Universidad Carlos III de Madrid
COSEC LAB· Dpto. Informática

Tema 1. Fundamentos Matemáticos. Cuerpos de Galois

Criptografía y seguridad informática

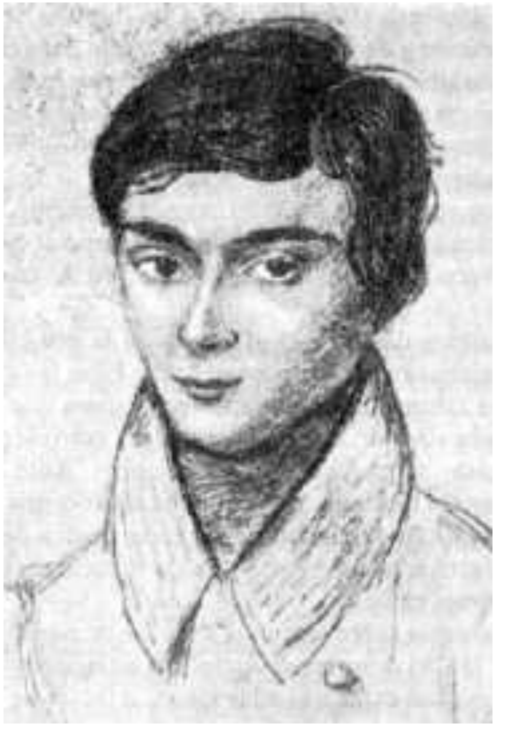
Seguridad en las tecnologías de la información

@ COSEC LAB

Curso 2016-2017

Galois

Nacimiento	25 de octubre de 1811 Bourg-la-Reine, Francia
Fallecimiento	31 de mayo de 1832 (20 años) París, Francia
Nacionalidad	Francia
Campo	Matemática
Conocido por	Trabajos sobre teoría de ecuaciones e integrales abelianas



Cuerpos de Galois CG(p)

- Sea $Z_p = \{0,1,2,......, p-1\}$ siendo p primo
  $\forall x \neq 0 \in Z_p$, x es primo relativo a p (coprimo) y, por tanto, existe x^{-1} respecto al módulo *p*
- Z_p es un cuerpo respecto a las operaciones de suma y multiplicación mod p:
  - Elemento neutro aditivo (0)
  - Elemento neutro multiplicativo (1)
  - Se cumplen las propiedades conmutativa, asociativa y distributiva respecto a las operaciones + y ·, tiene inverso aditivo, e inverso multiplicativo para los elementos distintos de 0
- Hay **p** elementos en CG(**p**)
- Φ(p) = p-1 (hay p-1 elementos en el campo coprimos con p)
- **Z_p** es un **cuerpo finito** denominado **Cuerpo de Galois CG(p)**

Z_p = CG(p) [= GF(p)]

Cuerpos de Galois CG(q^n)

- Otro cuerpo CG(q^n), relacionado con el anterior, se define así:
  - Está formado por los **polinomios de grado (n-1) o menor**
  - Los **coeficientes** pertenecen a $\mathbf{Z_q}$ **con *q* primo**
  - Si al operar con los polinomios (aritmética de polinomios) resulta un polinomio de grado n o mayor, se **reduce módulo** un polinomio **p(x) de grado n irreducible**

$n \leq 3$
$n-1 = 2$
x
1
$x+1$
8 x^2
x^2+x
x^2+1
x^2+x+1
0
$CG(2^3)$
? idea

$$a(x) \in CG(q^n)$$

$$a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots\ldots\ldots\ldots + a_1x + a_0,\ \ a_i \in Z_q \ \ mód\ p(x);$$

  - Se suele utilizar $\boxed{p(x) = x^n + x + 1}$ que es irreducible para n= 1, 3, 4, 6, 7, 9, 15, 22, 28, 30, 46, 60, 60, 63,127…
  - Existen **q^n** polinomios en CG(**q^n**)
  - Φ(p(x)) = q^n-1 (hay q^n-1 elementos "coprimos" con p(x))

Operaciones en Cuerpos de Galois CG(q^n)

- Las operaciones a realizar en $CG(q^n)$ son relativamente sencillas:
- Suma y resta
  - c(x)=a(x) ± b(x) mód p(x)
    - implica simplemente $c_i = (a_i \pm b_i) \, mód \; q$
- Multiplicación
  - c(x) = a(x) · b(x) mód p(x),
    - Multiplicamos los dos polinomios teniendo en cuenta que los coeficientes pertenecen a Z_q (deben reducirse mód q)

      ↳ si nos pasamos reducimos < div rest.
    - Obtendremos un polinomio de grado 2 · (n-1) = 2n-2 que deberá reducirse mód p(x): dividimos el polinomio entre p(x) y nos quedamos con el resto

Operaciones en Cuerpos de Galois CG(q^n)

- "División" (inverso multiplicativo)
  - $u(x) \cdot s(x) = v(x)$ mód $p(x)$ ¿$u(x)$?

$$\forall s(x) \in CG(q^n), \exists t(x) \in CG(q^n) \mid s(x) \cdot t(x) = 1 \, mód \; p(x)$$

  - ¿Cómo calcular $s(x)^{-1} \bmod p(x)$?
    - Aplicando el Teorema de Fermat/Euler
      - $\Phi(p(x)) = q^n - 1$ (# elementos en CG(q^n) coprimos con p(x))
      - $s(x)^{-1} \bmod p(x) = s(x)^{\Phi(p(x)) - 1} \bmod p(x) = s(x)^{q^n - 2} \bmod p(x)$

findwento · v(x)

    - Aplicando el algoritmo de Euclides modificado

Cuerpos de Galois CG(2^n)

- Dentro de estos cuerpos vamos a estudiar **CG(2^n)**
- Cada elemento de $a(x) \in CG(2^n)$ se representa mediante sus coeficientes $a_i = \{0,1\}$

0	(0 0 0)	x^2+x	(1 1 0)
1	(0 0 1)	x^2+1	(1 0 1)
x	(0 1 0)	⋮	⋮

  - En lugar de $a(x) = a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+ \cdots\cdots +a_1x+a_0$

$$\left(a_{n-1}, a_{n-2}, \ldots\ldots, a_1, a_0\right)$$

- El **número de elementos de CG(2^n) es 2^n**
  - Usamos **n bits** para representar un elemento
  - p(x) usará n+1 bits
- Ej. $x^2+1 \in CG(2^3)$ se representaría (1,0,1)

Cuerpos de Galois $CG(2^n)$

- Ventajas de la aritmética en $CG(2^n)$ mod $p(x)$ con respecto $CG(p)$:
  - Operaciones más simples y no es necesario reducir para la suma y la resta
  - Al tener un cardinal igual a una potencia de 2, $CG(2^n)$ aprovecha toda la capacidad de la representación electrónica (bits), que no suele ocurrir con $CG(p)$
    - Para 8 bits, Z_{256} no es un cuerpo
    - Z_{251} sí es un cuerpo pero desaprovechamos capacidad del byte
  - Cálculo de inversos más rápidamente para computadores.

Cuerpos de Galois $CG(2^n)$

- Los coeficientes operan en Z_2

Z_2

w	-w	w^{-1}
0	0	---
1	1	1

Suma:
w=u+v mod 2

u	v	w
0	0	0
0	1	1
1	0	1
1	1	2 = 0

igualr → 0
distinto → 1

Resta:
w=u-v mod 2

u	v	w
0	0	0
0	1	-1 = 1
1	0	1
1	1	0

La suma y la resta de coeficientes en Z_2 es equivalente a la operación XOR $\oplus$

Sumas y restas en Cuerpos de Galois CG(2^n)

- Suma y resta: c(x) = a(x) ± b(x) mod p(x)

$$c_i = (a_i \pm b_i) \bmod 2 = \begin{cases} 0 \quad si \ a_i = b_i \\ 1 \quad si \ a_i \neq b_i \end{cases}$$

Un XOR ⊕ sin acarreo

por lo que

$$c_i = (a_i \pm b_i) = a_i \oplus b_i$$

- Ej. a=(10110) y b=(10101) en CG(2^5). Calcular c=a+b

c=(10110)⊕(10101)= 00011

Es como hacer un XOR de ambos polinomios.

Multiplicación en Cuerpos de Galois CG(2^n)

- c(x)=a(x) ·b(x) mod p(x)
- En este caso, si el polinomio resultado de la multiplicación de los polinomios es de grado n o mayor que n, habrá que reducirlo mód p(x)

$$c(x) = \sum_{i=0}^{n-1} (a_i \cdot b(x)) \cdot x^i \bmod p(x)$$

$$a_i \cdot b(x) = \begin{cases} b(x) = b_{n-1}x^{n-1} + \ldots\ldots\ldots\ldots + b_0 & si\ a_i = 1 \\ 0 & si\ a_i = 0 \end{cases}$$

$$\left.\begin{array}{l} a(x) = x^2+1 \\ p(x) = x^3+x+1 \end{array}\right\} GC(2^3)$$

$a(x)^2 \Rightarrow (1\,0\,1)$

esto es la operación lógica AND

$$\begin{array}{r} 1\,0\,1 \\ 1\,0\,1 \\ \hline 1\,0\,1 \\ \oplus\ 1\,0\,1\ \ \ \ \\ \hline 1\,0\,0\,0\,1 \end{array} \bmod p(x)$$

$$\begin{array}{r|l} 10001 & 1011 \\ 1011 & 10 \\ \hline 00111 & \end{array}$$

$a^2(x) = 111 = \boxed{x^2+x+1}$

Multiplicación en Cuerpos de Galois CG(2^n)

- Ej. $a(x) = x^2 + 1 = (101)$ cálculo de c=a · a en CG(2^3) [n=3] con mód p(x) = $x^3 + x + 1$ =(1011)

  a · a=(101) · (101)

$$
\begin{array}{ccccc}
 & & 1 & 0 & 1 \\
 & & 1 & 0 & 1 \\
\hline
 & & 1 & 0 & 1 \\
1 & 0 & 1 & & \\
\hline
1 & 0 & 0 & 0 & 1
\end{array}
$$

Si el coeficiente que multiplica es 1, se copia el polinomio superior en su correspondiente sitio, si no, nada (la multiplicación es un AND)

Esta suma es un XOR

reduciendo mód p(x)

$$
\begin{array}{l|l}
10001 & 1011 \\
\cline{2-2}
1011 & 10 \\
\cline{1-1}
00111 & \\
....000 & \\
\cline{1-1}
....111 &
\end{array}
$$

Esta resta es un XOR también

Un polinomio en CG(2^n) es divisible entre otro ("cabe") si tiene el mismo número de bits o más

Hemos acabado cuando el polinomio que queda tiene n bits (menos bits que p(x), que se representa con n+1 bits)

El resultado final es c = (111) = $x^2 + x + 1$

División en Cuerpos de Galois

- Para realizar "b/a" mód p(x), necesitamos calcular $a^{-1} \cdot b$ mód p(x)
- Ya que p(x) es irreducible , $\forall a(x) \in CG(2^n)$ es coprimo con p(x), excepto el polinomio nulo
- Por tanto $\Phi(p(x))$, el número de elementos coprimos con p(x) es:

$$\Phi(p(x)) = 2^n - 1$$

Por tanto

$$a^{-1} = a^{\Phi(p(x))-1} \, mód \; p(x) = a^{2^n - 2} \, mód \; p(x)$$

$$\left.\begin{array}{l} a(x) = x^2 \\ p(x) = x^3 + x + 1 \end{array}\right\} GC(2^3)$$

$a(x)^{-1} \longrightarrow (100)$

$a^{-1} = a^{(2^3-1)-1} \bmod p(x) =$

$= (100)^6 \bmod p(x) =$

$= (100)^2 (100)^4 \bmod p(x) =$

$= (110)(110)^2 \bmod p(x)$

$= (110)(10) \bmod p(x)$

$= 1100 \bmod p(x)$

$\boxed{a^{-1} = 111 \bmod p(x)}$

$$\begin{array}{r} 100 \\ 100 \\ \hline 10000 \end{array} \qquad \begin{array}{r} 10000 \\ 1011 \\ \hline 00110 \end{array} \; \underline{|\,1011} \; 10$$

$$\begin{array}{r} 110 \\ 110 \\ \hline 000 \\ 110 \\ 110 \\ \hline 10100 \end{array} \qquad \begin{array}{r} 10100 \\ 1011 \\ \hline 00010 \end{array} \; \underline{|\,1011} \; 1$$

1100 | 1011
1011 | 1
0111

División en Cuerpos de Galois

- Ej. Halle el inverso de a(x)=(100)=x^2 en CG(2^3) con el mód p(x)=x^3+x+1=(1011)

$$a^{-1} = (100)^{2^3-2}\, m\acute{o}d(1001) = (100)^6\, m\acute{o}d(1011)$$

- Para calcular, vamos a desarrollarlo de esta forma (por ejemplo)

$$(100)^6 = (100)^2 (100)^4\, m\acute{o}d(1011)$$

División en Cuerpos de Galois

- Veamos cuanto vale $(100)^2$mód(1011)=(10000)mód(1011)=110

$$
\begin{array}{l|l}
10000 & 1011 \\ \cline{2-2}
1011 & 10 \\ \cline{1-1}
00110 & \\
....000 & \\ \cline{1-1}
....110 &
\end{array}
$$

- Veamos cuanto vale $(100)^4$mód(1011) = $(100)^2(100)^2$ = $(110)^2$mód(1011)

$$
\begin{array}{ccccc}
 & & 1 & 1 & 0 \\
 & & 1 & 1 & 0 \\ \hline
 & 1 & 1 & 0 & \\
1 & 1 & 0 & & \\ \hline
1 & 0 & 1 & 0 & 0
\end{array}
\qquad
\begin{array}{l|l}
10100 & 1011 \\ \cline{2-2}
1011 & 10 \\ \cline{1-1}
00010 & \\
..0000 & \\ \cline{1-1}
..0010 &
\end{array}
$$

División en Cuerpos de Galois

- Luego

$$(100)^6 = (100)^4(100)^2 \, m\acute{o}d(1011) = (110)(010) \, m\acute{o}d(1011) = (1100) \, m\acute{o}d(1011) = (111)$$

- Por tanto el inverso de $a(x)=(100)=x^2$ es $a^{-1}(x)=(111)=x^2+x+1$

Multiplicación en Cuerpos de Galois CG(2^n)

- Operación *xtime*:
- Xtime es "multiplicar por x", es decir, multiplicar por (10)
- Idea general:
  - Supongamos que estamos trabajando en CG(2^3).
  - Multiplicar el polinomio $a(x)=(a_2a_1a_0)$ por (10) es equivalente a desplazar 1 posición a la izquierda los "bits" de a(x). Llamémos a este polinomio desplazado a'(x).

$$a'(x) = (a_2a_1a_0) \cdot (10) \text{ mód } p(x) = (a_2a_1a_0 0) \text{ mód } p(x)$$

$(a_2 a_1 a_0)(010) = \cancel{\alpha_2}\, a_2 a_1 a_0 \varnothing$ y lo reducimos.

$(111)(010) = 1110$

$\oplus\ 1011 = p(x)$

0101

  - Si $a_2 = 0$, a'(x) es el resultado final:
    - $(a_1a_0 0)$
  - Si $a_2 = 1$, a'(x) debe reducirse mod. p(x) para obtener el resultado final:
    - ESTA REDUCCIÓN EQUIVALE A REALIZAR a'(x) XOR p(x)
    - $a(x) \cdot (10) \bmod p(x) = a'(x) \text{ XOR } p(x)$

↳ es una potencia de 10

$$a^{-1} = (100)^6 \bmod (1011)$$

$100 = (10)^2$

$$= (x^2)^6 \bmod (1011)$$

$$= x^{12} \bmod (1011)$$

$$x^3 = (100)(010) = 1000 + 1011 = 011$$

↳ pasa p(x)

$$x^4 = (011)(010) = 0110 = 110$$

como no pasa p(x)

$$x^5 = (0110)(010) = 1100 + 1011 = 0111 = 111$$

$$x^6 = (111)(010) = 1110 + 1011 = 0101 = 101$$

$$x^7 = (101)(010) = 1010 + 1011 = 0001 = 1$$

$\vdots \qquad \vdots$

Multiplicación en Cuerpos de Galois CG(2^n)

- Los ordenadores pueden computar muy eficientemente *xtime*:
  - $a^{-1} = (100)^6 \bmod (1011) = (x^2)^6 \bmod (x^3+x+1) =$
  - $= x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x^2 \bmod (x^3+x+1)$
  - $(010)(100) = (1000) \oplus (1011) = 011$ $\quad x^3 \bmod (x^3+x+1) = x+1$
  - $(010)(011) = (110)$ $\quad x^4 \bmod (x^3+x+1) = x^2 + x$
  - $(010)(110) = (1100) \oplus (1011) = 111$ $\quad x^5 \bmod (x^3+x+1) = x^2\, x+1$
  - $(010)(111) = (1110) \oplus (1011) = 101$ $\quad x^6 \bmod (x^3+x+1) = x^2 +1$
  - $(010)(101) = (1010) \oplus (1011) = 001$ $\quad x^7 \bmod (x^3+x+1) = 1$
  - $(010)(001) = (010)$ $\quad x^8 \bmod (x^3+x+1) = x$
  - $(010)(010) = (100)$ $\quad x^9 \bmod (x^3+x+1) = x^2$
  - $(010)(100) = (1000) \oplus (1011) = 011$ $\quad x^{10} \bmod (x^3+x+1) = x+1$
  - $(010)(011) = (110)$ $\quad x^{11} \bmod (x^3+x+1) = x^2 + x$
  - $(010)(110) = (1100) \oplus (1011) = 111$ $\quad x^{12} \bmod (x^3+x+1) = x^2\, x+1$