

## I Esonero di Matematica Discreta - a.a. 04/05

1. a. Si considerino i seguenti sottoinsiemi di  $\mathbf{R}$ :

$$A = \{x \in \mathbf{R} \mid x(x-2)(x-1)(x+1) = 0\}$$

$$B = \{x \in \mathbf{R} \mid 1/3 < x \leq 8\}$$

$$C = \{x \in \mathbf{R} \mid -2 \leq x < 5\}.$$

Determinare  $A \cap B$ ,  $B \cap C$ ,  $\mathcal{C}_{\mathbf{R}}(B) \cup C$ ,  $\mathcal{C}_{\mathbf{R}}(A) \cup C$  e  $C \setminus B$ .

- b. Scrivere esplicitamente l'insieme delle parti  $\mathcal{P}(A)$ .

- c. Esprimere l'insieme delle soluzioni della disequazione  $\frac{2x-3}{x+2} \geq 1$  in termini di alcuni dei precedenti sottoinsiemi di  $\mathbf{R}$ .

2. Sia  $f: \mathbf{Z} \rightarrow \mathbf{Q}$  l'applicazione definita come  $f(n) = 3^{-n}$  se  $n \geq 0$  e  $f(n) = \frac{1}{n}$  se  $n < 0$ .

- a. Provare che  $f$  è iniettiva.

- b. Determinare  $\text{Im } f \cap \mathbf{Z}$  e da quanto ricavato dedurre se  $f$  è suriettiva oppure no.

- c. Determinare  $f(D)$  e  $f^{-1}(E)$  dove  $D = \{-3, 0, 2\}$  ed  $E = \{-1/3, 1/3\}$ .

- d. Sia  $g: \mathbf{Z} \rightarrow \mathbf{Z}$  l'applicazione data da  $g(m) = m+2$  se  $m > 0$ ,  $g(0) = 1$  e  $g(m) = m-2$  se  $m < 0$ . Determinare esplicitamente l'applicazione composta  $f \circ g$ .

3. In  $\mathbf{N} \times \mathbf{N}$  si consideri la seguente relazione “ $(a, b) \sim (c, d)$  se e solo se  $a + b = c + d$ ”.

- a. Provare che  $\sim$  è una relazione di equivalenza.

- b. Determinare le classi di equivalenza di  $(0, 0)$ ,  $(1, 0)$  e  $(1, 3)$ .

- c. Indicato con  $X$  il quoziente  $\mathbf{N} \times \mathbf{N} / \sim$ , verificare che ponendo  $\varphi([(a, b)]) = a + b$  si ottiene una funzione  $\varphi: X \rightarrow \mathbf{N}$  ben definita e che l'applicazione  $\psi: \mathbf{N} \rightarrow X$  data da  $\psi(n) = [(n, 0)]$  è l'inversa di  $\varphi$ .

- d. Dire se la seguente relazione in  $X$  (dove  $X$  è il quoziente del punto precedente)

$$[(a, b)] \rho [(c, d)] \text{ se } a + b \text{ divide } c + d \text{ (ossia se } \exists h \in \mathbf{N} \text{ t.c. } c + d = h(a + b))$$

è una relazione d'ordine, e in caso affermativo dire se si tratta di un ordine parziale o totale.

4. Dimostrare mediante l'induzione che vale la seguente formula:

$$1 + 3 + 3^2 + \dots + 3^n = \frac{1}{2}(3^{n+1} - 1).$$

5. Supponiamo di avere a disposizione un mazzo usuale di 40 carte (con 10 carte dall'asso al re per ognuno dei 4 semi: cuori, quadri, fiori e picche).

- a. Facciamo pescare da un nostro amico 3 carte dal mazzo. Quanti sono in totale i gruppi di 3 carte che il nostro amico si può ritrovare in mano?

- b. In quanti modi diversi si possono scegliere dal mazzo una regina e un re?

- c. Siamo ad un tavolo con tre amici e distribuiamo una carta per ciascuno (compresi noi stessi). Quante sono le diverse distribuzioni di 4 carte che si possono avere?

- d. Se dal mazzo estraiamo 5 carte in sequenza annotando ogni carta estratta su un foglio e rimettendo la carta nel mazzo prima di fare la successiva estrazione, quante sono le possibili sequenze distinte che si possono ottenere?

## Svolgimento

### Esercizio 1

#### **Punto a.**

Sono dati i seguenti sottoinsiemi di  $\mathbf{R}$ :

$$A = \{x \in \mathbf{R} \mid x(x-2)(x-1)(x+1) = 0\} = \{0, 1, -1, 2\}$$

$$B = \{x \in \mathbf{R} \mid 1/3 < x \leq 8\} = (1/3, 8]$$

$$C = \{x \in \mathbf{R} \mid -2 \leq x < 5\} = [-2, 5)$$

allora risulta

$$A \cap B = \{1, 2\}$$

$$B \cap C = (1/3, 5)$$

$$\mathcal{C}_{\mathbf{R}}(B) \cup C = (-\infty, 5) \cup (8, +\infty)$$

$$\mathcal{C}_{\mathbf{R}}(A) \cup C = \mathbf{R}$$

$$C \setminus B = [-2, 1/3]$$

#### **Punto b.**

L'insieme delle parti  $\mathcal{P}(A)$  contiene tutti i sottoinsiemi di  $A = \{0, 1, -1, 2\}$ , ossia

$$\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{-1\}, \{2\}, \{0, 1\}, \{0, -1\}, \{0, 2\}, \{1, -1\}, \\ \{1, 2\}, \{-1, 2\}, \{0, 1, -1\}, \{0, 1, 2\}, \{0, -1, 2\}, \{1, -1, 2\}, A\}$$

#### **Punto c.**

La disequazione

$$\frac{2x-3}{x+2} \geq 1$$

è equivalente alla disequazione

$$\frac{x-5}{x+2} \geq 0$$

il cui insieme delle soluzioni  $S$  è dato da

$$S = (-\infty, -2) \cup [5, +\infty)$$

che in termini dei precedenti sottoinsiemi di  $\mathbf{R}$  è

$$S = \mathcal{C}_{\mathbf{R}}(C).$$

### Esercizio 2

Sia  $f: \mathbf{Z} \rightarrow \mathbf{Q}$  la funzione definita come

$$f(n) = \begin{cases} 3^{-n} & \text{se } n \geq 0 \\ \frac{1}{n} & \text{se } n < 0 \end{cases}$$

**Punto a.**

Siano  $n, m \in \mathbf{Z}$ :

se  $n \geq 0$  ed  $m \geq 0$ , con  $n \neq m$ , allora  $3^{-n} \neq 3^{-m}$ , per cui  $f(n) \neq f(m)$

se  $n < 0$  ed  $m < 0$ , con  $n \neq m$ , allora  $\frac{1}{n} \neq \frac{1}{m}$ , per cui  $f(n) \neq f(m)$

se  $n \geq 0$  ed  $m < 0$ , allora  $3^{-n} \geq 1$  e  $\frac{1}{m} < 0$ , per cui  $f(n) \neq f(m)$

pertanto  $f$  è una applicazione iniettiva.

**Punto b.**

Per come è definita la funzione  $f$  risulta che

per ogni intero  $n > 0$  allora  $f(n) = \frac{1}{3^n} \in \mathbf{Q} \setminus \mathbf{Z}$

$f(0) = 1 \in \mathbf{Z}$

per ogni intero  $n < 0$  allora  $f(n) = \frac{1}{n} \in \mathbf{Q} \setminus \mathbf{Z}$

pertanto  $\text{Im } f \cap \mathbf{Z} = \{1\}$ . Se ne deduce che  $f$  non è suriettiva.

**Punto c.**

Dati gli insiemi  $D = \{-3, 0, 2\}$  ed  $E = \{-1/3, 1/3\}$  risulta

$$f(D) = \left\{ -\frac{1}{3}, 1, \frac{1}{9} \right\}$$

poiché  $f(-3) = -\frac{1}{3}$ ,  $f(0) = 1$ ,  $f(2) = \frac{1}{9}$ , ed inoltre

$$f^{-1}(E) = \{-3, 1\}$$

poiché  $f(-3) = -\frac{1}{3}$  e  $f(1) = \frac{1}{3}$ .

**Punto d.**

Sia  $g: \mathbf{Z} \rightarrow \mathbf{Z}$  l'applicazione data da

$$g(m) = \begin{cases} m + 2 & \text{se } m > 0 \\ 1 & \text{se } m = 0 \\ m - 2 & \text{se } m < 0 \end{cases}$$

La funzione composta  $f \circ g$  è una applicazione da  $\mathbf{Z}$  in  $\mathbf{Z}$ . Risulta che

$$\text{se } m > 0 \quad \mapsto \quad g(m) = m + 2 > 0 \quad \mapsto \quad f(g(m)) = f(m + 2) = 3^{-(m+2)}$$

$$\text{se } m = 0 \quad \mapsto \quad g(0) = 1 > 0 \quad \mapsto \quad f(g(0)) = f(1) = 3^{-1} = \frac{1}{3}$$

$$\text{se } m < 0 \quad \mapsto \quad g(m) = m - 2 < 0 \quad \mapsto \quad f(g(m)) = f(m - 2) = \frac{1}{m - 2}$$

pertanto si ha

$$(f \circ g)(m) = \begin{cases} 3^{-(m+2)} & \text{se } m > 0 \\ \frac{1}{3} & \text{se } m = 0 \\ \frac{1}{m-2} & \text{se } m < 0 \end{cases}$$

### Esercizio 3

#### Punto a.

È data la relazione  $\sim$  in  $\mathbf{N} \times \mathbf{N}$  data da:  $(a, b) \sim (c, d) \Leftrightarrow a + b = c + d$ .

- Proprietà riflessiva:  $\forall (a, b) \in \mathbf{N} \times \mathbf{N}$  risulta  $a + b = a + b$ , quindi  $(a, b) \sim (a, b)$ .
- Proprietà simmetrica:  $\forall (a, b), (c, d) \in \mathbf{N} \times \mathbf{N}$  tali che  $(a, b) \sim (c, d)$  allora si ha  $a + b = c + d$ , pertanto  $c + d = a + b$ , ossia  $(c, d) \sim (a, b)$ .
- Proprietà transitiva:  $\forall (a, b), (c, d), (e, f) \in \mathbf{N} \times \mathbf{N}$  tali che  $(a, b) \sim (c, d)$  e  $(c, d) \sim (e, f)$ , allora si ha  $a + b = c + d$  e  $c + d = e + f$ , da cui segue che  $a + b = e + f$ , e dunque  $(a, b) \sim (e, f)$ .

$\sim$  è pertanto una relazione di equivalenza in  $\mathbf{N} \times \mathbf{N}$ .

#### Punto b.

Per definizione la classe di equivalenza individuata da  $(a, b) \in \mathbf{N} \times \mathbf{N}$  è data da

$$[(a, b)] = \{(n, m) \in \mathbf{N} \times \mathbf{N} \mid (n, m) \sim (a, b)\} = \{(n, m) \in \mathbf{N} \times \mathbf{N} \mid n + m = a + b\}$$

pertanto risulta

$$[(0, 0)] = \{(n, m) \in \mathbf{N} \times \mathbf{N} \mid n + m = 0\}$$

$$[(1, 0)] = \{(n, m) \in \mathbf{N} \times \mathbf{N} \mid n + m = 1\}$$

$$[(1, 3)] = \{(n, m) \in \mathbf{N} \times \mathbf{N} \mid n + m = 4\}$$

ovvero

$$[(0, 0)] = \{(0, 0)\}$$

$$[(1, 0)] = \{(1, 0), (0, 1)\}$$

$$[(1, 3)] = \{(4, 0), (3, 1), (2, 2), (1, 3), (0, 4)\}$$

#### Punto c.

Posto  $X = \mathbf{N} \times \mathbf{N} / \sim$  si deve verificare che  $\varphi: X \rightarrow \mathbf{N}$  data da  $\varphi([(a, b)]) = a + b$  è una funzione ben definita. Infatti per ogni  $[(a, b)] \in X$

$$\begin{aligned} [(a, b)] = [(c, d)] &\Leftrightarrow (a, b) \sim (c, d) \\ &\Leftrightarrow a + b = c + d \\ &\Rightarrow \varphi([(a, b)]) = \varphi([(c, d)]) \end{aligned}$$

e pertanto  $\varphi$  è ben definita.

Data ora l'applicazione  $\psi: \mathbf{N} \rightarrow X$  definita come  $\psi(n) = [(n, 0)]$  si deve verificare che  $\psi$  è l'inversa della funzione  $\varphi$ . Per ogni  $[(a, b)] \in X$  risulta

$$(\psi \circ \varphi)([(a, b)]) = \psi(\varphi([(a, b)])) = \psi(a + b) = [(a + b, 0)] = [(a, b)]$$

e per ogni  $n \in \mathbf{N}$  si ha

$$(\varphi \circ \psi)(n) = \varphi(\psi(n)) = \varphi([(n, 0)]) = n + 0 = n$$

pertanto

$$\psi \circ \varphi = \text{id}_X \quad \text{e} \quad \varphi \circ \psi = \text{id}_{\mathbf{N}}$$

ossia l'applicazione  $\psi$  è l'inversa di  $\varphi$ .

**Punto d.**

Nell'insieme quoziente  $X$  è data la seguente relazione

$$[(a, b)] \rho [(c, d)] \text{ se e solo se } \exists h \in \mathbf{N} \text{ tale che } c + d = h(a + b).$$

- Proprietà riflessiva:  $\forall [(a, b)] \in X$  esiste  $h = 1 \in \mathbf{N}$  tale che  $a + b = 1 \cdot (a + b)$ , ossia  $[(a, b)] \rho [(a, b)]$ .

- Proprietà antisimmetrica:  $\forall [(a, b)], [(c, d)] \in X$  tali che  $[(a, b)] \rho [(c, d)]$  e  $[(c, d)] \rho [(a, b)]$  allora esistono  $h, k \in \mathbf{N}$  tali che  $c + d = h(a + b)$  e  $a + b = k(c + d)$ , da cui segue che  $c + d = hk(c + d)$ , ossia  $(hk - 1)(c + d) = 0$ , quindi  $hk = 1$  in  $\mathbf{N}$ , per cui  $h = k = 1$  e dunque  $a + b = c + d$ , pertanto  $[(a, b)] = [(c, d)]$ .

- Proprietà transitiva:  $\forall [(a, b)], [(c, d)], [(e, f)] \in X$  tali che  $[(a, b)] \rho [(c, d)]$  e  $[(c, d)] \rho [(e, f)]$ , allora esistono  $h, k \in \mathbf{N}$  tali che  $c + d = h(a + b)$  e  $e + f = k(c + d)$ , quindi  $e + f = hk(a + b)$  dove  $hk \in \mathbf{N}$ , e quindi  $[(a, b)] \rho [(e, f)]$ .

Pertanto  $\rho$  è una relazione d'ordine in  $X$ .

Si tratta di un ordine parziale ma non totale, infatti risulta

$$[(5, 0)] \not\rho [(4, 0)] \quad \text{e} \quad [(4, 0)] \not\rho [(5, 0)]$$

poiché 5 non divide 4 e 4 non divide 5 in  $\mathbf{N}$ .

**Esercizio 4**

Si deve dimostrare mediante l'induzione che per ogni numero naturale vale l'uguaglianza:

$$1 + 3 + 3^2 + \dots + 3^n = \frac{1}{2}(3^{n+1} - 1).$$

Base dell'induzione:  $n = 0$

$$3^0 = 1 = \frac{1}{2}(3 - 1)$$

quindi la formula è vera per  $n = 0$ .

Passo induttivo: supponiamo vera l'uguaglianza per un qualche  $n \geq 0$  e verifichiamo che ne consegue la validità della formula per  $n + 1$ . Si ha (usando l'ipotesi induttiva)

$$\begin{aligned} 1 + 3 + \dots + 3^n + 3^{n+1} &= (1 + 3 + \dots + 3^n) + 3^{n+1} \\ &= \frac{1}{2}(3^{n+1} - 1) + 3^{n+1} \\ &= \frac{3}{2} \cdot 3^{n+1} - \frac{1}{2} \\ &= \frac{1}{2}(3^{n+2} - 1) \end{aligned}$$

Dunque per induzione la formula è valida per ogni numero naturale.

**Esercizio 5**

Si ha un usuale mazzo di 40 carte (con 10 carte dall'asso al re per ognuno dei 4 semi: cuori, quadri, fiori e picche).

**Punto a.**

Si tratta di contare quanti sottoinsiemi contenenti 3 elementi possiede un insieme di 40 elementi, ossia si tratta del numero di combinazioni semplici di 40 elementi a 3 a 3, quindi

$$C_{40,3} = \binom{40}{3} = \frac{40!}{3!37!}$$

**Punto b.**

In un mazzo di 40 carte ci sono 4 regine e 4 re (una regina e un re per ciascun seme), quindi in totale ci sono  $16 = 4 \times 4$  coppie formate da una regina e da un re.

**Punto c.**

Si richiede di contare il numero delle diverse distribuzioni di 4 carte (una carta a testa per 4 persone). Si tratta di disposizioni semplici di 40 elementi 4 a 4, quindi

$$D_{40,4} = \frac{40!}{(40-4)!} = \frac{40!}{36!} = 40 \cdot 39 \cdot 38 \cdot 37$$

**Punto d.**

Si richiede di contare il numero delle diverse estrazioni di 5 carte dal mazzo con reinserimento della carta estratta subito dopo la sua estrazione. Si tratta quindi di contare le disposizioni con ripetizione di 40 elementi a 5 a 5, dunque

$$D_{40,5}^r = 40^5$$

## II Esonero di Matematica Discreta - a.a. 04/05

- Trovare il MCD di 11237 e 3966 ed esplicitare l'identità di Bézout.
  - Trovare tutte le soluzioni dei seguenti sistemi di congruenze:

$$\begin{cases} 4x \equiv 5 \pmod{7} \\ 5x \equiv 3 \pmod{8} \\ 2x \equiv 8 \pmod{9} \end{cases} \quad \begin{cases} 2x \equiv 9 \pmod{15} \\ 11x \equiv 2 \pmod{20} \end{cases}$$

- Determinare la scrittura posizionale in base 7 del numero (che in base 10 si scrive) 1802 e la scrittura posizionale in base 10 del numero  $(233)_5$ , dove l'indice indica la base utilizzata.
- Nell'anello  $\mathbf{Z}_{51}$  delle classi di resto modulo 51 (notazione usata  $\bar{x} = [x]_{51}$ ) provare che  $\bar{6}$  è uno zero-divisore e determinare  $a \in \mathbf{Z}$  tale che  $\bar{a} \neq \bar{0}$  e  $\bar{6} \cdot \bar{a} = \bar{0}$ .
    - Dire se l'applicazione  $f: \mathbf{Z}_8 \rightarrow \mathbf{Z}_{12}$  data da  $f([n]_8) = [n^2]_{12}$  è ben definita.
    - Provare che l'applicazione  $g: \mathbf{Z}_8 \rightarrow \mathbf{Z}_{12}$  data da  $g([n]_8) = [3n]_{12}$  è ben definita e determinare  $\text{Im } g$ ,  $g^{-1}([0]_{12})$  e  $g^{-1}([1]_{12})$ .
  - Sia  $\mathbf{C}$  il campo dei numeri complessi:
    - Calcolare parte reale e coefficiente dell'immaginario del numero complesso:

$$\frac{(3 - 2i)^2}{1 + i}.$$

- Disegnare nel piano di Gauss l'insieme dei numeri complessi  $z$  tali che  $|z - 2| \leq 3$  e il cui argomento principale  $\theta$  verifica la condizione  $0 \leq \theta \leq \frac{\pi}{4}$ .
- Calcolare le radici terze del numero complesso  $\alpha = -125$ .
- Scomporre il polinomio  $F(X) = (X^3 + 125)(X^2 + X - 12)$  nel prodotto di fattori irriducibili in  $\mathbf{C}[X]$  e in  $\mathbf{R}[X]$ .
- Determinare le eventuali radici razionali del polinomio

$$G(X) = 2X^5 + 3X^4 + 11X^3 + 9X^2 + 1.$$

### 4. Esercizio Extra

Si consideri l'insieme  $E = \{z \in \mathbf{C} \mid z^n \in \mathbf{Z} \text{ per un qualche intero } n \geq 2\}$ .  
Dimostrare che  $E$  è numerabile.

### 5. Esercizio Extra

Dire, motivando la risposta, se nell'anello delle classi di resto  $\mathbf{Z}_{856}$  esiste un elemento  $[a]$  tale che l'insieme  $\{[a]^n \mid n \in \mathbf{N}\}$  contiene almeno 856 elementi distinti.

## Svolgimento

### Esercizio 1

#### **Punto a.**

Per calcolare il MCD di 11237 e 3966 si usa l'algoritmo di Euclide:

$$1) \quad 11237 = 3966 \cdot 2 + 3305$$

$$2) \quad 3966 = 3305 \cdot 1 + 661$$

$$3) \quad 3305 = 661 \cdot 5 + 0$$

pertanto il MCD cercato è l'ultimo resto non nullo, ossia

$$\text{MCD}(11237, 3966) = 661.$$

Per esplicitare l'identità di Bézout si utilizzano le divisioni successive precedenti, ma andando a ritroso, precisamente:

da **2)** si ha  $661 = 3966 - 3305$ ,

da **1)** si ha  $3305 = 11237 - 2 \cdot 3966$ , quindi sostituendo nell'uguaglianza precedente

$$661 = 3966 - (11237 - 2 \cdot 3966) = 3 \cdot 3966 - 11237,$$

pertanto l'identità di Bézout è

$$661 = (-1) \cdot 11237 + 3 \cdot 3966.$$

#### **Punto b.**

- Sistema di congruenze

$$\begin{cases} 4x \equiv 5 \pmod{7} \\ 5x \equiv 3 \pmod{8} \\ 2x \equiv 8 \pmod{9} \end{cases}$$

Risulta  $\text{MCD}(4, 7) = \text{MCD}(5, 8) = \text{MCD}(2, 9) = 1$ , quindi ognuna delle tre congruenze ammette soluzioni.

Si ha  $1 = 2 \cdot 4 - 7$ ,  $1 = 5 \cdot 5 - 3 \cdot 8$  e  $1 = 5 \cdot 2 - 9$ , quindi

$$[4]^{-1} = [2] \quad \text{in } \mathbf{Z}_7$$

$$[5]^{-1} = [5] \quad \text{in } \mathbf{Z}_8$$

$$[2]^{-1} = [5] \quad \text{in } \mathbf{Z}_9$$

per cui il sistema si trasforma nel seguente sistema equivalente

$$\begin{cases} x \equiv 10 \pmod{7} \\ x \equiv 15 \pmod{8} \\ x \equiv 40 \pmod{9} \end{cases}$$

ovvero

$$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 7 \pmod{8} \\ x \equiv 4 \pmod{9} \end{cases}$$

Risulta  $\text{MCD}(7, 8) = \text{MCD}(7, 9) = \text{MCD}(8, 9) = 1$  quindi per il Teorema Cinese dei Resti il sistema ammette sicuramente soluzioni, ed esiste un'unica soluzione  $x_0$  con  $0 \leq x_0 < 504 = 7 \cdot 8 \cdot 9 = \text{mcm}(7, 8, 9)$ .

L'insieme delle soluzioni della prima congruenza è

$$S_1 = \{3 + 7h \mid h \in \mathbf{Z}\} = \{3, 10, 17, 24, \mathbf{31}, 38, \dots\},$$

l'insieme delle soluzioni della seconda congruenza è

$$S_2 = \{7 + 8k \mid k \in \mathbf{Z}\} = \{7, 15, 23, \mathbf{31}, 39, \dots\},$$

mentre l'insieme delle soluzioni della terza congruenza è

$$S_3 = \{4 + 9l \mid l \in \mathbf{Z}\} = \{4, 13, 22, \mathbf{31}, 40, \dots\},$$

pertanto l'insieme delle soluzioni in  $\mathbf{Z}$  del sistema di congruenze è

$$S = \{31 + 504t \mid t \in \mathbf{Z}\}.$$

- Sistema di congruenze

$$\begin{cases} 2x \equiv 9 & \text{mod } 15 \\ 11x \equiv 2 & \text{mod } 20 \end{cases}$$

Risulta  $\text{MCD}(2, 15) = \text{MCD}(11, 20) = 1$  quindi le singole congruenze ammettono soluzioni, ma  $\text{MCD}(15, 20) = 5$  per cui non si può applicare il Teorema Cinese dei Resti, quindi non si può dire a priori se il sistema di congruenze ammette oppure no delle soluzioni.

Risulta  $1 = 8 \cdot 2 - 15$  e  $1 = 11 \cdot 11 - 10 \cdot 20$ , quindi

$$\begin{aligned} [2]^{-1} &= [8] && \text{in } \mathbf{Z}_{15} \\ [11]^{-1} &= [11] && \text{in } \mathbf{Z}_{20} \end{aligned}$$

per cui il sistema si trasforma nel seguente

$$\begin{cases} x \equiv 72 & \text{mod } 15 \\ x \equiv 22 & \text{mod } 20 \end{cases}$$

ossia

$$\begin{cases} x \equiv 12 & \text{mod } 15 \\ x \equiv 2 & \text{mod } 20 \end{cases}$$

Poiché  $\text{mcm}(15, 20) = 60$ , bisogna cercare se esiste una soluzione  $x_0$  comune alle due congruenze tale che  $0 \leq x_0 < 60$ . Ora l'insieme delle soluzioni della prima congruenza è

$$S_1 = \{12 + 15h \mid h \in \mathbf{Z}\} = \{12, 27, \mathbf{42}, 57, \dots\},$$

mentre l'insieme delle soluzioni della seconda congruenza è

$$S_2 = \{2 + 20k \mid k \in \mathbf{Z}\} = \{2, 22, \mathbf{42}, \dots\},$$

pertanto l'insieme delle soluzioni in  $\mathbf{Z}$  del sistema di congruenze è

$$S = \{42 + 60t \mid t \in \mathbf{Z}\}.$$

**Punto c.**

Per determinare la scrittura posizionale in base 7 del numero (che in base 10 si scrive) 1802 bisogna eseguire le seguenti divisioni con resto:

$$1802 = 257 \cdot 7 + 3$$

$$257 = 36 \cdot 7 + 5$$

$$36 = 5 \cdot 7 + 1$$

$$5 = 0 \cdot 7 + 5$$

quindi leggendo i resti di tali divisioni si ottiene che

$$(1802)_{10} = (5153)_7.$$

Per determinare la scrittura posizionale in base 10 del numero che in base 5 si scrive 233 si usa la definizione, ossia:

$$(233)_5 = 2 \cdot 5^2 + 3 \cdot 5 + 3 = 50 + 15 + 3 = (68)_{10}.$$

**Esercizio 2**

**Punto a.**

L'elemento  $\bar{6}$  nell'anello  $\mathbf{Z}_{51}$  delle classi di resto modulo 51 è uno zero-divisore perché risulta  $\text{MCD}(6, 51) = 3 > 1$ .

Per determinare  $a \in \mathbf{Z}$  tale che  $\bar{a} \neq \bar{0}$  e  $\bar{6} \cdot \bar{a} = \bar{0}$  basta osservare che

$$\text{mcm}(6, 51) = \frac{6 \cdot 51}{\text{MCD}(6, 51)} = \frac{6 \cdot 51}{3} = 6 \cdot 17$$

e pertanto  $a = 17$  verifica le condizioni richieste.

Oppure si può procedere nel seguente modo:

$$\begin{aligned} \text{risulta } \bar{6} \cdot \bar{a} = \bar{0} &\Leftrightarrow \overline{6a} = \bar{0} \\ &\Leftrightarrow 6a = 51k \quad \text{per un qualche } k \in \mathbf{Z} \end{aligned}$$

Dividendo ambo i membri dell'ultima uguaglianza per 3 si ottiene la relazione

$$2a = 17k$$

che risulta verificata (banalmente) prendendo  $a = 17$  e  $k = 2$ . Si ottiene quindi che in  $\mathbf{Z}_{51}$  risulta  $\bar{a} = \overline{17} \neq \bar{0}$  ed anche  $\bar{6} \cdot \overline{17} = \overline{102} = \bar{0}$ .

**Punto b.**

L'applicazione  $f: \mathbf{Z}_8 \rightarrow \mathbf{Z}_{12}$  data da  $f([n]_8) = [n^2]_{12}$  NON è ben definita, infatti si ha, ad esempio, che  $[0]_8 = [8]_8$  in  $\mathbf{Z}_8$  ma

$$\begin{aligned} f([0]_8) &= [0]_{12} \\ f([8]_8) &= [64]_{12} = [4]_{12} \end{aligned}$$

con  $[0]_{12} \neq [4]_{12}$  in  $\mathbf{Z}_{12}$ , ossia cambiando rappresentante ad una classe di equivalenza del dominio l'immagine mediante  $f$  cambia e pertanto  $f$  non è ben definita.

**Punto c.**

Per provare che l'applicazione  $g: \mathbf{Z}_8 \rightarrow \mathbf{Z}_{12}$  data da  $g([n]_8) = [3n]_{12}$  è ben definita bisogna verificare che cambiando rappresentante ad una qualsiasi classe di equivalenza nel dominio  $\mathbf{Z}_8$  non cambia l'immagine che si ottiene mediante  $g$ .

Sia quindi  $[n]_8 = [m]_8$  in  $\mathbf{Z}_8$ . Ciò è equivalente a dire che esiste  $k \in \mathbf{Z}$  tale che  $n = m + 8k$ , per cui

$$\begin{aligned} 3n &= 3(m + 8k) \\ &= 3m + 24k \\ &= 3m + 12 \cdot 2k \quad \text{con } 2k \in \mathbf{Z} \end{aligned}$$

dunque

$$[3n]_{12} = [3m]_{12}$$

ossia

$$[n]_8 = [m]_8 \quad \Rightarrow \quad g([n]_8) = g([m]_8)$$

e pertanto l'applicazione  $g$  è ben definita.

L'immagine di  $g$  è

$$\begin{aligned} \text{Im } g &= \{[x]_{12} \in \mathbf{Z}_{12} \mid [x]_{12} = g([n]_8) \text{ per qualche } [n]_8 \in \mathbf{Z}_8\} \\ &= \{[x]_{12} \in \mathbf{Z}_{12} \mid [x]_{12} = [3n]_{12} \text{ con } 0 \leq n \leq 7\} \\ &= \{[x]_{12} \in \mathbf{Z}_{12} \mid x = 3n \text{ con } 0 \leq n \leq 3\} \\ &= \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}. \end{aligned}$$

Inoltre si ha

$$\begin{aligned} g([n]_8) = [0]_{12} &\Leftrightarrow [3n]_{12} = [0]_{12} \\ &\Leftrightarrow 3n = 12k \text{ con } k \in \mathbf{Z} \\ &\Leftrightarrow n = 4k \text{ con } k \in \mathbf{Z} \end{aligned}$$

per cui

$$g^{-1}([0]_{12}) = \{[0]_8, [4]_8\},$$

d'altra parte  $[1]_{12} \notin \text{Im } g$  e dunque

$$g^{-1}([1]_{12}) = \emptyset.$$

**Esercizio 3**

**Punto a.**

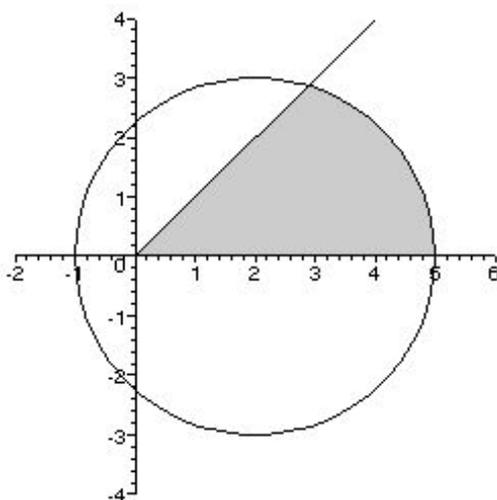
$$\begin{aligned} \frac{(3 - 2i)^2}{1 + i} &= \frac{(9 - 4) - 12i}{1 + i} \\ &= \frac{(5 - 12i)(1 - i)}{2} \\ &= \frac{(5 - 12) + (-5 - 12)i}{2} \\ &= -\frac{7}{2} - \frac{17}{2}i \end{aligned}$$

Pertanto

$$\operatorname{Re}\left(\frac{(3-2i)^2}{1+i}\right) = -\frac{7}{2} \quad \text{e} \quad \operatorname{Im}\left(\frac{(3-2i)^2}{1+i}\right) = -\frac{17}{2}.$$

**Punto b.**

I numeri complessi  $z$  tali che  $|z-2| \leq 3$  sono i complessi  $z = x+iy$  tali che  $(x-2)^2 + y^2 \leq 9$ , quindi sul piano di Gauss corrispondono ai punti interni alla circonferenza di centro il punto  $(2,0)$  e raggio 3. La seconda condizione su  $z$  è che il suo argomento principale  $\theta$  deve verificare la condizione  $0 \leq \theta \leq \frac{\pi}{4}$ , quindi nel piano di Gauss corrispondono ai punti compresi tra il semiasse reale positivo e la bisettrice del I quadrante. In conclusione nel piano di Gauss i numeri complessi cercati formano l'insieme colorato di grigio nel seguente disegno:



**Punto c.**

Per calcolare le radici terze di  $\alpha = -125$  bisogna determinare modulo e argomento principale di tale numero complesso. Per  $\alpha = -125$  si ha  $\rho = 125$  e  $\theta = \pi$ , quindi le radici terze di  $\alpha$  sono i tre numeri complessi (scritti in forma polare)

$$z_k = \left( \sqrt[3]{125}, \frac{\pi + 2k\pi}{3} \right) \quad k = 0, 1, 2$$

ossia

$$z_0 = \left( 5, \frac{\pi}{3} \right) = 5 \left( \cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right) = \frac{5}{2} + \frac{5\sqrt{3}}{2}i$$

$$z_1 = (5, \pi) = -5$$

$$z_2 = \left( 5, \frac{5\pi}{3} \right) = 5 \left( \cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3} \right) = \frac{5}{2} - \frac{5\sqrt{3}}{2}i$$

**Punto d.**

Tenendo conto del punto precedente, la scomposizione in fattori irriducibili del polinomio

$F(X) = (X^3 + 125)(X^2 + X - 12)$  in  $\mathbf{C}[X]$  è la seguente

$$F(X) = (X - (5 + 5\sqrt{3}i)/2)(X - (5 - 5\sqrt{3}i)/2)(X + 5)(X - 3)(X + 4),$$

mentre in  $\mathbf{R}[X]$  è la seguente

$$F(X) = (X^2 - 5X + 25)(X + 5)(X - 3)(X + 4).$$

**Punto e.**

Le eventuali radici razionali del polinomio  $G(X) = 2X^5 + 3X^4 + 11X^3 + 9X^2 + 1$  sono contenute nell'insieme  $\{\pm 1, \pm \frac{1}{2}\}$ .

Per prima cosa si osservi che se  $r$  è un numero razionale positivo allora sicuramente  $G(r) > 0$ , poiché  $G(X)$  ha tutti i coefficienti positivi, per cui 1 e  $\frac{1}{2}$  non possono essere radici di  $G(X)$ .

Per gli altri elementi dell'insieme precedente si procede con la verifica diretta.

Risulta

$$G(-1) = -2 + 3 - 11 + 9 + 1 = 0$$

pertanto il numero razionale  $-1$  è radice di  $G(X)$ .

Si ha inoltre

$$\begin{aligned} G\left(-\frac{1}{2}\right) &= 2 \cdot \left(-\frac{1}{2}\right)^5 + 3 \cdot \left(-\frac{1}{2}\right)^4 + 11 \cdot \left(-\frac{1}{2}\right)^3 + 9 \cdot \left(-\frac{1}{2}\right)^2 + 1 \\ &= -\frac{1}{2^4} + \frac{3}{2^4} - \frac{11}{2^3} + \frac{9}{2^2} + 1 \\ &= \frac{1}{2^3} - \frac{11}{2^3} + \frac{9}{2^2} + 1 \\ &= -\frac{5}{2^2} + \frac{9}{2^2} + 1 \\ &= 2 \neq 0 \end{aligned}$$

per cui  $-1/2$  non è radice di  $G(X)$ .

In conclusione l'unica radice razionale del polinomio  $G(X)$  è il numero  $-1$ .

**Esercizio 4**

L'insieme  $E = \{z \in \mathbf{C} \mid z^n \in \mathbf{Z} \text{ per un qualche intero } n \geq 2\}$  contiene l'insieme dei numeri interi  $\mathbf{Z}$ , infatti una qualsiasi potenza di un numero intero è ancora un numero intero. Ne segue che

$$\text{Card}(E) \geq \text{Card}(\mathbf{Z}) = \aleph_0.$$

D'altra parte tutti gli elementi di  $E$  sono numeri algebrici, poiché

$$E = \{\text{radici dei polinomi } X^n - a \text{ con } n \geq 2 \text{ e } a \in \mathbf{Z}\}$$

pertanto

$$\text{Card}(E) \leq \text{Card}(\mathbf{A}_{\mathbf{C}}) = \aleph_0.$$

In conclusione  $\text{Card}(E) = \aleph_0$ , ossia  $E$  è numerabile.

### Esercizio 5

Sia  $[a]$  un elemento dell'anello  $\mathbf{Z}_{856}$  delle classi di resto modulo 856, che possiamo supporre con rappresentante  $a$  tale che  $0 \leq a \leq 855$ .

Si osservi che 2 divide 856, mentre 5 non divide 856, per cui  $[2]$  è uno zero-divisore in  $\mathbf{Z}_{856}$ , mentre  $[5]$  è un elemento invertibile in  $\mathbf{Z}_{856}$ . Ne deriva che in  $\mathbf{Z}_{856}$  ci sono almeno due elementi che sono degli zero-divisori e almeno due elementi che sono invertibili. Indicata con  $\phi$  la funzione di Eulero, risulta pertanto che:

$$\text{n. zero-divisori in } \mathbf{Z}_{856} = 856 - \phi(856) \geq 2$$

da cui si ricava

$$\phi(856) \leq 854$$

ed inoltre

$$\text{n. elementi invertibili in } \mathbf{Z}_{856} = \phi(856) \geq 2$$

da cui si ottiene

$$856 - \phi(856) \leq 854.$$

Se  $a = 0$  oppure  $a = 1$  allora  $[a]^n = [a]$  per ogni  $n \in \mathbf{N}$  ( $n \neq 0$  se  $a = 0$ ).

Si può pertanto supporre  $a \neq 0$  e  $a \neq 1$ .

Se  $[a]$  è un elemento invertibile si ha  $\text{MCD}(a, 856) = 1$ , ma allora risulta  $\text{MCD}(a^n, 856) = 1$  per ogni  $n \in \mathbf{N}$ , dunque l'insieme  $\{[a]^n \mid n \in \mathbf{N}\}$  contiene solamente elementi invertibili, per cui al massimo può contenere  $\phi(856) < 856$  elementi.

Se invece  $[a]$  è uno zero-divisore si ha  $\text{MCD}(a, 856) > 1$ , ma allora risulta  $\text{MCD}(a^n, 856) > 1$  per ogni  $n \in \mathbf{N} \setminus \{0\}$ , dunque l'insieme  $\{[a]^n \mid n \in \mathbf{N}\}$  contiene solamente zero-divisori oltre a  $[1] = [a]^0$ , per cui al massimo può contenere  $856 - \phi(856) + 1 < 856$  elementi.

In conclusione non esiste un elemento  $[a]$  in  $\mathbf{Z}_{856}$  tale che l'insieme  $\{[a]^n \mid n \in \mathbf{N}\}$  contenga 856 elementi distinti.