Introduction

Let $E$ be an elliptic curve over the function field $K = \mathbb{F}_q(t)$. The arithmetic of $E$ is (or should be) encoded in three objects:

• $E(K)$, its Mordell-Weil group; a finitely generated group equipped with the canonical Néron-Tate height pairing $(\cdot, \cdot)_{NT}$.

• $\Sha(E/K)$, its Shafarevich-Tate group; conjecturally a finite group.

• $L(E/K, s)$, its $L$-function and the special value at $s = 1$, which appears in the Birch & Swinnerton-Dyer conjecture:

$$L'(E/K, 1) := \lim_{s \to 1} \frac{d}{ds} L(E/K, s).$$

Recall that the Néron-Tate regulator is defined as

$$\text{Reg}(E/K) = \det (P_1 \ldots P_n)_{P \in E(K)}^{(P_1 \ldots P_n)_{P \in E(K)}},$$

where $P_1, \ldots, P_n$ denotes a basis of the free part of $E(K)$. Consider the family of quadratic twists of constant $E$, $E_{D} : y^2 = x^3 - D$.

Theorem (G.) Consider the family of quadratic twists of constant elliptic curves over $K$ by $D = t^d + 1$ with $d \in \mathbb{N}$ prime to $q$:

$$E := \{ E_q \mid E/\mathbb{Q}(t) \text{ constant elliptic curve } \},$$

Then $\Sha(E/K)$ is finite for all $E_q \in E$ and

$$0 \leq \Sha(E_q/K) \leq 1 + o(1) \quad (d \to \infty).$$

Moreover, in the “supersingular case”, i.e. when $d$ runs through the (finite) set $D_q := \{ d \in \mathbb{N} \mid \exists \alpha \in \mathbb{N} \text{ such that } d \text{ divides } \alpha^q + 1 \}$, one has

$$\Sha(E_q/K) \to 1 \quad d \to \infty.$$

Comments & future works

This work is in progress.

• Can we also compute lim $\Sha(E_q/K)$ when $d$ is not necessarily in the “supersingular set” $D_q$? Is it still true that $\Sha(E_q/K) \to 1$?

• One can also twist the constant curve $E$ by an squarefree polynomial $D(t) \in \mathbb{F}_q[t]$ instead of $D(t) = t^d + 1$. In which case, we can easily prove that

$$o(1) \leq \Sha(E_q/K) \leq 1 + o(1) \quad (\deg D \to \infty).$$

• For which families of such $D$ can we explicitly compute $\Sha(E_q/K)$?

• Equivalently, can we compute the zeroes of the zeta-function of $C_D$, $y^2 = D(X)$?

• For which families of non-constant elliptic curves over $\mathbb{F}_q(t)$ can we compute (unconditionally) the limit of the Brauer-Siegel ratio?

• Is there one such family of elliptic curves for which lim $\Sha(E_q/K)$ is $< 1$ or $0$?

• In general, if BS(K) is known for $E(K)$, bounding $\Sha(E/K)$ is equivalent to finding good upper and lower bounds for $L(E/K, 1)$. The size of $L(E/K, 1)$ depends on how the zeroes of $L(E/K, s)$ are distributed on the line $\Re(s) = 1$. The main contribution comes from the “small zeroes”.

References


Ingredients of the proof

Let $C\alpha/F_q$ be the smooth hyperelliptic curve defined by

$$\bar{C}_\alpha : y^2 = x^q + 1.$$ 

Put $g_\alpha = [2(\bar{C}_\alpha)] \in \text{genus}(\bar{C}_\alpha)$ and write the L-function of $E_\alpha$ as

$$L(E_\alpha/F_q, s) = (1 - \alpha t)^{-1} \prod_{i=1}^{n} (1 - \alpha t^i).$$

(1) [Milne] showed that the III of any twist $E'$ of a constant elliptic curve is finite and that the full BSD conjecture is true for $E'$:

$$L'(E'/K, 1) = \text{Reg}(E'/K) \otimes \text{III}(E'/K) \otimes \text{Tani}(E'/K).$$

(2) Here, $\# \Sha(E'/K)$ is $Q(1)$ and Tate($E'/K) = o(g_\alpha)$. Thus, when $g_\alpha \to \infty$,

$$\Sha(E'/K) = 1 + \log L'(E'/K, 1) + o(1).$$

(3) Easy bounds for $|L(E'/K, 1)|$ imply $\#(\bar{C}_\alpha)$ and Tate($E'/K) = o(g_\alpha)$. Thus, $\aras{g_\alpha} \to \infty$,

$$\Sha(E'/K) = 1 + \log L'(E'/K, 1) + o(1).$$

(4) [Milne] also proved that

$$L'(E'/K, 1) = \log q \eta(k \epsilon E'/K) \cdot L_\rho^\alpha(\alpha - 1)^k,$$

where $L_\rho^\alpha(T) \in \mathbb{Z}[T]$ is the numerator $L_\rho^\alpha(T)$ of $E'/K$ is $Q(1)/\log q = o(g_\alpha)$.

(5) Using the explicit formula, one can show that

$$\eta(k \epsilon E'/K) = O(1/\log q) = o(g_\alpha).$$

(6) It follows from computations of [Well] that

$$L_\rho^\alpha(T) = \prod_{m \in \mathbb{Z}/(m \epsilon E'/K)} (1 - T - q \epsilon F_\alpha \cdot g_\alpha / q \epsilon F_\alpha) \sim [\bar{E}_\alpha] \sqrt{|q \epsilon F_\alpha / \gcd(g_\alpha, d)|},$$

where $u(m) = \text{ord } g_\alpha / \gcd(g_\alpha, d)$. $J_\alpha$ is a Jacobi sum.

(7) If $d$ divides $q^h + 1$ for some $n$, [Shafarevich & Tate] proved that $u(m)$ and $J_\alpha = -q^{-h(n)/2}$. So $L_\rho^\alpha(T)$ has the form $L_\rho^\alpha(T) = \eta(k \epsilon E'/K) \cdot L_\rho^\alpha(\alpha - 1)^k q \epsilon F_\alpha / g_\alpha$.

(8) At some point, we use Bilter-Wiithelz theorem. Write $\alpha = \sqrt{\eta} \epsilon q$, then for all $n \in \mathbb{N}$, either: log $|\cos n\theta| = 0$ or log $|\sin n\theta| \geq c \log(n)$. 

Contact

Richard Griffon – Ph.D. Student [Promotor: Marc Hindy]
Institut de Mathématiques de Jussieu – Université Paris Diderot
Department of Mathematics
E-mail: richard.griffon@imj-prg.fr