Álgebra relación 3

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

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

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

$\mathbb{Z}[\sqrt{10}]$

Supongamos que 2 es reducible:

$2 = \alpha\beta$ factorización propia

⇓

$\alpha \mid 2 \Rightarrow |\alpha| \mid |2| = 4 \Rightarrow |\alpha| \mid 4$

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

(*)

$|\alpha| = \pm 2$

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

↳ No podemos acotarlo, pero sí hacerlo mod 10

$a^2 = \pm 2 \bmod 10$

¿Es ± 2 un cuadrado mod 10?

cuadrados $\begin{cases} \{0,1,2,3,4,5,6,7,8,9\} \\ \{0,1,4,6,9,5,6,9,4,1\} \end{cases}$

$2 \bmod 10 = 2$
$-2 \bmod 10 = 8$ $\Big\} \notin$ ↑

Luego no tiene solución $\Rightarrow$ **2 es irreducible**

Repetimos el proceso con 3:

Supongo que es reducible $\Leftrightarrow$ Tiene factorización propia:

$3 = \alpha\beta \Rightarrow \alpha | 3 \Rightarrow |\alpha| \,|\, |3| \Rightarrow |\alpha| \,|\, 9$

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

Lo hacemos módulo 10

$a^2 = \pm 3 \bmod 10$

¿Es ± 3 un cuadrado mod 10?

$3 \bmod 10 = 3$
$-3 \bmod 10 = 7$ | usando la tabla de antes vemos que no $\Rightarrow$ **3 es irreducible**

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

Suponemos que $4+\sqrt{10}$ es reducible $\Rightarrow$ tiene factorización propia:

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

$|a|$: $\pm 1 \Rightarrow$ α unidad $\Rightarrow$ No vale
± 2 ± 13
$\pm 26 \Rightarrow$ β unidad $\Rightarrow$ No vale

26	13
2	2
1	

$a^2 - 10b^2 = \pm 2$ $\quad$ $a^2 - 10b^2 = \pm 13$

módulo 10

$a^2 = \pm 2 \bmod 10$ $\quad$ $a^2 = \pm 13 \bmod 10$

Ya hemos visto que no tiene solución

$a^2 = 3 \bmod 10$

$a^2 = 7 \bmod 10$

No tiene solución

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

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

Para probar que $\mathbb{Z}[\sqrt{10}]$ no es DFU, 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:

- $\frac{\mathbb{Z}[i]}{\langle 1+i \rangle} \cong \mathbb{Z}_2$
- $\frac{\mathbb{Z}[i]}{\langle i \rangle} \cong \mathbb{Z}$

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

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

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

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

$$[0] \xmapsto{f} 0 \qquad [0] \xmapsto{f^{-1}} 0$$

$$[i] \xmapsto{f} 1 \qquad [1] \xmapsto{f^{-1}} i$$

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

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

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

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

④ Calcular el mcd de:

- $a = -99$ y $b = 17$

1) Dividimos el mayor entre el menor

-99	17	17	3	3	2	2	1
3	-6	2	5	1	1	0	2

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

2) Coeficientes de Bezout

		u	v
	-99	1	0
	17	0	1
-6	3	1	6
5	2	-5	-31
1	1	6	37

$\Rightarrow 1 = (-99)6 + 17(37)$ ✓

- $a = 6643$, $b = 2873$

1) Dividimos

6643	2873	2873	897	897	182	182	169
897	2	182	3	169	4	13	1

169	13		
0	13		

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

2) Coeficientes de Bezout

		u	v
	6643	1	0
	2873	0	1
2	897	1	-2
3	182	-3	7
4	169	13	-30
1	13	-16	37

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

- $a = -7655$, $b = 1001$

1) Dividimos

$-7655 \mid 1001$ → $363 \mid -8$

$1001 \mid 363$ → $295 \mid 2$

$363 \mid 295$ → $68 \mid 1$

$295 \mid 68$ → $5 \mid 5$

$68 \mid 5$ → $3 \mid 11$

$5 \mid 3$ → $2 \mid 1$

$3 \mid 2$ → $1 \mid 1$

$2 \mid 1$ → $0 \mid 2$

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

2) Coeficientes de Bezout

	-7655	u	v
		1	0
	1001	0	1
-8	363	1	8
2	295	-2	-15
1	68	3	23
5	5	-17	-130
11	3	190	1453
1	2	-207	-1583
1	1	397	3036

$\Rightarrow 1 = (-7655) \cdot 397 + (1001) \cdot 3036$ ✓

• $a = 24230$, $b = 586$

1) Dividimos

24230	586	586	204	204	178
204	41	178	2	26	1

178	26	26	22	22	4	4	2
22	6	4	1	2	5	0	2

$\Rightarrow$ $\boxed{\text{mcd}(24230, 586) = 2}$

2) Usamos coeficientes de Bezout

		u	v
	24230	1	0
	586	0	1
41	204	1	-41
2	178	-2	83
1	26	3	-124
6	22	-20	827
1	4	23	-951
5	2	-135	5582

$\Rightarrow$

$\Rightarrow$ $2 = 24230(-135) + 586(5582)$ ✓

(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) Planteamos la ecuación

$$4050 \equiv a\,10 + b\,46$$

2) MCD

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

46 | 10	10 | 6	6 | 4	4 | 2
6 | 4	4 | 1	2 | 1	0 | 2

3) Coeficientes de Bezout

		u	v
	46	1	0
	10	0	1
4	6	1	-4
1	4	-1	5
1	2	2	-9

$2 = (2)46 + (-9)10$ ✓

4) Multiplicamos por:

$4050 \mid 2$
$0 \mid 2025$ ×

$2 = (2)46 + (-9)10$

$4050 = (4050)46 + (-18225)10$

5) Solución general

$$a = 4050 - \frac{10}{2}t = 4050 - 5t$$

$$b = -18225 + \frac{46}{2}t = -18225 + 23t$$

6) Solución particular

$t = 793 \Rightarrow \begin{cases} a = 14 \\ b = 35 \end{cases}$

⑦ Calcular en $\mathbb{Z}[\sqrt{-2}]$ el mcd y mcm de 3 y $2+\sqrt{2}$.

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

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

1) Módulo

$$|3| = 9$$

$$|2+\sqrt{-2}| = 2$$

2) Dividimos

$$3 \mid 2+\sqrt{-2}$$

$$-\ \frac{2+\sqrt{2}+(2-\sqrt{2})i}{1-\sqrt{2}+(2-\sqrt{2})i} \qquad 1-i$$

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

$$\begin{array}{l} 2+\sqrt{-2} \\ \underline{-2-\sqrt{2}\,i} \\ 0 \end{array} \qquad \begin{array}{l} 1-\sqrt{2}+(2-\sqrt{2})i \\ \underline{(-2-\sqrt{2})i} \end{array}$$

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

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

3) Coeficientes de Bezout

		u	v
	3	1	0
	$2+\sqrt{-2}$	0	1
$1-i$	$1-\sqrt{2}+(2-\sqrt{2})i$	1	$-1+i$

$1-\sqrt{2}+(2-\sqrt{2})i = 3+(2+\sqrt{-2})(-1+i)$ ✓

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

$$= \frac{6+(3\sqrt{2})i}{1-\sqrt{2}+(2-\sqrt{2})i} = \overline{|-(6+3\sqrt{2})i|}$$

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

$$4x+(3+3i)y = -1+5i$$

Encontrar la solución de módulo y mayor que $|32|$.

1) MCD

$|4| = 16$

$|3+3i| = 18$

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

$$\begin{array}{r|l} 3+3i & 4 \\ \hline -4-4i & 1+i \\ \hline -1-i & \end{array} \qquad \begin{array}{r|l} 4 & -1-i \\ \hline 0 & -2+2i \end{array}$$

$\dfrac{3+3i}{4} = \dfrac{3}{4}+\dfrac{3}{4}i \sim 1+i \qquad \dfrac{4}{-1-i} = -2+2i$

2) Coeficientes de Bezout

		u	v
	$3+3i$	1	0
	4	0	1
$1+i$	$-1-i$	1	$-1-i$

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

3) Multiplicamos la ecuación:

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

$$-1-i = (3+3i)(1) + (-1-i)4$$

$\times\ -2-3i$ ↓

$$-1+5i = (3+3i)(-2-3i) + (-1+5i)4$$

4) Solución general:

$$\left.\begin{aligned} y &= (-2-3i) + t\,\frac{3+3i}{-1-i} = (-2-3i) - 3t \\ x &= (-1+5i) + t\,\frac{4}{-1-i} = (-1+5i) + t(-2+2i) \end{aligned}\right\}$$

5) Solución particular:

$t = 50$

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

⑨ Calcular el resto de dividir 279^{823} entre 17.

$a^n \bmod b$

1) mcd (a, b)

mcd(279, 17) = 1 ✓

279 | 17	17 | 7	7 | 3
7 | 16	3 | 2	1 | 2

2) Usamos phi de Euler

$279^{\varphi(17)} \equiv 1 \bmod 17$

$\varphi(17) = 16$

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

3) Expresamos 279^{823} como:

823 | 16
3 | 20

$279^{823} = 279^{16 \cdot 20 + 3} = (279^{16})^{20} \cdot 279^3$

Luego:

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

$279^{16} \to 1$

4) Hacemos la división

279^3 | 17
3 | 9

5) Solución

$\boxed{r = 3}$

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

$a^n \mod b$

1) mcd (a,b)

mcd(320,13) = 1 ✓

320 | 13	13 | 8	8 | 5	5 | 3
8 24	5 1	3 1	2 1

3 | 2
1 1

2) Phi de Euler

$\varphi(13) = 12$

Luego, $320^{\varphi(13)} \mod 13 = 320^{12} \equiv 1 \mod 13$

3) Expresamos 320^{207} como:

207 | 12
3 17

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

4) Calculamos

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

$320^{12} \equiv 1$

Luego

320^3 | 13
5 9

$\boxed{r = 5}$

(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:

- $n = 5103$, $b = 125$, $y = 3335$

1) Factorizamos n

5103	3
1701	3
567	3
189	3
63	3
21	3
7	7
1	

$5103 = 3^6 \cdot 7$

2) Phi de Euler de n

$\varphi(5103) = \varphi(3^6 \cdot 7) = \varphi(3^6) \cdot \varphi(7) =$

$= 2 \cdot 3^5 \cdot 6 = 2916$

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

2916	125	125	41	41	2
41	23	2	3	1	20

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

4) Coeficientes de Bezout

		u	v
	2916	1	0
	125	0	1
23	41	1	-23
3	2	-3	70
20	1	61	-1423

$1 = 2916(61) + 1250(-1423)$ ✓

5) Solución que acompaña a b

$$V = -1428 + \frac{2916}{1} t \Rightarrow V_0 = 1493$$

6) Buscamos x:

$$x \equiv y^u \bmod n = 3835^{1493} \bmod 5103 = \boxed{55}$$

- $n = 1568$, $b = 125$, $y = 193$

1) Factorizamos n

1568	2
784	2
392	2
196	2
98	2
14	7
2	7
1	2

$1568 = 2^5 \cdot 7^2$

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) mcd $(\varphi(n), b)$

672 | 125 — 47 | 5

125 | 47 — 31 | 2

47 | 31 — 16 | 1

31 | 16 — 15 | 1

16 | 15 — 1 | 1

mcd (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

$1 = 672(8) + 125(-43)$ ✓

5) solución que acompaña a b

$$V = -43 + \frac{8}{1} 6 = -431 \, 8t \Rightarrow V_0 = 5$$

6) solución

$$X \equiv y^r \bmod n \equiv 103^5 \bmod 1568 = \underline{\underline{737}}$$

- $n = 18711$, $b = 1231$, $y = 9797$

1) Factorizamos n

$$18711 = 3^5 \cdot 7 \cdot 11$$

2) Phi de Euler de n

$$\varphi(18711) = \varphi(3^5) \cdot \varphi(7) \cdot \varphi(11) =$$

$$= 2 \cdot 3^4 \cdot 6 \cdot 10 = 9720$$

3) MCD(φ(n) , b)

9720 | 1231 — 1103 | 7

1231 | 1103 — 128 | 1

1103 | 128 — 79 | 8

128	79	79	49	49	30	30	19
49	1	30	1	19	1	11	1

19	11	11	8	8	3	3	2
8	1	3	1	2	2	1	1

4) Coeficientes de Bezout

		u	v
	9720	1	0
	1281	0	1
9	1103	1	-7
1	128	-1	8
8	79	9	-71
1	49	-10	79
1	30	19	-150
1	19	-29	229
1	11	48	-379
1	8	-77	608
1	3	125	-987
2	2	-327	2582
1	1	452	-3569

$1 = (452)9720 + (-3569)1281$ ✓

5) Solución general que acompaña a b:

$$v = -3569 + \frac{9720}{1} t \Rightarrow v_0 = 6151$$

6) Buscamos x

$$x \equiv y^{v} \bmod n = \underline{9797^{6151} \bmod 18711}$$

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

$$\begin{cases} x \equiv 7 \bmod 9 \\ x \equiv 2 \bmod 16 \\ 3x \equiv 22 \bmod 95 \end{cases}$$

Vamos asociando ecuaciones de dos en dos.

1) Expresamos la primera ecuación en función de t.

$x \equiv 7 \bmod 9 \Rightarrow x = 7 + 9t \Rightarrow 7 + 9t \equiv 2 \bmod 16 \Rightarrow$

$\Rightarrow 9t \equiv (-5) \bmod 16 \Rightarrow \underset{n_1}{9}t \equiv \underline{11} \bmod \underset{n_2}{16}$

2) MCD(n_1, n_2)

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

16 | 9	9 | 7	7 | 2
7 | 1	2 | 1	1 | 3

3) Coeficientes de Bezout

		u	v
	16	1	0
	9	0	1
1	7	1	-1
1	2	-1	2
3	1	4	-7

$1 = 16(4) + 9(-7)$ ✓

$\times 11$ ↘

$11 = 16(44) + 9(\underbrace{-77}_{\text{to}})$

4) Solución particular

$t_0 = -77$

$x_0 = a_1 + t_0 \cdot n_1$

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

5) Solución general

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

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

$x = -682 + k\,144 \Rightarrow \boxed{x \equiv -682 \bmod 144}$

6) Repetimos el proceso

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

1) Expresamos la primera ecuación en función de t:

$x \equiv -682 \bmod 144 \Rightarrow -682 + 144t = x \Rightarrow$

$\Rightarrow 3(-682 + 144t) \equiv 22 \bmod 95 \Rightarrow$

$\Rightarrow 432t \equiv 2068 \bmod 95 \Rightarrow 432t \equiv 78 \bmod 95$

2) MCD (n_1, n_2)

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

432 | 95	95 | 52	52 | 43
52 | 4	43 | 1	9 | 1

48 | 9	9 | 7	7 | 2
7 | 4	2 | 1	1 | 3

3) Coeficientes de Bezout

		u	v
	432	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	191

$1 = 432(-42) + 95(191)$ ✓

4) Solución particular

$\times 73$

$73 = 432(-42 \cdot 73) + 95(191 \cdot 73)$

$t_0 = -42 \cdot 73$

$x_0 = a_1 + t_0 \cdot n_1$

$x_0 = -652 + (-42) \cdot 432 \cdot 73 \quad -18825$

5) Solución general

$x = x_0 + K\,mcm(n_1, n_2)$

$x = -18825 + \frac{432 \cdot 95}{1} K$

$x = -18825 + 41040K$

Con $K = 1$, $x = 22215$

(12) Resolver el siguiente sistema de congruencias:

$$2000 < x_0 < 3000$$

$$\begin{cases} x \equiv 8 \bmod 11 \\ x \equiv 2 \bmod 9 \\ x \equiv 1 \bmod 5 \\ x \equiv 0 \bmod 2 \end{cases}$$

1) Expresamos la primera ecuación en función de t:

$x \equiv 8 \bmod 11 \Rightarrow x = 8 + 11t \Rightarrow 8 + 11t \equiv 2 \bmod 9 \Rightarrow$

$\Rightarrow 11t \equiv -6 \bmod 9 \Rightarrow 11t \equiv 3 \bmod 9$

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

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

11 | 9		9 | 2	
2	1	1	4

3) Coeficientes de Bezout

		u	v
	11	1	0
	9	0	1
1	2	1	-1
4	1	-4	5

$1 = 11(-4) + 9(5)$ ✓

$\times 3$ ↓

$3 = 11\underbrace{(-12)}_{t_0} + 9(15)$

4) Solución general

$t_0 = -12$

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

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

$\Rightarrow x \equiv -124 \bmod 99$

$$\begin{cases} x \equiv -124 \bmod 99 \equiv 74 \bmod 99 \\ x \equiv 4 \bmod 5 \\ x \equiv 0 \bmod 2 \end{cases}$$

1) Expresamos la primera ecuación en función de t

$x \equiv 74 \bmod 99 \Rightarrow x = 74 + 99t \Rightarrow$

$\Rightarrow 74 + 99t \equiv 4 \bmod 5 \Rightarrow 99t \equiv -70 \bmod 5 \Rightarrow$

$\Rightarrow 99t \equiv 2 \bmod 5$

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

$\text{mcd}(99, 5) = 1$

99 | 5	5 | 4
4 | 19	1 | 1

3) Coeficientes de Bezout

		u	v
	99	1	0
	5	0	1
19	4	1	-19
1	1	-1	20

$1 = 99(-1) + 5(20)$ ✓

$\times 2$ ↓

$2 = 99(-2) + 5(40)$

t_0

4) Solución particular

$t_0 = -2$

$x_0 = a_1 + t_0 n_1$

$x_0 = 74 + (-2)99 = -124$

5) Solución general

$x = x_0 + K \, mcm(n_1, n_2)$

$x = -124 + K\,495 \Rightarrow x \equiv -124 \bmod 495$

$$\begin{cases} x \equiv -124 \bmod 495 \equiv 373 \bmod 495 \\ x \equiv 0 \bmod 2 \end{cases}$$

1) Expresamos la primera ecuación en función de t:

$x \equiv 373 \bmod 495 \Rightarrow x \equiv 373 + 495t \Rightarrow$

$\Rightarrow 373 + 495t \equiv 0 \bmod 2 \Rightarrow 495t \equiv -373 \bmod 2 \Rightarrow$

$\Rightarrow 495t = 1 \bmod 2$

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

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

$495 \;|\; 2$

$1 \quad 247$

3) Coeficientes de Bezout

$495(1) + 2(-247) = 1$ ✓

$\times 1$ ↳ $495(1) + 2(-247) = 1$

n_0

4) Solución particular

$t_0 = 1$

$x_0 = a_1 + t_0 n_1$

$x_0 = 373 + 495 = 868$

5) Solución general

$x = x_0 + K \,\text{mcm}(n_1, n_2)$

$x = 868 + K990$

6) Solución final

como $x < 3000$ y $2000 < x$

$K = 2 \Rightarrow$ **$x = 2848$ manadas**

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

$$\begin{cases} x \equiv i \bmod 3 \\ x \equiv 2 \bmod (2+i) \\ x \equiv 1+i \bmod (3+2i) \\ x \equiv 3+2i \bmod (4+i) \end{cases}$$

1) Expresar la primera ecuación en función de t

$x \equiv i \bmod 3 \Rightarrow x = i + 3t \Rightarrow$

$\Rightarrow i + 3t \equiv 2 \bmod (2+i) \Rightarrow 3t \equiv 2 - i \bmod (2+i) \Rightarrow$

$\Rightarrow 3t \equiv 1+i \bmod (2+i)$

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

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

$|3| = 9$

$|2+i| = 3$

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

$$\frac{3}{2+i} = \frac{6}{5} - \frac{3}{5}i$$

$$\begin{array}{cc} 5 & 5 \\ 1 & -i \end{array}$$

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

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

3) Coeficientes de Bezout

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

$i = 3(1) + (2+i)(-1+i)$ ✓

$\times 1-i$ ↓

$1+i = 3(\underbrace{1-i}_{t_0}) + (2+i)(-2)$

4) Solución particular

$t_0 = 1-i$

$x_0 = a_1 + t_0 n_1$

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

5) Solución general

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

$x = 4-2i + K\,\frac{3(2+i)}{i}$

$x = 4-2i + (3-6i)K \Rightarrow x \equiv 4-2i \bmod (3-6i)$

Repetimos el proceso:

$$\begin{cases} x \equiv 4-2i \bmod (3-6i) \\ x \equiv 1+i \bmod (3+2i) \\ x \equiv 3+2i \bmod (4+i) \end{cases}$$

1) Expresamos la primera ecuación en función de t:

$x \equiv 4-2i \bmod (3-6i) \Rightarrow 4-2i + (3-6i)t = x \Rightarrow$

$\Rightarrow 4-2i + (3-6i)t \equiv 1+i \bmod (3+2i) \Rightarrow$

$\Rightarrow (3-6i)t \equiv (-3+3i) \bmod (3+2i) \Rightarrow (3-6i)t \equiv i \bmod (3+2i)$

2) mcd (n_1, n_2)

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

$|3-6i| = -27$

$|3+2i| = 5$

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

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

$$\begin{array}{r|l} 3-6i & -3-i \\ \hline -2+6i & 2i \\ \hline 1 & \end{array}$$

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

3) Coeficientes de Bezout

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

$1 = (3+2i)(-2i) + (3-6i)(-1)$ ✓

$\times i$ ↓

$i = (3+2i)(2) + (3-6i)\underbrace{(-i)}_{60}$

4) Solución particular

$t_0 = -i$

$x_0 = a_1 + t_0 n_1$

$x_0 = 4 - 2i + (-i)(3 - 6i) = -2 - i$

5) Solución general

$x = x_0 + K \, mcm(n_1, n_2)$

$x = -2 - i + K \, \frac{(3-6i)(3+2i)}{1}$

$x = -2 - i + (21 - 12i)K \Rightarrow x \equiv -2 - i \mod (21 - 12i)$

Repetimos el proceso:

$$\begin{cases} x \equiv -2 - i \mod (21 - 12i) \equiv 31 + 8i \mod (21 - 12i) \\ x \equiv 3 + 2i \mod (4 + i) \end{cases}$$

1) Expresamos la primera ecuación en función de t

$x \equiv 31 + 8i \mod (21 - 12i) \Rightarrow 31 + 8i + (21 - 12i)t = x \Rightarrow$

$\Rightarrow 31 + 8i + (21 - 12i)t \equiv 3 + 2i \mod (4 + i) \Rightarrow$

$\Rightarrow (21 - 12i)t \equiv -28 - 6i \mod (4 + i) \Rightarrow$

$\Rightarrow (21 - 12i)t \equiv i \mod (4 + i)$

2) $mcd(n_1, n_2)$

$mcd(21 - 12i, \; 4 + i) = 1$

$|21 - 12i| = 297$

$|4 + i| = 15$

$$\begin{array}{r|l} 21 - 12i & 4 + i \\ \hline -20 + 12i & 4 - 4i \\ \hline 1 & \end{array}$$

$$\frac{21 - 12i}{4 + i} = \frac{72}{17} - \frac{69}{17} i \sim 4 - 4i$$

3) Coeficientes de Bezout

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

$\cdot i$

$$i = (21-12i)(i) + (4+i)(-4-4i)$$

4) solución particular

$$t_0 = i$$

$$x_0 = a_1 + t_0 n_1$$

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

5) solución general

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

$$x = 10+20i + K\,\frac{(21-12i)(4+i)}{1} = 10+20i+(96-29i)K$$

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

$$\begin{cases} x \equiv 1+2\sqrt{-2} \mod (2-3\sqrt{-2}) \\ x \equiv 3 \mod (1+\sqrt{-2}) \end{cases}$$

1) Expresamos la primera ecuación en función de t

$$x \equiv 1+2\sqrt{-2} \mod (2-3\sqrt{-2}) \Rightarrow x = 1+2\sqrt{-2} + (2-3\sqrt{-2})t \Rightarrow$$

$$\Rightarrow 1+2\sqrt{-2} + (2-3\sqrt{-2})t \equiv 3 \mod (1+\sqrt{-2}) \Rightarrow$$

$$\Rightarrow (2-3\sqrt{-2})t \equiv 2-(2\sqrt{2})i \mod (1+\sqrt{-2}) \Rightarrow$$

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

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

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