Criptografía Multivariable

Miguel Esteban Pérez Ibarra

Centro de Investigación en Computación

February 24, 2020

Centro de Investigación
en Computación

Instituto Politécnico Nacional

Índice

Anillo de Polinomios sobre $F[x]$

- Para comenzar sea F un campo y se define:

$$F[x] = \{a_0 + a_1 x + \ldots + a_n x^n | a_i \in F\}$$

Algoritmo de la Division

Dados $f(x), g(x) \neq 0 \in F$ existen $q(x)$ y $r(x) \in F[x]$ tales que:

- $gr(r(x) < gr(g(x))$ ó $g(r(x)) = 0$.
- $f(x) = g(x)q(x) + r(x)$.

Observaciones

- ¿Ahora porque es importante que se mencione el algoritmo de la división?
- Para responder primero se necesita la definición de ideal.

¿Qué es un ideal?

- `Definición de Ideal`. Dado un anillo F si $I \subset F$, se dice que I es un ideal si $\forall x, y \in I$ y $\forall r \in F$:
  1. $x - y$.
  2. $rx \in I$.

Ideales principales en $F[x]$

- Dado $g(x) \in F[x]$ se obtiene que
$$(g(x)) = \{g(x)q(x) : q(x) \in F[x]\}$$
es un ideal principal.

Observación

- Con la ayuda de un ideal principal en $F[x]$ y el algoritmo de la división podemos introducir la noción de la clase de equivalencia $\equiv \mod(g(x))$.

Clase de Equivalencia $\equiv mod(g(x))$

- Se define la clase de equivalencia $\equiv mod(g(x))$ por:

  $f(x) - r(x) \in (g(x))$ si, y sólo si $f(x) \equiv r(x) \bmod (g(x))$

  $\forall f, r \in F[x]$

Observación

- Lo que se esta haciendo con la relación de equivalencia $\equiv$ mod $(g(x))$ es classificar un polinomio $f(x) \in F[x]$.

El Espacio Cociente $K = F[x]/(g(x))$

Finalmente gracias al concepto de ideal principal y algoritmo de la división se obtiene el espacio cociente:

- $K = F[x]/(g(x)) = \{(g(x)) + r(x) : r(x) \in F[x]\}$.

$K = F[x]/(g(x))$ como campo

- Ahora ya se puede hablar de K como campo al definir operaciones de suma y multiplicaión sobre K.

Operación Multiplicación en K

- Para poder multpilicar en $K = F[x]/(g(x))$ adecuadamente podemos hacer uso del algoritmo de la division.
- Tomemos como ejemplo cuando $F = \mathbb{Z}_2$ y $g(x) = \bar{1} + \bar{1}x + \bar{1}x^2$.

Tabla de Operaciones

Campo $K = \mathbb{Z}_2/(1 + x + x^2)$

$+$	P	$P+1$	$P+x$	$P+x+1$
P	P	$P+1$	$P+x$	$P+x+1$
$P+1$	$P+1$	P	$P+x+1$	$P+x$
$P+x$	$P+x$	$P+x+1$	P	$P+1$
$P+x+1$	$P+x+1$	$P+x$	$P+1$	P

$\cdot$	P	$P+1$	$P+x$	$P+x+1$
P	P	P	P	P
$P+1$	P	$P+1$	$P+x$	$P+x+1$
$P+x$	P	$P+x$	$P+x+1$	$P+1$
$P+x+1$	P	$P+x+1$	$P+1$	$P+x$

Costrucción de un Polinomio Multivariable

- Antes de introducir el concepto de polinomio multivariable contruíremos uno de tres variables.
- $K = \{0, 1, 2, 3\}$
- $K_1 = k[x_1] = \{a_0 + \cdots + a_m x^m : a_{i_1} = I + (c_0^i + c_1^i x)\}$
- $K_2 = k_1[x_2] = \{P_0(x_1) + \cdots + P_n(x_1)x_2^n : P_{i_2} \in K_1\}$
- $K_3 = K_2[x_3] = \{Q_0(x_2) + \cdots + Q_l(x_2)x_3^l : Q_{i_3}(x_2) \in K_2\}$

Construcción de un Polinomio Multivariable

$$\begin{aligned}\phi(x_3) &= Q_0(x_2) + Q_1(x_2)x_3 + Q_2(x_2)x_3^2 \\ &= (P_0^0(x_1) + P_1^0(x_1)x_2) + (P_0^1(x_1)x_2^2)x_3 + (P_0^2(x_1))x_3^2 \\ &= 2x_1 + x_1^2x_2 + x_1x_2^2x_3 + 3x_3^2\end{aligned}$$

Evaluando en $(1, 2, 3)$ se obtiene que:

$$\phi(1, 2, 3) = 1 * 2 + 1^2 * 2 + 1 * 2^2 * 3 + 3 * 3^2$$

Definición de un Polinomio Multivariable

Se define el anillo de polinomios en las n variables $x_1, \ldots x_n$ sobre R, como $R[x_1, \ldots x_n]$, en donde sus elementos son de la forma:

$$\sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$$

Criptografía Multivariable

Es el estudio de la criptografía asimétrica en donde la función trampa toma la forma de un polinomio cuadrático multivariable sobre un campo finito. En general la llave pública esta dada por un conjunto de polinomios cuadráticos:

$$P = (p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n))$$

MQ es en general NP-difícil

1. **Problema MQ**: Resuelva el sistema $p_1(x) = p_2(x) = \cdots = 0$, donde cada p_i es un polinomio cuadrático en $x = (x_1, \ldots, x_n)$. Todos los coeficientes y variables estan en $\mathbb{K} = \mathbb{F}_q$, el campo con q elementos.

Esquema de Cifrado

. Nuevamente consideré un llave púbica dada por:

$$S(x_1 \dots x_n) = (p_1(x_1, \dots, x_n) \dots p_n(x_1, \dots, x_n))$$

Dado cualquier texto plano $M = (x_1, \dots, x_n)$ este se cifra mediante la regla $S(M) = S(x_1, \dots, x_n) = (y_1, \dots, y_m)$.

Ejemplo de una Llave Pública

Utilizando el campo finito $K = \mathbb{Z}_2[x]/(1 + x + x^2) = \{0, 1, 2, 3\}$.
Se generan los siguientes polinomios:

1. $p_1 = 1 + x_3 + 2x_1x_3 + 3x_2^2 + 3x_2x_3 + x_3^2$
2. $p_2 = 1 + 3x_1 + 2x_1 + 2x_2 + x_3 + x_1^2 + x_1x_2 + 3x_1x_3 + x_2^2$
3. $p_3 = 3x_3 + x_1^2 + 3x_2^2 + x_2x_3 + 3x_3^2$

Así pues dado $M = (1, 2, 3)$ nuestra llave pública arroja el texto cifrado $S(M) = (0, 0, 1)$.

Fín