MAGIC online seminar

13. August 2020

Richard GRIFFON
Universität Basel

Elliptic curves with large Tate–Shafarevich groups over $\mathbb{F}_q(t)$

(joint with Guus de WIT)

ArXiv:1907.13038

Introduction

Elliptic curves over $\mathbb{F}_q(t)$

Setting

Let $K = \mathbb{F}_q(t)$, where $\mathbb{F}_q$ is a finite field of characteristic $p \geq 5$.

Let E be an elliptic curve over K:

$$E: \qquad Y^2 = X^3 + A(t) \cdot X + B(t),$$

for some $A(t), B(t) \in K$.

Arithmetic of E: largely analogous to that of an elliptic curve over a number field. Example: Mordell–Weil theorem.

First definition of $Ш(E)$

In terms of Galois cohomology:

$$Ш(E) = \ker\left(\mathrm{H}^1(E, K) \longrightarrow \prod_v \mathrm{H}^1(E, K_v)\right).$$

Tate-Shafarevich groups

Definition of $Ш(E)$

More geometric:

$$Ш(E) = \left\{ \begin{array}{c} (C, i) \text{ where } C/K \text{ curve of genus 1 s.t.} \\ i : \mathrm{Jac}(C) \simeq E \text{ and s.t. } C \text{ has a} \\ K_v\text{-rational point, for all places } v \text{ of } K \end{array} \right\} \Big/ (\text{isom.}),$$

where $K_v =$ completion of K at v for any place v.

$[(C, i)] \in Ш(E)$ is trivial if and only if C has a K-rational point.

"Size of $Ш(E)$" measures how badly the local-global principle fails.

Conjecture

$Ш(E)$ is finite.

Question: Assuming that $Ш(E)$ is finite: how big is it?

Height and conductor

- E has a conductor divisor $\mathcal{N}(E) = \sum f_v \cdot v \in \mathrm{Div}(\mathbb{P}^1)$. Encodes types of reduction of E at bad places.

Conductor

$$N(E) := q^{\deg \mathcal{N}(E)}.$$

- E admits a minimal integral Weierstrass model

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

with $a_1, \ldots, a_6 \in \mathbb{F}_q[t]$ satisfying a minimality condition. Let

$$\deg \omega_E := \min \{h \in \mathbb{Z}_{\geq 1} : \text{for all } i,\ \deg(a_i) \leq h \cdot i\}.$$

(Exponential differential) height

$$H(E) := q^{\deg \omega_E}.$$

Remark: $N(E)$ is the analogue of conductor of $E'/\mathbb{Q}$, $H(E)$ analogue of $\Delta_{min}(E'/\mathbb{Q})^{1/12}$ which is $\approx \exp(h_{Fal}(E'))$.

Size of Ш? Upper bounds

Question

Assuming that $Ш(E)$ is finite,
how big is $|Ш(E)|$ in terms of $\mathrm{H}(E)$ or $N(E)$?

Some **upper bounds** are known:

Theorem (Goldfeld & Szpiro, '95)

Let E/K be an elliptic curve s.t. $j(E) \in K \smallsetminus \mathbb{F}_q$. **If $Ш(E)$ is finite**, *we have*

(1) $\forall \epsilon > 0,\ |Ш(E)| \ll_{q,\epsilon} \mathrm{H}(E)^{1+\epsilon}$.

(2) *If, moreover, $j(E) \notin K^p$, then*
$\forall \epsilon > 0,\ |Ш(E)| \ll_{q,\epsilon} N(E)^{1/2+\epsilon}$.

Large Ш's?

What about **lower bounds**?

- Expected: there are infinitely many E/K with $|Ш(E)| = 1$.
  So cannot expect better than $|Ш(E)| \gg H(E)^0$ in general.
- But then, can't the exponents 1 and $1/2$ in Goldeld–Szpiro's theorem be replaced by smaller constants? or are they optimal?

Conjecture (de Weger, '98)

The exponents 1 and $1/2$ are essentially best possible:

(1) $\forall \epsilon > 0$, *there are infinitely many elliptic curves E/K with separable $j(E)$ such that* $|Ш(E)| \gg_{q,\epsilon} \mathrm{H}(E)^{1-\epsilon}$.

(2) $\forall \epsilon > 0$, *there are infinitely many elliptic curves E/K with separable $j(E)$ such that* $|Ш(E)| \gg_{q,\epsilon} N(E)^{1/2-\epsilon}$.

Remark: over $\mathbb{Q}$, modulo BSD:
(1) is proved (de Weger), "weak (2)" with exponent $1/4$ (Mai&Murty).

An example

Condition that $j(E) \notin K^p$? To avoid trivial situations in (1)!

An example

For any integer $n \geq 1$, let E_n/K be given by

$$E_n : \qquad Y^2 = X(X-1)(X-t^{p^n}).$$

E_n is the pullback of E_0 under p^n-th power Frobenius.
Hence $j(E_n)$ is a p^n-th power in K.

Then one can show

Proposition

(i) For all $n \geq 1$, $|Ш(E_n)|$ is finite.

(ii) As $n \to \infty$, we have $|Ш(E_n)| \geq |Ш(E_n)[p^\infty]| \geq H(E_n)^{1-o(1)}$.

(No result towards (2) because the E_n's are pairwise K-isogenous).

Large $Ш$! Our result

Conjecture (de Weger, '98)

(1) $\forall \epsilon > 0$, *there are infinitely many elliptic curves* E/K *with separable* $j(E)$ *such that* $|Ш(E)| \gg_{q,\epsilon} \mathrm{H}(E)^{1-\epsilon}$.

(2) $\forall \epsilon > 0$, *there are infinitely many elliptic curves* E/K *with separable* $j(E)$ *such that* $|Ш(E)| \gg_{q,\epsilon} N(E)^{1/2-\epsilon}$.

We prove (1) and a result towards (2):

Theorem (G. & de Wit, '19)

For all $\epsilon > 0$, *there are infinitely many elliptic curves* E *over* K *with separable* j*-invariant and finite* $Ш(E)$, *such that*

(1) $|Ш(E)| \geq \mathrm{H}(E)^{1-\epsilon}$.

(2) $|Ш(E)| \geq N(E)^{1/4-\epsilon}$.

The sequence $\{E_a\}_{a \geq 1}$

The sequence

Setting: $K = \mathbb{F}_q(t)$, where $\mathbb{F}_q$ is a finite field of characteristic $p \geq 5$.

The sequence

For all $a \geq 1$, consider E_a/K given by

$$E_a : \qquad Y^2 = X\big(X^2 + (t^{q^a} - t)X + 1\big).$$

$\{E_a\}_{a\geq 1}$ is an "Artin–Schreier family" of elliptic curves (Pries & Ulmer).

First observations:

- $j(E_a)$ not constant, and $j(E_a) \notin K^p$. Also $(\deg j(E_a))_a$ increasing.
- E_a's are pairwise not isomorphic over $\overline{K}$
- $H(E_a) = N(E_a)^4$. And $(N(E_a))_a$ increasing.
- E_a's are pairwise not isogenous over K.

Main theorem

For all $a \geq 1$, let $E_a : \ Y^2 = X\big(X^2 + (t^{q^a} - t)X + 1\big)$.

Main theorem (G. & de Wit, '19)

(0) For all $a \geq 1$, $j(E_a)$ is separable ($j(E_a) \notin K^p$).

(1) For all $a \geq 1$, $Ш(E_a)$ is finite.

(2) As $a \to +\infty$,
$$|Ш(E_a)| = \mathrm{H}(E_a)^{1+o(1)}.$$

(3) For all $a \geq 1$, $|Ш(E_a)[p^\infty]| = 1$.

Consequence: For any $\epsilon > 0$, all but finitely many E_a's satisfy

$$|Ш(E_a)| \geq H(E_a)^{1-\epsilon} \qquad \text{and} \qquad |Ш(E_a)| \geq N(E_a)^{1/4-\epsilon},$$

since $\mathrm{H}(E_a) = N(E_a)^{1/4}$.

Strategy of proof

Proof of $|Ш(E_a)| = \mathrm{H}(E_a)^{1+o(1)}$.

"Analytic approach": we study the L-function $L(E_a, s)$ of E_a.

I. Compute explicit expression of $L(E_a, s)$.

   Study at $s = 1$.

II. Show that BSD conjecture holds for E_a. Gives that

   (i) $Ш(E_a)$ is finite.
   (ii) relation $(\bigstar)$ between $|Ш(E_a)|$ and $L(E_a, 1)$.

III. Prove bounds on $L(E_a, 1)$. (Most difficult: lower bound).

   By $(\bigstar)$, deduce bounds on $|Ш(E_a)|$.

The L-function

Definition

For any place v of K, let $\mathbb{F}_v =$ residue field of K at v.
We write $[\mathbb{F}_v : \mathbb{F}_q] = \deg v$, and $\widetilde{(E_a)}_v/\mathbb{F}_v$ reduction of E_a at v
Let $a_v(E) = q^{\deg v} + 1 - |\widetilde{(E_a)}_v(\mathbb{F}_v)|$, and

$$L_v(E_a, s) = \begin{cases} 1 - a_v(E) \cdot q^{-s \deg v} + q^{-s(1-2\deg v)} & \text{if } \widetilde{(E_a)}_v \text{ smooth,} \\ 1 - a_v(E) \cdot q^{-s \deg v} & \text{otherwise.} \end{cases}$$

The L-function $L(E_a, s)$ of E_a/K is defined by

$$L(E_a, s) = \prod_v L_v(E_a, s)^{-1},$$

where v runs over all places of K.

Deep results: $L(E_a, s)$ entire, $L(E_a, s)$ satisfies a functional equation ($s \leftrightarrow 2 - s$), and the Riemann Hypothesis (Grothendieck, Deligne, ...).

Some notation

☐ For any $a \geq 1$, $P_a := \{\text{places } v \text{ of } K \text{ s.t. } v \neq 0, \infty \text{ and } \deg v \mid a\}$.

$P_a \leftrightarrow \{\text{closed pts. of } \mathbb{G}_m = \mathbb{P}^1 \smallsetminus \{0, \infty\} \text{ whose degree divides } a\}$.
A place $v \in P_a$ is a $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbit of points $\beta \in \overline{\mathbb{F}_q}^{\times}$.

☐ For $v \in P_a$, let $\mathbb{F}_v =$ residue field of K at v.
Write $\mathrm{Tr}_{\mathbb{F}_v/\mathbb{F}_p}, \mathrm{Nm}_{\mathbb{F}_v/\mathbb{F}_p}$ = trace and norm $\mathbb{F}_v \to \mathbb{F}_p$.
Define an additive character

$$\begin{array}{rccc} \psi_v : & \mathbb{F}_v & \longrightarrow & \mathbb{Q}(\zeta_p)^{\times} \\ & x & \mapsto & \zeta_p^{\mathrm{Tr}_{\mathbb{F}_v/\mathbb{F}_p}(x)} \end{array}$$

Two character sums

For any $v \in P_a$, pick any $\beta \in v$ and let

$$\mathbf{g}(v) := -\sum_{x \in \mathbb{F}_v^{\times}} \left(\frac{\mathrm{Nm}_{\mathbb{F}_v/\mathbb{F}_p}(x)}{p}\right) \cdot \psi_v(\beta x), \quad \mathbf{Kl}(v) := -\sum_{x \in \mathbb{F}_v^{\times}} \psi_v\left(x + \frac{\beta^2}{x}\right)$$

quadratic Gauss sum on $\mathbb{F}_v$ Kloosterman sum on $\mathbb{F}_v$

(values do not depend on $\beta \in v$!)

Expression for $L(E_a, s)$

For all $a \geq 1$,

- $P_a := \{\text{places } v \text{ of } K \text{ s.t. } v \neq 0, \infty \text{ and } \deg v \mid a\}$.

For all $v \in P_a$,

- $\mathbf{g}(v)$ is a quadratic Gauss sum on $\mathbb{F}_v$.
- $\mathbf{Kl}(v)$ is a Kloosterman sum on $\mathbb{F}_v$.

Theorem (G. & de Wit, '19)

For all $a \geq 1$,

$$L(E_a, s) = \prod_{v \in P_a} \left(1 - \mathbf{g}(v)\mathbf{Kl}(v) \cdot (q^{-s})^{\deg v} + \mathbf{g}(v)^2 \cdot (q^{1-2s})^{\deg v}\right).$$

Note: As a polynomial in q^{-s}, $L(E_a, s)$ has integral coefficients.

Non vanishing at $s = 1$ and consequences

Behaviour at central point

From previous theorem:

$$L(E_a, 1) = \prod_{v \in P_a} \left(1 - \frac{\mathbf{g}(v)\mathbf{Kl}(v)}{q^{\deg v}} + \frac{\mathbf{g}(v)^2}{q^{\deg v}}\right).$$

Angles of $\mathbf{g}(v)$ and $\mathbf{Kl}(v)$

For any $v \in P_a$,

- $\mathbf{g}(v) \in \mathbb{Q}(\zeta_p)$ and has the form $(4\text{-th root of } 1) \times |\mathbb{F}_v|^{1/2}$.
  There is $\alpha_v \in \{0, \pi/2, \pi, 3\pi/2\}$ s.t. $\mathbf{g}(v) = \mathrm{e}^{i\alpha_v} \cdot q^{\deg v/2}$.
- $\mathbf{Kl}(v) \in \mathbb{Q}(\zeta_p)$ is totally real and $|\mathbf{Kl}(v)| \leq 2|\mathbb{F}_v|^{1/2}$ (Weil bound).
  There is $\boldsymbol{\theta}_v \in [0, \pi]$ s.t. $\mathbf{Kl}(v) = 2q^{\deg v/2} \cdot \cos \boldsymbol{\theta}_v$.

After choice of $\mathbb{Q}(\zeta_p) \hookrightarrow \mathbb{C}$.

$$L(E_a, 1) = \prod_{v \in P_a} \left(1 - \mathrm{e}^{i(\alpha_v + \boldsymbol{\theta}_v)}\right)\left(1 - \mathrm{e}^{i(\alpha_v - \boldsymbol{\theta}_v)}\right).$$

Non-vanishing at $s = 1$

We have:

$$L(E_a, 1) = \prod_{v \in P_a} \left(1 - \mathrm{e}^{i(\alpha_v + \boldsymbol{\theta}_v)}\right)\left(1 - \mathrm{e}^{i(\alpha_v - \boldsymbol{\theta}_v)}\right).$$

Lemma

For any $v \in P_a$, $\boldsymbol{\theta}_v \notin \{0, \pi/2, \pi\}$.

Proof: $\mathbf{Kl}(v) \equiv 1 \bmod p$ in $\mathbb{Q}(\zeta_p)$, so $\mathbf{Kl}(v)$ is a p-adic unit.
Hence $\mathbf{Kl}(v) = 2q^{\deg v/2} \cdot \cos \boldsymbol{\theta}_v \neq 0, \pm 2q^{\deg v/2}$.

In particular $\alpha_v \pm \boldsymbol{\theta}_v \neq 0 \bmod 2\pi$. Hence

Corollary

For any $a \geq 1$, $L(E_a, 1) \neq 0$.

BSD conjecture

For any $a \geq 1$, $L(E_a, 1) \in \mathbb{Q}$ is nonzero. I.e., $\operatorname{ord}_{s=1} L(E_a, s) = 0$.

BSD is known for elliptic curves of analytic rank 0 over K (Tate, Milne).

Corollary (Birch&Swinnerton–Dyer conjecture for E_a)

For all $a \geq 1$, the BSD conjecture holds for E_a:

1. *$E_a(K)$ is finite.*
2. *$Ш(E_a)$ is finite.*
3. *$|Ш(E_a)| = L(E_a, 1) \cdot q^{-1} \mathrm{H}(E_a)$.* **(★)**

Remarks

- ☐ BSD first proved by Pries & Ulmer (geometric method).
- ☐ Other terms in BSD formula: cancel out.
- ☐ More precisely, $E_a(K) = \{\mathcal{O}, (0,0)\} \simeq \mathbb{Z}/2\mathbb{Z}$.

Bounds on $|Ш(E_a)|$

Goal

Now, we know that $Ш(E_a)$ **is finite**.

By Goldfeld–Szpiro, we have $|Ш(E_a)| \leq H(E_a)^{1+o(1)}$.

Remains to prove that $|Ш(E_a)| \geq H(E_a)^{1-o(1)}$.
By $(\bigstar)$, $|Ш(E_a)| = L(E_a, 1) \cdot q^{-1}\mathrm{H}(E_a)$, so we need to prove:

Goal

$$\frac{\log L(E_a, 1)}{\log H(E_a)} \geq -o(1), \qquad (\text{as } a \to \infty).$$

Remark: Generic lower bound is $\dfrac{\log L(E_a, 1)}{\log H(E_a)} \geq -1 - o(1)$.

Link with an average

Goal

$$\frac{\log L(E_a, 1)}{\log H(E_a)} \geq -o(1), \qquad (\text{as } a \to \infty).$$

Using our expression for $L(E_a, 1)$, we get

$$\frac{\log L(E_a, 1)}{\log H(E_a)} \geq \frac{|P_a|}{\log H(E_a)} \cdot \frac{1}{|P_a|} \sum_{v \in P_a} \log \left(\sin^2 \boldsymbol{\theta}_v \cdot \cos^2 \boldsymbol{\theta}_v \right).$$

We write $w(\theta) := \log \left(\sin^2 \theta \cdot \cos^2 \theta \right)$. Recall that $\boldsymbol{\theta}_v \notin \{0, \pi/2, \pi\}$.

To achieve **Goal**, it suffices to control the asymptotic behaviour of

$$\frac{1}{|P_a|} \sum_{v \in P_a} w(\boldsymbol{\theta}_v).$$

Clearly depends on the distribution of $\{\boldsymbol{\theta}_v\}_{v \in P_a}$ as $a \to \infty$.

Distribution of angles

- The set of angles of Kloosterman sums becomes equidistributed in $[0, \pi]$ with respect to the Sato–Tate measure (Katz).
- The set $\{\boldsymbol{\theta}_v\}_{v \in P_a}$ becomes equidistributed in $[0, \pi]$ with respect to the Sato–Tate measure (Fu–Liu).

Concretely,

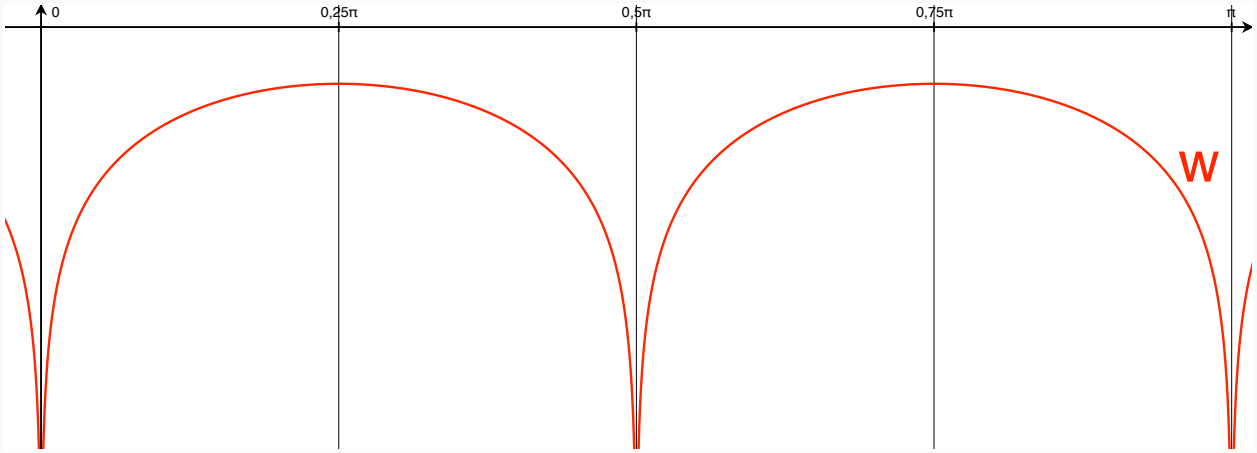
Theorem (Katz, '88 + Fu & Liu, '05)

For all continuous functions $f : [0, \pi] \to \mathbb{R}$,

$$\frac{1}{|P_a|} \sum_{v \in P_a} f(\boldsymbol{\theta}_v) \xrightarrow[a \to \infty]{} \frac{2}{\pi} \int_0^\pi f(\theta) \sin^2(\theta) \mathrm{d}\theta.$$

Not sufficient: $w(\theta) = \log\left(\sin^2\theta \cdot \cos^2\theta\right)$ has poles at $\{0, \pi/2, \pi\}$!

Approximation



Well, let's approximate *w* by regular functions! However,

- ☐ Introduces error terms, to be controlled.
- ☐ Need to "calibrate" the approximation.

Finer results are needed.

Quantitative equidistribution

We first need a quantitative version of Fu–Liu's theorem.

Theorem (G., '19)

For all continuously differentiable functions $g : [0, \pi] \to \mathbb{R}$,

$$\left| \frac{1}{|P_a|} \sum_{v \in P_a} g(\boldsymbol{\theta}_v) - \frac{2}{\pi} \int_0^\pi g(\theta) \sin^2(\theta) \mathrm{d}\theta \right| \ll_q \frac{a^{1/2}}{q^{a/4}} \cdot \int_0^\pi |g'(\theta)| \mathrm{d}\theta.$$

Proof: Explicit version of Katz&Fu–Liu's theorem + Tools from theory of distribution of sequences (Niederreiter).

"Calibration": find balance between

g approximates w well VS g has small enough variation.

Angles stay away from poles

We also need an effective version of the fact that $\boldsymbol{\theta}_v \notin \{0, \pi/2, \pi\}$.

Theorem (G.& de Wit, '19)

There is a constant $c > 0$ such that: for all $a \geq 1$,

$$\min_{v \in P_a} \left\{ \boldsymbol{\theta}_v, \left| \frac{\pi}{2} - \boldsymbol{\theta}_v \right|, \pi - \boldsymbol{\theta}_v \right\} \geq (q^a)^{-c}.$$

Proof: $\cos \boldsymbol{\theta}_v = \mathbf{Kl}(v)/q^{\deg v/2}$ is an algebraic number of bounded degree + Liouville's inequality.

Controls an error term: Shows that $\frac{1}{|P_a|} \sum_v w(\boldsymbol{\theta}_v) = \frac{1}{|P_a|} \sum_v g(\boldsymbol{\theta}_v)$ if $g \equiv w$ on $[0, \pi] \smallsetminus$ ("safe intervals" around $0, \pi/2, \pi$).

Consequence

Approximating w by suitable functions g, we get

Proposition (G.& de Wit, '19)

$$\frac{1}{|P_a|}\sum_{v\in P_a} w(\boldsymbol{\theta}_v) \xrightarrow[a\to\infty]{} \frac{2}{\pi}\int_0^\pi w(\theta)\sin^2\theta \mathrm{d}\theta = -\log 16.$$

Hence

$$\frac{\log L(E_a,1)}{\log H(E_a)} \geq \frac{|P_a|}{\log H(E_a)} \cdot \frac{1}{|P_a|}\sum_{v\in P_a} w(\boldsymbol{\theta}_v) \geq -o(1).$$

Therefore $|Ш(E_a)| \geq H(E_a)^{1-o(1)}$ by (★).

p-adic size of $L(E_a, 1)$

Claim: $|Ш(E_a)[p^\infty]| = 1$.

Start with **(★)**:

$$|Ш(E_a)| = L(E_a, 1) \cdot q^{-1}\mathrm{H}(E_a).$$

Take p-adic valuation on both sides.

Compute p-adic valuation of $L(E_a, 1) \in \mathbb{Q}^\times$ from:

$$L(E_a, 1) = \prod_{v \in P_a} \left(1 - \frac{\mathbf{g}(v)\mathbf{Kl}(v)}{q^{\deg v}} + \frac{\mathbf{g}(v)^2}{q^{\deg v}}\right).$$

and two facts: $\mathbf{Kl}(v)$ is a p-adic unit and $\mathbf{g}(v)^4 = q^{2\deg v}$.

We obtain that $\mathrm{val}_p(L(E_a, 1)) = -\mathrm{val}_p(q^{-1}\mathrm{H}(E_a))$.

Therefore $|Ш(E_a)|$ is prime to p, so $Ш(E_a)[p^\infty]$ **is trivial.**

Conclusion

For all $a \geq 1$, consider E_a/K given by

$$E_a : \qquad Y^2 = X\big(X^2 + (t^{q^a} - t)X + 1\big).$$

Theorem (G. & de Wit, '19)

(0) For all $a \geq 1$, $j(E_a)$ is separable ($j(E_a) \notin K^p$).

(1) For all $a \geq 1$, $Ш(E_a)$ is finite.

(2) As $a \to +\infty$,
$$|Ш(E_a)| = \mathrm{H}(E_a)^{1+o(1)}.$$

(3) For all $a \geq 1$, $|Ш(E_a)[p^\infty]| = 1$.

More details: `ArXiv:1907.13038`

Thank you for your attention!