Svolgimento Es. 1

(i) *

$$\mathbb{Z} \xhookrightarrow{j} \mathbb{Z}[i] \qquad m \longmapsto m + 0i$$

morfismo iniettivo ovviamente

$$\mathbb{Z}[i] \xrightarrow{\pi} \frac{\mathbb{Z}[i]}{(a+bi)} \qquad \alpha + \beta i \longmapsto [\alpha + \beta i] \bmod I$$

$\hat{I} := (a+bi)$ morfismo suriettivo ovviamente

$\Rightarrow$ la loro composizione

$$\mathbb{Z} \xhookrightarrow{j} \mathbb{Z}[i] \xrightarrow{\pi} \frac{\mathbb{Z}[i]}{(a+bi)} \qquad \varphi = \pi \circ j \text{ morfismo ovviamente}$$

* In $\mathbb{Z}[i]$ abbiamo

$$(a+bi)\cdot(a-bi) = a^2 + b^2 \Rightarrow a^2+b^2 \in (a+bi) = I$$

$$\Rightarrow \boxed{a^2+b^2 \in \mathbb{Z} \ \wedge \ a^2+b^2 \in \ker(\varphi)}$$

e contemporaneamente

* Dal Teorema di omomorfismo di anelli $\Rightarrow$

$\exists$ isomorfismo

$$\boxed{\frac{\mathbb{Z}}{\ker(\varphi)} \xrightarrow[\cong]{\overline{\varphi}} Im(\varphi) \subseteq \frac{\mathbb{Z}[i]}{(a+bi)}}$$

* Passo 1 $\quad \{ MCD(a,b) = 1 \Rightarrow \varphi \text{ suriettivo}$

Se dimostro ciò $\Rightarrow$

$$\boxed{\frac{\mathbb{Z}}{\ker(\varphi)} \underset{\overline{\varphi}}{\cong} \frac{\mathbb{Z}[i]}{(a+bi)} \text{ con inoltre } (a^2+b^2) \subseteq \ker(\varphi)}$$

Notiamo che

- $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}[i]/(a+bi) \qquad \varphi(1) = [1]_{\bmod \hat{I}}$ morfismo unitario
- $[i]_{\bmod \hat{I}} \in \frac{\mathbb{Z}[i]}{(a+bi)}$ è t.c. $[i]_{\bmod \hat{I}} \in Im(\varphi) \Leftrightarrow \exists\, m \in \mathbb{Z}$ t.c. $\varphi(m) = [i]_{\bmod \hat{I}}$

Ora

$$\boxed{\varphi(m) := [m]_{\bmod \hat{I}} = m + (a+bi) = m + \hat{I}} \qquad \forall m \in \mathbb{Z}$$

Perciò

$$[i]_{\bmod I} = \varphi(m) \Leftrightarrow [i]_{\bmod \hat{I}} = [m]_{\bmod I} \Leftrightarrow$$

$$i - m \in \hat{I} = (a+bi) \subset \mathbb{Z}[i]$$

i.e. $\nexists \Rightarrow \exists \ \alpha+\beta i \in \mathbb{Z}[i]$ t.c.

$$i - n = (a+bi)\cdot(\alpha+\beta i) \text{ in } \mathbb{Z}[i]$$

$$\Leftrightarrow \quad -n + 1\cdot i = (a\alpha - \beta b) + i(a\beta + \alpha b) \in \mathbb{Z}[i]$$

$$\nexists \Rightarrow \quad \boxed{\begin{cases} a\alpha - b\beta = -n \\ a\beta + b\alpha = 1 \end{cases} \text{ in } \mathbb{Z}}$$

* Visto che $1 = MCD(a,b)$ in $\mathbb{Z}$ $\Rightarrow$ $\exists\, \alpha_0, \beta_0 \in \mathbb{Z}$ t.c.

$\boxed{a\cdot\beta_0 + b\cdot\alpha_0 = 1}$ una Id. Bezout

Ma allora prendendo questi α_0 e β_0 determinati, posso porre

$\boxed{n_0 := a\cdot(-\alpha_0) + b\cdot(-\beta_0) \in \mathbb{Z}}$ $\Rightarrow$ ho trovato un intero $n_0 \in \mathbb{Z}$ t.c. soddisfi

$$\boxed{\varphi(n_0) = [i]_{\text{mod}\hat{I}}}$$

Perciò $\varphi(1) = [1]_{\text{mod}\hat{I}}$ e $\varphi(n_0) = [i]_{\text{mod}\hat{I}}$ $\Rightarrow$

- $\varphi(0) = \varphi(1+(-1)) \Rightarrow [0]_{\text{mod}I} = \varphi(1) + \varphi(-1) = [1] + \varphi(-1)$ (mod $\hat{I}$)
  $[0]_{\text{mod}\hat{I}}$ $\Rightarrow$ $\boxed{\varphi(-1) = -[1]_{\text{mod}\hat{I}}}$

- $n > 0 \Rightarrow \varphi(n) = \varphi(\underbrace{1+\cdots+1}_{n}) = \varphi(1)+\cdots+\varphi(1) = n\,[1]_{\text{mod}\hat{I}} = [n]_{\text{mod}\hat{I}}$

- $n < 0$ $\quad \varphi(|n|\cdot(-1)) = \varphi(|n|)\cdot\varphi(-1) = [|n|]\cdot(-[1]) = -[|n|]_{\text{mod}\hat{I}} = [n]_{\text{mod}\hat{I}}$ (mod I)

Perciò $\forall \ [\alpha+i\beta]_{\text{mod}\hat{I}} \in \dfrac{\mathbb{Z}[i]}{(a+bi)}$ $\Rightarrow$

$$\mathbb{Z} \ni \alpha + n_0\beta \xrightarrow{\varphi} [\alpha + n_0\beta]_{\text{mod}\hat{I}} = [\alpha+i\beta]_{\text{mod}\hat{I}}$$

$\nexists \Rightarrow$ φ suriettivo $\Rightarrow$ $\overline{\varphi}$ suriettivo

* **Passo 2**: $\ker(\varphi) = (a^2+b^2) \subseteq \mathbb{Z}$

• Sicuramente (*) $(a^2+b^2) \subseteq \ker(\varphi)$ perché

$a^2+b^2 = (a+bi)\cdot(a-bi) \Rightarrow a^2+b^2 \in (a+bi) \subseteq \mathbb{Z}[i]$

$\downarrow$ in $\mathbb{Z}[i]$

$\Rightarrow \varphi(a^2+b^2) = [0]_{\text{mod } I} \in A = \frac{\mathbb{Z}[i]}{(a+bi)} = \frac{\mathbb{Z}[i]}{I}$

• Viceversa, $\forall\, m \in \ker(\varphi) \subseteq \mathbb{Z} \Leftrightarrow \varphi(m) = [0]_{\text{mod } I} \frac{\mathbb{Z}[i]}{(a+bi)} = \frac{\mathbb{Z}[i]}{I} = A \Leftrightarrow$

- $m \in \mathbb{Z}$
- $j(m) = m + 0i \in (a+bi) \subset \mathbb{Z}[i]$
- $\exists\, (\alpha+\beta i) \in \mathbb{Z}[i]$ t.c. $m + 0i = (a+bi)\cdot(\alpha+\beta i) \Leftrightarrow$

(**) $\begin{cases} m = a\alpha - b\beta \\ 0 = a\beta + b\alpha \Rightarrow a\beta = -b\alpha \text{ in } \mathbb{Z} \end{cases}$

$$a\beta = -b\alpha \text{ in } \mathbb{Z} \quad (***)$$

Ma $MCD(a,b) = 1$ in $\mathbb{Z} \Rightarrow$

dalla (I) di (**) ↓

se $a = 1 \Rightarrow \beta = -b\alpha \Rightarrow m = 1\cdot\alpha + b^2\cdot\alpha = \alpha(b^2+1)$

$\Downarrow \to a = 1$

$m \in (1+b^2) = (a^2+b^2)$

$\Rightarrow \ker(\varphi) \subseteq (a^2+b^2)$

$\Downarrow$

$\ker(\varphi) = (a^2+b^2)$ ola (*)

Se $a > 1$ e $b \neq 0$

ola (***)

$a \mid b\alpha$ e $b \mid a\beta$ ma $MCD(a,b) = 1$ in $\mathbb{Z}$

$\Rightarrow$ $a \mid \alpha$ e $b \mid \beta$ i.e. $\exists\, s,t \in \mathbb{Z}$ t.c.

$\alpha = as$ e $\beta = bt$

Da (***)

$$a(bt) = -b(as) \iff abt = -b\cdot as \iff$$

$$ab(s+t) = 0 \text{ in } \mathbb{Z} \iff s = -t \text{ in } \mathbb{Z} \implies \begin{cases} \alpha = as \\ \beta = -\frac{b}{a}bs \end{cases}$$

$\mathbb{Z}$ intergo

$a \cdot b \neq 0$

per ipotesi

Ma allora dalla (I) eq. ch (**)

$$w = a^2 s - b(-bs) = s\cdot(a^2+b^2) \implies w \in (a^2+b^2)$$

$$\implies \ker(\varphi) \subseteq (a^2+b^2)$$

Da (*) $\boxed{\ker(\varphi) = (a^2+b^2)}$

Se infine $b = 0$ e $a > 1$ siccome $MCD(a,b) = 1$ questo caso non può capitare

$$\Downarrow$$

$$\boxed{\frac{\mathbb{Z}[i]}{(a+bi)} \cong \frac{\mathbb{Z}}{(a^2+b^2)}}$$

che pertanto è campo $\iff a^2+b^2 = p \in \mathbb{Z}$ primo $\iff N(\alpha) = p$ primo

Altrimenti non è nemmeno intergo

(ii) $\dfrac{\mathbb{Z}[i]}{(6+3i)}$

Ora $a+bi = 6+3i$ non sono coprimi $a=6$, $b=3$ ↓ non posso applicare (i)

Però $6+3i = 3\cdot(2+i)$ in $\mathbb{Z}[i]$

* 3 irriducibile in $\mathbb{Z}[i]$ perché $p=3\in\mathbb{Z}$ è $p\equiv 3 \pmod 4$
  $2+i$ irriducibile in $\mathbb{Z}[i]$ perché $N(2+i) = 4+1 = 5 \equiv 1 \pmod 4$
* Ora $(2+i)=(a+bi)$ $a=2$, $b=1$ stavolta ok il punto (i)

$$\Rightarrow \frac{\mathbb{Z}[i]}{(2+i)} \underset{\text{(i)}}{\cong} \frac{\mathbb{Z}}{(4+1)} = \frac{\mathbb{Z}}{5\mathbb{Z}}$$ campo con 5 elementi

* $\dfrac{\mathbb{Z}[i]}{(3)} =$ svolto esercitazione 26/5 Prof. Flamini Esercitazione 12 $\cong \dfrac{(\mathbb{Z}/3\mathbb{Z})[x]}{(x^2+\overline{1})}$

⇓ Campo con 9 elementi

$$\left\{ \bar{a}+\bar{b}\,i \;\middle|\; \bar{a},\bar{b}\in \mathbb{Z}/3\mathbb{Z},\ i^2 = -\bar{1} = \bar{2} \text{ in } \mathbb{Z}/3\mathbb{Z} \right\}$$

* Notiamo che

$$MCD(3,\ 2+i) \in U(\mathbb{Z}[i])$$

Infatti

$$N(3) = 9 \quad > \quad N(2+i) = 4+1 = 5$$

$\Rightarrow$ consideriamo per algoritmo euclideo

$\dfrac{3}{2+i}$ in $\mathbb{Q}[i] \cong \dfrac{\mathbb{Q}[x]}{(x^2+1)} \subseteq \mathbb{C}$ è

$$\frac{3}{2+i} = 3\cdot\frac{\overline{2+i}}{|2+i|^2} = 3\cdot\frac{(2-i)}{5} = \frac{6}{5} - \frac{3}{5}i \quad \Rightarrow \quad \frac{6}{5} = 1{,}2 \qquad -\frac{3}{5} = -0{,}6$$

Prendo $\boxed{\delta = 1-1i \in \mathbb{Z}[i]}$

$$\Rightarrow \quad 3-(2+i)\cdot\delta = 3-(2+i)(1-i) = +i$$

$\Rightarrow$ $3 = (2+i)(1-i) + i$

$\alpha = \beta \quad \delta + \omega$

$\omega = i$ resto

$i \sim 1$ associati in $\mathbb{Z}[i]$

Inoltre la divisione successiva $\beta : \omega$ fornisce

$(2+i) = (1-2i) \cdot i + 0 \rightarrow$ resto zero

$\Rightarrow$ Ultimo resto non nullo è $i \sim 1$ associati

$\Rightarrow$ $\boxed{MCD(3, 2+i) = 1 \quad (\text{a meno di associati})}$

* Posto $I := (3)$ e $J := (2+i)$

$\boxed{I + J = (MCD(3, 2+i)) = (1)}$ $\Rightarrow$ $I, J \subset \mathbb{Z}[i]$ ideali coprimi in $\mathbb{Z}[i]$

$\mathbb{Z}[i]$ è PID

$\Rightarrow$ Per Teorema CINESE DEI RESTI in anelli

$$\boxed{\frac{\mathbb{Z}[i]}{I \cdot J} \cong \frac{\mathbb{Z}[i]}{I} \times \frac{\mathbb{Z}[i]}{J}}$$

prodotto diretto anelli

$I \cap J = I \cdot J = (3 \cdot (2+i)) = (6+3i) = \hat{I}$

$$A = \frac{\mathbb{Z}[i]}{\hat{I}} = \frac{\mathbb{Z}[i]}{(6+3i)} \cong \frac{\mathbb{Z}[i]}{(3)} \times \frac{\mathbb{Z}[i]}{(2+i)}$$

$$\cong \frac{\mathbb{Z}/3\mathbb{Z}[x]}{(x^2+1)} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$$

$\frac{\mathbb{Z}/3\mathbb{Z}[x]}{(x^2+1)}$ campo con 9 elementi

$\frac{\mathbb{Z}}{5\mathbb{Z}}$ campo con 5 elementi

isomorfo a prodotto diretto di campi (no dominio)

$\Rightarrow$ ha 45 elementi $\Rightarrow$ $\boxed{\left| \frac{\mathbb{Z}[i]}{(6+3i)} \right| = 45}$

Posto

$$A := \frac{\mathbb{Z}[i]}{(6+3i)} \qquad \text{con } \hat{I} = (6+3i)$$

$\mathrm{Char}(A)$ = ordine additivo dell'unità moltiplicativa

cioè chi è il minimo $n \in \mathbb{N}$ t.c.

$$\underbrace{[1]_{\mathrm{mod}\hat{I}} + [1]_{\mathrm{mod}\hat{I}} + \dots + [1]_{\mathrm{mod}\hat{I}}}_{n\text{-volte}} = [\bar{0}]_{\mathrm{mod}\hat{I}} \ ?$$

Ma ciò è equivalente a considerare $n \in \mathbb{N}$ minimo t.c.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\ j\ } & \mathbb{Z}[i] \\ & \searrow^{\varphi} & \downarrow \pi \\ & & \dfrac{\mathbb{Z}[i]}{(6+3i)} = \dfrac{\mathbb{Z}[i]}{\hat{I}} = A \end{array}$$

$$\varphi(n) = [0]_{\mathrm{mod}(6+3i)} \iff j(n) \in (6+3i)$$

$$\| \quad [n]_{\mathrm{mod}(6+3i)}$$

$\iff \exists\ a+bi \in \mathbb{Z}[i]$ t.c.

$$n = (6+3i)\cdot(a+bi) \iff \begin{cases} n = 6a - 3b \\ 0 = 6b + 3a \end{cases}$$

$$6b + 3a = 0 \implies 3a = -6b \implies a = -2b$$

$$n = 6(-2b) - 3b = -15b = 15(-b)$$

$$\implies \boxed{n = 15 = (6+3i)(2-i)}$$

$\implies 15 \in (6+3i)$ ed è il minimo $n \in \mathbb{N}$ con tale proprietà

perché $N(6+3i) = 45 = 3^2 \cdot 5$ $\qquad N(15) = 225 = 3^2 \cdot 5^2$

15 è il minimo intero t.c. $j(n) \in (6+2i)$ la cui norma sia divisa da 45.

Svolgimento esercizio 2

(i) $\mathbb{Q}$ campo $\Rightarrow$ $\mathbb{Q}[x]$ euclideo $\Rightarrow$ $\mathbb{Q}[x]$ è DFU $\Rightarrow$

$(\mathbb{Q}[x])[y] \cong \mathbb{Q}[x,y]$ è DFU

Ora $f(x,y) = x^2 y^2 - 2x - 2 \in \mathbb{Q}[x,y] = (\mathbb{Q}[x])[y]$ cioè

$$F(y) := \underbrace{(x^2)}_{\text{coeff.}} y^2 + \underbrace{(2x+2)}_{\text{coeff}} \in (\mathbb{Q}[x])[y]$$

Ora $\mathbb{Q}[x]$ dominio euclideo $\Rightarrow$ $\mathbb{Q}(\mathbb{Q}[x]) = \mathbb{Q}(x)$

($\mathbb{Q}[x]$ ↪ $\mathbb{Q}(x)$; $\mathbb{Q}(x)$ = campo funzioni razionali a coeff in $\mathbb{Q}$)

$F(y) \in (\mathbb{Q}[x])[y] \subset \mathbb{Q}(x)[y]$ euclideo perché $\mathbb{Q}(x)$ campo

$\deg(F(y)) = 2$ come elemento $(\mathbb{Q}(x))[y]$

$\Rightarrow$ $\deg(F(y)) = 2$

è irriducibile in $(\mathbb{Q}(x))[y]$ (equiv. no radici in $\mathbb{Q}(x)$)

Infatti se esistesse una radice in $\mathbb{Q}(x) \ni \frac{P(x)}{Q(x)}$, con $MCD(P(x), Q(x)) = 1$ in $\mathbb{Q}[x]$

Allora $\frac{P(x)}{Q(x)}$ sarebbe soluzione di $F(y) = 0$

$\Rightarrow$ $x^2 \cdot \left(\frac{P(x)}{Q(x)}\right)^2 - 2x - 2 = 0$ in $\mathbb{Q}(x)$

$\Leftrightarrow$ $x^2 (P(x))^2 = (2x+2) Q(x)^2 = 2(x+2) \cdot (Q(x))^2$ in $\mathbb{Q}[x]$ (*)

Siccome $MCD(P(x), Q(x)) = 1$ in $\mathbb{Q}[x]$

$P(x) \nmid Q(x)$ in $\mathbb{Q}[x]$ e $x \nmid (x+2)$ in $\mathbb{Q}[x]$ e viceversa

Dalla eguaglianza in $\mathbb{Q}[x]$ (*) $\Rightarrow$ $x \mid Q(x)$ e $(x+2) \mid P(x)$ $\Leftarrow$

$Q(x) = x \cdot h(x)$ $\quad$ $P(x) = (x+2) \cdot g(x)$ per qualche $h(x), g(x) \in \mathbb{Q}[x]$

Siccome $MCD(P(x), Q(x)) = 1$ $\Rightarrow$ $MCD(g(x), h(x)) = 1$

$\Rightarrow$ $x^2 \cdot (x+2)^2 \cdot g(x)^2 = 2(x+2) \cdot x^2 \cdot h(x)^2$ in $\mathbb{Q}[x]$

$\Rightarrow$ $(x+2) \cdot (g(x))^2 = 2 \cdot (h(x))^2$

$h(x) \nmid g(x)$ e viceversa perché $MCD(g, h) = 1$

$(g(x))^2 \mid 2$ in $\mathbb{Q}[x]$ $\not\Rightarrow$ perché $\sqrt{2} \notin \mathbb{Q} \subset \mathbb{Q}[x]$

Infatti se $(g(x))^2 \mid 2 \Rightarrow \deg((g(x))^2) = 0 \Rightarrow \deg(g(x)) = 0$

$\Rightarrow g(x) \in \mathbb{Q}$ costante e $(g(x))^2 = 2$ $\not\Rightarrow$ in $\mathbb{Q}$, $\nexists\, \alpha \in \mathbb{Q}$ t.c. $\alpha^2 = 2$

$\Rightarrow$ $F(y)$ irriducibile in $(\mathbb{Q}(x))[y]$ euclideo

Poiché (coefficienti: x^2, $2x+2$)

$MCD(x^2, 2x+2) = 1$ in $\mathbb{Q}[x]$ $\Mapsto$

$F(y) = (x^2)\,y^2 - (2x+2) \in (\mathbb{Q}[x])[y]$ è PRIMITIVO

$\Mapsto$ $F(y)$ è irriducibile in $(\mathbb{Q}[x])[y]$

$\Rightarrow$ $f(x,y) \in \mathbb{Q}[x,y]$ è irriducibile

(iii) $B := \dfrac{\mathbb{Q}[x,y]}{(x^2+2x+2)}$

$g(x,y) = g(x) = x^2+2x+2 \in \mathbb{Q}[x] \subset (\mathbb{Q}[x])[y] = \mathbb{Q}[x,y]$

Allora

$g(x) \in \mathbb{Q}[x]$ è irriducibile perché lo è in $\mathbb{R}[x]$ e $\mathbb{Q}[x] \subset \mathbb{R}[x]$ entrambi euclidei

dunque $D \neq U$

e $\Delta = b^2 - 4ac = 4 - 8 = -4 < 0$

$\Rightarrow$ $g(x) \in (\mathbb{Q}[x])[y] = \mathbb{Q}[x,y]$ irriducibile

perché $U(\mathbb{Q}[x,y]) = U(\mathbb{Q}[x]) = \mathbb{Q}$

$\Rightarrow$ $g(x)$ è primo in $\mathbb{Q}[x,y]$ $D \neq U$

$\Rightarrow$ $(g(x)) = (x^2+2x+2)$ è ideale primo

$\Rightarrow$ B è dominio intero

Però

$\frac{\mathbb{Q}[x]}{(x^2+2x+2)}$ = $\mathbb{K}$ campo perché $\mathbb{Q}[x]$ euclideo $\Rightarrow$ $\mathbb{Q}[x]$ PID $\Rightarrow$ (x^2+2x+2) è primo = massimale

Si tratta di dimostrare

$$\frac{\mathbb{Q}[x,y]}{(x^2+2x+2)} \cong \left(\frac{\mathbb{Q}[x]}{(x^2+2x+2)}\right)[y] = \mathbb{K}[y]$$

↓ Euclideo quindi DFU

Gli elementi di $\mathbb{K}$ sono

$$\mathbb{K} = \{ a+bx \mid a,b \in \mathbb{Q},\ x^2 = -2x-2 \}$$

↓ classi resto modulo la divisione per x^2+2x+2 in $\mathbb{Q}[x]$

* Abbiamo un omomorfismo quelli suriettivo

$$\varphi : \mathbb{Q}[x,y] \twoheadrightarrow \mathbb{K}[y]$$

$\mathbb{Q} \ni \frac{m}{n} \longrightarrow \frac{m}{n}$ $\forall$ razionale $\frac{m}{n} \in \mathbb{Q}$

$x \longrightarrow x$

$x^2 \longrightarrow -2x-2$

$x^3 \longrightarrow x(-2x-2) = -2x^2-2x =$
$= -2(-2x-2)-2x =$
$= 4x+4-2x = 2x+4$

$\forall n \geq 4$ $x^n \longrightarrow$ quelli conti usando $x^2 = -2x-2$

$y \longrightarrow y$

$\forall n \geq 2$ $y^n \longrightarrow y^n$ indeterminata y priva di relazioni in B

* Chiaramente

$$I = (g(x)) = (x^2+2x+2) \subseteq \ker(\varphi)$$

$\forall\, h(x,y) = g(x)\cdot k(x,y) \in (x^2+2x+2)\cdot k(x,y)$

$$\Rightarrow \quad \varphi(h(x,y)) = \varphi(x^2+2x+2)\cdot\varphi(k(x,y)) = 0\cdot\varphi(k(x,y)) = 0$$

(φ morfismo anelli)

$\Downarrow$

$\boxed{(x^2+2x+2) \subseteq \ker(\varphi)}$

* Viceversa

$\forall\, h(x,y) \in \ker(\varphi) \subset \mathbb{Q}[x,y] = (\mathbb{Q}[x])[y]$, lo posso scrivere

$$h(x,y) = p_n(x)\cdot y^n + p_{n-1}(x)\cdot y^{n-1} + \cdots + p_0(x)$$

con $p_j(x) \in \mathbb{Q}[x]$, $0 \le j \le n$

$$\Rightarrow \quad \varphi(h(x,y)) = \varphi(p_n(x))\cdot\varphi(y^n) + \varphi(p_{n-1}(x))\cdot\varphi(y^{n-1}) + \cdots + \varphi(p_0(x))$$

(φ morfismo di anelli)

$$= \underbrace{\varphi(p_n(x))\cdot y^n + \varphi(p_{n-1}(x))\cdot y^{n-1} + \cdots + \varphi(p_0(x))}_{\in\, \mathbb{K}[y]}$$

perché $\varphi(p_j(x)) = [p_j(x)]_{\mathrm{mod}(x^2+2x+2)}$ per def. di φ

Perciò

$h(x,y) \in \ker(\varphi) \iff \varphi(h(x,y))$ polinomio identicamente nullo in $\mathbb{K}[y] \iff \varphi(p_j(x)) = 0 \quad \forall\, 0 \le j \le n$

$\iff p_j(x) \in (x^2+2x+2) \subset \mathbb{Q}[x] \quad \forall\, 0 \le j \le n$

$\iff g(x) \mid p_j(x) \quad \forall\, 0 \le j \le n \iff p_j(x) = g(x)\cdot \hat{p}_j(x)$

$\iff h(x,y) = g(x)\cdot\hat{p}_n(x)\,y^n + g(x)\cdot\hat{p}_{n-1}(x)\,y^{n-1} + \cdots + g(x)\hat{p}_0(x)$

$\iff h(x,y) = g(x)\cdot\left(\hat{p}_n(x)\cdot y^n + \cdots + \hat{p}_0(x)\right)$

$= g(x)\cdot\hat{h}(x,y)$

$\Leftrightarrow$ $h(x,y) \in (g(x)) = (x^2+2x+2)$

$\Rightarrow$ $\boxed{\ker(\varphi) \subseteq (x^2+2x+2)}$ $\Rightarrow$

Per doppia inclusione

$$\boxed{\ker(\varphi) = (x^2+2x+2)}$$

$$\Downarrow$$

$$\boxed{\frac{\mathbb{Q}[x,y]}{(x^2+2x+2)} \cong \mathbb{K}[y] = B}$$

dove $\mathbb{K} = \frac{\mathbb{Q}[x]}{(x^2+2x+2)}$ campo $\Rightarrow$ $\mathbb{K}[y]$ euclideo $\Rightarrow$

$\mathbb{K}[y]$ DFU $\Leftrightarrow$ B è DFU

Però

$$f(x,y) = x^2y^2 + 2x + 2 \in \mathbb{Q}[x,y]$$

$$\downarrow \varphi$$

$$\varphi(f(x,y)) \in \mathbb{K}[y] = B$$

è un elemento RIDUCIBILE di B

infatti $x^2 \equiv -(2x+2)$ in B

$$\varphi(f(x,y)) \equiv (-2x-2)y^2 + (2x+2) =$$

$$= (2x+2)(-y^2+1) = 2\cdot(x+1)\cdot(1-y^2) =$$

$$= \underbrace{2(x+1)}_{\in \mathbb{K}^*} \cdot (1-y) \cdot (1+y)$$

$(1-y)$, $(1+y)$ irriducibili perché lineari in $\mathbb{K}[y]$

$2(x+1) \in \mathbb{K}^* = U(\mathbb{K})$ $\Rightarrow$ a meno di associati

i fattori irriducibili in B di $\varphi(f(x,y))$ sono:

$$\boxed{(1-y) \quad e \quad (1+y)}$$

Svolgimento Es. 3

(i) Per ipotesi $MCD(a, n) = 1$ in $\mathbb{Z}$

$\Rightarrow$ $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ è invertibile $\Leftrightarrow$

$\bar{a} \in U(\mathbb{Z}/n\mathbb{Z})$ gruppo moltiplicativo con

$|U(\mathbb{Z}/n\mathbb{Z})| = \Phi(n)$, Φ di Eulero

Ma allora nel gruppo moltiplicativo vale

$$(\bar{a})^{\Phi(n)} = \bar{1}$$

i.e. in $\mathbb{Z}$ $\boxed{(a)^{\Phi(n)} \equiv 1 \pmod n}$

In particolare se $n = p \Rightarrow \mathbb{Z}/p\mathbb{Z}$ campo e $\Phi(p) = p-1$

$\forall\ \bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ gruppo invertibili

in $\mathbb{Z}/p\mathbb{Z}$ vale $\boxed{(\bar{a})^{p-1} = \bar{1}}$

$\Downarrow$

se moltiplico $\bar{a} \cdot \bar{a}^{p-1} = \bar{a} \cdot \bar{1} \Rightarrow \bar{a}^p = \bar{a} \Leftrightarrow$

$\Leftrightarrow$ in $\mathbb{Z}$ vale $\boxed{a^{p-1} \equiv 1 \mod p}$ (*)

$\forall\ a$ coprimo con p

$\Leftrightarrow$ in $\mathbb{Z}$ vale $\boxed{a^p \equiv a \mod p}$ (**)

$\forall\ a$ coprimo con p

[Ovviamente anche $0^p \equiv 0 \pmod p$

quindi l'ultima vale $\forall\ \bar{a} \in \mathbb{Z}/p\mathbb{Z}$ (***)]

(ii) Per semplicità notazionale sia

$$\boxed{b = 123456 \in \mathbb{Z}}$$

e sia $a \in \{0, 1, -, 10\}$ t.c.

$\bar{b} = \bar{a} \in \mathbb{Z}/11\mathbb{Z}$ cioè $\boxed{b \equiv a \pmod{11} \text{ in } \mathbb{Z} \text{ con } a \in \{0, 1, -, 10\}}$

Posto $b = 987654 \in \mathbb{N}$ sto cercando $x \in \{0,1,\dots,10\}$ t.c.

$$b^k \equiv x \pmod{11}$$

Ma se $a \in \{0,1,\dots,10\}$ t.c. $b \equiv a \pmod{11}$ $\Rightarrow$

$b = 11q + a$ e

$$b^k = (11q+a)^k \overset{\text{Newton}}{=} \sum_{j=0}^{k} \binom{k}{j} (11q)^j a^{k-j}$$

$\Rightarrow$ $$b^k = a^k + \binom{k}{1} 11 \cdot q \cdot a^{k-1} + \binom{k}{2} (11q)^2 a^{k-2} + \dots + \binom{k}{k} (11q)^k$$

↓ 11 divide ogni addendo

$\Rightarrow$ $$\boxed{b^k \equiv a^k \pmod{11}}$$

$\Downarrow$

Posso subito risolvere $b \pmod{11}$ per risolvere a $\Rightarrow$

Divido $b = 123456$ per 11 in $\mathbb{Z}$

$\Rightarrow$

$$123456 = (11) \cdot (11223) + 3$$
$$\| \quad\quad \| \quad\quad \| \quad\quad \|$$
$$D \quad\quad d \quad\quad q \quad\quad r = a$$

D → dividendo; d → divisore; q → quoziente; r → resto

$\Rightarrow$ $$\boxed{a = 3 \in \mathbb{Z}/11\mathbb{Z}}$$

$\Rightarrow$ $$\boxed{b^k \equiv 3^k \pmod{11}}$$ $\Rightarrow$ Qui riduco a risolvere $3^k \equiv x \pmod{11}$

* Ora in $U(\mathbb{Z}/11\mathbb{Z})$ ho cardinalità 10 da (i) sappiamo che vale identità di Eulero

$$\boxed{\overline{3}^{10} = \overline{1} \quad \text{in } U(\mathbb{Z}/11\mathbb{Z})}$$

cioè $3^{10} \equiv 1 \pmod{11}$ in $\mathbb{Z}$

Ma allora

$$3^{10 \cdot h} \equiv (3^{10})^h \equiv 1^h \equiv 1 \pmod{11} \quad \forall\, h \geq 1$$

Divido a libro l'esponente

$k = 987654$ per 10 $\Rightarrow$

$$\underset{\parallel}{987654} = \underset{\parallel}{10}\,(\underset{\parallel}{98765}) + \underset{\parallel}{4}$$

k = D dividendo — d divisore — q quoziente — r resto

Perciò

$$3^{k} = 3^{(10 \cdot 9 + 4)} = 3^{(10q)} \cdot 3^{4}$$

Dunque

$$3^{987654} = 3^{(10)\cdot 9} \cdot 3^{4} \equiv \overline{1} \cdot \overline{3}^{4} \pmod{11}$$

* In $\mathbb{Z}/11\mathbb{Z}$ si ha:

$$\overline{3}^{2} = \overline{9}\,, \quad \overline{3}^{3} = \overline{27} = \overline{5}\,, \quad \overline{3}^{4} = \overline{5}\cdot\overline{3} = \overline{15} = \overline{4}$$

In altre parole si ha che

$$\overline{b^{k}} = (123456)^{987654} = \overline{4} \text{ in } \mathbb{Z}/11\mathbb{Z}$$

cioè $\boxed{b^{k} \equiv 4 \pmod{11} \text{ in } \mathbb{Z}}$

cioè $\boxed{x = 4}$

(iii) (I) $x^2 \equiv 4 \pmod{14}$
(II) $x \equiv 3 \pmod{5}$

sistema congruenze non lineare

(II) $\Rightarrow$ $5 \mid (x-3)$ in $\mathbb{Z}$

(I) $14 \mid (x^2-4)$ in $\mathbb{Z}$ cioè

$2 \cdot 7 \mid (x^2-4)$ in $\mathbb{Z}$

$\Rightarrow$ $\begin{cases} 2 \mid (x^2-4) \iff 2 \mid x^2 \Rightarrow \boxed{x^2 \equiv 0 \pmod 2} \\ 7 \mid (x^2-4) \Rightarrow 7 \mid (x^2-4) \Rightarrow \boxed{x^2 \equiv 4 \bmod 7} \end{cases}$

Però:

- $x^2 \equiv x \pmod 2$ se x pari $\iff$ x^2 pari
  se x dispari $\iff$ x^2 dispari

  $x^2 \equiv 0 \pmod 2 \iff \boxed{x \equiv 0 \pmod 2 \iff x \text{ pari}}$

- $x^2 - 4 \equiv 0 \pmod 7 \iff 7 \mid (x^2-4) = (x-2)(x+2)$

  e 7 primo $\Rightarrow$ $\boxed{7 \mid (x-2) \text{ o } 7 \mid (x+2)}$

* Perciò il sistema di congruenze iniziale di viene equivalente a due diversi sistemi lineari

$\begin{cases} x = 2k \text{ pari} \\ x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod 5 \end{cases}$

↓

SISTEMA CINESE

$\begin{cases} x = 2k \text{ pari} \\ x \equiv -2 \equiv 5 \pmod 7 \\ x \equiv 3 \pmod 5 \end{cases}$

↓

SISTEMA CINESE

* I sistema cinese con $x = 2k$ diventa

$$\begin{cases} 2k \equiv 2 \pmod 7 \\ 2k \equiv 3 \pmod 5 \end{cases}$$

visto che $(\mathbb{Z}/7\mathbb{Z})$ campo e $(\mathbb{Z}/5\mathbb{Z})$ campo

$$\Leftrightarrow \begin{cases} k = \overline{1} \text{ in } \mathbb{Z}/7\mathbb{Z} \\ k = \overline{2}^{-1} \cdot \overline{3} \equiv \overline{3} \cdot \overline{3} = \overline{9} = \overline{4} \text{ in } \mathbb{Z}/5\mathbb{Z} \end{cases}$$

$\overline{3} \cdot \overline{2} = \overline{6} = 1$ in $\mathbb{Z}/5\mathbb{Z}$

$$\begin{cases} k \equiv 1 \pmod 7 \\ k \equiv 4 \pmod 5 \end{cases}$$

sistema cinese

Risolvo con algoritmo cinese

$R = 7 \cdot 5 \qquad r_1 = 7 \qquad r_2 = 5 \Rightarrow R_1 = \frac{R}{r_1} = 5 \qquad R_2 = \frac{R}{r_2} = 7$

$$\begin{cases} k \equiv c_1 \pmod{r_1} \\ k \equiv c_2 \pmod{r_2} \end{cases}$$

$\Rightarrow$ Rivedere esercitazione 10
6 Maggio 2025

Poiché $MCD(R_1, r_1) = 1 = MCD(R_2, r_2)$

$$\begin{cases} R_1 k \equiv c_1 \pmod{r_1} \longrightarrow \exists!\ k_1^\circ \text{ sol. } \pmod{r_1} \\ R_2 k \equiv c_2 \pmod{r_2} \longrightarrow \exists!\ k_2^\circ \text{ sol. } \pmod{r_2} \end{cases}$$

Ora

$$\begin{cases} R_1 k \equiv c_1 \pmod{r_1} \\ 7k \equiv c_2 \pmod{r_2} \end{cases} \qquad \begin{cases} 5k \equiv 1 \pmod 7 \\ 7k \equiv 4 \pmod 5 \end{cases} \Leftrightarrow$$

$$\begin{cases} \overline{5} k = \overline{1} \text{ in } \mathbb{Z}/7\mathbb{Z} \\ \overline{7} k = \overline{4} \text{ in } \mathbb{Z}/5\mathbb{Z} \end{cases}$$

$\overline{5}^{-1} = \overline{3}$ in $\mathbb{Z}/7\mathbb{Z}$ $\qquad \boxed{k_1^\circ = 3}$

$\overline{7} k = \overline{4}$ in $\mathbb{Z}/5\mathbb{Z} \Leftrightarrow$

$\overline{2} k = \overline{4}$ in $\mathbb{Z}/5\mathbb{Z} \Leftrightarrow$

$k = \overline{2}^{-1} \cdot \overline{4}$ in $\mathbb{Z}/5/7\mathbb{Z}$

$\overline{2}^{-1} = \overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$

$k_2^\circ = \overline{3} \cdot \overline{4} = \overline{12} = \overline{2} \Rightarrow \boxed{k_2^\circ = 2}$

Prendo

$$\overline{k^0} = k_1^0 \cdot R_1 + k_2^0 \cdot R_2 = k_1^0 n_2 + k_2^0 n_1$$

$$\overline{k^0} \equiv k_1^0 n_2 \pmod{n_1} \quad \text{e} \quad \overline{k^0} \equiv k_2^0 n_1 \pmod{n_2}$$

Perciò

$$\overline{k^0} = 3 \cdot 5 + 2 \cdot 7 = 15 + 14 = 29$$

$\overline{k^0} = 29$! soluzione ok $\begin{cases} k \equiv 1 \pmod 7 \\ k \equiv 4 \pmod 5 \end{cases}$

MODULO $R = 35$

$\Downarrow$

$\overline{x^0} = 2\,\overline{k^0} = 58$ unica soluz. ok

I sistema

$\begin{cases} x \text{ pari}, x \equiv 0 \pmod 2 \\ x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \end{cases}$

MODULO $R_{tot} = 2 \cdot 7 \cdot 5 = 70$

$$\boxed{\overline{x^0} = 58 \text{ unica } \pmod{70}}$$

* II sistema cinese

$$\begin{cases} x = 2k \\ 2k \equiv -2 \pmod 7 \\ 2k \equiv 3 \pmod 5 \end{cases} \iff \begin{cases} x = 2k \\ k \equiv -1 \pmod 7 \\ k \equiv 4 \pmod 5 \end{cases}$$

$k \equiv 4 \pmod 5$ → come prima

Ma $-\overline{1}$ in $\mathbb{Z}/7\mathbb{Z}$ è $\overline{6}$ in $\mathbb{Z}/7\mathbb{Z}$

$$\begin{cases} x = 2k \\ k \equiv 6 \mod 7 \\ k \equiv 4 \mod 5 \end{cases}$$

$\begin{cases} k \equiv 6 \pmod 7 \\ k \equiv 4 \pmod 5 \end{cases}$ è sistema cinese con 1 soluzione modulo 35

Metodo alternativo al precedente (sostituzioni successive)

(I) $\Rightarrow k = 6 + 7m, \quad m \in \mathbb{N}$

Nella II

$$6 + 7m \equiv 4 \pmod 5$$

$$7m \equiv 4 - 6 \pmod 5$$

In $\mathbb{Z}/5\mathbb{Z}$

$$\overline{7}\,\overline{m} = -\overline{2} \iff \overline{2}\,\overline{m} = \overline{3} \iff m = \overline{2}^{-1} \cdot \overline{3} = \overline{3} \cdot \overline{3} = \overline{9} = \overline{4}$$

$\overline{m} = \overline{4}$ in $\mathbb{Z}/5\mathbb{Z} \Rightarrow m = 4 + 5h$

Ma allora

$$k = 6 + 7 \cdot (4 + 5h) = 6 + 28 + 35h$$

$$= 34 + 35h$$

cioè $k \equiv 34 \pmod{35}$

$$\Rightarrow \quad x = 2(34 + 35h) = 68 + 70h$$

$x \overset{\circ}{=} 68 \pmod{70}$ unica soluzione mod 70

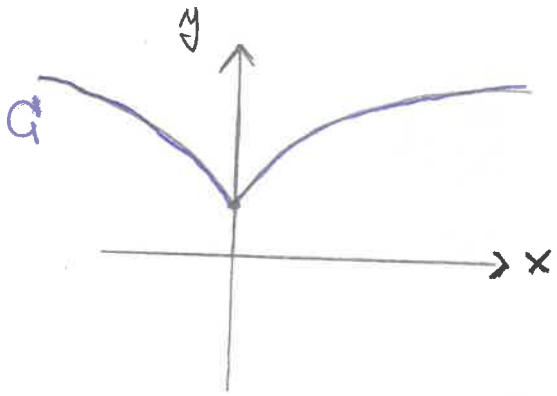
Pertanto il sistema originario

$\begin{cases} x^2 \equiv 4 \pmod{14} \\ x \equiv 3 \pmod 5 \end{cases}$ ha 2 soluzioni modulo 70

$x^\circ = 58$ e $x^\circ = 68$

Svolgimento esercizio 4

Consideriamo



$G = \{(x,y) \in \mathbb{R}^2 \mid y^3 = x^2 + 1\} \subset \mathbb{R}^2$ curva in $\mathbb{R}^2$ (algebrica)

Verificare che le uniche soluzioni in $\mathbb{Z} \times \mathbb{Z}$ (cioè punti interi di G) sono solo $(x_0, y_0) = (0, 1)$

* $G \cap (\mathbb{Z} \times \mathbb{Z}) \neq \emptyset$ poichè $(0,1) \in G \cap (\mathbb{Z} \times \mathbb{Z})$

* Sia $(x_0, y_0) \in G \cap (\mathbb{Z} \times \mathbb{Z})$ una soluzione
  $\Rightarrow$ $x_0 \in \mathbb{Z}$ è necessariamente pari

dim Se p.a. x_0 dispari $\vdash\!\triangleright$ x_0^2 dispari $\Rightarrow$ $x_0^2 + 1$ pari

$\Rightarrow$ y_0^3 è pari $\vdash\!\triangleright$ y_0 è pari $\vdash\!\triangleright$ y_0^3 è t.c

$$\boxed{y_0^3 \equiv 0 \pmod 8}$$ (se $y_0 = 2h \Rightarrow y_0^3 = 8h^3$)

$\Rightarrow$ $x_0^2 + 1 \equiv 0 \pmod 8$ $\Rightarrow$ $x_0^2 \equiv -1 \pmod 8$

i.e. $x_0^2 \equiv 7 \pmod 8$

Ma per $\forall\, x_0 \in \mathbb{Z}/8\mathbb{Z}$, $\{x_0^2 \mid x_0 \in \mathbb{Z}/8\mathbb{Z}\} = \{\bar 0, \bar 1, \bar 4\}$

perciò $\nexists\, x_0 \in \mathbb{Z}/8\mathbb{Z}$ per cui $x_0^2 = \bar 7$ in $\mathbb{Z}/8\mathbb{Z}$

$\vdash\!\triangleright$ x_0 è pari ∎

- (ii) $y^3 = x^2 + 1 = (x+i)\cdot(x-i)$

fattorizzazione in $(\mathbb{Z}[i])[x]$

Perciò se $(x_0, y_0) \in C \cap (\mathbb{Z} \times \mathbb{Z})$ è soluzione

$$(x_0+i),\ (x_0-i) \in \mathbb{Z}[i]$$

* Ora se consideriamo

$J := (x_0+i,\ x_0-i) \subset \mathbb{Z}[i]$ ideale

$\Rightarrow$ $x_0 + i - (x_0 - i) = 2i \in J$

$\Rightarrow$ $(-i)\cdot 2i = 2 \in J \cap \mathbb{Z}$

* Però $x_0^2 + 1 \in J$ perchè $x_0^2 + 1 = (x_0+i)\cdot(x_0-i) \in J$

e x_0 pari oppure (i) $\Rightarrow$ $x_0^2 + 1 \in \mathbb{Z}$, dispari

$\Rightarrow$ $x_0^2 + 1 \in J \cap \mathbb{Z}$ e x_0^2+1 dispari

Poichè $x_0^2 + 1 = 2k + 1$, $k \in \mathbb{Z}$

$x_0^2 + 1 \in J \ni 2$

$\Rightarrow$ $(x_0^2 + 1) - 2(k) = (2k+1) - 2k = 1$

$x_0^2+1 \in J$, $2 \in J$, $k \in \mathbb{Z} \subset \mathbb{Z}[i]$

$\Rightarrow$ $1 \in J$ $\Rightarrow$ $\boxed{J = (1)}$

$\Rightarrow$ $J = (x_0+i,\ x_0-i) = (1)$

$\Rightarrow$ $\exists\ \alpha, \beta \in \mathbb{Z}[i]$ t.c $(x_0+i)\cdot\alpha + (x_0-i)\cdot\beta = 1$

cioè $\boxed{MCD(x_0+i,\ x_0-i) = 1 \text{ in } \mathbb{Z}[i]}$

$\Rightarrow$ (x_0+i) e (x_0-i) coprimi in $\mathbb{Z}[i]$

(iii) Siccome $MCD(x_0+i, x_0-i)=1$ e vale

$$(x_0-i)\cdot(x_0+i) = y_0^3 \quad \text{in } \mathbb{Z}[i]$$

$y_0 \in \mathbb{Z} \subset \mathbb{Z}[i]$ euclideo $\Rightarrow$ DFU

$$y_0 = \prod_{j=1}^{k} \alpha_j \qquad \text{con } \alpha_j \in \mathbb{Z}[i]$$

tutti e soli gli irriducibili = primi di $\mathbb{Z}[i]$ della sua fattorizzazione (a meno di un.)

$$\Rightarrow \quad y_0^3 = \prod_{j=1}^{k} \alpha_j^3$$

$$\forall\, \alpha_j \mid y_0 \Rightarrow \alpha_j \mid (x_0-i)\cdot(x_0+i)$$

α_j primo $\Rightarrow$ o $\alpha_j \mid (x_0-i)$ oppure $\alpha_j \mid (x_0+i)$

Siccome $MCD(x_0-i, x_0+i) = 1$, se $\alpha_j \mid (x_0-i) \Rightarrow \alpha_j \nmid (x_0+i)$

Perciò possiamo assumere $\exists$ indice t t.c.

$$1 < t \leq k$$

per cui $\alpha_j \mid (x_0-i)$ e $\alpha_j \nmid (x_0+i)$, $1 \leq j \leq t$

$\alpha_s \nmid (x_0-i)$ e $\alpha_s \mid (x_0+i)$, $t < s \leq k$

$$\Rightarrow \quad (x_0-i) = \alpha_1^3 \cdot \ldots \cdot \alpha_t^3 = (\alpha_1 \cdot \ldots \cdot \alpha_t)^3$$

$$(x_0+i) = (\alpha_{t+1} \cdot \ldots \cdot \alpha_s)^3$$

$\Rightarrow$ x_0-i e x_0+i cubi in $\mathbb{Z}[i]$.

(iv) Visto che (x_0+i) e (x_0-i) cubi in $\mathbb{Z}[i] \Rightarrow$

$\exists (a+ib) \in \mathbb{Z}[i]$ t.c

$$(x_0+i) = (a+bi)^3 = (a^3 - 3ab^2) + i(3a^2b - b^3)$$

$$\Updownarrow$$

$$\begin{cases} (I) & x_0 = a\cdot(a^2 - 3b^2) \\ (II) & 1 = b\cdot(3a^2 - b^2) \end{cases} \quad \text{in } \mathbb{Z}$$

Dalla (II) equazione in $\mathbb{Z}$ $\Rightarrow$ $b = \pm 1 \in \mathbb{Z}$

- se $b = 1$ $\Rightarrow$ $3a^2 = 1$ $\nexists$ $a \in \mathbb{Z}$
- se $b = -1$ $\Rightarrow$ $3a^2 - 1 = -1$ $\Rightarrow$ $3a^2 = 0$ $\Rightarrow a = 0$

$\Rightarrow$ $a + bi = -i$ i.e. $\boxed{a = 0, b = -1}$

Ma allora dalla (I) $\Rightarrow$ $x_0 = 0$ $\Rightarrow$ $y_0 = 1$

$\boxed{(x_0, y_0) = (0, 1)}$ unica soluzione

Approccio classico di risolvere problemi in anelli A e approcciarli in sovraanelli

$$A \subsetneq B$$

$$\mathbb{Z} \qquad \mathbb{Z}[i]$$