Curvas Elípticas / $\mathbb{F}_q$ y Funciones L (15/10/21)

Curvas Elípticas / $\mathbb{F}_q$

Trabajamos ahora primordialmente en característica prima p, y en particular sobre un cuerpo finito $\mathbb{F}_q$ de cardinalidad $q = p^n$.

En general, una curva elíptica está dada por

(coords afines) $E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$,

junto con un punto $\mathcal{O}$ en el infinito, y está definida / $\mathbb{F}_q$ precisamente cuando cada $a_i \in \mathbb{F}_q$.

$\Updownarrow$

(coords proyectivas) $E : Y^2Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3$,

$\mathcal{O} = [0, 1, 0]$, cada $a_i \in \mathbb{F}_q$.

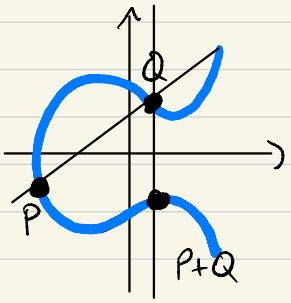
En característica $p \neq 2, 3$, tenemos que la forma de Weierstrass es de la forma

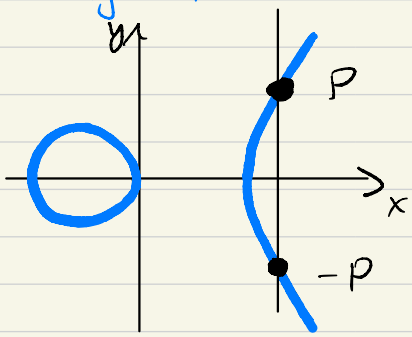
$$E : y^2 = x^3 - 27c_4 x - 54c_6$$

Tenemos también el discriminante y el j-invariante

$$\Delta = \frac{c_4^3 - c_6}{1728}, \quad j = \frac{c_4^3}{\Delta}$$

Ejemplos estándares son los siguientes





$y^2 = x^3 - 3x + 3$
$\Delta = -2160$

$y^2 = x^3 - x$
$\Delta = 64$

Suma en el grupo $E(\mathbb{F}_q)$

$p \neq 2, 3$

$y^2 = x^3 + Ax + B$

$P_i = (x_i, y_i) \in E(\mathbb{F}_q)$

$P_1, P_2 \neq \mathcal{O}$

$P_3 = P_1 + P_2$

Caso $x_1 \neq x_2$:

$x_3 = m^2 - x_1 - x_2$

$y_3 = m(x_1 - x_3) - y_1$

$m = \dfrac{y_2 - y_1}{x_2 - x_1}$

Caso $x_1 = x_2$, $y_1 \neq y_2$:

$P_1 + P_2 = \mathcal{O}$

Caso $P_1 = P_2$, $y_1 \neq 0$:

$$x_3 = m^2 - 2x_1$$
$$y_3 = m(x_1 - x_3) - y_1$$
$$m = \frac{3x_1^2 + A}{2y_1}$$

Caso $P_1 = P_2$, $y_1 = 0$:

$$P_1 + P_2 = \mathcal{O}$$

También: $P + \mathcal{O} = \mathcal{O}$, $\forall P$

Ejercicio 3.1: $p \neq 2, 3$

Tenemos un morfismo, de hecho endomorfismo

$$\alpha : E(\overline{\mathbb{F}_q}) \longrightarrow E(\overline{\mathbb{F}_q})$$

$\overline{\mathbb{F}_q}$ cerradura alg. de $\mathbb{F}_q$

multiplicación por $n \in \mathbb{Z}$

$$\alpha(P) = nP = \underbrace{P}_{n \text{ veces}} \quad (\text{sumar } P)$$

$$\alpha(x, y) = (R_1(x,y), R_2(x,y))$$

para:

(i) α mult. por 2.

(ii) α " " 3.

Ejercicio 3.2: Considerar la curva elíptica

$$y^2 = x^3 + 2$$

sobre el cuerpo finito $\mathbb{F}_7$.

Demostrar que

$$E(\mathbb{F}_7) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

- Encontrar $E(\mathbb{F}_7) = ?$ como conj.
- Demostrar que todo $P \in E(\mathbb{F}_7)$ satisface $3P = \mathcal{O}$
- De hecho $E(\mathbb{F}_7) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

De primordial importancia en característica p. es el endomorfismo de Frobenius

$$\varphi : E(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_q)$$

$$\varphi(x, y) = (x^q, y^q) \quad \left(\begin{array}{c}\text{en coords}\\ \text{afines}\end{array}\right)$$

Dado un endomorfismo (no trivial) sobre la cerradura alg. de $\mathbb{F}_q$

$$\alpha : E(\overline{\mathbb{F}_q}) \longrightarrow E(\overline{\mathbb{F}_q})$$

$$\alpha(x, y) = (R_1(x,y), R_2(x,y))$$

$$(\alpha(\mathcal{O}) = \mathcal{O}).$$

Hom $\Rightarrow \alpha(x,-y) = \alpha(-(x,y))$

$= -\alpha(x,y)$

$\Rightarrow R_1(x,-y) = R_1(x,y)$

$R_2(x,-y) = -R_2(x,y)$

Luego usando la forma de Weierstrass

$y^2 = x^3 + Ax + B$

nos permite escribir

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y} \cdot \frac{(p_3(x) - p_4(x))}{(p_3(x) - p_4(x)y)}$$

$$= \frac{q_1(x) + q_2(x)y}{q_3(x)}$$

(*) $\therefore \alpha(x,y) = (r_1(x), r_2(x)y)$

Def 3.3: Sea $\alpha : E(\overline{\mathbb{F}_q}) \longrightarrow E(\overline{\mathbb{F}_q})$

α como (*)

donde escribimos $r_1(x) = \frac{p(x)}{q(x)}$.

(i) α es **separable** si

$r'(x) \neq 0 \iff p'(x)$ ó $q'(x) \neq 0$

$\uparrow$ pdi. 0 (derivadas)

(ii) gdo $(\alpha) = \max(\text{gdo } p(x), \text{gdo } q(x))$.

Prop 3.4: El Frobenius $\varphi : E(\overline{\mathbb{F}_q}) \longrightarrow E(\overline{\mathbb{F}_q})$ es de gdo $\varphi = q$ y no es separable.

dem:

Suponemos $E: y^2 = x^3 + Ax + B$

$(x_i, y_i) \in E(\overline{\mathbb{F}_q})$ $i = 1, 2$ t.q.

$x_1 \neq x_2$.

Conocemos la suma explícita para (x_3, y_3)

$x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_3) - y_1$

φ } tomando el Frob.

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

$x_3^q = m'^2 - x_1^q - x_2^q$, $y_3^q = m'(x_1^q - x_1^q) - y_1^q$

$$m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}.$$

$\Rightarrow \varphi(x_3, y_3) = \varphi(x_1, y_1) + \varphi(x_2, y_2)$.

Notar que faltan otros casos, que se establecen directamente. ↳ **Obs:** cuando hay 2, 3 en la fórmula usamos

$p \neq 2, 3$

$\Rightarrow 2^q = 2$, $3^q = 3$ en $\mathbb{F}_q$.

Nos está dando un endomorfismo, su derivada en car p. es 0. $\Rightarrow \varphi$ no es separable.

Trabajando con

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

y con la forma de $\alpha(x,y) = (r_1(x), r_2(x)y)$

Obtenemos el siguiente

Teorema 3.5:

(i) El Frobenius

$$\varphi : E(\overline{\mathbb{F}}_q) \longrightarrow E(\overline{\mathbb{F}}_q)$$

es de grado q y no es separable.

(ii) Si tenemos un endomorfismo

$$\alpha : E(\overline{\mathbb{F}}_q) \longrightarrow E(\overline{\mathbb{F}}_q)$$

es separable, entonce

$$\text{gdo } \alpha = \#\ker(\alpha).$$

(iii) El endomorfismo mult. por $n \in \mathbb{Z}$

$$(x,y) \longmapsto n(x,y)$$ (sumar el punto n veces)

es separable $\iff p \nmid n$.

(iv) Dados $m, n \in \mathbb{Z}$, no ambos 0,

$m\varphi + n$ es separable $\iff p \nmid n$

(v) Para endomorfismos α, β:

$$\text{gdo}(m\alpha + n\beta) = m^2 \text{gdo}\,\alpha + n^2 \text{gdo}\,\beta + mn\{\text{gdo}(\alpha+\beta) - \text{gdo}(\alpha) - \text{gdo}(\beta)\}.$$

Proposición 3.6: E una curva elíptica $/\mathbb{F}_q$, y sea $n \geq 1$. Luego

(i) $\ker(\varphi^n - 1) = \#E(\mathbb{F}_{q^n})$.

(ii) $\varphi^n - 1$ es separable y se tiene

$$\#E(\mathbb{F}_{q^n}) = \text{gdo}(\varphi^n - 1).$$

Dem: Para (i), aplicamos el Frob. a Weierstrass

$$y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{F}_{q^n}$$

φ^n (φ^n actúa dentro de $\mathbb{F}_{q^n}$).

$$(y^{q^n}) = (x^{q^n})^3 + A x^{q^n} + B$$

$\Rightarrow (x^{q^n}, y^{q^n}) \in E(\mathbb{F}_{q^n})$ si $(x,y) \in E(\mathbb{F}_{q^n})$.

El Teorema 3.5 parte (iv)

$\Rightarrow \varphi^n - 1$ separable.

La def. del kernel y la parte (ii) del mismo Teo. dan

$$\text{gdo}(\varphi^n - 1) = \#\ker(\alpha).$$

Arribamos a un teorema importante

Teorema 7 (Hasse): Para $E/\mathbb{F}_q$, se tiene

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

dem: Esto se debe a que

$$a = \#E(\mathbb{F}_q) - q - 1 = \deg(\varphi - 1) - q - 1$$

Afirmación: Dados $m, n \in \mathbb{Z}$ t.q. $(m,n) = 1$

$$\Rightarrow \deg(m\varphi - n) = m^2 q + n^2 - mnq.$$

En verdad: Tenemos del Teo. 3.5 (v):

$$\deg(m\varphi - 1) = m^2 \deg(\varphi) + n^2 \deg(-1) + mn\left[\deg(\varphi - 1) - \deg(\varphi) - \deg(-1)\right]$$

y conocemos que

$$\deg(\varphi) = q, \quad \deg(-1) = 1.$$

$\Rightarrow$ Afirmación.

Continuamos, observando que

$$\deg(m\varphi - n) \geq 0$$

$$\Rightarrow q\left(\frac{m}{n}\right)^2 - a\left(\frac{m}{n}\right) + 1 \geq 0$$

$\forall m, n \in \mathbb{Z}$, $(m,n) = 1$

Este conj. de racionales es denso en $\mathbb{R}$.

$$\Rightarrow \underbrace{qx^2 - ax + 1}_{\text{cuadrática}} \geq 0 \quad \forall x \in \mathbb{R}$$

$\Rightarrow$ Discriminante ≤ 0 ó es 0.

$$\Rightarrow a^2 - 4q \leq 0 \Rightarrow |a| \leq 2\sqrt{q} \quad //.$$

Funciones L

La función Z de una curva elíptica $E/\mathbb{F}_q$ se define por medio de la exponencial de una serie de potencias

$$f(t) \in \mathbb{Q}[[t]] \quad \text{t.q.} \quad \sum_{n=1}^{\infty} c_n t^n \quad \rightsquigarrow \quad \exp(f(t)) = \sum_{k=0}^{\infty} \frac{f(t)^k}{k!}$$

Def 3.8: C una curva proyectiva definida sobre $\mathbb{F}_q$

$$Z(C,t) = \exp\left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} t^n \right).$$

Ejemplo 3.9: Sea $C = \mathbb{P}^1$, luego

$$\#\mathbb{P}^1(\mathbb{F}_{q^n}) = q^n + 1.$$

Entonces

$$Z(\mathbb{P}^1, t) = \exp\left(\sum_{n=1}^{\infty} \frac{q^n+1}{n} t^n \right)$$

$$= \exp\left(\underbrace{\sum_{n=1}^{\infty} \frac{q^n}{n} t^n}_{-\log(1-qt)} + \underbrace{\sum_{n=1}^{\infty} \frac{t^n}{n}}_{-\log(1-t)} \right)$$

$(\text{Si } |t| < q^{-1}) \rightsquigarrow$

$$\therefore \quad Z(\mathbb{P}^1, t) = \frac{1}{(1-t)(1-qt)}.$$

Obs: Debido a que estas funciones tienen interés analítico, podemos pasar a la función L corresp. en la var. $s \in \mathbb{C}$,

$$t = q^{-s}$$

$$L(s) = L(\mathbb{P}^1/\mathbb{F}_q, s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}$$

Luego, se tiene una ecuación funcional

$$\boxed{L(s) = \varepsilon(s) L(1-s)}$$

$$\varepsilon(s) = q^{1-2s} \quad \text{(cuando en } q^{-s}\text{)}$$

Teorema 3.10 (Hasse): E una curva elíptica / $\mathbb{F}_q$. Se cumple lo siguiente:

(i) **Racionalidad:**

$$Z(E,t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)}$$

donde

$$(1-\alpha t)(1-\beta t) = 1 - at + qt^2, \quad a \in \mathbb{Z}$$

$$|a| = |\beta| = \sqrt{q}.$$

(ii) **Ecuación funcional:**

$$Z(E,t) = Z\left(E, \frac{1}{qt}\right).$$

Indicamos:

$$\#E(\mathbb{F}_{q^n}) = |\ker(1-\varphi^n)|$$

$$= \deg(1-\varphi)$$

$\operatorname{End}(E(\mathbb{F}_p), E(\mathbb{F}_p))$ $\longleftrightarrow$ l-adificación

(Tate, Faltings) $\downarrow$

$\operatorname{End}(E(\mathbb{Q}_l), E(\mathbb{Q}_l))$ $= \det(1-\varphi_l^n)$

$$= 1-\alpha^n-\beta^n+q^n, \quad \alpha,\beta\in\mathbb{C}$$

$$|\alpha| = |\beta| = \sqrt{q}.$$

Regresando a calcular después de esa maquinaria

$$Z(E,t) = \exp\left(\sum_{n=1}^{\infty} \frac{1-\alpha^n-\beta^n+q^n}{n} t^n\right)$$

$$= \exp(\log \ldots + - \cdots)$$

$$= \frac{1-(\alpha+\beta)t+\alpha\beta t}{(1-t)(1-qt)}$$

$\rightsquigarrow$ $a = \alpha+\beta = \operatorname{Tr}(\varphi_l) = 1+q-\deg(1-\varphi) \in \mathbb{Z}$

$$\alpha\beta = \det(\varphi_l) = \deg(\varphi) = q.$$

Como anteriormente pasamos a la función L

$$L(E/\mathbb{F}_q, s) = \frac{1 - aq^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}, \quad s \in \mathbb{C}$$

Aquí, se obtiene

$$\boxed{L(E/\mathbb{F}_q, s) = L(E/\mathbb{F}_q, 1-s)}$$

$(\varepsilon(s) = 1)$.

Funciones L en diversos contextos

$E/\mathbb{Q}$

Def 3.11: Para una curva elíptica $/\mathbb{Q}$ con disc. Δ, su función L de Hasse-Weil se define:

$$L(E/\mathbb{Q}, s) = \underbrace{\prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}}_{\text{(infinito)}} \underbrace{\prod_{p \mid \Delta} \frac{1}{1 - a_p p^{-s}}}_{\text{(finito)}}.$$

Ejercicio 3.12: Demostrar que el prod. infinito converge para el semiplano $\mathrm{Re}(s) > \frac{3}{2}$.

Formas Modulares

Semiplano superior complejo

$$\mathcal{h} = \{ z \in \mathbb{C} \mid \mathrm{Im}(z) > 0 \}$$

Una forma modular de peso k

$$f : \mathcal{h} \longrightarrow \mathbb{C}$$

que satisface

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right),$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

... Tenemos al semiplano superior complejo

$$\mathcal{H} = \{ z \in \mathbb{C} \mid \mathrm{Im}(z) > 0 \}$$

(espacio hiperbólico).

Ejercicio 3.13: Chequear lo siguiente

$$z \in \mathcal{H}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \Rightarrow \frac{az+b}{cz+d} \in \mathcal{H}$$

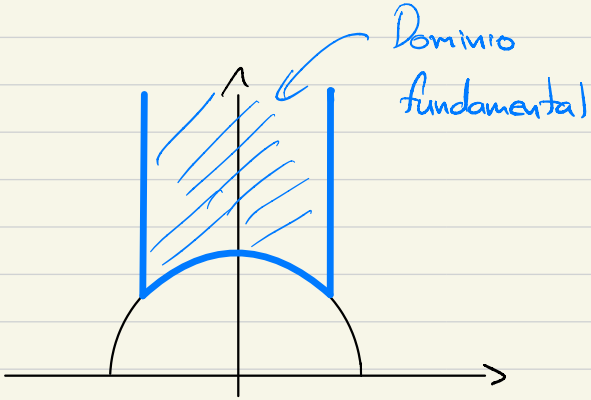
f es analítica y tiene simetría bajo

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Expansión de Fourier

$$f(q) = \sum a_n q^n,$$

$$q = e^{2\pi i z}$$



Lo anterior se generaliza a otros subgrupos de $SL_2(\mathbb{Z})$ como los subgrupos de congruencia

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod N \right\}$$

donde se tienen

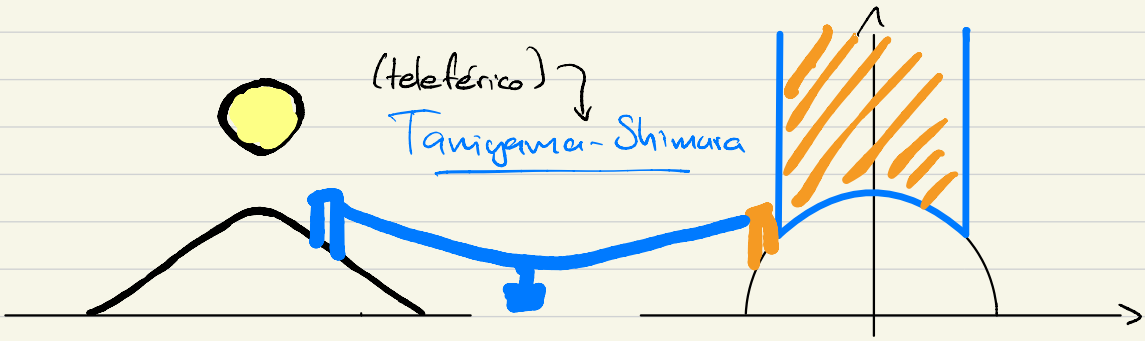
$$f : \Gamma_0(N) \backslash \mathfrak{h} \to \mathbb{C}.$$

Existe su función L:

$$L(f, s)$$

Ec. Funcional:

$$L(f, s) = (-1)^k L(f, 1-s)$$



$E/\mathbb{Q} \longleftrightarrow f_E$ forma modular

Teorema de Wiles, refinado y generalizado a modularidad por Breuil, Conrad, Diamond, Taylor.

Toda Curva Elíptica es Modular

$$L(E,s) = L(f,s)$$

Bibliografía:

- Milne, Elliptic Curves.
- Silverman, The Arithmetic of Elliptic Curves.
- Washington, Elliptic Curves: Number Theory and Criptography.

$E/\mathbb{F}_q$