Istituzioni di Algebra e Geometria — Algebra, a.a. 2025-2026
Soluzioni foglio 7

1. Con l'algoritmo euclideo troviamo $\mathrm{MCD}(707, 1991) = 1 = 873 \cdot 707 + (-310) \cdot 1991$:

$$\begin{aligned}
1991 &= 2 \cdot 707 + 577 \\
707 &= 1 \cdot 577 + 130 \\
577 &= 4 \cdot 130 + 57 \\
130 &= 2 \cdot 57 + 16 \\
57 &= 3 \cdot 16 + 9 \\
16 &= 1 \cdot 9 + 7 \\
9 &= 1 \cdot 7 + 2 \\
7 &= 3 \cdot 2 + \boxed{1} \\
2 &= 2 \cdot 1 + \mathbf{0}
\end{aligned}$$

Ripetendo i passaggi all'indietro troviamo:

$$\begin{aligned}
\boxed{1} &= 7 - 3 \cdot 2 \\
&= 7 - 3(9 - 1 \cdot 7) = 4 \cdot 7 - 3 \cdot 9 \\
&= 4(16 - 1 \cdot 9) - 3 \cdot 9 = 4 \cdot 16 - 7 \cdot 9 \\
&= 4 \cdot 16 - 7(57 - 3 \cdot 16) = 25 \cdot 16 - 7 \cdot 57 \\
&= 25(130 - 2 \cdot 57) - 7 \cdot 57 = 25 \cdot 130 - 57 \cdot 57 \\
&= 25 \cdot 130 - 57(577 - 4 \cdot 130) = 253 \cdot 130 - 57 \cdot 577 \\
&= 253(707 - 1 \cdot 577) - 57 \cdot 577 = 253 \cdot 707 - 310 \cdot 577 \\
&= 253 \cdot 707 - 310(1991 - 2 \cdot 707) = \boxed{873 \cdot 707 - 310 \cdot 1991}
\end{aligned}$$

Con lo stesso metodo, calcoliamo che $\mathrm{MCD}(3937, 3441) = 31 = 7 \cdot 3937 + (-8) \cdot 3441$:

$$\begin{aligned}
3937 &= 1 \cdot 3441 + 496 \\
3441 &= 6 \cdot 496 + 465 \\
496 &= 1 \cdot 465 + \boxed{31} \\
465 &= 15 \cdot 31 + \mathbf{0}
\end{aligned}$$

e risalendo nei passaggi sopra:

$$\begin{aligned}
\boxed{31} &= 496 - 1 \cdot 465 \\
&= 496 - 1(3441 - 6 \cdot 496) = 7 \cdot 496 - 1 \cdot 3441 \\
&= 7(3937 - 1 \cdot 3441) - 1 \cdot 3441 = \boxed{7 \cdot 3937 - 8 \cdot 3441}
\end{aligned}$$

Provate voi a calcolare che

- $\mathrm{MCD}(5407, 6077) = 1 = 460 \cdot 6077 + (-517) \cdot 5407$,
- $\mathrm{MCD}(14351, 14803) = 113 = 32 \cdot 14803 + (-33) \cdot 14351$.

2. (a) Se p è primo, per definizione, non può avere divisori d tali che $1 < d \leq \sqrt{p} < p$. Viceversa, se p non è primo, esistono $a, b \in \mathbb{Z}$, $a, b > 1$ tali che $p = ab$. Se $a, b > \sqrt{p}$, allora
$$p = ab = (\sqrt{p})^2 > p,$$
che è assurdo. Quindi almeno uno tra a e b deve essere minore o uguale a $\sqrt{p}$.

   (b) Si ha $21^2 = 441$: per quanto visto quindi sopra basta vedere quale fra 2, 3, 5, 7, 11, 13, 17, 19 divide i numeri dati. Chiaramente 435 non è primo, essendo multiplo di 3 e 5. Per i noti criteri di divisibilità, nessuno dei rimanenti numeri è divisibile per 2, 3, 5, 11. Infine l'unico tra 431, 433 e 37 tale che il resto della divisione intera per 13, 17, 19 è nullo è 437, che è un multiplo di 19. In conclusione, 431 e 433 sono numeri primi, 435 e 437 no.

3. Se $\mathrm{MCD}(a, b) = \mathrm{MCD}(a, c) = 1$, esistono interi $x, y, u, v \in \mathbb{Z}$ tali che: $1 = xa + yb$ e $1 = ua + vc$. Allora
$$1 = (xa + yb)(ua + vc) = xua^2 + xvac + yuab + yvbc = (xua + xvc + yub)a + (yv)bc,$$
da cui si deduce che $\mathrm{MCD}(a, bc) = 1$.

4. (a) Dati due interi $n, m \in \mathbb{Z}$, esistono $x, y \in \mathbb{Z}$ tali che $z = xn + ym$ se e solo se z è multiplo di $d = \mathrm{MCD}(n, m)$. Quindi
$$\begin{aligned}(n) + (m) &= \{z \in \mathbb{Z} \mid z = z_1 + z_2, z_1 \in (n), z_2 \in (m)\} \\ &= \{z \in \mathbb{Z} \mid z = xn + ym, \text{per qualche } x, y \in \mathbb{Z}\} \\ &= \{z \in \mathbb{Z} \mid z = \alpha d, d = \mathrm{MCD}(n, m), \alpha \in \mathbb{Z}\} = (d).\end{aligned}$$

   (b) Abbiamo che
$$\begin{aligned}(n) \cap (m) &= \{z \in \mathbb{Z} \mid z \in (n) \text{ e } z \in (m)\} \\ &= \{z \in \mathbb{Z} \mid z = xn \text{ e } z = ym, \text{per qualche } x, y \in \mathbb{Z}\} \\ &= \{z \in \mathbb{Z} \mid z = \alpha k, k = \mathrm{mcm}(n, m), \alpha \in \mathbb{Z}\} = (k).\end{aligned}$$

5. Sia $d = \mathrm{MCD}(n, m)$; verifichiamo che $n\mathbb{Z} \vee m\mathbb{Z} = d\mathbb{Z}$. Per definizione $n\mathbb{Z} \vee m\mathbb{Z}$ è il più piccolo sottogruppo che contiene l'unione insiemistica $n\mathbb{Z} \cup m\mathbb{Z}$. Ora, se $x \in n\mathbb{Z} \cup m\mathbb{Z}$, allora x è multiplo o di n o di m, e quindi è multiplo di d, quindi $x \in d\mathbb{Z}$. Poiché $d\mathbb{Z}$ è un sottogruppo, segue che $n\mathbb{Z} \vee m\mathbb{Z} \subseteq d\mathbb{Z}$. Viceversa, sia $x \in d\mathbb{Z}$, quindi x è della forma γd; a sua volta, d si scrive nella forma $\alpha n + \beta m$ per qualche $\alpha, \beta \in \mathbb{Z}$, quindi $x = \gamma d = \gamma(\alpha n + \beta m) = \gamma \alpha n + \gamma \beta m$, cioè x è della forma "elemento di $n\mathbb{Z}$ + elemento di $m\mathbb{Z}$", che come visto a lezione coincide con il sottogruppo unione. In altre parole, $n\mathbb{Z} \vee m\mathbb{Z} \supseteq d\mathbb{Z}$, e questo prova l'uguaglianza.

Sia $k = \mathrm{mcm}(n, m)$; verifichiamo che $n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$. Chiaramente $x \in n\mathbb{Z} \cap m\mathbb{Z}$ se e solo se x è multiplo sia di n che di m. Se ciò accade, allora è anche multiplo di k, dunque $x \in k\mathbb{Z}$ e quindi $n\mathbb{Z} \cap m\mathbb{Z} \subseteq k\mathbb{Z}$. Viceversa, se $x \in k\mathbb{Z}$ allora è multiplo di k, quindi anche di m e n, dunque $x \in n\mathbb{Z} \cap m\mathbb{Z}$ e quindi $n\mathbb{Z} \cap m\mathbb{Z} \supseteq k\mathbb{Z}$. Dalla doppia inclusione segue l'uguaglianza.

6. (a) Usando la formula di Bezout, se $d = \mathrm{MCD}(a, b)$, esistono $x, y \in \mathbb{Z}$ tali che $d = xa + yb$. Allora
$$1 = x\,\frac{a}{d} + y\,\frac{b}{d},$$
con $\frac{a}{d}$ e $\frac{b}{d}$ interi. Segue allora che $1 = \mathrm{MCD}(\frac{a}{d}, \frac{b}{d})$.

   (b) Distinguiamo i due casi: $c = 0$ e $c \neq 0$. Per definizione, $\mathrm{MCD}(0, 0) = 0$, quindi se $c = 0$ siamo a posto. Supponiamo $c \neq 0$ e sia $e = \mathrm{MCD}(ac, bc)$. Poiché c divide e, si ha che $\frac{e}{c}$ divide sia a che b. Per definizione di MCD allora $\frac{e}{c}$ divide d, quindi e divide $|c|d$. Viceversa: sappiamo che esistono $x, y \in \mathbb{Z}$ tali che $d = xa + yb$, quindi
$$|c|d = |c|(xa + yb) = \frac{c}{|c|}\ c\ (xa + yb) = \left(\frac{c}{|c|}x\right) ac + \left(\frac{c}{|c|}y\right) bc.$$
Deduciamo che $|c|d$ divide e. In totale quindi $e = |c|d$.

7. Poiché i divisori positivi di 4 sono solo 1, 2, e il 4 stesso, il fatto che $\mathrm{MCD}(a, 4) = 2$ implica che $2|a$, mentre il 4 non può dividere a. Quindi possiamo scrivere a nella forma $a = 2k$, con $k = 2m+1$ dispari, quindi $a = 2(2m + 1)$. Lo stesso ragionamento vale per b, e quindi $b = 2(2n + 1)$. Quindi $a + b = 2(2m + 1) + 2(2n + 1) = 2(2m + 2n + 2) = 4(m + n + 1)$, cioè $4|(a + b)$; concludiamo che $\mathrm{MCD}(a + b, 4) = 4$ (non ci possono essere divisori comuni più grandi di 4).

8. Sia $d = \mathrm{MCD}(a, b) = \mathrm{MCD}(a, c)$: quindi d è un divisore comune dei 3 numeri a, b e c, e quindi in particolare $d|\,\mathrm{MCD}(a, b, c)$. Se δ è un altro divisore comune di a, b e c allora in particolare δ è un divisore comune di a e b, e quindi per definizione di MCD $\delta|d$, che significa proprio che $d = \mathrm{MCD}(a, b, c)$.

9. La tavola di addizione di $\mathbb{Z}_9$ è la seguente, con ovvie notazioni:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{8}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$

Osserviamo in particolare che la tavola è simmetrica rispetto alla diagonale, come ci aspettiamo visto che l'addizione è commutativa.

La tavola di moltiplicazione è la seguente (tolgo direttamente lo $\overline{0}$, tanto moltiplicare qualsiasi cosa per $\overline{0}$ fa $\overline{0}$):

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{3}$	$\overline{7}$	$\overline{2}$	$\overline{6}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{6}$	$\overline{2}$	$\overline{7}$	$\overline{3}$	$\overline{8}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{8}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Dalla tavola di moltiplicazione si vede subito che $\mathbb{Z}_9^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$: infatti abbiamo visto a lezione che gli elementi di $\mathbb{Z}_9^*$ sono esattamente le classi degli elementi $x \in \mathbb{Z}$ tali che

$$\mathrm{MCD}(x, 9) = 1.$$

Risulta $\mathrm{ord}(\overline{1}) = 1$, $\mathrm{ord}(\overline{2}) = 6$, $\mathrm{ord}(\overline{4}) = 3$, $\mathrm{ord}(\overline{5}) = 6$, $\mathrm{ord}(\overline{7}) = 3$, $\mathrm{ord}(\overline{8}) = 2$. Osserviamo che l'ordine di ogni elemento di $\mathbb{Z}_9^*$ deve dividere l'ordine di $\mathbb{Z}_9^*$, che è 6.

Il gruppo $\mathbb{Z}_9^*$ è commutativo, quindi non può essere isomorfo a D_3. Inoltre $\mathbb{Z}_9^*$ ha 6 elementi, mentre A_3 ne ha 3. Concludiamo che $\mathbb{Z}_9^*$ è isomorfo o a $\mathbb{Z}_6$ o a $\mathbb{Z}_2 \times \mathbb{Z}_3$; però per il Teorema cinese dei resti $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, quindi $\mathbb{Z}_9^*$ o è isomorfo ad entrambi, o a nessuno dei due. Mostriamo che è isomorfo a $\mathbb{Z}_6$ costruendo esplicitamente l'isomorfismo $f : (\mathbb{Z}_9^*, \cdot) \to (\mathbb{Z}_6, +)$ nel modo seguente:

$$f([1]_9) = [0]_6, \quad f([2]_9) = [1]_6, \quad f([4]_9) = [2]_6, \quad f([5]_9) = [5]_6, \quad f([7]_9) = [4]_6, \quad f([8]_9) = [3]_6.$$

(Uso la notazione $[-]_n$ per le classi di resto, che è più "pesante" di quella con la barretta sopra ma in questo caso rende tutto più chiaro.) Osserviamo che f è biettiva, e manda l'elemento neutro $[1]_9$ nell'elemento neutro $[0]_6$. Inoltre si può calcolare esplicitamente che per ogni elemento x del dominio vale che $\mathrm{ord}(x) = \mathrm{ord}(f(x))$ nel codominio. Infine, si verifica che f è un omomorfismo, e cioè che vale $f(x \cdot y) = f(x) + f(y)$ per ogni coppia di elementi x e y del dominio. Ad esempio,

$$f([2]_9 \cdot [4]_9) = f([8]_9) = [3]_6 = [1]_6 + [2]_6 = f([2]_9) + f([4]_9),$$

$$f([2]_9 \cdot [5]_9) = f([1]_9) = [0]_6 = [1]_6 + [5]_6 = f([2]_9) + f([5]_9),$$

e così via.

10. Procediamo nello stesso modo dell'esercizio precedente. Di nuovo, troviamo 2 tavole simmetriche rispetto alla diagonale, perché entrambe le operazioni sono commutative. Per questo, ne scrivo esplicitamente solo la parte triangolare superiore (e nella tabella della moltiplicazione tolgo direttamente lo $\overline{0}$).

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{1}$		$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$
$\overline{2}$			$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$
$\overline{3}$				$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$					$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$						$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$							$\overline{4}$	$\overline{5}$
$\overline{7}$								$\overline{6}$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$		$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$			$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$				$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$					$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$						$\overline{4}$	$\overline{2}$
$\overline{7}$							$\overline{1}$

Dalla tavola di moltiplicazione si vede che $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, che come sappiamo sono precisamente le classi degli elementi $x \in \{0, 1, \ldots, 7\}$ che sono coprimi con 8.

Come sempre, $\mathrm{ord}(\overline{1}) = 1$; osserviamo poi che $\overline{3}^2 = \overline{5}^2 = \overline{7}^2 = \overline{1}$, che significa che $\mathrm{ord}(\overline{3}) = \mathrm{ord}(\overline{5}) = \mathrm{ord}(\overline{7}) = 2$.

Di conseguenza, poiché gli isomorfismi di gruppi mantengono l'ordine degli elementi, $(\mathbb{Z}_8^*, \cdot)$ non può essere isomorfo al gruppo additivo $(\mathbb{Z}_4, +)$, dove l'elemento $[1]_4$ ha ordine 4 (passo di nuovo alla notazione $[-]_n$ per chiarezza). Invece osserviamo che in

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{([0]_2, [0]_2), ([0]_2, [1]_2), ([1]_2, [0]_2), ([1]_2, [1]_2)\}$$

l'elemento neutro ha ordine 1, e gli altri 3 elementi hanno ordine 2. Definiamo allora l'applicazione biettiva $g : (\mathbb{Z}_8^*, \cdot) \to (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ tale che:

$$g([1]_8) = ([0]_2, [0]_2), \quad g([3]_8) = ([0]_2, [1]_2), \quad g([5]_8) = ([1]_2, [0]_2), \quad g([7]_8) = ([1]_2, [1]_2).$$

È immediato verificare che g è un omomorfismo, infatti:

$$g([3]_8 \cdot [5]_8) = g([7]_8) = ([1]_2, [1]_2) = ([0]_2, [1]_2) + ([1]_2, [0]_2) = g([3]_8) + g([5]_8);$$

$$g([3]_8 \cdot [7]_8) = g([5]_8) = ([1]_2, [0]_2) = ([0]_2, [1]_2) + ([1]_2, [1]_2) = g([3]_8) + g([7]_8);$$

$$g([5]_8 \cdot [7]_8) = g([3]_8) = ([0]_2, [1]_2) = ([1]_2, [0]_2) + ([1]_2, [1]_2) = g([5]_8) + g([7]_8).$$

11. (a) Per il Teorema cinese dei resti, poiché $\mathrm{MCD}(6, 5) = \mathrm{MCD}(3, 10) = 1$, i gruppi additivi $G = \mathbb{Z}_6 \times \mathbb{Z}_5$ e $H = \mathbb{Z}_3 \times \mathbb{Z}_{10}$ sono entrambi isomorfi a $\mathbb{Z}_{30}$: in particolare sono isomorfi fra di loro.

(b) Poiché $G \cong H$ come gruppi additivi, lo stesso vale per i gruppi moltiplicativi

$$G^* \cong H^* \cong \mathbb{Z}_{30}^* = \{[1]_{30}, [7]_{30}, [11]_{30}, [13]_{30}, [17]_{30}, [19]_{30}, [23]_{30}, [29]_{30}\}.$$

12. (a) Osserviamo intanto che, poiché $\mathrm{MCD}(2,9) = 1$, il gruppo additivo $H = \mathbb{Z}_2 \times \mathbb{Z}_9$ è isomorfo a $\mathbb{Z}_{18}$, mentre altrettanto non si può dire per $G = \mathbb{Z}_6 \times \mathbb{Z}_3$. Supponiamo infatti che esista un isomorfismo $\varphi\colon G \to H$. Allora $\mathrm{ord}(g) = \mathrm{ord}(\varphi(g))$: poiché tutti gli elementi di G hanno ordine che divide 6, mentre $([1]_2, [1]_9) \in H$ ha ordine 18, un tale φ non può esistere.

    (b) È facile verificare che

$$G^* = \{([1]_6, [1]_3), ([1]_6, [2]_3), ([5]_6, [1]_3), ([5]_6, [2]_3)\},$$

$$H^* = \{([1]_2, [1]_9), ([1]_2, [2]_9), ([1]_2, [4]_9), ([1]_2, [5]_9), ([1]_2, [7]_9), ([1]_2, [8]_9)\},$$

usando i risultati visti a lezione. In particolare $|G^*| = 4 \neq 6 = |H^*|$, quindi non può esistere un'applicazione biettiva $G^* \to H^*$, né tantomeno un isomorfismo.

13. Sappiamo che i gruppi $\mathbb{Z}$, $\mathbb{Z}_4$, $\mathbb{Z}_5$ sono tutti e tre ciclici, e che ogni automorfismo di gruppi ciclici deve trasformare generatori in generatori (potete rivedere l'esercizio 5 del foglio 5).

I generatori ciclici di $\mathbb{Z}$ sono 1 e -1. Quindi gli automorfismi di $\mathbb{Z}$ sono $\mathrm{id}\colon n \mapsto n$ e $-\mathrm{id}\colon n \mapsto -n$: in particolare $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

I generatori ciclici di $\mathbb{Z}_4$ sono le classi di 1 e di 3. Quindi, posto $\overline{n} = n \pmod 4$, gli automorfismi di $\mathbb{Z}_4$ sono $\mathrm{id}\colon \overline{n} \mapsto \overline{n}$ e $-\mathrm{id}\colon \overline{n} \mapsto \overline{3n}$: in particolare anche $\mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$.

Infine, ogni elemento non nullo di $\mathbb{Z}_5$ è un suo generatore ciclico. Quindi, posto $\overline{n} = n \pmod 5$, gli automorfismi di $\mathbb{Z}_5$ sono $\mathrm{id}\colon \overline{n} \mapsto \overline{n}$, $\varphi\colon \overline{n} \mapsto \overline{2n}$, $\psi\colon \overline{n} \mapsto \overline{3n}$, $\vartheta\colon \overline{n} \mapsto \overline{4n}$. In particolare $|\mathrm{Aut}(\mathbb{Z}_5)| = 4$, quindi o $\mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$ o $\mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Si noti che

$$\varphi^2(\overline{n}) = \overline{4n} = \vartheta(\overline{n}), \varphi^3(\overline{n}) = \overline{8n} = \overline{3n} = \psi(\overline{n}), \varphi^4(\overline{n}) = \overline{16n} = \overline{n} = \mathrm{id}(\overline{n}).$$

quindi $\mathrm{Aut}(\mathbb{Z}_5) = \{\mathrm{id}, \varphi, \varphi^2, \varphi^3\}$, da cui deduciamo che $\mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$.

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!