Reducción de funciones L de curvas elípticas módulo enteros

ArXiv: 2110.12156

Félix Baril Boudreau (University of Western Ontario)
fbarilbo@uwo.ca

Seminario Latinoamericano de Teoría de Números

15 de junio del 2022

Natural Sciences and Engineering Research Council of Canada
Conseil de recherches en sciences naturelles et en génie du Canada
Canada

Contexto

- $q := p^r$: potencia de un primo $p \geq 5$
- $C/\mathbb{F}_q$: curva suave, propia y geométricamente conexa de género g
- $K := \mathbb{F}_q(C)$: campo de funciones de $C/\mathbb{F}_q$
- $v \in |C|$: punto cerrado de C
- k_v : campo residual de v
- $d_v := [k_v : \mathbb{F}_q]$: grado de v
- E/K : curva elíptica cuyo invariante j no es constante

Motivación : funciones zeta

Tres puntos de vista de la función zeta $\mathrm{Z}(T, C/\mathbb{F}_q)$:

- Función generadora:
  $\mathrm{Z}(T, C/\mathbb{F}_q) := \exp\left(\sum_{m=1}^{\infty} \# C(\mathbb{F}_{q^m}) \frac{T^m}{m}\right)$
- Producto de Euler: $\mathrm{Z}(T, C/\mathbb{F}_q) = \prod_{v \in |C|} (1 - T^{d_v})^{-1}$
- Función racional: $\mathrm{Z}(T, C/\mathbb{F}_q) = \frac{P_1(T)}{(1-T)(1-qT)}$ (Schmidt, 1931)
- $P_1(T) = \sum_{i=0}^{2g} a_i T^i \in \mathbb{Z}[T]$

Motivación : calcular funciones zeta

Función generadora:

- Calcular $\#C(\mathbb{F}_{q^m})$ para suficientes m
  - Conteo de puntos genuino
  - Métodos p-ádicos : Kedlaya (empezando en 2001 [2]) y otros

Función racional:

- $P_1(T) = \sum_{i=0}^{2g} a_i T^i \in \mathbb{Z}[T]$, $|a_i| \leq c_i$
- Calcular $P_1(T)$ mod ℓ para suficientes ℓ
- Encontrar $P_1(T)$ con el teorema chino de residuos
  - Si C es una curva elíptica : algoritmo de Schoof (1985) [6]
  - $P_1(T) = 1 - a_1 T + qT^2$, $|a_1| \leq 2q^{1/2}$ (Hasse), $a_1 = 1 + q - \#E(\mathbb{F}_q)$
  - Para C general : algoritmo de Pila (1989-90) [5] y mejoras de Adleman y Huang (2001) [1]
  - $P_1(T) \equiv \det(1 - T\mathrm{Frob}_q|\mathrm{Jac}(C)(\overline{\mathbb{F}_q})_\ell)$ mod ℓ

Personaje principal 1 : Curva elíptica

Curva elíptica $(E/K, O)$

- Curva suave, proyectiva de genero 1 definida sobre K
- Punto racional $O = [0:1:0] \in E(K)$ en $\mathbb{P}^2$
- Modelo afín $y^2 = x^3 + Ax + B$, $A, B \in K$
- $\Delta(E) = -16(4A^3 + 27B^2) \neq 0$ (suave)
- $j(E) = -1728(4A)^3/\Delta(E) \in K - \mathbb{F}_q$ (no constante)
- $E(K)$: grupo abeliano, finitamente generado (por el teorema de Mordell)

Ejemplo: Reducción $E/\mathbb{F}_q(t) : y^2 + (1-t)xy - ty = x^3 - tx^2$

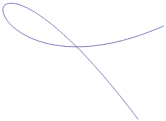
Toma $q := 61$. Entonces, $\Delta = t^5(t-32)(t-40)$.

Buena: $v \in U$

Curva elíptica
$E_{t-1}/\mathbb{F}_{61}$:
$y^2 - y = x^3 - x^2$

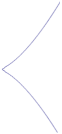
Multiplicativa:
$v \in \{M^{\mathrm{sp}}, M^{\mathrm{ns}}\}$

Nodo
$E_t/\mathbb{F}_{61}$:
$y^2 + xy = x^3$



Aditiva: $v \in A$

Cúspide
$E_v'/\mathbb{F}_{61}$: $y^2 = x^3$



Personaje principal 2 : Función L (producto de Euler)

- Producto de Euler:

$$a_v := \begin{cases} 1 + q^{d_v} - \#E_v(k_v) & \text{si } E_v/k_v \text{ curva elíptica (buena)} \\ 1 & \text{si } E_v/k_v \text{ nodo, tangentes en } k_v \\ -1 & \text{si } E_v/k_v \text{ nodo, tangentes no en } k_v \\ 0 & \text{si } E_v/k_v \text{ cúspide} \end{cases}$$

- $$L(T, E/K) = \prod_{v \text{ buena}} (1 - a_v T^{d_v} + q^{d_v} T^{2d_v})^{-1} \times \prod_{v \text{ mala}} (1 - a_v T^{d_v})^{-1}$$

Personaje principal 2 : Función L (función racional)

- $L(T, E/K) = \frac{P_1(T)}{P_0(T)P_2(T)} \in \mathbb{Q}(T)$ (Grothendieck 1964/1965), a priori...

- $j(E) \in K - \mathbb{F}_q \Rightarrow L(T, E/K) \in 1 + T \cdot \mathbb{Z}[T]$, (Deligne, Weil II, 1981)

- $L(T, E/K) = \sum_{i=0}^{d} a_i T^i$, entonces $|a_i| \leq \binom{d}{i} q^i$

- ¿Podemos imitar a Schoof? $L(T, E/K) \bmod \ell$

- En parte, sí (¡Por el momento!).

- Tema principal: Puntos de torsión de E.

Torsión - Caso I: Abajo

Teorema (Hall, 2003)

Si $\mathcal{T} < E(K)$ *es un subgrupo de orden* N *con* $(N, q) = 1$, *entonces*

$$\mathrm{L}(T, E/K) \equiv \cdots \mod N.$$

Prueba

- *Si* v *es buena, sigue* $a_v = 1 + q^{d_v} - \#E(k_v) \equiv 1 + q^{d_v} \mod N$.
- *Luego,* $1 - a_v T^{d_v} + q^{d_v} T^{2d_v} \equiv (1 - T^{d_v})(1 - q^{d_v} T^{d_v}) \mod N$.
- $\mathrm{Z}(q^i T, C) = \prod_{v \in |C|} (1 - q^{id_v} T^{d_v})^{-1}, i \in \{0, 1\}$
- $\frac{\mathrm{L}(T, E/K)}{\mathrm{Z}(T, C)\mathrm{Z}(qT, C)} \equiv \prod_{M^{sp}} \frac{(1 - T^{d_v})(1 - q^{d_v} T^{d_v})}{(1 - T^{d_v})}$
  $\times \prod_{M^{ns}} \frac{(1 - T^{d_v})(1 - q^{d_v} T^{d_v})}{(1 + T^{d_v})} \times \prod_{A} \frac{(1 - T^{d_v})(1 - q^{d_v} T^{d_v})}{1} \mod N$

Torsión - Caso I: Abajo (Continuado)

Teorema (Hall, 2003)

Si $\mathcal{T} < E(K)$ *tiene orden* N *con* $(N, q) = 1$, *entonces*

$$\mathrm{L}(T, E/K) \equiv \mathrm{Z}(T, C)\mathrm{Z}(qT, C) \times \prod_{M^{sp}} (1 - q^{d_v} T^{d_v})$$

$$\times \prod_{M^{ns}} \frac{(1 - T^{d_v})(1 - q^{d_v} T^{d_v})}{(1 + T^{d_v})}$$

$$\times \prod_{A} (1 - T^{d_v})(1 - q^{d_v} T^{d_v}) \bmod N$$

Remark

- $\mathrm{Z}(T, C) \bmod N$ *calculable : e.j. algoritmo de Pila*
- *Los otros factores : algoritmo de Tate*

Torsión - Caso II: torcidos cuadráticos (contexto)

- $f \in K^{\times}$ generando una extensión cuadrática K_f/K, de grupo de Galois G_f
- $E_f : y^2 = x^3 + fAx + f^2B$: torcido cuadrático de E por f

$$
\begin{array}{ccccc}
K_f & & E/K_f & \xrightarrow{\simeq} & E_f/K_f \\
\Big| {\scriptstyle G_f} & & & & \\
K & & E/K & & E_f/K
\end{array}
$$

- Si $E(K)[N] \neq \{O\}$, entonces posiblemente $E_f(K)[N] = \{O\}$.

Torsión - Caso II: torcidos cuadráticos (Teorema A)

- Sea χ el carácter cuadrático de G_f.
- Función L de Artin L: $L(T,\chi) :=$
$$\prod_{v \text{ se descompone en } K_f} (1 - T^{d_v})^{-1} \times \prod_{v \text{ es inerte en } K_f} (1 + T^{d_v})^{-1}$$

Teorema (Baril Boudreau, 2021)

Sea $N \geq 5$ con $(N,q) = 1$. Si $E(K)[N] \neq \{O\}$ y $f \in K^\times$ genera K_f/K, entonces

$$\mathrm{L}(T, E_f/K) \equiv \mathrm{L}(T,\chi)\mathrm{L}(qT,\chi) \times \prod_{v \in M_{unr}^{sp}} \alpha_v(inerte, descompone)(T)$$
$$\times \prod_{v \in M_{unr}^{ns}} \beta_v(inerte, descompone)(T) \bmod N,$$

dónde $\alpha_v, \beta_v \in \mathbb{Q}(T)$ depende del comportamiento de v en K_f.

También tomamos en cuenta los casos $N \in \{2,3,4\}$.

Esboce de prueba - Teorema A

- $\mathrm{L}(T, E/K_f) = \mathrm{L}(T, E/K)\mathrm{L}(T, E_f/K)$
- Como $E(K)[N] \neq \{O\}$, entonces $E(K_f)[N] \neq \{O\}$
- Usa el teorema de Hall para E/K y E/K_f.
- $\mathrm{Z}(T, C_f) = \mathrm{Z}(T, C)\mathrm{L}(T, \chi)$ ■

Torsión - Caso II: torcidos cuadráticos (Teorema B)

Teorema (Baril Boudreau, 2021)

Sea $f_1, f_2 \in K^\times$. Como $\mathrm{L}(T, E_{f_i}/K) \in 1 + T \cdot \mathbb{Z}[T]$, entonces $\mathrm{L}(T, E_{f_1}/K)/\mathrm{L}(T, E_{f_2}/K) \in 1 + T \cdot \mathbb{Z}[[T]]$.
Sea

$$U_{f_1,f_2} := (U_{f_1} \cap U_{f_2}) \bigcup (M_{f_1} \cap M_{f_2}) \bigcup (A_{f_1} \cap A_{f_2}) .$$

Entonces,

$$\frac{L(T, E_{f_1}/K)}{L(T, E_{f_2}/K)} \equiv \prod_{v \notin U_{f_1,f_2}} \frac{L(T^{d_v}, E_{f_2}/k_v)}{L(T^{d_v}, E_{f_1}/k_v)} \bmod 2.$$

$K = \mathbb{F}_q(t)$, E/K semiestable, multiplicative en ∞, con $f, \Delta(E) \in \mathbb{F}_q[t]$ coprimos, f libre de cuadrados y par:
$\mathrm{L}(T, E_f/K) \equiv \prod_{v \text{mala}} (1 + \#E(k_v) T^{d_v} + T^{2d_v}) \mathrm{L}(T, E/K) \bmod 2$

Torsión - Caso III: Arriba (Contexto)

- $\ell \neq p$ primo
- $\mu_\ell \subset \mathbb{F}_q$
- $E(K)[\ell] = \{O\}$

$$\begin{array}{ccc} K_\ell = K(E[\ell]) & \qquad & E/K_\ell \\ \Big| {\scriptstyle G_\ell} & & \\ K & & E/K \end{array}$$

- Como $\mu_\ell \subset \mathbb{F}_q$, entonces $q \equiv 1 \bmod \ell$
- $G_\ell < \mathrm{SL}_2(\mathbb{F}_\ell)$

Torsión - Caso III: Arriba (Teorema C)

Z : conjunto de puntos de mala reducción para E/K
C_ℓ: la curva que corresponde al campo K_ℓ

Teorema (Baril Boudreau, 2022)

Si $\ell \geq 5$ y si G_ℓ tiene un subgrupo normal H_ℓ tal que $(\#H_\ell, \ell) = 1$ y $(\#G_\ell/H_\ell, \#E[\ell]^{H_\ell}) = 1$. Entonces,

$$\mathrm{L}(T, E/K) \equiv \det\left(1 - T\mathrm{Frob}_q | A_\ell\right) / \det\left(1 - T\mathrm{Frob}_q | B_\ell\right) \times \prod_{\substack{v \in Z \\ I_{\ell n}, n \geq 1}} (1 - T^{d_v}) \times \prod_{\substack{v \in Z \\ I_{\ell n, 2}, n \geq 1}} (1 + T^{d_v}) \bmod \ell.$$

dónde $A_\ell := (\mathrm{Jac}(C_\ell)(k)_\ell^{G_\ell})^{\oplus 2}$ y B_ℓ un cierto Frob_q-módulo

También tomamos en cuenta los casos $\ell \in \{2, 3\}$.

Torsión - Caso III: Arriba (Acerca de las hipótesis)

- Válido para todos los subgrupos de $\mathrm{SL}_2(\mathbb{F}_\ell)$ que tienen orden coprimo con ℓ
- Válido para todos los subgrupos de $\mathrm{SL}_2(\mathbb{F}_\ell)$ que tienen orden divisible por ℓ y que contienen el centro.
- E.j., Válido para $\mathrm{SL}_2(\mathbb{F}_\ell)$: $H_\ell = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ y $E[\ell]^{H_\ell} = \{O\}$
- No es válido para los subgrupos de $\mathrm{SL}_2(\mathbb{F}_\ell)$ que tienen orden divisible por ℓ **pero que no contienen el centro**, e.j.: $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$

Torsión - Caso III: Arriba (Un corolario)

Corolario (Baril Boudreau, 2022)

Si el orden de G_ℓ no es divisible por ℓ, entonces

$$\mathrm{L}(T, E/K) \equiv (1-T)^4 \mathrm{Z}(T, C)^2 \times \prod_{\substack{v \in Z \\ I_{\ell n}, n \geq 1}} (1 - T^{d_v}) \times \prod_{\substack{v \in Z \\ I_{\ell n, 2}, n \geq 1}} (1 + T^{d_v}) \bmod \ell.$$

Esboce de Prueba (Teorema C) : Modelo minimal y modelo de Néron

- Si $v \in C$, existe una superficie $\pi_v : \mathcal{X}_v \to \mathrm{Spec}(\mathcal{O}_{C,v})$ con π_v propio, regular, fibra genérica E/K_v + prop. univ.
- $\mathcal{E}_v$ modelo de Néron de E/K_v: subsesquema abierto de $\mathcal{X}_v$ de los puntos suaves de π_v

$$\begin{tikzcd} E \arrow[rr] \arrow[d] & & \mathcal{X}_v \arrow[d, "\pi_v"] & \mathcal{E}_v \arrow[l, hook'] \\ \mathrm{Spec}(\mathrm{K_v}) = \mathrm{Spec}(k_\eta) \arrow[rr] & & \mathrm{Spec}(\mathcal{O}_{C,v}) & \end{tikzcd}$$

- $\mathcal{E}_v$ es suave y separado + prop. univ. que hace le único (hacía isomorfismo) y tiene una estructura de grupo en esquemas que extiende la de E/K_v.
- Los $\mathcal{E}_v$ se pegan y dan un modelo de Néron global $\mathcal{E} \to C$.

Esboce de Prueba (Teorema C) : Secuencia exacta corta

- Si $v \in C$, existe un esquema en grupos finito Φ_v que es étale sobre k_v, junto con un morfismo sobreyectiva $f_v : \mathcal{E}_v \to \Phi_v$ con una propriedad universal. Φ_v es el *grupo de componentes* de $\mathcal{E}_v$.
- Sea $\mathcal{E}_v^0$, la fibra $\mathcal{E}_{v,f_v(e)}$, dónde e es la identidad de $\mathcal{E}_v$. Es conexa y un esquema en subgrupos 3algebraico de $\mathcal{E}_v$. $\mathcal{E}_v^0$ es el *componente identidad* de $\mathcal{E}_v$.
- La secuencia exacta se globaliza.

$$0 \to \mathcal{E}^0 \to \mathcal{E} \to \Phi \to 0$$

- Para $\ell \neq p$, también tenemos la secuencia exacta

$$0 \to \mathcal{E}_\ell^0 \to \mathcal{E}_\ell \to \Phi_\ell \to 0.$$

Esboce de Prueba (Teorema C) : Cohomología y función L módulo ℓ

- Como $q \equiv 1 \bmod \ell$ y $E(K)[\ell] = \{O\}$,

$$L(T, E/K) \equiv \det(1 - T\mathrm{Frob}_q | \mathrm{H}^1(\overline{C}_{\text{ét}}, \mathcal{E}_\ell^0)) \bmod \ell.$$

- $0 \to \Phi_\ell(\overline{Z}) \to \mathrm{H}^1(\overline{C}_{\text{ét}}, \mathcal{E}_\ell^0) \to \mathrm{H}^1(\overline{C}_{\text{ét}}, \mathcal{E}_\ell) \to 0$ de $\mathbb{F}_\ell$-espacios vectoriales de dimensión finita.
- Entender polinomio característico de Frob_q sobre $\Phi_\ell(\overline{Z})$ y $\mathrm{H}^1(\overline{C}_{\text{ét}}, \mathcal{E}_\ell)$

Esboce de Prueba (Teorema C) : Descenso

- $f : \overline{C_\ell} \to \overline{C}$ morfismo finito, dónde C_ℓ corresponde a $K_\ell := K(E[\ell])$.
- $f^*(\mathcal{E}_\ell) \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$
- $\mathrm{H}^1(\overline{C}_{\text{ét}}, f^*(\mathcal{E}_\ell) \simeq \mathrm{Jac}(C_\ell)(k)_\ell^{\oplus 2}$
- Bajo las hipótesis: existe $H_\ell \trianglelefteq G_\ell$ tal que $(\#H_\ell, \ell) = 1$ y $(\#G_\ell/H_\ell, E[\ell]^{H_\ell}) = 1$, tenemos

$$0 \to \mathrm{H}^1(\overline{C}_{\text{ét}}, \mathcal{E}_\ell) \to (\mathrm{Jac}(C_\ell)(k)_\ell^{G_\ell})^{\oplus 2} \to B_\ell \to 0.$$

■

ADLEMAN, Leonard M. and Ming-Deh HUANG, *Counting points on curves and abelian varieties over finite fields*. J. Symbolic Comput.,Vol. 32, Num. 3, 2001, 171-189.

KEDLAYA, Kiran S. *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*. J. Ramanujan Math. Soc. 16 (2001), no. 4, p. 323–338, Erratum : J. Ramanujan Math. Soc. 18 (2003), no. 4, 417–418.

DELIGNE, Pierre, *La conjecture de Weil II*. Pub. Math. I.H.E.S. 52, 313-428, 1981.

HALL, Chris. *L-functions of twisted Legendre curves*. Journal of Number Theory 119 (1), 128-147, 2006.

PILA, Jonathan. *Frobenius maps of abelian varieties and finding roots of unity in finite fields*. Math. Comp. 55 (1990), no. 192, 745–763.

SCHOOF, René. *Elliptic Curves over Finite Fields and the Computation of Square Roots mod p*. Math. Comp., 44 (170),