Problema 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.

Solució. Volem caracteritzar els elements invertibles de $\mathbb{Z}/m\mathbb{Z}$.

Sigui $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$, $\overline{a} \neq \overline{0}$.

$\overline{a}$ és invertible $\Leftrightarrow$ Existeix $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$, tal que $\overline{a} \cdot \overline{b} = \overline{1}$ $\Leftrightarrow$ Existeix $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ tal que $\overline{a}\overline{b} - \overline{1} = \overline{0}$.

Siguin a, b representants respectius de $\overline{a}, \overline{b}$. La igualtat anterior es tradueix a:

$\overline{a}$ invertible $\Leftrightarrow$ Existeix $b \in \mathbb{Z}$ tal que $ab - 1 = \lambda m$, per a un cert $\lambda \in \mathbb{Z}$. Però això és equivalent a $1 = ab - \lambda m$, per a certs b, λ de $\mathbb{Z}$. Això ens diu que a i m són coprimers. Per tant, els elements invertibles de $\mathbb{Z}/m\mathbb{Z}$ són els $\overline{a}$ tals que $m.c.d(a, m) = 1$ en $\mathbb{Z}$.

Parlem ara dels divisors de zero de $\mathbb{Z}/m\mathbb{Z}$. Fem la següent afirmació: $\overline{a} \neq \overline{0}$ és un divisor de zero de $\mathbb{Z}/m\mathbb{Z}$ si, i només si, $m.c.d(a, m) = c$, amb $c \neq \pm 1, \pm m$, i on a i m són representants de $\overline{a}$ i $\overline{m}(= \overline{0})$ respectivament.

$\Rightarrow$)

Suposem que $\overline{a} \neq \overline{0}$ és un divisor de zero. Per l'apartat anterior, si fos $c = \pm 1$, llavors $\overline{a}$ seria invertible. Sabem, però, que els elements invertibles no són mai divisors de zero. En efecte, si A és un anell i tenim que $xy = 0$ amb $x \in A$ invertible i $y \neq 0$, multiplicant per x^{-1} a tots dos costats, arribem a $y = 0$, absurd. Per tant c no pot ser ± 1.

D'altra banda, si c fos $\pm m$, llavors a seria un múltiple de m i per tant la seva classe seria $\overline{0}$, en contradicció amb el que suposem.

$\Leftarrow$)

Si suposem $m.c.d(a, m) = c$, $c \neq \pm 1, \pm m$, llavors existeixen $x, y \in \mathbb{Z}$ tals que $a = xc, m = yc$. En aquest cas, trobar un $\overline{b} \neq \overline{0}$ tal que $\overline{a}\overline{b} = \overline{0}$ és trivial. És suficient prendre la classe $\overline{y}$, ja que tindrem $\overline{a}\,\overline{y} = \overline{xcy} = \overline{x}\,\overline{m} = \overline{x}\overline{0} = \overline{0}$ i $\overline{a}, \overline{y} \neq \overline{0}$.

Finalment, demostrem $\mathbb{Z}/m\mathbb{Z}$ és domini d'integritat $\Leftrightarrow$ $\mathbb{Z}/m\mathbb{Z}$ és cos $\Leftrightarrow$ m és primer.

(2) $\Rightarrow$ (1)

Trivial, ja que tot cos és domini d'integritat .

(1) $\Rightarrow$ (3)

Si $\mathbb{Z}/m\mathbb{Z}$ és domini d'integritat, no té divisors de zero i per tant tot enter $1 < a < m$ és coprimer amb m, com acabem de veure. En particular, això implica que m és un nombre primer.

$(3) \Rightarrow (2)$

Sigui $\overline{a}$ un element no nul de $\mathbb{Z}/m\mathbb{Z}$. Podem triar un representant de $\overline{a}$ de la forma $1 < a < m$. Com que m és un nombre primer, $m.c.d(a, m) = 1$ i per la identitat de Bézout, existeixen λ, μ en $\mathbb{Z}$ tals que $1 = a\lambda + m\mu$. És a dir, existeixen λ, μ tals que $1 - m\mu = a\lambda$. Passant al quocient $\mathbb{Z}/m\mathbb{Z}$, tenim $\overline{a}\overline{\lambda} = \overline{1} - \overline{0} = \overline{1}$. Acabem de trobar l'invers de $\overline{a}$, és precisament $\overline{\lambda}$.