es. 1)

Dim. che $a \in \mathbb{Z}$ è divisibile per 3 $\Longleftrightarrow$ la somma delle sue cifre è divisibile per 3

$\Rightarrow$ sia $a = a_0 + 10 \cdot a_1 + \dots + 10^n \cdot a_n$

$\Rightarrow$ Consideriamo
$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z}$$
$$a \longmapsto a + 3\mathbb{Z} = [a]$$

si ha:

$$
\begin{aligned}
[a] &= [a_0 + 10 \cdot a_1 + \dots + 10^n \cdot a_n] \\
&\overset{!}{=} [a_0] + [10] \cdot [a_1] + \dots + [10]^n \cdot [a_n] \\
&\overset{!}{=} [a_0] + [a_1] + \dots + [a_n] \\
&\overset{!}{=} [a_0 + \dots + a_n]
\end{aligned}
$$

$[10] = [9+1] = [1]$

In particolare:

$$[a] = [0] \Longleftrightarrow [a_0 + \dots + a_n] = [0]$$

q.e.d.

---

es. 2)

Stabilire un criterio di divisibilità per 11

$\Rightarrow$ sia $a = a_0 + 10 \cdot a_1 + \dots + 10^n \cdot a_n$

$\Rightarrow$ Consideriamo
$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/11\mathbb{Z}$$
$$a \longmapsto a + 11\mathbb{Z} = [a]$$

si ha:

$$
\begin{aligned}
[a] &= [a_0 + 10 \cdot a_1 + \dots + 10^n \cdot a_n] \\
&\overset{!}{=} [a_0] + [10] \cdot [a_1] + \dots + [10]^n \cdot [a_n] \\
&\overset{!}{=} [a_0] - [a_1] + \dots + [-1]^n \cdot [a_n]
\end{aligned}
$$

$[10] = [-1]$

$\Rightarrow$ $a \in \mathbb{Z}$ divisibile per 11 $\Leftrightarrow$ la somma delle cifre di posto pari − la somma delle cifre di posto dispari è divisibile per 11

---

es. 3) Dato l'anello $\mathbb{Z}/18\mathbb{Z}$

1) Trovare tutti gli elementi invertibili e dim. che il gruppo $(\mathbb{Z}/18\mathbb{Z})^*$ è isomorfo a $\mathbb{Z}/6\mathbb{Z}$
2) Calcolare $[11]^{805}$

$\Rightarrow$ 1) Gli elementi invertibili di $\mathbb{Z}/18\mathbb{Z}$ sono esattamente gli interi $[0,17]$ che sono coprimi con 18

$\Rightarrow$ il numero di tali elementi è $\varphi(18)$ dove φ è la funzione di Eulero)

$\Rightarrow$ essi sono $\{1, 5, 7, 11, 15, 17\}$

$\Rightarrow (\mathbb{Z}/18\mathbb{Z})^* = \{1, 5, 7, 11, 15, 17\}$

Mostriamo che $(\mathbb{Z}/18\mathbb{Z})^*$ è ciclico:

$\Rightarrow 5^1 = 5, \quad 5^2 = [25] = 7, \quad 5^3 = [35] = 17$

$\Rightarrow 5^4 = [-1]\cdot 5 = 13, \quad 5^5 = [-5]\cdot 5 = 11$

$\Rightarrow 5^6 = [11]\cdot 5 = 55 = 1$

$\Rightarrow (\mathbb{Z}/18\mathbb{Z})^* = \langle 5 \rangle \Rightarrow (\mathbb{Z}/18\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$

Cerchiamo gli inversi di ciascun elemento:

$1^{-1} = 1, \quad 5^{-1} = 11, \quad 7^{-1} = 13, \quad 11^{-1} = 5, \quad 13^{-1} = 7, \quad 17^{-1} = 17$

$\Rightarrow$ 2) Calcoliamo:

$[11]^{805} \Rightarrow 805 = 804 + 1 = 6k + 1$

$$\Rightarrow [11]^{805} = 11^{6K+1} = 11^{6K} \cdot 11 = 1 \cdot 11 = 11$$

---

es. 4)

Dato $\mathbb{Z}[\sqrt{-7}] = \{ a + b\sqrt{-7} \mid a, b \in \mathbb{Z} \} \subseteq \mathbb{C}$ sottoanello, trovare un omomorfismo suriettivo $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[\sqrt{-7}]$ t.c. $\operatorname{Ker} \varphi = (x^2+7)\mathbb{Z}[x]$ e concludere che gli anelli $\mathbb{Z}[\sqrt{-7}]$ e $\mathbb{Z}[x]/(x^2+7)\mathbb{Z}[x]$ sono isomorfi

$\Rightarrow$ sappiamo che dati S anello commutativo, $R \subseteq S$ sottoanello, $s \in S$, $\exists! \varphi$ omomorfismo da $R[x]$ in S t.c. $\varphi(a) = a \quad \forall a \in R \wedge \varphi(x) = s$

$\Rightarrow$ tale φ è detto φ_s l'omomorfismo di valutazione in s

$\Rightarrow R[s] = \overrightarrow{\varphi_s}(R[x])$

$\Rightarrow$ Nel nostro caso:

$$\mathbb{Z} \subseteq \mathbb{C}, \quad s = \sqrt{-7} \quad \Rightarrow \mathbb{Z}[\sqrt{-7}] = \overrightarrow{\varphi_{\sqrt{-7}}}(\mathbb{Z}[x])$$

che equivale a:

$$\mathbb{Z}[\sqrt{-7}] = \{ a + b \cdot \sqrt{-7} \mid a, b \in \mathbb{Z} \}$$

$\Rightarrow$ il candidato φ è $\varphi_{\sqrt{-7}}$:

$$\operatorname{Ker} \varphi_{\sqrt{-7}} \stackrel{?}{=} (x^2+7)\mathbb{Z}[x]$$

mostriamolo per doppia inclusione:

1) $\supseteq \Rightarrow f \in (x^2+7)\mathbb{Z}[x] \Longleftrightarrow f(x) = (x^2+7)\, g(x)$

$$\Rightarrow \varphi_{\sqrt{-7}}(f) = f(\sqrt{-7}) = (-7+7) \cdot g(x) = 0$$

$$\Rightarrow f \in \operatorname{Ker} \varphi_{\sqrt{-7}}$$

2) $\subseteq$ $\Rightarrow f \in \operatorname{Ker} \varphi_{\sqrt{-7}} \Rightarrow f = (x^2+7)g(x) + ax + b$

(tale divisione è possibile dato che x^2+7 è monico). Mostriamo che $ax+b=0$

$\Rightarrow 0 = \varphi_{\sqrt{-7}}(f) = (-7+7)g(x) + (a\sqrt{-7}+b)$

$\Leftrightarrow a\sqrt{-7}+b = 0 \Rightarrow$ se $a=b=0$, concludo.

se $a \neq 0$, anche $b \neq 0$ ($\mathbb{C}$ è dominio) e quindi

$\sqrt{-7} = -\frac{b}{a} \in \mathbb{Q}$ ↯ $\Rightarrow a = b = 0$

$\Rightarrow f \in (x^2+7)\mathbb{Z}[x]$

$\Rightarrow \operatorname{Ker} \varphi_{\sqrt{-7}} = (x^2+7)\mathbb{Z}[x]$

$\Rightarrow \mathbb{Z}[\sqrt{-7}] \cong \mathbb{Z}[x]/(x^2+7)\mathbb{Z}[x]$ (per il Teorema di omomorfismo), infatti:

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[rr, "\varphi_{\sqrt{-7}}"] \arrow[dr, "\pi"'] & & \mathbb{Z}[\sqrt{-7}] \\
& \mathbb{Z}[x]/(x^2+7)\mathbb{Z}[x] \arrow[ur, dotted, "\exists!\ \sim"'] &
\end{tikzcd}$$