On the prime Selmer ranks of cyclic prime twist families of elliptic curves over global function fields

Sun Woo Park

University of Wisconsin-Madison

May 17, 2023

Preliminary

Let $K = \mathbb{F}_q(t)$ of characteristic $\neq 2, 3$.
Fix a non-isotrivial elliptic curve $E : y^2 = x^3 + Ax + B$ over K.
Given a polynomial $f \in \mathbb{F}_q[t]$, denote by E_f the quadratic twist of E by f:

$$E_f : y^2 = x^3 + f^2 Ax + f^3 B$$

Question A

As the degree of f grows arbitrarily large, what is the probability that $\mathrm{Rank}(E_f(K)) = r$?

$$\lim_{d \to \infty} \frac{\#\{f \in \mathbb{F}_q[t] \mid \deg f = d,\ \mathrm{Rank}(E_f(K)) = r\}}{\#\{f \in \mathbb{F}_q[t] \mid \deg f = d\}}$$

Preliminary

Strategy: Use p-Selmer groups: $\operatorname{rank}(E(K)) \leq \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K)$.

Question A'

As the degree of f grows arbitrarily large, what is the probability that $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_f/K) = r$?

$$\lim_{d \to \infty} \frac{\#\{f \in \mathbb{F}_q[t] \mid \deg f = d,\ \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_f/K) = r\ \}}{\#\{f \in \mathbb{F}_q[t] \mid \deg f = d\}}$$

Bhargava-Kane-Lenstra-Poonen-Rains Heuristics (2015)

Given any prime number p coprime to $\operatorname{char}(K)$, the desired probability that $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_f/K) = r$ converges to

$$BKLPR(p,r) := \left(\prod_{j \geq 0} \frac{1}{1+p^{-j}} \right) \left(\prod_{j=1}^{r} \frac{p}{p^j - 1} \right)$$

Previous Studies

There are two parameters to control.

- q: **# Constant Field**
- d: **Degree**

Question 1: Large q, then Large d

$$\lim_{d\to\infty}\lim_{q\to\infty}\frac{\#\{f\in\mathbb{F}_q[t]\,|\,\deg f=d,\ \dim_{\mathbb{F}_p}\mathrm{Sel}_p(E_f/K)=r\ \}}{\#\{f\in\mathbb{F}_q[t]\,|\,\deg f=d\}} \tag{1}$$

Question 2: Large d, then Large q

$$\lim_{q\to\infty}\lim_{d\to\infty}\frac{\#\{f\in\mathbb{F}_q[t]\,|\,\deg f=d,\ \dim_{\mathbb{F}_p}\mathrm{Sel}_p(E_f/K)=r\ \}}{\#\{f\in\mathbb{F}_q[t]\,|\,\deg f=d\}} \tag{2}$$

Previous Studies

	Family		Large q, Large d		Large d, Large q	
	Univ.	Quad.	Average	Prob.	Average	Prob.
Landesman (2021)	✓		✓			
P., Wang (2021)		✓	✓			
Feng Landesman (2022) Rains	✓			✓		
de Jong (2002)	✓				✓ ($p = 3$)	
Hô Lê Húng (2013) Ngô	✓				✓ ($p = 2$)	

Previous studies (Optional)

Motivation (1st moments):

- A representable finite étale cover $\tau_d \to \mathcal{M}_d$ over moduli space of quad. twist families of elliptic curves E_f in $\mathcal{M}_d$ twisted by degree d polynomials f over $\mathbb{F}_q$.
- Want: $\mathbb{F}_q$-rational points of geometric fibers of $\tau_d \to \mathcal{M}_d$ to parametrize $\mathrm{Sel}_p(E_f/K)$.
- Grothendieck-Lefschetz trace formula

$$\mathbb{E}[\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_f/K) = r \mid \deg f = d] = \frac{1}{q^d} \sum_{i=0}^{2d} (-1)^i \mathrm{Tr} Frob_q | H^i_{\text{ét,c}}((\tau_d)_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)$$

- **Question 1**: Suffice to understand $H^{2d}_{\text{ét,c}}((\tau_d)_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)$.
- **Question 2**: Understand $H^i_{\text{ét,c}}((\tau_d)_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)$ for all $0 \leq i \leq 2d$.
- **Large q**: $O(\frac{1}{\sqrt{q}})$, originating from $H^i_{\text{ét,c}}((\tau_d)_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)$ for $i \leq 2d-1$.

Previous Studies

Let's return back to the original question.

$$\lim_{d\to\infty} \frac{\#\{f \in \mathbb{F}_q[t] \mid \deg f = d,\ \mathrm{Sel}_p(E_f/K) = r\ \}}{\#\{f \in \mathbb{F}_q[t] \mid \deg f = d\}}$$

Meanwhile...

Let's use the generalized Riemann hypothesis over $\mathbb{F}_q(t)$.
Here are some notable consequences:

1. Effective Chebotarev density theorem
2. Effective Erdös-Kac theorem

Previous Studies

	Family		Large q, Large d		Large d, Large q	
	Univ.	Quad.	Average	Prob.	Average	Prob.
Landesman (2021)	✓		✓			
P., Wang (2021)		✓	✓			
Feng Landesman (2022) Rains	✓			✓		
de Jong (2002)	✓				✓ ($p = 3$)	
Hô Lê Húng (2013) Ngô	✓				✓ ($p = 2$)	

Previous Studies

	Family		Large q, Large d		Large d, Large q		**Large d**
	Univ.	Quad.	Average	Prob.	Average	Prob.	**Prob.**
Landesman (2021)	✓		✓				
P., Wang (2021)		✓	✓				
Feng Landesman (2022) Rains	✓			✓			
de Jong (2002)	✓				✓ ($p = 3$)		
Hô Lê Húng (2013) Ngô	✓				✓ ($p = 2$)		

Previous Studies

	Family		Large q, Large d		Large d, Large q		**Large d**
	Univ.	Quad.	Average	Prob.	Average	Prob.	**Prob.**
Landesman (2021)	✓		✓				
P., Wang (2021)		✓	✓				
Feng Landesman (2022) Rains	✓			✓			
de Jong (2002)	✓				✓ ($p = 3$)		
Hồ Lê Húng (2013) Ngô	✓				✓ ($p = 2$)		
P. (2022)		✓					✓ ($p = 2$)

Main Theorem

Theorem (P. (2022))

Suppose E/K satisfies the following three conditions.

1. E is non-isotrivial.
2. $\mathrm{Gal}(K(E[2])/K) \cong S_3$.
3. E has a place of split multiplicative reduction.

Then for sufficiently large d, there exists a fixed constant $B > 0$ independent of d and q such that

$$|\mathbb{P}[\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_f) = r \mid \deg f = d] - BKLPR(2, r)| < B \cdot d^{-1/3}.$$

Motivation

Key Tools:

1. Effective Erdös-Kac Theorem
2. Effective Chebotarev Density Theorem
3. Ergodicity of Markov chains

Klagsbrun, Mazur, Rubin (2014): (Number fields) Loosely speaking...

1. Variations of **non-canonically ordered** $\mathrm{Sel}_2(E_{p_1 p_2 \cdots p_k})$ twisted by consecutive **k** prime twists $p_1, p_2, \cdots, p_k$.
2. Apply Markov Chain by **k** iterations.

Motivation

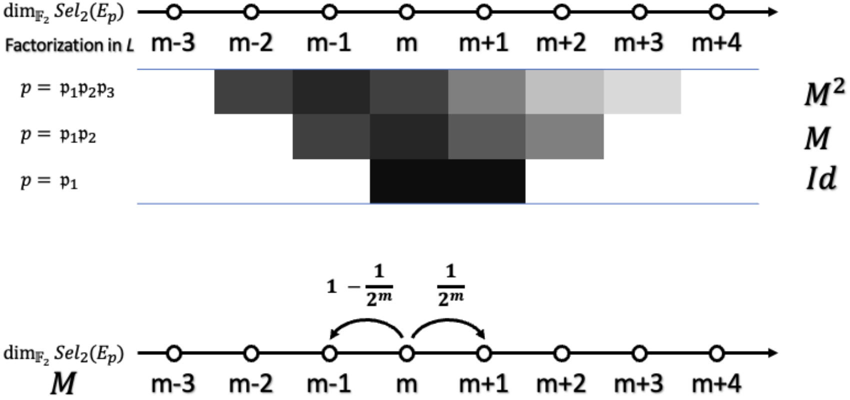
$E_p^{[1]}: py^2 = x^3 + x - 1$
$0 < p < 500{,}000$
$\dim_{\mathbb{F}_2} Sel_2(E^{[1]}) = 1$
$L = \mathbb{Q}[x]/(x^3 + x - 1)$

$\dim_{\mathbb{F}_2} Sel_2(E_p^{[1]})$ / Factorization in L	0	1	2	3	4	5	6	7
$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	12.56	65.95	12.49	9.00	0	0	0	0
$p = \mathfrak{p}_1\mathfrak{p}_2$	37.41	25.01	37.58	0	0	0	0	0
$p = \mathfrak{p}_1$	25.04	74.96	0	0	0	0	0	0

$E_p^{[2]}: py^2 = x^3 + 4x + 1$
$0 < p < 500{,}000$
$\dim_{\mathbb{F}_2} Sel_2(E^{[2]}) = 1$
$L = \mathbb{Q}[x]/(x^3 + 4x + 1)$

$\dim_{\mathbb{F}_2} Sel_2(E_p^{[2]})$ / Factorization in L	0	1	2	3	4	5	6	7
$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	18.63	43.80	29.94	6.04	1.59	0	0	0
$p = \mathfrak{p}_1\mathfrak{p}_2$	25.14	37.68	24.68	12.50	0	0	0	0
$p = \mathfrak{p}_1$	0	50.04	49.96	0	0	0	0	0

Motivation



$\dim_{\mathbb{F}_2} Sel_2(E_p)$
Factorization in L
m-3 m-2 m-1 m m+1 m+2 m+3 m+4
$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$
$p = \mathfrak{p}_1\mathfrak{p}_2$
$p = \mathfrak{p}_1$
M^2
M
Id
$1 - \frac{1}{2^m}$
$\frac{1}{2^m}$
$\dim_{\mathbb{F}_2} Sel_2(E_p)$
M
m-3 m-2 m-1 m m+1 m+2 m+3 m+4

Idea of Proof

1. Markov Chain of our interest:

$$\frac{1}{3} + \frac{1}{2}M + \frac{1}{6}M^2 \tag{3}$$

2. **Use Chebotarev density theorem** over L^*/K:

$$L^* := \text{Fixed field of} \bigcap_{c \in \mathrm{Sel}_2(E_{p_1 p_2 \cdots p_k})} \mathrm{Ker}\left(c : \mathrm{Gal}(\overline{K}/K(E[2])) \to E[2]\right)$$

(Require that $\mathrm{Gal}(K(E[2])/K) \cong S_3$.)

Yes: Consecutive iteration of $M_L \iff$ Consecutive prime twist of E.

But: Assume $0 < |p_1| \ll |p_2| \ll \cdots \ll |p_k|$.

Non-canonical ordering of E_f's.

Unknown explicit error terms.

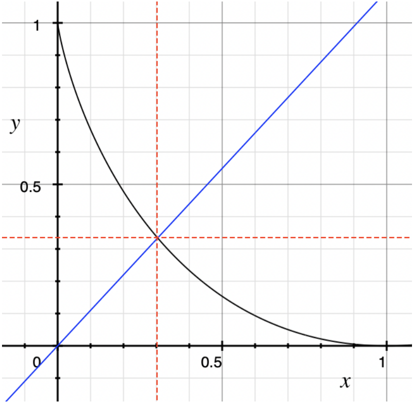
Idea of Proof

Fix a constant $0 < \rho < 1$.

1. **Erdös-Kac**: # iterations of M_L
   - Distinct # prime factors: At least $\rho \ln d$ factors.
   - **Error term**: $\epsilon_{EK} \sim O(d^{-\rho \ln \rho + \rho - 1})$.
2. **Chebotarev**: Deviation from M_L under **canonical order**
   - Growth of prime factors: $\deg p_i > \frac{4(\ln d)^2}{\ln q}$ (for every i)
   - Reordering: $\deg p^* > \sqrt[3]{d}$ for at least one inert prime factor p^*.
   - **Error term**: $\epsilon_{Cheb} \sim O(d^{-\ln d})$.
3. **Ergodicity**: Limiting behavior of M_L
   - Stationary Distribution: BKLPR probability distribution.
   - Convergence rate: Geometric convergence at a rate $\gamma > \frac{1}{3}$.
   - **Error term**: $\epsilon_{Markov} \sim O(d^{-\rho \ln 3})$.

Idea of Proof

Total Error: $B(\epsilon_{EK} + \epsilon_{Cheb} + \epsilon_{Markov}) \sim B \cdot \left(\frac{1}{d^{\rho \ln \rho + 1 - \rho}} + d^{-\ln d} + \frac{1}{d^{\rho \ln 3}}\right)$.



Hence, we can choose $\rho \sim 0.304$ to obtain the desired error bounds

$$B \cdot \left(\frac{1}{d^{\rho \ln \rho + 1 - \rho}} + d^{-\ln d} + \frac{1}{d^{\rho \ln 3}}\right) \sim B \cdot d^{-1/3}.$$

Ending Remarks (Optional)

Mazur, Rubin (2007): Assume $\mu_p \subset K$.

$$E_{p,f} := \mathrm{Ker}\left(\mathbb{N} : \mathrm{Res}_K^{K(\sqrt[p]{f})} E \to E\right) \tag{4}$$

Note $\mathrm{Gal}(K(\sqrt[p]{f})/K) \cong \mathbb{Z}/p\mathbb{Z}$.
Choose a cyclic generator $\sigma_{p,f} \in \mathrm{Gal}(K(\sqrt[p]{f})/K)$.
Similar to quadratic twist families, assume $\mathrm{Gal}(K(E[p])/K) \supset \mathrm{SL}_2(\mathbb{F}_p)$,

$$\left|\mathbb{P}[\dim_{\mathbb{F}_p} \mathrm{Sel}_{1-\sigma_{p,f}}(E_f) = r \mid \deg f = d] - BKLPR(p,r)\right| < B \cdot \frac{1}{d^{\alpha(p)}} \tag{5}$$

If Alex Smith's work is applicable to $K = \mathbb{F}_q(t)$, then we can hope:

$$\lim_{n\to\infty} \mathbb{P}\left[\mathrm{Corank}_{\mathbb{Z}_p} \mathrm{Sel}_{(1-\sigma_{p,f})^\infty}(E_{p,f}/K) = r \mid \deg f = d\right] = \begin{cases} \frac{1}{2} & \text{if } r = 0 \\ \frac{1}{2} & \text{if } r = 1 \\ 0 & \text{otherwise} \end{cases}$$

Ending Remarks (Optional)

Future Directions: Non-abelian twist families over global fields

$$E_n/\mathbb{Q} : y^2 = x^3 - 432n^2 \tag{6}$$

Consider the following 4-dimensional abelian variety over $\mathbb{Q}$:

$$B_n := \mathrm{Ker}\left(\mathbb{N} : \mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_3, \sqrt[3]{n})} E_1 \to \mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_3)} E_1\right) \tag{7}$$

Pick a generator of the cyclic subgroup $\sigma_{3,n} \in \mathbb{Z}/3\mathbb{Z} \subset S_3$.

$$\begin{gathered} B_n[1 - \sigma_{3,n}] \cong E_1[3]^{\oplus 2}. \\ \mathrm{Rank}(E_n(\mathbb{Q})) + \mathrm{Rank}(E_{n^2}(\mathbb{Q})) \leq \dim_{\mathbb{F}_3} \mathrm{Sel}_{1-\sigma_{3,n}}(B_n/\mathbb{Q}). \end{gathered} \tag{8}$$

In progress: Compute upper / lower bounds on the probability of the addition of ranks of E_n and E_{n^2} over $\mathbb{Q}$, assuming GRH.

References

Zev Klagsbrun, Barry Mazur, and Karl Rubin (2014)
A Markov model for Selmer ranks in families of twists
Compositio Mathematica 150, pp 1077–1106

Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra Jr., Bjorn Poonen, and Eric Rains (2015)
Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves
Cambridge Journal of Mathematics 3(3), pp. 275–321

Tony Feng, Aaron Landesman, and Eric Rains (2022)
The geometric distribution of Selmer groups of elliptic curves over function fields
Mathematische Annalen https://doi.org/10.1007/s00208-022-02429-1

Alexander Smith (2022)
The distribution of l^∞ Selmer groups in degree l twist families
Available on arxiv https://arxiv.org/abs/2207.05674

Sun Woo Park (2022)
On the prime Selmer ranks of cyclic prime twist families of elliptic curves over global function fields