

II Esonero di Matematica Discreta - a.a. 06/07

Versione B

1. Nell'anello dei numeri interi $\mathbf{Z}$:

- a. Determinare la scrittura posizionale in base 9 del numero (che in base 10 si scrive) 5293 e la scrittura posizionale in base 10 del numero $(2314)_5$, dove l'indice indica la base utilizzata.
- b. Determinare le ultime due cifre del numero 47913^{6403} .
- c. Calcolare il massimo comun divisore di 5746 e 1651.
- d. (*) Per ogni $k \in \mathbf{N}$ si consideri l'insieme:

$$A_k = \{a \in \mathbf{Z} \mid \text{l'equazione } 1651x + (5746 \cdot 2^k)y = a \text{ ammette soluzioni intere}\}.$$

Dimostrare che gli insiemi A_k sono tutti uguali e determinarne esplicitamente gli elementi.

2. Risolvere i seguenti sistemi di congruenze lineari:

$$\begin{cases} 3x \equiv 3 \pmod{4} \\ 6x \equiv 3 \pmod{15} \end{cases} \quad \begin{cases} 5x \equiv 4 \pmod{12} \\ 11x \equiv 2 \pmod{14} \end{cases}$$

3. Si consideri l'anello $\mathbf{Z}_{270}$ delle classi di resto modulo 270.

- a. Calcolare il numero di elementi invertibili contenuti nell'anello $\mathbf{Z}_{270}$.
- b. Verificare che $[83]$ è un elemento invertibile di $\mathbf{Z}_{270}$ e determinare esplicitamente il suo inverso.
- c. Verificare che l'applicazione $f: \mathbf{Z}_{270} \rightarrow \mathbf{Z}_{150}$ data da $f([n]) = \overline{5n}$ è ben definita (dove $[n]$ indica la classe di resto rappresentata da n in $\mathbf{Z}_{270}$ e $\overline{x}$ indica la classe di resto rappresentata da x in $\mathbf{Z}_{150}$).
- d. (*) Dimostrare che $[a]$ è invertibile in $\mathbf{Z}_{270}$ se e solo se $\overline{a}$ è invertibile in $\mathbf{Z}_{150}$. Se ne può dedurre che gli anelli $\mathbf{Z}_{270}$ e $\mathbf{Z}_{150}$ hanno lo stesso numero di elementi invertibili? Perché?

4. a. Calcolare parte reale e coefficiente dell'immaginario del numero complesso:

$$w = \frac{i^{51}(2 - 3i)}{1 + i}.$$

b. Disegnare nel piano di Gauss l'insieme di numeri complessi

$$E = \{z \in \mathbf{C} \mid 1 \leq \operatorname{Im}(z) \leq 5 \text{ e } 2 \leq |z| \leq 4\}.$$

c. Calcolare le radici terze del numero complesso $z = -8i$.

d. (*) Dimostrare che il numero complesso $\alpha = \frac{3}{2} + \frac{1}{4}i$ è algebrico.

5. Dato il polinomio $F(X) = (X^2 - 3)^2(X^3 - X^2 - 4X - 6)$ trovare:

- i) tutte le radici razionali,
- ii) tutte le radici reali,
- iii) tutte le radici complesse,

specificando per ciascuna la relativa molteplicità ed esplicitando la decomposizione di $F(X)$ in fattori irriducibili rispettivamente in $\mathbf{Q}[X]$, in $\mathbf{R}[X]$ e in $\mathbf{C}[X]$.

Svolgimento

Esercizio 1

Punto a.

Per determinare la scrittura posizionale in base 9 del numero (che in base 10 si scrive) 5293 bisogna eseguire le seguenti divisioni con resto:

$$5293 = 588 \cdot 9 + 1$$

$$588 = 65 \cdot 9 + 3$$

$$65 = 7 \cdot 9 + 2$$

$$7 = 0 \cdot 9 + 7$$

quindi leggendo i resti di tali divisioni si ottiene che

$$(5293)_{10} = (7231)_9.$$

Per determinare la scrittura posizionale in base 10 del numero che in base 5 si scrive 2314 si usa la definizione, ossia:

$$\begin{aligned} (2314)_5 &= 2 \cdot 5^3 + 3 \cdot 5^2 + 1 \cdot 5 + 4 \\ &= 2 \cdot 125 + 3 \cdot 25 + 5 + 4 \\ &= 250 + 75 + 5 + 4 \\ &= (334)_{10}. \end{aligned}$$

Punto b.

Calcolare le ultime due cifre di 47913^{6403} significa trovare il resto della divisione di tale numero per 100, ossia determinare a quale intero, compreso fra 0 e 99, è congruo modulo 100 il numero dato. Poiché $47913 \equiv 13 \pmod{100}$, $\text{MCD}(13, 100) = 1$ ed inoltre

$$\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\phi(5^2) = 2(2-1) \cdot 5(5-1) = 40$$

(dove ϕ è la funzione di Eulero), per il Teorema di Eulero risulta che $13^{40} \equiv 1 \pmod{100}$. Facendo la divisione di 6403 per 40 = $\phi(100)$ si ottiene $6403 = 160 \cdot 40 + 3$ e pertanto

$$47913^{6403} \equiv 13^{6403} \equiv (13^{40})^{160} \cdot 13^3 \equiv 1^{160} \cdot 13^3 \equiv 13^3 \equiv 2197 \equiv 97 \pmod{100}$$

Pertanto le ultime due cifre del numero 47913^{6403} sono 97.

Punto c.

Per calcolare il massimo comun divisore di 5746 e 1651 si usa l'algoritmo euclideo:

$$5746 = 1651 \cdot 3 + 793$$

$$1651 = 793 \cdot 2 + 65$$

$$793 = 65 \cdot 12 + 13$$

$$65 = 13 \cdot 5 + 0$$

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

$$\text{MCD}(5746, 1651) = 13.$$

Punto d.

Poiché 2 non divide 1651, ne segue che per ogni $k \in \mathbf{N}$

$$\text{MCD}(1651, 5746 \cdot 2^k) = \text{MCD}(1651, 5746) = 13$$

(si veda quanto calcolato al punto precedente).

Inoltre, fissato $a \in \mathbf{Z}$, l'equazione $1651x + (5746 \cdot 2^k)y = a$ ammette soluzioni intere se e solo se $\text{MCD}(1651, 5746 \cdot 2^k)$ divide a , ossia se e solo se 13 divide a .

Dunque per ogni $k \in \mathbf{N}$ l'insieme A_k contiene tutti e soli i multipli di 13, quindi gli insiemi A_k sono tutti uguali e coincidono con l'insieme $13\mathbf{Z} = \{13k \mid k \in \mathbf{Z}\}$.

Esercizio 2

- Sistema di congruenze

$$\begin{cases} 3x \equiv 3 & \text{mod } 4 \\ 6x \equiv 3 & \text{mod } 15 \end{cases}$$

Risulta $\text{MCD}(3, 4) = 1$ e $\text{MCD}(6, 15) = 3$ che divide il termine noto 3, quindi le singole congruenze ammettono soluzioni, e il sistema dato risulta equivalente al sistema seguente

$$\begin{cases} 3x \equiv 3 & \text{mod } 4 \\ 2x \equiv 1 & \text{mod } 5 \end{cases}$$

Poiché $\text{MCD}(4, 5) = 1$, per il Teorema Cinese dei Resti si può dire a priori che il sistema ammette soluzioni, ed esiste una ed una sola soluzione x_0 tale che $0 \leq x_0 < 20 = \text{mcm}(4, 5)$. Si ha $1 = 3 \cdot 3 - 2 \cdot 4$ e $1 = 3 \cdot 2 - 5$, quindi

$$\begin{aligned} [3]^{-1} &= [3] & \text{in } \mathbf{Z}_4 \\ [2]^{-1} &= [3] & \text{in } \mathbf{Z}_5 \end{aligned}$$

per cui il sistema si trasforma nel seguente sistema equivalente

$$\begin{cases} x \equiv 1 & \text{mod } 4 \\ x \equiv 3 & \text{mod } 5 \end{cases}$$

L'insieme delle soluzioni della prima congruenza è dato da

$$S_1 = \{1 + 4h \mid h \in \mathbf{Z}\} = \{1, 5, 9, \mathbf{13}, 17, \dots\}$$

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

$$S_2 = \{3 + 5k \mid k \in \mathbf{Z}\} = \{3, 8, \mathbf{13}, 18, \dots\}$$

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

$$S = \{13 + 20t \mid t \in \mathbf{Z}\}.$$

- Sistema di congruenze

$$\begin{cases} 5x \equiv 4 & \text{mod } 12 \\ 11x \equiv 2 & \text{mod } 14 \end{cases}$$

Risulta $\text{MCD}(5, 12) = \text{MCD}(11, 14) = 1$, quindi le singole congruenze ammettono soluzioni, ma $\text{MCD}(12, 14) = 2 > 1$ 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.

Si ha $1 = 5 \cdot 5 - 2 \cdot 12$ e $1 = 4 \cdot 14 - 5 \cdot 11$, quindi

$$\begin{aligned} [5]^{-1} &= [5] && \text{in } \mathbf{Z}_{12} \\ [11]^{-1} &= [-5] = [9] && \text{in } \mathbf{Z}_{14} \end{aligned}$$

per cui il sistema si trasforma nel seguente sistema equivalente

$$\begin{cases} x \equiv 20 & \text{mod } 12 \\ x \equiv 18 & \text{mod } 14 \end{cases}$$

ovvero

$$\begin{cases} x \equiv 8 & \text{mod } 12 \\ x \equiv 4 & \text{mod } 14 \end{cases}$$

Poiché $\text{mcm}(12, 14) = 84$, bisogna cercare se esiste una soluzione x_0 comune alle due congruenze tale che $0 \leq x_0 < 84$. L'insieme delle soluzioni della prima congruenza è dato da

$$S_1 = \{8 + 12h \mid h \in \mathbf{Z}\} = \{8, 20, \mathbf{32}, \dots\}$$

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

$$S_2 = \{4 + 14k \mid k \in \mathbf{Z}\} = \{4, 18, \mathbf{32}, \dots\}$$

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

$$S = \{32 + 84t \mid t \in \mathbf{Z}\}.$$

Esercizio 3

Punto a.

Il numero di elementi invertibili nell'anello $\mathbf{Z}_{270}$ delle classi di resto modulo 270 è dato da $\phi(270)$, dove ϕ è la funzione di Eulero. Ora $270 = 2 \cdot 3^3 \cdot 5$, quindi, essendo ϕ una funzione moltiplicativa, risulta

$$\phi(270) = \phi(2)\phi(3^3)\phi(5) = (2-1) \cdot 3^2(3-1) \cdot (5-1) = 1 \cdot 18 \cdot 4 = 72.$$

Pertanto l'anello $\mathbf{Z}_{270}$ contiene esattamente 72 elementi invertibili.

Punto b.

L'elemento $[83]$ è invertibile in $\mathbf{Z}_{270}$ poiché $\text{MCD}(83, 270) = 1$. Infatti usando l'algoritmo euclideo

- 1) $270 = 83 \cdot 3 + 21$
- 2) $83 = 21 \cdot 3 + 20$
- 3) $21 = 20 + 1$

pertanto il massimo comun divisore di 83 e 270 è 1, e quindi $[83]$ è un elemento invertibile nell'anello $\mathbf{Z}_{270}$ e per determinare il suo inverso è sufficiente esplicitare l'identità di Bézout. Dunque utilizzando le divisioni successive precedenti, ma andando a ritroso, si ottiene:

da **3)** si ha $1 = 21 - 20$,

da **2)** si ha $20 = 83 - 3 \cdot 21$, quindi sostituendo nell'uguaglianza precedente

$$1 = 21 - (83 - 3 \cdot 21) = 4 \cdot 21 - 83,$$

da **1)** si ha $21 = 270 - 3 \cdot 83$, quindi sostituendo nell'uguaglianza precedente

$$1 = 4 \cdot (270 - 3 \cdot 83) - 83 = 4 \cdot 270 - 13 \cdot 83,$$

pertanto l'identità di Bézout è

$$1 = 4 \cdot 270 + (-13) \cdot 83.$$

Se ne deduce che l'inverso di $[83]$ in $\mathbf{Z}_{270}$ è:

$$[83]^{-1} = [-13] = [257].$$

Punto c.

Per verificare che l'applicazione $f: \mathbf{Z}_{270} \rightarrow \mathbf{Z}_{150}$ data da $f([n]) = \overline{5n}$ è ben definita bisogna controllare che cambiando rappresentante ad una qualsiasi classe nel dominio $\mathbf{Z}_{270}$ non cambia l'immagine in $\mathbf{Z}_{150}$ che si ottiene mediante f .

Sia quindi $[n] = [m]$ in $\mathbf{Z}_{270}$. Ciò è equivalente a dire che esiste $k \in \mathbf{Z}$ tale che $n = m + 270k$, per cui

$$5n = 5(m + 270k) = 5m + 5 \cdot 270k = 5m + 150 \cdot 9k \quad \text{con } 9k \in \mathbf{Z},$$

dunque

$$\overline{5n} = \overline{5m} \quad \text{in } \mathbf{Z}_{150}$$

ossia

$$f([n]) = f([m])$$

e pertanto l'applicazione f è ben definita.

Punto d.

Le fattorizzazioni in primi di 270 e di 150 sono

$$270 = 2 \cdot 3^3 \cdot 5 \quad \text{e} \quad 150 = 2 \cdot 3 \cdot 5^2$$

quindi 270 e 150 hanno gli stessi fattori primi, per la precisione 2, 3 e 5. Ne segue che un numero intero a è coprimo con 270 se e solo se è coprimo con 150. Pertanto

$$[a] \text{ è invertibile in } \mathbf{Z}_{270}$$

$$\Updownarrow$$

$$\text{MCD}(a, 270) = 1$$

$$\Updownarrow$$

$$\text{MCD}(a, 150) = 1$$

$$\Updownarrow$$

$$\overline{a} \text{ è invertibile in } \mathbf{Z}_{150}$$

Da ciò non si può dedurre che gli anelli $\mathbf{Z}_{270}$ e $\mathbf{Z}_{150}$ contengono lo stesso numero di elementi invertibili. In effetti $\mathbf{Z}_{270}$ contiene sicuramente un numero maggiore di elementi invertibili rispetto a $\mathbf{Z}_{150}$. Se si considerano ad esempio i numeri interi 1 e 151, essi individuano degli elementi invertibili sia in $\mathbf{Z}_{270}$ che in $\mathbf{Z}_{150}$, ma risulta $[1] \neq [151]$ in $\mathbf{Z}_{270}$, mentre $\overline{1} = \overline{151}$ in $\mathbf{Z}_{150}$. D'altra parte il numero di elementi invertibili in un anello di classi di resto è dato dal valore assunto dalla funzione ϕ di Eulero e risulta $\phi(270) > \phi(150)$, infatti, per il punto a. $\phi(270) = 72$, mentre $\phi(150) = \phi(2)\phi(3)\phi(5^2) = 1 \cdot 2 \cdot 20 = 40$.

Esercizio 4

Punto a.

Usando il fatto che $51 = 12 \cdot 4 + 3$ e che $i^4 = 1$, per cui $i^{51} = (i^4)^{12} \cdot i^3 = i^3 = -i$, risulta

$$\begin{aligned} w &= \frac{i^{51}(2-3i)}{1+i} = i^3 \cdot \frac{(2-3i)(1-i)}{2} \\ &= (-i) \cdot \frac{(2-3) + i(-2-3)}{2} \\ &= (-i) \cdot \left(-\frac{1}{2} - \frac{5}{2}i\right) \\ &= -\frac{5}{2} + \frac{1}{2}i \end{aligned}$$

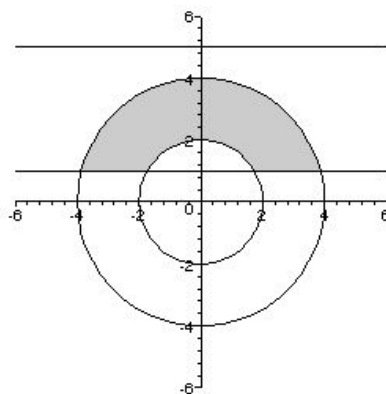
Pertanto

$$\operatorname{Re}(w) = -\frac{5}{2} \quad \text{e} \quad \operatorname{Im}(w) = \frac{1}{2}.$$

Punto b.

I numeri complessi z tali che $1 \leq \operatorname{Im}(z) \leq 5$, dove $\operatorname{Im}(z)$ indica il coefficiente dell'immaginario di z , sono rappresentati nel piano di Gauss dai punti con ordinata y compresa tra 1 e 5, ossia dai punti della striscia di piano delimitata dalle rette $y = 1$ e $y = 5$.

D'altra parte, i numeri complessi z il cui modulo $|z|$ verifica le condizioni $2 \leq |z| \leq 4$ sono rappresentati nel piano di Gauss dai punti della corona circolare delimitata dalla circonferenza di centro l'origine e raggio 2 e dalla circonferenza di centro l'origine e raggio 4. Pertanto nel piano di Gauss i numeri complessi considerati sono rappresentati dalla zona di piano indicata in grigio nel seguente disegno:



Insieme E

Punto c.

Per calcolare le radici terze di $z = -8i$ bisogna determinare modulo e argomento principale di tale numero complesso. Per $z = -8i$ si ha $\rho = 8$ e $\theta = \frac{3\pi}{2}$, quindi le radici terze di $z = -8i$ sono i tre numeri complessi (scritti in forma polare)

$$z_k = \left(\sqrt[3]{8}, \frac{\frac{3\pi}{2} + 2k\pi}{3} \right) \quad k = 0, 1, 2$$

ossia

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

$$z_1 = \left(2, \frac{7\pi}{6} \right) = 2 \left(\cos \frac{7\pi}{6} + i \sin \frac{7\pi}{6} \right) = 2 \left(-\frac{\sqrt{3}}{2} - \frac{1}{2}i \right) = -\sqrt{3} - i$$

$$z_2 = \left(2, \frac{11\pi}{6} \right) = 2 \left(\cos \frac{11\pi}{6} + i \sin \frac{11\pi}{6} \right) = 2 \left(\frac{\sqrt{3}}{2} - \frac{1}{2}i \right) = \sqrt{3} - i$$

Punto d.

Per dimostrare che il numero complesso $\alpha = \frac{3}{2} + \frac{1}{4}i$ è algebrico bisogna mostrare che esiste almeno un polinomio a coefficienti razionali che ammette α come radice. Si consideri il coniugato di α , ossia $\bar{\alpha} = \frac{3}{2} - \frac{1}{4}i$. Risulta

$$\alpha + \bar{\alpha} = 2 \cdot \operatorname{Re}(\alpha) = 3 \quad \text{e} \quad \alpha \cdot \bar{\alpha} = |\alpha|^2 = \left(\frac{3}{2} \right)^2 + \left(\frac{1}{4} \right)^2 = \frac{9}{4} + \frac{1}{16} = \frac{37}{16}.$$

Si consideri quindi il polinomio

$$F(X) = (X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \alpha \cdot \bar{\alpha} = X^2 - 3X + \frac{37}{16}$$

Si tratta di un polinomio a coefficienti razionali che, per costruzione, possiede α tra le sue radici. Pertanto il numero complesso α è algebrico.

Esercizio 5

È dato il polinomio $F(X) = (X^2 - 3)^2(X^3 - X^2 - 4X - 6)$.

Il fattore $X^2 - 3$ ha quali radici i numeri irrazionali $\sqrt{3}$ e $-\sqrt{3}$.

Posto $G(X) = X^3 - X^2 - 4X - 6$, le eventuali radici razionali di $G(X)$, essendo un polinomio a coefficienti interi, sono contenute nell'insieme $\{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Si procede con la verifica diretta:

$$G(1) = 1 - 1 - 4 - 6 = -10 \neq 0$$

$$G(-1) = -1 - 1 + 4 - 6 = -4 \neq 0$$

$$G(2) = 8 - 4 - 8 - 6 = -10 \neq 0$$

$$G(-2) = -8 - 4 + 8 - 6 = -10 \neq 0$$

$$G(3) = 27 - 9 - 12 - 6 = 0$$

$$G(-3) = -27 - 9 + 12 - 6 = -30 \neq 0$$

$$G(6) = 216 - 36 - 24 - 6 = 150 \neq 0$$

$$G(-6) = -216 - 36 + 24 - 6 = -234 \neq 0$$

pertanto l'unica radice razionale di $G(X)$, e dunque anche di $F(X)$, è 3.

Dividendo $G(X)$ per $X - 3$ si ottiene $G(X) = (X - 3)(X^2 + 2X + 2)$.

Le radici del polinomio di secondo grado $X^2 + 2X + 2$ sono i due numeri complessi coniugati $z_1 = -1 + i$ e $z_2 = -1 - i$.

Pertanto il polinomio $F(X)$ ha le seguenti radici:

- i) radici razionali: 3 semplice;
- ii) radici reali: 3 semplice, $\sqrt{3}$ doppia, $-\sqrt{3}$ doppia;
- iii) radici complesse: 3 semplice, $\sqrt{3}$ doppia, $-\sqrt{3}$ doppia, z_1 semplice, z_2 semplice;

(dove radice semplice significa di molteplicità 1 e radice doppia significa di molteplicità 2) e quindi $F(X)$ ha le seguenti decomposizioni in fattori irriducibili:

$$F(X) = (X - 3)(X^2 - 3)^2(X^2 + 2X + 2) \quad \text{in } \mathbf{Q}[X]$$

$$F(X) = (X - 3)(X - \sqrt{3})^2(X + \sqrt{3})^2(X^2 + 2X + 2) \quad \text{in } \mathbf{R}[X]$$

$$F(X) = (X - 3)(X - \sqrt{3})^2(X + \sqrt{3})^2(X - z_1)(X - z_2) \quad \text{in } \mathbf{C}[X]$$