Istituzioni di Algebra e Geometria — Algebra, a.a. 2023-2024

Soluzioni foglio 6

1. (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 sopra basta vedere quale fra 2, 3, 5, 7, 11, 13, 17, 19 divide i numeri dati. Chiaramente 435 non è primo. Per i noti criteri di divisibilità, nessuno dei rimanenti numeri è divisibile per 2, 3, 5, 11. Infine il resto della divisione intera per 13, 17, 19 è nullo se e solo se 437: in particolare 431 e 433 sono primi, 435 e 437 non sono primi.

2. 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:

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

Provate voi a calcolare che

- $\mathrm{MCD}(3937, 3441) = 31 = 7 \cdot 3937 + (-8) \cdot 3441$,
- $\mathrm{MCD}(5407, 6077) = 1 = 460 \cdot 6077 + (-517) \cdot 5407$,
- $\mathrm{MCD}(14351, 14803) = 113 = 32 \cdot 14803 + (-33) \cdot 14351$.

3. (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 a/d e b/d interi. Segue allora che $1 = \mathrm{MCD}(a/d, b/d)$.

   (b) Distinguiamo i due casi $c = 0$, $c \neq 0$. 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 e/c divide sia a che b. Per definizione di MCD allora 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 $e = |c|d$.

4. 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 $\mathrm{MCD}(a, bc) = 1$.

5. 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 $\mathbb{Z}_9^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$: gli elementi di $\mathbb{Z}_9^*$ sono esattamente le classi degli elementi $x \in \mathbb{Z}$ tali che

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

Risulta $\overline{1} = 1$, $\overline{2} = 6$, $\overline{4} = 3$, $\overline{5} = 6$, $\overline{7} = 3$, $\overline{8} = 2$. Si noti 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 $\mathbb{Z}_2 \times \mathbb{Z}_3$: provate a dimostrare voi che $\mathbb{Z}_9^*$ è isomorfo a entrambi.

6. Questo è sostanzialmente la stessa cosa che l'esercizio 13, foglio 5, controllate!

7. Calcoliamo direttamente che $2 \cdot 220 = 440 = 55 \cdot 8$, quindi $2 \cdot 220 \equiv 0 \pmod 8$, cioè 220 non soddisfa il sistema di congruenze. D'altra parte $2 \cdot 119 = 238 = 29 \cdot 8 + 6$, $9 \cdot 119 = 1071 = 97 \cdot 11 + 4$, $2 \cdot 119 = 238 = 47 \cdot 5 + 3$, quindi 119 soddisfa il sistema di congruenze.

   Lascio a voi la verifica dei casi restanti.

8. Dalla prima congruenza ricaviamo che $x = 9 + 14y$ con $y \in \mathbb{Z}$. Sostituendo nella seconda congruenza otteniamo $14y \equiv 14 \pmod 9$. Moltiplicando ambo i membri per 2 otteniamo allora $y \equiv 1 \pmod 9$, cioè $y = 1 + 9z$ con $z \in \mathbb{Z}$. Pertanto il sistema di congruenze ha come soluzione

$$x = 23 + 126z, \qquad z \in \mathbb{Z}.$$

9. Osserviamo che 2 e 3 sono invertibili modulo 13: i loro inversi sono rispettivamente 7 e 9. Quindi i due sistemi sono rispettivamente equivalenti a

$$\begin{cases} x \equiv 11 \pmod{13} \\ 3x \equiv 6 \pmod 9, \end{cases} \qquad \begin{cases} 2x \equiv 4 \pmod 6 \\ x \equiv 11 \pmod{13}. \end{cases}$$

   Le soluzioni della congruenza $3x \equiv 6 \pmod 9$ sono tutti e soli gli interi che soddisfano l'equazione $3x = 6 + 9y$ per qualche $y \in \mathbb{Z}$, cioè sono tutti e soli gli interi della forma $x = 2 + 3y$ per qualche $y \in \mathbb{Z}$: quindi la congruenza $3x \equiv 6 \pmod 9$ è equivalente alla congruenza $x \equiv 2 \pmod 3$.

   Per gli stessi motivi anche la congruenza $2x \equiv 4 \pmod 6$ è equivalente a $x \equiv 2 \pmod 3$, dunque entrambi i sistemi di congruenze sono equivalenti a

$$\begin{cases} x \equiv 11 \pmod{13} \\ x \equiv 2 \pmod 3. \end{cases}$$

   Poiché 3 e 13 sono (co)primi, sappiamo che le soluzioni esistono. Abbiamo

$$1 = \alpha \cdot 13 + \beta \cdot 3 = 1 \cdot 13 + (-4) \cdot 3,$$

   quindi la soluzione è

$$x = 11 \cdot (-4) \cdot 3 + 2 \cdot 1 \cdot 13 \pmod{13 \cdot 3} = -106 \pmod{39} = 11 \pmod{39}.$$

   Alternativamente, dalla prima congruenza ricaviamo che $x = 11 + 13y$, $y \in \mathbb{Z}$. Sostituendo nella seconda otteniamo $11 + 13y \equiv 2 \pmod 3$ che è equivalente a $y \equiv 0 \pmod 3$: le sue soluzioni sono $y = 3z$ con $z \in \mathbb{Z}$, quindi le soluzioni del sistema sono $x = 11 + 39z$, $z \in \mathbb{Z}$.

10. (a) Per il Teorema cinese dei resti, $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ e $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$, dunque entrambi i gruppi additivi sono isomorfi a $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$: in particolare sono isomorfi fra di loro.

    (b) Lascio a voi verificare che $G^* \cong H^*$.

11. (a) Supponiamo 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 $(1,1) \in H$ ha ordine 18, deduciamo che un tale φ non può esistere.

    (b) Lascio a voi verificare che

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

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

    Se esistesse un isomorfismo $\varphi\colon G^* \to H^*$, questo sarebbe anche un'applicazione biettiva. In particolare si dovrebbe avere $|G^*| = |H^*|$. Deduciamo che un tale φ non può esistere.

12. Si osservi che i tre gruppi $\mathbb{Z}$, $\mathbb{Z}_4$, $\mathbb{Z}_5$ sono tutti e tre ciclici. è evidente che ogni automorfismo di gruppi ciclici deve trasformare generatori ciclici in generatori ciclici.

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

    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 $id\colon \overline{n} \mapsto \overline{n}$, $\varphi\colon \overline{n} \mapsto \overline{2n}$, $\psi\colon \overline{n} \mapsto \overline{3n}$, $\vartheta\colon \overline{n} \mapsto \overline{4n}$. 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

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

    quindi $\mathrm{Aut}(\mathbb{Z}_5) = \{id, \varphi, \varphi^2, \varphi^3\}$, 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!