



Universidad Nacional Autónoma de México

Facultad de Ciencias

Álgebra superior 2

Tarea examen 2

Elías López Rivera

elias.lopezr@ciencias.unam.mx

Fecha: 27/07/2025



Problema 1

Para $n \in \mathbb{Z}$ define $D(n) = \{x \in \mathbb{Z} \mid x|n\}$

- I. Encuentra $D(20)$ y $D(25)$
- II. Encuentra $D(20) \cup D(25)$
- III. Encuentra el $\text{mcd}(20, 25)$
- IV. Expresa $\text{mcd}(20, 25)$ de 5 maneras diferentes como combinación lineal de 20 y 25

Demostración.

i) Tenemos que:

$$D(20) := \{-20, -10, -5, -4, -2, -1, 1, 2, 4, 5, 10, 20\}$$

$$D(25) := \{-25, -5, -1, 1, 5, 25\}$$

ii) Encontramos que:

$$D(20) \cup D(25) := \{-5, -1, 1, 5\}$$

iii) Tenemos que $\text{mcd}(5, 25) := \max\{D(20) \cup D(25)\} = 5$

iv) Tenemos que:

I. $20(-1) + 25(1) = 5$

II. $20(4) + 25(-3) = 5$

III. $20(9) + 25(-7) = 5$

IV. $20(14) + 25(-11) = 5$

V. $20(19) + 25(-15) = 5$

□

Problema 2

Si $a|b$ y $b \neq 0$ definimos $b/a \in \mathbb{Z}$ como aquel entero tal que $a(b/a) = b$

I. Encuentra b/a para los siguientes pares $a|b$: $1|23$, $7|14$, $1|81$, $2|4$, $3|162$, que debe ocurrir para que $2n|4m$

II. Demuestra que: $\forall a, b, c \in \mathbb{Z} \left(b \neq 0 \wedge c|a \wedge c|b \implies \text{mcd}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\text{mcd}(a,b)}{c} \right)$, tomando en cuenta que $K_1 = \frac{a}{c}$, $K_2 = \frac{b}{c}$

Demostración.

i) $\frac{23}{1} = 23$, $\frac{14}{7} = 2$, $\frac{4}{2} = 2$, $\frac{162}{3} = 54$

Si $2n|4m$, entonces existe $r \in \mathbb{Z}$ tal que $4m = (2n)r$, luego $2(2m) = 2(nr)$, como \mathbb{Z} es dominio entero $2m = nr$, por tanto $n|2m$ y tenemos que $\frac{4m}{2n} = \frac{2m}{n}$

ii) Como $K_1c = a$ y $K_2c = b$, entonces:

$$c(K_1, K_2) = (K_1c, K_2c) = (a, b)$$

Luego como $c|a$ y $c|b$ entonces $c|(a, b)$, por tanto $(a, b) = c \frac{(a,b)}{c}$, luego como \mathbb{Z} es dominio entero

$$c(K_1, k_2) = c \frac{(a, b)}{c} \implies (K_1, K_2) = \frac{(a, b)}{c}$$

□

Problema 3

Para $n \in \mathbb{Z}$ definimos $M(n) := \{k \in \mathbb{Z} \mid n|k\}$

- I. Encuentra $M(6) \cap M(10)$
- II. Encuentra el mínimo entero positivo en $M(6) \cap M(10)$
- III. Haz lo mismo para 20 y 25
- IV. Es verdad que $\text{mcd}(20, 5)\text{mcm}(20, 5) = 20(5)$

Demostración.

i) Tenemos que:

$$M(6) \cap M(10) = \{l = 2(3)(5)(q) \mid q \in \mathbb{Z}\}$$

Ya que la factorización prima de $6 = 2(3)$ y $10 = 5(2)$, por tanto cada uno de sus múltiplos debe contener los factores primos 2, 3, 5

ii) tenemos que el mínimo entero positivo posible del conjunto es el caso $q = 1$, es decir 30

iii) De nuevo $25 = (5)(5)$ y $20 = (2)(2)(5)$, por tanto aplicando el mismo argumento

$$M(25) \cup M(20) = \{l = (5^2)(2^2)q \mid q \in \mathbb{Z}\}$$

De nuevo el mínimo entero positivo del conjunto es $25(4) = 100$

iv) Si $(20, 25)[20, 25] = 5(100) = 500 = 20(25)$

□

Problema 4

Demuestra que $\forall a, b \in \mathbb{Z}$

I. $1|a$ y $-1|a$

II. $a|a$

III. $a|b \implies (-a|b \wedge a|(-b) \wedge (-a)|(-b))$

IV. $a|b \wedge b|a \implies a = b \vee a = -b$

Demostración.

i) Como 1 es unidad en \mathbb{Z} , sea $a \in \mathbb{Z}$ se cumple que $a(1) = a$ por tanto $1|a$, luego por propiedades del producto en \mathbb{Z} $a = (-1)(-a)$, por tanto $-1|a$

ii) Sea $a \in \mathbb{Z}$ de lo anterior se tiene que $a = (1)a$, por tanto $a|a$

iii) Sean $a, b \in \mathbb{Z}$ tal que $a|b$, entonces se tiene que existe $r \in \mathbb{Z}$ tal que $b = ra$, por propiedades del producto en \mathbb{Z} se tiene que $b = (-r)(-a)$, $-b = (-r)a$, $-b = (r)(-a)$, por tanto $-a|b \wedge a|(-b) \wedge (-a)|(-b)$

iv) Sean $a, b \in \mathbb{Z}$ tal que $a|b \wedge b|a$, existen $r, s \in \mathbb{Z}$ tal que $b = ra$ y $a = bs$, luego tenemos que $b(1) = bs(r)$, aplicando la ley de cancelación $1 = sr$, es decir s y r necesariamente son unidades en \mathbb{Z} de esto se sigue que $a = b$ ó $a = -b$ \square

Problema 5

Di si los siguientes enunciados son verdaderos o falsos. justifica tu respuesta

I. $6|42$

II. $4|50$

III. $0|15$

Demostración.

i) Tenemos que $42 = 7(6)$, por tanto $\exists m \in \mathbb{Z}$ tal que $42 = 6m$, es decir $6|42$

ii) Tenemos que $50 = 12(4) + 2$, como $2 < 4$, es imposible encontrar un $m \in \mathbb{Z}$ tal que $50 = 4m$, por tanto 4 no divide a 50

iii) Como $0 = 15(0)$, por tanto $\exists m \in \mathbb{Z}$ tal que $0 = 15m$, es decir $0|15$ \square

Problema 6

Demuestra lo siguiente:

- I. $\forall a, b \in \mathbb{Z} (mcd(a, b) | mcm[a, b])$
- II. $\forall a, b \in \mathbb{Z} (mcd(a, b) = mcm[a, b] \implies a = b)$
- III. $\forall a, b \in \mathbb{Z} (mcd(a, b) = 1 \iff mcd(a + b, ab) = 1)$

Demostración.

- i) Sean $a, b \in \mathbb{Z}$, tenemos que como $(a, b) | a$ y $(a, b) | b$, además que $a | [a, b]$ y $b | [a, b]$, entonces $(a, b) | [a, b]$
- ii) Sean $a, b \in \mathbb{Z}$, tenemos que $[a, b] = (a, b) | a$ y $a | [a, b]$, por tanto $[a, b] = (a, b) = a$, de la misma manera $[a, b] = (a, b) | b$ y $b | [a, b]$ por tanto $a = [a, b] = (a, b) = b$
- iii) \Leftarrow) Sean $a, b \in \mathbb{Z}$ tales que $(a + b, ab) = 1$, tenemos que $\exists r, s \in \mathbb{Z}$ tal que:

$$a(s + tb) + b(s) = s(a + b) + t(ab) = 1$$

Como 1 se puede escribir como combinación lineal de a y b entonces $(a, b) = 1$

\Rightarrow) Sean $a, b \in \mathbb{Z}$ tales que $(a, b) = 1$, entonces existen $s, t \in \mathbb{Z}$ tales que:

$$as + tb = 1 \implies (as + tb)^2 = 1^2 \implies a^2s^2 + 2(abst) + b^2t^2 = 1$$

luego sea $abs^2 + abt^2 - abs^2 - abt^2 = 0$, tenemos que:

$$a^2s^2 + abs^2 + b^2t^2 + abt^2 + 2(abst) - abs^2 - abt^2 = (a^2s^2 + b^2t^2)(a + b) + ab(2st - s^2 - t^2) = 1$$

Por tanto 1 se puede ver como combinación lineal de ab y $a + b$, es decir $(ab, a + b) = 1$

□

Problema 7

Encuentra el máximo común divisor de 1984 y 34131 y expresalo como combinación lineal de 1984 y 34131

Demostración.

Aplicamos el algoritmo de Euclides para encontrar $(1984, 34131)$:

$$\text{I. } 34131 = 17(1984) + 403$$

$$\text{II. } 1984 = 4(403) + 372$$

$$\text{III. } 403 = 1(372) + 31$$

$$\text{IV. } 372 = 31(12)$$

Por tanto $(34131, 1984) = 31$, luego procedemos a escribirlo como combinación lineal de 34131 y 1984

$$\text{I. } 31 = 403 - 372$$

$$\text{II. } 31 = 403 - (1984 - 4(403))$$

$$\text{III. } 31 = 5(403) - 1984$$

$$\text{IV. } 31 = 5(34131 - 17(1984)) - 1984$$

$$\text{V. } 31 = 5(34131) - (86)(1984)$$

□

Problema 8

Encuentra todas las soluciones enteras de la ecuación $20x + 72y = 56$

Demostración.

Sabemos que la ecuación tiene soluciones si y solo si $(20, 72) | 56$, porcedemos a obtener $(20, 72)$ por el algoritmo de Euclides

$$\text{I. } 72 = (20)3 + 12$$

$$\text{II. } 20 = 12(1) + 8$$

$$\text{III. } 12 = 8(1) + 4$$

$$\text{IV. } 8 = 4(2)$$

Por tanto $(20, 72) = 4$, como $4|56$, tenemos que la ecuación tiene una infinidad de soluciones de la forma:

$$\begin{cases} x = x_0 + \frac{72}{(20,72)} t \\ y = y_0 - \frac{20}{(20,72)} t \end{cases}$$

Donde $t \in \mathbb{Z}$, y x_0, y_0 son soluciones particulares de la ecuación, encontramos una solución particular expresando a $(20, 72)$ como combinación lineal de 20 y 72

I. $4 = 12 - 8$

II. $4 = (20 - 8) - (20 - 12)$

III. $4 = (20 - (20 - 12)) - (20 - 12)$

IV. $4 = 2(12) - 20$

V. $4 = 2(72 - 3(20)) - 20$

VI. $4 = 2(72) - 7(20)$

Como $56 = 14(4)$, entonces tenemos que:

$$56 = 14(4) = 14(2)(72) - 14(7)(20)$$

Por tanto $x_0 = -14(7)$ y $y_0 = 14(2)$ son soluciones particulares de esta ecuación, por tanto las soluciones de la ecuación pueden ser escritas como:

$$\begin{cases} x = -14(7) + 18t \\ y = 14(2) - 5t \end{cases}$$

Con $t \in \mathbb{Z}$

□

Problema 9

Demuestra que $\forall a, b, c \in \mathbb{Z} (mcm[ca, cb] = |c|mcm[a, b])$

Demostración.

Sean $a, b, c \in \mathbb{Z}$ tenemos que se cumple que $(ca, cb)[ca, cb] = c^2|ab|$, a su vez tenemos que $|ab| = (a, b)[a, b]$, por tanto $(ca, cb)[ca, cb] = c^2(a, b)[a, b] = |c|[a, b](|c|(a, b))$, luego como $(ca, cb) = |c|(a, b)$, por tanto $|c|(a, b)[ca, cb] = |c|[a, b](|c|(a, b))$, como \mathbb{Z} es dominio entero tenemos que $[ca, cb] = |c|[a, b]$

□

Problema 10

Demuestra que no existe un número racional tal que $r^2 = 2$

Demostración.

Procedemos por contradicción es decir $\exists a, b \in \mathbb{Z}$, con $(a, b) = 1$, tales que:

$$\sqrt{2} = \frac{a}{b} \implies 2 = \frac{a^2}{b^2} \implies 2b^2 = a^2$$

Como $(b, a) = 1$ entonces $(b^2, a^2) = 1$, luego tenemos que:

$$1 = (a^2, b^2) = (2b^2, b^2) = b^2(2, 1) = b^2$$

por tanto $b^2 \in \mathbb{Z}$ es unidad, luego tendríamos que necesariamente $2 = a^2$, una contradicción pues 2 no es un cuadrado perfecto

□

Problema 11

Demuestra que si $n \in \mathbb{N}$ no es un cuadrado perfecto, entonces \sqrt{n} es irracional

Demostración.

Procedemos por contradicción es decir $\exists m, n \in \mathbb{Z}$, con $(m, n) = 1$, tales que:

$$\sqrt{n} = \frac{a}{b} \implies n = \frac{a^2}{b^2} \implies b^2 n = a^2$$

Como $(b, a) = 1$ entonces $(b^2, a^2) = 1$, luego tenemos que:

$$1 = (a^2, b^2) = (b^2 n, b^2) = b^2(n, 1) = b^2$$

por tanto $b^2 \in \mathbb{Z}$ es unidad, luego tendríamos que necesariamente $n = a^2$ una contradicción ya que por hipótesis este no es un cuadrado perfecto, como nuestra única suposición fue que \sqrt{n} era racional concluimos que \sqrt{n} es irracional \square

Problema 12

Demuestra que $\sqrt{3} + \sqrt{2}$ es irracional

Demostración.

Procedemos por contradicción es decir existen $q \in \mathbb{Q}$, tales que:

$$\sqrt{3} + \sqrt{2} = q \implies 3 + 2\sqrt{6} + 2 = q^2 \implies \sqrt{6} = \frac{q^2 - 5}{2} \in \mathbb{Q}$$

Una contradicción ya que 6 no es un cuadrado perfecto por tanto $\sqrt{6}$ es irracional, como nuestra única suposición fue que $\sqrt{3} + \sqrt{2} \in \mathbb{Q}$ se tiene que necesariamente este es irracional \square

Problema 13

Sean $a, b, c, d \in \mathbb{Z}$ y $m, n \in \mathbb{Z}^+$. demuestre que:

- I. $a \cong b \pmod{m}$ si y solo si $a + c \cong b + c \pmod{m}$
- II. Si $a \cong b \pmod{m}$ y $c \cong d \pmod{m}$, entonces $ax + cy \cong bx + dy \pmod{m}$
- III. Si $a \cong b \pmod{m}$, entonces $\text{mcd}(a, m) = \text{mcd}(b, m)$

Demostración.

i) \Rightarrow) Sean $a, b \in \mathbb{Z}$ tales que $a \cong b \pmod{m}$, entonces $m|a - b$, luego tenemos que sea $c \in \mathbb{Z}$ $a - b = a + c - b - c = a + c - (b + c)$, por tanto $m|a + c - (b + c)$, se sigue que $a + c \cong b + c \pmod{m}$

\Leftarrow) Luego si tomamos $a, b \in \mathbb{Z}$ tales que $a + c \cong b + c \pmod{m}$ entonces $m|(a + c) - (b + c)$, por el argumento antes dado $m|a - b$ es decir $a \cong b \pmod{m}$

ii) Sean $a, b, c, d \in \mathbb{Z}$ tales que $a \cong b \pmod{m}$ y $c \cong d \pmod{m}$ tenemos que $m|a - b$ y $m|c - d$, luego sean $x, y \in \mathbb{Z}$ se sigue que $m|x(a - b)$ y $m|y(c - d)$, luego $m|x(a - b) + y(c - d)$, luego tenemos que $x(a - b) + y(c - d) = ax + cy - (bx + dy)$ por tanto $m|ax + cy - (bx + dy)$, por tanto $ax + cy \cong bx + dy \pmod{m}$

iv) Sean $a, b \in \mathbb{Z}$ tal que $a \cong b \pmod{m}$, entonces tenemos que $m|b - a$ por tanto existe $s \in \mathbb{Z}$ tal que $a - b = ms$ por tanto tenemos que $a = ms + b$ como por hipótesis $m \neq 0$ por tanto aplicando el lema usado en el algoritmo de Euclides, tenemos que $(a, m) = (b, m)$

□

Problema 14

Diga si los siguientes enunciados son verdaderos o falsos justifique su respuesta

- I. $7 \cong 5 \pmod{2}$
- II. $8 \cong 12 \pmod{3}$
- III. $50 \cong 208 \pmod{4}$
- IV. $5 \cong -5 \pmod{5}$

Demostración.

1) Tenemos que $2|7 - 5 = 2$ por tanto $7 \cong 5 \pmod{2}$

ii) Esto no es cierto ya que 3 no divide a $8 - 12 = -4$

iii) Tenemos que 4 no divide a $50 - 208 = -158$, por tanto el enunciado es falso

iv) Claramente $5| -5$ y $5|5$ por tanto $5|5 - (-5)$ es decir $5 \cong -5 \pmod{5}$

□