An Elliptic Curve Prime Race Problem

Kin Ming Tsang

University of British Columbia

Comparative Prime Number Theory Symposium
June 21, 2024

joint with Yifeng Huang and Chi Hoi (Kyle) Yip

Beginning

Undergraduate research program on Elliptic Curves by my advisor.

Beginning

Undergraduate research program on Elliptic Curves by my advisor.

Given an elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Q}$, where $a, b \in \mathbb{Z}$. We know that the trace of Frobenius at good prime p are given by

$$a_p(E) = p + 1 - \#E(\mathbb{F}_p)$$

Beginning

Undergraduate research program on Elliptic Curves by my advisor.

Given an elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Q}$, where $a, b \in \mathbb{Z}$. We know that the trace of Frobenius at good prime p are given by

$$a_p(E) = p + 1 - \#E(\mathbb{F}_p)$$

Fix prime $\ell \neq p$, the undergraduates plot some graphs on the race of a_p for $a_p \equiv r_1 \mod \ell$ and $a_p \equiv r_{-1} \mod \ell$, for some $0 \leq r_1, r_{-1} \leq \ell - 1$.

Beginning

Undergraduate research program on Elliptic Curves by my advisor.

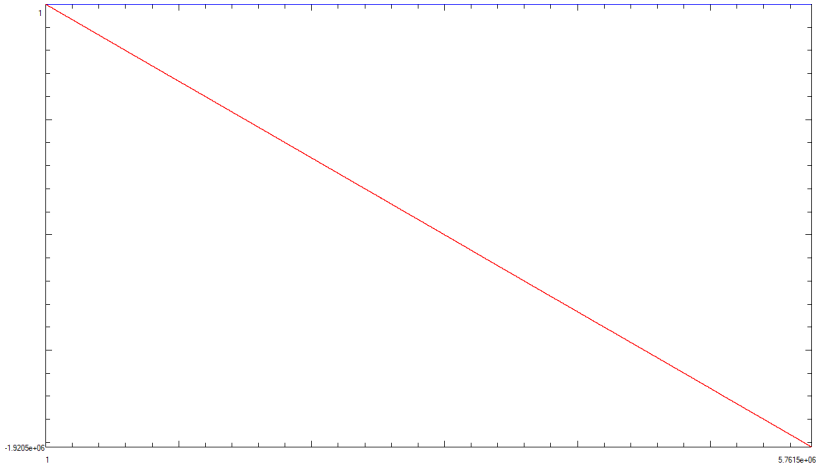
Given an elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Q}$, where $a, b \in \mathbb{Z}$. We know that the trace of Frobenius at good prime p are given by

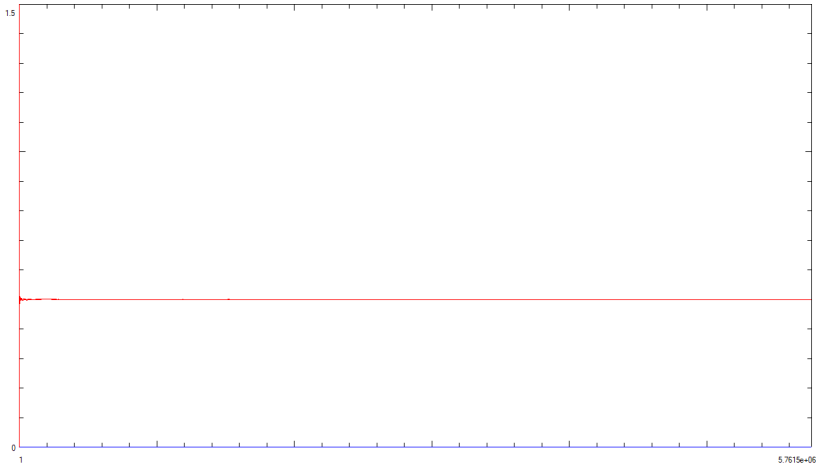
$$a_p(E) = p + 1 - \#E(\mathbb{F}_p)$$

Fix prime $\ell \neq p$, the undergraduates plot some graphs on the race of a_p for $a_p \equiv r_1 \mod \ell$ and $a_p \equiv r_{-1} \mod \ell$, for some $0 \leq r_1, r_{-1} \leq \ell - 1$.

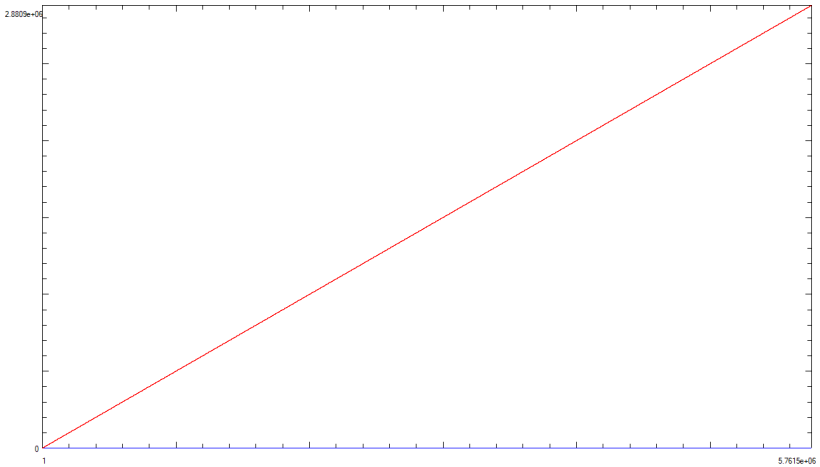
Graphs of elliptic curves LMFDB label 37.b1 (credits to Tighe McAsey) on next slide.

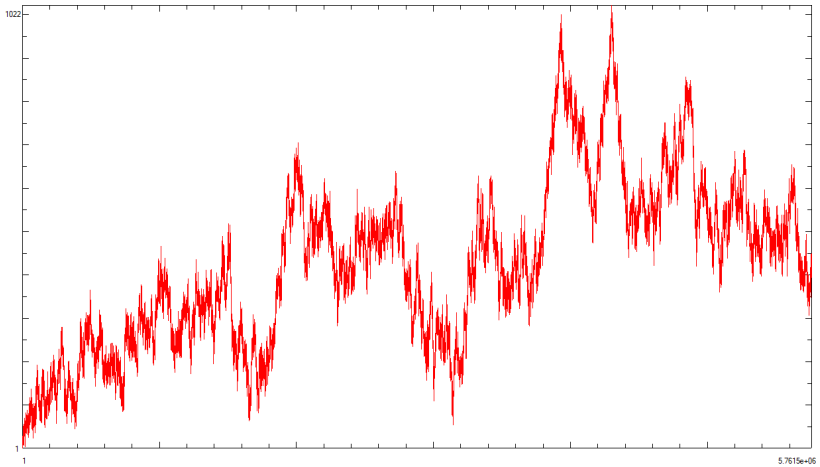
$$change = \begin{cases} +1 & \text{if } a_p \equiv r_1 \pmod{\ell} \\ -1 & \text{if } a_p \equiv r_{-1} \pmod{\ell} \end{cases}$$





LHS: $\ell = 2$, $r_1 = 1$, $r_{-1} = 0$; RHS: ratio





LHS: $\ell = 3$, $r_1 = 0$, $r_{-1} = 1$; RHS $\ell = 3$, $r_1 = 0$, $r_{-1} = 2$

Natural question: Explain the slope of the graph.

Natural question: Explain the slope of the graph.

Fact 1

Let p be a prime of good reduction for $E/\mathbb{Q}$, $\ell \neq p$ be prime and $E[\ell]$ be the ℓ-torsion. We have the representation

$$\overline{\rho}_\ell : \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Then

$$\mathrm{tr}(\overline{\rho}_\ell(\mathrm{Frob}_p)) = a_p(E) \pmod{\ell}$$

where Frob_p is the Frobenius substitution.

Natural question: Explain the slope of the graph.

Fact 1

Let p be a prime of good reduction for $E/\mathbb{Q}$, $\ell \neq p$ be prime and $E[\ell]$ be the ℓ-torsion. We have the representation

$$\overline{\rho}_\ell : \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Then

$$\mathrm{tr}(\overline{\rho}_\ell(\mathrm{Frob}_p)) = a_p(E) \pmod{\ell}$$

where Frob_p is the Frobenius substitution.

Takeaway

By Chebotarev density theorem, the distribution of $a_p(E) \mod \ell$ is governed by the distribution of Frob_p in $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ and the trace map $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \to \mathbb{Z}/\ell\mathbb{Z}$.

mod 2 example

Q: Can we describe $E[\ell]$ and the trace map?

mod 2 example

Q: Can we describe $E[\ell]$ and the trace map? A: Yes if $\ell = 2$.

mod 2 example

Q: Can we describe $E[\ell]$ and the trace map? A: Yes if $\ell = 2$.

Let $E/\mathbb{Q}$ be an elliptic curve in the reduced Weierstrass form

$$y^2 = x^3 + ax + b = f(x),$$

where $a, b \in \mathbb{Q}$, with discriminant $\Delta = -(4a^3 + 27b^2)$ and α_1, α_2 and α_3 be the roots of $f(x)$. Let

$$S_0 = \{p \text{ prime} : a_p(E) \equiv 0 \mod 2\}$$
$$S_1 = \{p \text{ prime} : a_p(E) \equiv 1 \mod 2\}.$$

Let $L = \mathbb{Q}(E[2])$, $G = \mathrm{Gal}(L/\mathbb{Q})$ and δ be any density of set of primes (say natural density).

Case 1: Suppose $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ with $[L : \mathbb{Q}] = 6$. Then $G \cong S_3$. Up to conjugacy, we have

$$\begin{array}{rcl} \mathrm{Gal}(L/\mathbb{Q}) & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{class size} \\ (1)(2)(3) & \longmapsto & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \xrightarrow{\mathrm{tr}} 0 \mod 2 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 1 \\ (12)(3) & \longmapsto & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \xrightarrow{\mathrm{tr}} 0 \mod 2 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 3 \\ (123) & \longmapsto & \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \xrightarrow{\mathrm{tr}} 1 \mod 2 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 2 \end{array}$$

Hence, $\delta(S_0) = \frac{1+3}{6} = \frac{2}{3}$.

Case 2: $f(x)$ splits completely in $\mathbb{Q}$, i.e. $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$. Then $L = \mathbb{Q}$ and G is trivial. Hence, $\delta(S_0) = 1$.

Case 2: $f(x)$ splits completely in $\mathbb{Q}$, i.e. $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$. Then $L = \mathbb{Q}$ and G is trivial. Hence, $\delta(S_0) = 1$.
Case 3: $\alpha_1 \in \mathbb{Q}$ but $\alpha_2, \alpha_3 \notin \mathbb{Q}$. Then $L = \mathbb{Q}(\alpha_2)$ and $G \cong C_2$. Hence, $\delta(S_0) = 1$.

Case 2: $f(x)$ splits completely in $\mathbb{Q}$, i.e. $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$. Then $L = \mathbb{Q}$ and G is trivial. Hence, $\delta(S_0) = 1$.
Case 3: $\alpha_1 \in \mathbb{Q}$ but $\alpha_2, \alpha_3 \notin \mathbb{Q}$. Then $L = \mathbb{Q}(\alpha_2)$ and $G \cong C_2$. Hence, $\delta(S_0) = 1$.
Case 4: Suppose $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ with $[L : \mathbb{Q}] = 3$. Then $G \cong C_3$. Fix a basis $\{P_1, P_2\}$ for $E[2]$ and one can see $P_3 = P_1 + P_2$. We have

$$\begin{aligned} \mathrm{Gal}(L/\mathbb{Q}) &\longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \\ id &\longmapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \xrightarrow{\text{tr}} 0 \mod 2 \\ (123) &\longmapsto \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \xrightarrow{\text{tr}} 1 \mod 2 \\ (132) &\longmapsto \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \xrightarrow{\text{tr}} 1 \mod 2 \end{aligned}$$

Hence, $\delta(S_0) = \frac{1}{3}$.

Theorem 2

Let $E/\mathbb{Q}$ be an elliptic curve in the reduced Weierstrass form

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Q}$, with discriminant $\Delta = -(4a^3 + 27b^2)$. Let $f(x) = x^3 + ax + b$ and α_1, α_2 and α_3 be the roots of $f(x)$. Let $S_0 = \{p \text{ prime} : a_p(E) \equiv 0 \mod 2\}$ and $S_1 = \{p \text{ prime} : a_p(E) \equiv 1 \mod 2\}$. Let δ be any density of set of primes (say natural density). We have the following cases:

1. *If f is reducible over $\mathbb{Q}$, then $\delta(S_0) = 1$ and $\delta(S_1) = 0$.*
2. *If f is irreducible over $\mathbb{Q}$ and $\sqrt{\Delta} \in \mathbb{Q}$, then $\delta(S_0) = 1/3$ and $\delta(S_1) = 2/3$.*
3. *If f is irreducible over $\mathbb{Q}$ and $\sqrt{\Delta} \notin \mathbb{Q}$, then $\delta(S_0) = 2/3$ and $\delta(S_1) = 1/3$.*

Further question to be asked

Classical prime number race: the prime race between 1 mod 4 and 3 mod 4

Further question to be asked

Classical prime number race: the prime race between 1 mod 4 and 3 mod 4

Our question: After suitable weightings, the a_p race between r_1 mod ℓ and r_{-1} mod ℓ.

Warning: In literature, prime race of an elliptic curve refers to the a_p race between positives and negatives.

Framework

Fixing ℓ. The a_p values of an elliptic curve are determined by the Galois representation. We will get to Chebyshev Bias in Galois settings.

Framework

Fixing ℓ. The a_p values of an elliptic curve are determined by the Galois representation. We will get to Chebyshev Bias in Galois settings.

Let L/K be a normal extension of number fields. Let $G = \mathrm{Gal}(L/K)$ be the corresponding Galois group and let C be a conjugacy class of G. Let $\mathfrak{p}$ be a prime of K which is unramified in L. Define the Frobenius substitution attached to $\mathfrak{p}$ be the conjugacy class

$$\mathrm{Frob}_{\mathfrak{p}} = \{\mathrm{Frob}_{\mathfrak{P}} : \mathfrak{P} \text{ lying over } \mathfrak{p}\}.$$

Define the prime counting functions

$$\pi(x; K) = \#\{N\mathfrak{p} \leq x : \mathfrak{p} \text{ (unramified) prime of } K\}$$
$$\pi(x; C) = \#\{N\mathfrak{p} \leq x : \mathrm{Frob}_{\mathfrak{p}} = C \text{ and } \mathfrak{p} \text{ (unramified) prime of } K\}$$

(We follow the treatment in Ng's thesis) Assume GRH throughout.
Notation:

$$E(x; C) := \frac{\log x}{\sqrt{x}} \left(\frac{|G|}{|C|} \pi(x; C) - \pi(x; K) \right)$$

$$\psi(x, \chi) := \sum_{N\mathfrak{p}^m \leq x,\ \mathfrak{p} \text{ unramified}} \chi(\mathrm{Frob}_{\mathfrak{p}}^m) \log(N\mathfrak{p})$$

$$sq^{-1}(C) := \bigcup_{i=1}^{t} C_i, \quad \text{where } C_i^2 \subset C$$

(We follow the treatment in Ng's thesis) Assume GRH throughout.
Notation:

$$E(x; C) := \frac{\log x}{\sqrt{x}} \left(\frac{|G|}{|C|} \pi(x; C) - \pi(x; K) \right)$$

$$\psi(x, \chi) := \sum_{N\mathfrak{p}^m \leq x,\ \mathfrak{p} \text{ unramified}} \chi(\mathrm{Frob}_{\mathfrak{p}}^m) \log(N\mathfrak{p})$$

$$sq^{-1}(C) := \bigcup_{i=1}^{t} C_i, \quad \text{where } C_i^2 \subset C$$

Lemma 3 (Ng, 2000)

$$E(x; C) = \left(1 - \frac{|sq^{-1}(C)|}{|C|}\right) - \sum_{\chi \neq \chi_0} \overline{\chi(C_1)} \frac{\psi(x, \chi)}{\sqrt{x}} + O\left(\frac{1}{x}\right)$$

To race between two conjugacy classes,

$$\begin{aligned} E_{C_1-C_2}(x) :=& E(x; C_1) - E(x; C_2) \\ =& c(C_2) - c(C_1) - \sum_{\chi \neq \chi_0} (\overline{\chi(C_1)} - \overline{\chi(C_2)}) \sum_{0<|\gamma_\chi| \leq X} \frac{x^{i\gamma_\chi}}{\frac{1}{2} + i\gamma_\chi} \\ &+ O\left(\frac{\sqrt{x}\log^2 X}{X} + \frac{1}{\log x}\right) \end{aligned} \tag{1}$$

where $c(C_i) = c_{sq}(C_i) + c_{\frac{1}{2}}(C_i)$ with

$$c_{sq}(C) = -1 + \frac{|sq^{-1}(C)|}{|C|}$$

$$c_{\frac{1}{2}}(C) = 2\sum_{\chi \neq 1} \overline{\chi}(C)\eta_\chi$$

and $\eta_\chi = \mathrm{ord}_{s=\frac{1}{2}} L(s, \chi)$.

To race between two conjugacy classes,

$$\begin{aligned} E_{C_1-C_2}(x) :=& E(x; C_1) - E(x; C_2) \\ =& c(C_2) - c(C_1) - \sum_{\chi \neq \chi_0} (\overline{\chi(C_1)} - \overline{\chi(C_2)}) \sum_{0<|\gamma_\chi| \leq X} \frac{x^{i\gamma_\chi}}{\frac{1}{2} + i\gamma_\chi} \qquad (1) \\ &+ O\left(\frac{\sqrt{x}\log^2 X}{X} + \frac{1}{\log x}\right) \end{aligned}$$

where $c(C_i) = c_{sq}(C_i) + c_{\frac{1}{2}}(C_i)$ with

$$c_{sq}(C) = -1 + \frac{|sq^{-1}(C)|}{|C|}$$

$$c_{\frac{1}{2}}(C) = 2\sum_{\chi \neq 1} \overline{\chi}(C)\eta_\chi$$

and $\eta_\chi = \mathrm{ord}_{s=\frac{1}{2}} L(s, \chi)$.
The term $c(C_i)$ is the bias factor. There is bias factor c_{sq} in classical Chebyshev bias but not $c_{\frac{1}{2}}$.

S_3 Mod 2 Example

We work with the case $\mathrm{Gal}(L/K) = S_3$.
Let $G = \mathrm{Gal}(L/\mathbb{Q}) = S_3$. There are three conjugacy classes in this group, namely

$$C_1 = \{(1)\}, \quad C_2 = \{(12), (13), (23)\}, \quad \text{and} \quad C_3 = \{(123), (132)\}.$$

S_3 Mod 2 Example

We work with the case $\mathrm{Gal}(L/K) = S_3$.
Let $G = \mathrm{Gal}(L/\mathbb{Q}) = S_3$. There are three conjugacy classes in this group, namely

$$C_1 = \{(1)\}, \quad C_2 = \{(12), (13), (23)\}, \quad \text{and} \quad C_3 = \{(123), (132)\}.$$

Straight forward computation:

$$C_1^2 = C_1, \quad C_2^2 = C_1 \quad \text{and} \quad C_3^2 = C_3$$

and hence

$$-1 + \frac{|sq^{-1}(C_1)|}{|C_1|} = 3; \quad -1 + \frac{|sq^{-1}(C_2)|}{|C_2|} = -1,$$
$$-1 + \frac{|sq^{-1}(C_3)|}{|C_3|} = 0$$

This is not quite what we want!

We want to group conjugacy class according to the mod 2 behavior. i.e. want to race $C_1 \cup C_2$ vs C_3 corresponding to 0 vs 1 mod 2.

We want to group conjugacy class according to the mod 2 behavior. i.e. want to race $C_1 \cup C_2$ vs C_3 corresponding to 0 vs 1 mod 2.
We can also calculate the bias terms with union of conjugacy classes. Let $C_{2,0} = C_1 \cup C_2$ and $C_{2,1} = C_3$. Then, one can calculate

$$-1 + \frac{|sq^{-1}(C_{2,0})|}{|C_{2,0}|} = 0, \quad \text{and} \quad -1 + \frac{|sq^{-1}(C_{2,1})|}{|C_{2,1}|} = 0$$

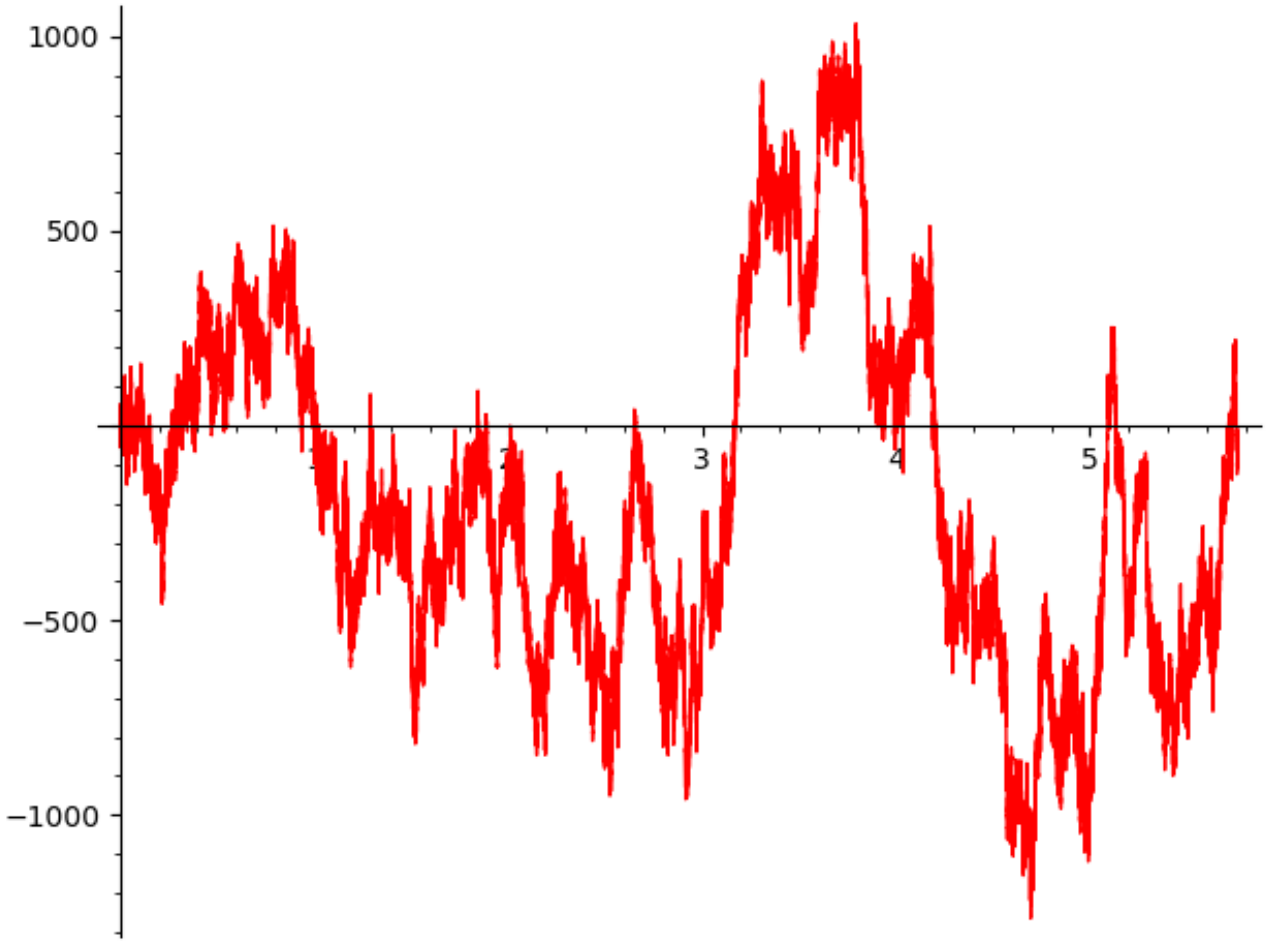
We have no bias coming from the term c_{sq}.

We want to group conjugacy class according to the mod 2 behavior. i.e. want to race $C_1 \cup C_2$ vs C_3 corresponding to 0 vs 1 mod 2.
We can also calculate the bias terms with union of conjugacy classes. Let $C_{2,0} = C_1 \cup C_2$ and $C_{2,1} = C_3$. Then, one can calculate

$$-1 + \frac{|sq^{-1}(C_{2,0})|}{|C_{2,0}|} = 0, \quad \text{and} \quad -1 + \frac{|sq^{-1}(C_{2,1})|}{|C_{2,1}|} = 0$$

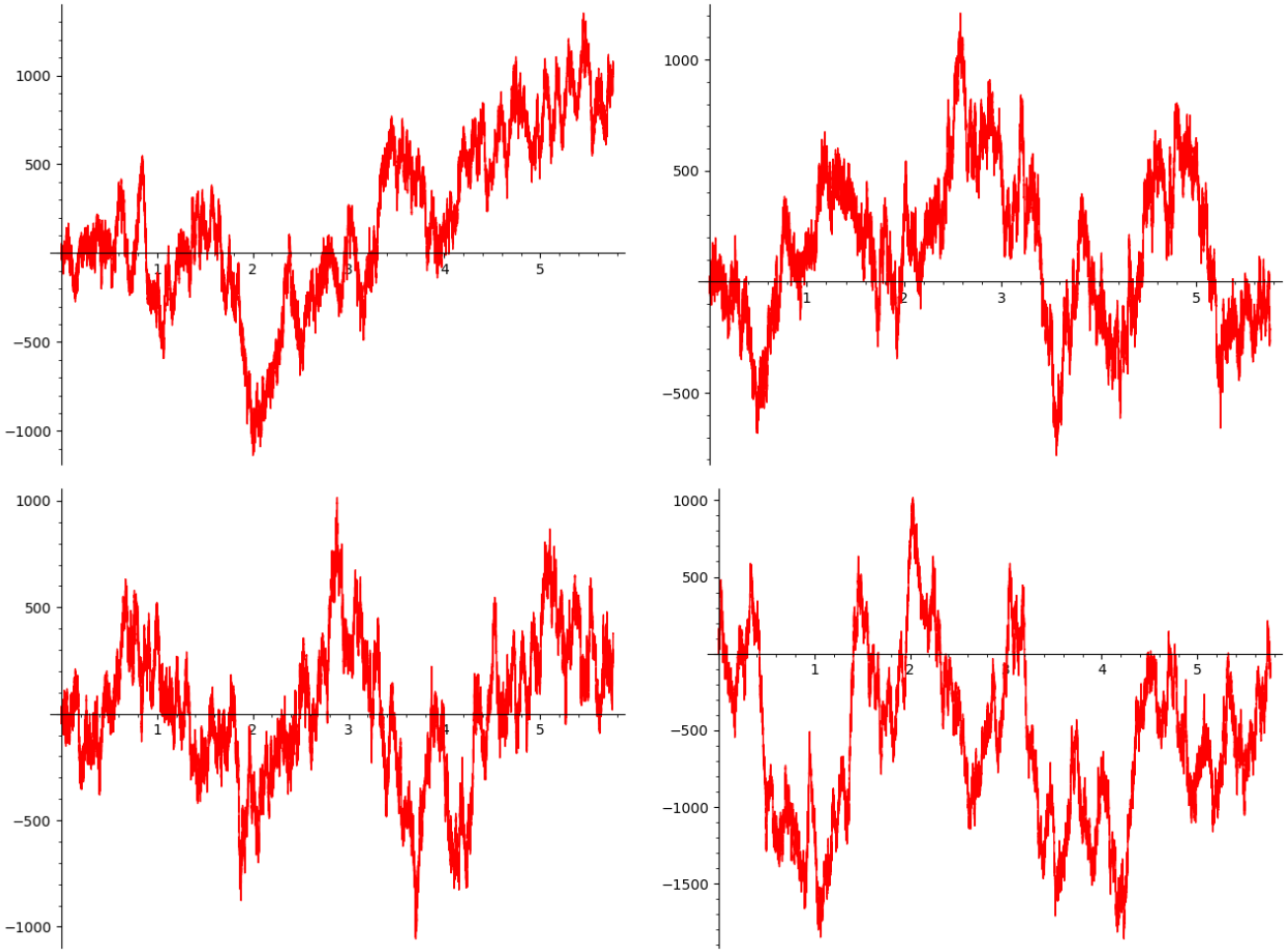
We have no bias coming from the term c_{sq}.
We then have to estimate bias from $c_{\frac{1}{2}}$ term. In S_3, we do not expect there is any bias from $c_{\frac{1}{2}}$.

37.b1 mod 2 race



LMFDB 37.b1; $\ell = 2$, $r_1 = 0$, $r_{-1} = 1$ with suitable weightings.

more mod 2 race



UL: 11.a1, UR: 57.a1, LL: 1862.a1, LR: 19047851.a1;
$\ell = 2$, $r_1 = 0$, $r_{-1} = 1$ with suitable weightings.

Story again

Story begins when we want to find more $G = S_3$ examples. It happens when we plot mod 3 for elliptic curves $E/\mathbb{Q}$, which has torsion subgroup $\mathbb{Z}/3\mathbb{Z}$.

Story again

Story begins when we want to find more $G = S_3$ examples. It happens when we plot mod 3 for elliptic curves $E/\mathbb{Q}$, which has torsion subgroup $\mathbb{Z}/3\mathbb{Z}$.

Not interesting: $a_p \equiv p + 1 \mod 3$. In fact, we will have a plot C_{+1} vs C_{-1}, where

$$C_{+1} := C_1 \cup C_3 = \{(1), (123), (132)\}$$
$$C_{-1} := C_2 = \{(12), (13), (23)\}.$$

Story again

Story begins when we want to find more $G = S_3$ examples. It happens when we plot mod 3 for elliptic curves $E/\mathbb{Q}$, which has torsion subgroup $\mathbb{Z}/3\mathbb{Z}$.
Not interesting: $a_p \equiv p + 1 \mod 3$. In fact, we will have a plot C_{+1} vs C_{-1}, where

$$C_{+1} := C_1 \cup C_3 = \{(1), (123), (132)\}$$
$$C_{-1} := C_2 = \{(12), (13), (23)\}.$$

Question: Is it all such race between C_{+1} vs C_{-1} in S_3 is just prime race?

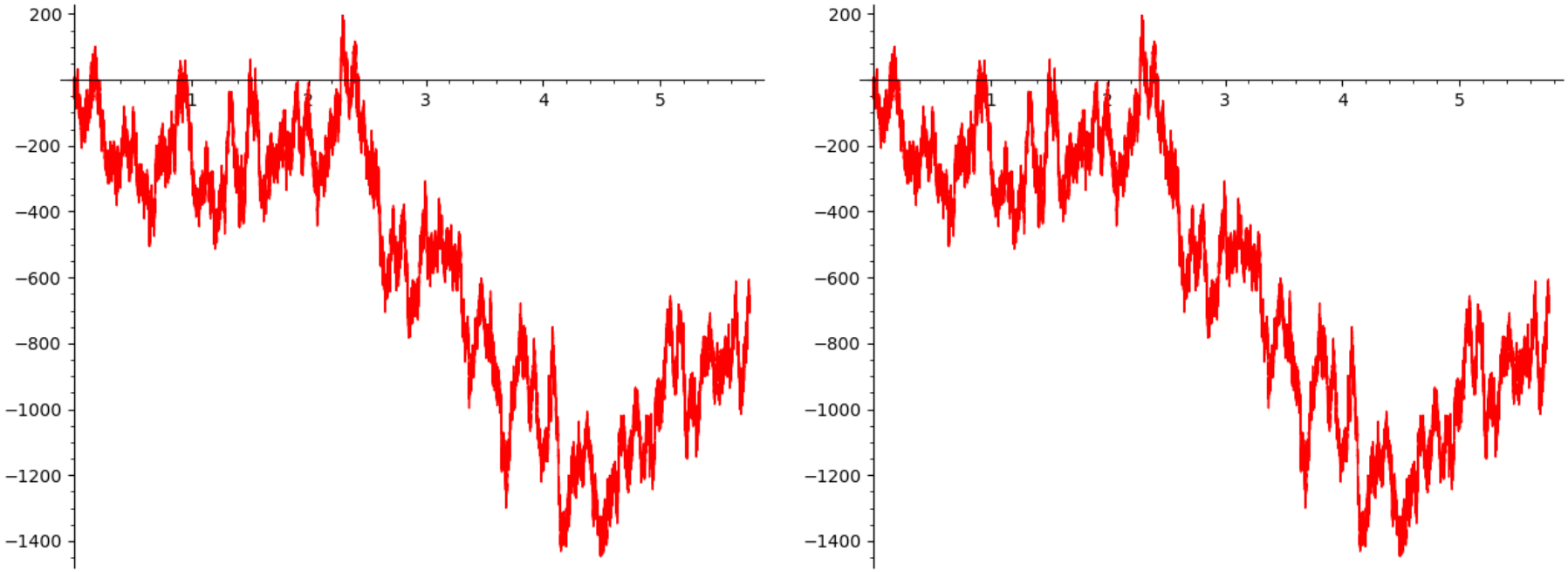
Theorem 4

Let $G = \mathrm{Gal}(L/\mathbb{Q}) = S_3$. Let d be the discriminant of any of the three cubic subfields of L over $\mathbb{Q}$. Denote

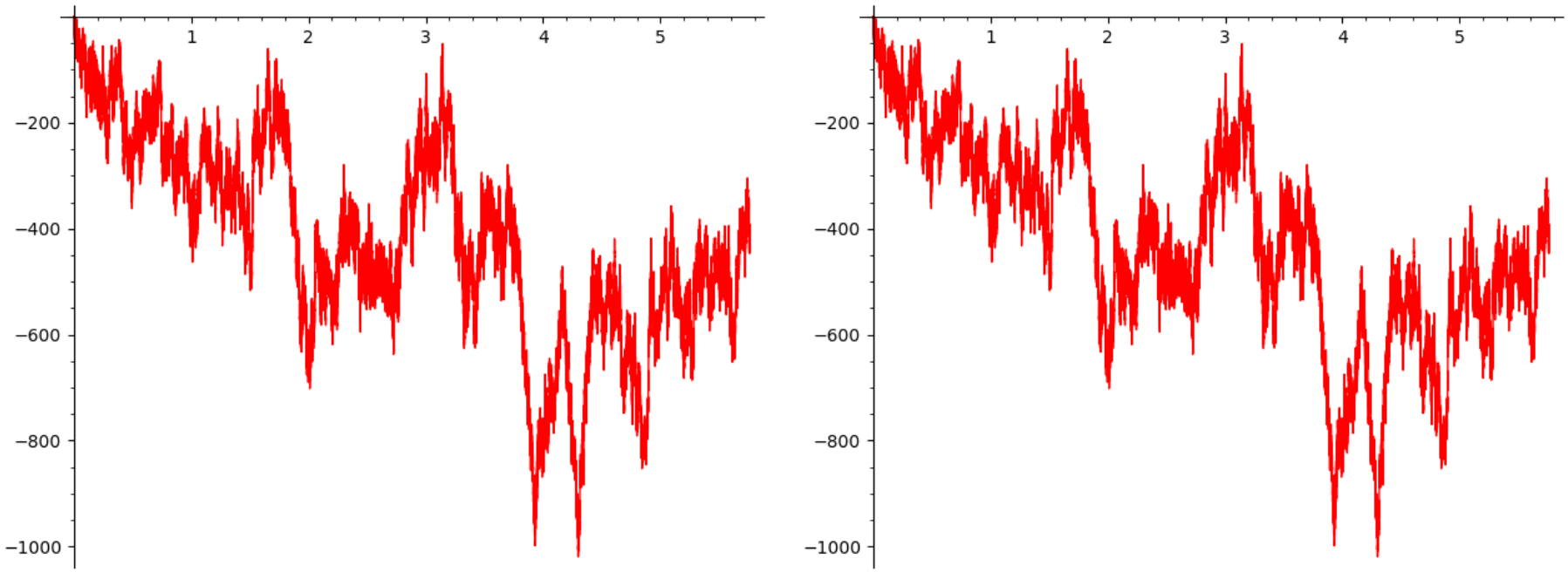
$$C_{+1} := C_1 \cup C_3 = \{(1), (123), (132)\}$$
$$C_{-1} := C_2 = \{(12), (13), (23)\}.$$

the union of conjugacy classes of S_3. The race between C_{+1} vs C_{-1} are equivalent to the prime race between quadratic residue vs quadratic non-residue modulo $|d|$.

plots



LHS: Galois race of defining polynomial $f(x) = x^3 - x^2 + 1$, $D = -23$;
RHS: residue vs non-residue prime mod 23.
They are the same.



LHS: Galois race of defining polynomial $f(x) = x^3 - x^2 - 3x - 3$, $D = -300$;
RHS: residue vs non-residue prime mod 300.
They are the same.

Thank you!