1. **Sigui $A$ un anell (unitari i commutatiu). Proveu les propietats següents.**

   (a) **Si $a \in A$ és una unitat (o sigui, un element invertible), aleshores $a$ no és un divisor de zero.**

   $\boxed{\textbf{Solucio}}$

   Sabem que:

$$\begin{aligned} a \in A \text{ és unitat } &\overset{def}{\iff} \exists a^{-1} \in A: \ (aa^{-1} = a^{-1}a = 1) \\ a \in A \text{ no és divisor de } 0 &\overset{def}{\iff} \nexists b \in A: \ (b \neq 0 \implies ab = 0) \\ &\iff \forall b \in A: \ (ab = 0 \implies b = 0) \end{aligned}$$

   Llavors només cal demostrar:

$$(\exists a^{-1} \in A: \ (aa^{-1} = a^{-1}a = 1)) \implies (\forall b \in A: \ (ab = 0 \implies b = 0))$$

   Per tant:

$$\begin{aligned} \forall b \in A: \ (ab = 0) &\implies a^{-1}(ab) = a^{-1}0 \\ &\implies (a^{-1}a)b = 0 \\ &\implies 1b = 0 \\ &\implies b = 0 \end{aligned}$$

   (b) **Si un ideal $I$ de $A$ conté una unitat, aleshores $I = A$.**

   $\boxed{\textbf{Solucio}}$

   Sabem que:

$$\begin{aligned} u \in A \text{ és unitat } &\overset{def}{\iff} \exists u^{-1} \in A: \ (uu^{-1} = u^{-1}u = 1) \\ I \subseteq A \text{ és ideal de } A &\overset{def}{\iff} ((I, +) \text{ subgrup abelia}) \wedge (\forall a \in A, \ b \in I: \ ab \in I) \end{aligned}$$

   Primer de tot, veiem que:

$$\left.\begin{aligned} \exists u^{-1} \in A: \ (uu^{-1} = u^{-1}u = 1) \\ u^{-1} \in A, \ u \in I \implies u^{-1}u \in I \end{aligned}\right\} \implies u^{-1}u = 1 \in I$$

   Aplicant el resultat anterior, tenim:

$$\forall a \in A: \ (a1 = 1a = a) \implies \forall a \in A: \ a1 = a \in I$$

   Per tant:

$$\left.\begin{aligned} \forall a \in A: \ a1 = a \in I &\implies A \subseteq I \\ I \text{ és ideal de } A &\implies I \subseteq A \end{aligned}\right\} \implies I = A$$

   (c) **Si $a \in A$ i $u \in A$ és una unitat, aleshores $(ua) = (a)$.**

   $\boxed{\textbf{Solucio}}$

   Sabem que:

$$(ua) = (a) \iff ((ua) \subset (a)) \wedge ((ua) \supset (a))$$

   Llavors:

$\boxed{\subset}$ $\forall b \in A:\ ba \in (a) \implies \exists u \in A:\ ua \in (a)$
$\implies \forall b \in A:\ (b(ua) \in (ua) \implies b(ua) \in (a))$
$\implies (ua) \subset (a)$

$\boxed{\supset}$ $u$ unitat $\implies \exists u^{-1} \in A:\ u^{-1}(ua) \in (ua)$
$\implies u^{-1}(ua) = (u^{-1}u)a = a \in (ua)$
$\implies \forall b \in A:\ (ba \in (a) \implies ba \in (ua))$
$\implies (a) \subset (ua)$

(d) **Si $A$ és un domini d'integritat i $a, b \in A$, aleshores $(a) = (b)$ si, i només si, $b = au$ per a alguna unitat $u$ de $A$.**

**Solucio**

Demostrem les dos implicacions:

$\boxed{\Rightarrow}$ Sabem que $(a) = (b)$:

$$\left.\begin{array}{l} a \in (b) \implies \exists c \in A:\ a = cb \\ b \in (a) \implies \exists d \in A:\ b = da \end{array}\right\} \implies a = cb = c(da) = (cd)a \implies a - adc = 0 \\ \implies a(1 - dc) = 0$$

Llavors, com $A$ és un domini d'integritat, tenim $1 - dc = 0$ o $a = 0$.

- $1 - dc = 0 \implies dc = 1 \implies d$ invertible i $b = da = ad$
- $a = 0 \implies (a) = (0) = \{0\} = (b)$
  $\implies b = 0$
  $\implies \forall u \in A:\ (u \text{ invertible} \implies 0 = 0u)$

$\boxed{\Leftarrow}$ Sigui $u \in A$ unitat, $b = ua \implies (b) = (ua)$. Llavors:

$$\left.\begin{array}{l} \forall c \in A:\ [c(ua) \in (ua) \implies c(ua) = (cu)a \in (a)] \implies (ua) \subset (a) \\ \forall c \in A:\ [ca \in (a) \implies ca = (cu^{-1})(ua) \in (ua)] \implies (a) \subset (ua) \end{array}\right\} \implies (a) = (b)$$

2. **Caracteritzeu, en funció del nombre enter $m > 1$, quins són els elements invertibles i quins els divisors de zero de l'anell $\mathbb{Z}/m\mathbb{Z}$. Deduïu que $\mathbb{Z}/m\mathbb{Z}$ és un domini d'integritat si, i només si, $\mathbb{Z}/m\mathbb{Z}$ és un cos; si, i només si, $m$ és un nombre primer.**

**Solucio**

Sigui $(\mathbb{Z}/m\mathbb{Z})^*$ el conjunt dels elements invertibles de $\mathbb{Z}/m\mathbb{Z}$ i $z(\mathbb{Z}/m\mathbb{Z})$ el conjunt dels elements divisors de 0 de $\mathbb{Z}/m\mathbb{Z}$. Primer de tot trobarem els elements de $(\mathbb{Z}/m\mathbb{Z})^*$:

$$\begin{aligned} x \in (\mathbb{Z}/m\mathbb{Z})^* &\iff \exists y \in \mathbb{Z}/m\mathbb{Z}:\ xy \equiv 1\ (mod\ m) \\ &\iff \exists \lambda \in \mathbb{Z}:\ xy = 1 + \lambda m \\ &\iff xy - \lambda m = 1 \\ &\implies \exists d \in \mathbb{Z}:\ [mcd(x, n) = d \implies d \mid x \wedge d \mid m] \\ &\implies d \mid xy - \lambda m = 1 \\ &\implies d = mcd(x, m) = 1 \end{aligned}$$

$$\begin{aligned} x \in \mathbb{Z}/m\mathbb{Z}:\ mcd(x, m) = 1 &\implies \exists a,\ b \in \mathbb{Z}:\ xa + mb = 1 \\ &\iff xa = 1 - mb \\ &\iff xa \equiv 1\ (mod\ m) \\ &x \in (\mathbb{Z}/m\mathbb{Z})^* \end{aligned}$$

Per tant, $(\mathbb{Z}/m\mathbb{Z})^* = \{x \in \mathbb{Z}/m\mathbb{Z} \mid mcd(x,m) = 1\}$.

Llavors, busquem els elements de $z(\mathbb{Z}/m\mathbb{Z})$. Sabem que si un element dsadas

Suposem $a \in \mathbb{Z}/m\mathbb{Z}$ no invertible, i considerem $mcd(a,m) = d$, tal que $\exists \lambda : \ a = \lambda d$ i $m = \mu d$. Llavors, sigui $b \in \mathbb{Z}/m\mathbb{Z}$:

$$\begin{aligned}
ab \equiv 0 \ (mod\ m) &\iff \exists k \in \mathbb{Z} : \ ab = 0 + km \\
&\iff ab = (\lambda d) b \\
&\implies [b = \mu \neq 0 \implies ab = (\lambda d)\mu = \lambda m = 0 + km] \\
&\implies a \text{ divisor de } 0
\end{aligned}$$