1. Ecuaciones lineales en cuerpos finitos

Un *cuerpo* es un conjunto $\mathbb{F}$ dotado de dos operaciones suma y producto, usualmente denotadas por $+$ y $\cdot$ que satisfacen los axiomas de los números reales, exceptuando los relativos al orden. Más precisamente, se cumplen

(S1) la suma es asociativa: $a + (b + c) = (a + b) + c$;

(S2) la suma es conmutativa: $a + b = b + a$;

(S3) la suma tiene un elemento nulo $0 \in \mathbb{F}$ tal que $a + 0 = a$;

(S4) existen los opuestos: para cada $a \in \mathbb{F}$ existe $-a \in \mathbb{F}$ tal que $a + (-a) = 0$;

(P1) el producto es asociativo: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(P1) el producto es conmutativo: $a \cdot b = b \cdot a$;

(P3) el producto tiene un elemento neutro $1 \in \mathbb{F}$, $1 \neq 0$, tal que $a \cdot 1 = a$;

(P4) existen los inversos de elementos no nulos: para cada $a \in \mathbb{F}$, $a \neq 0$, existe $a^{-1} \in \mathbb{F}$ tal que $a \cdot a^{-1} = 1$;

(D) propiedad distributiva: $a \cdot (b + c) = a \cdot b + a \cdot c$,

para todos $a, b, c \in \mathbb{F}$. Notar que al igual que hacemos con los números reales, el producto $a \cdot b$ entre los elementos a y b de $\mathbb{F}$ se denota simplemente por ab.

Observar que cualquier propiedad que hayamos probado para los números reales (o complejos o racionales) usando los axiomas (S1), ..., (S4), (P1), ..., (P4), (D) también será válida para un cuerpo arbitrario $\mathbb{F}$.

Ejemplo 1.1. Los números racionales $\mathbb{Q}$, reales $\mathbb{R}$ y complejos $\mathbb{C}$ forman cuerpos con las operaciones usuales.

Ejemplo 1.2. Consideremos el subconjunto de los números reales definido por

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Entonces $\mathbb{Q}[\sqrt{2}]$ es un cuerpo con las operaciones heredadas de $\mathbb{R}$. En primer lugar observemos que las operaciones están bien definidas. En efecto, si $a, b, c, d \in \mathbb{Q}$, entonces

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

y

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

A partir de esto, es muy fácil verificar que se satisfacen todas las propiedades de la suma y el producto (pues ya sabemos que se satisfacen en $\mathbb{R}$). La única propiedad no trivial es (P4), sobre la existencia de inversos. Para verificar esto, observemos primero que $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ es nulo si y sólo si $a = b = 0$. Si así no fuera, tendríamos que $a \neq 0$, $b \neq 0$ y por ende $\sqrt{2} = -a/b$ sería un número racional, lo cual es absurdo. Para encontrar el inverso multiplicativo de $a + b\sqrt{2}$ en $\mathbb{Q}[\sqrt{2}]$ debemos encontrar $c, d \in \mathbb{Q}$ tales que

$(a+b\sqrt{2})(c+d\sqrt{2}) = 1$. Esto se hace usando el llamado procedimiento de racionalización en los números reales

$$\begin{aligned}\frac{1}{a+b\sqrt{2}} &= \frac{1}{(a+b\sqrt{2})}\frac{(a-b\sqrt{2})}{(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-ab\sqrt{2}+ba\sqrt{2}-2b^2} \\ &= \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}.\end{aligned}$$

Luego, si $c = a/(a^2-2b^2)$ y $d = -b/(a^2-2b^2)$, entonces $1/(a+b\sqrt{2}) = c+d\sqrt{2}$. Es decir, el inverso multiplicativo en $\mathbb{R}$ de $a+b\sqrt{2}$ es un elemento de $\mathbb{Q}[\sqrt{2}]$. Dejamos como ejercicio para el alumno verificar que si $a, b \in \mathbb{Q}$, entonces $a^2-2b^2 \neq 0$.

Ejemplo 1.3. Consideremos en el conjunto de dos elementos $\mathbb{Z}_2 = \{0,1\}$ la operaciones de suma y producto definidas por las siguientes tablas

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Es fácil verificar que $\mathbb{Z}_2$ con estas operaciones forma un cuerpo, en el cual 0 es el elemento nulo de la suma y 1 es el elemento neutro para el producto. Observar que en este cuerpo se satisface la relación $1+1=0$. Esto también puede expresarse como $1=-1$.

Observemos también que en $\mathbb{Z}_2$ no puede definirse un orden compatible con las operaciones de suma y producto. Es decir, no puede definirse un orden $<$ tal que $a+c<b+c$ y $ac<bc$ para $c>0$. En efecto, como $\mathbb{Z}_2$ tiene solo dos elementos, sólo tenemos dos posibles órdenes: uno tal que $0<1$ y otro tal que $1<0$. En el primer caso tenemos que $0<1$ implicaría $0+1<1+1$ o sea $1<0$ y en el segundo $1<0$ implica $1+1<0+1$, es decir, $0<1$. En ambos casos se llega a una contradicción, por lo cual no existe en $\mathbb{Z}_2$ un orden compatible con la suma.

Observar que en un cuerpo $\mathbb{F}$, uno puede sumar reiteradas veces el elemento neutro $1 \in \mathbb{F}$. En algunos casos, por ejemplo cuando $\mathbb{F} = \mathbb{R}$, con este procedimiento se obtienen los números naturales

$$1,\ 1+1=2,\ 1+1+1=3,\ 1+1+1+1=4,\ 1+1+1+1+1=5,\ldots$$

y en otros casos como en ejemplo anterior $\mathbb{F} = \mathbb{Z}_2$, uno obtiene que la suma iterada de 1 empieza a repetirse

$$1,\ 1+1=0,\ 1+1+1=1,\ 1+1+1+1=0, 1+1+1+1+1=1,\ldots.$$

Esto permite definir la llamada *característica* de un cuerpo $\mathbb{F}$. Decimos que $\mathbb{F}$ tiene característica p, si p es el menor natural tal que

$$\underbrace{1+1+1+\cdots+1}_{p \text{ veces}} = 0.$$

Si no existe p con esta propiedad, decimos que $\mathbb{F}$ tiene característica 0. Equivalentemente, en un cuerpo de característica 0, la suma del 1 una cantidad finita de veces es siempre no nula.

Ejemplo 1.4. $\mathbb{R}$ tiene característica 0 pues $n < n+1$ para todo $n \in \mathbb{N}$. $\mathbb{Z}_2$ tiene característica 2 pues en este cuerpo $1 \neq 0$ y $1+1=0$.

Teorema 1.5. *Si $\mathbb{F}$ es un cuerpo de característica $p \neq 0$, entonces p es un número primo.*

Demostración. Recordemos que un número natural $p \geq 2$ se dice primo si cada vez que escribimos $p = ab$ como producto de dos números naturales a y b, entonces $a = 1$ o $b = 1$. Supongamos por el absurdo que existen $a, b \in \mathbb{N}$ tales que $a \neq 1$, $b \neq 1$ y $p = ab$. Entonces, usando la propiedad asociativa de la suma y la propiedad distributiva obtenemos que

$$\begin{aligned} 0 &= 1+1+\cdots+1 \quad (p \text{ veces}) \\ &= \underbrace{(1+\cdots+1)}_{a \text{ veces}} + \cdots + \underbrace{(1+\cdots+1)}_{a \text{ veces}} \quad (b \text{ veces}) \\ &= \underbrace{(1+\cdots+1)}_{a \text{ veces}} \underbrace{(1+\cdots+1)}_{b \text{ veces}}, \end{aligned}$$

de donde sigue que $\underbrace{1+\cdots+1}_{a \text{ veces}} = 0$ o bien $\underbrace{1+\cdots+1}_{b \text{ veces}} = 0$. Absurdo, pues $a < p$, $b < p$ y p es el menor natural tal que 1 sumado p veces es igual a 0. □

Observación 1.6. Para cada primo p existe un cuerpo con p elementos, al cual denotaremos por $\mathbb{Z}_p$. A continuación mostramos cómo construir este cuerpo. Consideremos en primer lugar el conjunto

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}.$$

Las operaciones suma y producto en $\mathbb{Z}_p$ son las llamadas operaciones de la aritmética módulo p. Es decir, para calcular la suma $a+b$ de dos elementos $a+b \in \mathbb{Z}_p$, se calcular la suma en $\mathbb{Z}$, pero el resultado se considera el resto de hacer la división entera de $a+b$ por p. Con respecto a la división entera por p, recordar que siempre existen $q, r \in \mathbb{Z}$ tales que

$$a+b = qp+r, \qquad 0 \leq r < p,$$

en donde q es el cociente de la división por p y r el resto. Así, la suma en $\mathbb{Z}_p$ es

$$a+b = r.$$

Análogamente, para calcular el producto ab en $\mathbb{Z}_p$ se calcula el producto en $\mathbb{Z}$, pero se toma el resto de éste cuando lo dividimos por p.

No es difícil ver, usando propiedades de la división entera, que $\mathbb{Z}_p$ es un cuerpo con las operaciones así definidas.

Ejemplo 1.7. Veamos las tablas de sumar y multiplicar en $\mathbb{Z}_3 = \{0, 1, 2\}$.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Así, por ejemplo, para calcular $1+2$, hacemos la suma en $\mathbb{Z}$ (la cual da 3 y tiene resto 0 dividido 3), por ende $1+2=0$. Equivalentemente, $-1=2$. Similarmente, cuando calculamos $2 \cdot 2$ hacemos el producto en $\mathbb{Z}$ (el cual da 4 y tiene resto 1 dividido 3), por ende $2 \cdot 2 = 1$. Equivalentemente, $2^{-1} = 2$ en $\mathbb{Z}_3$

Ejemplo 1.8. Para $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ se tiene

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ejemplo 1.9. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ no es un cuerpo con las operaciones dadas por la aritmética módulo 4. En efecto, si bien se satisfacen todos los axiomas de la suma, no es cierto que todo elemento no nulo tenga inverso: el elemento $2 \in \mathbb{Z}_4$ no tiene inverso multiplicativo pues

$$2 \cdot 0 = 0, \qquad 2 \cdot 1 = 2, \qquad 2 \cdot 2 = 0, \qquad 2 \cdot 3 = 4$$

y por ende no existe $b \in \mathbb{Z}_4$ tal que $2 \cdot b = 1$.

A continuación vemos un caso particular del teorema del binomio para cuerpos de característica p.

Teorema 1.10. *Sea $\mathbb{F}$ un cuerpo de característica $p \neq 0$, entonces para todos $a, b \in \mathbb{F}$ vale*

$$(a + b)^p = a^p + b^p.$$

Demostración. Observemos que para cualquier cuerpo $\mathbb{F}$ vale el teorema del binomio: para todo $n \in \mathbb{N}$,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k},$$

en donde a^k significa elevar a la k en $\mathbb{F}$, es decir multiplicar a por sí mismo k veces (ídem con b^{n-k}) y la notación

$$\binom{n}{k} a^k b^{n-k}$$

significa sumar $\binom{n}{k}$ veces el elemento $a^k b^{n-k}$. En particular, para $n = p$ tenemos

$$(a + b)^p = \binom{p}{0} b^p + \binom{p}{1} a b^{p-1} + \binom{p}{2} a^2 b^{p-2} + \cdots + \binom{p}{p-1} a^{p-1} b + \binom{p}{p} a^p.$$

Ahora bien, observemos que para cada $1 \leq k \leq p - 1$, el número combinatorio

$$\binom{p}{k} = \frac{p!}{(p-k)!k!}$$

es divisible por p (probar esto como ejercicio), es decir, existe $n_k \in \mathbb{N}$ tal que $\binom{p}{k} = p n_k$ y por ende $\binom{p}{k} a^k b^{n-k} = 0$ en $\mathbb{Z}_p$ para todo $k = 1, \ldots, p - 1$. Así, la expresión anterior se simplifica en

$$(a + b)^p = a^p + b^p$$

como queríamos probar. □

En lo que sigue mostraremos como trabajar con matrices con coeficientes en $\mathbb{Z}_p$ y por ende como resolver ecuaciones lineales en $\mathbb{Z}_p$. Como $\mathbb{Z}_p$ es un cuerpo para todo p primo, toda la teoría desarrollada sobre matrices y determinantes seguirá siendo valida si consideramos matrices con coeficientes en $\mathbb{Z}_p$, pero hay que tener algunas precauciones. Por ejemplo si $A \in (\mathbb{Z}_p)^{n\times n}$ y B es la matriz que se obtiene de A intercambiando la fila 1 con la fila 2, entonces $\det B = -\det A = (-1)\det A$, pero en $\mathbb{Z}_p$, el opuesto de 1 es $p-1$, pues $1 + (p-1) = 0$, luego

$$\det B = (p-1)\det A.$$

Ejemplo 1.11. Consideremos la matriz $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ con coeficientes en $\mathbb{Z}_2$. Observemos que si intercambiamos la fila 1 con la fila 2 se obtiene la matriz identidad. Por lo tanto

$$\det A = (-1)\det I = \det I = 1 \neq 0,$$

de donde se concluye que A es invertible.

Ejemplo 1.12. Sea la matriz $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ con coeficientes en $\mathbb{Z}_2$.

1. Decidir si A es invertible.
2. Resolver el sistema lineal $AX = 0$ sobre $\mathbb{Z}_2$.

Utilizamos operaciones elementales por fila para llevar A a una matriz escalón reducida por filas y así responder ambos ítems a la vez.

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} = R.$$

Observar que la forma reducida R de A tiene la última fila nula y por lo tanto ni R ni A son invertibles. Además el sistema $AX = 0$,

$$\begin{cases} x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \\ x_2 + x_3 = 0 \end{cases}$$

es equivalente a

$$\begin{cases} x_1 + x_3 = 0 \\ x_2 + x_3 = 0 \end{cases}$$

de donde sigue que $x_1 = x_2 = -x_3 = x_3$. Luego el conjunto de soluciones del sistema $AX = 0$ es

$$\text{Sol} = \{(x_3, x_3, x_3) : x_3 \in \mathbb{Z}_2\} = \{(0,0,0), (1,1,1)\}.$$

Observar entonces que $AX = 0$ es un sistema compatible indeterminado, pero no tiene infinitas soluciones (nunca podría tenerlas pues $\mathbb{Z}_2$ es un cuerpo finito).

Ejemplo 1.13. Sea la matriz $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ con coeficientes en $\mathbb{Z}_3$.

1. Decidir si A es invertible.
2. Resolver el sistema lineal $AX = Y$ sobre $\mathbb{Z}_3$, donde $Y = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$.

Esta vez utilizaremos el método de la adjunta. Dejamos como ejercicio verificar que

$$\det A = 1 \neq 0$$

y por ende A es invertible, y que

$$\operatorname{adj} A = \begin{pmatrix} -1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 2 \end{pmatrix}.$$

Luego

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 2 \end{pmatrix}$$

y el sistema $AX = Y$ tiene solución única

$$Y = A^{-1}Y = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2+2 \\ 1+2\cdot 2 \\ 2+2\cdot 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}.$$

Los ejemplos anteriores son casos particulares de las llamadas matrices de Hankel. Estas matrices se caracterizan por tener las antidiagonales constantes y por ende resultan simétricas. Otros ejemplos notables de matrices de Hankel son las matrices $p \times p$ que se obtienen de la tabla de la suma en $\mathbb{Z}_p$. Es decir, nos referimos a una matriz A tamaño $p \times p$ tal que $A_{ij} = (i-1) + (j-1)$. Para los casos $p = 2, 3, 5$ hemos dado explícitamente las tablas de la suma en $\mathbb{Z}_p$, luego las correspondientes matrices de Hankel son

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in (\mathbb{Z}_2)^{2\times 2}, \qquad \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \in (\mathbb{Z}_3)^{3\times 3}, \qquad \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} \in (\mathbb{Z}_5)^{5\times 5}.$$

Proposición 1.14. *Sea p un número primo, $p \neq 2$, y sea $A \in (\mathbb{Z}_p)^{p\times p}$ la matriz de Hankel dada por $A_{ij} = (i-1) + (j-1)$. Entonces* $\det A = 0$.

Demostración. Aplicamos a la matriz A las operaciones elementales por filas $e_1, \ldots, e_{p-1}$ donde $e_i =$ "$\mathtt{f_p} \to \mathtt{f_p} + \mathtt{f_i}$", es decir, e_i es la operación elemental que a la fila p les suma la fila i. Llamemos a la matriz obtenida $B = e_{p-1}(\ldots(e_2(e_1(A)))\ldots)$. Observemos que como en cada columna de A aparecen, en distinto orden, todos los elementos $0, 1, \ldots, p-1$,

entonces la última fila B tiene todos sus coeficientes iguales a $0+1+2+\cdots+(p-1)$. Para calcular este valor usamos la conocida fórmula

$$1+2+\cdots+(p-1)=\frac{1}{2}(p-1)p.$$

Ahora bien, en $\mathbb{Z}_p$ tenemos que $1/2=(p+1)/2$ (el cual está bien definido, pues al ser p un primo impar, $p+1$ es un número par) y $p=0$. Luego B tiene la última fila nula y por lo tanto $\det A=\det B=0$. □

A continuación mostramos algunos ejemplos de aplicación de sistemas de ecuaciones lineales con coeficientes en $\mathbb{Z}_p$.

Ejemplo 1.15. Se sabe que el sistema de ecuaciones lineales sobre $\mathbb{Q}$ dado por

$$\begin{cases} 100000x+99999y=1231244 \\ 100001x+100000y=1120021 \end{cases}$$

tiene solución única con x,y enteros. Determinar la paridad de la solución. Para resolver este problema observemos que una la solución del sistema anterior será solución del sistema con coeficientes en $\mathbb{Z}_2$. Notar que en $\mathbb{Z}_2$ se tiene

$$100000=1231244=0 \qquad \text{y} \qquad 100001=99999=1120021=1,$$

luego, debemos estudiar sobre $\mathbb{Z}_2$ el sistema

$$\begin{cases} 0x+1y=0 \\ 1x+0y=1 \end{cases}$$

de donde claramente se desprende que $x=1$ e $y=0$. Esto significa que en la solución del sistema original sobre $\mathbb{Q}$, x es impar e y es par.

Ejemplo 1.16. Determinar qué día de la semana fue el 20 de noviembre del año pasado. Al momento de escribir estas notas estamos en el 20 de noviembre de 2015 y es viernes. Podemos resolver este problema resolviendo una ecuación en $\mathbb{Z}_7$ como sigue: asignamos números del 0 al 6 a los días de la semana

$$\begin{aligned} 0&=\text{domingo} \\ 1&=\text{lunes} \\ 2&=\text{martes} \\ 3&=\text{miércoles} \\ 4&=\text{jueves} \\ 5&=\text{viernes} \\ 6&=\text{sábado} \end{aligned}$$

Luego, si al 20 de noviembre de 2014 le corresponde el día x, entonces (ya que 2015 no es bisiesto), tenemos que

$$x+365=5$$

pues hoy es viernes 20 de noviembre. Ahora bien, observar que en $\mathbb{Z}_7$ tenemos que $365 = 52 \cdot 7 + 1 = 1$. Luego

$$x = 5 - 365 = 5 - 1 = 5 + 6 = 4,$$

de donde sigue que el 20 de noviembre de 2014 fue jueves.

Ejemplo 1.17. Determinar qué día de la semana fue el 20 de noviembre de 1810. Aquí conviene hacer una breve digresión sobre el calendario gregoriano, que es el que usamos en la actualidad. El calendario gregoriano, promovido por el Papa Gregorio XIII, sustituyó a partir de 1582 al llamado calendario juliano. El calendario gregoriano distingue entre años comunes de 365 días y años bisiestos de 366 días. Además están los llamados años seculares, que son los años múltiplos de 100, por ejemplo 1800, 1900, 2000, 2100. Los años bisiestos son aquellos que son múltiplo de 4, como por ejemplo 2012, 2016, 2020. Pero hay una excepción con respecto a los años seculares: un año secular es bisiesto sólo si es múltiplo de 400, así, por ejemplo, los años 1800 y 1900 no son bisiestos, en tanto que el año 2000 sí es bisiesto.

Ahora bien, supongamos que al 20 de noviembre de 1810 le corresponde el día $x \in \mathbb{Z}_7$ (usando identificación de los días de la semana con los elementos $0, 1, \ldots, 6$ que vimos en el ejemplo anterior) y contemos cuántos días pasaron hasta el 20 de noviembre de 2015. Antes que nada, observemos que desde 1810 hasta 2015 transcurrieron $2015 - 1810 = 205$ años, luego desde x hasta el 20 de noviembre de 2015 transcurrieron $205 \cdot 365 + N$ días, donde N es la cantidad de años bisiestos entre 1810 y 2015. Notar que 1810 no es múltiplo de 4 y por ende este año no es bisiesto. Luego el último año bisiesto antes de 1810 es 1808 y el último año bisiesto antes de 2015 es 2012. Luego entre 1810 y 2015 hay

$$\frac{2012 - 1808}{4} - 1 = 50$$

años bisiestos (observar que excluimos al año secular 1900 que no es bisiesto). Así tenemos que transcurrieron $205 \cdot 365 + 50$ días desde el 20 de noviembre de 1810 hasta el 20 de noviembre de 2015. Además en $\mathbb{Z}_7$ tenemos que

$$365 = 52 \cdot 7 + 1 = 1, \qquad 205 = 29 \cdot 7 + 2 = 2, \qquad 50 = 7 \cdot 7 + 1 = 1,$$

y como el 20 de noviembre de 2015 es viernes, al cual le corresponde el número 5, tenemos que

$$5 = x + 205 \cdot 365 + 50 = x + 3$$

de donde sigue que $x = 2$ y por ende el 20 de noviembre de 1810 fue martes.

Finalizamos estas notas con una observación sobre funciones polinomiales sobre $\mathbb{Z}_p$. Dado un cuerpo arbitrario $\mathbb{F}$, una función $Q : \mathbb{F} \to \mathbb{F}$ se dice una *función polinomial* (a veces llamada simplemente un polinomio) si tiene la forma

$$Q(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

para algún $n \geq 0$ y ciertos $a_0, a_1, \ldots, a_n \in \mathbb{F}$. Observemos que no necesariamente una función $f : \mathbb{F} \to \mathbb{F}$ es polinomial. Por ejemplo, si $\mathbb{F} = \mathbb{R}$ y consideramos la función $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = 2^x$, entonces f no es polinomial. Una forma de ver esto es

la siguiente: del análisis matemático sabemos que $f(x) = e^{x \log 2}$, y por tanto, la n-ésima derivada de $f(x)$ es

$$f^{(n)}(x) = (\log 2)^n \, 2^x.$$

Luego, todas las derivadas de $f(x)$ son no nulas. Esto muestra $f(x)$ no es un polinomio, pues las derivadas de un polinomio a coeficientes reales se anulan eventualmente (cuando derivamos más veces que el grado del polinomio).

Sin embargo, la situación es muy diferente para cuerpos como $\mathbb{F} = \mathbb{Z}_p$ (donde no tenemos una noción clara de derivada), como se desprende del siguiente teorema.

Teorema 1.18. *Toda función $f : \mathbb{Z}_p \to \mathbb{Z}_p$ es una función polinomial.*

Para poder demostrar este teorema usaremos el siguiente resultado general.

Lema 1.19. *Sea $\mathbb{F}$ u cuerpo y sean $a_1, \ldots, a_n \in \mathbb{F}$. Consideremos la matriz $V \in \mathbb{F}^{n \times n}$ dada por*

$$V = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}.$$

Entonces

$$\det V = \prod_{i<j} (a_j - a_i).$$

En particular, si $a_1, \ldots, a_n$ son todos distintos, entonces V es invertible.

Demostración. Ejercicio. □

La matriz V definida en el lema anterior es llamada matriz de Vandermonde asociada a los escalares $a_1, \ldots, a_n$.

Demostración del Teorema 1.18. Se plantea la existencia de un polinomio

$$Q(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1} x^{p-1}$$

tal que $Q(x) = f(x)$ para todo $x \in \mathbb{Z}_p$. Esto lleva naturalmente al sistema de p ecuaciones con p incógnitas $a_0, a_1, \ldots, a_{p-1}$ dado por

$$\begin{aligned} f(0) &= a_0 + a_1 0 + a_2 0^2 + \cdots + a_{p-1} 0^{p-1} \\ f(1) &= a_0 + a_1 1 + a_2 1^2 + \cdots + a_{p-1} 1^{p-1} \\ f(2) &= a_0 + a_1 2 + a_2 2^2 + \cdots + a_{p-1} 2^{p-1} \\ &\vdots \\ f(p-1) &= a_0 + a_1 (p-1) + a_2 (p-1)^2 + \cdots a_{p-1} (p-1)^{p-1} \end{aligned}$$

Observar que la matriz de este sistema es

$$\begin{pmatrix} 1 & 0 & 0^2 & \cdots & 0^{p-1} \\ 1 & 1 & 1^2 & \cdots & 1^{p-1} \\ 1 & 2 & 2^2 & \cdots & 2^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & p-1 & (p-1)^2 & \cdots & (p-1)^{p-1} \end{pmatrix},$$

es decir, la matriz de Vandermonde asociada a los elementos (distintos) $0, 1, 2, \ldots, p-1$ de $\mathbb{Z}_p$, la cual resulta invertible por el lema anterior. Por consiguiente, existen únicos $a_0, a_1, a_2, \ldots, a_{p-1} \in \mathbb{Z}_p$ tales que $Q(x) = f(x)$. □

Nota 1.20. Observar que la demostración del teorema nos dice que dada una función $f : \mathbb{Z}_p \to \mathbb{Z}_p$, existe un único polinomio $Q(x)$ de grado a lo sumo $p-1$ tal que $Q(x) = f(x)$ para todo x.

Ejemplo 1.21. Sea $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ dada por $f(x) = 2^x$. Encontrar un polinomio $Q(x)$ de grado a lo sumo 2, con coeficientes en $\mathbb{Z}_3$, tal que $Q(x) = f(x)$. Escribimos

$$Q(x) = ax^2 + bx + c.$$

Observemos que

$$f(0) = 2^0 = 1, \qquad f(1) = 2^1 = 2, \qquad f(2) = 2^2 = 1.$$

Luego, debemos resolver el sistema lineal

$$\begin{cases} a0^2 + b0 + c = 1 \\ a1^2 + b1 + c = 2 \\ a2^2 + b2 + c = 1 \end{cases}$$

o en forma matricial

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}.$$

Pasamos a la matriz ampliada y la llevamos a su forma escalón reducida por filas

$$\left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 2 \\ 1 & 2 & 1 & 1 \end{array}\right) \to \left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 2 & 0 & 0 \end{array}\right) \to \left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 2 \end{array}\right)$$

$$\to \left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 2 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right),$$

de donde sigue que $a = b = 2$ y $c = 1$. Luego

$$Q(x) = 2x^2 + 2x + 1 = 2^x$$

para todo $x \in \mathbb{Z}_3$.