

PRÁCTICA 3. ARITMÉTICA ENTERA Y MODULAR

ESCRIBE TU NOMBRE Y GRUPO

1. ECUACIONES DIOFÁNTICAS

Una ecuación diofántica es una ecuación en la que nos piden únicamente las soluciones enteras. Una ecuación puede tener soluciones, por ejemplo

$$2x + 4y = 3$$

tiene infinitas soluciones, pero no tiene ninguna solución entera porque si x e y se sustituyen por valores enteros, el primer miembro será siempre un número par y no podrá ser nunca igual a 3, por eso las técnicas de resolución de las ecuaciones diofánticas son específicas y no nos valen muchos de los métodos de resolución de las ecuaciones habituales.

Importante

En las ecuaciones diofánticas en las que nos piden soluciones en el conjunto de los números enteros, las matrices y las reducciones se tienen que hacer en \mathbb{ZZ} . Hacer reducciones en \mathbb{QQ} en este tipo de problemas cuando haya que hacerlas en \mathbb{ZZ} anula todo el ejercicio que será valorado con 0.

El ejemplo fundamental de ecuaciones diofánticas al que reduciremos muchos de los problemas del tema es el de una ecuación con dos incógnitas. Tal y como hemos visto en teoría, este tipo de ecuaciones tiene solución si y solo si el máximo común divisor de los coeficientes divide al término independiente. Vamos a ver cómo resolverlos usando `sage`.

Ejemplo 1. Encuentra todas las soluciones enteras de la ecuación

$$35x_1 + 25x_2 = 55$$

Solución:

```
A = matrix(ZZ,[35,25])
At1 = block_matrix([[A.T,1]])
At1R = At1.echelon_form()
Q = At1R[:,1:].T
```

Construimos la matriz de los coeficientes $A = \begin{pmatrix} 35 & 25 \end{pmatrix}$ que vamos a reducir por columnas, para ello la trasponemos y ampliamos con la matriz identidad, reducimos y obtenemos lo siguiente:

$$\left(\begin{array}{c|cc} 35 & 1 & 0 \\ 25 & 0 & 1 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 5 & 3 & -4 \\ 0 & 5 & -7 \end{array} \right)$$

El teorema fundamental de la reducción por filas, nos dice que

$$\left(\begin{array}{cc} 3 & -4 \\ 5 & -7 \end{array} \right) \left(\begin{array}{c} 35 \\ 25 \end{array} \right) = \left(\begin{array}{ccc} 0 & 5 & -7 \end{array} \right)$$

que si trasponemos (recordemos que la traspuesta del producto es el producto de las traspuestas cambiadas de orden) no dice que

$$\left(\begin{array}{cc} 35 & 25 \end{array} \right) \left(\begin{array}{cc} 3 & 5 \\ -4 & -7 \end{array} \right) = \left(\begin{array}{cc} 5 & 0 \end{array} \right)$$

que es el equivalente por columnas al teorema fundamental de la reducción por filas.

Este producto nos da dos ecuaciones:

$$35 \cdot 3 + 25 \cdot (-4) = 5$$

$$35 \cdot 5 + 25 \cdot (-7) = 0$$

La primera relación es el máximo común divisor expresado como combinación de los coeficientes. Vamos a buscar valores enteros u_1 y u_2 de forma que multiplicando la primera ecuación por u_1 y la segunda por u_2 y sumando, obtengamos la solución del problema.

$$\begin{aligned} (35 \cdot 3 + 25 \cdot (-4) = 5) \cdot u_1 \\ (35 \cdot 5 + 25 \cdot (-7) = 0) \cdot u_2 \end{aligned}$$

Para conseguir de esa ecuación una solución del sistema tenemos que multiplicar toda la ecuación por 11 para obtener el término independiente igual a 55 (es decir, $u_1 = 55/5 = 11$). Si el término independiente no hubiera sido múltiplo de 5 (el máximo común divisor de los coeficientes) la ecuación no tendría soluciones enteras porque para cualesquiera x_1 y x_2 enteros, el primer miembro sería múltiplo de 5.

La segunda ecuación la podemos multiplicar por un parámetro libre $u_2 = t$ que sea un número entero y obtener las ecuaciones

$$\begin{aligned} 35 \cdot 3 \cdot 11 + 25 \cdot (-4) \cdot 11 &= 5 \cdot 11 = 55 \\ 35 \cdot 5 \cdot t + 25 \cdot (-7) \cdot t &= 0 \cdot t = 0 \end{aligned}$$

Sumando y sacando factor común los coeficientes de la ecuación tenemos

$$35(33 + 5t) + 25(-44 - 7t) = 55$$

con lo que obtenemos las soluciones

$$\begin{aligned} x_1 &= 33 + 5t \\ x_2 &= -44 - 7t \end{aligned}$$

siendo t un número entero cualquiera.

```
Pol.<t> = ZZ[]
U = matrix([[11],[t]])
```

Esto se podría también hacer automáticamente si partimos del teorema fundamental de la reducción por columnas y tomando $X = QU$ para un vector U que representa los coeficientes por los que multiplicamos cada ecuación:

$$\begin{pmatrix} 35 & 25 \end{pmatrix} \begin{pmatrix} 3 & 5 \\ -4 & -7 \end{pmatrix} = \begin{pmatrix} 5 & 0 \end{pmatrix}$$

con lo que tenemos para cualquier valor entero t que

$$\underbrace{\begin{pmatrix} 35 & 25 \end{pmatrix}}_A \underbrace{\begin{pmatrix} 3 & 5 \\ -4 & -7 \end{pmatrix}}_X \begin{pmatrix} 11 \\ t \end{pmatrix} = \begin{pmatrix} 5 & 0 \end{pmatrix} \begin{pmatrix} 11 \\ t \end{pmatrix} = \underbrace{\begin{pmatrix} 55 \\ \end{pmatrix}}_B$$

y las soluciones son

$$X = QU = \begin{pmatrix} 3 & 5 \\ -4 & -7 \end{pmatrix} \begin{pmatrix} 11 \\ t \end{pmatrix} = \begin{pmatrix} 5t + 33 \\ -7t - 44 \end{pmatrix}.$$

Resuelve el siguiente ejercicio siguiendo la muestra del ejemplo anterior.

Ejercicio 1. Encuentra todas las soluciones enteras de la ecuación

$$3811x_1 + 2923x_2 = 8621$$

Solución:

Lo que se hace para dos variables, también se puede hacer con más variables añadiendo más parámetros.

Ejemplo 2. Encuentra todas las soluciones enteras de $19x_1 - 57x_2 + 38x_3 = 95$.

Solución:

```
A = matrix(ZZ,[[19,-57,38]])
At1 = block_matrix([[A.T,1]])
R = At1.echelon_form()
Q = R[:,1:].T
```

Construimos la matriz de los coeficientes $\begin{pmatrix} 19 & -57 & 38 \end{pmatrix}$, la trasponemos y ampliamos con la identidad.

$$\left(\begin{array}{ccc|ccc} 19 & & & 1 & 0 & 0 \\ -57 & & & 0 & 1 & 0 \\ 38 & & & 0 & 0 & 1 \end{array} \right)$$

La reducimos y obtenemos la matriz de paso por la derecha

$$\left(\begin{array}{cccc} 19 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 3 \end{array} \right) \quad Q = \left(\begin{array}{ccc} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 2 & 1 & 3 \end{array} \right)$$

Comprobamos el teorema fundamental de la reducción por columnas

$$AQ = \begin{pmatrix} 19 & -57 & 38 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 19 & 0 & 0 \end{pmatrix}$$

Esto nos da tres ecuaciones

$$19 \cdot 0 + (-57) \cdot 1 + 38 \cdot 2 = 19$$

$$19 \cdot 1 + (-57) \cdot 1 + 38 \cdot 1 = 0$$

$$19 \cdot 0 + (-57) \cdot 2 + 38 \cdot 3 = 0$$

Vamos a multiplicar cada una de las ecuaciones por un valor u_i y luego los sumaremos todos para obtener la solución general.

$$\begin{aligned} & \left(19 \cdot 0 + (-57) \cdot 1 + 38 \cdot 2 = 19 \right) \cdot u_1 \\ & \left(19 \cdot 1 + (-57) \cdot 1 + 38 \cdot 1 = 0 \right) \cdot u_2 \\ & \left(19 \cdot 0 + (-57) \cdot 2 + 38 \cdot 3 = 0 \right) \cdot u_3 \end{aligned}$$

La primera ecuación nos da el máximo común divisor de los coeficientes, 19, que divide al término independiente $19 \cdot 5 = 95$ así que multiplicaremos la primera ecuación por $u_1 = 5$ y la segunda y la tercera por parámetros libres $u_2 = s$ y $u_3 = t$ con lo que obtendremos

$$19 \cdot 0 \cdot 5 + (-57) \cdot 1 \cdot 5 + 38 \cdot 2 \cdot 5 = 19 \cdot 5 = 95$$

$$19 \cdot 1 \cdot s + (-57) \cdot 1 \cdot s + 38 \cdot 1 \cdot s = 0s = 0$$

$$19 \cdot 0 \cdot t + (-57) \cdot 2 \cdot t + 38 \cdot 3 \cdot t = 0t = 0$$

Sumando y sacando factor común tenemos

$$19s - 57(5 + s + 2t) + 38(10 + s + 3t) = 95$$

y de ahí sacamos el valor de las variables

$$x_1 = s$$

$$x_2 = 5 + s + 2t$$

$$x_3 = 10 + s + 3t$$

```
Pol.<s,t> = ZZ[]
U = matrix([[5],[s],[t]])
```

También se puede hacer automáticamente partiendo de la relación fundamental de la reducción por columnas

$$AQ = \begin{pmatrix} 19 & -57 & 38 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 19 & 0 & 0 \end{pmatrix}$$

y multiplicando por $U = \begin{pmatrix} 5 \\ s \\ t \end{pmatrix}$ (para parámetros libres s y t en el conjunto de los números enteros) tenemos

$$AX = \underbrace{\begin{pmatrix} 19 & -57 & 38 \end{pmatrix}}_A \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix}}_X \begin{pmatrix} 5 \\ s \\ t \end{pmatrix} = \begin{pmatrix} 19 & 0 & 0 \end{pmatrix} \begin{pmatrix} 5 \\ s \\ t \end{pmatrix} = \begin{pmatrix} 95 \end{pmatrix} = B$$

y por lo tanto tenemos las soluciones

$$X = QU = \begin{pmatrix} s \\ s + 2t + 5 \\ s + 3t + 10 \end{pmatrix}.$$

Ejercicio 2. *Calcula todas las soluciones enteras de la ecuación diofántica*

$$741x_1 + 1311x_2 + 897x_3 = 363$$

Solución:

2. TEOREMA CHINO DE LOS RESTOS

El problema básico que resuelve el Teorema Chino de los Restos es encontrar los valores de n tales que se cumplan simultáneamente las relaciones

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

Cuando este problema tiene solución, será de la forma

$$n \equiv a \pmod{\text{mcm}(m_1, m_2)}$$

Este tipo de problemas los podemos reducir a una ecuación diofántica lineal. Vamos a verlo con un ejemplo.

Ejemplo 3. *Encuentra todos los números enteros n tales que*

$$\begin{aligned} n &\equiv 12 \pmod{35} \\ n &\equiv 42 \pmod{55} \end{aligned}$$

Solución:

La primera relación nos dice que $n = 12 + 35x_1$ y la segunda $n = 42 + 55x_2$ para valores enteros indeterminados x_1 y x_2 . Igualando ambas ecuaciones tenemos que

$$12 + 35x_1 = 42 + 55x_2$$

Esto nos da la ecuación diofántica

$$35x_1 - 55x_2 = 42 - 12 = 30$$

```
A = matrix(ZZ, [[35, -55]])
At1 = block_matrix([[A.T, 1]])
At1R = At1.echelon_form()
Q = At1R[:, 1:].T
```

Tomamos la matriz de los coeficientes $A = \begin{pmatrix} 35 & -55 \end{pmatrix}$ y vamos a reducir por columnas, para ello trasponemos y ampliamos con la identidad para reducir por filas

$$\left(\begin{array}{c|cc} 35 & 1 & 0 \\ -55 & 0 & 1 \end{array} \right) \rightarrow \left(\begin{array}{ccc} 5 & 8 & 5 \\ 0 & 11 & 7 \end{array} \right)$$

La matriz que queda a la derecha es la traspuesta de la matriz de paso por la derecha, que podemos comprobar que cumple el teorema fundamental de la reducción por columnas

$$Q = \begin{pmatrix} 8 & 11 \\ 5 & 7 \end{pmatrix} \quad \begin{pmatrix} 35 & -55 \end{pmatrix} \begin{pmatrix} 8 & 11 \\ 5 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 0 \end{pmatrix}$$

El máximo común divisor es 5 que divide al término independiente que es 30. Para conseguirlo tenemos que multiplicar por 6.

`Pol.<t> = ZZ[]`

`U = matrix(Pol,[[6],[t]])`

`X = Q*U`

La solución es $X = \begin{pmatrix} 8 & 11 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 6 \\ t \end{pmatrix} = \begin{pmatrix} 11t + 48 \\ 7t + 30 \end{pmatrix}$ para un valor entero cualquiera t y que podemos comprobar viendo que

$$AX = \begin{pmatrix} 35 & -55 \end{pmatrix} \begin{pmatrix} 11t + 48 \\ 7t + 30 \end{pmatrix} = \begin{pmatrix} 30 \end{pmatrix}.$$

Con los valores x_1 y x_2 podemos obtener el valor de n . Cualquiera de las dos relaciones nos sirve

$$n = 12 + 35x_1 = 12 + 35(11t + 48) = 385t + 1692$$

$$n = 42 + 55x_2 = 42 + 55(7t + 30) = 385t + 1692$$

Esto es equivalente a decir que n es 1692 salvo múltiplos de 385, es decir

$$n \equiv 1692 \pmod{385}$$

Podemos reducir módulo 385 para obtener un valor de n entre 0 y 384,

$$n \equiv 1692 \equiv 152 \pmod{385}$$

Podemos ver que el resultado nos ha salido módulo 385 = $5 \cdot 7 \cdot 11$ que es el mínimo común múltiplo de $35 = 5 \cdot 7$ y $55 = 5 \cdot 11$.

Para entender un poco mejor lo que está pasando en este problema, vamos a replantearlo del siguiente modo: Llamemos $n = x_0$ y vamos a escribir de nuevo las ecuaciones

$$x_0 = 12 + 35x_1$$

$$x_0 = 42 + 55x_2$$

o lo que es lo mismo

$$x_0 - 35x_1 = 12$$

$$x_0 - 55x_2 = 42$$

Lo que hacemos al igualar los valores de n en realidad es resolver este sistema de ecuaciones diofánticas restando a la segunda ecuación la primera para así eliminar x_0 (que es n) lo que nos deja

$$x_0 - 35x_1 = 12$$

$$35x_1 - 55x_2 = 30$$

Resolvemos la segunda ecuación en dos variables y luego utilizamos la primera para sacar el valor de x_0 que es el que necesitamos. Por lo tanto lo que estamos haciendo con este sistema no es más que resolver un caso particular de sistema de ecuaciones diofánticas de dos ecuaciones y tres incógnitas.

Ejercicio 3. *Calcula todos los valores enteros n tales que*

$$n \equiv 20 \pmod{111}$$

$$n \equiv 56 \pmod{75}$$

Solución:

Cuando en lugar de tener dos relaciones de congruencia, tenemos tres o más, lo más eficiente es ir agrupando de dos en dos las relaciones para ir reduciendo su número ya que la combinación de dos relaciones de congruencia es una nueva relación de congruencia. Veámoslo con un ejemplo:

Ejemplo 4. *Encuentra todos los valores enteros n tales que*

$$n \equiv 27 \pmod{102}$$

$$n \equiv 12 \pmod{35}$$

$$n \equiv 42 \pmod{55}$$

Solución 1:

Lo primero que vamos a notar es que en el Ejemplo 3 encontramos los valores n que cumplían las dos últimas ecuaciones, por lo tanto las dos relaciones de congruencia

$$n \equiv 12 \pmod{35}$$

$$n \equiv 42 \pmod{55}$$

son equivalentes a la relación de congruencia

$$n \equiv 152 \pmod{385}$$

y por lo tanto nuestro problema lo podemos reducir a encontrar los valores n tales que

$$n \equiv 27 \pmod{102}$$

$$n \equiv 152 \pmod{385}$$

que resolveremos usando la técnica habitual de dos variables:

$$n = 27 + 102x_1 \quad n = 152 + 385x_2$$

igualando las dos ecuaciones tenemos que

$$27 + 102x_1 = 152 + 385x_2$$

de donde obtenemos la ecuación en la forma habitual

$$102x_1 - 385x_2 = 152 - 27 = 125$$

```
A = matrix(ZZ, [[102, -385]])
At1 = block_matrix([[A.T, 1]])
At1R = copy(At1.echelon_form())
At1R.subdivide([], [1])
Q = At1R.subdivision(0, 1).T
Pol.<t, x1, x2> = ZZ[]
U = matrix(Pol, [[125], [t]])
XX = Q*U
X = matrix(Pol, [[x1], [x2]])
sol = 27+102*XX[0,0]
```

Tomamos la matriz de los coeficientes $A = \begin{pmatrix} 102 & -385 \end{pmatrix}$ la trasponemos, ampliamos con la identidad y reducimos sobre el conjunto de los números enteros

$$\left(\begin{array}{c|cc} 102 & 1 & 0 \\ -385 & 0 & 1 \end{array} \right) \rightarrow \left(\begin{array}{c|cc} 1 & 268 & 71 \\ 0 & 385 & 102 \end{array} \right)$$

La matriz de paso por la derecha es $Q = \begin{pmatrix} 268 & 385 \\ 71 & 102 \end{pmatrix}$ y el teorema fundamental de la reducción por columnas nos dice que

$$\begin{pmatrix} 102 & -385 \end{pmatrix} \begin{pmatrix} 268 & 385 \\ 71 & 102 \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

En este caso el máximo común divisor de los coeficientes es 1 y la ecuación seguro que tiene solución que podremos obtener tomando

$$\begin{pmatrix} 102 & -385 \end{pmatrix} \begin{pmatrix} 268 & 385 \\ 71 & 102 \end{pmatrix} \begin{pmatrix} 125 \\ t \end{pmatrix} = \begin{pmatrix} 102 & -385 \end{pmatrix} \begin{pmatrix} 385t + 33500 \\ 102t + 8875 \end{pmatrix} = \begin{pmatrix} 125 \end{pmatrix}$$

lo que nos dice que las soluciones para x_1 y x_2 son

$$X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 385t + 33500 \\ 102t + 8875 \end{pmatrix}$$

De ahí, sustituyendo en el valor de n tenemos que

$$n = 27 + 102x_1 = 27 + 102(385t + 33500) = 39270t + 3417027$$

El resultado nos lo da salvo múltiplos de $39270 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17$ que es precisamente el $mcm(102, 35, 55) = mcm(2 \cdot 3 \cdot 17, 5 \cdot 7, 5 \cdot 11)$. Podemos reducir y obtener

$$n = 3417027 \equiv 537 \pmod{39270}.$$

Solución 2:

Nota del Coordinador

Esta solución está puesta para que podáis ver un método alternativo, pero sólo necesitáis aprender a resolver este problema usando la primera solución que, aunque es más larga que la segunda (recordad que a la que está aquí escrita hay que añadir la solución del Ejemplo 3) reduce un problema complejo a dos problemas básicos pueden ser largos, pero son sencillos.

Leandro Marín

Vamos a ver una segunda solución a este problema planteándolo como sistema de ecuaciones diofánticas. Vamos a llamar $n = x_0$ y reescribiremos las relaciones del enunciado como

$$x_0 = 27 + 102x_1$$

$$x_0 = 12 + 35x_2$$

$$x_0 = 42 + 55x_3$$

```
A = matrix(ZZ, [[1, -102, 0, 0], [1, 0, -35, 0], [1, 0, 0, -55]])
```

```
B = matrix(ZZ, [[27], [12], [42]])
```

```
Pol.<x0,x1,x2,x3,u0,u1,u2,u3,t> = ZZ[]
```

```
X = matrix(Pol, [[x0], [x1], [x2], [x3]])
```

```
AB = block_matrix([[A,B]])
```

```
ABR = copy(AB.echelon_form())
```

```
ABR.subdivide([], 4)
```

```
AA = ABR.subdivision(0, 0)
```

```
BB = ABR.subdivision(0, 1)
```

Escrito en forma matricial, estas relaciones son equivalentes a la ecuación matricial

$$\begin{pmatrix} 1 & -102 & 0 & 0 \\ 1 & 0 & -35 & 0 \\ 1 & 0 & 0 & -55 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 27 \\ 12 \\ 42 \end{pmatrix}$$

Construimos la ampliada del sistema y reducimos sobre el conjunto de los números enteros

$$\left(\begin{array}{cccc|c} 1 & -102 & 0 & 0 & 27 \\ 1 & 0 & -35 & 0 & 12 \\ 1 & 0 & 0 & -55 & 42 \end{array} \right) \rightarrow \left(\begin{array}{cccc|c} 1 & 0 & 0 & -55 & 42 \\ 0 & 102 & 0 & -55 & 15 \\ 0 & 0 & 35 & -55 & 30 \end{array} \right)$$

El sistema diofántico que tenemos que resolver en su forma reducida es

$$\begin{pmatrix} 1 & 0 & 0 & -55 \\ 0 & 102 & 0 & -55 \\ 0 & 0 & 35 & -55 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 42 \\ 15 \\ 30 \end{pmatrix}$$

```
AAt1 = block_matrix([[AA.T,1]])
AAt1R = copy(AAt1.echelon_form())
AAt1R.subdivide([],3)
Q = AAt1R.subdivision(0,1).T
U = matrix(Pol,[[u0],[u1],[u2],[u3]])
```

Para reolverlo vamos a hacer lo mismo que cuando tenemos una sola ecuación, vamos a sacar la matriz de paso por la derecha con una reducción por columnas. Para ello trasponemos y reducimos por filas

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 102 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 35 & 0 & 0 & 1 & 0 & 0 \\ -55 & -55 & -55 & 0 & 0 & 0 & 1 & 0 \end{array} \right) \rightarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 27335 & 268 & 781 & 497 \\ 0 & 0 & 5 & 16830 & 165 & 481 & 306 & 0 \\ 0 & 0 & 0 & 39270 & 385 & 1122 & 714 & 0 \end{array} \right)$$

La matriz de paso por la derecha es

$$Q = \begin{pmatrix} 1 & 27335 & 16830 & 39270 \\ 0 & 268 & 165 & 385 \\ 0 & 781 & 481 & 1122 \\ 0 & 497 & 306 & 714 \end{pmatrix}$$

y el teorema fundametal de la reducción por columnas nos dice que

$$\begin{pmatrix} 1 & 0 & 0 & -55 \\ 0 & 102 & 0 & -55 \\ 0 & 0 & 35 & -55 \end{pmatrix} \begin{pmatrix} 1 & 27335 & 16830 & 39270 \\ 0 & 268 & 165 & 385 \\ 0 & 781 & 481 & 1122 \\ 0 & 497 & 306 & 714 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 5 & 0 \end{pmatrix} = R'$$

Nuestro objetivo es encontrar un vector U tal que $X = QU$ sea la solución del sistema. Vamos a ver qué condiciones tendría que cumplir

$$\begin{pmatrix} 42 \\ 15 \\ 30 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -55 \\ 0 & 102 & 0 & -55 \\ 0 & 0 & 35 & -55 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 & -55 \\ 0 & 102 & 0 & -55 \\ 0 & 0 & 35 & -55 \end{pmatrix} \overbrace{\left(\begin{pmatrix} 1 & 27335 & 16830 & 39270 \\ 0 & 268 & 165 & 385 \\ 0 & 781 & 481 & 1122 \\ 0 & 497 & 306 & 714 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix} \right)}^X =$$

$$\underbrace{\left(\begin{pmatrix} 1 & 0 & 0 & -55 \\ 0 & 102 & 0 & -55 \\ 0 & 0 & 35 & -55 \end{pmatrix} \begin{pmatrix} 1 & 27335 & 16830 & 39270 \\ 0 & 268 & 165 & 385 \\ 0 & 781 & 481 & 1122 \\ 0 & 497 & 306 & 714 \end{pmatrix} \right)}_{R'} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 5 & 0 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} u_0 \\ u_1 \\ 5u_2 \end{pmatrix}$$

Tomando el principio y el final tenemos que $\begin{pmatrix} u_0 \\ u_1 \\ 5u_2 \end{pmatrix} = \begin{pmatrix} 42 \\ 15 \\ 30 \end{pmatrix}$ y de ahí deducimos que $u_0 = 42$, $u_1 = 15$, $u_2 = 6$ (la división en este caso es posible, si no hubiera sido posible el sistema no tendría solución) y u_3 puede tomar cualquier valor, por lo que la llamaremos t como solemos hacer a los parámetros libres. Esto nos dice que

$$X = \begin{pmatrix} 1 & 27335 & 16830 & 39270 \\ 0 & 268 & 165 & 385 \\ 0 & 781 & 481 & 1122 \\ 0 & 497 & 306 & 714 \end{pmatrix} \begin{pmatrix} 42 \\ 15 \\ 6 \\ t \end{pmatrix} = \begin{pmatrix} 39270t + 511047 \\ 385t + 5010 \\ 1122t + 14601 \\ 714t + 9291 \end{pmatrix}$$

El valor que realmente nos interesa es el de $x_0 = n$ que nos dice que es

$$n = 39270t + 511047$$

para un valor cualquiera de t , o lo que es lo mismo

$$n \equiv 511047 \pmod{39270}$$

Si reducimos para obtener el representante más pequeño, tenemos que

$$n \equiv 511047 \equiv 537 \pmod{39270}$$

que es el mismo valor que nos salía por el primer método.

Ejercicio 4. Encuentra todos los valores enteros n tales que

$$n \equiv 18 \pmod{34}$$

$$n \equiv 24 \pmod{25}$$

$$n \equiv 8 \pmod{28}$$

Solución:

3. DESPEJANDO n EN LAS CONGRUENCIAS.

En los problemas de Teorema Chino de los Restos necesitamos ecuaciones del tipo

$$n \equiv a \pmod{m}$$

o lo que es lo mismo, $n = a$ en \mathbb{Z}_m . A veces no tenemos las ecuaciones de esta forma y tenemos expresiones un poco más complicadas del tipo

$$5n + 4 \equiv 6 \pmod{7}$$

Si el módulo es primo como en este ejemplo, ésta ecuación se puede resolver despejando $5n = 6 - 4$ y por lo tanto $n = 5^{-1}(6 - 4) = 3 \cdot 2 = 6$ en \mathbb{Z}_7 . El inverso modular 5^{-1} se tiene que calcular en \mathbb{Z}_7 . Esto se puede hacer aunque el módulo no sea primo siempre que el inverso modular exista. Por ejemplo

Ejemplo 5. Despeja el valor de n en la siguiente relación de congruencia

$$128n + 65 \equiv 41 \pmod{4477}.$$

Solución:

El 65 no da problema porque lo podemos pasar restando al segundo miembro.

$$128n \equiv 41 - 65 = -24 \equiv 4553 \pmod{4477}$$

Para eliminar el 128 debemos comprobar si ese elemento es invertible módulo 4477 lo cual sucederá cuando el máximo común divisor entre 128 y 4477 sea 1. Podríamos hacerlo con un único comando en **sage** pero lo vamos a hacer usando el algoritmo de euclides extendido.

```
A = matrix(ZZ, [[218, 4477]])
At1 = block_matrix([[A.T, 1]])
At1R = copy(At1.echelon_form())
At1R.subdivide([], [1])
Q = At1R.subdivision(0, 1).T
```

Procedemos como en el caso de las ecuaciones diofánticas.

$$\left(\begin{array}{c|cc} 218 & 1 & 0 \\ 4477 & 0 & 1 \end{array} \right) \rightarrow \left(\begin{array}{c|cc} 1 & 3635 & -177 \\ 0 & 4477 & -218 \end{array} \right)$$

Calculamos la matriz de paso por la derecha Q y el teorema fundamental de la reducción por columnas nos dice que

$$Q = \begin{pmatrix} 3635 & 4477 \\ -177 & -218 \end{pmatrix} \quad \left(\begin{array}{cc} 218 & 4477 \end{array} \right) \begin{pmatrix} 3635 & 4477 \\ -177 & -218 \end{pmatrix} = \left(\begin{array}{cc} 1 & 0 \end{array} \right)$$

El máximo común divisor es 1 y el Lema de Bézout nos dice que

$$1 = 218 \cdot 3635 + 4477 \cdot (-177)$$

por lo que 3635 es el inverso modular de 218 módulo 4477.

También podemos tener el caso en que el coeficiente que multiplica a n no sea invertible. En ese caso procederemos del siguiente modo:

Ejemplo 6. *Despeja el valor de n en la siguiente relación de congruencia:*

$$165n \equiv 3618 \pmod{4551}$$

Solución:

Esta relación es equivalente a decir que $165n = 3618 + 4551t$ para algún valor de t . Vamos a ver si 165 es invertible módulo 4551 calculando el máximo común divisor de 165 y 4551.

```
A = matrix(ZZ, [[165, 4551]])
```

```
R = A.T.echelon_form()
```

Tomamos la matriz columna con ambos valores y reducimos:

$$\left(\begin{array}{c} 165 \\ 4551 \end{array} \right) \rightarrow \left(\begin{array}{c} 3 \\ 0 \end{array} \right)$$

Esto nos dice que el máximo común divisor es 3 y vamos a dividir toda la ecuación $165n = 3618 + 4551t$ por 3.

$$55n = 1206 + 1517t$$

Todos los términos han resultado ser divisibles por 3 (para 165 y 4551 estábamos seguros porque 3 era su máximo común divisor, pero podría haber fallado para el término independiente 3618 en cuyo caso no habría ningún n cumpliendo las condiciones). La ecuación $55n = 1206 + 1517t$ para algún valor de t es equivalente a

$$55n \equiv 1206 \pmod{1517}$$

con la ventaja de que ahora el máximo común divisor de 55 y 1517 sí es 1 y por lo tanto podemos calcular el inverso modular de 55 módulo 1517 y proceder como en el ejemplo anterior, o directamente poner

$$n \equiv 55^{-1} \cdot 1206 \equiv 331 \cdot 1206 \equiv 215 \pmod{1517}.$$

Ejercicio 5. *Despeja del valor de n en las siguientes relaciones de congruencia:*

- (1) $5n + 1 \equiv 4 \pmod{7}$
- (2) $45n - 23 \equiv 44 \pmod{121}$
- (3) $15n - 4 \equiv 6 \pmod{20}$
- (4) $814n + 14 \equiv 4343 \pmod{4551}$

Solución:

- (1) $5n + 1 \equiv 4 \pmod{7}$
- (2) $45n - 23 \equiv 44 \pmod{121}$
- (3) $15n - 4 \equiv 6 \pmod{20}$
- (4) $814n + 14 \equiv 4343 \pmod{4551}$

4. EJERCICIOS ADICIONALES

Ejercicio 6 (Examen Junio 2024). *En nuestro almacén recibimos furgonetas pequeñas con una capacidad de 108 ordenadores y salen furgonetas grandes con una capacidad de 201 ordenadores. En este momento tenemos en el almacén 74 ordenadores, pero sospechamos que podríamos haber sufrido un robo de un ordenador. Sabiendo que las furgonetas siempre van al máximo de su capacidad determina si efectivamente hemos sufrido ese robo y cuantas furgonetas han podido entrar y salir del almacén.*

Solución: