es. 1) Teorema cinese del Resto:

a) Dati $m, n \in \mathbb{N}$ primi tra loro, dim. che

$$f: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$
$$x \longmapsto (x+n\mathbb{Z},\ x+m\mathbb{Z})$$

induce un isomorfismo $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$\Rightarrow f(x) = (x+n\mathbb{Z},\ x+m\mathbb{Z})$

$\Rightarrow \operatorname{Ker} f = \{x \in \mathbb{Z} \mid x+m\mathbb{Z} = 0, x+n\mathbb{Z} = 0\}$
$\overset{!}{=} \{x \in \mathbb{Z} \mid x \in n\mathbb{Z} \cap m\mathbb{Z}\} = n\mathbb{Z} \cap m\mathbb{Z}$

$\Rightarrow n\mathbb{Z} \cap m\mathbb{Z} = mn\mathbb{Z}$ (m,n coprimi)

Teorema di Omomorfismo:

$$\begin{tikzcd}
\mathbb{Z} \arrow[rr, "f"] \arrow[dr] & & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\
& \mathbb{Z}/mn\mathbb{Z} \arrow[ur, "\exists!"'] &
\end{tikzcd}$$

SE f suriettiva

Mostriamo che f è suriettiva:

$\exists x \in \mathbb{Z}$ t.c. $(a,b) = f(x)$ $\forall (a,b) \in \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}$

$$\Leftrightarrow \begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

per Bézout si ha che $\exists \alpha, \beta \in \mathbb{Z}$ t.c. $\alpha n + \beta m = 1$

$$\Rightarrow \begin{cases} (\bmod\ n) \Rightarrow \beta m \equiv 1 \\ (\bmod\ m) \Rightarrow \alpha n \equiv 1 \end{cases} \Rightarrow b\alpha n + a\beta m = 1$$

$$\Rightarrow b\alpha n + a\beta m \equiv \left\langle \begin{matrix} a \pmod{n} \\ b \pmod{m} \end{matrix} \right. \Rightarrow \text{sia } x = b\alpha n + a\beta m$$

$\Rightarrow f(x) = (a + n\mathbb{Z},\ b + m\mathbb{Z}) \Rightarrow f$ è suriettiva

$\Rightarrow$ vale il Teorema di omomorfismo.

q.e.d.

b) Dati $n, m \in \mathbb{Z}$ coprimi, $a, b \in \mathbb{Z}$, trovare $x \in \mathbb{Z}$ t.c.

$x + n\mathbb{Z} = a + n\mathbb{Z}$, $x + m\mathbb{Z} = b + m\mathbb{Z}$.

$\Rightarrow$ visto sopra: $x = b\alpha n + a\beta m$ con $\alpha n + \beta m = 1$

c) Risolvere il problema di Sun Tsu: determinare $x \in \mathbb{N}$ t.c. $x/3$ dia resto 2, $x/5$ dia resto 3 e $x/7$ dia resto 2

$$\Rightarrow \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \Rightarrow \quad \begin{tikzcd} \mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/mn\mathbb{Z} \arrow[ur, "\sim"'] & \end{tikzcd}$$

$\Rightarrow$ siano α, β t.c. $3\alpha + 5\beta = 1$:

$$\begin{aligned} 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 3 - 2 \cdot 1 \\ &\overset{!}{=} 3 - (5 - 3 \cdot 1) \cdot 1 \\ &\overset{!}{=} 2 \cdot 3 - 5 \end{aligned} \quad \Rightarrow \alpha = 2, \ \beta = -1$$

$\Rightarrow 3 \cdot 3 \cdot 2 + 2 \cdot 5 \cdot (-1) = 8 = x$

$$\Rightarrow \begin{tikzcd} \mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ \mathbb{Z}/105\mathbb{Z} \arrow[ur, "\sim"'] & \end{tikzcd}$$

$\Rightarrow \alpha \cdot 15 + \beta \cdot 7 = 1$

$\Rightarrow \alpha = 1, \ \beta = -2$

$\Rightarrow 1 \cdot 15 - 2 \cdot 7 = 1$

$\Rightarrow x = 2 \cdot 1 \cdot 15 - 8 \cdot 2 \cdot 7 = -82$

$\Rightarrow -82 + 105\mathbb{Z} = 23 + 105\mathbb{Z}$

---

es. 2)

Calcolare il MCD tra $x^2 + x + 1$ e $x^2 + 2x + 2$ in $\mathbb{R}[x]$ ed esprimerlo come combinazione lineare.

$$\Rightarrow \quad \begin{array}{ccc|c} x^2 & +\,2x & +\,2 & x^2+x+1 \\ \cline{4-4} x^2 & +\,x & +\,1 & 1 \\ \hline // & x & +\,1 & \end{array} \qquad \Rightarrow x^2+2x+2 = (x^2+x+1)+(x+1)$$

$$\Rightarrow \quad \begin{array}{ccc|c} x^2 & +\,x & +\,1 & x+1 \\ \cline{4-4} x^2 & +\,x & & x \\ \hline // & // & 1 & \end{array} \qquad \Rightarrow x^2+x+1 = (x+1)x+1$$

$$\Rightarrow (x+1) = 1(x^2+2x+2) - 1(x^2+x+1)$$

$$\begin{aligned} \Rightarrow 1 &= 1(x^2+x+1) - x(x+1) \\ &\overset{!}{=} 1(x^2+x+1) - x\left[1(x^2+2x+2) - 1(x^2+x+1)\right] \\ &\overset{!}{=} \underbrace{(1+x)}_{\alpha}(x^2+x+1)\underbrace{-\,x}_{\beta}(x^2+2x+2) \end{aligned}$$

N.B.

La richiesta dell'esercizio è assolutamente equivalente alla seguente:
Calcolare l'inverso di x^2+x+1 in $\mathbb{R}[x]/(x^2+2x+2)\mathbb{R}[x]$
(se possibile, ovvero $\Leftrightarrow$ MCD $= 1$)

---

es. 3)

Dato $R = \mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ (interi di Gauss), sia
$$\delta : R\setminus\{0\} \longrightarrow \mathbb{N}, \quad x \longmapsto a^2+b^2 = \|x\|^2$$

a) Dato $z \in \mathbb{C}$, trovare $q \in \mathbb{Z}[i]$ t.c. $\|z-q\|^2 \leq \frac{1}{2}$

$\Rightarrow z = a+ib$, $a, b \in \mathbb{R} \Rightarrow$ siano $\tilde{a}, \tilde{b} \in \mathbb{Z}$ t.c.
$\|a-\tilde{a}\| \leq \frac{1}{2}$, $\|b-\tilde{b}\| \leq \frac{1}{2}$

$\Rightarrow \| z - q \| = \dots = \| a - \tilde{a} \|^2 + \| b - \tilde{b} \|^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$

b) Dim. che $(R, +, \delta)$ è anello euclidea

$\Rightarrow$ Dati $z, w \in \mathbb{Z}[i]$ dobbiamo trovare $q, r \in \mathbb{Z}[i]$ t.c. $z = wq + r$ con $\delta(r) < \delta(w)$

$\Rightarrow \frac{z}{w} \in \mathbb{C}$. Per (a) $\exists q \in \mathbb{Z}[i]$ t.c. $\| \frac{z}{w} - q \|^2 \leq \frac{1}{2}$

$\Rightarrow \tilde{r} = \frac{z}{w} - q \leq \frac{1}{2} \Rightarrow w\left(\frac{z}{w} - q\right) = w\tilde{r}$

$\Rightarrow z - wq = w\tilde{r} \Rightarrow w\tilde{r} = r \Rightarrow z = wq + r$ con $w, q \in \mathbb{Z}[i] \Rightarrow \delta(r) = \|r\|^2 = \|w\tilde{r}\|^2 = \delta(w)\delta(\tilde{r}) \leq \frac{1}{2}\delta(w) < \delta(w)$

c) Determinare R^* (elementi invertibili di R):

$z \in R^* \Leftrightarrow \exists w \in \mathbb{Z}[i]$ t.c. $zw = wz = 1$

$\Rightarrow \delta(zw) = \delta(1) \Rightarrow \delta(z)\delta(w) = 1 \Rightarrow \delta(z) = \delta(w) = 1$

$\Rightarrow R^* = \{1, -1, i, -i\}$

d) Scomporre in fattori irriducibili l'elemento 2

$2 = (1+i)(1-i)$

---

es. 4)

Calcolare la divisione euclidea tra $a = -2 + 5i$ e $b = 1 + 2i$

$\Rightarrow \delta(a) = 29, \ \delta(b) = 5 \Rightarrow \frac{a}{b} = \frac{-2+5i}{1+2i} \cdot \frac{1-2i}{1-2i} = \frac{8+9i}{5}$

$= 1{,}6 + 1{,}8i = (2 - 0{,}4) + (2 - 0{,}2)i$

$= \underbrace{(2 + 2i)}_{q} + \underbrace{(-0{,}4 - 0{,}2i)}_{\tilde{r}}, \quad r = (1+2i)\left(-\frac{2}{5} - \frac{1}{5}i\right) = -i$

$\Rightarrow \underbrace{-2 + 5i}_{a} = \underbrace{(1+2i)}_{b}\underbrace{(2+2i)}_{q} + \underbrace{(-i)}_{r}$

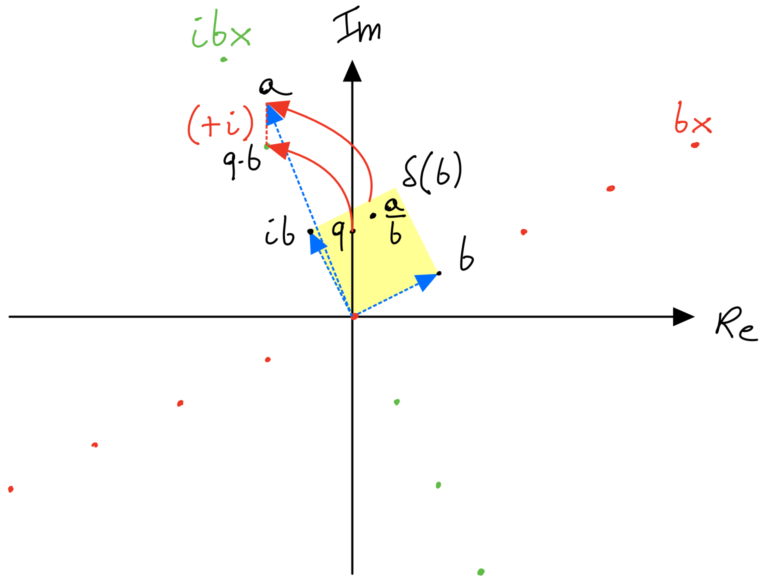
Interpretazione grafica ($b = 2+i$):

$a = bq + r$

$\delta(b) = \|b\|^2 = 5$

$b \cdot q = b(x+iy)$

$= \underset{\in \mathbb{Z}}{bx} + \underset{\in \mathbb{Z}}{byi}$



N.B.

Tale divisione euclidea NON È UNICA (nemmeno in $\mathbb{Z}$)