

Esame di Simulazione – Algebra Informatica

Questo esame non sarà valutato per un voto. Verrà fornito un feedback sugli esami simulati restituiti entro il 1° Maggio 2023. La struttura degli esami è soggetta a modifiche. Il punteggio dell'esame è 8 più il numero dei punti ottenuti, fino a un massimo di 26. Come discusso a lezione, per ottenere un voto superiore a 26, uno studente deve sostenere la prova orale.

✗ **Problema 1:** Dimostrare che esistono infiniti numeri primi. [3 punti]

✗ **Problema 2:** [Un punto ciascuno]

✗(a) Trova due interi u e v tale che $\text{mcd}(237, 13) = 237u + 13v$.

✗(b) Trova due polinomi u e $v \in \mathbb{Q}[x]$ tali che

$$\text{mcd}(x^4 + x^3 + x^2 + x + 1, x^2 + x + 1) = u(x^4 + x^3 + x^2 + x + 1) + v(x^2 + x + 1)$$

✗ **Problema 3:** [Un punto ciascuno]

✗(a) Elenca tutti i possibili gruppi abeliani di ordine 100 (modulo isomorfismi).

✗(b) Calcola $\phi(100)$ dove ϕ è la funzione toziente di Eulero.

✗(c) Calcola $3^{42} \pmod{100}$.

✗ **Problema 4:** Sia $L = \{(x, y, z) \in \mathbb{Z}^3 \mid x + 2y + 3z \equiv 0 \pmod{6}\}$. Trova un insieme di vettori $\{u_1, u_2, u_3\}$ in \mathbb{Z}^3 tale che $L = \{a_1u_1 + a_2u_2 + a_3u_3 \mid a_1, a_2, a_3 \in \mathbb{Z}\}$. [2 punti]

✗ **Problema 5:** Sia R un anello commutativo con identità.

✗(a) Dimostrare che la formula binomiale $(r + s)^n = \sum_{k=0}^n \binom{n}{k} r^k s^{n-k}$ è valida in R . [2 punti]

✗(b) Sia \sim la relazione su R definita da $a \sim b$ se e solo se esiste un intero positivo n tale che $(a - b)^n = 0$. Dimostrare che \sim è una relazione di equivalenza. (Nota: n può dipendere da $a - b$). [1 punto]

✗ **Problema 6:**

✗(a) Qual è l'ordine del gruppo $G = GL_2(\mathbb{Z}_2)$ di matrici 2 per 2 invertibili con elementi in \mathbb{Z}_2 . [2 punti]

✗(b) Qual è il centro $Z(G)$ di G . [1 punto]

✗(c) Qual è l'equazione di classe per G . [1 punto]

✗ **Problema 7:**

✗(a) Verificare che $\mathbb{Q}(e^{\pi\sqrt{-1}/4}) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$. [2 punti]

✗(b) Calcola $[\mathbb{Q}(e^{\pi\sqrt{-1}/4}) : \mathbb{Q}]$. [1 punto]

PROBLEMA 1

Sia $S = \{ p \in \mathbb{N}^*: p \text{ è primo} \}$

Supponiamo $|S| < \infty$, allora $S = \{ p_1, \dots, p_s \}$

Sia $m = p_1 \cdots p_s$ il prodotto di tutti gli elementi di S .

Allora $\forall j \quad p_j \nmid m+1$

$\Rightarrow m+1$ è primo oppure ha un fattore primo $\notin S$
ma questa è una contraddizione

$\Rightarrow |S| = \infty$

PROBLEMA 2

$$\begin{aligned} a) \quad \text{EE}(237, 13) &\rightarrow \langle 1, -4, 1+4 \left\lfloor \frac{237}{13} \right\rfloor \rangle = \langle 1, -4, 73 \rangle \\ \text{EE}(13, 3) &\rightarrow \langle 1, 1, 0 - \left\lfloor \frac{13}{3} \right\rfloor \rangle = \langle 1, 1, -4 \rangle \\ \text{EE}(3, 1) &\rightarrow \langle 1, 0, 1 - 0 \rangle = \langle 1, 0, 1 \rangle \\ \text{EE}(1, 0) &\rightarrow \langle 1, 1, 0 \rangle \\ &\qquad\qquad\qquad \langle m, v', u' - v' \cdot \left\lfloor \frac{a}{b} \right\rfloor \rangle \end{aligned}$$

$$\text{MCD}(237, 13) = 1 ; \quad u = -4 ; \quad v = 73$$

$$\begin{aligned} b) \quad \text{EE}(x^4 + x^3 + x^2 + x + 1, x^2 + x + 1) &\rightarrow \langle 1, -x, 1+x(x^2) \rangle \\ \text{EE}(x^2 + x + 1, x + 1) &\rightarrow \langle 1, 1, 0 - x \rangle = \langle 1, 1, -x \rangle \\ \text{EE}(x + 1, 1) &\rightarrow \langle 1, 0, 1 \rangle \\ \text{EE}(1, 0) &\rightarrow \langle 1, 1, 0 \rangle \end{aligned}$$

$$\text{MCD}(x^4 + x^3 + x^2 + x + 1, x^2 + x + 1) = 1 ; \quad u = -x ; \quad v = 1 + x^3$$

$$\begin{array}{c} x^4 + x^3 + x^2 + x + 1 \\ \underline{x^4 + x^3 + x^2} \\ \hline x + 1 \end{array} \quad \left| \begin{array}{c} x^2 + x + 1 \\ \hline x^2 \end{array} \right.$$

$$\begin{array}{c} x^2 + x + 1 \\ \underline{x^2 + x} \\ \hline 1 \end{array} \quad \left| \begin{array}{c} x + 1 \\ \hline x \end{array} \right.$$

PROBLEMA 3

a) $|G| = 100 = 5^2 \cdot 2^2 \rightarrow 2, 1+1$

\therefore ci sono $2 \cdot 2 = 4$ gruppi

abeliani di ordine 100

100	5
20	5
4	2
2	2
1	

FATIQUI INUARIANTI:

1) $(a^2 b^2) = (100)$

TUTTI I POSSIBILI GRUPPI
ABELIANI DI ORDINE 100:

\mathbb{Z}_{100}

2) $(ab, ab) = (10, 10)$

$\mathbb{Z}_{10} \times \mathbb{Z}_{10}$

3) $(ab^2, a) = (20, 5)$

$\mathbb{Z}_{20} \times \mathbb{Z}_5$

4) $(a^2 b, b) = (50, 2)$

$\mathbb{Z}_{50} \times \mathbb{Z}_2$

b) $\phi(100) = \phi(5^2 \cdot 2^2) = \phi(5^2) \phi(2^2) = 20 \cdot 2 = 40$



PERCHÉ

$\text{MCD}(25, 4) = 1$

$$\phi(5^2) = 5^2 \left(1 - \frac{1}{5}\right) = 5^2 \cdot \frac{4}{5} = 20$$

$$\phi(2^2) = 2^2 \left(1 - \frac{1}{2}\right) = 2^2 \cdot \frac{1}{2} = 2$$

c) $3^{42} \pmod{100} = 3^{32+8+2} \pmod{100}$

Tramite quadrature successive:

$$3^1 \pmod{100} = 3$$

$$3^2 \pmod{100} = 9$$

$$3^4 \pmod{100} = 9^2 \pmod{100} = 81$$

$$3^8 \pmod{100} = 81^2 \pmod{100} = 61$$

$$3^{16} \pmod{100} = 61^2 \pmod{100} = 21$$

$$3^{32} \pmod{100} = 21^2 \pmod{100} = 41$$

$$\begin{aligned}
 3^{42} \bmod 100 &= (3^{32} \bmod 100)(3^8 \bmod 100)(3^2 \bmod 100) \bmod 100 \\
 &= (41 \cdot 61 \cdot 9) \bmod 100 \\
 &= 9
 \end{aligned}$$

OPPURE POSSEREMO DI ENTRARO:

$$\begin{aligned}
 \text{MCD}(a, n) = 1 &\Rightarrow a^{\phi(n)} \equiv 1 \pmod{n} \\
 \phi(100) = 40, \text{MCD}(3, 100) = 1 &\Rightarrow 3^{40} \cdot 3^2 \equiv 1 \pmod{100} \\
 &\Rightarrow 9 \equiv 1 \pmod{100}
 \end{aligned}$$

PROBLEMA 5

$$a) (r+s)^n = \sum_{k=0}^n \binom{n}{k} r^k s^{n-k}$$

R anello \Rightarrow su R sono definite le seguenti mappe:

$$+: R \times R \rightarrow R \quad e \quad *: R \times R \rightarrow R$$

Per induzione:

$$\cdot n=0: (r+s)^0 = 1 \quad \checkmark$$

$$\begin{aligned}
 \cdot n+1: (r+s)^{n+1} &= (r+s)^n(r+s) = \left(\sum_{k=0}^n \binom{n}{k} r^k s^{n-k} \right) (r+s) = \\
 &= \sum_{k=0}^n \binom{n}{k} r^k s^{n-k} + \sum_{k=0}^n \binom{n}{k} r^k s^{n+1-k} = \\
 &= r^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} r^{k+1} s^{n-k} + s^{n+1} + \sum_{k=1}^n \binom{n}{k} r^k s^{n+1-k} = \\
 &= r^{n+1} + s^{n+1} + \sum_{k=1}^n \left[\binom{n}{k-1} + \binom{n}{k} \right] r^k s^{n+1-k} \\
 \Rightarrow (r+s)^{n+1} &= r^{n+1} + s^{n+1} + \underbrace{\sum_{k=1}^n \binom{n+1}{k} r^k s^{n+1-k}}_{\text{PERCHÉ, PER LA REGOLA DI PASCAL}} \\
 &= \sum_{k=0}^{n+1} \binom{n+1}{k} r^k s^{n+1-k} \\
 &\quad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \\
 \Rightarrow \binom{n+1}{k} &= \binom{n-1}{k-1} + \binom{n}{k}
 \end{aligned}$$

b) $a \sim b \iff \exists n \in \mathbb{Z}, n > 0 \text{ t.c. } (a-b)^n = 0 \iff a = b$

- $a \sim a : (a-a)^n = 0 \quad \forall n$
- $a \sim b \Rightarrow b \sim a : (a-b)^n = 0 \Rightarrow (b-a)^n = 0$
- $a \sim b, b \sim c \Rightarrow a \sim c : (a-b)^n = 0, (b-c)^m = 0$
 $\Rightarrow (a-c)^{m+n} = ((a-b) + (b-c))^{m+n} =$
 $= \sum_{k=0}^{m+n} \binom{m+n}{k} (a-b)^k (b-c)^{m+n-k}$
 $k \leq n \Rightarrow m+n-k \geq m$
 $\Rightarrow (b-c)^{m+n-k} = 0$

PROBLEMA 6

a) $G = GL_2(\mathbb{Z}_2)$

$$a_{ij} = x \bmod 2 = \begin{cases} 0 \\ 1 \end{cases}$$

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

$$|G| = 6$$

b) $Z(G) = \{X \in G : AX = XA \ \forall A \in G\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} = I$

c) $|G| = |Z(G)| + \sum_{|C(x_i)| > 1} \underbrace{[G : C(x_i)]}_{|G / C(x_i)|}$

$$6 = 1 + \underbrace{2 + 3}_{\text{PERCEBE}} [G : C(x_i)] \mid |G| = 6$$

$$[G : C(x_i)] = 1, 2, 3, 6$$

$$|Z(G)| = 1 \Rightarrow G = 1 + 2 + 3$$

PROBLEMA 7

a) $\mathbb{Q}(e^{\frac{\pi i \sqrt{-1}}{4}}), \mathbb{Q}(\sqrt{-1}, \sqrt{2})$

i) $\mathbb{Q}(e^{\frac{\pi i \sqrt{-1}}{4}}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2})$

ii) $\mathbb{Q}(\sqrt{-1}, \sqrt{2}) \subseteq \mathbb{Q}(e^{\frac{\pi i \sqrt{-1}}{4}})$ } $\Rightarrow \mathbb{Q}(e^{\frac{\pi i \sqrt{-1}}{4}}) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$

$$y = e^{(\pi i)/4} = \cos(\pi/4) + i\sin(\pi/4) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

per la formula di EULER

$$e^{i\theta} = \cos\theta + i\sin\theta$$

$$i) y \in \mathbb{Q}(\sqrt{-1}, \sqrt{2}) \Rightarrow \mathbb{Q}(y) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2})$$

$$ii) y^2 = e^{(\pi i)/2} = \cos(\frac{\pi}{2}) + i\sin(\frac{\pi}{2}) = i \in \mathbb{Q}(y)$$

$$y^3 = e^{(3\pi i)/4} = \cos(\frac{3\pi}{4}) + i\sin(\frac{3\pi}{4}) = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

$$\Rightarrow y - y^3 = \frac{\sqrt{2}}{2} + i\cancel{\frac{\sqrt{2}}{2}} + \sqrt{2} - \cancel{\frac{\sqrt{2}}{2}}i = \sqrt{2} \in \mathbb{Q}(y)$$

$$\Rightarrow \mathbb{Q}(\sqrt{-1}, \sqrt{2}) \subseteq \mathbb{Q}(y)$$

$$b) [\mathbb{Q}(e^{\pi\sqrt{-1}/4}) : \mathbb{Q}]$$

$$m_{e^{\pi\sqrt{-1}/4}}(t) = t^4 + 1, m(e^{\pi\sqrt{-1}/4}) = 0$$

$$\partial_4 = 1 \Rightarrow m_{e^{\pi\sqrt{-1}/4}} \text{ é monico}$$

$$m(0) = 1 \pmod{3}$$

$$m(1) = 2 \pmod{3}$$

$$m(2) = 2 \pmod{3}$$

$$\Rightarrow m \text{ é irreducibile im } \mathbb{Z}_3[x]$$

$$\Rightarrow m \text{ é irreducibile im } \mathbb{Z}[x]$$

$$\deg(m_{e^{\pi\sqrt{-1}/4}}(t)) = 4 \Rightarrow [\mathbb{Q}(e^{\pi\sqrt{-1}/4}) : \mathbb{Q}] = 4$$

PROBLEMA 4

$$x + 2y + 3z \equiv 0 \pmod{6} \Rightarrow x + 2y + 3z = 6n$$

Applicando l' algoritmo per trovare una base del kernel a $(1 \ 2 \ 3 \ -6)$:

$$y=1, z=0, n=0 \Rightarrow x+2=0 \Rightarrow x=-2$$

$$\therefore v_1 = (-2, 1, 0, 0)$$

$$z=1, y=0, n=0 \Rightarrow x+3=0 \Rightarrow x=-3$$

$$\therefore v_2 = (-3, 0, 1, 0)$$

$$n=1, y=0, z=0 \Rightarrow x-6=0 \Rightarrow x=6$$

$$\therefore v_3 = (6, 0, 0, 1)$$

$$\therefore (u_1, u_2, u_3) \in \mathbb{Z}^3 \text{ sono } u_1 = (-2, 1, 0)$$

$$u_2 = (-3, 0, 1)$$

$$u_3 = (6, 0, 0)$$