Cuerpos finitos $\mathbb{F}_p$

Si p es un numero primo

los enteros modulo p $\left(\mathbb{Z}/_{p}\mathbb{Z}\right)$ ← notación

forman un cuerpo $\left(\{0;1;\dots;p-1\};+;\cdot\right)$

y se denota $\mathbb{F}_p$. Tiene p elementos

Obs: $\mathbb{Z}/_6\mathbb{Z}$ no es un cuerpo porque $2x \equiv 1 \pmod 6$ no tiene solución } esto pasa cuando se elige p que no sea numero primo

Ej: $\mathbb{F}_7$

Tabla a^6 en $\mathbb{F}_7$

a	2	3	4	5	6	
2	4	1	2	4	.....	orden (2) = 3
3	2	6	4	5	1 ...	orden (3) = 6
4	2	1 ...				orden (4) = 3
5	4	6	2	3	1	orden (5) = 6
6	1					orden (6) = 2

$$2^{50} = 2^{48} \cdot 2$$
$$= (2^3)^{16} \cdot 2^2$$
$$= 1 \cdot 4$$
$$2^{50} = 4 \pmod 7$$

Teorema Lagrange: orden (a) siempre divide $(p-1)$

notación multiplicativo

no es x equis

Teorema

① El "grupo multiplicativo" $\mathbb{F}_p^{\times}$

$(\{1; \dots ; p-1\} ; \cdot)$ es un grupo

② $\mathbb{F}_p^{\times}$ es cíclico, es decir, existe por lo menos un elemento $a \in \mathbb{F}_p^{\times}$ tal que $\text{orden}(a) = p-1$, en otras palabras

a "genera" todo $\mathbb{F}_p^{\times}$

Protocolo de intercambio de claves Diffie-Hellman

Permite a dos partes (Alice y Bob) establecer una clave secreta, sin haber compartido previamente ninguna informacion secreta

1) - Se elige un numero primo p (grande)

2) - Se elige un generador g de $\mathbb{F}_p^{\times}$

3) - Alice elige un numero secreto a
   Bob elige un numero secreto b

4) - Alice calcula $A \equiv g^a \pmod p$
   Bob calcula $B \equiv g^b \pmod p$

5) - Se comparte A y B

6) - Clave compartida

Alice calcula $B^a \equiv (g^a)^b = g^{ab} \equiv K \pmod p$

Bob calcula $A^b \equiv (g^b)^a = g^{ab} \equiv K \pmod p$

La clave es K

Ejemplo

$$\begin{cases} p = 23 & g = 5 \\ a = 6 & b = 15 \end{cases}$$

$$A \equiv 5^6 \equiv 2^3 \equiv 8 \pmod{23}$$

$$B \equiv 5^{15} \equiv 5^6 . 5^6 . 5^3 = 8.8.10 \equiv (-5).10 \equiv 19 \pmod{23}$$

Alice calcula $19^6 \equiv (-4)^6 \equiv 5^2 \equiv 2 \pmod{23}$

$$\left((-4)^3 = -64 \equiv 5 \pmod{23}\right)$$

Bob calcula $8^{15} \equiv (8^4)^3 . 8^3 \equiv 2^3 . 8^3$

$\left(8^4 \equiv 2 \pmod{23}\right)$ $\equiv 8^4 \equiv 2 \pmod{23}$

Sea $p > 3$ un numero primo (no se elige 2 y 3 por que complica el calculo)

Una curva eliptica sobre $\mathbb{F}_p$ es el conjunto de soluciones de

$$E: \quad y^2 = x^3 + ax + b$$

(Ecuacion de Weierstrass)

donde $a, b \in \mathbb{F}_p$, junto con el "punto en el infinito" O,

y tal que $\Delta \equiv 4a^3 + 27b^2 \not\equiv 0 \pmod{p}$

Denotamos por $E(\mathbb{F}_p)$ los puntos racionales al conjunto (x, y) tal que $x, y \in \mathbb{F}_p$ satisfacen la ecuacion E

Ej: $y^2 = x^3 + 2x + 1 \quad / \quad \mathbb{F}_5$

Calculo de $E(\mathbb{F}_5)$

m	m^2
0	0
1	1
2	4
3	4
4	1

m	$m^3 + 2m + 1$
0	1
1	4
2	3
3	4
4	3

$$E(\mathbb{F}_5) = \{(0;\pm 1); (1;\pm 2); (3;\pm 2); \underset{\text{el infinito}}{O}\} \quad \not\ni (0;0)$$

Esta CE tiene 7 puntos racionales

$P = (x_1, y_1)$; $Q = (x_2, y_2)$

Si $x_1 \neq x_2 \rightsquigarrow \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

$x_1 = x_2 \rightsquigarrow \lambda = \dfrac{3x_1^2 + a}{2y_1}$

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1 \qquad P + Q = (x_3; y_3)$

Tomemos $P = (0;1)$; $Q = (1;2)$

$x_2 - x_1 = 1 - 0 = 1$

$\lambda = y_2 - y_1 = 2 - 1 = 1$

$x_3 = 1 - 0 - 1 = 0$

$y_3 = 1.(0 - 0) - 1 = -1$

Luego $(0;1)$ "+" $(1;2) = (0;-1)$

Esta suma "+" hace que $\mathbb{F}_p$ sea un grupo

$P(0;1)$

$2P = P + P$

Como $x_1 = x_2 \rightarrow \lambda = \dfrac{3x_1^2 + a}{2y_1} = \dfrac{3.0^2 + 2}{2} = 2.2^{-1} = 1$

$x_3 = 1^2 - 0 - 0 = 1$

$y_3 = 1.(0-1) - 1 = -2$ $\qquad 2P = (1; -2)$

$3P = 2P + P$

$x_1 \neq x_2 \qquad \lambda = \dfrac{-2-1}{1-0} = -3$

$x_3 = 4 - 1 - 0 = 3$ $\qquad 3P = (3; -2)$

$y_3 = (-3).(1-3) - (-2) = 3$
$\downarrow$
$= -2 \pmod 5$

$4P = 2(2P) = 2.(1;-2)$

$\lambda = \dfrac{3(1)^2 + 2}{2(-2)} = \dfrac{0}{-4} = 0$

$x_3 = \lambda^2 - 2x_1 = 0 - 2(1) = -2 = 3 \pmod 5$ $\qquad 4P = (3; 2)$

$y_3 = \cancel{\lambda}^{0}(x_1 - x_3) - y_1 = -y_1 = 2$

$5P = 4P + P$

inv multiplicativo

$\lambda = \dfrac{1-2}{0-3} = \dfrac{1}{3} = 2$

$x_3 = 2^2 - 0 - 3 = 1$ $\qquad 5P = (1; 2)$

$y_3 = 2(3-1) - 2 = 2$

$6P = 2(3P) \qquad \lambda = \dfrac{3.3^2 + 2}{2.(-2)} = \dfrac{4}{-4} = -1$

$x_3 = (-1)^2 - 2(3) = 1 - 6 = 0$ $\qquad 6P = (0; -1)$

$y_3 = -1(3-0) - (-2) = -1$

$7P = 0$

$P + 6P = 0$

$(0;1) + (0;-1)$

siempre $(x;y) + (x;-y) = 0$

Los cuerpos $\mathbb{F}_{p^2}$

$$\mathbb{F}_p \subset \mathbb{F}_{p^2}$$

Consideramos un polinomio de grado 2

$f \in \mathbb{F}_p[x]$; irreductible / analogo a primos pero en los polinomios

Ej $\mathbb{F}_2[x]_{\leq 2} = \{ \underbrace{0; 1; x; x+1}_{\text{grado } 1} ; \underbrace{x^2; x^2+x; x^2+1; x^2+x+1}_{\text{grado } 2} \}$

x^2+1 ← no irreductible porque $x^2+1 = 1(x^2+1)$
$= (x+1)(x+1)$

$x^2+x = x(x+1)$ ← no irred.

x^2+x+1 es irreductible

Entonces el cuerpo

$$\mathbb{F}_{2^2} \text{ "es" } \mathbb{F}_2[x]/(f)$$

esta formado por $\{0; 1; x; x+1\}$ (tiene $2^2 = 4$ elementos)

analogamente

$$(x) + (1) = (x+1)$$

$$(x+1) + (x) = \cancel{2}^{\,0} x + 1 = (1)$$

los coef estan en mod 2

$$2 \pmod 2 = 0$$

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

$$x(x+1) = x^2 + x \equiv 1 \pmod{x^2+x+1}$$

Ejercicio de desafío

$$E: \; y^2 = x^3 + 2x + 1 \; / \; \mathbb{F}_3 \text{ o } \mathbb{F}_2$$

$$E(\mathbb{F}_{3^2})$$

verificar que el discriminante no es cero