

ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 23/02/2026 ore 10.00 - aula 1

1) Risolvere il sistema di equazioni

$$\begin{cases} 12x \equiv 6 \pmod{18} \\ 15x \equiv 12 \pmod{72}. \end{cases}$$

2) Determinare il sottogruppo di $(\mathbb{Z}/11\mathbb{Z})^*$ generato da 5 e trovare tutte le soluzioni intere dell'equazione

$$5^x \equiv 4 \pmod{11}.$$

3) Fattorizzare in irriducibili il polinomio $p(x) = x^4 + 6x^3 - 7 \in \mathbb{Q}[x]$ e dimostrare che esiste un anello A tale che

$$\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q} \times A.$$

A è un campo? A è un dominio di integrità?

4) Fattorizzare in irriducibili di $\mathbb{Z}[i]$ il numero 323 e classificare il gruppo moltiplicativo $(\mathbb{Z}[i]/(323))^*$ per potenze di primi o per divisori elementari (a scelta).

ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 23/02/2026 ore 10.00 - aula 1

SOLUZIONI

1) Poiché $(18, 12) = 6 \mid 6$ l'equazione $12x \equiv 6 \pmod{18}$ è risolubile ed è equivalente all'equazione $2x \equiv 1 \pmod{3}$.

Analogamente poiché $(72, 15) = 3 \mid 12$ l'equazione $15x \equiv 12 \pmod{72}$ è risolubile ed è equivalente all'equazione $5x \equiv 4 \pmod{24}$.

Dunque il sistema dato è equivalente al sistema

$$\begin{cases} 2x \equiv 1 \pmod{3} \\ 5x \equiv 4 \pmod{24}. \end{cases}$$

Poiché $3 \mid 24$ questo sistema è risolubile se e solo se le due equazioni sono compatibili modulo 3: ora l'equazione $5x \equiv 4 \pmod{3}$ è uguale all'equazione $2x \equiv 1 \pmod{3}$ perché $5 \equiv 2 \pmod{3}$ e $4 \equiv 1 \pmod{3}$.

Quindi il sistema dato è equivalente all'equazione $5x \equiv 4 \pmod{24}$.

Notiamo che $5^2 \equiv 1 \pmod{24}$; quindi l'equazione $5x \equiv 4 \pmod{24}$, che equivale all'equazione $5^2 x \equiv 5 \cdot 4 \pmod{24}$, è equivalente all'equazione

$$x \equiv 20 \pmod{24},$$

che è dunque la soluzione del sistema dato.

2) Sia G il sottogruppo di $(\mathbb{Z}/11\mathbb{Z})^*$ generato da 5. Allora

$$G = \{1, 5, 5^2 \equiv 3, 5^3 \equiv 5 \cdot 3 \equiv 4, 5^4 \equiv 3^2 \equiv 9\} = \{1, 5, 3, 4, 9\}$$

perché $5^5 \equiv 5 \cdot 9 \equiv 1 \pmod{11}$.

Ne segue che $5^3 \equiv 4 \pmod{11}$ e che 5 ha ordine 5 in $(\mathbb{Z}/11\mathbb{Z})^*$, cioè le soluzioni dell'equazione data sono i numeri interi $x \equiv 3 \pmod{5}$, cioè i numeri della forma $x = 3 + 5k$ al variare di $k \in \mathbb{Z}$.

3) Le radici razionali del polinomio $p(x)$ devono essere divisori del coefficiente di grado zero (che è 7), cioè sono contenute nell'insieme $\{\pm 1, \pm 7\}$. È immediato verificare che $p(1) = 0$, dunque $(x-1) \mid p(x) = (x-1)q(x)$ con $q(x) \in \mathbb{Q}[x]$; dividendo $p(x)$ per $x-1$ si trova che

$$q(x) = x^3 + 7x^2 + 7x + 7.$$

Per il criterio di Eisenstein $q(x)$ è irriducibile: in particolare $(x-1, q(x)) = 1$.

Dunque per il teorema cinese

$$\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}[x]/(x-1) \times \mathbb{Q}[x]/(q(x)) \cong \mathbb{Q} \times \mathbb{Q}[x]/(q(x)).$$

Ne segue che l'anello A cercato è $A = \mathbb{Q}[x]/(q(x))$.

Poiché $q(x)$ è irriducibile, A è un campo ed è un dominio di integrità.

4) $323 = 17 \cdot 19$ è la fattorizzazione di 323 in irriducibili di $\mathbb{Z}$.

19 è irriducibile anche in $\mathbb{Z}[i]$ perché $19 \equiv 3 \pmod{4}$.

Invece $17 \equiv 1 \pmod{4}$, quindi si fattorizza nel prodotto di due irriducibili in $\mathbb{Z}[i]$, della forma $a \pm bi$ con $a, b \in \mathbb{N}$ tali che $a^2 + b^2 = 17$.

Poiché $17 = 1 + 16$, si ha che $17 = (1 + 4i)(1 - 4i)$ è la fattorizzazione di 17 in irriducibili di $\mathbb{Z}[i]$.

Dunque $323 = 19(1 + 4i)(1 - 4i)$ è la fattorizzazione di 323 in irriducibili di $\mathbb{Z}[i]$.

Poiché 19, $1 + 4i$ e $1 - 4i$ sono irriducibili a due a due primi tra loro, il teorema cinese implica che

$$\mathbb{Z}[i]/(323) \cong \mathbb{Z}[i]/(19) \times \mathbb{Z}[i]/(1 + 4i) \times \mathbb{Z}[i]/(1 - 4i)$$

e ognuno dei tre fattori è un campo.

In particolare $\mathbb{Z}[i]/(19)$ è un campo con $19^2 = 361$ elementi mentre i campi $\mathbb{Z}[i]/(1 \pm 4i)$ sono isomorfi a $\mathbb{Z}/(17)$.

Il gruppo moltiplicativo di un prodotto di anelli è il prodotto dei gruppi moltiplicativi; il gruppo moltiplicativo di un campo finito è ciclico. Quindi

$$\begin{aligned} (\mathbb{Z}[i]/(323))^* &\cong (\mathbb{Z}[i]/(19))^* \times (\mathbb{Z}[i]/(1 + 4i))^* \times (\mathbb{Z}[i]/(1 - 4i))^* \cong \\ &\cong \mathbb{Z}/360\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}. \end{aligned}$$

Ora $360 = 2^3 \cdot 3^2 \cdot 5$, quindi

$$(\mathbb{Z}[i]/(323))^* \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$$

è la classificazione di questo gruppo per potenze di primi, mentre

$$(\mathbb{Z}[i]/(323))^* \cong \mathbb{Z}/720\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$$

è la sua classificazione per divisori elementari ($8|16|720 = 5 \cdot 9 \cdot 16$).