Preliminares matemáticos

Anillos de polinomios
Cuerpo de Galois
Operaciones en el algoritmo AES

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
KISA

Anillos de polinomios

Dado un cuerpo $\mathbb{F}$, un *polinomio en la indeterminada x sobre $\mathbb{F}$* es una expresión de la forma

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

donde cada $a_i \in \mathbb{F}$ y $n \geq 0$.

El elemento a_i se llama *coeficiente i-ésimo* de $f(x)$ y el mayor m para el cual $a_m \neq 0$ es el *grado* de $f(x)$.

El conjunto de polinomios en la indeterminada x sobre $\mathbb{F}$ se denota por $\mathbb{F}[x]$.

La *suma* y *producto* de polinomios se definen de forma habitual.

Ejemplo

Consideramos el cuerpo $\mathbb{Z}_2$ y dos polinomios de $\mathbb{Z}_2[x]$:

$$f(x) = x^3 + x + 1, \quad g(x) = x^2 + x.$$

Entonces

$$f(x) + g(x) = x^3 + x^2 + 2x + 1 = x^3 + x^2 + 1,$$

$$f(x) \cdot g(x) = x^5 + x^4 + x^3 + 2x^2 + x = x^5 + x^4 + x^3 + x.$$

Un polinomio $f(x) \in \mathbb{F}[x]$ de grado mayor o igual a 1 es *irreducible* si no puede ser puesto como producto de otros dos polinomios de grado positivo en $\mathbb{F}[x]$.

Ejemplo

$f(x) = x^5 + x^4 + x^3 + x \in \mathbb{Z}_2[x]$ **no** es irreducible:

$$x^5 + x^4 + x^3 + x = (x^3 + x + 1) \cdot (x^2 + x).$$

$g(x) = x^4 + 1 \in \mathbb{Z}_2[x]$ **no** es irreducible:

$$x^4 + 1 = (x^2 + 1)^2 = (x + 1)^4.$$

$h(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ es irreducible.

Propiedades de la suma y del producto de polinomios

- $(+)$ es asociativa: $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$.
- $(+)$ es conmutativa: $f(x) + g(x) = g(x) + f(x)$.
- $(+)$ tiene elemento neutro (0): $f(x) + 0 = f(x)$.
- Todo polinomio tiene simétrico para $(+)$: $f(x) + (-f(x)) = 0$.

$(\mathbb{F}[x], +)$ es un grupo conmutativo.

- $(\cdot)$ es asociativo $(f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x))$.
- $(\cdot)$ es conmutativo: $f(x) \cdot g(x) = g(x) \cdot f(x)$.
- $(\cdot)$ tiene elemento neutro (1): $f(x) \cdot 1 = f(x)$.
- $(\cdot)$ es distributivo con respecto a $(+)$.

$(\mathbb{F}[x], +, \cdot)$ es un anillo conmutativo unitario.

Recordemos: $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo unitario.
Fijado $n \in \mathbb{Z}$ y dados $a, b \in \mathbb{Z}$,

$$a \equiv b \mod n \text{ si } n \mid a - b.$$

Igual que en $\mathbb{Z}$, podemos definir en $\mathbb{F}[x]$ una aritmética modular:

Definición

Sea $f(x) \in \mathbb{F}[x]$ un polinomio fijo. Dados $g(x), h(x) \in \mathbb{F}[x]$, se dice que $g(x)$ es congruente con *$h(x)$* módulo *$f(x)$ si*

$$f(x) \mid g(x) - h(x).$$

Es decir, si existe un polinomio $k(x) \in \mathbb{F}[x]$ tal que

$$g(x) = h(x) + k(x)f(x).$$

Se escribe

$$g(x) \equiv h(x) \mod f(x).$$

Recordemos: en $\mathbb{Z}$, cada $a \in \mathbb{Z}$ es congruente módulo n a un único entero r, $0 \leq r < n$.

$$\begin{array}{r|l} a & n \\ \hline r & q \end{array} \quad a = qn + r,\ 0 \leq r < n.$$

$$\mathbb{Z}_n = \text{conjunto de posibles restos} = \{0, 1, \ldots, n-1\}.$$

En $\mathbb{F}[x]$, cada polinomio $g(x) \in \mathbb{F}[x]$ es congruente módulo $f(x)$ a un único polinomio de grado menor que el de $f(x)$:

$$\begin{array}{r|l} g(x) & f(x) \\ \hline r(x) & q(x) \end{array} \quad g(x) = f(x)q(x) + r(x),\ \text{grado}(r(x)) < \text{grado}(f(x)).$$

$$g(x) \equiv r(x) \quad \text{mód } f(x).$$

Denotaremos por $\mathcal{P}_f(\mathbb{F})$ el conjunto de posibles restos.

Si $\text{grado}(f(x)) = n$, $\mathcal{P}_f(\mathbb{F})$ es el conjunto de polinomios de grado menor que n.

Ejemplo

Sea $\mathbb{F} = \mathbb{Z}_2$.

- Si $f(x) = x^2 + 1$, entonces

$$\mathcal{P}_f(\mathbb{Z}_2) = \{0,\ 1,\ x,\ x+1\}.$$

Por ejemplo,

$$\begin{array}{r|l} x^4 + x^2 + x & x^2 + 1 \\ \cline{2-2} x & x^2 \end{array}$$

$$x^4 + x^2 + x \equiv x \mod x^2 + 1.$$

- Si $f(x) = x^3 + x$, entonces

$$\mathcal{P}_f(\mathbb{Z}_2) = \{0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1\}.$$

Recordemos: en $\mathbb{Z}_n$ se definen la suma y el producto módulo n y $(\mathbb{Z}_n, +, \cdot)$ es un anillo conmutativo y unitario.

En $\mathcal{P}_f(\mathbb{F})$ se definen la suma y el producto módulo $f(x)$.

Ejemplo

Si $\mathbb{F} = \mathbb{Z}_2$ y $f(x) = x^2 + 1$, entonces $\mathcal{P}_f(\mathbb{Z}_2) = \{0, 1, x, x+1\}$.

$$x + (x+1) \equiv 1 \mod f(x).$$

$$x \cdot (x+1) = x^2 + x \qquad \begin{array}{r|l} x^2 + x & x^2 + 1 \\ x + 1 & \hline 1 \end{array}$$

$$x \cdot (x+1) \equiv x + 1 \mod f(x).$$

$(\mathcal{P}_f(\mathbb{F}), +, \cdot)$ es un anillo conmutativo y unitario.

Recordemos: $(\mathbb{Z}_n, +, \cdot)$ es cuerpo $\Leftrightarrow$ n es primo.
Si n es primo, el inverso de $a \in \mathbb{Z}_n$ se obtiene aplicando el algoritmo extendido de Euclides: $ua + vn = 1$, $a^{-1} \equiv u$ mód n.

$$(\mathcal{P}_f(\mathbb{F}), +, \cdot) \text{ es cuerpo } \Leftrightarrow f(x) \text{ es irreducible.}$$

Es decir, si $f(x)$ es irreducible, todo polinomio diferente de cero tiene inverso módulo $f(x)$.

El inverso de un polinomio $g(x)$ se obtiene aplicando el algoritmo extendido de Euclides: existen $u(x)$, $v(x)$ tales que

$$u(x)g(x) + v(x)f(x) = 1, \quad g(x)^{-1} \equiv u(x) \quad \text{mód } f(x).$$

Los polinomios irreducibles desempeñan en $\mathbb{F}[x]$ el mismo papel que el de los números primos en $\mathbb{Z}$.

Cuerpo de Galois

En el anillo $\mathbb{Z}_2[x]$, todos los coeficientes de los polinomios pueden valer 0 o 1, por lo que un polinomio puede ser representado por una cadena de bits.

Ejemplo

- Si $f(x) = x^2 + 1 = 101$, entonces

$$\mathcal{P}_f(\mathbb{Z}_2) = \{0,\ 1,\ x,\ x+1\} = \{00, 01, 10, 11\}.$$

- Si $f(x) = x^3 + x = 1010$, entonces

$$\mathcal{P}_f(\mathbb{Z}_2) = \{0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1\}$$

$$= \{000, 001, 010, 011, 100, 101, 110, 111\}.$$

Si $f(x)$ es un polinomio irreducible de grado n, entonces $(\mathcal{P}_f(\mathbb{Z}_2), +, \cdot)$ es un cuerpo.

Los elementos de este cuerpo pueden ser representados por polinomios de grado menor que n, es decir, por cadenas de bits de longitud n.

Por tanto, el número de elementos del cuerpo es 2^n.

Se llama *cuerpo de Galois*. Se representa por $\mathrm{GF}(2^n)$.

Ejemplo

Consideremos el polinomio irreducible

$$f(x) = x^8 + x^4 + x^3 + x + 1.$$

Genera un cuerpo $\mathrm{GF}(2^8)$, cuyos elementos pueden representarse indistintamente por cadenas de 8 bits o por polinomios de grado menor que 8.
La suma y producto en este cuerpo se realizan módulo $f(x)$.
Por ejemplo, dados los elementos:

$$00100010 = x^5 + x, \quad 00011011 = x^4 + x^3 + x + 1,$$

$$(x^5 + x) + (x^4 + x^3 + x + 1) = x^5 + x^4 + x^3 + 1,$$

$$00100010 + 00011011 = 00111001.$$

$$f(x) = x^8 + x^4 + x^3 + x + 1.$$

$$(x^5 + x)(x^4 + x^3 + x + 1) = x^9 + x^8 + x^6 + x^4 + x^2 + x.$$

$$\begin{array}{l|l} x^9 + x^8 + x^6 + x^4 + x^2 + x & x^8 + x^4 + x^3 + x + 1 \\ \cline{2-2} x^6 + x^5 + x^4 + x^3 + x + 1 & x + 1 \end{array}$$

$$x^9 + x^8 + x^6 + x^4 + x^2 + x \equiv x^6 + x^5 + x^4 + x^3 + x + 1 \mod f(x).$$

En $\mathrm{GF}(2^8)$:

$$(x^5 + x) \cdot (x^4 + x^3 + x + 1) = x^6 + x^5 + x^4 + x^3 + x + 1.$$

$$00100010 \cdot 00011011 = 01111011.$$

Operaciones en el algoritmo AES

En el algoritmo AES se realizan operaciones a nivel de byte y a nivel de palabra.

A nivel de byte

Un byte representa un polinomio en $\mathbb{Z}_2[x]$:

$$b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0 \leftrightarrow b_7 x^7 + b_6 x^6 + \cdots + b_1 x + b_0$$

Por ejemplo, $01010111 = 57_{HEX} = x^6 + x^4 + x^2 + x + 1$.

Los bytes son considerados elementos en el cuerpo $\mathrm{GF}(2^8)$ generado por el polinomio irreducible

$$m(x) = x^8 + x^4 + x^3 + x + 1.$$

Es decir, el producto se realiza módulo $m(x)$.

Ejemplo

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2.$$

$$01010111 + 10000011 = 11010100, \qquad HEX : 57 + 83 = d4.$$

$$(x^6+x^4+x^2+x+1)(x^7+x+1) = x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$$

$$\equiv x^7 + x^6 + 1 \mod m(x).$$

$$01010111 \cdot 10000011 = 11000001 \qquad HEX : 57 \cdot 83 = c1.$$

A nivel de palabra

Una palabra es un registro de 32 bits = 4 bytes.

$$a_3a_2a_1a_0,\ a_i\ \text{byte} \longleftrightarrow a_3x^3 + a_2x^2 + a_1x + a_0$$

Por ejemplo, $(c1, ff, 57, 80) \longleftrightarrow c1x^3 + ffx^2 + 57x + 80.$

Se interpreta como un elemento en el anillo de polinomios de grado menor que 4 con coeficientes en $\mathrm{GF}(2^8)$ generado por el polinomio no irreducible

$$M(x) = x^4 + 1.$$

Es decir, las palabras son elementos de $\mathcal{P}_M(\mathrm{GF}(2^8))$: polinomios de grado menor que 4, cuyos coeficientes son polinomios de $\mathrm{GF}(2^8)$.

El producto se realiza módulo $M(x)$.

Ejemplo

$$(00, 00, 01, 57) \cdot (01, 00, 00, 83) = (01x + 57) \cdot (01x^3 + 83)$$

$$= 01 \cdot 01x^4 + 57 \cdot 01x^3 + 01 \cdot 83x + 57 \cdot 81 = 01x^4 + 57x^3 + 83x + c1.$$

$$\begin{array}{r|l} 01x^4 + 57x^3 + 83x + c1 & 01x^4 + 01 \\ \cline{2-2} 57x^3 + 83x + c0 & 01 \end{array}$$

$$01x^4 + 57x^3 + 83x + c1 \equiv 57x^3 + 83x + c0 \quad \text{mód } (01x^4 + 01).$$

$$(00, 00, 01, 57) \cdot (01, 00, 00, 83) = (57, 00, 83, c0).$$

Como $M(x) = x^4 + 1$ no es irreducible, no todos los polinomios de $\mathcal{P}_M(\mathrm{GF}(2^8))$ tienen inverso. En el algoritmo AES se fija un polinomio invertible.

Puede probarse que el producto modular en $\mathcal{P}_M(\mathrm{GF}(2^8))$ puede realizarse por medio de una matriz circulante:

$$a_3 a_2 a_1 a_0 \cdot b_3 b_2 b_1 b_0 = d_3 d_2 d_1 d_0$$

donde

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Ejemplo

Dadas las dos palabras

$$a = (00, 00, 01, 57), \quad b = (01, 00, 00, 83),$$

para efectuar el producto $a \cdot b$:

$$\begin{bmatrix} 57 & 00 & 00 & 01 \\ 01 & 57 & 00 & 00 \\ 00 & 01 & 57 & 00 \\ 00 & 00 & 01 & 57 \end{bmatrix} \begin{bmatrix} 83 \\ 00 \\ 00 \\ 01 \end{bmatrix} = \begin{bmatrix} 57 \cdot 83 + 01 \cdot 01 \\ 01 \cdot 83 \\ 00 \\ 57 \cdot 01 \end{bmatrix}.$$

Realizando las operaciones a nivel de byte:

$$57 \cdot 83 + 01 \cdot 01 = c1 + 01 = c0, \quad 01 \cdot 83 = 83, \quad 57 \cdot 01 = 57.$$

$$(00, 00, 01, 57) \cdot (81, 00, 00, 83) = (57, 00, 83, c0).$$

Fin de la sección