EL MAPA DE FROBENIUS

OBJETIVO: SUMAR PUNTOS "RÁPIDAMENTE" EN CURVAS ELÍPTICAS SOBRE CUERPOS FINITOS.

VIMOS: DADO $m \in \mathbb{N}$, PODEMOS ESCRIBIR, SI $k = \lfloor \log_2 m \rfloor + 1$,

$$m = u_0 + u_1 \cdot 2 + \cdots + u_k 2^k,$$

CON $u_i \in \{-1, 0, 1\}$, $\#\{i : u_i \neq 0\} \leq k/2$

$\rightsquigarrow$ PODEMOS, DADO $P \in E(\mathbb{F}_q)$, CALCULAR mP

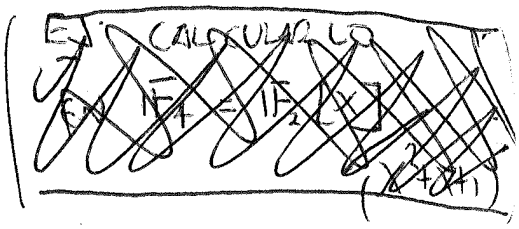
HACIENDO $\rightarrow$ $k+1$ DUPLICACIONES

$\searrow \leq k/2$ SUMAS

QUEREMOS MEJORAR ESTO.

DEF: p PRIMO, $k \geq 1$. EL MAPA DE FROBENIUS ES LA FUNCIÓN

$$\tau : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}, \quad \alpha \mapsto \alpha^p$$



PROP: 1) $\tau(xy) = \tau(x) \cdot \tau(y)$

2) $\tau(x+y) = \tau(x) + \tau(y)$

3) $\tau(x) = x \quad \forall x \in \mathbb{F}_p$ (RECORDAR: $\mathbb{F}_p \subseteq \mathbb{F}_{p^k}$)

Dem: 2) $p \mid \binom{p}{k}$ si $1 \leq k \leq p-1$. ☒

$\hookrightarrow$ Ej: si $p=2$, $(x+y)^2 = x^2 + \overbrace{2xy}^{=0} + y^2$

$= x^2 + y^2$.

SEA $E/\mathbb{F}_p$ UNA CURVA ELÍPTICA

PROP: SEA $P \in E(\mathbb{F}_{p^k})$, DIGAMOS $P = (x, y)$.
SEA $\tau(P) := (\tau(x), \tau(y))$. ENTONCES, $\tau(P) \in E(\mathbb{F}_{p^k})$.

DEM: SI $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$
CON LOS $a_i \in \mathbb{F}_p$, ENTONCES COMO $\tau|_{\mathbb{F}_p} = id$,
$\tau(y)^2 + a_1 \tau(x)\tau(y) + a_3 \tau(y) = \tau(x)^3 + a_2 \tau(x)^2 + a_4 \tau(x) + a_6$ ☒

PROP: SEAN $P, Q \in E(\mathbb{F}_{p^k})$. ENTONCES,
$\tau(P+Q) = \tau(P) + \tau(Q)$
"$\tau : E(\mathbb{F}_{p^k}) \to E(\mathbb{F}_{p^k})$ ES MORF. DE GRUPOS"

DEM: HAY QUE REVISAR LA FÓRMULA DE LA SUMA... ☒

TEO: DEFINAMOS

$$a := p + 1 - \#E(\mathbb{F}_p)$$

DE MANERA QUE $a = \alpha + \beta$

i) $|a| \leq 2\sqrt{p}$ (TEO. DE HASSE)

ii) SEAN $\alpha, \beta \in \mathbb{C}$ LAS RAÍCES DE $f(x) = x^2 - ax + p$.
ENTONCES $|\alpha| = |\beta| = \sqrt{p}$

iii) $\forall k \geq 1$, $\#E(\mathbb{F}_{p^k}) = p^k + 1 - \alpha^k - \beta^k$
"$\#E(\mathbb{F}_p)$ DETERMINA $\#E(\mathbb{F}_{p^k})$ $\forall k \geq 1$".

iv) EL MAPA DE FROB. $\tau : E(\mathbb{F}_{p^k}) \to E(\mathbb{F}_{p^k})$
SATISFACE QUE
$$\tau^2(P) - a\tau(P) + p \cdot P = 0 \quad \forall P \in E(\mathbb{F}_{p^k})$$
"$\tau^2 - a\tau + p = 0$, COMO FUNCIÓN EN $E(\mathbb{F}_{p^k})$".

EJEMPLO: SI $E/\mathbb{F}_2$ ES LA CURVA DE KOBLITZ

$$E: \quad y^2 + xy = x^3 + 1,$$

ENTONCES $a = -1$, Y POR LO TANTO τ SATISFACE

$$\tau^2 + \tau + 2 = 0.$$

PROP: SEA τ "ALGO" SATISFACIENDO $\tau^2 + \tau + 2 = 0$.
SEA $m \in \mathbb{N}$. ENTONCES, PODEMOS ESCRIBIR

$$m = v_0 + v_1 \tau + \cdots + v_\ell \tau^\ell,$$

CON $v_i \in \{-1, 0, 1\}$, $\ell \approx 2 \log m$, $\frac{\#\{i : v_i \neq 0\}}{\ell} \leq 1/3$.

EJEMPLO: SEA $m = 7$. ENTONCES,

$$7 = 1 + 3 \cdot 2 = 1 + 3(-\tau - \tau^2) = 1 - 3\tau - 3\tau^2$$
$$= 1 - \tau - \tau^2 - 2\tau - 2\tau^2 = 1 - \tau - \tau^2 - (-\tau - \tau^2)\tau$$
$$- (-\tau - \tau^2)\tau^2 = 1 - \tau + 2\tau^3 + \tau^4$$
$$= 1 - \tau + (-\tau - \tau^2)\tau^3 + \tau^4 = 1 - \tau - \tau^5.$$

EJERCICIO: IMPLEMENTAR ESTO.

APLICACIÓN: SI $E/\mathbb{F}_2$ ES LA CURVA DE KOBLITZ Y $P \in E(\mathbb{F}_{2^k})$, SI ESCRIBIMOS m COMO EN PROP, PODEMOS CALCULAR $m \cdot P$ COMO

$$m \cdot P = v_0 P + v_1 \tau(P) + \cdots + v_\ell \tau^\ell(P);$$

$\tau^k(P)$ SE CALCULA MUCHO MÁS RÁPIDO QUE $2^k \cdot P$.

EJEMPLOS (PARA IR MECHANDO):

1) $T : \mathbb{F}_4 \to \mathbb{F}_4$, CALCULAR SUS VALORES.
VERIFICAR QUE $T|_{\mathbb{F}_2} = id$, Y QUE RESPETA SUMAS Y PRODUCTOS.

2) CALCULAR $T : E(\mathbb{F}_4) \to E(\mathbb{F}_4)$, $E/\mathbb{F}_2$ C. DE WEIERSTRASS
EJ: VERIFICAR QUE ES MORFISMO.

3) VERIFICAR i, ii y iii DEL TEO PARA .

i. $a = 3 - 4 = -1$; $|a| = 1 \leq 2\sqrt{2}$

ii. SEA $f(x) = x^2 + x + 2$. SUS RAÍCES SON

$\alpha = \frac{-1 + \sqrt{7}\cdot i}{2}$, $\beta = \frac{-1 - \sqrt{7}\cdot i}{2}$ $(= \bar{\alpha})$;

$$|\alpha| = \frac{1}{2}\sqrt{1^2 + \sqrt{7}^2} = \frac{\sqrt{8}}{2} = \sqrt{2}$$

iii $\# E_1(\mathbb{F}_4) = 8 = 2^2 + 1 - \alpha^2 - \beta^2 = 2^2 + 1 + 3$:

- SABEMOS QUE $\alpha\cdot\beta = 2$, $\alpha + \beta = -1$

$$\Rightarrow 1 = (\alpha+\beta)^2 = \alpha^2 + \beta^2 + 2\alpha\beta = \alpha^2 + \beta^2 + 4$$

$$\Rightarrow \alpha^2 + \beta^2 = -3 \quad \checkmark$$