CUERPOS FINITOS

VIMOS: DADOS p PRIMO Y $d \in \mathbb{N}$, EXISTE UN ÚNICO (SALVO ISOMORFISMO) CUERPO K DE ORDEN p^d. PODEMOS OBTENER UN TAL K VÍA

$$K = \mathbb{Z}_p[X]/(f),$$

CON $f \in \mathbb{Z}_p[X]$ IRRED. DE GRADO d.

(EJEMPLO: PARA $d=1$, TOMAMOS $f(X) = X$; RESULTA QUE $\mathbb{F}_p = \mathbb{Z}_p[X]/(X) \simeq \mathbb{Z}_p$)

NOT: $K = \mathbb{F}_{p^d} = \mathbb{F}_q$

EJEMPLO: SEA $f(X) = X^2+X+1 \in \mathbb{F}_2[X]$.

f ES IRREDUCIBLE. SI NO, $f = g \cdot h$ CON g DE GRADO 1. LUEGO, COMO g TIENE UNA RAÍZ, f TAMBIÉN. PERO $f(0) = 1$; $f(1) = 1$. ABS!

$\rightsquigarrow$ ASÍ, $\mathbb{F}_4 = \mathbb{Z}_2[X]/(f)$ ES EL CUERPO FINITO DE CUATRO ELEMENTOS.

IMPORTANTE: $\mathbb{F}_4 \neq \mathbb{Z}_4$. $\mathbb{Z}_4$ NO ES UN CUERPO, YA QUE $2 \cdot 2 = 0$; EN GRAL, $\mathbb{Z}_m$ ES UN CUERPO SII m ES PRIMO.
$\neq 0 \quad \neq 0$

¿CÓMO HACEMOS CUENTAS EN $\mathbb{F}_4$? O PRIMERO, ¿QUIÉN ES $\mathbb{F}_4$? SON LOS POSIBLES RESTOS DE DIVIDIR POR f EN $\mathbb{Z}_2[X]$. EXPLÍCITAMENTE,

$\mathbb{F}_4 = \{0, 1, X, X+1\}$ (EN VERDAD, $\mathbb{F}_4 = \{\bar{0}, \bar{1}, \bar{X}, \overline{X+1}\}$; SON CLASES)

TABLA DE MULTIPLICACIÓN: TAL COMO HACEMOS EN $\mathbb{Z}/n$, MULTIPLICAMOS EN $\mathbb{F}_2[X]$ Y LUEGO DIVIDIMOS POR f.

·	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

SIMIL SUDOKU

- $X^2 = (X^2+X+1) + X+1 \equiv X+1 \ (f)$
- $X(X+1) = X^2+X \equiv X+X+1 \equiv 1 \ (f)$ (LUEGO, $(X+1)^{-1} = X$)
- $(X+1)(X+1) \equiv X \ (f)$

OBS: $\mathbb{F}_4^\times$ ES CÍCLICO, POR EJ $\mathbb{F}_4^\times = \{1, X, X^2 = X+1\}$, Y TAMBIÉN $\mathbb{F}_4^\times = \{1, X+1, (X+1)^2 = X\}$.

¿POR QUÉ LOS CUERPOS FINITOS TIENEN ORDEN p^d?
¿POR QUÉ NO HAY CUERPOS DE ÓRDENES 6, 100, ETC.?

DEF: $\mathbb{F}$ CUERPO. LA CARACTERÍSTICA DE $\mathbb{F}$ ES

$$\mathrm{car}(\mathbb{F}) := \min\{n \in \mathbb{N} : \underbrace{1+1+\cdots+1}_{n \text{ VECES}} = 0 \text{ EN } \mathbb{F}\} = \mathrm{ord}_{(\mathbb{F},+)}(1).$$

(SI TAL MÍN NO EXISTE, $\mathrm{car}(\mathbb{F}) = 0$)

PROP: SI $\mathbb{F}$ ES FINITO, $\mathrm{car}(\mathbb{F}) > 0$.

PROP: $\mathrm{car}(\mathbb{F})$ ES UN NÚMERO PRIMO, SI ES POSITIVO.

DEM: SI $\overline{m \cdot m} = 0$, ENTONCES $\bar{m} = 0$ Ó $\bar{m} = 0$ ⊠

SEA $\mathbb{F}$ CUERPO FINITO, Y SEA $p = \mathrm{car}(\mathbb{F})$.

LLAMEMOS $k = \{0, 1, \ldots, p-1\} \subseteq \mathbb{F}$ (MIRAR EL EJ. $\mathbb{F} = \mathbb{F}_4$)

AFIRMO: k ES UN CUERPO; DE HECHO, $k \simeq \mathbb{F}_p$.

LUEGO COMO $\mathbb{F}$ ES UN k-EV., SI $d = \dim_k(\mathbb{F})$ Y $\{v_1, \ldots, v_d\}$ ES UNA BASE DE $\mathbb{F}$ COMO k-EV,

↘ d<∞ PUES $\mathbb{F}$ ES FINITO

/2

SE TIENE QUE $\mathbb{F} = \{\sum_{i=1}^{d} a_i v_i : a_i \in k\}$ TIENE ORDEN $|k|^d = p^d$,
DE HECHO, $\mathbb{F} \simeq k^d$
↓
COMO k-E.V. ///

CURVAS ELÍPTICAS SOBRE $\mathbb{F}_{2^d}$

→ MEJOR DICHO, SOBRE CUERPOS DE CARACTERÍSTICA CUALQUIERA

DADO UN CUERPO F, DEFINIMOS UNA CURVA ELÍPTICA E SOBRE F COMO UNA EC. DE LA FORMA

$$E: \quad y^2 = x^3 + Ax + B,$$

→ "EC. EN FORMA DE WEIERSTRASS"

CON $A, B \in F$ Y $\Delta = -16(4A^3 + 27B^2) \neq 0$;

DADOS $P_1, P_2 \in E$ CON $P_1, P_2 \neq \mathcal{O}$ Y $P_1 \neq -P_2$

DEFINIMOS $P_1 + P_2 = (x_3, y_3)$, DONDE SI $P_i = (x_i, y_i)$,

SE TIENE $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, CON

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{SI } P_1 \neq P_2 \\ \dfrac{3x_1^2 + A}{2y_1}, & \text{SI } P_1 = P_2 \end{cases}$$

PROBLEMA: ESTO FUNCIONA BIEN SI $\operatorname{car}(F) \neq 2, 3$.

DEF: SEA F UN CUERPO. UNA CURVA ELÍPTICA E SOBRE F ES UNA ECUACIÓN DE LA FORMA

$$E: \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad \text{CON } a_i \in F,$$

DONDE SI PONEMOS

$b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$,

$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$,

SE TIENE QUE

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0.$$

NOT: $E(F) = \{(x,y) \in F \times F$ QUE RESUELVEN LA EC $\} \cup \{\mathcal{O}\}$.

OBS: SI $\mathrm{car}(F) \neq 2, 3$, COMPLETANDO $\square$ Y $\square^3$, Y CAMBIANDO VARIABLES, SE PUEDE LLEVAR LA ECUACIÓN A LA FORMA DE WEIERSTRASS.

DEF: SEAN $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E(F) \setminus \{\mathcal{O}\}$. DEFINIMOS $P_3 := (P_1, P_2)$ COMO EL PUNTO CON COORD $(\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3)$, DONDE

- SI $x_1 \neq x_2$, $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$, $\nu = \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$

- SI $x_1 = x_2$ Y $2y_1 + a_1x_1 + a_3 \neq 0$,

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

SI $x_1 = x_2$ Y $2y_1 + a_1x_1 + a_3 = 0$, DEFINIMOS $P_1 + P_2 := \mathcal{O}$.

FÓRMULAS: SI $P = (x, y) \in E(F)$,

- $-P = (x, -y - a_1x - a_3)$
- $x(2P) = \dfrac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$.

EJEMPLO: SEA $E/\mathbb{F}_2$ LA CURVA DADA POR

$E: y^2 + xy = x^3 + 1$ "CURVA DE KOBLITZ".

- $a_1 = 1, a_3 = 0, a_2 = 0, a_4 = 0, a_6 = 1.$
- $b_2 = 1, b_4 = 0, b_6 = 0, b_8 = 1$
- $\Delta = 1$

TENEMOS QUE

$E(\mathbb{F}_2) = \{\mathcal{O}, (0,1), (1,0), (1,1)\}$ ⇝ GRUPO ABELIANO, ORDEN 4.

- $-(0,1) = (0,1)$ ⇝ PUNTO DE ORDEN 2
- $-(1,0) = (1,1)$
- $-(1,1) = (1,0)$
- $(1,0) + (1,0) = (0,1)$
- $(1,1) + (1,1) = (0,1)$
- $(1,0) + (0,1) = (1,1) + (1,1) + (1,0) = (1,1) + \mathcal{O} = (1,1)$
- $(1,1) + (0,1) = (1,0) + (0,1) + (0,1) = (1,0) + \mathcal{O} = (1,0)$

+	$\mathcal{O}$	$(0,1)$	$(1,0)$	$(1,1)$
$\mathcal{O}$	$\mathcal{O}$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$\mathcal{O}$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$\mathcal{O}$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$\mathcal{O}$

OBS: $E(\mathbb{F}_2) \simeq \mathbb{Z}_4$!

OBS: $|p + 1 - \#E(\mathbb{F}_p)| \leq \sqrt{p}$ ← TEO. DE HASSE

OBS: COMO $\mathbb{F}_2 \subseteq \mathbb{F}_4$, PODEMOS PENSAR A E TAMBIÉN DEFINIDA SOBRE $\mathbb{F}_4$.

CAMBIEMOS NOTACIÓN EN $\bar{\mathbb{F}}_4$, $t \leftarrow x$.

- PUNTOS $P \in E(\bar{\mathbb{F}}_4)$ CON $x(P) = t$:

$$y^2 + t\cdot y = \underbrace{t^3}_{=t^3} + 1 = 0 \iff y^2 + ty = 0$$

$$\iff y(y+t) = 0$$

$\rightsquigarrow$ TENEMOS $(t,0)$ Y (t,t)

- PUNTOS $P \in E(\bar{\mathbb{F}}_4)$ CON $x(P) = t+1$:

$$y^2 + (t+1)y = 1+1 = 0 \iff y(y+(t+1)) = 0$$

$\rightsquigarrow$ TENEMOS $(t+1,0)$ Y $(t+1, t+1)$

$\rightsquigarrow$ ASÍ, $E(\bar{\mathbb{F}}_4) = \{\mathcal{O}, (0,1), (1,0), (1,1), (t,0), (t,t), (t+1,0), (t+1,t+1)\}$

↓ LOS QUE YA TENÍA

(OJO: ¿POR QUÉ NO HAY MÁS CON $x(P) = 0$ Ó $x(P) = 1$?)