

Álgebra relación 3

- ① Sea D un DFU y $a, b \in D$. Demostrar que si $ab \neq 0$ y $d \in D$, es divisor de ab coprimo con a , entonces d divide a, b .

a y d son coprimos $\Rightarrow \text{mcd}(a, d) = 1$ \Rightarrow

\downarrow Porque
como D es DFU

$$\Rightarrow \text{mcd}(ab, db) = b$$

$$ab \neq 0$$

$$\left. \begin{array}{l} d \mid ab \\ d \mid db \end{array} \right\} \Rightarrow d \mid \text{mcd}(ab, db) = b \Rightarrow \boxed{d \mid b}$$

- ② comprobar que los elementos $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$ en $\mathbb{Z}[\sqrt{10}]$ son irreducibles y deducir que $\mathbb{Z}[\sqrt{10}]$ no es un DFU.

$$2 \mid 12 \mid 121 \mid 121 = 4 \times 30 \in \mathbb{Z}[\sqrt{10}]$$

Supongamos que 2 es reducible:

descomponer en factores primos \Rightarrow $2 = d\beta$

$$2 = d\beta \text{ factorización propia}$$

\Downarrow

$$d \mid 2 \Rightarrow |d| \mid 121 = 4 \Rightarrow |d| \mid 4$$

$$|d| = \begin{cases} \pm 1 & \rightarrow |d| = \pm 1 \Rightarrow d \text{ es una unidad} \Rightarrow \text{No vale} \\ \pm 2 & \rightarrow (*) \\ \pm 4 & \rightarrow |d| = \pm 4 \Rightarrow |\beta| = \pm 1 \Rightarrow \beta \text{ unidad} \Rightarrow \text{No vale} \end{cases}$$

(*)

$$|z| = \pm 2$$

$$a^2 - 10b^2 = \pm 2$$

No podemos acotar b, pero si hacerlo mod 10

$$a^2 \equiv \pm 2 \pmod{10}$$

d es ± 2 un cuadrado mod 10?

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

cuadrados

$$\{0, 1, 4, 6, 9, 5, 6, 9, 4, 1\}$$

$$\begin{aligned} 2 \pmod{10} &= 2 \\ -2 \pmod{10} &= 8 \end{aligned} \quad \left\{ \notin \right. \quad \uparrow$$

Luego no tiene solución $\Rightarrow |z|$ es irreducible

Repetimos el proceso con $|z| = 3$: se aplica el mismo

sabemos que es reducible \Rightarrow Tiene factorización propia:

$$z = \alpha \beta \Rightarrow |\alpha| |\beta| \Rightarrow |\alpha| |9$$

$$|\alpha| = \begin{cases} \pm 1 & \Rightarrow \alpha \text{ unidad} \Rightarrow \text{No vale} \\ \pm 3 & \Rightarrow |\beta| = \pm 1 \Rightarrow \beta \text{ unidad} \Rightarrow \text{No vale} \\ \pm 9 & \Rightarrow a^2 - 10b^2 = \pm 3 \end{cases}$$

Lo hacemos módulo 10

$$a^2 \equiv \pm 3 \pmod{10} \Rightarrow \text{Si}$$

d es ± 3 un cuadrado mod 10?

$$\begin{aligned} z \pmod{10} &= 3 \\ -z \pmod{10} &= 7 \end{aligned} \quad \left\{ \begin{array}{l} \text{osando en la tabla A de arriba vemos} \\ 3 \rightarrow 9 \\ 7 \rightarrow 1 \end{array} \right\} \Rightarrow \text{No vale}$$

que no $\Rightarrow |z|$ es irreducible

Repetimos con $4 + \sqrt{10}$:

Suponemos que $4 + \sqrt{10}$ es reducible \Rightarrow tiene factorizaciones propias:

$$4 + \sqrt{10} = \alpha\beta \Rightarrow \alpha | 4 + \sqrt{10} \Rightarrow |\alpha| | |4 + \sqrt{10}| \Rightarrow |\alpha| | 26$$

$$|\alpha| = \begin{cases} \pm 1 & \Rightarrow \alpha \text{ unidad} \Rightarrow \text{No vale} \\ \pm 2 & \pm 13 \\ \pm 26 & \Rightarrow \beta \text{ unidad} \Rightarrow \text{No vale} \end{cases}$$

$$\begin{array}{c|cc} 26 & 13 & a^2 - 10b^2 = \pm 2 \\ 2 & 2 & a^2 - 10b^2 = \pm 13 \\ 1 & & \text{m\'odulo } 10 \end{array}$$

$a^2 = \pm 2 \pmod{10}$ $a^2 = \pm 13 \pmod{10}$

↓
Ya hemos visto
que no tiene
soluci\'on

$a^2 = 3 \pmod{10}$
 $a^2 = 7 \pmod{10}$

↓
No tiene soluci\'on

$\Rightarrow 4 + \sqrt{10}$ es irreducible

Con $4 - \sqrt{10}$, al ser el conjugado de $4 + \sqrt{10}$ para lo mismo

Para probar que $\mathbb{Z}[\sqrt{10}]$ no es OFU, buscamos un elemento con 2 factorizaciones propias, por ejemplo:

$$6 = 2 \cdot 3$$

$$6 = (4 - \sqrt{10})(4 + \sqrt{10})$$

③ Decidir razonadamente si existen isomorfismos de anillos:

$$\frac{\mathbb{Z}[C]}{\langle 1+i \rangle} \cong \mathbb{Z}_2 \quad \text{y} \quad \frac{\mathbb{Z}[C]}{\langle i \rangle} \cong \mathbb{Z}_2$$

Para que sean isomorfos, debe existir un morfismo de $\frac{\mathbb{Z}[C]}{\langle 1+i \rangle} \rightarrow \mathbb{Z}_2$

$$f: \frac{\mathbb{Z}[C]}{\langle 1+i \rangle} \rightarrow \mathbb{Z}_2$$

$$f^{-1}: \mathbb{Z}_2 \rightarrow \frac{\mathbb{Z}[C]}{\langle 1+i \rangle}$$

Los elementos de $\frac{\mathbb{Z}[C]}{\langle 1+i \rangle}$ son de la forma $a+bi$, al hacerlos módulo $1+i$, obtenemos que los elementos de $\frac{\mathbb{Z}[C]}{\langle 1+i \rangle}$ son:

Obtener el resto de dividir por $1+i$

$$\frac{\mathbb{Z}[C]}{\langle 1+i \rangle} = \{ 0, i \} \quad \mathbb{Z}_2 = \{ 0, 1 \}$$

$$\begin{aligned} [0] &\xrightarrow{f} 0 & [0] &\xrightarrow{f^{-1}} 0 \\ [i] &\xrightarrow{f} 1 & [1] &\xrightarrow{f^{-1}} i \end{aligned}$$

Por tanto, se verifica $\frac{\mathbb{Z}[C]}{\langle 1+i \rangle} \cong \mathbb{Z}_2$

Repetimos el proceso con $\frac{\mathbb{Z}[C]}{\langle i \rangle} \cong \mathbb{Z}$

Los elementos de $\frac{\mathbb{Z}[C]}{\langle i \rangle}$ son de la forma $a+bi$. Al hacerlos módulo i , obtenemos:

$$\frac{\mathbb{Z}[C]}{\langle i \rangle} = \{ 0 \} \Rightarrow \text{No existe morfismo}$$

④ Calcular el mod de:

$$\bullet \quad a = -99 \quad y \quad b = 17$$

1) Dividimos el mayor entre el menor

$$\begin{array}{r} -99 \quad 17 \\ \underline{-6} \quad \quad 3 \\ 3 \quad 5 \end{array} \quad \begin{array}{r} 17 \quad 13 \\ \underline{13} \quad \quad 4 \\ 1 \quad 1 \end{array} \quad \begin{array}{r} 3 \quad 12 \\ \underline{12} \quad \quad 0 \\ 1 \quad 1 \end{array} \quad \begin{array}{r} 2 \quad 1 \\ \underline{0} \quad \quad 2 \\ 2 \end{array}$$

El mod es el ultimo resto no nulo $\Rightarrow \text{mod}(-99, 17) = 1$

2) Coeficientes de Bezout

	u	v
-99	1	0
17	0	1
-6	1	6
5	-5	-3
1	6	37

$$\Rightarrow 1 = (-99)6 + 17(37) \quad \checkmark$$

$$\bullet \quad a = 6643, \quad b = 2873$$

1) Dividimos

$$6643 \quad | \quad 2873 \\ \underline{897} \quad \quad 2$$

$$2873 \quad | \quad 897 \\ \underline{182} \quad \quad 3$$

$$897 \quad | \quad 182 \\ \underline{189} \quad \quad 4$$

$$182 \quad | \quad 169$$

$$169 \quad | \quad 13 \\ \underline{13} \quad \quad 0$$

$$189 \quad | \quad 13 \\ \underline{13} \quad \quad 0$$

$$\Rightarrow \boxed{\text{mod}(6643, 2873) = 13}$$

2) Coeficientes de Bezout

	u	v
6643	0	0
2873	0	1
2	897	1
3	182	-3
4	169	13
1	13	-16

$$\Rightarrow 13 = 6643(-16) + 2873(37) \quad \checkmark$$

• $a = -7655$, $b = 1001$

1) Dividimos

$$\begin{array}{r} -7655 \\ \underline{-363} \\ 1001 \end{array}$$

$$\begin{array}{r} 1001 \\ \underline{-805} \\ 205 \end{array}$$

$$\begin{array}{r} 1001 \\ \underline{-805} \\ 205 \end{array}$$

$$\begin{array}{r} 1001 \\ \underline{-805} \\ 205 \end{array}$$

$$\begin{array}{r} 295 \\ \underline{5} \\ 168 \end{array}$$

$$\begin{array}{r} 58 \\ \underline{3} \\ 15 \end{array}$$

$$\begin{array}{r} 5 \\ \underline{2} \\ 12 \end{array}$$

$$\begin{array}{r} 21\frac{1}{2} \\ 0 \\ \hline \end{array}$$

$$\Rightarrow \boxed{\text{mod}(-7655, 1001) = 1}$$

2) Coeficientes de Bézout

-7655	u	v
1001	1	0
-8	297	1
2	295	-2
1	58	3
5	5	-13
11	3	190
1	2	-207
1	1	3086

$$\Rightarrow 1 = (-7655) \cdot 297 + (1001) \cdot 3086$$

$$\boxed{d = (8655, 1001)}$$

Resumen de estimación 68

7655	1001	3086
0	0	0
1	0	0
2	1	1
5	0	1
11	0	0
1	1	0
1	0	1

$$a = 24280, \quad b = 886$$

2) Dividimos

$$\begin{array}{r} 24286 \\ \underline{-204} \\ 41 \\ \underline{-178} \\ 13 \end{array}$$

$$\begin{array}{r} 178 \quad 126 \\ \underline{-22} \quad 6 \\ \hline \end{array} \quad \begin{array}{r} 26 \quad 122 \\ \underline{-4} \quad 1 \\ \hline \end{array} \quad \begin{array}{r} 22 \quad 14 \\ \underline{-2} \quad 5 \\ \hline \end{array} \quad \begin{array}{r} 4 \quad 12 \\ \underline{-0} \quad 2 \\ \hline \end{array}$$

$$\Rightarrow \boxed{\text{mod}(24220, 586) = 2}$$

2) Usamos coeficientes de Berout

		<u>u v</u>
24230	20	
586	01	
44	204	1 -41
2	178	-2 83
1	26	3 -124
6	22	-20 827
1	4	23 -951
5	2	-135 5582 =>

$$\Rightarrow z = 24280(-135) + 586(56821) \quad \checkmark$$

$$0.7(25000) + 30000 = 50000$$

$$\left\{ \begin{array}{l} 300+0000 = 2 \cdot \frac{24}{5} + 0000 = 0 \\ 300+0000 = 2 \cdot \frac{24}{5} + 0000 = 0 \end{array} \right.$$

- ⑤ Se disponen de 4050 euros para gastar en bolígrafos de 10 euros y en plumas de 46 euros. Calcular cuántos bolígrafos y plumas se pueden comprar si se quiere el menor número de bolígrafos.

1) Plantear la ecuación

$$4050 = a \cdot 10 + b \cdot 46$$

2) MCD

$$\text{mcd}(10, 46) = \text{mcd}(46, 20) = 2$$

$$\begin{array}{r} 46 \\ \underline{-} 4 \\ 6 \end{array} \quad \begin{array}{r} 10 \\ \underline{-} 4 \\ 6 \end{array} \quad \begin{array}{r} 16 \\ \underline{-} 10 \\ 6 \end{array} \quad \begin{array}{r} 14 \\ \underline{-} 10 \\ 4 \end{array} \quad \begin{array}{r} 12 \\ \underline{-} 10 \\ 2 \end{array}$$

3) Coeficientes de Bézout

	u	v			
46	1	0			
10	0	1			
4	1	-4			
1	4	-15			
1	2	-9			
			$2 = (2)46 + (-1)10$	\checkmark	
			$4 = (2)46 + (-1)10$	\checkmark	
			$6 = (2)46 + (-1)10$	\checkmark	

4) Multiplicar por:

$$\begin{array}{r} 4050 \\ \underline{-} 2025 \\ 0 \end{array} \times \left(\begin{array}{r} 2 \\ -1 \end{array} \right) = \begin{array}{r} 2 = (2)46 + (-1)10 \\ 4 = (2)46 + (-1)10 \\ 6 = (2)46 + (-1)10 \end{array}$$

5) ecuación general

$$\begin{aligned} a &= 4050 - \frac{10}{2}t = 4050 - 5t \\ b &= -18225 + \frac{46}{2}t = -18225 + 23t \end{aligned} \quad \left. \begin{array}{l} \\ \end{array} \right\}$$

6) solución particular

$$t = 393 \Rightarrow \begin{cases} a = 14 \\ b = 35 \end{cases}$$

② Calcular en $\mathbb{K}[\sqrt{-2}]$ el mcd y mmc de 3 y $2+\sqrt{-2}$.

$$\mathbb{K}[\sqrt{-2}] = a + b\sqrt{-2}$$

$$\text{mod } (3, 2+\sqrt{-2})$$

1) Módulo

$$|3| = 3$$

$$|2+\sqrt{-2}| = \sqrt{2^2 + (-2)^2} = \sqrt{8} = 2\sqrt{2}$$

2) Dividimos

$$\begin{array}{r} 3 \mid 2+\sqrt{-2} \\ - 2+\sqrt{-2} + (2-\sqrt{-2})c \\ \hline 1-\sqrt{-2} + (2-\sqrt{-2})c \end{array}$$

$$\frac{3}{2+\sqrt{-2}} = \frac{3(2-\sqrt{-2})}{(2+\sqrt{-2})(2-\sqrt{-2})} = \frac{6-3\sqrt{-2}}{6} = 1 - \frac{\sqrt{-2}}{2}c \approx 1 - c$$

$$\begin{array}{r} 2+\sqrt{-2} \quad | 1-\sqrt{-2} + (2-\sqrt{-2})c \\ - 2-\sqrt{-2}c \quad (-2-\sqrt{-2})c \\ \hline 0 \end{array}$$

$$\frac{2+\sqrt{-2}}{1-\sqrt{-2} + (2-\sqrt{-2})c} = -(2+\sqrt{-2})c$$

$$\boxed{\text{Luego } \text{mcd}(3, 2+\sqrt{-2}) = 1-\sqrt{-2} + (2-\sqrt{-2})c}$$

3) Coeficientes de Bézout

$$\begin{array}{c|cc|cc|c} & u & v & & & \\ \hline 3 & 1 & 0 & & & \\ 2+\sqrt{-2} & 0 & 1 & & & \\ \hline 1-\sqrt{-2} & 1-\sqrt{-2} & 1 & -1+\sqrt{-2} & & \\ & 1-\sqrt{-2} & 1 & -1+\sqrt{-2} & & \\ & & 1 & -1+\sqrt{-2} & & \\ & & 1 & -1+\sqrt{-2} & & \\ & & & & & \end{array}$$

$$1-\sqrt{-2} + (2-\sqrt{-2})\zeta = 3 + (2+\sqrt{-2})(-1+\zeta) \quad \checkmark$$

$$(1) \text{ calculamos el mcm } (3, 2+\sqrt{-2}) = \frac{3(2+\sqrt{-2})}{\text{mcd}(3, 2+\sqrt{-2})} =$$

$$= \frac{6+(3\sqrt{-2})\zeta}{1-(2-\sqrt{-2})\zeta} = \frac{1-(6+3\sqrt{-2})\zeta}{1-(2-\sqrt{-2})\zeta} = 3+2\zeta$$

(8) Da la solución, si existe, de la ecuación diferencial en $\mathbb{Z}[\zeta]$:

$$4x + (3+3\zeta)y = -1+5\zeta \quad (1)$$

Encontrar la solución de módulo y mayor que 12321.

$$\text{1) (3, MCD)} (3+3\zeta)(1-\zeta) = \frac{3+3\zeta}{3-\zeta} \cdot (1-\zeta) = x$$

$$|4| = 16$$

$$|3+3\zeta| = 18$$

$$\text{mcd}(3+3\zeta, 4) = -1-\zeta$$

$$= 1+3\zeta = 3(8+2\zeta)^{-1} = y$$

$$\begin{array}{r} 3+3\zeta \\ -4-4\zeta \\ \hline -1-\zeta \end{array}$$

$$\begin{array}{r} 4 \\ 0 \\ \hline 1-\zeta \end{array}$$

$$\frac{3+3\zeta}{4} = \frac{3}{4} + \frac{3}{4}\zeta \sim 1+\zeta$$

$$\frac{4}{-1-\zeta} = -2+2\zeta$$

2) Coeficientes de Berout

$$\left| \begin{array}{c|ccccc} & u & v & w & & \\ \hline 3+3i & 1 & 0 & 0 & 8 & 5 \\ 4 & 0 & 1 & 0 & 0 & -5+2i \\ \hline 1+i & -1-i & 1 & -1-i & 1+2i & 0 \\ \end{array} \right|$$

$$(3+3i)(1) + (-1-i)4 = -1-i \quad \checkmark$$

3) Multiplicación (a continuación):

$$\frac{-1+5i}{-1-i} = -2-3i$$

$$(-1+5i)(1) + (-1-i)(-2-3i) + 3(-1)$$

$$-1+5i = (3+3i)(1) + (-1-i)(-2-3i) + 3(-1)$$

$$\times -2-3i$$

$$-1+5i = (3+3i)(-2-3i) + (-1-i)(-2-3i) \quad \text{ok}$$

4) Solución general:

$$y = (-2-3i) + t \frac{3+3i}{-1-i} = (-2-3i) - 3t$$

$$x = (-1+5i) + t \frac{4}{-1-i} = (-1+5i) + t(-2+2i)$$

5) Solución particular:

$$t=50$$

$$y = -152-3i \Rightarrow |y| =$$

$$\sqrt{(-152)^2 + (-3)^2} = \sqrt{23105} = 152\sqrt{10}$$

$$\sqrt{(-152)^2 + (-3)^2} = \sqrt{23105} = \sqrt{15^2 \cdot 10} = 15\sqrt{10}$$

⑨ Calcular el resto de dividir 279^{323} entre 17.

$$a^n \bmod b$$

1) $\text{mcd}(a, b)$

$$\text{mcd}(279, 17) = 1 \quad \checkmark$$

$$\begin{array}{r} 279 \\ \overline{17} \\ 3 \end{array} \quad \begin{array}{r} 17 \\ \overline{17} \\ 0 \end{array} \quad \begin{array}{r} 7 \\ \overline{1} \\ 2 \end{array}$$

$$279 \equiv 1 \pmod{17}$$

2) Usamos ϕ de Euler

$$279^{\phi(17)} \equiv 1 \pmod{17}$$

$$\phi(17) = 16$$

$$\text{Luego, } 279^{16} \equiv 1 \pmod{17}$$

$$279^{16} \equiv 1 \pmod{17}$$

3) Expresamos 279^{323} como:

$$323 \mid 16$$

$$3 \mid 20$$

$$279^{323} = 279^{16 \cdot 20 + 3} = (279^{16})^{20} \cdot 279^3$$

Luego:

$$(279^{16})^{20} \cdot 279^3 \pmod{17} \equiv 1^{20} \cdot 279^3 \pmod{17}$$

\downarrow

$$279^3 \mid 17$$

$$3 \mid 9$$

4) Hacemos la división

$$\boxed{r=3}$$

Calcular el resto de dividir 320^{207} entre 13

$$a^n \bmod b$$

1) $\text{mod}(a, b)$

$$\text{mod}(320, 13) = \pm \sqrt{320} \bmod 13$$

$$\begin{array}{r} 320 \\ \hline 8 \end{array} \quad \begin{array}{r} 13 \\ \hline 5 \end{array} \quad \begin{array}{r} 8 \\ \hline 3 \end{array} \quad \begin{array}{r} 5 \\ \hline 2 \end{array}$$

$$\begin{array}{r} 3 \\ \hline 1 \end{array}$$

2) Φ de Euler

$$\Phi(13) = 12$$

$$\text{Luego, } 320^{\Phi(13)} \bmod 13 = 320^{12} \equiv 1 \bmod 13$$

3) Expresamos 320^{207} como:

$$\begin{array}{r} 207 \\ \hline 3 \end{array} \quad \begin{array}{r} 12 \\ \hline 17 \end{array}$$

$$320^{207} = 320^{17 \cdot 12 + 3} = 320^{17 \cdot 12} \cdot 320^3$$

4) calculando

$$320^{17 \cdot 12} \cdot 320^3 \bmod 13 = (320^{12})^{17} \cdot 320^3 \bmod 13$$

Luego

$$\begin{array}{r} 320^3 \\ \hline 5 \end{array} \quad \begin{array}{r} 13 \\ \hline 9 \end{array} \quad \boxed{r=5}$$

- ⑩ El valor de x ha sido codificado usando RSA con las llaves públicas n y b y hemos obtenido el valor y . calcular el valor de x en cada caso:

$$\bullet \quad n = 5103, \quad b = 125, \quad y = 3835$$

1) Factorizamos n

$$\begin{array}{c|c} 5103 & 3 \\ \hline 1701 & 3 \\ & 3 \\ 567 & 3 \\ & 3 \\ 189 & 3 \\ & 3 \\ 63 & 3 \\ & 3 \\ 21 & 3 \\ & 7 \\ & 1 \end{array} \quad \text{5103 es divisible por } 3^6 \cdot 7$$

a continuación (2)

$$\begin{array}{c|c} 2 & 3216 \\ \hline 1608 & 1608 \\ 804 & 804 \\ 402 & 402 \\ 201 & 201 \\ 100 & 100 \\ 50 & 50 \\ 25 & 25 \\ 12 & 12 \\ 6 & 6 \\ 3 & 3 \\ 1 & 1 \end{array}$$

2) ϕ de Euler de n

$$\begin{aligned} \phi(5103) &= \phi(3^6 \cdot 7) = \phi(3^6) \cdot \phi(7) = \\ &= 2 \cdot 3^5 \cdot 6 = 2916 \end{aligned}$$

3) $\text{mcd}(\phi(n), b)$

$$\begin{array}{r} 2916 \quad 125 \\ \hline 41 \quad 28 \end{array} \quad \begin{array}{r} 125 \quad 41 \\ \hline 3 \quad 1 \end{array} \quad \begin{array}{r} 41 \quad 12 \\ \hline 20 \quad 20 \end{array}$$

$$\text{Luego, } \text{mcd}(\phi(n), b) = 1$$

4) Coeficientes de Bezout

$$\begin{array}{c|cc} & 2916 & 125 \\ \hline 2916 & 1 & 0 \\ 125 & 0 & 1 \\ \hline 23 & 41 & 1 -23 \\ 3 & 2 & -3 70 \\ 20 & 1 & 61 -1423 \end{array}$$

$$x = 2916(64) + 125(-1423) \checkmark$$

ahora contamos q d es la resta de ambas soluciones

5) ecuación que acompaña a b

$$V = -1423 + \frac{2916}{1423} t \Rightarrow V_0 = \underline{\underline{1423}}$$

6) buscando x:

$$x = y^u \mod n = 3835^{1423} \mod 5203 = \boxed{55}$$

$$\bullet n = 1568, b = 125, y = 103$$

1) Factorizamos n

$$\begin{array}{c|c} 1568 & 2 \\ 784 & 2 \\ 392 & 2 \\ 196 & 2 \\ 98 & 2 \\ 49 & 7 \\ 2 & 7 \\ 1 & 2 \end{array} \quad 1568 = 2^5 \cdot 7^2 \quad \text{(d, 103)} \text{ lcm } 68$$

2) Phi de Euler de n

$$\varphi(1568) = \varphi(2^5 \cdot 7^2) = \varphi(2^5) \cdot \varphi(7^2) =$$

$$= 2^4 \cdot 7 \cdot 6 = 672$$

3) mod ($\varphi(n), b$)

$$\begin{array}{c|c} 672 & 125 \\ \hline 47 & 5 \\ \hline 1 & \end{array} \quad \begin{array}{c|c} 125 & 142 \\ \hline 31 & 2 \\ \hline 1 & \end{array} \quad \begin{array}{c|c} 47 & 131 \\ \hline 16 & 1 \\ \hline 1 & \end{array}$$

$$\begin{array}{c|c} 31 & 16 \\ \hline 15 & 1 \\ \hline 1 & \end{array} \quad \begin{array}{c|c} 16 & 15 \\ \hline 15 & 1 \\ \hline 1 & \end{array} \quad \begin{array}{c|c} 17 & 55 \\ \hline 17 & 2 \\ \hline 1 & \end{array}$$

$$\text{mod}(672, 125) = 1$$

4) Coeficientes de Bezout

		u	v
	672	1	0
	125	0	1
5	47	1	-5
2	31	-2	11
1	16	3	-16
1	15	-5	27
1	1	8	-43

$$1 = 672(8) + 125(-43) \checkmark$$

5) Solución que acompaña a b

$$V = -43 + \frac{8}{1} U = -43 + 8U \Rightarrow V_0 = 5$$

6) Solución

$$X \equiv y^r \pmod{n} \equiv 103^5 \pmod{18711} = \underline{\underline{9797}}$$

$$\bullet n = 18711, \quad b = 1231, \quad y = 103$$

1) Factorizamos n

$$18711 = 3^5 \cdot 7 \cdot 11 \cdot 23 \cdot 5 + 0 \text{ resto}$$

2) Phi de Euler de n

$$\begin{aligned} \varphi(18711) &= \varphi(3^5) \cdot \varphi(7) \cdot \varphi(11) \cdot \varphi(23) \cdot \varphi(5) \\ &= 2 \cdot 3^4 \cdot 6 \cdot 10 = 9720 \end{aligned}$$

3) NCD($\varphi(n)$, b)

$$\begin{array}{r} 9720 \ 1231 \\ \hline 1403 \ 7 \end{array} \quad \begin{array}{r} 1231 \ 1231 \\ \hline 128 \end{array} \quad \begin{array}{r} 128 \ 128 \\ \hline 1 \end{array} \quad \begin{array}{r} 1103 \ 1103 \\ \hline 79 \end{array} \quad \begin{array}{r} 1103 \ 1128 \\ \hline 68 \end{array}$$

$$\begin{array}{r} 128 \\ \underline{-49} \\ 79 \end{array}$$

$$\begin{array}{r} 79 \\ \underline{-30} \\ 49 \end{array}$$

$$\begin{array}{r} 49 \\ \underline{-19} \\ 30 \end{array}$$

$$\begin{array}{r} 30 \\ \underline{-11} \\ 19 \end{array}$$

$$\begin{array}{r} 19 \\ \underline{-8} \\ 11 \end{array}$$

$$\begin{array}{r} 13 \\ \underline{-3} \\ 10 \end{array}$$

$$\begin{array}{r} 8 \\ \underline{-3} \\ 5 \end{array}$$

$$\begin{array}{r} 8 \\ \underline{-3} \\ 5 \end{array}$$

4) Coeficientes de Berlout

	u	v
q ₇₂₀	1	0
q ₂₈₁	0	1
9	1203	1 -7
3	128	-1 8
8	79	9 -71
1	49	-10 79
1	30	19 -180
1	19	-29 229
1	11	48 -379
1	8	-77 608
1	3	125 -987
2	2	-327 2582
1	1	452 -3569

$$1 = (452)q_{720} + (-3569)q_{281}$$



✓ 2203

5) ecuación general que acompaña a la 3) anterior

$$v = -3569 + \frac{q_{720}}{1} t \Rightarrow v_0 = 6151$$

6) Bisecciones x

$$x \equiv y^r \pmod{n} \Rightarrow \frac{q_{720}}{1} \pmod{1871}$$

- (11) Resolver el siguiente sistema de congruencias, da la solución general y una que sea mayor a 12345.

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 2 \pmod{16} \\ 3x \equiv 22 \pmod{96} \end{cases}$$

Vamos asociando ecuaciones de dos en dos.

- 1) Expressamos la primera ecuación en función de t .

$$\begin{aligned} x &\equiv 7 \pmod{9} \Rightarrow x = 7 + 9t \Rightarrow 7 + 9t \equiv 2 \pmod{16} \Rightarrow \\ &\Rightarrow 9t \equiv (-5) \pmod{16} \Rightarrow \textcircled{1} t \equiv \frac{-5}{9} \pmod{\textcircled{16}_{n_2}} \end{aligned}$$

- 2) $\text{MCD}(n_1, n_2)$

$$\text{mcd}(9, 16) = \text{mcd}(16, 9) = 1$$

$$\begin{array}{r} 16 \longdiv{9} & 9 \longdiv{17} & 2 \longdiv{12} \\ \underline{-1} & \underline{-2} & \underline{-1} \\ \hline -7 & -5 & 1 \end{array}$$

- 3) Coeficientes de Bezout

n_1	n_2	u_1	v_1
16	1	1	0
9	0	0	1
1	7	1	-1
1	2	-1	2
3	1	4	-7

$$1 = 16(4) + 9(-7) \quad \checkmark$$

$$\begin{matrix} x_{11} \\ \hline \end{matrix} \quad \begin{matrix} 12 = 16(44) + 9(\underbrace{-77}_{t_0}) \end{matrix}$$

4) ecuación particular

sección de la ecuación de la recta: $t_0 = -77$ con $y = 11$

$$x_0 = a_1 + t_0 \cdot n_2$$

$$x_0 = 11 + (-77) \cdot 9 = -682$$

5) ecuación general

$$x = x_0 + k \operatorname{nm}(n_1, n_2)$$

$$x = -682 + k \frac{16 \cdot 9}{1}$$

$$x = -682 + k \cdot 144 \Rightarrow \boxed{x \equiv -682 \pmod{144}}$$

6) Repetimos el proceso

$$\begin{cases} x \equiv -682 \pmod{144} \\ 3x \equiv 22 \pmod{95} \end{cases}$$

1) Expressamos la primera ecuación en función

de t :

$$x \equiv -682 \pmod{144} \Rightarrow -682 + 144t = x \Rightarrow$$

$$\Rightarrow 3(-682 + 144t) \equiv 22 \pmod{95} \Rightarrow$$

$$\Rightarrow 432t \equiv 2068 \pmod{95} \Rightarrow 432t \equiv 78 \pmod{95}$$

2) MCD(n_1, n_2)

$$\operatorname{mcd}(432, 95) = 1$$

$$\begin{array}{r} 432 \ 1 \\ \underline{-4} \quad 4 \end{array}$$

$$\begin{array}{r} 95 \ 1 \\ \underline{-4} \quad 1 \end{array}$$

$$\begin{array}{r} 52 \ 1 \\ \underline{-4} \quad 1 \\ \quad 9 \end{array}$$

$$\begin{array}{r} 48 \ 1 \\ \underline{-4} \quad 1 \\ \quad 4 \end{array}$$

$$\begin{array}{r} 9 \ 1 \\ \underline{-3} \quad 1 \\ \quad 6 \end{array}$$

$$\begin{array}{r} 2 \ 1 \\ \underline{-1} \quad 1 \\ \quad 1 \end{array}$$

$$(432 \cdot 1 + 144 \cdot 3) \cdot 95 = 22$$

3) Coeficientes de Beaufort

	u	v
482	1	0
95	0	1
4	52	1 -4
1	43	-1 5
1	9	2 -9
4	7	-9 41
1	2	11 -50
3	1	-42 101

$$\left. \begin{array}{l} 482 \cdot 101 = 482 \\ 95 \cdot 101 = 950 \\ 4 \cdot 101 = 404 \\ 1 \cdot 101 = 101 \\ 1 \cdot 101 = 101 \\ 4 \cdot 101 = 404 \\ 1 \cdot 101 = 101 \end{array} \right\}$$

$$t_0 = 482(-42) + 95(101) \quad \checkmark$$

$\downarrow \times 73$

4) Edición particular

$$73 = 482(-42 \cdot 73) + 95(101 \cdot 73)$$

$$73 = 482(-2946) + 95(7301)$$

$$t_0 = -42 \cdot 73$$

$$x_0 = a_2 + t_0 \cdot n_2$$

$$x_0 = -682 + (-42) \cdot 482 \cdot 73 = -18825$$

5) Edición general

$$x = x_0 + K \operatorname{mcn}(n_1, n_2)$$

$$x = -18825 + \frac{482 \cdot 95}{K}$$

$$x = -18825 + 42040K$$

$$\boxed{\text{con } K = 1, x = 22215}$$

$$(482 \cdot 101 + 95 \cdot 101) \cdot 101 = 22215$$

$$48200 + 9500 + 950000 + 10100 = 22215$$

✓

Leyendo resultado

22215

$$482 \cdot 101 + 95 \cdot 101 + 95 \cdot 101 + 101 \cdot 101 = 22215$$

$$(482 + 95 + 95 + 101) \cdot 101 = 22215$$

Primer resultado es 22215

(12) Resolver el siguiente sistema de congruencias:

$$2000 < x_0 < 3000$$

$$\left\{ \begin{array}{l} x \equiv 8 \pmod{11} \\ x \equiv 2 \pmod{9} \\ x \equiv 5 \pmod{5} \\ x \equiv 0 \pmod{2} \end{array} \right.$$

$n_1 = 11$	$n_2 = 9$	$\text{mcm}(n_1, n_2)$
0	1	99
1	0	99
2	-1	99
3	-2	99
4	-3	99
5	-4	99
6	-5	99
7	-6	99
8	-7	99
9	-8	99

1) Expressamos la primera ecuación en función de t :

$$\begin{aligned} x \equiv 8 \pmod{11} &\Rightarrow x = 8 + 11t \Rightarrow 8 + 11t \equiv 2 \pmod{9} \Rightarrow \\ &\Rightarrow 11t \equiv -6 \pmod{9} \Rightarrow 11t \equiv 3 \pmod{9} \end{aligned}$$

2) $\text{mcd}(n_1, n_2)$

$$\text{mcd}(11, 9) = 1$$

$$\begin{array}{r} 11 \mid 9 \\ 2 \quad 1 \end{array} \quad \begin{array}{r} 9 \mid 12 \\ 1 \quad 4 \end{array} \quad \begin{array}{r} 12 \mid 12 \\ 1 \quad 1 \end{array} \quad \begin{array}{r} 12 \mid 12 \\ 1 \quad 1 \end{array}$$

3) Coeficientes de Bézout

	u	v
11	1	0
9	0	1
1	2	-1
4	1	-4

$$1 = 11(-4) + 9(5) \quad \checkmark$$

$\times 3 \downarrow$

$$3 = 11(-12) + 9(15)$$

to

4) Solución general

$$t_0 = -12$$

$$x_0 = a_1 + t_0 n_1 = 8 + (-12) \cdot 11 = -124$$

$$x = x_0 + k \text{ mcm}(n_1, n_2) = -124 + k(99)$$

$$\Rightarrow x \equiv -124 \pmod{99}$$

$$\left\{ \begin{array}{l} x \equiv -124 \pmod{495} \equiv 74 \pmod{495} \\ x \equiv 4 \pmod{5} \\ x \equiv 0 \pmod{2} \end{array} \right. \quad \left. \begin{array}{l} \text{x tiene resto 1} \\ \text{x tiene resto 0} \end{array} \right\}$$

1) Expresamos la primera ecuación en función de t

$$x \equiv 74 \pmod{495} \Rightarrow x = 74 + 495t \Rightarrow$$

$$\Rightarrow 74 + 495t \equiv 4 \pmod{5} \Rightarrow 495t \equiv -70 \pmod{5} \Rightarrow$$

$$\Rightarrow 495t \equiv 2 \pmod{5}$$

2) $\text{mcd}(n_1, n_2)$

$$\text{mcd}(495, 5) = 1$$

$$\begin{array}{r} 495 \\ 5 \\ \hline 49 \end{array} \quad \begin{array}{r} 5 \\ 1 \\ \hline 1 \end{array}$$

3) coeficientes de Bezout

	<u>u</u>	<u>v</u>
495	1	0
5	0	1
49	4	-19
1	1	-120

$$\begin{matrix} 1 = 49(-1) + 5(20) & \checkmark \\ 2 = 49(-2) + 5(40) \\ \hline 60 \end{matrix}$$

4) solución particular

$$t_0 = -2$$

$$x_0 = a_1 + t_0 n_2$$

$$x_0 = 74 + (-2)495 = -124$$

5) solución general

$$x = x_0 + k \text{ mcd}(n_1, n_2)$$

$$x = -124 + k \cdot 495 \Rightarrow x \equiv -124 \pmod{495}$$

$$\left\{ \begin{array}{l} x \equiv -124 \pmod{495} \Rightarrow 373 \pmod{495} \\ x \equiv 0 \pmod{2} \end{array} \right. \quad \left. \begin{array}{l} 0 \pmod{2} \\ 1 \pmod{2} \end{array} \right\}$$

1) b) Expresar la primera ecuación en función de t :

$$\begin{aligned} x &\equiv 373 + 495t \pmod{2} \Rightarrow 0 \pmod{2} \text{ para } 373 + 495t \equiv 0 \pmod{2} \\ x &\equiv 373 \pmod{495} \Rightarrow x = 373 + 495t \Rightarrow \\ &\Rightarrow 373 + 495t \equiv 0 \pmod{2} \Rightarrow 495t \equiv -373 \pmod{2} \Rightarrow \\ &\Rightarrow 495t \equiv 1 \pmod{2} \end{aligned}$$

2) $\text{mcd}(n_1, n_2)$

$$\text{mcd}(495, 2) = 1$$

$$\begin{array}{r} 495 \ 12 \\ \underline{-} \ 247 \end{array}$$

$$\begin{array}{r} 1 \ 2 \\ \underline{-} \ 0 \end{array} \quad \begin{array}{r} 1 \ 2 \\ \underline{-} \ 0 \end{array}$$

3) Coeficientes de Bézout

$$\begin{aligned} 495(1) + 2(-247) &= 1 \\ 495(1) + 2(-247) &= 1 \\ 495(1) + 2(-247) &= 1 \\ 495(1) + 2(-247) &= 1 \end{aligned}$$

$$\begin{array}{c|ccccc} 495 & 1 & 2 & 0 & 1 & 0 \\ 247 & & & 1 & 0 & 1 \\ \hline 247 & 1 & 0 & 0 & 1 & 0 \\ 247 & & & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 0 & 1 \end{array}$$

4) Solución particular

$$t_0 = 1$$

$$x_0 = a_1 t_0 + b_1 n_2$$

$$x_0 = 373 + 495 = 868$$

5) Solución general

$$x = x_0 + k \text{ mcd}(n_1, n_2)$$

$$x = 868 + k \cdot 495$$

6) Solución final

$$\text{como } x < 3000 \quad \text{y} \quad 2000 < x$$

$$k = 2 \Rightarrow x = 2848 \text{ monedas}$$

(13)

Resolver el siguiente sistema en $\mathbb{Z}[i]$:

$$\begin{cases} x \equiv i \pmod{3} \\ x \equiv 2 \pmod{2+i} \\ x \equiv 1+i \pmod{3+2i} \\ x \equiv 3+2i \pmod{4+i} \end{cases}$$

i	$2+i$	$3+2i$
$1+i$	3	$4+i$
$3+2i$	3	i

1) Expressar la primera ecuación en función de t

$$x \equiv i \pmod{3} \Rightarrow x = i + 3t \Rightarrow$$

$$\Rightarrow i + 3t \equiv 2 \pmod{2+i} \Rightarrow 3t \equiv 2 - i \pmod{2+i} \Rightarrow$$

$$\Rightarrow 3t \equiv 1+i \pmod{2+i} \quad \text{y} \quad (3-i)t \equiv 1+i$$

2) $\text{mcd}(n_1, n_2)$

$$\text{mcd}(3, 2+i) = i$$

$$|3| = 9$$

$$|2+i| = \sqrt{2^2 + 1^2} = \sqrt{5}$$

$$3 \cdot 5 - 2 \cdot 2 = 13 \quad (3-2)(3+2) = 5$$

$$12+i = 3(2+i)$$

$$\begin{array}{r} 3 | 2+i \\ - 2+i \quad 1-i \\ \hline i \end{array}$$

$$\begin{array}{l} (3)(1-i) \text{ da } 3i - 3 \\ -(3+2)i \quad 1+i \\ \hline 5 \end{array}$$

$$\frac{3}{2+i} = 2 - \frac{6}{5} - \frac{3}{5}i \quad 4(2-i) + 5i - 5 = 8$$

$$\begin{matrix} s & s \\ 1-i & \end{matrix}$$

$$- 4(2-i) + 5i - 5 = 8$$

$$(32-8) \text{ da } 32-8 = 8 \quad \left. \begin{array}{l} (32-8) \text{ da } 32-8 = 8 \\ (32-8) \text{ da } 32-8 = 8 \end{array} \right\}$$

$$\begin{array}{l} (32-8) \text{ da } 32-8 = 8 \\ (32-8) \text{ da } 32-8 = 8 \end{array} \quad \left. \begin{array}{l} (32-8) \text{ da } 32-8 = 8 \\ (32-8) \text{ da } 32-8 = 8 \end{array} \right\}$$

$$\begin{array}{r} 2+i \quad |i \\ -2-i \quad 1-2i \\ \hline 0 \end{array}$$

$$\frac{2+i}{5} = 2 - 2i \Leftrightarrow (32-8) \text{ da } 32-8 = 8$$

$$\Leftrightarrow 8 = (32-8) \text{ da } 32-8 = 8(32-8) + 32-8 = 8$$

$$\Leftrightarrow 8 = (32-8) \text{ da } 32-8 = 8(32-8) + 32-8 = 8$$

3) Coeficientes de Bézout

	u	v	
3	1	0	(3, 15) bdm & ex
$2+c$	0	1	(2+c, 15) bdm & ex
$1-c$	c	1 - 1 + c	

$$\left\{ \begin{array}{l} 3 = 3(1) + (2+c)(-1+c) \\ 2+c = 3(1-c) + (2+c)(-2) \end{array} \right.$$

$$\begin{aligned} 1-c &= 3(1-c) + (2+c)(-2) \\ &\sim \\ &= 6+c \end{aligned}$$

4) Solución particular

$$t_0 = 1 - c$$

$$x_0 = a_1 + t_0 n_1$$

$$x_0 = (1-c) + (1-c) \cdot 3 = 4 - 2c$$

5) Solución general

$$x = x_0 + k \operatorname{lcm}(n_1, n_2)$$

$$x = 4 - 2c + k \frac{3(2+c)}{c}$$

$$x = 4 - 2c + (3 - 6c)k \Rightarrow x \equiv 4 - 2c \pmod{3-6c}$$

Repetimos el proceso:

$$\begin{cases} x \equiv 4 - 2c \pmod{3-6c} \\ x \equiv 1 + c \pmod{3+2c} \\ x \equiv 3+2c \pmod{4+c} \end{cases}$$

1) Expresamos la primera condición en función de t :

$$x \equiv 4 - 2c \pmod{3-6c} \Rightarrow 4 - 2c + (3-6c)t = x \Rightarrow$$

$$\Rightarrow 4 - 2c + (3-6c)t \equiv 1 + c \pmod{3+2c} \Rightarrow$$

$$\Rightarrow (3-6c)t \equiv (-3+3c) \pmod{3+2c} \Rightarrow (3-6c)t \equiv c \pmod{3+2c}$$

2) $\text{mod}(n_1, n_2)$

$$\text{mod}(3+2i, 3-6i) = \text{mod}(3+2i, 3-6i) = 1$$

$$|3-6i| = -27$$

$$|3+2i| = 5$$

$$\begin{array}{r} 3+2i \\ -6-3i \\ \hline -3-i \end{array}$$

$$(3+2i)(-2) + (-6-3i) = -6-4i + 12+6i = 6i$$

$$\frac{3+2i}{3-6i} = -\frac{1}{15} + \frac{8}{15}i \approx i$$

$$\begin{array}{r} 3-6i \\ -2+6i \\ \hline 2 \end{array}$$

$$\frac{3-6i}{-3-i} = -\frac{3}{10} + \frac{21}{10}i \approx 2i$$

3) Coeficientes de Bezout

	u	v
$3+2i$	-1	0
$3-6i$	0	1
i	-3-i	1-i
$2i$	1	-2i -1

$$1 = (3+2i)(-2) + (3-6i)(-1) \quad \checkmark$$

$$i = (3+2i)(2) + (3-6i)(-i)$$

4) Solución particular

Combinar fracciones

$$t_0 = -c$$

$$x_0 = \alpha_1 + t_0 n_2 = (25+8c) + (-c)(21-12c)$$

$$x_0 = 4-2c + (-c)(21-12c) = -2c$$

5) Solución general

$c \in \mathbb{Z}$

$$x = x_0 + k \operatorname{mcm}(n_1, n_2)$$

$$x = -2c + k \frac{(21-12c)(4+c)}{4}$$

$$x = -2c + (21-12c)k \Rightarrow x \equiv -2c \pmod{21-12c}$$

Repetimos el proceso:

$$\begin{cases} x \equiv -2c \pmod{21-12c} \equiv 31+8c \pmod{21-12c} \\ x \equiv 3+2c \pmod{4+c} \end{cases}$$

1) Expresamos la primera ecuación en función de c

$$x \equiv 31+8c \pmod{21-12c} \Rightarrow 31+8c + (21-12c)t = x \Rightarrow$$

$$\Rightarrow 31+8c + (21-12c)t \equiv 3+2c \pmod{4+c} \Rightarrow$$

$$\Rightarrow (21-12c)t \equiv -28-6c \pmod{4+c} \Rightarrow$$

$$\Rightarrow (21-12c)t \equiv c \pmod{4+c}$$

2) $\operatorname{mcm}(n_1, n_2)$

$$\operatorname{mcm}(21-12c, 4+c) = 1$$

$$|21-12c| = 207$$

$$|4+c| = 15$$

21-12c	3	15
4+c	1	15
1	1	15

$$\frac{21-12c}{4+c} = \frac{4+c}{4-4c} \quad | \quad (21-12c)(4-4c) + (3-3)(3-3) = 0$$

$$\frac{21-12c}{4+c} = \frac{72-6c}{17} \quad c \sim 4-4c$$

3) Coeficientes de Bezout

$$1 = (21 - 12\zeta)(1) + (4 + \zeta)(-4 + 4\zeta) \quad \checkmark$$

x0 ↴

$$\zeta = (21 - 12\zeta)(\zeta) + (4 + \zeta)(-4 - 4\zeta)$$

$$b_0 \frac{21\zeta}{57\zeta} + \frac{4}{57} = \frac{-4 - 4\zeta}{57\zeta}$$

4) Solución particular

$$t_0 = \zeta$$

$$x_0 = a_2 t_0 + b_0 n_2$$

$$x_0 = -2 - \zeta + (\zeta)(21 - 12\zeta) = 10 + 20\zeta$$

5) Solución general

$$x = x_0 + k \operatorname{mod}(n_1, n_2)$$

$$x = 10 + 20\zeta + k \frac{(21 - 12\zeta)(4 + \zeta)}{1} = 10 + 20\zeta + (96 - 23\zeta)k$$

(14) En el anillo $\mathbb{Z}[\sqrt{-2}]$ resolver el siguiente sistema de congruencias

$$\begin{cases} x \equiv 1 + 2\sqrt{-2} \pmod{2 - 3\sqrt{-2}} \\ x \equiv 3 \pmod{1 + \sqrt{-2}} \end{cases}$$

1) Expresamos la primera ecuación en función de t

$$\begin{aligned} x &\equiv 1 + 2\sqrt{-2} \pmod{2 - 3\sqrt{-2}} \Rightarrow x = 1 + 2\sqrt{-2} + (2 - 3\sqrt{-2})t \Rightarrow \\ &\Rightarrow 1 + 2\sqrt{-2} + (2 - 3\sqrt{-2})t \equiv 3 \pmod{1 + \sqrt{-2}} \Rightarrow \\ &\Rightarrow (2 - 3\sqrt{-2})t \equiv 2 - (2\sqrt{-2}) \pmod{1 + \sqrt{-2}} \end{aligned}$$

2) $\operatorname{mod}(n_1, n_2)$

$$\operatorname{mod}(2 - 3\sqrt{-2}, 1 + \sqrt{-2}) = \operatorname{mod}(1 + \sqrt{-2}, 2 - 3\sqrt{-2}) =$$

$$|2 - 3\sqrt{-2}| = -14 \quad |1 + \sqrt{-2}| = -1$$