$$\mathbb{F}_{p^m} := \frac{\mathbb{F}_p[x]}{(f)}$$

CUERPO FINITO CON p^m ELEMENTOS

f UN POLINOMIO IRREDUCIBLE GRADO m

$a(x)$, $\deg(a) \leq n$: $a(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$

LO REPRESENTAMOS POR $a = (a_0, \ldots, a_{m-1}) \in \mathbb{F}_p$

LOS ELEMENTOS DE $\mathbb{F}_{p^m}$ SON VECTORES DE $\mathbb{F}_p^m$ (QUE REPRESENTAN LOS COEFICIENTES DE LA CLASE DE UN POLINOMIO MÓDULO f)

$+$? SUMA COORDENADA A COORDENADA

$a = (a_0, \_, a_{n-1})$

$b = (b_0, \_, b_{n-1})$

$\Big\}$ $a + b = (\underbrace{a_0 + b_0}_{\text{EN } \mathbb{F}_p}\ g \ \_ \ g \underbrace{a_{n-1} + b_{n-1}}_{\text{EN } \mathbb{F}_p})$

Y ES COMPATIBLE CON $a(x) + b(x)$ EN $\mathbb{F}_p[x]$

- ? MULTIPLICACIÓN MÓDULO f

$a \cdot b = ?$

$\exists!\ q(x), r(x)$, $\deg r(x) < \deg(f) = n$ /

$a(x)\, b(x) = q(x) f(x) + r(x)$

$a \cdot b = r$ I.E. $a \cdot b$ ES $a(x) \cdot b(x)$ MOD f

$(\mathbb{F}_{p^m}, +, \cdot)$ ES UN CUERPO $\quad 0 = 0_+$, $1 = 1_\cdot$

¿INVERSO? ALGORITMO EUCLIDES EXTENDIDO

EXISTENCIA: a^{-1}? $a \neq 0$

$\Delta = \{a \cdot h \mid h \in \mathbb{F}_{p^m} \setminus \{0\}\}$ ← TENEMOS QUE DEMOSTRAR QUE $1 \in \Delta$

- $0 \notin \Delta$, SI NO $f(x) \mid a(x)$ o $f(x) \mid h(x)$
- Y SON DIFERENTES: SI $a \cdot h_1 = a h_2 \Rightarrow$

$f(x) \mid a(x)(h_1(x) - h_2(x)) \Rightarrow f(x) \mid a(x)$ o $f(x) \mid (h_1(x) - h_2(x))$

↑ f IRREDUCIBLE

PERO $\deg(a(x)) < \deg(f)$ Y $\deg(h_1 - h_2) < \deg(f)$

$\Rightarrow h_1(x) = h_2(x)$

$\Rightarrow A = \mathbb{F}_{pm} \setminus \langle 0, q \rangle \quad y \quad 1 \in A.$

Ej: $\mathbb{F}_4 = \mathbb{F}_2[x]/(f)$ $\qquad f = x^2 + x + 1$

$\mathbb{F}_4 \neq \mathbb{Z}_4 \qquad \mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$

$\mathbb{F}_4 = \{0, 1, x, x+1\}$

$\mathbb{F}_4 = \{(0,0), (1,0), (0,1), (1,1)\}$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

+	(00)	(10)	(01)	(11)
(00)	(0,0)	(1,0)	(0,1)	(1,1)
(10)	(1,0)	(0,0)	(1,1)	(0,1)
(01)	(0,1)	(1,1)	(0,0)	(1,0)
(11)	(1,1)	(0,1)	(1,0)	(0,0)

$\cdot$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

$$f = X^2 + X + 1$$

$X \cdot X = X^2 = X + 1$

$X^2 \quad \lfloor X^2+X+1$

$\underline{X^2+X+1} \quad 1$

$X+1$

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

$X^2+1 \quad \lfloor X^2+X+1$

$\underline{X^2+X+1} \quad 1$

X

$X+1 \cdot X = X^2 + X$

$X^2+X \quad \lfloor X^2+X+1$

$\underline{X^2+X+1} \quad 1$

1

TRUC $\quad X^2 + X + 1 = 0$

$\Rightarrow X^2 = X + 1$ | $\Rightarrow X^2 + X = 1$

$\Rightarrow X^2 + 1 = X$

$a(x)\,b(x) = r(x)$ DONDE

$a(x)\,b(x) = q(x)\,f(x) + r(x)$ CON

$\deg(r(x)) < \deg f(x)$

$$\mathbb{F}_4 = \mathbb{F}_2[x]/_{x^2+x+1} = \mathbb{F}_2^2 = \{0\} \cup \{\alpha^i / i = 0,1,2\}$$

$\{0, 1, x, x+1\}$

$\{(0,0), (1,0), (0,1), (1,1)\}$

$\{0\} \cup \{\alpha^0, \alpha^1, \alpha^2\}$

$\alpha = [x]$

$\alpha^0 = x^0 = 1$

$\alpha^1 = x^1 = x$

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

$$\mathbb{F}_{q=p^m} = \mathbb{F}_p[x]/(f) = \mathbb{F}_p^m = \{0\} \cup \{\alpha^i \mid i = 0, \dots, q-2\}$$

$\deg(f) = m$

f IRREDUCIBLE

$(a_0, \dots, a_{m-1})$

$a_i \in \mathbb{F}_p$

$a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$

$\alpha = x$

0

α^i $\quad i = 0, \dots, q-2$

EXPONENTES MODULO $q-1$

$0 \cdot \alpha^i = 0 \qquad 0 \cdot 0 = 0$

$\alpha^i \cdot \alpha^j = \alpha^{i+j}$ MODULO $q-1$

MUY FÁCIL

$\alpha^i + \alpha^j = x^i + x^j \rightarrow$ MODULO f NO FÁCIL

¿CÓMO SUMA Y MULTIPLICA UN ORDENADOR?

·	0	$1 = \alpha^0$	α^1	α^2
0	0	0	0	0
$1 = \alpha^0$	0	$\alpha^0 = 1$	α^1	α^2
α^1	0	α^1	α^2	$\alpha^0 = 1$
α^2	0	α^2	$\alpha^0 = 1$	α^1

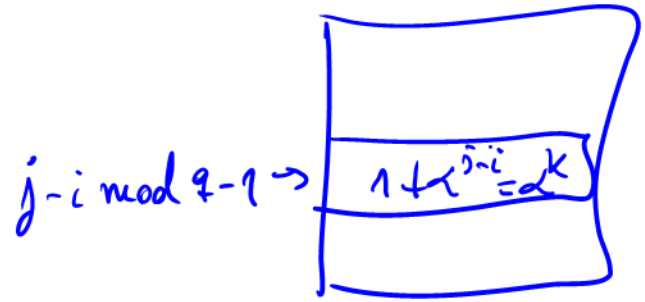
$q-1=3$

$\alpha^3 = \alpha^0$

$\alpha^4 = \alpha$

$q-1$ = MODULO 3 EXPONENTES

$+$? TABLA $1+\alpha^i$



NO ES NECESARIO HACER UNA BÚSQUEDA

$$\alpha^i + \alpha^j = \alpha^i \left(\underbrace{1+\alpha^{j-i}}\right) = \alpha^i \alpha^k = \alpha^{i+k \bmod q-1}$$

MIRAMOS TABLA $\rightarrow \alpha^k$

↳ QUE ES UN SIMPLE ARRAY

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

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

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

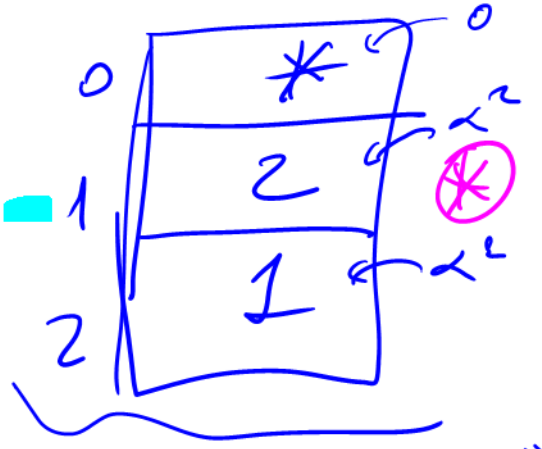


TABLA "$1+\alpha^{FILA}$"

$x^2 + x + 1 = 0$

$\alpha^0 = 1$, $\alpha^1 = x$, $\alpha^2 = x+1$

$\alpha + \alpha^2 = \alpha(1 + \alpha^1) = \alpha(\alpha^2) = \alpha^3 = \alpha^{3 \bmod 3} = \alpha^0 = 1$

$x + x^2 = 1$

$x^2 + x + 1 = 0$

$(x^2 + x) = 1$

ORDENADOR MEJOR 3º FORMA GRACIAS A LA TABLA. MÁS RÁPIDO

PERO SIEMPRE PODEMOS TRABAJAR DE FORMA 1º y 2ª

$\mathbb{F}_{16}$ $(0\,1\,0\,0) \equiv X \equiv \alpha$

(PAG 25 JOSTEINSEN HØHOLDT)

ex 7.7.3.

$X^0 = 1$, $X^1 = X$, $X^2 = X^2$, $X^3 = X^3$, $X^4 = \alpha^4 = X + 1$

$\mathbb{F}_{16} = \mathbb{F}_2[X]/(f)$ $\qquad f = X^4 + X + 1$