AMD Curso 2023-2024

Tarea Semana 3

Ejercicio 1. *Calcula, usando la reducción de matrices, el inverso de* 76860393 *en* $\mathbb{Z}_{433362740}$.

Solución.-

```
A = matrix(ZZ, [[x1], [n1]])
Ap = block_matrix([[A, 1]])
Ar = Ap.echelon_form()
Ar = copy(Ar)
Ar.subdivide([], 1)
S = Ar.subdivision(0, 1)
R = S * A
```

$$A' = [A|I] = \left(\begin{array}{r|rr} 76860393 & 1 & 0 \\ 433362740 & 0 & 1 \end{array}\right)$$

$$\left(\begin{array}{r|rr} 1 & 332767437 & -59019001 \\ 0 & 433362740 & -76860393 \end{array}\right)$$

El $\operatorname{mcd}(76860393, 433362740) = 1$, por tanto es invertible.

$$\begin{pmatrix} 332767437 & -59019001 \\ 433362740 & -76860393 \end{pmatrix} \begin{pmatrix} 76860393 \\ 433362740 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

La expresión del mcd de 76860393 y 433362740

$$332767437 \cdot 76860393 + (-59019001) \cdot 433362740 = 1$$

$$332767437 \cdot 76860393 = 1$$

$$76860393^{-1} = 332767437 \text{ en } (\mathbb{Z}_{433362740})$$

Ejercicio 2. *Dada la ecuación* $19165x + 18666y = 145$, *indica si tiene solución y (caso de tener) calcula todas las posibles soluciones.*

Solución.-

```
A = matrix(ZZ, [[a2], [b2]])
Ap = block_matrix([[A, 1]])
Ar = Ap.echelon_form()
R = Ar[:, 1:] * A
```

$$A' = [A|I] = \left(\begin{array}{r|rr} 19165 & 1 & 0 \\ 18666 & 0 & 1 \end{array}\right)$$

reducida

$$\begin{pmatrix} 1 & 16459 & -16899 \\ 0 & 18666 & -19165 \end{pmatrix}$$

$\mathrm{mcd}(19165, 18666) = 1$ es divisor de 145, por tanto hay solución.

$$\begin{pmatrix} 16459 & -16899 \\ 18666 & -19165 \end{pmatrix} \begin{pmatrix} 19165 \\ 18666 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Desarrollar

$$16459 \cdot 19165 + (-16899) \cdot 18666 = 1$$
$$18666 \cdot 19165 + (-19165) \cdot 18666 = 0$$

Multiplicar primera relación por m para tener m, y segunda relación por t

$$16459 \cdot 19165 \cdot 145 + (-16899) \cdot 18666 \cdot 145 = 145$$
$$18666 \cdot 19165 \cdot t + (-19165) \cdot 18666 \cdot t = 0$$

Sumar las dos

$$19165(2386555 + 18666t) + 18666(-2450355 - 19165t) = 145$$

Extraer x e y

$$x = 2386555 + 18666t$$
$$y = -2450355 - 19165t$$

Ejercicio 3. *Obtener todas las soluciones del siguiente sistema de congruencias:*

$$n \equiv 1792944400 \pmod{4959384998}$$
$$n \equiv 16054429802 \pmod{18622220374}$$

Solución.-

```
A = matrix(ZZ, [[m31], [-m32]])
Ap = block_matrix([[A, 1]])
Ar = Ap.echelon_form()
Ar = copy(Ar)
Ar.subdivide([], 1)
As = Ar[:, 1:]
R = Ar[:, :1]

mcd = R[0, 0]

a3n = 1792944400
b3n = 16054429802
d = b3n - a3n
```

```
F = d / mcd

c3 = a3n + (m31 * As[0, 0] * F)
cm3 = m31 * As[1, 0]
```

mcd(4959384998, 18622220374)

$$[A|I] = \left(\begin{array}{r|rr} 4959384998 & 1 & 0 \\ -18622220374 & 0 & 1 \end{array}\right)$$

reducida

$$\left(\begin{array}{r|rr} 2002174 & 5884 & 1567 \\ 0 & 9301 & 2477 \end{array}\right)$$

mcd(4959384998, 18622220374) = 2002174 $\neq 1$ es un caso 2

$$n = 1792944400 + 4959384998x$$
$$n = 16054429802 + 18622220374y$$

$$1792944400 + 4959384998x = 16054429802 + 18622220374y$$

$$4959384998x - 18622220374y = 14261485402 = d$$

$$F = \frac{14261485402}{2002174} = 7123$$

El mcd es divisor de d, por tanto hay solución

$$\begin{pmatrix} 5884 & 1567 \\ 9301 & 2477 \end{pmatrix} \cdot \begin{pmatrix} 4959384998 \\ -18622220374 \end{pmatrix} = \begin{pmatrix} 2002174 \\ 0 \end{pmatrix}$$

$$5884 \cdot 4959384998 + 1567 \cdot (-18622220374) = 2002174$$
$$9301 \cdot 4959384998 + 2477 \cdot (-18622220374) = 0$$

Multiplicar la de arriba para dar d, y abajo por t

$$5884 \cdot 4959384998 \cdot 7123 + 1567 \cdot (-18622220374) \cdot 7123 = 14261485402$$
$$9301 \cdot 4959384998 \cdot t + 2477 \cdot (-18622220374) \cdot t = 0$$

Al sumarlas

$$4959384998(41911732 + 9301t) - 18622220374(11161741 + 2477t) = 14261485402$$

$$x = 41911732 + 9301t$$
$$y = 11161741 + 2477t$$

$$
\begin{aligned}
n &= 1792944400 + 4959384998x = 1792944400 + 4959384998(41911732 + 9301t) \\
&= 207856416713940936 + 46127239866398t \\
&= 207856416713940936 \pmod{46127239866398}
\end{aligned}
$$