Sums of Euler products and statistics of elliptic curves

Dimitris Koukoulopoulos
(joint work with C. David and E. Smith)

Université de Montréal

Elementary, analytic, and algorithmic number theory :
Research inspired by the mathematics of Carl Pomerance

University of Georgia
June 10, 2015

Basic set-up

Main question: given a prime p, what is the statistical behaviour of the elliptic curves $E/\mathbb{F}_p$?

Basic set-up

Main question: given a prime p, what is the statistical behaviour of the elliptic curves $E/\mathbb{F}_p$?

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

Basic set-up

Main question: given a prime p, what is the statistical behaviour of the elliptic curves $E/\mathbb{F}_p$?

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

Analogous questions when E is fixed and p varies.

Basic set-up

Main question: given a prime p, what is the statistical behaviour of the elliptic curves $E/\mathbb{F}_p$?

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

Analogous questions when E is fixed and p varies.

Advantage when E varies: access to the work of Deuring.

Basic set-up

Main question: given a prime p, what is the statistical behaviour of the elliptic curves $E/\mathbb{F}_p$?

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

Analogous questions when E is fixed and p varies.

Advantage when E varies: access to the work of Deuring.

If $E/\mathbb{F}_p$, then $a_p(E) := p + 1 - \#E(\mathbb{F}_p)$.

Basic set-up

Main question: given a prime p, what is the statistical behaviour of the elliptic curves $E/\mathbb{F}_p$?

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

Analogous questions when E is fixed and p varies.

Advantage when E varies: access to the work of Deuring.

If $E/\mathbb{F}_p$, then $a_p(E) := p + 1 - \#E(\mathbb{F}_p)$.

- $|a_p(E)| < 2\sqrt{p}$

Basic set-up

Main question: given a prime p, what is the statistical behaviour of the elliptic curves $E/\mathbb{F}_p$?

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

Analogous questions when E is fixed and p varies.

Advantage when E varies: access to the work of Deuring.

If $E/\mathbb{F}_p$, then $a_p(E) := p + 1 - \#E(\mathbb{F}_p)$.

- $|a_p(E)| < 2\sqrt{p}$
- $E(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z} \quad$ with $p \equiv 1 \pmod{m}$.

Examples of possible questions

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

Examples of possible questions

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

- $\mathbb{P}(a_p(E) = t)$ for some given $t \in \mathbb{Z}$?

Examples of possible questions

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

- $\mathbb{P}(a_p(E) = t)$ for some given $t \in \mathbb{Z}$?
- $\sum_{p \le x} \mathbb{P}(a_p(E) = t) \sim ?, \quad \mathbb{P}(\alpha \le \frac{a_p(E)}{2\sqrt{p}} \le \beta) \overset{?}{\sim} \frac{2}{\pi} \int_\alpha^\beta \sqrt{1 - u^2} du.$

Examples of possible questions

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

- $\mathbb{P}(a_p(E) = t)$ for some given $t \in \mathbb{Z}$?
- $\sum_{p \leq x} \mathbb{P}(a_p(E) = t) \sim ?, \quad \mathbb{P}(\alpha \leq \frac{a_p(E)}{2\sqrt{p}} \leq \beta) \overset{?}{\sim} \frac{2}{\pi} \int_\alpha^\beta \sqrt{1 - u^2} du.$
- $\mathbb{P}(\#E(\mathbb{F}_p) = \text{prime}) = ?$

Examples of possible questions

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

- $\mathbb{P}(a_p(E) = t)$ for some given $t \in \mathbb{Z}$?
- $\sum_{p \leq x} \mathbb{P}(a_p(E) = t) \sim ?, \quad \mathbb{P}(\alpha \leq \frac{a_p(E)}{2\sqrt{p}} \leq \beta) \overset{?}{\sim} \frac{2}{\pi} \int_\alpha^\beta \sqrt{1 - u^2} du.$
- $\mathbb{P}(\# E(\mathbb{F}_p) = \text{prime}) = ?$
- $\mathbb{P}(E(\mathbb{F}_p) \cong G)$ for some given G? $\mathbb{P}(E(\mathbb{F}_p) = \text{cyclic}) = ?$

Examples of possible questions

$$A \subset \mathcal{C}_p := \left\{ \begin{array}{l} \text{isom. classes} \\ \text{of e.c. over } \mathbb{F}_p \end{array} \right\}, \quad \mathbb{P}(A) := \frac{1}{p} \sum_{E \in A} \frac{1}{|\operatorname{Aut}(E)|} = \frac{|A| + O(1)}{|\mathcal{C}_p|}.$$

- $\mathbb{P}(a_p(E) = t)$ for some given $t \in \mathbb{Z}$?
- $\sum_{p \le x} \mathbb{P}(a_p(E) = t) \sim ?, \quad \mathbb{P}(\alpha \le \frac{a_p(E)}{2\sqrt{p}} \le \beta) \overset{?}{\sim} \frac{2}{\pi} \int_\alpha^\beta \sqrt{1 - u^2} du.$
- $\mathbb{P}(\# E(\mathbb{F}_p) = \text{prime}) = ?$
- $\mathbb{P}(E(\mathbb{F}_p) \cong G)$ for some given G? $\mathbb{P}(E(\mathbb{F}_p) = \text{cyclic}) = ?$
- Dynamics of elliptic curves:

$$\sum_{\substack{p_1, \dots, p_k \le x \\ p_{k+1} = p_1}} \mathbb{P}\left(\# E_j(\mathbb{F}_{p_j}) = p_{j+1} \ (1 \le j \le k) \,\middle|\, E_j \in \mathbb{F}_{p_j} \ (1 \le j \le k) \right) = ?$$

Deuring's theorem and an application

$$D := t^2 - 4p < 0, \quad \mathbb{P}(a_p(E) = t) = \frac{H(D)}{p} := \frac{1}{p} \sum_{d^2 \mid D} \frac{h(D/d^2)}{w(D/d^2)}$$

Deuring's theorem and an application

$$D := t^2 - 4p < 0, \quad \mathbb{P}(a_p(E) = t) = \frac{H(D)}{p} := \frac{1}{p} \sum_{d^2 | D} \frac{h(D/d^2)}{w(D/d^2)}$$

$$\implies \quad \mathbb{P}(a_p(E) = t) = \frac{\sqrt{|D|}}{2\pi} \sum_{\substack{d^2 | D \\ D/d^2 \equiv 0,1 \pmod 4}} \frac{L\left(1, \left(\frac{D/d^2}{\cdot}\right)\right)}{d}$$

Deuring's theorem and an application

$$D := t^2 - 4p < 0, \quad \mathbb{P}(a_p(E) = t) = \frac{H(D)}{p} := \frac{1}{p} \sum_{d^2 \mid D} \frac{h(D/d^2)}{w(D/d^2)}$$

$$\implies \quad \mathbb{P}(a_p(E) = t) = \frac{\sqrt{|D|}}{2\pi} \sum_{\substack{d^2 \mid D \\ D/d^2 \equiv 0,1 \pmod 4}} \frac{L\left(1, \left(\frac{D/d^2}{\cdot}\right)\right)}{d}$$

$$\sum_{p \le x} \mathbb{P}(a_p(E) = t) \sim \sum_{d=1}^{\infty} \frac{1}{2\pi d} \sum_{\substack{p \le x \\ t^2 - 4p \equiv 0, d^2 \pmod{4d^2}}} \frac{L\left(1, \left(\frac{(t^2-4p)/d^2}{\cdot}\right)\right)}{\sqrt{p}}$$

$$\sim \frac{\sqrt{x}}{\log x} \cdot \frac{2}{\pi} \prod_{\ell \mid t} \left(1 - \frac{1}{\ell}\right)^{-1} \prod_{\ell \nmid t} \frac{\ell(\ell^2 - \ell - 1)}{(\ell - 1)(\ell^2 - 1)}.$$

Equidistribution of Frobenius

Let $(N, p) = 1$ and $E/\mathbb{F}_p$. Then

$$E[N] \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

Equidistribution of Frobenius

Let $(N, p) = 1$ and $E/\mathbb{F}_p$. Then

$$E[N] \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

Choosing a basis for $E[N]$, the action of $\mathrm{Frob}_p(E)$ is given by a matrix $F_E \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with

$$\det(F_E) \equiv p \pmod{N}, \quad \mathrm{tr}(F_E) \equiv a_p(E) \pmod{N}.$$

Equidistribution of Frobenius

Let $(N, p) = 1$ and $E/\mathbb{F}_p$. Then

$$E[N] \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

Choosing a basis for $E[N]$, the action of $\mathrm{Frob}_p(E)$ is given by a matrix $F_E \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with

$$\det(F_E) \equiv p \pmod N, \quad \mathrm{tr}(F_E) \equiv a_p(E) \pmod N.$$

Writing $\mathrm{GL}_2^{(p)}(\mathbb{Z}/N\mathbb{Z}) = \{\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \det(\sigma) \equiv p \,(\mathrm{mod}\, N)\}$,

Theorem (Castryck-Huberts)

Let $(N, p) = 1$. For any conjugacy class $\mathcal{F}$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with determinant p, we have

$$\left| \mathbb{P}(F_E \in \mathcal{F}) - \frac{\#\mathcal{F}}{\#\,\mathrm{GL}_2^{(p)}(\mathbb{Z}/N\mathbb{Z})} \right| \ll \frac{N^2 \log\log N}{\sqrt{p}}.$$

Equidistribution of Frobenius

Let $(N, p) = 1$ and $E/\mathbb{F}_p$. Then

$$E[N] \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

Choosing a basis for $E[N]$, the action of $\mathrm{Frob}_p(E)$ is given by a matrix $F_E \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with

$$\det(F_E) \equiv p \pmod N, \quad \mathrm{tr}(F_E) \equiv a_p(E) \pmod N.$$

Writing $\mathrm{GL}_2^{(p)}(\mathbb{Z}/N\mathbb{Z}) = \{\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \det(\sigma) \equiv p \pmod N\}$,

Theorem (Castryck-Huberts)

Let $(N, p) = 1$. For any conjugacy class $\mathcal{F}$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with determinant p, we have

$$\left| \mathbb{P}(F_E \in \mathcal{F}) - \frac{\#\mathcal{F}}{\#\,\mathrm{GL}_2^{(p)}(\mathbb{Z}/N\mathbb{Z})} \right| \ll \frac{N^2 \log\log N}{\sqrt{p}}.$$

(Cebotarev on the modular covering $X(p^2; \zeta_N) \to X(1; 1)$. Similar result by Achter via the Katz-Sarnak equidistribution theorem.)

Probabilistic interpretations of Euler products

If $p > N^{4+\epsilon}$, then the Castryck-Hubert result implies

$$\frac{\mathbb{P}(a_p(E) = t \pmod{N})}{1/N} \sim \prod_{\ell^r \| N} \frac{\ell^r \cdot \#\{\sigma \in \mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z}) : \mathrm{tr}(\sigma) \equiv t \pmod{\ell^r}\}}{|\,\mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z})|}$$

Probabilistic interpretations of Euler products

If $p > N^{4+\epsilon}$, then the Castryck-Hubert result implies

$$\frac{\mathbb{P}(a_p(E) = t \pmod N)}{1/N} \sim \prod_{\ell^r \| N} \frac{\ell^r \cdot \#\{\sigma \in \mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z}) : \mathrm{tr}(\sigma) \equiv t \pmod{\ell^r}\}}{|\,\mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z})|}$$

Similarly, a direct computation reveals that the result of Fouvry-Murty and David-Papallardi can be rewritten as

$$\sum_{p \le x} \mathbb{P}(a_p(E) = t) \sim \frac{\sqrt{x}}{\log x} \cdot \frac{2}{\pi} \prod_{\ell} \frac{\ell \cdot \#\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(\sigma) \equiv t \pmod{\ell}\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}.$$

Probabilistic interpretations of Euler products

If $p > N^{4+\epsilon}$, then the Castryck-Hubert result implies

$$\frac{\mathbb{P}(a_p(E) = t \,(\mathrm{mod}\, N))}{1/N} \sim \prod_{\ell^r \| N} \frac{\ell^r \cdot \#\{\sigma \in \mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z}) : \mathrm{tr}(\sigma) \equiv t \,(\mathrm{mod}\, \ell^r)\}}{|\,\mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z})|}$$

Similarly, a direct computation reveals that the result of Fouvry-Murty and David-Papallardi can be rewritten as

$$\sum_{p \le x} \mathbb{P}(a_p(E) = t) \sim \frac{\sqrt{x}}{\log x} \cdot \frac{2}{\pi} \prod_{\ell} \frac{\ell \cdot \#\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(\sigma) \equiv t \,(\mathrm{mod}\, \ell)\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}.$$

Gekeler showed the following remarkable identity:

$$\mathbb{P}(a_p(E) = t) = f_\infty(t, p) \prod_{\ell} f_\ell(t, p), \quad f_\infty(t, p) = \frac{\sqrt{1 - (\frac{t}{2\sqrt{p}})^2}}{\pi\sqrt{p}},$$

$$f_\ell(t, p) = \lim_{r \to \infty} \ell^r \cdot \frac{\#\{\sigma \in \mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z}) : \mathrm{tr}(\sigma) \equiv t \,(\mathrm{mod}\, \ell^r)\}}{|\,\mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z})|} \quad (\ell \neq p).$$

Average Lang-Trotter, revisited

$$\sum_{p \le x} \mathbb{P}(a_p(E) = t) = \sum_{p \le x} f_\infty(t,p) \prod_\ell f_\ell(t,p) = W \cdot \mathbb{E}_{p \le x}\left[\prod_\ell f_\ell(t,p)\right],$$

Average Lang-Trotter, revisited

$$\sum_{p\le x}\mathbb{P}(a_p(E)=t)=\sum_{p\le x}f_\infty(t,p)\prod_\ell f_\ell(t,p)=W\cdot\mathbb{E}_{p\le x}\left[\prod_\ell f_\ell(t,p)\right],$$

where $w_p=f_\infty(t,p)\sim\frac{1}{\pi\sqrt{p}}$, $W=\sum_{p\le x}w_p\sim\frac{2\sqrt{x}}{\pi\log x}$, and

$$\mathbb{E}_{p\le x}[g(p)]=\frac{1}{W}\sum_{p\le x}w_p g(p).$$

Average Lang-Trotter, revisited

$$\sum_{p \le x} \mathbb{P}(a_p(E) = t) = \sum_{p \le x} f_\infty(t,p) \prod_\ell f_\ell(t,p) = W \cdot \mathbb{E}_{p \le x} \left[\prod_\ell f_\ell(t,p) \right],$$

where $w_p = f_\infty(t,p) \sim \frac{1}{\pi\sqrt{p}}$, $W = \sum_{p \le x} w_p \sim \frac{2\sqrt{x}}{\pi \log x}$, and

$$\mathbb{E}_{p \le x}[g(p)] = \frac{1}{W} \sum_{p \le x} w_p g(p).$$

$$f_\ell(t,p) = \lim_{r \to \infty} F_{\ell^r}(t,p), \quad F_{\ell^r}(t,p) = \frac{\#\left\{ \begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \det(\sigma) \equiv p \pmod{\ell^r} \\ \mathrm{tr}(\sigma) \equiv t \pmod{\ell^r} \end{array} \right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|/\phi(\ell^{2r})},$$

for $\ell \ne p$, and F_{ℓ^r} depends only on $t, p \pmod{\ell^r}$.

Average Lang-Trotter, revisited

$$\sum_{p\le x}\mathbb{P}(a_p(E)=t)=\sum_{p\le x} f_\infty(t,p)\prod_\ell f_\ell(t,p)=W\cdot\mathbb{E}_{p\le x}\left[\prod_\ell f_\ell(t,p)\right],$$

where $w_p=f_\infty(t,p)\sim\frac{1}{\pi\sqrt{p}}$, $W=\sum_{p\le x} w_p\sim\frac{2\sqrt{x}}{\pi\log x}$, and

$$\mathbb{E}_{p\le x}[g(p)]=\frac{1}{W}\sum_{p\le x} w_p g(p).$$

$$f_\ell(t,p)=\lim_{r\to\infty}F_{\ell^r}(t,p),\qquad F_{\ell^r}(t,p)=\frac{\#\left\{\begin{array}{l}\sigma\in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})\\ \det(\sigma)\equiv p \pmod{\ell^r}\\ \mathrm{tr}(\sigma)\equiv t\pmod{\ell^r}\end{array}\right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|/\phi(\ell^{2r})},$$

for $\ell\neq p$, and F_{ℓ^r} depends only on $t,p \pmod{\ell^r}$.

$$\implies\quad \sum_{p\le x}\mathbb{P}(a_p(E)=t)\overset{\mathrm{CRT}}{\sim} W\cdot\prod_\ell\mathbb{E}_{p\le x}[f_\ell(t,p)].$$

$$f_\ell(t,p) = \lim_{r\to\infty} F_{\ell^r}(t,p), \quad F_{\ell^r}(t,p) = \frac{\#\left\{\begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \det(\sigma) \equiv p \pmod{\ell^r} \\ \mathrm{tr}(\sigma) \equiv t \pmod{\ell^r} \end{array}\right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|/\phi(\ell^{2r})} \ (\ell \neq p)$$

$$f_\ell(t,p) = \lim_{r\to\infty} F_{\ell^r}(t,p), \quad F_{\ell^r}(t,p) = \frac{\#\left\{\begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \det(\sigma) \equiv p \pmod{\ell^r} \\ \mathrm{tr}(\sigma) \equiv t \pmod{\ell^r} \end{array}\right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|/\phi(\ell^{2r})} \;\; (\ell \neq p)$$

$$\begin{aligned}
\mathbb{E}_{p\le x}[f_\ell(t,p)] &= \lim_{r\to\infty} \mathbb{E}_{p\le x}[F_{\ell^r}(t,p)] \\
&= \lim_{r\to\infty} \frac{\phi(\ell^r)\ell^r}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|} \sum_{\substack{\sigma\in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \mathrm{tr}(\sigma)\equiv t \pmod{\ell^r}}} \mathbb{P}_{p\le x}(p \equiv \det(\sigma) \pmod{\ell^r})) \\
&\overset{\mathrm{PNT}}{\sim} \lim_{r\to\infty} \frac{\ell^r \cdot \#\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \mathrm{tr}(\sigma) \equiv t \pmod{\ell^r})\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}.
\end{aligned}$$

$$f_\ell(t,p) = \lim_{r\to\infty} F_{\ell^r}(t,p), \quad F_{\ell^r}(t,p) = \frac{\#\left\{\begin{array}{l}\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \det(\sigma) \equiv p \pmod{\ell^r} \\ \mathrm{tr}(\sigma) \equiv t \pmod{\ell^r}\end{array}\right\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|/\phi(\ell^{2r})} \ (\ell \neq p)$$

$$\begin{aligned}\mathbb{E}_{p\le x}[f_\ell(t,p)] &= \lim_{r\to\infty} \mathbb{E}_{p\le x}[F_{\ell^r}(t,p)] \\ &= \lim_{r\to\infty} \frac{\phi(\ell^r)\ell^r}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|} \sum_{\substack{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \mathrm{tr}(\sigma)\equiv t \pmod{\ell^r}}} \mathbb{P}_{p\le x}(p \equiv \det(\sigma) \pmod{\ell^r})) \\ &\overset{\mathrm{PNT}}{\sim} \lim_{r\to\infty} \frac{\ell^r \cdot \#\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \mathrm{tr}(\sigma) \equiv t \pmod{\ell^r})\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}.\end{aligned}$$

$$\implies \quad \sum_{p\le x} \mathbb{P}(a_p(E) = t) \sim \frac{\sqrt{x}}{\log x} \cdot \frac{2}{\pi} \prod_\ell \frac{\ell \cdot \#\left\{\begin{array}{l}\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \\ \mathrm{tr}(\sigma) \equiv t \pmod{\ell}\end{array}\right\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}.$$

Justification of steps

$$f_\ell(t,p) = 1 + \left(\frac{t^2 - 4p}{\ell}\right) + O\left(\frac{1}{\ell^2}\right) \quad (\ell \nmid t^2 - 4p)$$

Justification of steps

$$f_\ell(t,p) = 1 + \left(\frac{t^2-4p}{\ell}\right) + O\left(\frac{1}{\ell^2}\right) \qquad (\ell \nmid t^2-4p)$$

$$\overset{\text{zero-density}}{\Longrightarrow} \qquad \prod_{\ell} f_\ell(t,p) \sim \prod_{\ell \le (\log x)^A} f_\ell(t,p) \quad \text{for all but } x^\epsilon \text{ primes } p \le x$$

Justification of steps

$$f_\ell(t,p) = 1 + \left(\frac{t^2-4p}{\ell}\right) + O\left(\frac{1}{\ell^2}\right) \quad (\ell \nmid t^2-4p)$$

$$\overset{\text{zero-density}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \prod_{\ell \le (\log x)^A} f_\ell(t,p) \quad \text{for all but } x^\epsilon \text{ primes } p \le x$$

$$\overset{\text{smooths are sparse}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \sum_{\substack{P^+(n) \le (\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\delta_n(p) \quad \text{for most } p \le x,$$

where $\delta_n(p) = \prod_{\ell | n}(f_\ell(t,p) - 1)$.

Justification of steps

$$f_\ell(t,p) = 1 + \left(\frac{t^2-4p}{\ell}\right) + O\left(\frac{1}{\ell^2}\right) \quad (\ell \nmid t^2-4p)$$

$$\overset{\text{zero-density}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \prod_{\ell \le (\log x)^A} f_\ell(t,p) \quad \text{for all but } x^\epsilon \text{ primes } p \le x$$

$$\overset{\text{smooths are sparse}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \sum_{\substack{P^+(n) \le (\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\delta_n(p) \quad \text{for most } p \le x,$$

where $\delta_n(p) = \prod_{\ell | n}(f_\ell(t,p) - 1)$.

$$\Longrightarrow \quad \mathbb{E}_{p\le x}\left[\prod_{\ell} f_\ell(t,p)\right] \sim \sum_{\substack{P^+(n) \le (\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\mathbb{E}_{p\le x}\left[\delta_n(t,p)\right].$$

Justification of steps

$$f_\ell(t,p) = 1 + \left(\frac{t^2-4p}{\ell}\right) + O\left(\frac{1}{\ell^2}\right) \quad (\ell \nmid t^2-4p)$$

$$\overset{\text{zero-density}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \prod_{\ell \le (\log x)^A} f_\ell(t,p) \quad \text{for all but } x^\epsilon \text{ primes } p \le x$$

$$\overset{\text{smooths are sparse}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \sum_{\substack{P^+(n) \le (\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\delta_n(p) \quad \text{for most } p \le x,$$

where $\delta_n(p) = \prod_{\ell \mid n}(f_\ell(t,p)-1)$.

$$\Longrightarrow \quad \mathbb{E}_{p\le x}\left[\prod_{\ell} f_\ell(t,p)\right] \sim \sum_{\substack{P^+(n) \le (\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\mathbb{E}_{p\le x}\left[\delta_n(t,p)\right].$$

$f_\ell(t,p) = F_{\ell^r}(t,p)$ if $r > \nu_\ell(t^2-4p)$, where $F_{\ell^r}(t,\cdot)$ is ℓ^r-periodic.

Justification of steps

$$f_\ell(t,p) = 1 + \left(\frac{t^2-4p}{\ell}\right) + O\left(\frac{1}{\ell^2}\right) \quad (\ell \nmid t^2-4p)$$

$$\overset{\text{zero-density}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \prod_{\ell \le (\log x)^A} f_\ell(t,p) \quad \text{for all but } x^\epsilon \text{ primes } p \le x$$

$$\overset{\text{smooths are sparse}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \sum_{\substack{P^+(n) \le (\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\delta_n(p) \quad \text{for most } p \le x,$$

where $\delta_n(p) = \prod_{\ell | n}(f_\ell(t,p) - 1)$.

$$\Longrightarrow \quad \mathbb{E}_{p \le x}\left[\prod_{\ell} f_\ell(t,p)\right] \sim \sum_{\substack{P^+(n) \le (\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\mathbb{E}_{p \le x}\left[\delta_n(t,p)\right].$$

$f_\ell(t,p) = F_{\ell^r}(t,p)$ if $r > \nu_\ell(t^2-4p)$, where $F_{\ell^r}(t,\cdot)$ is ℓ^r-periodic. So $a \to \delta_n(a)$ is q-periodic, where $q = \prod_{\ell | n} \ell^{e_\ell}$, if $t^2 - 4a \not\equiv 0 \pmod{\ell^{e_\ell}}$.

Justification of steps

$$f_\ell(t,p) = 1 + \left(\frac{t^2-4p}{\ell}\right) + O\left(\frac{1}{\ell^2}\right) \quad (\ell \nmid t^2-4p)$$

$$\overset{\text{zero-density}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \prod_{\ell \le (\log x)^A} f_\ell(t,p) \quad \text{for all but } x^\epsilon \text{ primes } p \le x$$

$$\overset{\text{smooths are sparse}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \sum_{\substack{P^+(n)\le(\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\delta_n(p) \quad \text{for most } p \le x,$$

where $\delta_n(p) = \prod_{\ell|n}(f_\ell(t,p)-1)$.

$$\Longrightarrow \quad \mathbb{E}_{p\le x}\left[\prod_{\ell} f_\ell(t,p)\right] \sim \sum_{\substack{P^+(n)\le(\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\mathbb{E}_{p\le x}\left[\delta_n(t,p)\right].$$

$f_\ell(t,p) = F_{\ell^r}(t,p)$ if $r > \nu_\ell(t^2-4p)$, where $F_{\ell^r}(t,\cdot)$ is ℓ^r-periodic. So $a \to \delta_n(a)$ is q-periodic, where $q = \prod_{\ell|n} \ell^{e_\ell}$, if $t^2 - 4a \not\equiv 0 \pmod{\ell^{e_\ell}}$.

Usually, $\nu_\ell(t^2-4p)$ is small, so q is of comparable size with n (maybe $n^{O(1)}$)

Justification of steps

$$f_\ell(t,p) = 1 + \left(\frac{t^2-4p}{\ell}\right) + O\left(\frac{1}{\ell^2}\right) \quad (\ell \nmid t^2-4p)$$

$$\overset{\text{zero-density}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \prod_{\ell \le (\log x)^A} f_\ell(t,p) \quad \text{for all but } x^\epsilon \text{ primes } p \le x$$

$$\overset{\text{smooths are sparse}}{\Longrightarrow} \quad \prod_{\ell} f_\ell(t,p) \sim \sum_{\substack{P^+(n) \le (\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\delta_n(p) \quad \text{for most } p \le x,$$

where $\delta_n(p) = \prod_{\ell | n}(f_\ell(t,p) - 1)$.

$$\Longrightarrow \quad \mathbb{E}_{p \le x}\left[\prod_{\ell} f_\ell(t,p)\right] \sim \sum_{\substack{P^+(n) \le (\log x)^A \\ n \le x^\epsilon}} \mu^2(n)\mathbb{E}_{p \le x}\left[\delta_n(t,p)\right].$$

$f_\ell(t,p) = F_{\ell^r}(t,p)$ if $r > \nu_\ell(t^2-4p)$, where $F_{\ell^r}(t,\cdot)$ is ℓ^r-periodic. So $a \to \delta_n(a)$ is q-periodic, where $q = \prod_{\ell | n} \ell^{e_\ell}$, if $t^2 - 4a \not\equiv 0 \pmod{\ell^{e_\ell}}$.

Usually, $\nu_\ell(t^2-4p)$ is small, so q is of comparable size with n (maybe $n^{O(1)}$) $\Longrightarrow$ need info on primes in APs of size $x^{O(\epsilon)}$.

Sums of Euler products : axiomatic framework

$$S := \sum_{\boldsymbol{a} \in \mathcal{A}} w_{\boldsymbol{a}} \prod_{\ell} (1 + \delta_{\ell}(\boldsymbol{a})),$$

Sums of Euler products : axiomatic framework

$$S := \sum_{\boldsymbol{a} \in \mathcal{A}} w_{\boldsymbol{a}} \prod_{\ell} (1 + \delta_\ell(\boldsymbol{a})),$$

$\mathcal{A} \subset \mathbb{Z}^d \cap [-X, X]^d$ living in sets $\mathcal{G}(q) \subset (\mathbb{Z}/q\mathbb{Z})^d$ satisfying CRT

Sums of Euler products : axiomatic framework

$$S := \sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} \prod_{\ell} (1 + \delta_\ell(\boldsymbol{a})),$$

$\mathcal{A} \subset \mathbb{Z}^d \cap [-X, X]^d$ living in sets $\mathcal{G}(q) \subset (\mathbb{Z}/q\mathbb{Z})^d$ satisfying CRT

Assume $\mathcal{A}$ is well-distributed among members of $\mathcal{G}(q)$, $q \leq X^\epsilon$,

Sums of Euler products : axiomatic framework

$$S := \sum_{\boldsymbol{a} \in \mathcal{A}} w_{\boldsymbol{a}} \prod_{\ell} (1 + \delta_\ell(\boldsymbol{a})),$$

$\mathcal{A} \subset \mathbb{Z}^d \cap [-X, X]^d$ living in sets $\mathcal{G}(q) \subset (\mathbb{Z}/q\mathbb{Z})^d$ satisfying CRT

Assume $\mathcal{A}$ is well-distributed among members of $\mathcal{G}(q)$, $q \leq X^\epsilon$,

$$\delta_\ell(\boldsymbol{a}) = \Delta_{\ell^r}(\boldsymbol{a}) \quad (r > \nu_\ell(P(\boldsymbol{a}))),$$

where Δ_{ℓ^r} is ℓ^r-periodic and $P \in \mathbb{Z}[x_1, \ldots, x_d]$,

Sums of Euler products : axiomatic framework

$$S := \sum_{\boldsymbol{a} \in \mathcal{A}} w_{\boldsymbol{a}} \prod_{\ell} (1 + \delta_\ell(\boldsymbol{a})),$$

$\mathcal{A} \subset \mathbb{Z}^d \cap [-X, X]^d$ living in sets $\mathcal{G}(q) \subset (\mathbb{Z}/q\mathbb{Z})^d$ satisfying CRT

Assume $\mathcal{A}$ is well-distributed among members of $\mathcal{G}(q)$, $q \leq X^\epsilon$,

$$\delta_\ell(\boldsymbol{a}) = \Delta_{\ell^r}(\boldsymbol{a}) \quad (r > \nu_\ell(P(\boldsymbol{a}))),$$

where Δ_{ℓ^r} is ℓ^r-periodic and $P \in \mathbb{Z}[x_1, \ldots, x_d]$,

$$\Delta_\ell := \lim_{r \to \infty} \frac{1}{|\mathcal{G}(\ell^r)|} \sum_{\boldsymbol{a} \in \mathcal{G}(\ell^r)} \Delta_{\ell^r}(\boldsymbol{a}) \quad \text{exists},$$

Sums of Euler products : axiomatic framework

$$S := \sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} \prod_{\ell} (1+\delta_\ell(\boldsymbol{a})),$$

$\mathcal{A} \subset \mathbb{Z}^d \cap [-X, X]^d$ living in sets $\mathcal{G}(q) \subset (\mathbb{Z}/q\mathbb{Z})^d$ satisfying CRT

Assume $\mathcal{A}$ is well-distributed among members of $\mathcal{G}(q)$, $q \leq X^\epsilon$,

$$\delta_\ell(\boldsymbol{a}) = \Delta_{\ell^r}(\boldsymbol{a}) \quad (r > \nu_\ell(P(\boldsymbol{a}))),$$

where Δ_{ℓ^r} is ℓ^r-periodic and $P \in \mathbb{Z}[x_1, \ldots, x_d]$,

$$\Delta_\ell := \lim_{r\to\infty} \frac{1}{|\mathcal{G}(\ell^r)|} \sum_{\boldsymbol{a}\in\mathcal{G}(\ell^r)} \Delta_{\ell^r}(\boldsymbol{a}) \quad \text{exists,}$$

$$\delta_\ell(\boldsymbol{a}) = \lambda_1\left(\frac{D_1(\boldsymbol{a})}{\ell}\right) + \cdots + \lambda_k\left(\frac{D_k(\boldsymbol{a})}{\ell}\right) + O\left(\frac{1}{\ell^2}\right)$$

if $\ell \nmid B_{\boldsymbol{a}} \leq e^{(\log X)^2}$, where $D_1, \ldots, D_k \in \mathbb{Z}[x_1, \ldots, x_d]$ of height $X^{O(1)}$.

Sums of Euler products : axiomatic framework

$$S := \sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} \prod_{\ell}(1+\delta_\ell(\boldsymbol{a})),$$

$\mathcal{A} \subset \mathbb{Z}^d \cap [-X, X]^d$ living in sets $\mathcal{G}(q) \subset (\mathbb{Z}/q\mathbb{Z})^d$ satisfying CRT

Assume $\mathcal{A}$ is well-distributed among members of $\mathcal{G}(q)$, $q \leq X^\epsilon$,

$$\delta_\ell(\boldsymbol{a}) = \Delta_{\ell^r}(\boldsymbol{a}) \quad (r > \nu_\ell(P(\boldsymbol{a}))),$$

where Δ_{ℓ^r} is ℓ^r-periodic and $P \in \mathbb{Z}[x_1, \dots, x_d]$,

$$\Delta_\ell := \lim_{r\to\infty} \frac{1}{|\mathcal{G}(\ell^r)|} \sum_{\boldsymbol{a}\in\mathcal{G}(\ell^r)} \Delta_{\ell^r}(\boldsymbol{a}) \quad \text{exists},$$

$$\delta_\ell(\boldsymbol{a}) = \lambda_1\left(\frac{D_1(\boldsymbol{a})}{\ell}\right) + \cdots + \lambda_k\left(\frac{D_k(\boldsymbol{a})}{\ell}\right) + O\left(\frac{1}{\ell^2}\right)$$

if $\ell \nmid B_{\boldsymbol{a}} \leq e^{(\log X)^2}$, where $D_1, \dots, D_k \in \mathbb{Z}[x_1, \dots, x_d]$ of height $X^{O(1)}$.

$$\text{Then} \quad S \sim W \prod_{\ell}(1+\Delta_\ell), \quad \text{where} \quad W = \sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}}.$$

1st application : Sato-Tate for short intervals

$$S = \mathbb{P}\left(\alpha \leq \frac{a_p(E)}{2\sqrt{p}} \leq \beta\right) \sim \frac{2}{\pi}\int_\alpha^\beta \sqrt{1-u^2}du \quad (\beta - \alpha > p^{-1/2+\epsilon})$$

1st application : Sato-Tate for short intervals

$$S = \mathbb{P}\left(\alpha \leq \frac{a_p(E)}{2\sqrt{p}} \leq \beta\right) \sim \frac{2}{\pi}\int_{\alpha}^{\beta}\sqrt{1-u^2}du \quad (\beta - \alpha > p^{-1/2+\epsilon})$$

$$S = \sum_{2\alpha\sqrt{p}\leq t\leq 2\beta\sqrt{p}} \mathbb{P}(a_p(E) = t) = \sum_{2\alpha\sqrt{p}\leq t\leq 2\beta\sqrt{p}} f_{\infty}(t,p)\prod_{\ell} f_{\ell}(t,p).$$

1st application : Sato-Tate for short intervals

$$S = \mathbb{P}\left(\alpha \le \frac{a_p(E)}{2\sqrt{p}} \le \beta\right) \sim \frac{2}{\pi}\int_\alpha^\beta \sqrt{1-u^2}du \quad (\beta - \alpha > p^{-1/2+\epsilon})$$

$$S = \sum_{2\alpha\sqrt{p}\le t\le 2\beta\sqrt{p}} \mathbb{P}(a_p(E) = t) = \sum_{2\alpha\sqrt{p}\le t\le 2\beta\sqrt{p}} f_\infty(t,p)\prod_\ell f_\ell(t,p).$$

Proof: write $S = \sum_{a\in\mathcal{A}} w_a \prod_\ell (1+\delta_\ell(a))$ with

$$\mathcal{A} = [2\alpha\sqrt{p}, 2\beta\sqrt{p}] \cap \mathbb{Z}, \quad w_a = f_\infty(a,p), \quad \mathcal{G}(q) = \mathbb{Z}/q\mathbb{Z},$$

1st application : Sato-Tate for short intervals

$$S = \mathbb{P}\left(\alpha \leq \frac{a_p(E)}{2\sqrt{p}} \leq \beta\right) \sim \frac{2}{\pi}\int_\alpha^\beta \sqrt{1-u^2}du \quad (\beta - \alpha > p^{-1/2+\epsilon})$$

$$S = \sum_{2\alpha\sqrt{p} \leq t \leq 2\beta\sqrt{p}} \mathbb{P}(a_p(E) = t) = \sum_{2\alpha\sqrt{p} \leq t \leq 2\beta\sqrt{p}} f_\infty(t,p) \prod_\ell f_\ell(t,p).$$

Proof: write $S = \sum_{a \in \mathcal{A}} w_a \prod_\ell (1 + \delta_\ell(a))$ with

$$\mathcal{A} = [2\alpha\sqrt{p}, 2\beta\sqrt{p}] \cap \mathbb{Z}, \quad w_a = f_\infty(a,p), \quad \mathcal{G}(q) = \mathbb{Z}/q\mathbb{Z},$$

$$\delta_\ell(a) = f_\ell(a,p) - 1, \quad \Delta_{\ell^r}(a) = -1 + \ell^r \cdot \frac{\#\left\{\begin{array}{c} \sigma \in \mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \mathrm{tr}(\sigma) \equiv a \,(\mathrm{mod}\, \ell^r) \end{array}\right\}}{|\,\mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z})|},$$

1st application : Sato-Tate for short intervals

$$S = \mathbb{P}\left(\alpha \leq \frac{a_p(E)}{2\sqrt{p}} \leq \beta\right) \sim \frac{2}{\pi}\int_\alpha^\beta \sqrt{1-u^2}du \quad (\beta - \alpha > p^{-1/2+\epsilon})$$

$$S = \sum_{2\alpha\sqrt{p} \leq t \leq 2\beta\sqrt{p}} \mathbb{P}(a_p(E) = t) = \sum_{2\alpha\sqrt{p} \leq t \leq 2\beta\sqrt{p}} f_\infty(t,p) \prod_\ell f_\ell(t,p).$$

Proof: write $S = \sum_{a \in \mathcal{A}} w_a \prod_\ell (1 + \delta_\ell(a))$ with

$$\mathcal{A} = [2\alpha\sqrt{p}, 2\beta\sqrt{p}] \cap \mathbb{Z}, \quad w_a = f_\infty(a,p), \quad \mathcal{G}(q) = \mathbb{Z}/q\mathbb{Z},$$

$$\delta_\ell(a) = f_\ell(a,p) - 1, \quad \Delta_{\ell^r}(a) = -1 + \ell^r \cdot \frac{\#\left\{\begin{array}{c} \sigma \in \mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \mathrm{tr}(\sigma) \equiv a \pmod{\ell^r} \end{array}\right\}}{|\,\mathrm{GL}_2^{(p)}(\mathbb{Z}/\ell^r\mathbb{Z})|},$$

$$\Delta_\ell = -1 + \lim_{r\to\infty} \frac{1}{\ell^r} \sum_{a \pmod{\ell^r}} \Delta_{\ell^r}(a) = 0.$$

2nd application : e.c. with a prime number of points

$$S := \mathbb{P}(\#E(F_p) = \text{prime}) = \frac{1 + O(\epsilon)}{\log p} \prod_{\ell} \frac{\# \left\{ \begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \\ \ell \nmid \det(\sigma) + 1 - \mathrm{tr}(\sigma) \end{array} \right\}}{(1 - \frac{1}{\ell}) |\, \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|},$$

2nd application : e.c. with a prime number of points

$$S := \mathbb{P}(\#E(F_p) = \text{prime}) = \frac{1 + O(\epsilon)}{\log p} \prod_{\ell} \frac{\# \left\{ \begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \\ \ell \nmid \det(\sigma) + 1 - \mathrm{tr}(\sigma) \end{array} \right\}}{(1 - \frac{1}{\ell}) |\, \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|},$$

where ϵ is small if we can show that there is the right proportion of primes in $[p - 2\sqrt{p} + 1, p + 2\sqrt{p} + 1]$ among APs $a \pmod{q}$, $q \le p^{\delta}$.

2nd application : e.c. with a prime number of points

$$S := \mathbb{P}(\#E(F_p) = \text{prime}) = \frac{1+O(\epsilon)}{\log p} \prod_{\ell} \frac{\#\left\{ \begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \\ \ell \nmid \det(\sigma) + 1 - \mathrm{tr}(\sigma) \end{array} \right\}}{(1-\frac{1}{\ell})|\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|},$$

where ϵ is small if we can show that there is the right proportion of primes in $[p - 2\sqrt{p} + 1, p + 2\sqrt{p} + 1]$ among APs $a \pmod q$, $q \le p^{\delta}$.

Proof: Note that

$$\begin{aligned} S &= \sum_{\substack{q \text{ prime} \\ p-2\sqrt{p}+1<q<p+2\sqrt{p}+1}} f_\infty(p+1-q,p) \prod_{\ell} f_\ell(p+1-q,p) \\ &= \sum_{a\in\mathcal{A}} w_a \prod_{\ell} (1+\delta_\ell(a)), \end{aligned}$$

where

$$\begin{aligned} \mathcal{A} = \{q \text{ prime} : |q-p-1| < 2\sqrt{p}\}, &\quad w_a \sim f_\infty(p+1-a,p), \\ \mathcal{G}(b) = (\mathbb{Z}/b\mathbb{Z})^*, &\quad \delta_\ell(a) = \mathbf{1}_{\ell\nmid a} \cdot (f_\ell(p+1-a,p) - 1). \end{aligned}$$

$$S = \sum_{a \in \mathcal{A}} w_a \prod_{\ell} (1 + \delta_\ell(a)),$$

where $\mathcal{A} = \{q \text{ prime} : |q - p - 1| < 2\sqrt{p}\}$, $\delta_\ell(a) = \lim_{r\to\infty} \Delta_{\ell^r}(a)$ with

$$\Delta_{\ell^r}(a) = -1 + \frac{\# \left\{ \begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \det(\sigma) \equiv p \pmod{\ell^r} \\ \mathrm{tr}(\sigma) \equiv p + 1 - a \pmod{\ell^r} \end{array} \right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|/\phi(\ell^{2r})}$$

$$S = \sum_{a \in \mathcal{A}} w_a \prod_{\ell} (1 + \delta_\ell(a)),$$

where $\mathcal{A} = \{q \text{ prime} : |q - p - 1| < 2\sqrt{p}\}$, $\delta_\ell(a) = \lim_{r\to\infty} \Delta_{\ell^r}(a)$ with

$$\Delta_{\ell^r}(a) = -1 + \frac{\#\left\{\begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \det(\sigma) \equiv p \pmod{\ell^r} \\ \mathrm{tr}(\sigma) \equiv p + 1 - a \pmod{\ell^r} \end{array}\right\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|/\phi(\ell^{2r})}$$

$$1 + \Delta_\ell = \lim_{r\to\infty} \frac{1}{\phi(\ell^r)} \sum_{a \in (\mathbb{Z}/\ell^r\mathbb{Z})^*} \Delta_{\ell^r}(a) = \frac{\#\left\{\begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \\ \ell \nmid \det(\sigma) + 1 - \mathrm{tr}(\sigma) \end{array}\right\}}{(1 - \frac{1}{\ell})|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}.$$

3rd application : e.c. with a given group structure

$$G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}, \quad N = |G| = m^2 k,$$

$$\sum_p \mathbb{P}(E(F_p) \cong G) = \frac{1 + O(\epsilon)}{\log N} \prod_\ell \lim_{r \to \infty} \frac{\# \left\{ \begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \mathrm{tr}(\sigma) \equiv \\ \det(\sigma) + 1 - N \pmod{\ell^r}, \\ \sigma \equiv I \pmod{\ell^{\nu_\ell(m)}}, \\ \sigma \not\equiv I \pmod{\ell^{\nu_\ell(m)+1}} \end{array} \right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|/\ell^r},$$

3rd application : e.c. with a given group structure

$$G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}, \quad N = |G| = m^2 k,$$

$$\sum_p \mathbb{P}(E(F_p) \cong G) = \frac{1 + O(\epsilon)}{\log N} \prod_\ell \lim_{r \to \infty} \frac{\# \left\{ \begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \mathrm{tr}(\sigma) \equiv \\ \det(\sigma) + 1 - N \pmod{\ell^r}, \\ \sigma \equiv I \pmod{\ell^{\nu_\ell(m)}}, \\ \sigma \not\equiv I \pmod{\ell^{\nu_\ell(m)+1}} \end{array} \right\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|/\ell^r},$$

where ϵ is small if we can show that there is the right proportion of primes in $[N - 2\sqrt{N} + 1, N + 2\sqrt{N} + 1]$ among APs $a \pmod{qm}$, $a \equiv 1 \pmod{m}$, $q \leq k^\delta$.

3rd application : e.c. with a given group structure

$$G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}, \quad N = |G| = m^2 k,$$

$$\sum_p \mathbb{P}(E(F_p) \cong G) = \frac{1 + O(\epsilon)}{\log N} \prod_\ell \lim_{r\to\infty} \frac{\# \left\{ \begin{array}{l} \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \mathrm{tr}(\sigma) \equiv \\ \det(\sigma) + 1 - N \pmod{\ell^r}, \\ \sigma \equiv I \pmod{\ell^{\nu_\ell(m)}}, \\ \sigma \not\equiv I \pmod{\ell^{\nu_\ell(m)+1}} \end{array} \right\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|/\ell^r},$$

where ϵ is small if we can show that there is the right proportion of primes in $[N - 2\sqrt{N} + 1, N + 2\sqrt{N} + 1]$ among APs $a \pmod{qm}$, $a \equiv 1 \pmod{m}$, $q \leq k^\delta$.

Need analogue of Gekeler's formula for $\mathbb{P}(E(\mathbb{F}_p) \cong G)$.