{n} \in \mathbf{Z}_m^*$ ha ordine 8.
(c) Dimostrare che ogni divisore primo $q > 2$ di $n^4 + 1$ soddisfa $q \equiv 1 \pmod{8}$.
9. (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 $\bar{x} \cdot \bar{x} = \bar{1}$ per ogni $\bar{x} \in \mathbf{Z}_n^*$. (Sugg. distinguere due casi: 5 divide n o meno)
10. Sia G il gruppo $\mathbf{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. Determinare le classi laterali dei sottogruppi $H_1 = \{\bar{1}, \bar{3}\}$, di $H_2 = \{\bar{1}, \bar{5}\}$ e di $H_3 = \{\bar{1}, \bar{7}\}$.