

## I Esonero di Matematica Discreta - a.a. 03/04

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

$$X = \{x \in \mathbf{R} \mid 1/2 \leq x < 10\} \quad \text{e} \quad Y = \{x \in \mathbf{R} \mid -2 < x < 3\}.$$

Determinare  $X \cup Y$ ,  $X \cap \mathcal{C}_{\mathbf{R}}(Y)$ ,  $\mathcal{P}(Y \cap \mathbf{N})$ .

- b. Sia  $f: A \rightarrow B$  una applicazione e siano  $C$  e  $D$  due sottoinsiemi di  $A$ . Verificare che risulta  $f(C \cap D) \subseteq f(C) \cap f(D)$ .
- c. (**Extra**) Fornire una condizione su  $f$  necessaria e sufficiente affinché valga l'uguaglianza  $f(C \cap D) = f(C) \cap f(D)$  per ogni coppia di sottoinsiemi di  $A$ , dimostrando quanto asserito.
2. Dato  $a \in \mathbf{N} \setminus \{0\}$  indicheremo con  $a\mathbf{N}$  l'insieme dei numeri naturali multipli di  $a$ . Si consideri l'applicazione  $f: \mathbf{N} \rightarrow \mathbf{N}$  definita da

$$f(n) = \begin{cases} 2n & \text{se } n \text{ è un multiplo dispari di } 3 \\ 3n & \text{se } n \text{ è pari} \\ 0 & \text{se } n \text{ è dispari ma non è multiplo di } 3 \end{cases}$$

- a. Per ciascuno dei seguenti due sottoinsiemi  $\Gamma_1$  e  $\Gamma_2$  di  $\mathbf{N} \times \mathbf{N}$  dire se è il grafico di  $f$ , se è il grafico di una funzione diversa da  $f$ , se non è il grafico di alcuna funzione:

$$\Gamma_1 = \{(n, 3n) \mid n \in 2\mathbf{N}\} \cup \{(n, 2n) \mid n \in 3\mathbf{N}\}$$

$$\Gamma_2 = \{(n, 3n) \mid n \in 2\mathbf{N}\} \cup \{(n, 2n) \mid n \in 3\mathbf{N} \setminus 2\mathbf{N}\}.$$

- b. Dire se la funzione  $f$  sopra definita è iniettiva.
- c. Determinare  $f^{-1}(0)$  e  $f^{-1}(1)$ .
- d. Caratterizzare le applicazioni  $g: \mathbf{N} \rightarrow \mathbf{N}$  tali che  $g \circ f = f$  e provare che per esse si ha anche  $g^k \circ f = f$  per ogni  $k \in \mathbf{N} \setminus \{0\}$ , dove  $g^{k+1} = g \circ g^k$ .
3. In  $\mathbf{Z}$  si consideri la seguente relazione “ $x \sim y$  se  $2x + y$  è multiplo di 3”.
- a. Provare che  $\sim$  è una relazione di equivalenza.
- b. Determinare le classi di equivalenza  $[0]$ ,  $[1]$  e  $[2]$ . Perché possiamo dire che l'insieme quoziente  $\mathbf{Z}/\sim$  ha 3 elementi?
- c. È vero che “[ $x$ ] $\mathcal{R}$ [ $y$ ] se  $x \leq y$  in  $\mathbf{Z}$ ” definisce una relazione d'ordine  $\mathcal{R}$  nel quoziente?
4. Riccardo, un bambino di 10 anni, ha costruito con del cartone i modelli di 5 poligoni regolari: un triangolo, un quadrato, un pentagono, un esagono e un ottagono, inoltre ha a disposizione 8 colori: rosso, verde, giallo, blu, bianco, nero, arancione e viola.
- a. In quanti modi diversi può colorare i poligoni con i colori che ha a disposizione?
- b. In quanti modi può colorare i poligoni con i colori che ha a disposizione se decide che ogni poligono deve essere di un colore diverso?
- c. In quanti modi può scegliere due dei colori a sua disposizione?

## Svolgimento

### Esercizio 1

#### **Punto a.**

Dati i seguenti sottoinsiemi di  $\mathbf{R}$ :

$$X = \{x \in \mathbf{R} \mid 1/2 \leq x < 10\} = [1/2, 10)$$

$$Y = \{x \in \mathbf{R} \mid -2 < x < 3\} = (-2, 3)$$

risulta

$$X \cup Y = \{x \in \mathbf{R} \mid -2 < x < 10\} = (-2, 10)$$

$$X \cap \mathcal{C}_{\mathbf{R}}(Y) = \{x \in \mathbf{R} \mid 3 \leq x < 10\} = [3, 10)$$

$$Y \cap \mathbf{N} = \{0, 1, 2\}$$

e quindi

$$\mathcal{P}(Y \cap \mathbf{N}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, Y \cap \mathbf{N}\}.$$

#### **Punto b.**

Sia  $f: A \rightarrow B$  una applicazione e siano  $C, D \subseteq A$ .

Preso un qualsiasi elemento  $b \in f(C \cap D)$ , allora esiste  $a \in C \cap D$  tale che  $b = f(a)$ , ma

$$\begin{aligned} a \in C \cap D &\Rightarrow a \in C \quad \text{e} \quad a \in D \\ &\Rightarrow b = f(a) \in f(C) \quad \text{e} \quad b = f(a) \in f(D) \\ &\Rightarrow b \in f(C) \cap f(D) \end{aligned}$$

pertanto vale l'inclusione  $f(C \cap D) \subseteq f(C) \cap f(D)$ .

#### **Punto c.**

Sia  $f: A \rightarrow B$  una applicazione. Condizione necessaria e sufficiente affinché valga l'uguaglianza  $f(C \cap D) = f(C) \cap f(D)$  per ogni coppia di sottoinsiemi  $C$  e  $D$  di  $A$  è che  $f$  sia iniettiva.

Infatti, sia  $f$  iniettiva, allora basta verificare che per ogni  $C, D \subseteq A$  vale l'inclusione  $f(C) \cap f(D) \subseteq f(C \cap D)$ , poiché l'inclusione opposta vale sempre (si veda il Punto b.). Preso un qualsiasi elemento  $b \in f(C) \cap f(D)$  allora  $b \in f(C)$  e  $b \in f(D)$ , ma allora esistono  $a_1 \in C$  e  $a_2 \in D$  tali che  $f(a_1) = b = f(a_2)$ , per ipotesi  $f$  è iniettiva per cui  $a_1 = a_2$ , ossia esiste un elemento  $a = a_1 = a_2 \in C \cap D$  tale che  $f(a) = b$ , e pertanto  $b \in f(C \cap D)$ .

Viceversa, supponiamo che valga l'uguaglianza  $f(C \cap D) = f(C) \cap f(D)$  per ogni  $C, D \subseteq A$ . Presi due elementi qualsiasi  $a_1, a_2 \in A$  con  $a_1 \neq a_2$ , si considerino i seguenti sottoinsiemi di  $A$ :

$$A_1 = \{a_1\} \quad \text{e} \quad A_2 = \{a_2\},$$

ovviamente risulta  $A_1 \cap A_2 = \emptyset$  e quindi  $f(A_1 \cap A_2) = \emptyset$ . Per ipotesi si ha

$$f(A_1) \cap f(A_2) = f(A_1 \cap A_2)$$

ossia

$$\{f(a_1)\} \cap \{f(a_2)\} = \emptyset$$

cioè  $f(a_1) \neq f(a_2)$ , e pertanto  $f$  è iniettiva.

### Esercizio 2

#### **Punto a.**

È data la funzione  $f: \mathbf{N} \rightarrow \mathbf{N}$  definita da

$$f(n) = \begin{cases} 2n & \text{se } n \text{ è un multiplo dispari di } 3 \\ 3n & \text{se } n \text{ è pari} \\ 0 & \text{se } n \text{ è dispari ma non è multiplo di } 3 \end{cases}$$

Il grafico di  $f$  è il seguente sottoinsieme  $\Gamma$  di  $\mathbf{N} \times \mathbf{N}$

$$\Gamma = \{(n, 3n) \mid n \in 2\mathbf{N}\} \cup \{(n, 2n) \mid n \in 3\mathbf{N} \setminus 2\mathbf{N}\} \cup \{(n, 0) \mid n \notin 2\mathbf{N} \cup 3\mathbf{N}\}$$

pertanto né  $\Gamma_1$  né  $\Gamma_2$  è il grafico di  $f$ , essendo entrambi diversi da  $\Gamma$ .

$\Gamma_1$  non può essere il grafico di alcuna funzione poiché risulta ad esempio

$$(6, 18) \in \Gamma_1 \quad \text{perché } 6 \text{ è multiplo di } 2$$

$$(6, 12) \in \Gamma_1 \quad \text{perché } 6 \text{ è multiplo di } 3$$

ossia la corrispondenza definita da  $\Gamma_1$  non è funzionale. (In generale per ogni intero  $m$  multiplo sia di 2 che di 3, ossia multiplo di 6, risulta  $(m, 3m) \in \Gamma_1$  e  $(m, 2m) \in \Gamma_1$  con  $3m \neq 2m$ .)

$\Gamma_2$  non è il grafico di una funzione se si prende  $\mathbf{N}$  come dominio, infatti la corrispondenza definita da  $\Gamma_2$  risulta essere funzionale ma non ovunque definita (per ogni naturale  $n$  dispari non multiplo di 3 non esiste coppia in  $\Gamma_2$  con  $n$  come primo elemento). Se invece consideriamo come dominio l'insieme  $2\mathbf{N} \cup 3\mathbf{N}$ , allora  $\Gamma_2$  è il grafico di una funzione.

#### **Punto b.**

La funzione  $f$  sopra definita non è iniettiva, infatti risulta

$$5 \neq 7 \quad \text{ma} \quad f(5) = f(7) = 0.$$

#### **Punto c.**

Risulta:

$$\begin{aligned} f^{-1}(0) &= \{n \in \mathbf{N} \mid n \text{ è dispari ma non è multiplo di } 3 \text{ oppure } n = 0\} \\ &= (\mathbf{N} \setminus (2\mathbf{N} \cup 3\mathbf{N})) \cup \{0\} \\ f^{-1}(1) &= \emptyset \end{aligned}$$

#### **Punto d.**

Le applicazioni  $g: \mathbf{N} \rightarrow \mathbf{N}$  tali che  $g \circ f = f$  devono verificare la condizione

$$g(f(n)) = f(n) \quad \forall n \in \mathbf{N},$$

ossia

$$g(m) = m \quad \forall m \in \text{Im } f.$$

Ora risulta  $\text{Im } f = 6\mathbf{N}$ , quindi le funzioni cercate sono caratterizzate dal fatto che  $g(m) = m$  per ogni  $m \in 6\mathbf{N}$ . Si noti che esistono infinite applicazioni  $g: \mathbf{N} \rightarrow \mathbf{N}$  che soddisfano la precedente condizione, tra cui la funzione identica di  $\mathbf{N}$ .

Per tali funzioni risulta  $g^k \circ f = f$  per ogni  $k \in \mathbf{N} \setminus \{0\}$ , infatti, si ha

$$g \circ f = f \quad (\text{base dell'induzione})$$

per definizione delle funzioni  $g$ , ed inoltre, fissato  $k \geq 1$ , supponiamo per ipotesi induttiva che risulti  $g^k \circ f = f$ , allora (usando la proprietà associativa di  $\circ$ , l'ipotesi induttiva e la base dell'induzione)

$$g^{k+1} \circ f = (g \circ g^k) \circ f = g \circ (g^k \circ f) = g \circ f = f$$

e quindi per induzione risulta verificato che  $g^k \circ f = f$  per ogni  $k \in \mathbf{N} \setminus \{0\}$ .

### **Esercizio 3**

In  $\mathbf{Z}$  si consideri la seguente relazione “ $x \sim y$  se e solo se  $\exists k \in \mathbf{Z}$  tale che  $2x + y = 3k$ ”.

#### **Punto a.**

- Proprietà riflessiva:  $\forall x \in \mathbf{Z}$  risulta  $2x + x = 3x$  con  $x \in \mathbf{Z}$ , per cui  $x \sim x$  per ogni  $x \in \mathbf{Z}$ .
- Proprietà simmetrica:  $\forall x, y \in \mathbf{Z}$  tali che  $x \sim y$ , allora per definizione di  $\sim$  si ha  $2x + y = 3k$  per un opportuno  $k \in \mathbf{Z}$ . Dall'ultima uguaglianza si ricava  $y = 3k - 2x$ , da cui  $2y = 6k - 4x$ , quindi sommando  $x$  ad ambo i membri si ottiene

$$2y + x = 6k - 4x + x = 6k - 3x = 3(2k - x) \quad \text{con} \quad 2k - x \in \mathbf{Z}.$$

Pertanto da  $x \sim y$  segue  $y \sim x$ .

- Proprietà transitiva:  $\forall x, y, z \in \mathbf{Z}$  tali che  $x \sim y$  e  $y \sim z$ , allora esistono  $k, h \in \mathbf{Z}$  tali che  $2x + y = 3k$  e  $2y + z = 3h$ . Dalla prima uguaglianza si ricava  $y = 3k - 2x$ , da cui  $2y = 6k - 4x$ , mentre dalla seconda uguaglianza, utilizzando quanto ricavato, si ha  $z = 3h - 2y = 3h - 6k + 4x$ , e dunque

$$2x + z = 2x + 3h - 6k + 4x = 3(h - 2k + 2x) \quad \text{con} \quad h - 2k + 2x \in \mathbf{Z}.$$

Pertanto da  $x \sim y$  e  $y \sim z$  segue  $x \sim z$ .

In conclusione la relazione  $\sim$  è una relazione di equivalenza.

#### **Punto b.**

Risulta:

$$\begin{aligned} m \in [0] &\Leftrightarrow 0 \sim m \\ &\Leftrightarrow \exists k \in \mathbf{Z} \text{ t.c. } m = 3k \\ m \in [1] &\Leftrightarrow 1 \sim m \\ &\Leftrightarrow \exists h \in \mathbf{Z} \text{ t.c. } 2 + m = 3h \\ &\Leftrightarrow \exists h \in \mathbf{Z} \text{ t.c. } m = 3h - 2 = 3(h - 1) + 1 \\ &\Leftrightarrow \exists k \in \mathbf{Z} \text{ t.c. } m = 3k + 1 \\ m \in [2] &\Leftrightarrow 2 \sim m \\ &\Leftrightarrow \exists h \in \mathbf{Z} \text{ t.c. } 4 + m = 3h \\ &\Leftrightarrow \exists h \in \mathbf{Z} \text{ t.c. } m = 3h - 4 = 3(h - 2) + 2 \\ &\Leftrightarrow \exists k \in \mathbf{Z} \text{ t.c. } m = 3k + 2 \end{aligned}$$

pertanto

$$\begin{aligned} [0] &= \{m \in \mathbf{Z} \mid m = 3k \text{ con } k \in \mathbf{Z}\} \\ [1] &= \{m \in \mathbf{Z} \mid m = 3k + 1 \text{ con } k \in \mathbf{Z}\} \\ [2] &= \{m \in \mathbf{Z} \mid m = 3k + 2 \text{ con } k \in \mathbf{Z}\} \end{aligned}$$

Poiché le classi di equivalenza formano una partizione dell'insieme in cui è definita la relazione di equivalenza ed evidentemente si ha

$$[0] \cup [1] \cup [2] = \mathbf{Z}$$

si può dire che l'insieme quoziente  $\mathbf{Z}/\sim$  contiene esattamente 3 elementi.

**Punto c.**

La condizione “[ $x$ ] $\mathcal{R}$ [ $y$ ] se  $x \leq y$  in  $\mathbf{Z}$ ” non definisce una relazione d'ordine nel quoziente  $\mathbf{Z}/\sim$  poiché  $\mathcal{R}$  non è neppure ben definita, infatti

$$[0]\mathcal{R}[1] \quad \text{perché } 0 \leq 1 \text{ in } \mathbf{Z},$$

ma  $[0] = [3]$  in  $\mathbf{Z}/\sim$  per cui si dovrebbe avere

$$[3]\mathcal{R}[1] \quad \text{ma } 3 > 1 \text{ in } \mathbf{Z}.$$

**Esercizio 4**

**Punto a.**

Si tratta di disposizioni con ripetizione di 8 elementi a 5 a 5, per cui in totale i modi diversi in cui si possono colorare i 5 poligoni con gli 8 colori sono

$$D_{8,5}^r = 8^5.$$

**Punto b.**

Si tratta di disposizioni semplici di 8 elementi a 5 a 5, per cui in totale i modi diversi in cui si possono colorare i 5 poligoni con gli 8 colori in modo che ogni poligono sia di un colore diverso sono

$$D_{8,5} = \frac{8!}{(8-5)!} = \frac{8!}{3!} = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4.$$

**Punto c.**

Si tratta di combinazioni semplici di 8 elementi a 2 a 2, per cui in totale i modi in cui possono essere scelti 2 fra gli 8 colori sono

$$C_{8,2} = \binom{8}{2} = \frac{8!}{2!(8-2)!} = \frac{8!}{2!6!} = \frac{8 \cdot 7}{2} = 28.$$

## II Esonero di Matematica Discreta - a.a. 03/04

- Trovare il MCD di 7729 e 8777 ed esplicitare l'identità di Bézout.
  - Calcolare la cifra delle unità di  $74523^{74523}$ .
  - Dire, motivando la risposta, per quali dei seguenti numeri  $x_i$  vale una relazione del tipo  $x_i = 8a_i + 12b_i$  per opportuni coefficienti  $a_i, b_i \in \mathbf{Z}$ :

$$x_1 = 2, \quad x_2 = 3, \quad x_3 = -4, \quad x_4 = 6, \quad x_5 = 20.$$

- Trovare tutte le soluzioni dei seguenti sistemi di congruenze:

$$\begin{cases} 3x \equiv 4 \pmod{16} \\ 4x \equiv 8 \pmod{15} \end{cases} \quad \begin{cases} 3x \equiv 4 \pmod{15} \\ 4x \equiv 8 \pmod{16} \end{cases}$$
$$\begin{cases} 3x \equiv 2 \pmod{14} \\ 4x \equiv 8 \pmod{16} \end{cases} \quad \begin{cases} 3x \equiv 3 \pmod{14} \\ 4x \equiv 8 \pmod{16} \end{cases}$$

- Determinare la scrittura posizionale in base 3 del numero (che in base 10 si scrive) 128.
- Siano  $\mathbf{Z}_5$  e  $\mathbf{Z}_{25}$  gli anelli delle classi di resto modulo 5 e modulo 25.
    - Provare che  $[a]_5$  è un elemento invertibile in  $\mathbf{Z}_5$  se e solo se  $[a]_{25}$  è un elemento invertibile in  $\mathbf{Z}_{25}$ .
    - È vero che il numero di elementi invertibili in  $\mathbf{Z}_5$  è uguale a quello degli elementi invertibili in  $\mathbf{Z}_{25}$ ?
    - Verificare se l'applicazione  $f: \mathbf{Z}_5 \rightarrow \mathbf{Z}_{25}$  data da  $f([n]_5) = [5n^2]_{25}$  è ben definita.

- Sia  $\mathbf{C}$  il campo dei numeri complessi:

- Calcolare parte reale e coefficiente dell'immaginario del numero complesso:

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

- Disegnare nel piano di Gauss i seguenti insiemi:

$$A = \{z \in \mathbf{C} \mid z \cdot \bar{z} \leq 16 \quad \text{e} \quad \operatorname{Re}(z - (1+i)) \geq 1\}$$
$$B = \{z = (\rho, \theta) \in \mathbf{C} \mid 1 \leq \rho \leq 2 \quad \text{e} \quad 0 \leq \theta \leq \pi\}.$$

- Calcolare le radici quarte del numero complesso  $z = 2$ .
- Scomporre il polinomio  $X^4 - 2$  nel prodotto di fattori irriducibili in  $\mathbf{C}[X]$  e in  $\mathbf{R}[X]$ .
- Determinare tutte le radici razionali del polinomio

$$F(X) = 2X^6 + 42X^4 - 55X^3 + 11.$$

- Dire, motivando la risposta, se ogni numero complesso del tipo  $a + ib$ , con  $a, b \in \mathbf{Q}$ , è un numero algebrico.

## Svolgimento

### Esercizio 1

#### **Punto a.**

Per calcolare il MCD di 7729 e 8777 si usa l'algoritmo di Euclide:

- 1)  $8777 = 7729 \cdot 1 + 1048$
- 2)  $7729 = 1048 \cdot 7 + 393$
- 3)  $1048 = 393 \cdot 2 + 262$
- 4)  $393 = 262 \cdot 1 + 131$
- 5)  $262 = 131 \cdot 2 + 0$

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

$$\text{MCD}(7729, 8777) = 131.$$

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

da **4)** si ha  $131 = 393 - 262$ ,

da **3)** si ha  $262 = 1048 - 2 \cdot 393$ , quindi sostituendo nell'uguaglianza precedente

$$131 = 393 - (1048 - 2 \cdot 393) = 3 \cdot 393 - 1048,$$

da **2)** si ha  $393 = 7729 - 7 \cdot 1048$ , quindi sostituendo nell'uguaglianza precedente

$$131 = 3 \cdot (7729 - 7 \cdot 1048) - 1048 = 3 \cdot 7729 - 22 \cdot 1048,$$

da **1)** si ha  $1048 = 8777 - 7729$ , quindi sostituendo nell'uguaglianza precedente

$$131 = 3 \cdot 7729 - 22 \cdot (8777 - 7729) = 25 \cdot 7729 - 22 \cdot 8777,$$

pertanto l'identità di Bézout è

$$131 = 25 \cdot 7729 + (-22) \cdot 8777.$$

#### **Punto b.**

Calcolare la cifra delle unità di  $74523^{74523}$  significa trovare il resto della divisione di tale numero per 10, ossia determinare a quale intero compreso fra 0 e 9 è congruo il numero dato modulo 10. Ora  $74523 \equiv 3 \pmod{10}$ ,  $\text{MCD}(3, 10) = 1$  e  $\phi(10) = \phi(2)\phi(5) = 4$  (dove  $\phi$  è la funzione di Eulero), quindi per il Teorema di Eulero risulta che  $3^4 \equiv 1 \pmod{10}$ . Facendo la divisione di 74523 per 4 =  $\phi(10)$  si ottiene  $74523 = 18630 \cdot 4 + 3$  e pertanto

$$74523^{74523} \equiv 3^{74523} \equiv (3^4)^{18630} \cdot 3^3 \equiv 3^3 \equiv 27 \equiv 7 \pmod{10}$$

In conclusione la cifra delle unità di  $74523^{74523}$  è 7.

#### **Punto c.**

Sussiste una relazione del tipo  $x_i = 8a_i + 12b_i$  se e solo se  $\text{MCD}(8, 12) = 4$  divide  $x_i$ . Pertanto la risposta è:

NO per  $x_1 = 2, x_2 = 3, x_4 = 6,$

SÌ per  $x_3 = -4, x_5 = 20.$

**Punto d.**

- Sistema di congruenze

$$\begin{cases} 3x \equiv 4 \pmod{16} \\ 4x \equiv 8 \pmod{15} \end{cases}$$

Risulta  $\text{MCD}(3, 16) = \text{MCD}(4, 15) = \text{MCD}(16, 15) = 1$ , quindi per il Teorema Cinese dei Resti il sistema ammette sicuramente delle soluzioni.

Si ha  $1 = 11 \cdot 3 - 2 \cdot 16$  e  $1 = 4 \cdot 4 - 15$ , quindi

$$\begin{aligned} [3]^{-1} &= [11] \quad \text{in } \mathbf{Z}_{16} \\ [4]^{-1} &= [4] \quad \text{in } \mathbf{Z}_{15} \end{aligned}$$

per cui il sistema si trasforma nel seguente sistema equivalente

$$\begin{cases} x \equiv 44 \pmod{16} \\ x \equiv 32 \pmod{15} \end{cases}$$

ovvero

$$\begin{cases} x \equiv 12 \pmod{16} \\ x \equiv 2 \pmod{15} \end{cases}$$

Poiché  $\text{mcm}(15, 16) = 15 \cdot 16 = 240$ , esiste un'unica soluzione  $x_0$  del sistema di congruenze tale che  $0 \leq x_0 < 240$ . L'insieme delle soluzioni della prima congruenza è dato da

$$S_1 = \{12 + 16h \mid h \in \mathbf{Z}\} = \{12, 28, 44, 60, 76, \mathbf{92}, 108, \dots\}$$

mentre l'insieme delle soluzioni della seconda congruenza è dato da

$$S_2 = \{2 + 15k \mid k \in \mathbf{Z}\} = \{2, 17, 32, 47, 62, 77, \mathbf{92}, 107, \dots\}$$

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

$$S = \{92 + 240t \mid t \in \mathbf{Z}\}.$$

- Sistema di congruenze

$$\begin{cases} 3x \equiv 4 \pmod{15} \\ 4x \equiv 8 \pmod{16} \end{cases}$$

Poiché  $\text{MCD}(3, 15) = 3$  non divide 4 la prima congruenza è incompatibile, per cui il sistema non ammette soluzioni.

- Sistema di congruenze

$$\begin{cases} 3x \equiv 2 \pmod{14} \\ 4x \equiv 8 \pmod{16} \end{cases}$$

Risulta  $\text{MCD}(3, 14) = 1$  e  $\text{MCD}(4, 16) = 4$  che divide 8, quindi le singole congruenze ammettono soluzioni, ma  $\text{MCD}(14, 16) = 2$  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.

Il sistema dato è equivalente al seguente

$$\begin{cases} 3x \equiv 2 \pmod{14} \\ x \equiv 2 \pmod{4} \end{cases}$$

Si ha  $1 = 5 \cdot 3 - 14$ , quindi

$$[3]^{-1} = [5] \quad \text{in } \mathbf{Z}_{14}$$

per cui il sistema si trasforma nel seguente

$$\begin{cases} x \equiv 10 \pmod{14} \\ x \equiv 2 \pmod{4} \end{cases}$$

ossia (essendo  $2 \equiv 10 \pmod{4}$ )

$$\begin{cases} x \equiv 10 \pmod{14} \\ x \equiv 10 \pmod{4} \end{cases}$$

Poiché  $\text{mcm}(14, 4) = 28$ , l'insieme delle soluzioni in  $\mathbf{Z}$  del sistema di congruenze è

$$S = \{10 + 28t \mid t \in \mathbf{Z}\}.$$

- Sistema di congruenze

$$\begin{cases} 3x \equiv 3 \pmod{14} \\ 4x \equiv 8 \pmod{16} \end{cases}$$

Risulta  $\text{MCD}(3, 14) = 1$  e  $\text{MCD}(4, 16) = 4$  che divide 8, quindi le singole congruenze ammettono soluzioni, ma  $\text{MCD}(14, 16) = 2$  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.

Il sistema dato è equivalente al seguente

$$\begin{cases} 3x \equiv 3 \pmod{14} \\ x \equiv 2 \pmod{4} \end{cases}$$

Si ha  $1 = 5 \cdot 3 - 14$ , quindi

$$[3]^{-1} = [5] \quad \text{in } \mathbf{Z}_{14}$$

per cui il sistema si trasforma nel seguente

$$\begin{cases} x \equiv 15 \pmod{14} \\ x \equiv 2 \pmod{4} \end{cases}$$

ovvero

$$\begin{cases} x \equiv 1 \pmod{14} \\ x \equiv 2 \pmod{4} \end{cases}$$

L'insieme delle soluzioni della prima congruenza è dato da

$$S_1 = \{1 + 14k \mid k \in \mathbf{Z}\} \subseteq \{\text{interi dispari}\}$$

mentre l'insieme delle soluzioni della seconda congruenza è dato da

$$S_2 = \{2 + 4h \mid h \in \mathbf{Z}\} \subseteq \{\text{interi pari}\}$$

e ovviamente risulta  $S_1 \cap S_2 = \emptyset$ , pertanto il sistema di congruenze dato non ammette soluzioni.

**Punto e.**

Per determinare la scrittura posizionale in base 3 del numero (che in base 10 si scrive) 128 bisogna eseguire le seguenti divisioni con resto:

$$128 = 42 \cdot 3 + 2$$

$$42 = 14 \cdot 3 + 0$$

$$14 = 4 \cdot 3 + 2$$

$$4 = 1 \cdot 3 + 1$$

$$1 = 0 \cdot 3 + 1$$

quindi leggendo i resti di tali divisioni si ottiene che

$$(128)_{10} = (11202)_3.$$

**Esercizio 2**

**Punto a.**

Poiché  $25 = 5^2$  risulta che

$$\begin{aligned} [a]_5 \text{ è invertibile in } \mathbf{Z}_5 &\Leftrightarrow \text{MCD}(a, 5) = 1 \\ &\Leftrightarrow \text{MCD}(a, 25) = 1 \\ &\Leftrightarrow [a]_{25} \text{ è invertibile in } \mathbf{Z}_{25}. \end{aligned}$$

**Punto b.**

NO, il numero di elementi invertibili in  $\mathbf{Z}_5$  non è uguale al numero di elementi invertibili in  $\mathbf{Z}_{25}$ , infatti risulta

$$\phi(5) = 5 - 1 = 4$$

mentre

$$\phi(25) = \phi(5^2) = 5(5 - 1) = 20$$

dove  $\phi$  è la funzione di Eulero, e quindi  $\phi(n)$  è uguale al numero di elementi invertibili nell'anello delle classi di resto  $\mathbf{Z}_n$ .

**Punto c.**

Per verificare se l'applicazione  $f: \mathbf{Z}_5 \rightarrow \mathbf{Z}_{25}$  data da  $f([n]_5) = [5n^2]_{25}$  è ben definita bisogna controllare che cambiando rappresentante ad una qualsiasi classe di equivalenza nel dominio  $\mathbf{Z}_5$  non cambia l'immagine in  $\mathbf{Z}_{25}$  che si ottiene mediante  $f$ .

Sia quindi  $[n]_5 = [m]_5$ . Ciò è equivalente a dire che esiste  $k \in \mathbf{Z}$  tale che  $n = m + 5k$ , per cui

$$\begin{aligned} 5n^2 &= 5(m + 5k)^2 \\ &= 5(m^2 + 10mk + 25k^2) \\ &= 5m^2 + 25(2mk + k^2) \quad \text{con } 2mk + k^2 \in \mathbf{Z} \end{aligned}$$

dunque

$$[5n^2]_{25} = [5m^2]_{25}$$

ossia

$$[n]_5 = [m]_5 \quad \Rightarrow \quad f([n]_5) = f([m]_5)$$

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

**Esercizio 3**

**Punto a.**

$$\begin{aligned} \frac{2+i}{1-3i} + \frac{i}{1+2i} &= \frac{(2+i)(1+3i)}{10} + \frac{i(1-2i)}{5} \\ &= \frac{(2-3) + (6+1)i}{10} + \frac{2+i}{5} \\ &= \left(-\frac{1}{10} + \frac{7}{10}i\right) + \left(\frac{2}{5} + \frac{1}{5}i\right) \\ &= \left(-\frac{1}{10} + \frac{2}{5}\right) + \left(\frac{7}{10} + \frac{1}{5}\right)i \\ &= \frac{3}{10} + \frac{9}{10}i \end{aligned}$$

Pertanto

$$\operatorname{Re}\left(\frac{2+i}{1-3i} + \frac{i}{1+2i}\right) = \frac{3}{10}$$

e

$$\operatorname{Im}\left(\frac{2+i}{1-3i} + \frac{i}{1+2i}\right) = \frac{9}{10}.$$

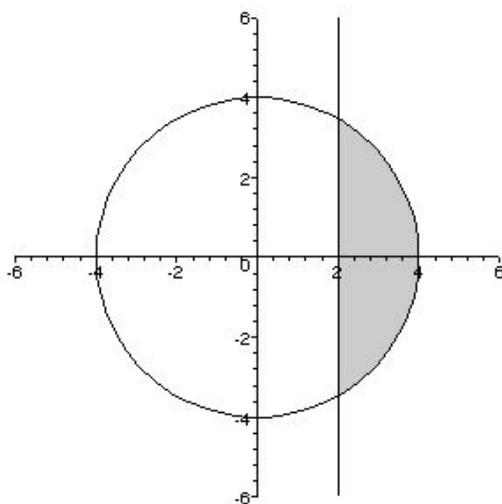
**Punto b.**

Sono dati gli insiemi di numeri complessi

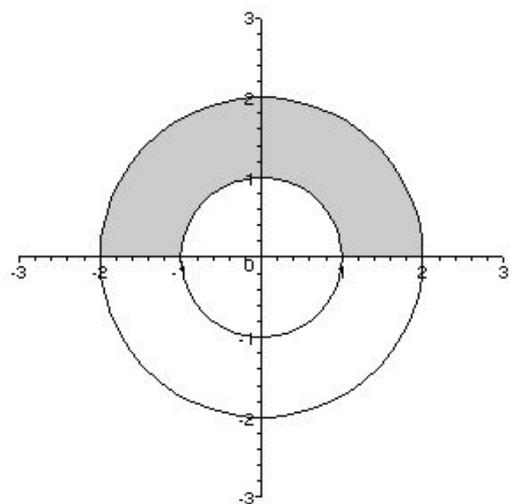
$$A = \{z \in \mathbf{C} \mid z \cdot \bar{z} \leq 16 \text{ e } \operatorname{Re}(z - (1+i)) \geq 1\} = \{x+iy \in \mathbf{C} \mid x^2 + y^2 \leq 16 \text{ e } x \geq 2\}$$

$$B = \{z = (\rho, \theta) \in \mathbf{C} \mid 1 \leq \rho \leq 2 \text{ e } 0 \leq \theta \leq \pi\}$$

per cui nel piano di Gauss si ha (gli insiemi  $A$  e  $B$  sono indicati in grigio):



Insieme  $A$



Insieme  $B$

**Punto c.**

Per calcolare le radici quarte di  $z = 2$  bisogna determinare modulo e argomento principale di tale numero complesso. Per  $z = 2$  si ha  $\rho = 2$  e  $\theta = 0$ , quindi le radici quarte di  $z$  sono i quattro numeri complessi (scritti in forma polare)

$$z_k = \left( \sqrt[4]{2}, \frac{2k\pi}{4} \right) \quad k = 0, 1, 2, 3$$

ossia

$$z_0 = (\sqrt[4]{2}, 0) = \sqrt[4]{2}$$

$$z_1 = \left( \sqrt[4]{2}, \frac{\pi}{2} \right) = \sqrt[4]{2} i$$

$$z_2 = (\sqrt[4]{2}, \pi) = -\sqrt[4]{2}$$

$$z_3 = \left( \sqrt[4]{2}, \frac{3\pi}{2} \right) = -\sqrt[4]{2} i$$

**Punto d.**

Tenendo conto del punto precedente, la scomposizione in fattori irriducibili del polinomio  $X^4 - 2$  in  $\mathbf{C}[X]$  è la seguente

$$X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - \sqrt[4]{2}i)(X + \sqrt[4]{2}i),$$

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

$$X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2}).$$

**Punto e.**

Le eventuali radici razionali del polinomio  $F(X) = 2X^6 + 42X^4 - 55X^3 + 11$  sono contenute nell'insieme  $\{\pm 1, \pm 11, \pm \frac{1}{2}, \pm \frac{11}{2}\}$ .

Per prima cosa si osservi che se  $a$  è un numero razionale negativo allora sicuramente  $F(a) > 0$ , per cui  $-1, -11, -\frac{1}{2}$  e  $-\frac{11}{2}$  non possono essere radici di  $F(X)$ .

Per gli altri numeri razionali contenuti nell'insieme precedente si procede con la verifica diretta.

Risulta

$$F(1) = 2 + 42 - 55 + 11 = 0$$

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

Si ha

$$\begin{aligned} F(11) &= 2 \cdot 11^6 + 42 \cdot 11^4 - 55 \cdot 11^3 + 11 \\ &= 2 \cdot 11^6 + 42 \cdot 11^4 - 5 \cdot 11^4 + 11 \\ &= 2 \cdot 11^6 + 37 \cdot 11^4 + 11 > 0 \end{aligned}$$

per cui 11 non è radice di  $F(X)$ .

Si ha

$$\begin{aligned} F\left(\frac{1}{2}\right) &= 2 \cdot \left(\frac{1}{2}\right)^6 + 42 \cdot \left(\frac{1}{2}\right)^4 - 55 \cdot \left(\frac{1}{2}\right)^3 + 11 \\ &= \frac{1}{2^5} + \frac{21}{2^3} - \frac{5 \cdot 11}{2^3} + \frac{8 \cdot 11}{2^3} \\ &= \frac{1}{2^5} + \frac{21}{2^3} + \frac{33}{2^3} > 0 \end{aligned}$$

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

Si ha

$$\begin{aligned} F\left(\frac{11}{2}\right) &= 2 \cdot \left(\frac{11}{2}\right)^6 + 42 \cdot \left(\frac{11}{2}\right)^4 - 55 \cdot \left(\frac{11}{2}\right)^3 + 11 \\ &= \frac{11^6}{2^5} + 21 \cdot \frac{11^4}{2^3} - 5 \cdot \frac{11^4}{2^3} + 11 \\ &= \frac{11^6}{2^5} + 16 \cdot \frac{11^4}{2^3} + 11 > 0 \end{aligned}$$

per cui  $11/2$  non è radice di  $F(X)$ .

In conclusione l'unica radice razionale del polinomio  $F(X)$  è 1.

**Punto f.**

Dato un qualsiasi numero complesso  $z = a + ib$  con  $a, b \in \mathbf{Q}$ , esso è radice del polinomio

$$G(X) = (X - z)(X - \bar{z}) = X^2 - 2aX + a^2 + b^2$$

che è un polinomio a coefficienti razionali, poiché  $2a \in \mathbf{Q}$  e  $a^2 + b^2 \in \mathbf{Q}$ . Pertanto ogni numero complesso del tipo  $a + ib$ , con  $a$  e  $b$  numeri razionali, è un numero algebrico perché è radice di un polinomio a coefficienti razionali.