Istituzioni di Algebra e Geometria — Algebra, 2023-2024
Esercizi, foglio 6

1. (a) Dimostrare che $p \in \mathbb{N}$ è primo se e solo se non ha divisori d tali che $1 < d \leq \sqrt{p}$.
   (b) Stabilire quale fra i seguenti numeri è primo: 431, 433, 435, 437.

2. Calcolare il massimo comune divisore delle seguenti coppie di numeri tramite l'algoritmo d'Euclide, e poi esprimerlo come combinazione lineare dei due interi.

$$(707, 1991), \qquad (3937, 3441), \qquad (5407, 6077), \qquad (14351, 14803).$$

3. Siano $a, b \in \mathbb{Z}$.
   (a) Dimostrare che se $d = \mathrm{MCD}(a, b)$ allora a/d e b/d sono coprimi.
   (b) Dimostrare che per ogni $c \in \mathbb{Z}$ risulta $\mathrm{MCD}(ac, bc) = |c|\,\mathrm{MCD}(a, b)$.

4. Siano $a, b, c \in \mathbb{Z}$. Dimostrare che se $\mathrm{MCD}(a, b) = \mathrm{MCD}(a, c) = 1$, allora $\mathrm{MCD}(a, bc) = 1$.

5. Determinare la tavola di addizione e moltiplicazione di $\mathbb{Z}_9$. Elencare gli elementi del gruppo moltiplicativo $\mathbb{Z}_9^*$ calcolandone l'ordine: stabilire se il gruppo moltiplicativo $\mathbb{Z}_9^*$ è isomorfo a $\mathbb{Z}_6$, a $\mathbb{Z}_2 \times \mathbb{Z}_3$, a D_3, o a A_3.

6. Dimostrare che valgono le seguenti uguaglianze fra sottogruppi del gruppo additivo $\mathbb{Z}$:

$$n\mathbb{Z} \vee m\mathbb{Z} = \mathrm{MCD}(n, m)\mathbb{Z}, \qquad n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{mcm}(n, m)\mathbb{Z}.$$

7. Stabilire quali fra i seguenti numeri interi

$$220, \quad 119, \quad 101, \quad -101, \quad 779, \quad 769, \quad -779, \quad -321, \quad 981.$$

è soluzione del seguente sistema di congruenze

$$\begin{cases} 2x \equiv 6 \pmod{8} \\ 9x \equiv 4 \pmod{11} \\ 2x \equiv 3 \pmod{5}. \end{cases}$$

8. Stabilire se il seguente sistema di congruenze

$$\begin{cases} x \equiv 9 \pmod{14} \\ x \equiv 14 \pmod{9} \end{cases}$$

ha soluzione. In caso affermativo determinarne le soluzioni in $\mathbb{Z}$.

9. Stabilire se il seguenti sistemi di congruenze

$$\begin{cases} 2x \equiv 9 \pmod{13} \\ 3x \equiv 6 \pmod{9} \end{cases} \qquad \begin{cases} 2x \equiv 4 \pmod{6} \\ 3x \equiv 7 \pmod{13} \end{cases}$$

sono equivalenti. In caso affermativo determinarne le soluzioni in $\mathbb{Z}$.

10. Siano dati $G = \mathbb{Z}_6 \times \mathbb{Z}_5$ e $H = \mathbb{Z}_3 \times \mathbb{Z}_{10}$.
    (a) Esiste un isomorfismo dei gruppi additivi G e H?
    (b) Esiste un isomorfismo dei gruppi moltiplicativi G^* e H^*?

11. Siano dati $G = \mathbb{Z}_6 \times \mathbb{Z}_3$ e $H = \mathbb{Z}_2 \times \mathbb{Z}_9$.
    (a) Esiste un isomorfismo dei gruppi additivi G e H?
    (b) Esiste un isomorfismo dei gruppi moltiplicativi G^* e H^*?

12. Determinare $\mathrm{Aut}(\mathbb{Z})$, $\mathrm{Aut}(\mathbb{Z}_4)$, $\mathrm{Aut}(\mathbb{Z}_5)$.

N.B. Ricordate che in generale il metodo per risolvere un esercizio non è unico. Se qualche cosa non vi è chiara, e/o se pensate di aver trovato un errore di stampa, fatemi sapere!