Cálculo de inversos

Si queremos calcular a^{-1} para algún $\overset{\neq 0}{a} \in F = \mathbb{F}_q[x]/(f)$

estamos buscando b tal que $a.b = 1 \quad (f)$
y como f es irreducible y $a \neq 0 \ (f)$ entonces $\text{mcd}(a, f) = 1$ y por lo tanto usando el algoritmo de Euclides podemos escribir

$$1 = b.a + c.f$$

Por ejemplo: Supongamos que buscamos el inverso del elemento $a = \alpha^2+\alpha$ en $\mathbb{F}_8$.

$$\mathbb{F}_8 = \mathbb{F}_2(\alpha) \qquad \alpha^3+\alpha+1=0$$

$$= \mathbb{F}_2[x]/(x^3+x+1)$$

$$= \{0, 1, \alpha, \underbrace{\alpha+1}_{a^{-1}}, \alpha^2, \alpha^2+1, \overbrace{\alpha^2+\alpha}^{a}, \alpha^2+\alpha+1\}$$

$$\begin{array}{l|l}
\alpha^3+\alpha+1 & \alpha^2+\alpha \\ \hline
-\alpha^3+\alpha^2 & \alpha+1 \\ \hline
\alpha^2+\alpha+1 & \\
-\alpha^2+\alpha & \\ \hline
1 &
\end{array}$$

$$\alpha^3+\alpha+1 = \underbrace{(\alpha^2+\alpha)}\underbrace{(\alpha+1)}+1$$

$$\Rightarrow (\alpha^2+\alpha)^{-1} = \alpha+1$$

$\mathbb{F}_7 = \{0,1,2,3,4,5,6\}$ $\qquad 2.b = 1 \quad (7)$

$2^{-1} = 4$

$7 \underline{|\ 2\ }$

$\ \ 1 \quad 3$

$7 = 2.3+1$

$0 \equiv 2.3+1 \quad (7)$

$2.4 = 8 \equiv 1 \quad (7)$

$2(-3) \equiv 1 \quad (7)$

Como $-3 \equiv \underbrace{4} \quad (7)$

<u>Exponenciación</u>

$a \in F = \mathbb{F}_q$ $\qquad a^q = a$

$= \mathbb{F}_p(\alpha)$ $\qquad f(\alpha) = 0$

$a^n = \underbrace{a.a\ldots a}_{n \text{ veces}}$

Supongamos que queremos calcular a^n módulo m con $a, m \in \mathbb{Z}$, $n \in \mathbb{N}$. Si $n = s_0 + s_1.2 + \ldots + s_{k-1}2^{k-1}$ (expresión binaria de n) el siguiente algoritmo nos permite calcular la potencia utilizando multiplicaciones:

$b = 1$

Desde $j = k-1$ hasta 0

si $s_j = 1$ entonces $b = b * a \pmod m$

si $j > 0$ entonces $b = b^2 \pmod m$

El resultado es $a^n = b \pmod n$

Ejemplo: 3^{67} (5) $\quad a=3$

$b=1$

Desde $j=k-1$ hasta 0:

si $s_j=1 \Rightarrow b=b\cdot a$ (m)

si $j>0 \Rightarrow b=b^2$

$$67 = \underset{s_6}{1}\cdot 2^6 + \underset{s_5}{0}\cdot 2^5 + \underset{s_4}{0}\cdot 2^4 + \underset{s_3}{0}\cdot 2^3 + \underset{s_2}{0}\cdot 2^2 + \underset{s_1}{1}\cdot 2 + \underset{s_0}{1}\cdot 2^0$$

$b=1$

$j=6 \quad b=b\cdot a = 3 \qquad b=3^2=9 \equiv 4 \ (5)$

$j=5 \quad b=4^2=16 \equiv 1 \ (5)$

$j=4 \quad b=1$

$j=3 \quad b=1$

$j=2 \quad b=1$

$j=1 \quad b=1\cdot 3 = 3 \qquad b=4 \ (5)$

$j=0 \quad b=4\cdot 3 = 12 = 2 \ (5)$

$\Rightarrow$ Retornar: $2 = 3^{67} \ (5)$

El mismo algoritmo (la misma idea) puede adaptarse para hacer la cuenta con la operación en un cuerpo finito $\mathbb{F}_q$ no necesariamente con q primo.

Exemplo: $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ $\quad \alpha^3+\alpha^2+1=0$ $\qquad \alpha^6 = \alpha^2+\alpha.$

$$\alpha^3 = \alpha^2+1$$
$$\alpha^4 = \alpha.\alpha^3 = \alpha(\alpha^2+1) = \alpha^3+\alpha = \alpha^2+1+\alpha$$
$$\alpha^5 = \alpha.\alpha^4 = \alpha^3+\alpha+\alpha^2 = \cancel{\alpha^2}+1+\alpha+\cancel{\alpha^2} = \alpha+1$$
$$\alpha^6 = \alpha.\alpha^5 = \alpha^2+\alpha.$$

Em este caso $\quad 6 = \underset{\substack{\uparrow \\ s_2}}{1}.2^2 + \underset{\substack{\uparrow \\ s_1}}{1}.2 + \underset{\substack{\uparrow \\ s_0}}{0}.2^0 \qquad a=\alpha$

$b=1$

$j=2 \quad b = 1.\alpha = \alpha \qquad\qquad b = \alpha^2$

$j=1 \quad b = \alpha^2.\alpha = \alpha^3 = \alpha^2+1 \qquad\qquad b = (\alpha^2+1)^2 =$

$= \alpha^4+1 =$

$= \alpha^2+\alpha$

$j=0 \longrightarrow$ retorno$(\alpha^2+\alpha)$

En el caso de cuerpos binarios, la exponenciación puede simplificarse usando bases normales

Proposición: Supongamos que $a \in F = \mathbb{F}_{q^m}$ y que $\mathcal{B} = \{\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}\}$ es una base normal de $F/K = \mathbb{F}_q$;

y sean $a_0, a_1, \dots, a_{m-1}$ los coeficientes de a en la base $\mathcal{B}$, es decir

$$a = a_0 \cdot \alpha + a_1 \alpha^q + \dots + a_{m-1} \alpha^{q^{m-1}} \qquad a_0, \dots, a_{m-1} \in K$$

Entonces el elemento a^q tiene por coeficientes a $a_{m-1}, a_0, \dots, a_{m-2}$

es decir

$$a^q = a_{m-1} \alpha + a_0 \alpha^q + \dots + a_{m-2} \alpha^{q^{m-1}}$$

Demostración

$$a^q = \left(a_0 \alpha + a_1 \alpha^q + \dots + a_{m-1} \alpha^{q^{m-1}}\right)^q$$

$$= \underset{\textstyle a_0}{\underset{\shortparallel}{a_0^q}} \alpha^q + \underset{\textstyle a_1}{\underset{\shortparallel}{a_1^q}} \alpha^{q^2} + \dots + \underset{\textstyle a_{m-1}}{\underset{\shortparallel}{a_{m-1}^q}} \underset{\textstyle \alpha}{\underset{\shortparallel}{\alpha^{q^m}}}$$

$$= a_{m-1} \alpha + a_0 \alpha^q + \dots + a_{m-2} \alpha^{q^{m-1}}$$

$\blacksquare$

Luego en el caso $q=2$ y $\mathbb{F}=\mathbb{F}_{2^m}$ la elevación al cuadrado tiene costo cero pues implica simplemente una permutación circular.

Ejemplo $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ $\alpha^3+\alpha^2+1=0$ $\{\alpha, \alpha^2, \alpha^4\}$

$$\alpha^3 = \alpha^2+1$$
$$\alpha^4 = \alpha^3+\alpha = \alpha^2+\alpha+1$$

$$a = a_0\,\alpha + a_1\,\alpha^2 + a_2\,\alpha^4$$
$$a^2 = a_2\,\alpha + a_0\,\alpha^2 + a_1\,\alpha^4$$

en particular

$$a = \alpha^2+1$$
$$a = \cancel{\alpha^2} + \alpha^4 + \cancel{\alpha^2} + \alpha =$$
$$a = 1.\alpha + 0.\alpha^2 + 1.\alpha^4$$

$$a^2 = 1.\alpha + 1.\alpha^2 + 0.\alpha^4 = \alpha+\alpha^2.$$

$$a^2 = (\alpha^2+1)^2 = \alpha^4+1 = \cancel{\alpha^4} + \cancel{\alpha^4} + \alpha^2 + \alpha = \alpha^2+\alpha.$$

Revisamos ejercicios

<u>Ejercicio</u>: Considerar $\mathbb{F}_{27} = \mathbb{F}_3(\alpha)$ $\quad \alpha^3 + 2\alpha + 1 = 0$

1) Verificar que $p(x) = x^3 + 2x + 1$ es irreducible$/\mathbb{F}_3$.

2) Calcular las tablas de mult. para la base $\{\underbrace{1}_{\alpha_0}, \underbrace{\alpha}_{\alpha_1}, \underbrace{\alpha^2}_{\alpha_2}\}$

1) $p(0) = 1 \qquad p(1) = 1 \qquad p(2) = 1$

2)

$$\alpha_0 \cdot \alpha_0 = 1 \cdot 1 = 1 = \underbrace{1}_{t^0_{00}} \cdot \alpha_0 + \underbrace{0}_{t^1_{00}} \cdot \alpha_1 + \underbrace{0}_{t^2_{00}} \cdot \alpha_2$$

$$\alpha_0 \cdot \alpha_1 = 1 \cdot \alpha = \alpha = \underbrace{0}_{t^0_{01}} \cdot \alpha_0 + \underbrace{1}_{t^1_{01}} \cdot \alpha_1 + \underbrace{0}_{t^2_{01}} \cdot \alpha_2$$

$$\alpha_0 \cdot \alpha_2 = 1 \cdot \alpha^2 = \underbrace{0}_{t^0_{02}} \cdot \alpha_0 + \underbrace{0}_{t^1_{02}} \cdot \alpha_1 + \underbrace{1}_{t^2_{02}} \cdot \alpha_2$$

$$T_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix} \qquad T_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

$$T_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

$\{1, \alpha, \alpha^2\}$, $\alpha = \alpha_1$, $\alpha^2 = \alpha_2$

$\alpha^3 + 2\alpha + 1 = 0$

$\alpha^3 = -2\alpha - 1$

$\alpha^3 = \alpha + 2$

$$\alpha_1 . \alpha_2 = \alpha . \alpha^2 = \alpha^3 = 2 + \alpha$$
$$= 2 . 1 + 1 . \alpha + 0 . \alpha^2$$
$$= 2 . \alpha_0 + 1 . \alpha_1 + 0 . \alpha_2$$

$\rightarrow$ $t_{12}^{0} = 2$ $\quad t_{12}^{1} = 1$ $\quad t_{12}^{2} = 0$

$$\underbrace{\alpha_1}.\underbrace{\alpha_1} = \alpha . \alpha = \alpha^2 = 0 . 1 + 0 . \alpha + 1 . \alpha^2$$
$$= 0 . \alpha_0 + 0 . \alpha_1 + 1 . \alpha_2$$

$t_{\underbrace{11}}^{0} = 0$ $\quad t_{\underbrace{11}}^{1} = 0$ $\quad t_{\underbrace{11}}^{2} = 1$

$$\alpha_2 . \alpha_2 = \alpha^2 . \alpha^2 = \alpha^4 = \alpha . \alpha^3 = \alpha(\alpha + 2)$$
$$= \alpha^2 + 2\alpha = 0 . \underbrace{\overset{\alpha_0}{1}} + 2 . \overset{\alpha_1}{\alpha} + 1 . \overset{\alpha_2}{\alpha^2}$$

$t_{22}^{0} = 0$ $\quad t_{22}^{1} = 2$ $\quad t_{22}^{2} = 1$

$$(a_0 \cdot 1 + a_1 \cdot \alpha + a_2 \alpha^2)(b_0 \cdot 1 + b_1 \alpha + b_2 \alpha^2)$$

$\mathbb{F}_{27}$

$$a = 2 + 2\alpha + \alpha^2$$

$$b = 2\alpha^2 + \alpha + 1$$

$$a \cdot b = \underset{(2,2,1)}{(2 + 2\alpha + \alpha^2)} \; \underset{(1,1,2)}{(2\alpha^2 + \alpha + 1)} = c_0 + c_1\alpha + c_2\alpha^2$$

i) Hacerlo a mano.

ii) Hacerlo con las tablas.

$$c_0 = (2,2,1)\, T_0 \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}. \qquad c_1 = (2,2,1)\, T_1 \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$$

$$c_2 = (2,2,1)\, T_2 \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$$

$$\alpha^3+2\alpha+1=0$$

$$\alpha_i \cdot \alpha_j = t_{ij}^0 \cdot \alpha_0 + t_{ij}^1 \alpha_1 + \dots + t_{ij}^n \alpha_n .$$

$$\alpha^3 = 2\alpha+1$$

2.12

$a \in \mathbb{F}_q$ $\quad b \in \mathbb{F}_q$ $\quad b^p = a$

$p = \mathrm{char}(\mathbb{F}_q)$

$$\underbrace{\sigma : \mathbb{F}_q \to \mathbb{F}_q \,/\, \sigma(z) = z^{p^n}.}$$

es inyectivo.

$x^{p^n} = y^{p^n}$

$x^{p^n} - y^{p^n} = 0$

$(x-y)^{p^n} = 0 \to x - y = 0 \to x = y.$

Ejercicio $\quad \mathbb{F}_{p^n = q} \quad \alpha^q = \alpha$

$$\mathbb{F}_q^* = \langle \alpha \rangle = \langle \alpha^p \rangle = \langle \alpha^{p^n} \rangle$$

(2.13) Símbolo de Legendre: $\left(\frac{a}{q}\right) = \begin{cases} 1 & \text{si } a \text{ es un } \square \text{ en } \mathbb{F}_q \\ -1 & \text{si } a \text{ no es un } \square \text{ en } \mathbb{F}_q. \end{cases}$

$a^{\frac{p-1}{2}} = \left(\frac{a}{q}\right)$

$\underbrace{a \text{ tiene una raiz cuadrada}}_{\exists\, b \in \mathbb{F}_q \quad b^2 = a} \overset{\Longrightarrow}{\Longleftarrow} a^{p-1/2} = 1.$

$\Rightarrow a^{p-1/2} = (b^2)^{\frac{q-1}{2}} = b^{q-1} = 1.$

$\Leftarrow)$ q es impar $\Rightarrow F^* = \langle g \rangle \quad g \neq 1.$

$a = g^k = \boxed{\left(g^{k/2}\right)^2} \rightarrow b.$

$q-1 = 2.l \rightarrow l = \frac{(q-1)}{2}$

$1 = a^{p-1/2} = (g^k)^{p-1/2} = g^{k.l}$

$q-1 \mid k.l$

$k.l = r.(q-1)$

$k.\frac{(q-1)}{2} = r.(q-1)$

$k = 2r. \qquad b = g^r \quad b^2 = a.$

SAGE - COCALC

is_normal_basis(α)

$\{\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}\}$

GF(p)

GF(p^2) ← GF(p^2, 'a')

$\left| Tr(\alpha_i \alpha_j) \right| \neq 0$