Arithmetic properties of the Frobenius traces of an abelian variety

A.C. Cojocaru (Univ. Illinois - Chicago & IMAR - Bucharest)

joint work with
R. Davis (Univ. Wisconsin - Madison)
A. Silverberg (Univ. California - Irvine)
K. Stange (Univ. Colorado - Boulder)

with contributions by
J-P. Serre (Collège de France)

June 2017

General problem

Given an abelian variety $A/\mathbb{Q}$,

General problem

Given an abelian variety $A/\mathbb{Q}$,

study its p-Weil polynomials

General problem

Given an abelian variety $A/\mathbb{Q}$,

study its p-Weil polynomials

as p varies over primes of good reduction.

Elliptic curves

Let $A/\mathbb{Q}$ be an abelian variety of $\dim A = 1$.

Elliptic curves

Let $A/\mathbb{Q}$ be an abelian variety of $\dim A = 1$.
This means A is an elliptic curve, i.e. it is the geometric locus of

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

for some

$$a, b \in \mathbb{Z}, -16\left(4a^3 + 27b^2\right) \neq 0, \text{ with } [0:1:0] \in A(\mathbb{Q}).$$

Elliptic curves

Let $A/\mathbb{Q}$ be an abelian variety of $\dim A = 1$.
This means A is an elliptic curve, i.e. it is the geometric locus of

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

for some

$$a, b \in \mathbb{Z}, -16\left(4a^3 + 27b^2\right) \neq 0, \text{ with } [0:1:0] \in A(\mathbb{Q}).$$

Then

$$P_{A,p}(X) = X^2 - a_p X + p \in \mathbb{Z}[X],$$

where

$$a_p := p + 1 - |A_p(\mathbb{F}_p)|.$$

Elliptic curves

Let $A/\mathbb{Q}$ be an abelian variety of $\dim A = 1$.
This means A is an elliptic curve, i.e. it is the geometric locus of

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

for some

$$a, b \in \mathbb{Z}, -16\left(4a^3 + 27b^2\right) \neq 0, \text{ with } [0 : 1 : 0] \in A(\mathbb{Q}).$$

Then

$$P_{A,p}(X) = X^2 - a_p X + p \in \mathbb{Z}[X],$$

where

$$a_p := p + 1 - |A_p(\mathbb{F}_p)|.$$

The Weil bound: $|a_p| \leq 2\sqrt{p}$.

Problem: investigate the sequence (a_p).

Problem: investigate the sequence (a_p).

Sample of emerging **directions**:

Problem: investigate the sequence (a_p).

Sample of emerging **directions**:

- modularity

Problem: investigate the sequence (a_p).

Sample of emerging **directions**:

- modularity
- Sato-Tate

Problem: investigate the sequence (a_p).

Sample of emerging **directions**:

- modularity
- Sato-Tate
- Lang-Trotter

Lang-Trotter Conjecture on Frobenius traces, 1976

Let $A/\mathbb{Q}$ elliptic curve and let $t \in \mathbb{Z}$.

Lang-Trotter Conjecture on Frobenius traces, 1976

Let $A/\mathbb{Q}$ elliptic curve and let $t \in \mathbb{Z}$.

Assume $\text{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ **or** $t \neq 0$.

Lang-Trotter Conjecture on Frobenius traces, 1976

Let $A/\mathbb{Q}$ elliptic curve and let $t \in \mathbb{Z}$.

Assume $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ **or** $t \neq 0$.

Then

- either $\#\{p : a_p = t\} < \infty$

Lang-Trotter Conjecture on Frobenius traces, 1976

Let $A/\mathbb{Q}$ elliptic curve and let $t \in \mathbb{Z}$.

Assume $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ **or** $t \neq 0$.

Then

- either $\#\{p : a_p = t\} < \infty$
- or $\exists\ C(A,t) > 0$ such that

$$\pi_A(x,t) := \#\{p \leq x : a_p = t\} \sim C(A,t)\ \frac{\sqrt{x}}{\log x}.$$

Partial results

CM case

Partial results

CM case i.e. $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \not\simeq \mathbb{Z}$

Partial results

CM case i.e. $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \not\simeq \mathbb{Z}$

• upper bound

$$\pi_A(x,t) \ll \frac{\sqrt{x}}{\log x}$$

(sieve methods & connections to prime values of quadratic polynomials)

Partial results

CM case i.e. $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \not\simeq \mathbb{Z}$

- upper bound

$$\pi_A(x, t) \ll \frac{\sqrt{x}}{\log x}$$

(sieve methods & connections to prime values of quadratic polynomials)

Non-CM case

Partial results

CM case i.e. $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \not\simeq \mathbb{Z}$

- upper bound

$$\pi_A(x,t) \ll \frac{\sqrt{x}}{\log x}$$

(sieve methods & connections to prime values of quadratic polynomials)

Non-CM case i.e. $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$

Partial results

CM case i.e. $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \not\simeq \mathbb{Z}$

- upper bound

$$\pi_A(x,t) \ll \frac{\sqrt{x}}{\log x}$$

(sieve methods & connections to prime values of quadratic polynomials)

Non-CM case i.e. $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$

- *unconditional* upper bound

$$\pi_A(x,t) \ll \frac{x}{(\log x)^{2-\varepsilon}}$$

by V.K. Murty, 1997

Partial results

CM case i.e. $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \not\simeq \mathbb{Z}$

- upper bound

$$\pi_A(x,t) \ll \frac{\sqrt{x}}{\log x}$$

(sieve methods & connections to prime values of quadratic polynomials)

Non-CM case i.e. $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$

- *unconditional* upper bound

$$\pi_A(x,t) \ll \frac{x}{(\log x)^{2-\varepsilon}}$$

by V.K. Murty, 1997

- *GRH* upper bound

$$\pi_A(x,t) \ll x^{\frac{4}{5}}$$

by M.R. Murty - V.K. Murty - N. Saradha, 1988

• stronger for special t, e.g. $t = 0$, $t = 1$

(B. Mazur, J-P. Serre, N. Elkies, É. Fouvry - M.R. Murty, M. Kaneko)

- stronger for special t, e.g. $t = 0$, $t = 1$

(B. Mazur, J-P. Serre, N. Elkies, É. Fouvry - M.R. Murty, M. Kaneko)

- average results confirming the conjectural asymptotic

(É. Fouvry - M.R. Murty, C. David - F. Pappalardi, S. Baier, W. Banks - I. Shparlinski, N. Jones etc)

- stronger for special t, e.g. $t = 0$, $t = 1$

(B. Mazur, J-P. Serre, N. Elkies, É. Fouvry - M.R. Murty, M. Kaneko)

- average results confirming the conjectural asymptotic

(É. Fouvry - M.R. Murty, C. David - F. Pappalardi, S. Baier, W. Banks - I. Shparlinski, N. Jones etc)

- numerical computations confirming the conjectural asymptotic

(S. Lang - H. Trotter, research experience for undergraduates by K. James and by ACC)

Basic ideas for proving upper bounds

Basic ideas for proving upper bounds

(i) If A has CM, then $\exists\ f = f_{A,t} \in \mathbb{Z}[X]$ **quadratic** such that

$$a_p = t \neq 0 \ \Rightarrow \ p = f(n) \text{ for some } n \in \mathbb{Z}.$$

Basic ideas for proving upper bounds

(i) If A has CM, then $\exists\ f = f_{A,t} \in \mathbb{Z}[X]$ **quadratic** such that

$$a_p = t \neq 0 \ \Rightarrow \ p = f(n) \text{ for some } n \in \mathbb{Z}.$$

Use **sieve methods**.

Basic ideas for proving upper bounds

(i) If A has CM, then $\exists\ f = f_{A,t} \in \mathbb{Z}[X]$ **quadratic** such that

$$a_p = t \neq 0 \ \Rightarrow \ p = f(n) \text{ for some } n \in \mathbb{Z}.$$

Use **sieve methods**.

(ii) In general,

Basic ideas for proving upper bounds

(i) If A has CM, then $\exists\ f = f_{A,t} \in \mathbb{Z}[X]$ **quadratic** such that

$$a_p = t \neq 0 \ \Rightarrow \ p = f(n) \text{ for some } n \in \mathbb{Z}.$$

Use **sieve methods**.

(ii) In general,

$$a_p = t \ \Rightarrow \ a_p \equiv t (\bmod n)$$

$$\Rightarrow \ \left(\frac{\mathbb{Q}(A[n])/\mathbb{Q}}{p}\right) \subseteq \ \{M \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \mathrm{tr}\, M \equiv t (\bmod n)\}.$$

Basic ideas for proving upper bounds

(i) If A has CM, then $\exists\ f = f_{A,t} \in \mathbb{Z}[X]$ **quadratic** such that

$$a_p = t \neq 0 \ \Rightarrow \ p = f(n) \text{ for some } n \in \mathbb{Z}.$$

Use **sieve methods**.

(ii) In general,

$$a_p = t \ \Rightarrow \ a_p \equiv t (\bmod n)$$

$$\Rightarrow \ \left(\frac{\mathbb{Q}(A[n])/\mathbb{Q}}{p}\right) \subseteq \ \{M \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \mathrm{tr}\, M \equiv t (\bmod n)\}.$$

Use **effective Chebotarev density theorem** with $n = n(x)$ as parameter.

Abelian varieties

Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g.

Abelian varieties

Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g.

Let

$$\rho_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}),$$

Abelian varieties

Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g.

Let

$$\rho_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}),$$

$$\bar{\rho}_{A,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}),$$

Abelian varieties

Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g.

Let

$$\rho_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}),$$

$$\bar{\rho}_{A,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}),$$

$$\rho_{A,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$$

Abelian varieties

Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g.

Let

$$\rho_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}),$$

$$\bar{\rho}_{A,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}),$$

$$\rho_{A,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$$

be the representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the division points of $A/\overline{\mathbb{Q}}$:

$$A[m] := \{P \in A(\overline{\mathbb{Q}}) : mP = 0_A\}.$$

For each good prime p, the p-Weil polynomial of A is uniquely determined by

$$P_{A,p}(X) = \det\left(X\ I_{2g} - \rho_{A,\ell}(\mathrm{Frob}_p)\right) \quad \forall \ell \neq p.$$

For each good prime p, the p-Weil polynomial of A is uniquely determined by

$$P_{A,p}(X) = \det\left(X\ I_{2g} - \rho_{A,\ell}(\mathrm{Frob}_p)\right) \quad \forall \ell \neq p.$$

We have

$$P_{A,p}(X) = X^{2g} + a_{1,p}X^{2g-1} + \ldots + a_{g,p}X^{g} + pa_{g-1,p}X^{g-1} + \ldots + p^{g-1}a_{1,p}X + p^{g}$$

with integer coefficients.

For each good prime p, the p-Weil polynomial of A is uniquely determined by

$$P_{A,p}(X) = \det\left(X\ I_{2g} - \rho_{A,\ell}(\mathrm{Frob}_p)\right) \quad \forall \ell \neq p.$$

We have

$$P_{A,p}(X) = X^{2g} + a_{1,p}X^{2g-1} + \ldots + a_{g,p}X^{g} + pa_{g-1,p}X^{g-1} + \ldots + p^{g-1}a_{1,p}X + p^{g}$$

with integer coefficients.

The Weil bound: $|a_{1,p}| \leq 2g\sqrt{p}.$

Theorem 1

$\begin{cases} \text{J-P. Serre, 1981} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange \& J-P. Serre} & \text{for } g \geq 2 \end{cases}$

Theorem 1 $\begin{cases} \text{J-P. Serre, 1981} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange \& J-P. Serre} & \text{for } g \geq 2 \end{cases}$

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Theorem 1 $\begin{cases} \text{J-P. Serre, 1981} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange \& J-P. Serre} & \text{for } g \geq 2 \end{cases}$

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Let $t \in \mathbb{Z}$.

Theorem 1 $\begin{cases} \text{J-P. Serre, 1981} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange \& J-P. Serre} & \text{for } g \geq 2 \end{cases}$

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Let $t \in \mathbb{Z}$.

Consider

$$\pi_A(x, t) := \# \{p \leq x : a_{1,p} = t\}.$$

Theorem 1 $\begin{cases} \text{J-P. Serre, 1981} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange \& J-P. Serre} & \text{for } g \geq 2 \end{cases}$

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Let $t \in \mathbb{Z}$.

Consider

$$\pi_A(x, t) := \#\left\{p \leq x : a_{1,p} = t\right\}.$$

Define

$$\alpha := \frac{1}{2g^2 + g + 1},$$

$$\beta := \begin{cases} \frac{1}{3} & \text{if } g = 1, \\ \frac{1}{2g^2 - g + 3} & \text{if } g \geq 2, \end{cases} \qquad \gamma := \begin{cases} \frac{1}{2} & \text{if } g = 1, \\ \frac{1}{8} & \text{if } g = 2, \\ \frac{1}{2g^2 - g + 1} & \text{if } g \geq 3. \end{cases}$$

Assume $\operatorname{Im}\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.

Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.
Then

(i1) unconditionally,

Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.
Then

(i1) unconditionally,

$$\pi_A(x, t) \ll_{A,\varepsilon} \frac{x}{(\log x)^{1+\alpha-\varepsilon}};$$

Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.
Then

(i1) unconditionally,

$$\pi_A(x, t) \ll_{A,\varepsilon} \frac{x}{(\log x)^{1+\alpha-\varepsilon}};$$

(i2) under GRH,

Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.
Then

(i1) unconditionally,

$$\pi_A(x, t) \ll_{A,\varepsilon} \frac{x}{(\log x)^{1+\alpha-\varepsilon}};$$

(i2) under GRH,

$$\pi_A(x, t) \ll_{A,\varepsilon} x^{1-\frac{\alpha}{2}+\varepsilon};$$

Assume $\operatorname{Im}\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.
Then

(i1) unconditionally,

$$\pi_A(x,t) \ll_{A,\varepsilon} \frac{x}{(\log x)^{1+\alpha-\varepsilon}};$$

(i2) under GRH,

$$\pi_A(x,t) \ll_{A,\varepsilon} x^{1-\frac{\alpha}{2}+\varepsilon};$$

(ii) if $t \neq \pm 2g$, then (i1) and (i2) hold with α replaced by β;

Assume $\mathrm{Im}\,\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.
Then

(i1) unconditionally,

$$\pi_A(x,t) \ll_{A,\varepsilon} \frac{x}{(\log x)^{1+\alpha-\varepsilon}};$$

(i2) under GRH,

$$\pi_A(x,t) \ll_{A,\varepsilon} x^{1-\frac{\alpha}{2}+\varepsilon};$$

(ii) if $t \neq \pm 2g$, then (i1) and (i2) hold with α replaced by β;

(iii) if $t = 0$, then (i1) and (i2) hold with α replaced by γ.

Corollary

Corollary

Setting and notation of Theorem 1.

Corollary

Setting and notation of Theorem 1.

For any $\varepsilon > 0$ we have:

Corollary

Setting and notation of Theorem 1.

For any $\varepsilon > 0$ we have:

(i) unconditionally,

$$\#\left\{p \leq x : |a_{1,p}| \geq (\log p)^{\alpha-\varepsilon}\right\} \sim \pi(x);$$

Corollary

Setting and notation of Theorem 1.

For any $\varepsilon > 0$ we have:

(i) unconditionally,

$$\#\left\{p \le x : |a_{1,p}| \ge (\log p)^{\alpha-\varepsilon}\right\} \sim \pi(x);$$

(ii) under GRH,

$$\#\left\{p \le x : |a_{1,p}| \ge p^{\frac{\alpha}{2}-\varepsilon}\right\} \sim \pi(x).$$

Further arithmetic investigation of $a_{1,p}$

Further arithmetic investigation of $a_{1,p}$

Context:

Further arithmetic investigation of $a_{1,p}$

Context:

- G. H. Hardy & S. Ramanujan, 1920:

$$\nu(p-1) \text{ has } \textbf{normal} \text{ order } \log\log p.$$

Further arithmetic investigation of $a_{1,p}$

Context:

- G. H. Hardy & S. Ramanujan, 1920:

$$\nu(p-1) \text{ has } \textbf{normal} \text{ order } \log\log p.$$

- P. Erdös & M. Kac, 1940:

$$\nu(p-1) \text{ has a } \textbf{normal} \text{ distribution.}$$

Further arithmetic investigation of $a_{1,p}$

Context:

- G. H. Hardy & S. Ramanujan, 1920:

$$\nu(p-1) \text{ has } \textbf{normal} \text{ order } \log\log p.$$

- P. Erdös & M. Kac, 1940:

$$\nu(p-1) \text{ has a } \textbf{normal} \text{ distribution.}$$

Here:

$$\nu(n) := \sum_{\ell | n} 1;$$

Further arithmetic investigation of $a_{1,p}$

Context:

- G. H. Hardy & S. Ramanujan, 1920:

$$\nu(p-1) \text{ has } \textbf{normal} \text{ order } \log\log p.$$

- P. Erdös & M. Kac, 1940:

$$\nu(p-1) \text{ has a } \textbf{normal} \text{ distribution}.$$

Here:

$$\nu(n) := \sum_{\ell | n} 1;$$

$$f(p) \text{ has } \underline{\text{normal order } \log\log p} \text{ if:}$$

$$\#\{p \leq x : (1-\varepsilon)\log\log p < f(p) < (1+\varepsilon)\log\log p\} \sim \pi(x).$$

Theorem 2 (ACC - R. Davis - A. Silverberg - K. Stange)

Theorem 2 (ACC - R. Davis - A. Silverberg - K. Stange)

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Theorem 2 (ACC - R. Davis - A. Silverberg - K. Stange)

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.

Theorem 2 (ACC - R. Davis - A. Silverberg - K. Stange)

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.

Assume GRH.

Theorem 2 (ACC - R. Davis - A. Silverberg - K. Stange)

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.

Assume GRH.
Then, for any $\tau \in \mathbb{R}$,

Theorem 2 (ACC - R. Davis - A. Silverberg - K. Stange)

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Assume $\mathrm{Im}\,\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.

Assume GRH.
Then, for any $\tau \in \mathbb{R}$,

$$\lim_{x \to \infty} \frac{\#\left\{p \leq x : p \nmid N_A, a_{1,p} \neq 0, \nu(a_{1,p}) \leq \log\log p + \tau\sqrt{\log\log p}\right\}}{\pi(x)}$$

$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\tau} e^{-\frac{t^2}{2}}\ dt.$$

Theorem 2 (ACC - R. Davis - A. Silverberg - K. Stange)

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.

Assume GRH.
Then, for any $\tau \in \mathbb{R}$,

$$\lim_{x \to \infty} \frac{\#\left\{p \leq x : p \nmid N_A, a_{1,p} \neq 0, \nu(a_{1,p}) \leq \log\log p + \tau\sqrt{\log\log p}\right\}}{\pi(x)}$$

$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\tau} e^{-\frac{t^2}{2}}\, dt.$$

In particular, $\nu(a_{1,p})$ has normal order $\log\log p$.

Conjecture $\begin{cases} \text{S. Lang - H. Trotter, 1976} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange} & \text{for } g \geq 2 \end{cases}$

Conjecture $\begin{cases} \text{S. Lang - H. Trotter, 1976} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange} & \text{for } g \geq 2 \end{cases}$

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Conjecture $\left\{ \begin{array}{ll} \text{S. Lang - H. Trotter, 1976} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange} & \text{for } g \geq 2 \end{array} \right.$

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Let $t \in \mathbb{Z}$.

Conjecture $\left\{ \begin{array}{ll} \text{S. Lang - H. Trotter, 1976} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange} & \text{for } g \geq 2 \end{array} \right.$

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Let $t \in \mathbb{Z}$.

- Assume $t \neq 0$.

Conjecture $\left\{ \begin{array}{ll} \text{S. Lang - H. Trotter, 1976} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange} & \text{for } g \geq 2 \end{array} \right.$

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Let $t \in \mathbb{Z}$.

- Assume $t \neq 0$.
- Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.

Conjecture $\left\{ \begin{array}{ll} \text{S. Lang - H. Trotter, 1976} & \text{for } g=1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange} & \text{for } g \geq 2 \end{array} \right.$

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Let $t \in \mathbb{Z}$.

- Assume $t \neq 0$.
- Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.
- Assume that $\forall\ I \subseteq [-1,1]$ we have

$$\lim_{x \to \infty} \frac{\# \left\{ p \leq x : p \nmid N_A, \frac{a_{1,p}}{2g\sqrt{p}} \in I \right\}}{\pi(x)} = \int_I \Phi(t)\ dt$$

for some $\Phi : [-1,1] \longrightarrow [0,\infty)$.

Conjecture $\left\{ \begin{array}{ll} \text{S. Lang - H. Trotter, 1976} & \text{for } g = 1 \\ \text{ACC - R. Davis - A. Silverberg - K. Stange} & \text{for } g \geq 2 \end{array} \right.$

Let $A/\mathbb{Q}$ pp abelian variety, $\dim A = g \geq 1$.

Let $t \in \mathbb{Z}$.

- Assume $t \neq 0$.
- Assume $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.
- Assume that $\forall\ I \subseteq [-1, 1]$ we have

$$\lim_{x \to \infty} \frac{\# \left\{ p \leq x : p \nmid N_A, \frac{a_{1,p}}{2g\sqrt{p}} \in I \right\}}{\pi(x)} = \int_I \Phi(t)\, dt$$

for some $\Phi : [-1, 1] \longrightarrow [0, \infty)$.
Then

$$\pi_A(x, t) \sim \frac{\Phi(0)}{g} \cdot C_{\text{chebotarev}}(A, t) \cdot \frac{\sqrt{x}}{\log x},$$

where $C_{\text{chebotarev}}(A, t)$ is described explicitly, as follows:

where $C_{\text{chebotarev}}(A, t)$ is described explicitly, as follows:

$$\operatorname{Im}\rho_A \text{ open in } \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \quad \Rightarrow \quad \exists \quad m_A \text{ smallest integer such that}$$

$$\rho_A(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \left(\mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})\right)^{-1}(\operatorname{Im}\bar{\rho}_{A,m}).$$

where $C_{\text{chebotarev}}(A, t)$ is described explicitly, as follows:

$$\operatorname{Im} \rho_A \text{ open in } \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \quad \Rightarrow \quad \exists \quad m_A \text{ smallest integer such that}$$

$$\rho_A(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \left(\mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})\right)^{-1} (\operatorname{Im} \bar{\rho}_{A,m}) .$$

Define

$$m_{A,t} := m_A \prod_{\ell \mid m_A} \ell^{v_\ell(t)}.$$

We conjecture that

$$C_{\text{chebotarev}}(A, t)$$

$$= \frac{m_{A,t} \ \ |\{M \in \operatorname{Im} \bar{\rho}_{A, m_{A,t}} : \operatorname{tr} M \equiv t (\operatorname{mod} m_{A,t})\}|}{|\operatorname{Im} \bar{\rho}_{A, m_{A,t}}, |}$$

$$\cdot \prod_{\ell \nmid m_A} \frac{\ell^{v_{\ell(t)}+1} \ \ |\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^{v_\ell(t)+1}\mathbb{Z}) : \operatorname{tr} M \equiv t (\operatorname{mod} \ell^{v_\ell(t)+1})\}|}{|\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^{v_\ell(t)+1}\mathbb{Z})|}.$$

Behind the scenes

(1) The **large image** assumption encompasses the **generic** case:

Behind the scenes

(1) The **large image** assumption encompasses the **generic** case:

true for any A with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ for $g = 1, 2, 6$ or odd

Behind the scenes

(1) The **large image** assumption encompasses the **generic** case:

true for any A with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ for $g = 1, 2, 6$ or odd

J-P. Serre 1972, 1985-1986

Behind the scenes

(1) The **large image** assumption encompasses the **generic** case:

true for any A with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ for $g = 1, 2, 6$ or odd

J-P. Serre 1972, 1985-1986

It gives us access to the relevant Galois groups:

mostly GSp_{2g} groups.

Behind the scenes

(1) The **large image** assumption encompasses the **generic** case:

true for any A with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ for $g = 1, 2, 6$ or odd

J-P. Serre 1972, 1985-1986

It gives us access to the relevant Galois groups:

mostly GSp_{2g} groups.

(2) To prove Theorems 1 and 2, we use **effective Chebotarev**:

- for finite Galois extensions: J.C. Lagarias - A.M. Odlyzko, 1975

Behind the scenes

(1) The **large image** assumption encompasses the **generic** case:

true for any A with $\text{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ for $g = 1, 2, 6$ or odd

J-P. Serre 1972, 1985-1986

It gives us access to the relevant Galois groups:

mostly GSp_{2g} groups.

(2) To prove Theorems 1 and 2, we use **effective Chebotarev**:

- for finite Galois extensions: J.C. Lagarias - A.M. Odlyzko, 1975
- for infinite ℓ-adic extensions: J-P. Serre, 1981

Behind the scenes

(1) The **large image** assumption encompasses the **generic** case:

true for any A with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ for $g = 1, 2, 6$ or odd

J-P. Serre 1972, 1985-1986

It gives us access to the relevant Galois groups:

mostly GSp_{2g} groups.

(2) To prove Theorems 1 and 2, we use **effective Chebotarev**:

- for finite Galois extensions: J.C. Lagarias - A.M. Odlyzko, 1975
- for infinite ℓ-adic extensions: J-P. Serre, 1981

GRH allows for **best error** terms in x.

(3) To prove Theorem 1, we also need

"**exercises in Lie groups**"

i.e. dimension calculations of conjugacy classes in GSp;

(3) To prove Theorem 1, we also need

"**exercises in Lie groups**"

i.e. dimension calculations of conjugacy classes in GSp;

Serre's contributions give optimal such bounds

(3) To prove Theorem 1, we also need

“**exercises in Lie groups**”

i.e. dimension calculations of conjugacy classes in GSp;

Serre’s contributions give optimal such bounds

(4) To prove Theorem 2, we follow a general

Central Limit **probabilistic strategy** of P. Billingsley (1970)

(5) For arbitrary t, our heuristic gives

$$\pi_{A,x}(t) \sim \frac{\Phi(0)}{g} \cdot \lim_{m\to\infty} \frac{m \ \ |\{M \in \operatorname{Im} \bar{\rho}_{A,m} : \operatorname{tr} M \equiv t (\operatorname{mod} m)\}|}{|\operatorname{Im} \bar{\rho}_{A,m}|} \cdot \frac{\sqrt{x}}{\log x},$$

(5) For arbitrary t, our heuristic gives

$$\pi_{A,x}(t) \sim \frac{\Phi(0)}{g} \cdot \lim_{m \to \infty} \frac{m \ \left|\{M \in \operatorname{Im} \bar{\rho}_{A,m} : \operatorname{tr} M \equiv t (\operatorname{mod} m)\}\right|}{|\operatorname{Im} \bar{\rho}_{A,m}|} \cdot \frac{\sqrt{x}}{\log x},$$

The **nonzero assumption** on t ensures that the limit equals the infinite product $C_{\text{chebotarev}}(A, t)$.

(6) We prove that

(6) We prove that

$$\frac{|\{M \in \mathsf{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) : \operatorname{tr} M \equiv t \pmod{\ell}\}|}{|\,\mathsf{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} = \frac{1}{\ell} + \mathsf{O}\left(\frac{1}{\ell^3}\right).$$

(6) We prove that

$$\frac{|\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) : \operatorname{tr} M \equiv t (\bmod \ell)\}|}{|\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} = \frac{1}{\ell} + \mathrm{O}\left(\frac{1}{\ell^3}\right).$$

This ensures that

$$\prod_{\ell} \frac{\ell|\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) : \operatorname{tr} M \equiv t (\bmod \ell)\}|}{|\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} \quad \textbf{converges}$$

(6) We prove that

$$\frac{|\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) : \operatorname{tr} M \equiv t \pmod{\ell}\}|}{|\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} = \frac{1}{\ell} + \mathrm{O}\left(\frac{1}{\ell^3}\right).$$

This ensures that

$$\prod_{\ell} \frac{\ell|\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) : \operatorname{tr} M \equiv t \pmod{\ell}\}|}{|\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} \quad \textbf{converges}$$

and that

$$C_{\text{chebotarev}}(A, t) < \infty.$$

(7) The **existence** of m_A is **ensured by the large image** assumption.

(7) The **existence** of m_A is **ensured by the large image** assumption.

The **calculation** of m_A is highly **non-trivial**:

(7) The **existence** of m_A is **ensured by the large image** assumption.

The **calculation** of m_A is highly **non-trivial**:

- recipe by Serre, 1972, for $g = 1$ and **largest** Galois, i.e.

$$|\,\mathrm{GL}_2(\hat{\mathbb{Z}}) : \mathrm{Im}\,\rho_A| = 2$$

(7) The **existence** of m_A is **ensured by the large image** assumption.

The **calculation** of m_A is highly **non-trivial**:

- recipe by Serre, 1972, for $g = 1$ and **largest** Galois, i.e.

$$|\operatorname{GL}_2(\hat{\mathbb{Z}}) : \operatorname{Im} \rho_A| = 2$$

Recent example of **infinite** such family by H.B. Daniels.

(7) The **existence** of m_A is **ensured by the large image** assumption.

The **calculation** of m_A is highly **non-trivial**:

- recipe by Serre, 1972, for $g = 1$ and **larges<u>t</u>** Galois, i.e.

$$|\,\mathrm{GL}_2(\hat{\mathbb{Z}}) : \mathrm{Im}\,\rho_A| = 2$$

  Recent example of **infinite** such family by H.B. Daniels.
- open for $g \geq 2$.

(8) The **equidistribution assumption** in our conjecture is a consequence of a far-reaching

generalization of the 1960s **Sato-Tate** Conjecture,

proposed by Serre in 2011 (after N. Katz - P. Sarnak 1999);

(8) The **equidistribution assumption** in our conjecture is a consequence of a far-reaching

generalization of the 1960s **Sato-Tate** Conjecture,

proposed by Serre in 2011 (after N. Katz - P. Sarnak 1999);

known only **for** $g = 1$.

(L. Clozel, M. Harris, N. Shepherd-Barron, R. Taylor, 2008-2010)

(8) The **equidistribution assumption** in our conjecture is a consequence of a far-reaching

generalization of the 1960s **Sato-Tate** Conjecture,

proposed by Serre in 2011 (after N. Katz - P. Sarnak 1999);

known only **for** $g = 1$.

(L. Clozel, M. Harris, N. Shepherd-Barron, R. Taylor, 2008-2010)

For $g = 1$, $\Phi(x) = \frac{2}{\pi}\sqrt{1 - x^2}$, giving rise to

$$\Phi(0) = \frac{2}{\pi}.$$

(8) The **equidistribution assumption** in our conjecture is a consequence of a far-reaching

generalization of the 1960s **Sato-Tate** Conjecture,

proposed by Serre in 2011 (after N. Katz - P. Sarnak 1999);

known only **for** $g = 1$.

(L. Clozel, M. Harris, N. Shepherd-Barron, R. Taylor, 2008-2010)

For $g = 1$, $\Phi(x) = \frac{2}{\pi}\sqrt{1 - x^2}$, giving rise to

$$\Phi(0) = \frac{2}{\pi}.$$

For $g = 2$, $\Phi(x)$ can also be calculated explicitly, giving rise to

$$\Phi(0) = \frac{256}{15\pi^2}.$$

(8) The **equidistribution assumption** in our conjecture is a consequence of a far-reaching

generalization of the 1960s **Sato-Tate** Conjecture,

proposed by Serre in 2011 (after N. Katz - P. Sarnak 1999);

known only **for** $g = 1$.

(L. Clozel, M. Harris, N. Shepherd-Barron, R. Taylor, 2008-2010)

For $g = 1$, $\Phi(x) = \frac{2}{\pi}\sqrt{1 - x^2}$, giving rise to

$$\Phi(0) = \frac{2}{\pi}.$$

For $g = 2$, $\Phi(x)$ can also be calculated explicitly, giving rise to

$$\Phi(0) = \frac{256}{15\pi^2}.$$

(F. Fité, K.S. Kedlaya, V. Rotger, A.V. Sutherland, 2012)

(9) In general, Φ is provably continuous and nonzero at 0:

(9) In general, Φ is provably continuous and nonzero at 0:

N. Katz and J-P. Serre, 2015

(9) In general, Φ is provably continuous and nonzero at 0:

N. Katz and J-P. Serre, 2015

(10) Computations related to $a_{1,p}$ were performed using examples previously studied by

L. Dieulefait (2003) for $g = 2$ and Y. Zarhin (2000) for any g.

(9) In general, Φ is provably continuous and nonzero at 0:

N. Katz and J-P. Serre, 2015

(10) Computations related to $a_{1,p}$ were performed using examples previously studied by

L. Dieulefait (2003) for $g = 2$ and Y. Zarhin (2000) for any g.

Thank you!