Definición de polinomio

Definición (Polinomios con coeficientes en A)

Sea A un anillo. Llamaremos conjunto de polinomios con coeficientes en A, y lo denotaremos por A[x], al conjunto de las expresiones de la forma

$$a(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$$

con los $a_i \in A$ y $m \in N$.

Grado de un polinomio

Definición (Grado)

El grado de un polinomio *a(x)*, notado *grado(a(x))*, es el mayor entero n tal que $a_n \neq 0$. El polinomio cuyos coeficientes son todos nulos se llama **polinomio nulo** y se denota por 0. Por convención, su grado es grado(0) = $-\infty$.

Definiciones

Sea $a(x) = \sum_{i=0}^{n} a_i x^i \in k[x]$ un polinomio no nulo con $a_n \neq 0$ (de grado n).

Llamaremos **término líder** de a(x) al término $a_n x^n$, **coeficiente líder** a a_n y **término constante** a a_0.

Un polinomio es **mónico** si su coeficiente líder es 1.

Los polinomios se dicen **constantes** cuando su grado es cero, así como el polinomio nulo.

El anillo A[x]

- Teorema:
- El conjunto *A[x]* con la suma y producto habituales es un anillo. Además:
- Si A es un anillo conmutativo, *A[x]* es conmutativo.
- Si A es un anillo con elemento unidad, *A[x]* tiene elemento unidad.
- Si A es dominio de integridad, *A[x]* es dominio de integridad.

El anillo A[x]

- Observación
- Sean los polinomios $a(x) = \sum_{i=0}^{n} a_i \, x^i \in k[x]$ y $b(x) = \sum_{i=0}^{m} b_i \, x^i \in k[x]$ Entonces:
  - grado(a(x) + b(x)) ≤ max {grado(a(x)) , grado(b(x))}, no dándose la igualdad solamente cuando m = n y $a_m + b_n = 0$.
  - grado(a(x)b(x)) ≤ grado(a(x)) + grado(b(x)) (se da la igualdad cuando A es dominio de integridad)

Unidades de A[x]

- Si *A* es un dominio de integridad, un polinomio de *A[x]* es una unidad si y solo si es una constante y es una unidad en *A*. Es decir, el grupo multiplicativo *A[x]** de las unidades de *A[x]* es el grupo *A** de las unidades de *A*.

División euclídea de polinomios

- Teorema (Teorema de división)
  Sean $f(x); g(x) \in k[x]$ dos polinomios, con $g(x) \neq 0$. Entonces, existen dos únicos polinomios $q(x); r(x) \in k[x]$ tales que
  - $f(x) = q(x)g(x) + r(x)$ y $\text{grado}(r(x)) < \text{grado}(g(x))$.

Algoritmo de división

- Para calcular el cociente y el resto de la división entre $f(x)$ y $g(x)$, de grados respectivos m y n.
- Si $m \geq n$ tomar
  - $f_1(x) = f(x) - (a/b)x^{m-n}g(x)$, $q_1(x) = (a/b)x^{m-n}$.
- Repetir con $f_1(x)$ y $g(x)$ hasta que $\text{grado}(f_t(x)) < \text{grado}(g(x))$. El cociente y el resto son
  - $q(x)) = q_1(x) + \ldots + q_{t-1}(x)$, $r(x) = f_t(x)$.
- Si $m < n$, el cociente es 0 y el resto el propio $f(x)$.

División euclídea de polinomios

- Teorema del resto

  Sea un polinomio $f(x) \in k[x]$, y sea un elemento del cuerpo $a \in k$.

  Entonces $f(a)$ es el resto de dividir $f(x)$ por $x - a$.

Divisibilidad

- Divisibilidad
  - Sean *f(x) y g(x)* dos polinomios de *A[x]*, decimos que *g(x)* divide a *f(x)*, y lo escribimos $g(x)|f(x)$ si existe un polinomio *h(x)* tal que $f(x) = g(x) \cdot h(x)$.
- Observaciones
  - Un polinomio divide a cualquier polinomio no nulo de *k[x]* si y solo si es una constante no nula.
  - En *k[x]* $g(x)|f(x)$ si y solo si el resto de dividir *f(x)* entre *g(x)* es nulo.
  - En *k[x]*, si $g(x)|f(x)$ y $f(x)|g(x)$ entonces $grado(f(x)) = grado(g(x))$ y $f(x) = a \cdot g(x)$ donde $a \in k\setminus\{0\}$ es una constante no nula.

Raíz de un polinomio

- Definición
  - Se dice que un elemento $a \in A$ es raíz del polinomio $f(x) \in A[x]$ si $f(a) = 0$. es decir, si al sustituir x por a en $f(x)$ se obtiene el valor 0.
- Corolario
  - Sea un polinomio $f(x) \in k[x]$ de grado positivo. Entonces $f(x)$ tiene una raíz $a \in k$ si y solo si es divisible por x – a.
- Multiplicidad de una raíz
  - Sean f(x) ∈ A[x] un polinomio y a ∈ A una raíz. Se llama multiplicidad de a al mayor entero positivo m tal que $(x - a)^m$ divide a $f(x)$.

Teorema del residuo

El residuo obtenido de la división de $f(x)$ por $(x - c)$, es igual al valor numérico del polinomio $f(x)$ para $x = c$.

Demostración. Como el divisor es de primer grado, el residuo debe ser una constante r. Entonces

$$f(x) = (x - c)q(x) + r$$

Evaluando en $x = c$.

$$f(c) = (c - c)q(x) + r = r$$

Aplicaciones

Demostrar que $f(x) = x^3 + x^2 - 5x + 3$ es divisible entre $x + 3$.

$f(-3) = (-3)^3 + (-3)^2 - 5(-3) + 3 = -27 + 9 + 15 + 3 = 0$

Por lo tanto el residuo vale 0.

Demostrar que $x^n - c^n$ es divisible entre $x - c$.

Debido a que $f(c) = c^n - c^n = 0$, es divisible entre $x - c$.

En que condiciones $x^n + c^n$ es divisible entre $x + c$.

$(-c)^n + c^n = c^n + c^n = 2c^n$ si n es par

$(-c)^n + c^n = -c^n + c^n = 0$ si n es impar

Máximo común divisor

- Definición
  - Sean dos polinomios $f(x)$, $g(x) \in k[x]$. Un polinomio $p(x) \in k[x]$ es un **máximo común divisor** de $f(x)$ y $g(x)$ si verifica:
  - 1. $p(x)|f(x)$ y $p(x)|g(x)$
  - 2. Si $q(x)$ es otro polinomio que divide a $f(x)$ y a $g(x)$ entonces $q(x)|p(x)$.
- Observación
  - El máximo común divisor de dos polinomios no es único. Si $p(x) = mcd(f(x), g(x))$, entonces, para cualquier $a \in k\backslash\{0\}$, $ap(x) = mcd(f(x), g(x))$.
  - Por eso cuando hablamos de un máximo común divisor, podremos acordar que estamos tomando un polinomio mónico y, en esas condiciones, sí que es único.
- Proposición
  - Sean $f(x), g(x) \in k[x]$ dos polinomios. Si $f(x) = q(x)g(x)+r(x)$, entonces se tiene que $mcd(f(x), g(x)) = mcd(g(x),r(x))$.

Algoritmo de Euclides

- Algoritmo de Euclides
  - Sean $f(x)$ y $g(x)$ dos polinomios no nulos con $grado(f(x)) \geq grado(g(x))$. Entonces, haciendo divisiones sucesivas se obtiene:

$$f(x) = q(x) \cdot g(x) + r(x) \quad grado(r(x)) < grado(g(x))$$

$$g(x) = q_0(x) \cdot r(x) + r_1(x) \quad grado(r_1(x)) < grado(r(x))$$

$$r(x) = q_1(x) \cdot r_1(x) + r_2(x) \quad grado(r_2(x)) < grado(r_1(x))$$

$$\ldots$$

$$r_{n-2}(x) = q_{n-1}(x) \cdot r_{n-1}(x) + r_n(x) \quad grado(r_n(x)) < grado(r_{n-1}(x))$$

$$r_{n-1}(x) = q_n(x) \cdot r_n(x)$$

  - Este proceso es finito y, con las notaciones anteriores, $mcd(f(x) , g(x)) = r_n(x)$.

Ejemplo

Encontrar el mcd de $x^6 + 2x^5 + x^3 + 3x^2 + 3x + 2$ y $x^4 + 4x^3 + 4x^2 - x - 2$

1 2 0 1 3 3 2   1 4 4 -1 -2

1 4 4 -1 -2   1 -2 4

-2 -4 2 5 3

-2 -8 -8 2 4

0 4 10 3 -1 2

4 16 16 -4 -8

0 -6 -13 3 10

$f_2 = -6x^3 - 13x^3 + 3x + 10$

f_1 f_2

1	4	4	-1	-2	x 6				
6	24	24	-6	-12		-6	-13	3	10
6	13	-3	-10		x 6	-1	-11		
	11	27	4	-12					
	66	162	24	-72					
	66	143	-33	-110	/ 19				
		19	57	38	f_2				
		1	3	2					
	-6	-13	3	10		1	3	2	
	-6	-18	-12			-6	5		
		5	15	10					
		5	15	10					
		0	0	0					

f_2

Mcd = $x^2 + 3x + 2$

Ejemplo

Calcular el cociente y el resto de la división del polinomio p(x) = $2x^4 + 3x^3 + 5x + 1$ entre q(x) = $3x^3 + x + 6$ en $Z_7[x]$

Notemos en primer lugar que gr(p(x)) > gr(q(x)).

Calculamos 3^{-1}. Se tiene que $3^{-1} = 5$.

Tomamos entonces el término $2 \cdot 5 \cdot x^{4-3} = 3x$.

Hallamos $p_1(x) = p(x) - 3xq(x) = p(x) + 4xq(x) = 3x^3 + 4x^2 + x + 1$.

Dado que *gr(p1(x)) ¸ gr(q(x))* continuamos dividiendo. Tomamos el término $3 \cdot 5x^{3-3} = 1$

Hallamos $p_2(x) = p_1(x) - 1q(x) = p_1(x) + 6q(x) = 4x^2 + 2$.

Dado que $gr(p_2(x)) < gr(q(x))$ la división ha terminado. El cociente es c(x) = $3x + 1$ y el resto $r(x) = 4x2 + 2$.

2 3 0 5 1 | 3 0 1 6

5 0 4 3   3 1

3 4 1 1

4 0 6 1

4 0 2

Identidad de Bézout

- Teorema (Identidad de Bézout)
  - Sean *f(x)* y *g(x)* dos polinomios de *k[x]* no nulos y sea *d(x) = mcd(f(x), g(x))*. Entonces existen unos polinomios *a(x), b(x)* ∈ *k[x]* tales que

$$d(x) = a(x) \cdot f(x) + b(x) \cdot g(x).$$

Ejemplo

Sean $p(x) = x^5 + 2x^4 + x^2 + 2x + 2$, $q(x) = x^5 + 2x^3 + x^2 + x + 1 \in Z_3[x]$.
Vamos a calcular su máximo común divisor y a expresarlo en función de $p(x)$ *y* $q(x)$.

$p(x)$	$q(x)$	$r(x)$	$c(x)$	$u(x)$	$v(x)$
				1	0
				0	1
$x^5+2x^4+x^2+2x+2$	$x^5+2x^3+x^2+x+1$	$2x^4+x^3+x+1$	1	1	2
$x^5+2x^3+x^2+x+1$	$2x^4+x^3+x+1$	$2x^2+2$	$2x+2$	$x+1$	$2x$
$2x^4+x^3+x+1$	$2x^2+2$	0			
	x^2+1			$2x+2$	x

Luego $mcd(x^5 + 2x^4 + x^2 + 2x + 2, x^5 + 2x^3 + x^2 + x + 1) = x^2 + 1$ *y*
$x^2 + 1 = (x^5 + 2x^4 + x^2 + 2x + 2)(2x + 2) + (x^5 + 2x^3 + x^2 + x + 1)(x)$

Polinomio irreducible

- Definición
  - Un polinomio $p(x) \in k[x]$ es irreducible si no es una constante, y si el que podamos escribir $p(x) = f(x)g(x)$ implica que uno de los dos factores sea una unidad (una constante).
- Proposición
  - Sea $p(x) \in k[x]$ un polinomio irreducible. Si $f(x)$ es un polinomio que no es divisible por $p(x)$, entonces $\mathrm{mcd}(f(x), p(x)) = 1$.
- Observación
  - Nótese que si $p(x) \in k[x]$ es reducible y $gr(p(x)) = n$ entonces $p(x)$ tiene un divisor no constante de grado menor o igual que $n/2$.
- Teorema de Euclides
  - Sea $p(x) \in k[x]$ un polinomio irreducible. Dados dos polinomios $f(x), g(x) \in k[x]$, si $p(x)|f(x)g(x)$, entonces $p(x)$ divide a alguno de los dos.

Irreducibilidad

- Descomposición en factores irreducibles
  - Cualquier polinomio no constante de $k[x]$ es irreducible o factoriza en producto de polinomios irreducibles. Este producto es único en tanto que si tenemos dos factorizaciones de $f(x)$ en producto de polinomios irreducibles en $k[x]$ de la forma

$$f(x) = p_1(x) \cdots p_s(x) = q_1(x) \cdots q_t(x)$$

necesariamente $s = t$ y existe una correspondencia uno a uno entre los factores $p_1(x) \cdots p_s(x)$ y $q_1(x) \cdots q_t(x)$ donde si $p_i(x)$ se corresponde con $q_j(x)$, existe un $\alpha \in k\backslash\{0\}$, tal que $p_i(x) = \alpha_{qj}(x)$.

Factorización en R[x]

- Todo polinomio de R[x] de grado impar tiene una raíz en R. Todo polinomio se descompone en producto de polinomios de grados 1 o 2.
- Sea f(x) $\in$ k[x] un polinomio de grado 2 o 3. En ese caso, f(x) es reducible si y sólo si tiene una raíz en k. En efecto, el hecho de que f(x) sea reducible es equivalente a decir que tiene un divisor que es de grado 1. Si éste es *ax - b*, entonces *b/a* es una raíz de f(x).
- Lo anterior no funciona para grados mayores. Un polinomio de grado 4 se puede descomponer, por ejemplo, en dos factores irreducibles de grado 2, como $x^4 + 3x^2 + 2$ en Q, luego no tiene por qué tener raíces en k.

Factorización en Q[x]

- Sea el polinomio de grado $n > 0$

  $$f(x) = a_n x^n + a_{n-1}x^{n-1} + : : : + a_1 x + a_0 \,;\ a_i \in Z,\ i = 0, 1, \dots, n$$

- Regla de Ruffini:
  - Supongamos que *f(x)* tiene una raíz racional $\alpha = a/b$ con *a* y *b* primos entre sí. Entonces $a|a_0$ y $b|a_n$.
- Criterio de Eisenstein:
  - Supongamos que existe un elemento irreducible p $\in Z$ que divide a todos los coeficientes, salvo a a_n, y cuyo cuadrado p^2 no divide a a_0. Entonces *f(x)* es irreducible en *Q[x]*.

Lema de Gauss

- Contenido de un polinomio
  - Dado un polinomio $f(x) \in Z[x]$ no nulo, se llama contenido de f (x) al máximo común divisor de sus coeficientes. Se denota por $c(f)$. Se dirá que $f(x)$ es **primitivo** si su contenido es 1.
- Lema de Gauss
  - El producto de dos polinomios primitivos es primitivo.
- Corolario
  - Si $f(x), g(x) \in Z[x]$ son polinomios no nulos, entonces $c(fg) = c(f)c(g)$.
- Corolario
  - Sea $f(x) \in Z[x]$ un polinomio de grado positivo, digamos n, que se descompone en $Q[x]$ en producto de dos polinomios de grados estrictamente menores que n. Entonces, se descompone en $Z[x]$ en producto de dos polinomios de esos mismos grados.
- Corolario
  - Sea $f(x) \in Z[x]$ un polinomio de grado positivo, digamos n, y primitivo, entonces $f(x)$ es reducible *en* $Z[x]$ si y sólo si lo es en $Q[x]$.

Factorización de polinomios con coeficientes en un cuerpo

- Teorema
  - Todo polinomio no constante $K[x]$ se puede expresar como producto de polinomios irreducibles. La factorización es única salvo producto por constantes y reordenaciones de los factores.
- Teorema
  - Sea K un cuerpo y $f(X) \in K[x]$. Se verifica: $x-\alpha$ es divisor de $f(X)$ si, y sólo si, $f(\alpha) = 0$ *en* K.
- Teorema
  - Sea K un cuerpo y $f(X) \in K[x]$ con grado $n \geq 1$ Se verifica que la ecuación $f(X) = 0$ tiene como mucho *n raíces en K.*

Factorización en un cuerpo F_p

- Teorema
  - En $Z_p[x]$ existen polinomios irreducibles de todos los grados.
- Sea

  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in Z[x]$

  primitivo, sea p un primo que no divida a a_n, y llamemos $\dot{f}(x)$ al polinomio

  $\dot{f}(x) = \bar{a}_n x^n + \bar{a}_{n-1} x^{n-1} + \ldots + \bar{a}_1 x + \bar{a}_0 \in F_p[x]$

  siendo $\bar{a}_i = a_i \ (mod\ p),\ 0 \leq i \leq n$
- Proposición
  - Si $\dot{f}(x)$ es irreducible en $F_p[x]$ entonces $f(x)$ es irreducible en $Q[x]$.

Factorización en un cuerpo F_p

- Sea

  $f(x) = x^4 - x^3 + x^2 - x + 1 \in Z[x]$

  primitivo, sea p un primo que no divida a a_n, y llamemos $\dot{f}(x)$ al polinomio

  $\dot{f}(x) = \bar{a}_n x^n + \bar{a}_{n-1} x^{n-1} + : : : + \bar{a}_1 x + \bar{a}_0 \in F_p[x]$

  siendo $\bar{a}_i = a_i \ (mod\ p),\ 0 \leq i \leq n$
- Tomemos $p = 2$, entonces $\dot{f}(x) = x^4 - x^3 + x^2 - x + 1 \in F_2$ *ya que* $\dot{f}(0)=1$ *y* $\dot{f}(1)= 1$ *no tiene raíces en* F_2
- Intentemos factorizar f(x) de forma artesanal. Como en caso de ser reducible, ningún factor de la descomposición de f(x) será de grado 1, pongamos por caso que

  $\dot{f}(x) = (x^2 + ax + b)(x^2 + cx + d).$

Factorización en un cuerpo F_p

- Operando e igualando coeficientes obtenemos el sistema

$$S : \begin{cases} 1 & = & a + c \\ 1 & = & b + ac + d \\ 1 & = & ad + bc \\ 1 & = & bd \end{cases}$$

- La última ecuación nos dice que b = d = 1, y sustituyendo en el resto nos quedamos con

$$S : \begin{cases} 1 & = & a + c \\ 1 & = & ac \end{cases}$$

- que no tiene solución. Por tanto, $\dot{f}(x)$ es irreducible en F_2 y así, por la proposición, f(x) es irreducible sobre Q.

Congruencia de polinomios

Sea *p(x)*∈ *k[x]* un polinomio. Dados dos polinomios *f(x), g(x)* ∈ *k[x],* diremos que *f(x)* y *g(x)* son **congruentes módulo** *p(x)*, y escribiremos *f(x)* ≡ *g(x) (mod p(x)),* si *p(x)* divide a *f(x) - g(x).*

Si un polinomio *m(x)* tiene grado d, cualquier clase de congruencia modulo *m(x)* tiene un único representante *r(x)* de grado estrictamente menor que d.

el conjunto de polinomios de *k[x]* de grado estrictamente menor que el de *m(x)* es un conjunto completo de representantes para *k[x]/(m(x)).*

Congruencia de polinomios: Ejemplo

- Sea $m(x) = x^2 + 1 \in Q[x]$. Por la proposición, cada elemento de $Q[x]/(m(x))$ tiene un representante de grado menor o igual que 1.
- Como $x^2 \equiv -1 \pmod{x^2 + 1}$, multiplicando por x tenemos que $x^3 \equiv -x \pmod{x^2 + 1}$.
- Por inducción en n tenemos $x^{2n} \equiv (-1)^n \pmod{x^2 + 1}$, $x^{2n+1} \equiv (-1)^n x \pmod{x^2 + 1}$.
- Como Q es un cuerpo infinito, existen infinitos polinomios de grado menor o igual que 1 en Q[x], y por tanto $Q[x]=(x^2 + 1)$ es un conjunto infinito.
- Si utilizáramos ahora F_3 en lugar de Q, por lo anterior tendríamos que

  $(F_3)[x]=(x^2 + 1) = \{ 0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2 \}$.

Teorema chino del resto

- Sean $m_1(x) \cdots m_s(x) \in k[x]$, polinomios primos entre sí dos a dos, y sean $a_1(x) \cdots a_s(x) \in k[x]$ otros polinomios arbitrarios. Entonces existe $f(x) \in k[x]$:

$$f(x) \equiv a_1(x) \ (mod\ m_1(x))$$

$$f(x) \equiv a_2(x) \ (mod\ m_2(x))$$

$$\ldots$$

$$f(x) \equiv a_n(x) \ (mod\ m_n(x))$$

$$r_{n-1}(x) = q_n(x) \cdot r_n(x)$$

- Además, para que el polinomio $f(x) \in k[x]$ sea otra solución es condición necesaria y suficiente que se verifique que

$$f(x) \equiv \dot{f}(x) \pmod{m_1(x)m_2(x) \ldots m_n(x)}.$$

Sistemas lineales de congruencias

Para resolver el sistema $f(x) \equiv a_i(x) \pmod{m_i(x)}$, $i = 1, \ldots, n$,

siendo los $m_i(x)$ polinomios primos entre sí y los $a_i(x)$ polinomios cualesquiera.

Tome, para cada i, $I_i(x) = \dfrac{\prod_{j=1}^{n} m_j(x)}{m_i(x)}$.

Tome, para cada i,

Aplique la identidad de Bézout a cada pareja I_i, m_i para obtener la igualdad $1 = \alpha_i(x)m_i(x) + \beta_i(x)I_i(x)$.

Aplique la identidad de Bézout a cada pareja I_i, m_i para obtener la igualdad $1 = \alpha_i(x)m_i(x) + \beta_i(x)I_i(x)$.

Las soluciones son $f(x) = \alpha_1(x)\beta_1(x)I_1(x) + \alpha_2(x)\beta_2(x)I_2(x) + \ldots + \alpha_n(x)\beta_n(x)I_n(x)$

Las soluciones son $f(x) = \alpha_1(x)\beta_1(x)I_1(x) + \alpha_2(x)\beta_2(x)I_2(x) + \ldots + \alpha_n(x)\beta_n(x)I_n(x)$

y los polinomios congruentes con el modulo $\prod_{j=1}^{n} m_j(x)$

y los polinomios congruentes con el modulo

- ¿Cuánto vale la siguiente expresión?

$$2 \cdot 3 + 2 \cdot 2 + 1$$

$Z_2 = \{0,1\}$

+	**0**	**1**
0	0	1
1	1	0

.	**0**	**1**
0	0	0
1	0	1

$Z_3 = \{0,1,2\}$

+	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

×	**0**	**1**	**2**
0	0	0	0
1	0	1	2
2	0	2	1

$Z_4 = \{0,1,2,3\}$

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

.	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$Z_5 = \{0,1,2,3,4\}$

+	**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

.	**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

Z_6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

+	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

¡¡ Interesa trabajar con conjuntos donde todos los elementos no nulos tengan inverso !!

Ese tipo de conjuntos se llaman <u>cuerpos de Galois</u> (1811-1832), en inglés GF (Galois Field)

- **Z_n con *n* primo es cuerpo.**
- **De manera que, por ejemplo, Z_8 no es cuerpo**
- **¿Existe un cuerpo con 8 elementos?.**

- **Galois demostró que sí.**
- **En realidad demostró algo mucho mejor: que el número de elementos de cualquier cuerpo finito era de la forma con *p* primo.** p

- **¿Pero cómo se construye este cuerpo?.**
- **Vamos a verlo.**

Construcción del cuerpo GF(2^3)=GF(8)

- Consideremos el conjunto formado por todos los polinomios del tipo:

$$ax^2 + bx + c$$

- donde los coeficientes son ceros o unos
    - ¿Cuántos polinomios se pueden formar?

a	b	c	$ax^2 + bx + c$	Binario	Decimal
0	0	0	0	000	0
0	0	1	1	001	1
0	1	0	x	010	2
0	1	1	$x+1$	011	3
1	0	0	x^2	100	4
1	0	1	x^2+1	101	5
1	1	0	x^2+x	110	6
1	1	1	x^2+x+1	111	7

Construcción del cuerpo GF(2^3)=GF(8)

- Vamos a hacer la tabla de sumar.
- Los polinomios se suman como siempre sólo que ahora los coeficientes valen cero o uno **(suma de Z_2)**

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

- Ejemplo:

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

Construcción del cuerpo GF(2^3)=GF(8)

- La tabla de sumar anterior se puede escribir con números:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

$$2+5=010_{(2}+101_{(2}=x+x^2+1=x^2+x+1=111_{(2}=7$$

$$3+7=011_{(2}+111_{(2}=x+1+x^2+x+1=x^2=100_{(2}=4$$

Construcción del cuerpo GF(2^3)=GF(8)

- Vamos a hacer la tabla de multiplicar.
- Los polinomios se multiplican como siempre pero sólo con ceros y unos.

$$p(x)=x| \quad \} \Rightarrow p(x)\cdot q(x)=x^2+x$$

$$p(x)=x+1| \quad \} \Rightarrow p(x)\cdot q(x)=(x+1)(x+1)=x^2+x+x+1=x^2+1$$

$$p(x)=x^2+x| \quad \} \Rightarrow p(x)\cdot q(x)=x^3+x^2+x^2+x=x^3+x$$

¡¡El resultado se sale fuera de donde estamos trabajando!!

¿Y ahora qué hacemos?

Construcción del cuerpo GF(2^3)=GF(8)

- Pues vamos a dividir el polinomio que nos salga entre el polinomio:

$$m(x) = x^3 + x + 1$$

- Y así nos aseguramos que el resultado siempre sea un polinomio de grado dos (como mucho).

$$p(x) = x^2 + x| \quad \} \Rightarrow p(x) \cdot q(x) = x^3 + x^2 + x^2 + x = x^3 + x$$

$$x^3 + x \,|\underline{x^3 + x + 1}$$
$$\underline{x^3 + x + 1}1$$
$$1$$

- Ahora nos quedamos con el resto:

$$p(x) \cdot q(x) = x^3 + x = 1(\text{mod}\, m(x))$$

Construcción del cuerpo GF(2^3)=GF(8)

•	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Construcción del cuerpo GF(2^3)=GF(8)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

$$4\cdot 3 = 100_{(2}\cdot 011_{(2} = x^2\,(x+1) = x^3+x^2 = x^2+x+1 = 111_{(2} = 7$$

$$x^3+x^2 \;\; |\underline{x^3+x+1}$$
$$\underline{x^3+x+1}\,1$$
$$x^2+x+1$$

Construcción del cuerpo GF(2^3)=GF(8)

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

Ejemplos:

$$2\cdot 3+2\cdot 2+1 = 6+4+1 = 2+1 = 3$$
$$5\cdot 4+6\cdot 3+7 = 2+1+7 = 3+7 = 4$$

Ahora ya se puede contestar a la pregunta del inicio

- En la aritmética habitual:

$$2 \cdot 3 + 2 \cdot 2 + 1 = 11$$

- En la aritmética en Z_5 :

$$2 \cdot 3 + 2 \cdot 2 + 1 = 1 + 4 + 1 = 1$$

- En la aritmética en GF(8):

$$2 \cdot 3 + 2 \cdot 2 + 1 = 6$$

¡¡ El resultado depende del conjunto donde estamos trabajando !!

Referencias

- Olalla Acosta, Miguel Ángel. “Polinomios”
- Medellín Anaya, Héctor Eduardo. “Polinomios”
- “Algoritmo AES, campos de Galois”