---

1. 1, 3, 7 e 9 são as unidades de $\mathbb{Z}_{10}$ pois em $\mathbb{Z}_n$ um elemento a é invertível se e só se $\mathrm{mdc}(a, n) = 1$.

A factorização $2 = 2 \cdot 6$ mostra que 2 é redutível (pois nem 2 nem 6 são unidades). Suponhamos agora que $2|ab$ em $\mathbb{Z}_{10}$. Então $ab = 2k$ para algum $k \in \mathbb{Z}_{10}$. Isto implica $ab - 2k = 10r$, isto é, $ab = 2(k + 5r)$, para algum inteiro r. Então $2|ab$ em $\mathbb{Z}$. Como 2 é primo em $\mathbb{Z}$, isto implica $2|a$ ou $2|b$ em $\mathbb{Z}$. Imediatamente $2|a$ ou $2|b$ em $\mathbb{Z}_{10}$.

2. **(a-i)** Suponhamos que $p = x^2 + y^2$, $x, y \in \mathbb{Z}$, e $x + yi = (a + bi)(c + di)$ em $\mathbb{Z}[i]$. Então $p = x^2 + y^2 = (a^2 + b^2)(c^2 + d^2)$. Logo $a^2 + b^2$ é uma unidade de $\mathbb{Z}$ (o que significa que $a + bi$ é uma unidade de $\mathbb{Z}[i]$) ou $c^2 + d^2$ é uma unidade de $\mathbb{Z}$ (o que significa que $c + di$ é uma unidade de $\mathbb{Z}[i]$). Uma vez que $x, y \neq 0$, então $x + yi$ não é nulo nem uma unidade, logo é um primo gaussiano. Além disso, como $p = (x + yi)(x - yi)$, p não é um primo gaussiano.

(a-ii) Se p não fosse um primo gaussiano, existiriam inteiros de Gauss não invertíveis $a + bi$ e $c + di$ tais que $p = (a + bi)(c + di)$, donde $p^2 = (a^2 + b^2)(c^2 + d^2)$. Como $a^2 + b^2$ e $c^2 + d^2$ são inteiros $\neq 0, 1, -1$, só podemos ter $p = a^2 + b^2$ ou $p = c^2 + d^2$, uma contradição.

(a-iii) Suponhamos que $p = x^2 + y^2$, $x, y \in \mathbb{Z}$. Como p é ímpar, então x é ímpar e y é par ou x é par e y é ímpar. Sem perda de generalidade, admitamos o primeiro caso: $x = 2a + 1$ e $y = 2b$. Então

$$p = x^2 + y^2 = (2a + 1)^2 + (2b)^2 = 4a^2 + 4a + 1 + 4b^2 \equiv 1 \,(\mathrm{mod}\, 4).^1$$

(b) Pelas alíneas anteriores, qualquer primo euclidiano $p \equiv 3 \,(\mathrm{mod}\, 4)$ (como, por exemplo, 3, 7, 11, 19) é também um primo gaussiano. Como $2 = (1 + i)(1 - i)$ e $5 = (2 + i)(2 - i)$, 2 e 5 são primos euclidianos que não são primos gaussianos.

3. **(a)** Como é de grau ≥ 1, se $f(x)$ não fosse primitivo, existiria um inteiro $d \neq 1, -1$ que dividiria todos os coeficientes de $f(x)$, ou seja, teríamos uma factorização $f(x) = d \cdot g(x)$ onde d não é uma unidade e $g(x)$ também (pois tem grau ≥ 1).

[1] A implicação recíproca também é verdadeira, mas muito mais difícil de provar. Juntando esta equivalência às alíneas anteriores podemos concluir que um primo euclidiano $p \neq 2$ é um primo gaussiano se e só se $p \not\equiv 1 \,(\mathrm{mod}\, 4)$, isto é, $p \equiv 3 \,(\mathrm{mod}\, 4)$.
Mostrando que existem infinitos primos euclidianos da forma $p = 4n + 1$ e da forma $p = 4n + 3$ é possível então concluir que, sendo P o conjunto dos primos euclidianos e G o conjunto dos primos gaussianos, $P \setminus G$ e $G \setminus P$ são ambos conjuntos *infinitos*.

(b-i) Suponhamos $I = \langle f(x) \rangle$ para algum $f(x) \in \mathbb{Z}[x]$. Como $d \in I = \langle f(x) \rangle$, então d é múltiplo de $f(x)$. Logo $\text{gr}(f(x)) = 0$, ou seja, $f(x) = a \in \mathbb{Z}$. Por outro lado, $x \in I$, pelo que também x é múltiplo de $f(x)$, isto é, $x = ag(x)$ para algum $g(x) \in \mathbb{Z}[x]$. Em particular, $\text{gr}(g(x)) = 1$. Seja $g(x) = b_1x + b_0$ ($b_1, b_0 \in \mathbb{Z}$, $b_1 \neq 0$). Como $x = a(b_1x + b_0) = ab_1x + ab_0$, então $1 = ab_1$ e a é invertível. Mas $a \in I$ logo $I = \mathbb{Z}[x]$. Isto é um absurdo, uma vez que $1 \notin I$ (observe que é impossível escrever 1 como soma de um múltiplo de x com um múltiplo de d pois $d \neq 1, -1$).

Solução alternativa: Comece por observar que

$$I = \{a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x] : d | a_0\}.$$

(b-ii) Claro que existe, pois $\mathbb{Z}[x]$ é um DFU, e é claramente igual a $\{1, -1\}$.

(c) Como $\mathbb{Z}$ é um DFU então $\mathbb{Z}[x]$ é um DFU. Pela alínea anterior não é um DIP.
