Effective Sato-Tate conjecture for abelian varieties with applications

Alina Bucur (UCSD), Francesc Fité[1] (MIT), Kiran S. Kedlaya (UCSD)

Joint Mathematics Meetings 2020 (Denver)

01/15/2020

[1]Funded by the National Science Foundation grant DMS-1638352 and the Simons Foundation grant 550033.

Notations

Throughout the talk:

- k is a number field.
- A/k is an abelian variety of dimension $g \geq 1$.
- N denotes the absolute conductor of A.
- For a prime ℓ,

$$\varrho_{A,\ell}\colon G_k \to \mathrm{Aut}(V_\ell(A))$$

  the ℓ-adic representation attached to A, where

$$T_\ell(A) := \varprojlim A[\ell^n](\overline{\mathbb{Q}}) \simeq \mathbb{Z}_\ell^{2g}\,, \qquad V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell\,.$$

- For a prime $\mathfrak{p}$ of k not dividing $N\ell$, let
  - $a_\mathfrak{p} := a_\mathfrak{p}(A) := \mathrm{Tr}(\varrho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}))$ denote the Frobenius trace at $\mathfrak{p}$.
  - $\overline{a}_\mathfrak{p} := \dfrac{a_\mathfrak{p}}{\mathrm{Nm}(\mathfrak{p})^{1/2}} \in [-2g, 2g]$ be the normalized Frobenius trace at $\mathfrak{p}$.

Sato-Tate group and Sato-Tate measure

- From now on, we will assume the following conjecture.

Conjecture (Banaszak-Kedlaya)

Denote by G_ℓ the Zariski closure of the image of $\varrho_{A,\ell}$ in $\mathrm{GSp}_{2g}/\mathbb{Q}_\ell$. Then there exists an algebraic subgroup G of $\mathrm{GSp}_{2g}/\mathbb{Q}$ such that

$$G_\ell = G \times_{\mathbb{Q}} \mathbb{Q}_\ell\,.$$

- Known in many cases: it is implied by the Mumford–Tate conjecture.
- The *Sato–Tate group* of A, denoted $\mathrm{ST}(A)$, is a maximal compact subgroup of $(G \cap \mathrm{Sp}_{2g})(\mathbb{C})$. It is thus a subgroup of $\mathrm{USp}(2g)$.
- Let μ denote the push forward of the Haar measure of $\mathrm{ST}(A)$ via

$$\mathrm{Tr}\colon \mathrm{ST}(A) \to [-2g, 2g]\,.$$

We call μ the *Sato–Tate measure* of A.

Sato-Tate group and Sato-Tate measure

- From now on, we will assume the following conjecture.

Conjecture (Banaszak-Kedlaya)

Denote by G_ℓ the Zariski closure of the image of $\varrho_{A,\ell}$ in $\mathrm{GSp}_{2g}/\mathbb{Q}_\ell$. Then there exists an algebraic subgroup G of $\mathrm{GSp}_{2g}/\mathbb{Q}$ such that

$$G_\ell = G \times_{\mathbb{Q}} \mathbb{Q}_\ell\,.$$

- Known in many cases: it is implied by the Mumford–Tate conjecture.
- The *Sato–Tate group* of A, denoted $\mathrm{ST}(A)$, is a maximal compact subgroup of $(G \cap \mathrm{Sp}_{2g})(\mathbb{C})$. It is thus a subgroup of $\mathrm{USp}(2g)$.
- Let μ denote the push forward of the Haar measure of $\mathrm{ST}(A)$ via

$$\mathrm{Tr}\colon \mathrm{ST}(A) \to [-2g, 2g]\,.$$

We call μ the *Sato–Tate measure* of A.

Sato-Tate group and Sato-Tate measure

- From now on, we will assume the following conjecture.

Conjecture (Banaszak-Kedlaya)

Denote by G_ℓ the Zariski closure of the image of $\varrho_{A,\ell}$ in $\mathrm{GSp}_{2g}/\mathbb{Q}_\ell$. Then there exists an algebraic subgroup G of $\mathrm{GSp}_{2g}/\mathbb{Q}$ such that

$$G_\ell = G \times_{\mathbb{Q}} \mathbb{Q}_\ell \,.$$

- Known in many cases: it is implied by the Mumford–Tate conjecture.
- The *Sato–Tate group* of A, denoted $\mathrm{ST}(A)$, is a maximal compact subgroup of $(G \cap \mathrm{Sp}_{2g})(\mathbb{C})$. It is thus a subgroup of $\mathrm{USp}(2g)$.
- Let μ denote the push forward of the Haar measure of $\mathrm{ST}(A)$ via

$$\mathrm{Tr}\colon \mathrm{ST}(A) \to [-2g, 2g]\,.$$

We call μ the *Sato–Tate measure* of A.

Sato-Tate group and Sato-Tate measure

- From now on, we will assume the following conjecture.

Conjecture (Banaszak-Kedlaya)

Denote by G_ℓ the Zariski closure of the image of $\varrho_{A,\ell}$ in $\mathrm{GSp}_{2g}/\mathbb{Q}_\ell$. Then there exists an algebraic subgroup G of $\mathrm{GSp}_{2g}/\mathbb{Q}$ such that

$$G_\ell = G \times_{\mathbb{Q}} \mathbb{Q}_\ell\,.$$

- Known in many cases: it is implied by the Mumford–Tate conjecture.
- The *Sato–Tate group* of A, denoted $\mathrm{ST}(A)$, is a maximal compact subgroup of $(G \cap \mathrm{Sp}_{2g})(\mathbb{C})$. It is thus a subgroup of $\mathrm{USp}(2g)$.
- Let μ denote the push forward of the Haar measure of $\mathrm{ST}(A)$ via

$$\mathrm{Tr}\colon \mathrm{ST}(A) \to [-2g, 2g]\,.$$

We call μ the *Sato–Tate measure* of A.

The Sato-Tate conjecture

Sato-Tate conjecture for abelian varieties

For any subinterval I of $[-2g, 2g]$, we have

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \text{ and } \overline{a}_{\mathfrak{p}} \in I\}}{\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x\}} = \mu(I)\,.$$

Equivalently,

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_{\mathfrak{p}}) = \mu(I)\,\mathrm{Li}(x) + o\left(\frac{x}{\log(x)}\right),$$

where

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)} \quad \text{and} \quad \delta_I \text{ is the characteristic function of } I\,.$$

The Sato-Tate conjecture

Sato-Tate conjecture for abelian varieties

For any subinterval I of $[-2g, 2g]$, we have

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \le x \text{ and } \overline{a}_{\mathfrak{p}} \in I\}}{\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \le x\}} = \mu(I)\,.$$

Equivalently,

$$\sum_{\mathrm{Nm}(\mathfrak{p})\le x} \delta_I(\overline{a}_{\mathfrak{p}}) = \mu(I)\,\mathrm{Li}(x) + o\left(\frac{x}{\log(x)}\right)\,,$$

where

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)} \quad \text{and} \quad \delta_I \text{ is the characteristic function of } I\,.$$

The effective Sato–Tate conjecture

Effective Sato-Tate conjecture for abelian varieties

There exists $\varepsilon > 0$ depending exclusively on $\mathrm{ST}(A)$ (and therefore, in fact, only on g) such that, for every subinterval I of $[-2g, 2g]$, we have

$$\sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_I(\overline{a}_{\mathfrak{p}}) = \mu(I)\,\mathrm{Li}(x) + O(x^{1-\varepsilon}) \qquad \text{for } x \gg_I 0\,,$$

where the implicit constant in the O-notation depends exclusively on the field k, the dimension g, and the absolute conductor N.

The Sato–Tate conjecture and L-functions

- To every irreducible representation Γ of $\mathrm{ST}(A)$, one attaches *à la Artin* an Euler product:

$$L(\Gamma(A), s) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(\Gamma(A), \mathrm{Nm}(\mathfrak{p})^{-s})^{-1},$$

which is absolutely convergent for $\Re(s) > 1$.

Theorem (Serre '68)

Suppose that $L(\Gamma(A), s)$ extends to a holomorphic function on an open neighborhood of $\Re(s) \geq 1$ and that does not vanish at $\Re(s) = 1$ for every irreducible nontrivial representation Γ of $\mathrm{ST}(A)$.
Then the Sato–Tate conjecture holds for A.

The Sato–Tate conjecture and L-functions

- To every irreducible representation Γ of $\mathrm{ST}(A)$, one attaches *à la Artin* an Euler product:

$$L(\Gamma(A), s) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(\Gamma(A), \mathrm{Nm}(\mathfrak{p})^{-s})^{-1},$$

which is absolutely convergent for $\Re(s) > 1$.

Theorem (Serre '68)

Suppose that $L(\Gamma(A), s)$ extends to a holomorphic function on an open neighborhood of $\Re(s) \geq 1$ and that does not vanish at $\Re(s) = 1$ for every irreducible nontrivial representation Γ of $\mathrm{ST}(A)$.
Then the Sato–Tate conjecture holds for A.

The effective Sato–Tate conjecture and L-functions

- $L(\Gamma(A), s)$ gives rise to a completed L-function

$$\Lambda(\Gamma(A), s) := B^{s/2} \cdot L(\Gamma(A), s) \cdot L_\infty(\Gamma(A), s)\,.$$

Conjecture (Generalized Riemann hypothesis (GRH) for $\Lambda(\Gamma(A), s)$)

- $\Lambda(\Gamma(A), s)$ extends to a meromorphic function over $\mathbb{C}$. It has simple poles at $s = 0, 1$ if Γ is trivial and it is analytic otherwise.
- $\Lambda(\Gamma(A), s) = \varepsilon \cdot \Lambda(\Gamma^\vee(A), 1 - s)$ for some $\varepsilon \in \mathbb{C}$ with $|\varepsilon| = 1$.
- All zeroes of $\Lambda(\Gamma(A), s)$ lie on the line $\Re(s) = 1/2$.

Theorem (Murty '83)

Suppose that $A/\mathbb{Q}$ is an elliptic curve without CM and that GRH holds for $\Lambda(\mathrm{Sym}^l(A), s)$ for every $l \geq 0$. For every subinterval $I \subseteq [-2, 2]$, we have

$$\sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_I(\overline{a}_p) = \mu(I)\,\mathrm{Li}(x) + O(x^{3/4}(\log(Nx))^{1/2}) \qquad \text{for } x \gg_I 0\,.$$

The effective Sato–Tate conjecture and L-functions

- $L(\Gamma(A), s)$ gives rise to a completed L-function

$$\Lambda(\Gamma(A), s) := B^{s/2} \cdot L(\Gamma(A), s) \cdot L_\infty(\Gamma(A), s)\,.$$

Conjecture (Generalized Riemann hypothesis (GRH) for $\Lambda(\Gamma(A), s)$)

- $\Lambda(\Gamma(A), s)$ extends to a meromorphic function over $\mathbb{C}$. It has simple poles at $s = 0, 1$ if Γ is trivial and it is analytic otherwise.
- $\Lambda(\Gamma(A), s) = \varepsilon \cdot \Lambda(\Gamma^\vee(A), 1 - s)$ for some $\varepsilon \in \mathbb{C}$ with $|\varepsilon| = 1$.
- All zeroes of $\Lambda(\Gamma(A), s)$ lie on the line $\Re(s) = 1/2$.

Theorem (Murty '83)

Suppose that $A/\mathbb{Q}$ is an elliptic curve without CM and that GRH holds for $\Lambda(\mathrm{Sym}^l(A), s)$ for every $l \geq 0$. For every subinterval $I \subseteq [-2, 2]$, we have

$$\sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_I(\overline{a}_p) = \mu(I)\,\mathrm{Li}(x) + O(x^{3/4}(\log(Nx))^{1/2}) \qquad \text{for } x \gg_I 0\,.$$

The effective Sato–Tate conjecture and L-functions

- $L(\Gamma(A), s)$ gives rise to a completed L-function

$$\Lambda(\Gamma(A), s) := B^{s/2} \cdot L(\Gamma(A), s) \cdot L_\infty(\Gamma(A), s)\,.$$

Conjecture (Generalized Riemann hypothesis (GRH) for $\Lambda(\Gamma(A), s)$)

- $\Lambda(\Gamma(A), s)$ extends to a meromorphic function over $\mathbb{C}$. It has simple poles at $s = 0, 1$ if Γ is trivial and it is analytic otherwise.
- $\Lambda(\Gamma(A), s) = \varepsilon \cdot \Lambda(\Gamma^\vee(A), 1 - s)$ for some $\varepsilon \in \mathbb{C}$ with $|\varepsilon| = 1$.
- All zeroes of $\Lambda(\Gamma(A), s)$ lie on the line $\Re(s) = 1/2$.

Theorem (Murty '83)

Suppose that $A/\mathbb{Q}$ is an elliptic curve without CM and that GRH holds for $\Lambda(\mathrm{Sym}^l(A), s)$ for every $l \geq 0$. For every subinterval $I \subseteq [-2, 2]$, we have

$$\sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_I(\overline{a}_p) = \mu(I)\,\mathrm{Li}(x) + O(x^{3/4}(\log(Nx))^{1/2}) \qquad \text{for } x \gg_I 0\,.$$

Main result

Theorem (Bucur-F.-Kedlaya)

Suppose that $\mathrm{ST}(A)$ *is connected and that GRH for* $\Lambda(\Gamma(A), s)$ *holds for every irreducible representation* Γ *of* $\mathrm{ST}(A)$. *Set*

$$\varepsilon := \frac{1}{2(q+\varphi)},$$

where q *denotes the rank of the Lie algebra of* $\mathrm{ST}(A)$ *and* φ *denotes the number of positive roots of its semisimple part. Then, for every subinterval* I *of* $[-2g, 2g]$, *we have*

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_p) = \mu(I)\,\mathrm{Li}(x) + O\left(\frac{x^{1-\varepsilon}(\log(Nx))^{2\varepsilon}}{\log(x)^{1-4\varepsilon}}\right) \qquad \text{for } x \gg_I 0\,,$$

where the implicit constant in the O-notation depends exclusively on k *and* g.

Main result

Theorem (Bucur-F.-Kedlaya)

Suppose that $\mathrm{ST}(A)$ *is connected and that GRH for* $\Lambda(\Gamma(A), s)$ *holds for every irreducible representation* Γ *of* $\mathrm{ST}(A)$*. Set*

$$\varepsilon := \frac{1}{2(q+\varphi)},$$

where q *denotes the rank of the Lie algebra of* $\mathrm{ST}(A)$ *and* φ *denotes the number of positive roots of its semisimple part. Then, for every subinterval* I *of* $[-2g, 2g]$*, we have*

$$\sum_{\mathrm{Nm}(\mathfrak{p}) \le x} \delta_I(\overline{a}_\mathfrak{p}) = \mu(I)\,\mathrm{Li}(x) + O\left(\frac{x^{1-\varepsilon}(\log(Nx))^{2\varepsilon}}{\log(x)^{1-4\varepsilon}}\right) \qquad \text{for } x \gg_I 0\,,$$

where the implicit constant in the O-notation depends exclusively on k *and* g*.*

Main result

Theorem (Bucur-F.-Kedlaya)

Suppose that $\mathrm{ST}(A)$ *is connected and that GRH for* $\Lambda(\Gamma(A), s)$ *holds for every irreducible representation* Γ *of* $\mathrm{ST}(A)$*. Set*

$$\varepsilon := \frac{1}{2(q+\varphi)},$$

where q *denotes the rank of the Lie algebra of* $\mathrm{ST}(A)$ *and* φ *denotes the number of positive roots of its semisimple part. Then, for every subinterval* I *of* $[-2g, 2g]$*, we have*

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_{\mathfrak{p}}) = \mu(I)\,\mathrm{Li}(x) + O\left(\frac{x^{1-\varepsilon}(\log(Nx))^{2\varepsilon}}{\log(x)^{1-4\varepsilon}}\right) \qquad \text{for } x \gg_I 0\,,$$

where the implicit constant in the O*-notation depends exclusively on* k *and* g*.*

Predictions for dimensions $g = 1$ and $g = 2$

- This extends Murty's result and previous work by Bucur and Kedlaya, who considered the case $A = E \times E'$, where E and E' are nonisogenous elliptic curves without CM.

g	Splitting of A	ST(A)	ε	Error term
1	E	SU(2)	1/4	$O(x^{3/4}\log(Nx)^{1/2})$
1	E_{CM}	U(1)	1/2	$O(x^{1/2}\log(Nx)\log(x))$
2	S	USp(4)	1/12	$O(x^{11/12}\log(Nx)^{1/6}\log(x)^{-2/3})$
2	S_{RM} $E \times E'$	SU(2) × SU(2)	1/8	$O(x^{7/8}\log(Nx)^{1/4}\log(x)^{-1/2})$
2	$E \times E'_{CM}$	SU(2) × U(1)	1/6	$O(x^{5/6}\log(Nx)^{1/3}\log(x)^{-1/3})$
2	$E_{CM} \times E'_{CM}$ S_{CM}	U(1) × U(1)	1/4	$O(x^{3/4}\log(Nx)^{1/2})$
2	E^2 S_{QM}	SU(2)	1/4	$O(x^{3/4}\log(Nx)^{1/2})$
2	E^2_{CM}	U(1)	1/2	$O(x^{1/2}\log(Nx)\log(x))$

- Numerical data suggests that $\varepsilon = 1/2$ in all cases.

Predictions for dimensions $g = 1$ and $g = 2$

- This extends Murty's result and previous work by Bucur and Kedlaya, who considered the case $A = E \times E'$, where E and E' are nonisogenous elliptic curves without CM.

g	Splitting of A	ST(A)	ε	Error term
1	E	SU(2)	1/4	$O(x^{3/4}\log(Nx)^{1/2})$
1	E_{CM}	U(1)	1/2	$O(x^{1/2}\log(Nx)\log(x))$
2	S	USp(4)	1/12	$O(x^{11/12}\log(Nx)^{1/6}\log(x)^{-2/3})$
2	S_{RM} $E \times E'$	SU(2) × SU(2)	1/8	$O(x^{7/8}\log(Nx)^{1/4}\log(x)^{-1/2})$
2	$E \times E'_{CM}$	SU(2) × U(1)	1/6	$O(x^{5/6}\log(Nx)^{1/3}\log(x)^{-1/3})$
2	$E_{CM} \times E'_{CM}$ S_{CM}	U(1) × U(1)	1/4	$O(x^{3/4}\log(Nx)^{1/2})$
2	E^2 S_{QM}	SU(2)	1/4	$O(x^{3/4}\log(Nx)^{1/2})$
2	E^2_{CM}	U(1)	1/2	$O(x^{1/2}\log(Nx)\log(x))$

- Numerical data suggests that $\varepsilon = 1/2$ in all cases.

Predictions for dimensions $g = 1$ and $g = 2$

- This extends Murty's result and previous work by Bucur and Kedlaya, who considered the case $A = E \times E'$, where E and E' are nonisogenous elliptic curves without CM.

g	Splitting of A	ST(A)	ε	Error term
1	E	SU(2)	1/4	$O(x^{3/4}\log(Nx)^{1/2})$
1	E_{CM}	U(1)	1/2	$O(x^{1/2}\log(Nx)\log(x))$
2	S	USp(4)	1/12	$O(x^{11/12}\log(Nx)^{1/6}\log(x)^{-2/3})$
2	S_{RM} $E \times E'$	SU(2) × SU(2)	1/8	$O(x^{7/8}\log(Nx)^{1/4}\log(x)^{-1/2})$
2	$E \times E'_{CM}$	SU(2) × U(1)	1/6	$O(x^{5/6}\log(Nx)^{1/3}\log(x)^{-1/3})$
2	$E_{CM} \times E'_{CM}$ S_{CM}	U(1) × U(1)	1/4	$O(x^{3/4}\log(Nx)^{1/2})$
2	E^2 S_{QM}	SU(2)	1/4	$O(x^{3/4}\log(Nx)^{1/2})$
2	E^2_{CM}	U(1)	1/2	$O(x^{1/2}\log(Nx)\log(x))$

- Numerical data suggests that $\varepsilon = 1/2$ in all cases.

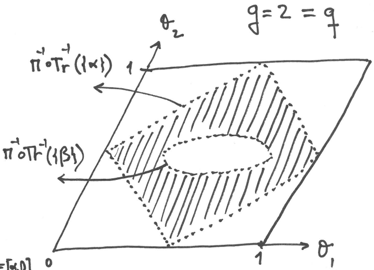
Ingredients in the proof (I): the Vinogradov function

We construct a function:

$$F_I : \mathbb{R}^q \longrightarrow [0,1]$$

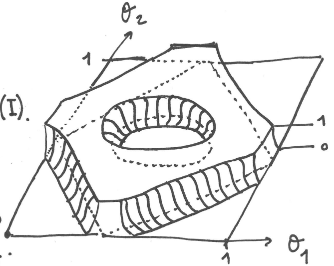
$$\mathbb{R}^q \xrightarrow{\ \pi\ } [0,1]^q/W \simeq \mathrm{Conj}(ST(A)) \longrightarrow [0,1]$$

$$\mathrm{Conj}(ST(A)) \xrightarrow{\ \mathrm{Tr}\ } [-2g, 2g] \supseteq I = [\alpha, \beta]$$



with the properties:

- F_I is a continuous approximation of the characteristic function of $\pi^{-1} \circ \mathrm{Tr}^{-1}(I)$.
- $F_I(\underline{\theta}) = \sum_{\underline{m} \in \mathbb{Z}^q} c_{\underline{m}} e^{2\pi i \underline{\theta} \cdot \underline{m}}$ has Fourier coefficients of rapid decay.



Ingredients of the proof (II): Murty's estimate

- By construction

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_\mathfrak{p}) \approx \sum_{\mathrm{Nm}(\mathfrak{p})\leq x} F_I(\mathrm{Frob}_\mathfrak{p})\,.$$

- Write $F_I = \sum_\chi c_\chi \chi$. The c_χ are still of rapid decay and $c_1 \approx \mu(I)$.
- Then

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_\mathfrak{p}) \approx \mu(I)\,\mathrm{Li}(x) + \sum_{\chi\neq 1} c_\chi \sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \chi(\mathrm{Frob}_\mathfrak{p})\,.$$

- For $\chi \neq 1$ Murty's estimate gives

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \chi(\mathrm{Frob}_\mathfrak{p}) = O(d_\chi x^{1/2}\log(N(x+w_\chi)))\,.$$

- The *rapid decay* of the coefficients c_χ compensates the *rapid growth* of the dimensions d_χ, which is exponential in φ.

Ingredients of the proof (II): Murty's estimate

- By construction

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_\mathfrak{p}) \approx \sum_{\mathrm{Nm}(\mathfrak{p})\leq x} F_I(\mathrm{Frob}_\mathfrak{p})\,.$$

- Write $F_I = \sum_\chi c_\chi \chi$. The c_χ are still of rapid decay and $c_1 \approx \mu(I)$.
- Then

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_\mathfrak{p}) \approx \mu(I)\,\mathrm{Li}(x) + \sum_{\chi\neq 1} c_\chi \sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \chi(\mathrm{Frob}_\mathfrak{p})\,.$$

- For $\chi \neq 1$ Murty's estimate gives

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \chi(\mathrm{Frob}_\mathfrak{p}) = O(d_\chi x^{1/2}\log(N(x+w_\chi)))\,.$$

- The *rapid decay* of the coefficients c_χ compensates the *rapid growth* of the dimensions d_χ, which is exponential in φ.

Ingredients of the proof (II): Murty's estimate

- By construction

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_\mathfrak{p}) \approx \sum_{\mathrm{Nm}(\mathfrak{p})\leq x} F_I(\mathrm{Frob}_\mathfrak{p})\,.$$

- Write $F_I = \sum_\chi c_\chi \chi$. The c_χ are still of rapid decay and $c_1 \approx \mu(I)$.
- Then

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_\mathfrak{p}) \approx \mu(I)\,\mathrm{Li}(x) + \sum_{\chi\neq 1} c_\chi \sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \chi(\mathrm{Frob}_\mathfrak{p})\,.$$

- For $\chi \neq 1$ Murty's estimate gives

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \chi(\mathrm{Frob}_\mathfrak{p}) = O(d_\chi x^{1/2} \log(N(x + w_\chi)))\,.$$

- The *rapid decay* of the coefficients c_χ compensates the *rapid growth* of the dimensions d_χ, which is exponential in φ.

Ingredients of the proof (II): Murty's estimate

- By construction

$$\sum_{\mathrm{Nm}(\mathfrak{p})\le x} \delta_I(\overline{a}_{\mathfrak{p}}) \approx \sum_{\mathrm{Nm}(\mathfrak{p})\le x} F_I(\mathrm{Frob}_{\mathfrak{p}})\,.$$

- Write $F_I = \sum_\chi c_\chi \chi$. The c_χ are still of rapid decay and $c_1 \approx \mu(I)$.
- Then

$$\sum_{\mathrm{Nm}(\mathfrak{p})\le x} \delta_I(\overline{a}_{\mathfrak{p}}) \approx \mu(I)\,\mathrm{Li}(x) + \sum_{\chi\neq 1} c_\chi \sum_{\mathrm{Nm}(\mathfrak{p})\le x} \chi(\mathrm{Frob}_{\mathfrak{p}})\,.$$

- For $\chi \neq 1$ Murty's estimate gives

$$\sum_{\mathrm{Nm}(\mathfrak{p})\le x} \chi(\mathrm{Frob}_{\mathfrak{p}}) = O(d_\chi x^{1/2} \log(N(x + w_\chi)))\,.$$

- The *rapid decay* of the coefficients c_χ compensates the *rapid growth* of the dimensions d_χ, which is exponential in φ.

Ingredients of the proof (II): Murty's estimate

- By construction

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_\mathfrak{p}) \approx \sum_{\mathrm{Nm}(\mathfrak{p})\leq x} F_I(\mathrm{Frob}_\mathfrak{p})\,.$$

- Write $F_I = \sum_\chi c_\chi \chi$. The c_χ are still of rapid decay and $c_1 \approx \mu(I)$.
- Then

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_\mathfrak{p}) \approx \mu(I)\,\mathrm{Li}(x) + \sum_{\chi\neq 1} c_\chi \sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \chi(\mathrm{Frob}_\mathfrak{p})\,.$$

- For $\chi \neq 1$ Murty's estimate gives

$$\sum_{\mathrm{Nm}(\mathfrak{p})\leq x} \chi(\mathrm{Frob}_\mathfrak{p}) = O(d_\chi x^{1/2} \log(N(x + w_\chi)))\,.$$

- The *rapid decay* of the coefficients c_χ compensates the *rapid growth* of the dimensions d_χ, which is exponential in φ.

Ingredients of the proof (II): Murty's estimate

- By construction

$$\sum_{\mathrm{Nm}(\mathfrak{p})\le x} \delta_I(\overline{a}_{\mathfrak{p}}) \approx \sum_{\mathrm{Nm}(\mathfrak{p})\le x} F_I(\mathrm{Frob}_{\mathfrak{p}})\,.$$

- Write $F_I = \sum_\chi c_\chi \chi$. The c_χ are still of rapid decay and $c_1 \approx \mu(I)$.
- Then

$$\sum_{\mathrm{Nm}(\mathfrak{p})\le x} \delta_I(\overline{a}_{\mathfrak{p}}) \approx \mu(I)\,\mathrm{Li}(x) + \sum_{\chi\neq 1} c_\chi \sum_{\mathrm{Nm}(\mathfrak{p})\le x} \chi(\mathrm{Frob}_{\mathfrak{p}})\,.$$

- For $\chi \neq 1$ Murty's estimate gives

$$\sum_{\mathrm{Nm}(\mathfrak{p})\le x} \chi(\mathrm{Frob}_{\mathfrak{p}}) = O(d_\chi x^{1/2} \log(N(x+w_\chi)))\,.$$

- The *rapid decay* of the coefficients c_χ compensates the *rapid growth* of the dimensions d_χ, which is exponential in φ.

Interval variant of Linnik's problem for abelian varieties

Corollary 1

Assume the hypotheses of the main result. For every subinterval I of $[-2g, 2g]$, there exists a prime $\mathfrak{p}$ not dividing N such that $\overline{a}_{\mathfrak{p}} \in I$ and

$$\mathrm{Nm}(\mathfrak{p}) = O(\nu(\min\{|I|, \mu(I)\}) \cdot \log(2N)^2 \cdot \log(\log(4N))^4)\,.$$

The implicit constant in the O-notation depends exclusively on k and g, and $\nu : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is defined by

$$\nu(z) := \max\left\{1, \frac{\log(z)^6}{z^{1/\varepsilon}}\right\}\,.$$

- This generalizes work of Chen–Park–Swaminathan, who considered the case in which A is an elliptic curve.

Interval variant of Linnik's problem for abelian varieties

Corollary 1

Assume the hypotheses of the main result. For every subinterval I of $[-2g, 2g]$, there exists a prime $\mathfrak{p}$ not dividing N such that $\overline{a}_{\mathfrak{p}} \in I$ and

$$\mathrm{Nm}(\mathfrak{p}) = O(\nu(\min\{|I|, \mu(I)\}) \cdot \log(2N)^2 \cdot \log(\log(4N))^4) \,.$$

The implicit constant in the O-notation depends exclusively on k and g, and $\nu : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is defined by

$$\nu(z) := \max\left\{1, \frac{\log(z)^6}{z^{1/\varepsilon}}\right\} \,.$$

- This generalizes work of Chen–Park–Swaminathan, who considered the case in which A is an elliptic curve.

Sign variant of Linnik's problem for two elliptic curves

- On this slide, let $A, A'/\mathbb{Q}$ be elliptic curves of conductors N, N'.

Theorem (Faltings '83; corollary of the Isogeny theorem)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \neq a_p(A')$.

- Under GRH for Artin L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^{12})$$

(Serre '86; using "Effective Chebotarev").

Theorem (Harris '09; corollary of Sato-Tate for $A \times A'$ over $\mathbb{Q}$)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \cdot a_p(A') < 0$.

- Under GRH for Symmetric power L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^6)$$

(Bucur and Kedlaya '12; using "Effective Sato-Tate").

Sign variant of Linnik's problem for two elliptic curves

- On this slide, let $A, A'/\mathbb{Q}$ be elliptic curves of conductors N, N'.

Theorem (Faltings '83; corollary of the Isogeny theorem)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \neq a_p(A')$.

- Under GRH for Artin L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^{12})$$

(Serre '86; using "Effective Chebotarev").

Theorem (Harris '09; corollary of Sato-Tate for $A \times A'$ over $\mathbb{Q}$)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \cdot a_p(A') < 0$.

- Under GRH for Symmetric power L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^6)$$

(Bucur and Kedlaya '12; using "Effective Sato-Tate").

Sign variant of Linnik's problem for two elliptic curves

- On this slide, let $A, A'/\mathbb{Q}$ be elliptic curves of conductors N, N'.

Theorem (Faltings '83; corollary of the Isogeny theorem)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \neq a_p(A')$.

- Under GRH for Artin L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^{12})$$

(Serre '86; using "Effective Chebotarev").

Theorem (Harris '09; corollary of Sato-Tate for $A \times A'$ over $\mathbb{Q}$)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \cdot a_p(A') < 0$.

- Under GRH for Symmetric power L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^6)$$

(Bucur and Kedlaya '12; using "Effective Sato-Tate").

Sign variant of Linnik's problem for two elliptic curves

- On this slide, let $A, A'/\mathbb{Q}$ be elliptic curves of conductors N, N'.

Theorem (Faltings '83; corollary of the Isogeny theorem)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \neq a_p(A')$.

- Under GRH for Artin L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^{12})$$

(Serre '86; using "Effective Chebotarev").

Theorem (Harris '09; corollary of Sato-Tate for $A \times A'$ over $\mathbb{Q}$)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \cdot a_p(A') < 0$.

- Under GRH for Symmetric power L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^{6})$$

(Bucur and Kedlaya '12; using "Effective Sato-Tate").

Sign variant of Linnik's problem for two elliptic curves

- On this slide, let $A, A'/\mathbb{Q}$ be elliptic curves of conductors N, N'.

Theorem (Faltings '83; corollary of the Isogeny theorem)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \neq a_p(A')$.

- Under GRH for Artin L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^{12})$$

(Serre '86; using "Effective Chebotarev").

Theorem (Harris '09; corollary of Sato-Tate for $A \times A'$ over $\mathbb{Q}$)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \cdot a_p(A') < 0$.

- Under GRH for Symmetric power L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^{6})$$

(Bucur and Kedlaya '12; using "Effective Sato-Tate").

Sign variant of Linnik's problem for two abelian varieties

Conjecture

If $\mathrm{Hom}(A, A') = 0$, then there exists $\mathfrak{p} \nmid NN'$ such that $a_{\mathfrak{p}}(A) \cdot a_{\mathfrak{p}}(A') < 0$.

Corollary 2

Let A, A' be abelian varieties such that $\mathrm{ST}(A)$, $\mathrm{ST}(A')$ are connected, and

$$\mathrm{ST}(A \times A') \simeq \mathrm{ST}(A) \times \mathrm{ST}(A'). \tag{1}$$

Assume that GRH for $\Lambda(\Gamma(A) \otimes \Gamma'(A'), s)$ holds for all irreducible rep. Γ, Γ'. Then, there exists $\mathfrak{p} \nmid NN'$ such that $a_{\mathfrak{p}}(A) \cdot a_{\mathfrak{p}}(A') < 0$ and

$$\mathrm{Nm}(\mathfrak{p}) = O(\log(2NN')^2 \log(\log(4NN'))^6). \tag{2}$$

- Using Bach kernel integration, we can
  - replace (1) with the weaker condition $\mathrm{Hom}(A, A') = 0$.
  - improve (2) to $O(\log(2NN')^2)$.

Sign variant of Linnik's problem for two abelian varieties

Conjecture

If $\mathrm{Hom}(A, A') = 0$, then there exists $\mathfrak{p} \nmid NN'$ such that $a_\mathfrak{p}(A) \cdot a_\mathfrak{p}(A') < 0$.

Corollary 2

Let A, A' be abelian varieties such that $\mathrm{ST}(A)$, $\mathrm{ST}(A')$ are connected, and

$$\mathrm{ST}(A \times A') \simeq \mathrm{ST}(A) \times \mathrm{ST}(A')\,. \tag{1}$$

Assume that GRH for $\Lambda(\Gamma(A) \otimes \Gamma'(A'), s)$ holds for all irreducible rep. Γ, Γ'. Then, there exists $\mathfrak{p} \nmid NN'$ such that $a_\mathfrak{p}(A) \cdot a_\mathfrak{p}(A') < 0$ and

$$\mathrm{Nm}(\mathfrak{p}) = O(\log(2NN')^2 \log(\log(4NN'))^6)\,. \tag{2}$$

- Using Bach kernel integration, we can
  - replace (1) with the weaker condition $\mathrm{Hom}(A, A') = 0$.
  - improve (2) to $O(\log(2NN')^2)$.

Sign variant of Linnik's problem for two abelian varieties

Conjecture

If $\mathrm{Hom}(A, A') = 0$, then there exists $\mathfrak{p} \nmid NN'$ such that $a_{\mathfrak{p}}(A) \cdot a_{\mathfrak{p}}(A') < 0$.

Corollary 2

Let A, A' be abelian varieties such that $\mathrm{ST}(A)$, $\mathrm{ST}(A')$ are connected, and

$$\mathrm{ST}(A \times A') \simeq \mathrm{ST}(A) \times \mathrm{ST}(A') \,. \tag{1}$$

Assume that GRH for $\Lambda(\Gamma(A) \otimes \Gamma'(A'), s)$ holds for all irreducible rep. Γ, Γ'. Then, there exists $\mathfrak{p} \nmid NN'$ such that $a_{\mathfrak{p}}(A) \cdot a_{\mathfrak{p}}(A') < 0$ and

$$\mathrm{Nm}(\mathfrak{p}) = O(\log(2NN')^2 \log(\log(4NN'))^6) \,. \tag{2}$$

- Using Bach kernel integration, we can
  - replace (1) with the weaker condition $\mathrm{Hom}(A, A') = 0$.
  - improve (2) to $O(\log(2NN')^2)$.

Frobenius traces attaining the Weil bound

- On this slide, let A be an elliptic curve with CM (defined over k).
- Consider the set of "record primes"

$$R(x) = \{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \text{ and } a_{\mathfrak{p}} = \lfloor 2\sqrt{\mathrm{Nm}(\mathfrak{p})} \rfloor\}.$$

- Serre has conjectured[2]

$$\#R(x) \sim \frac{4}{3\pi}\frac{x^{3/4}}{\log(x)} \qquad \text{as } x \to \infty.$$

Corollary 3

Suppose that GRH holds for the Hecke L-function attached to any integral power of the Hecke character of A. Then

$$\#R(x) \asymp \frac{x^{3/4}}{\log(x)} \qquad \text{for } x \gg 0.$$

[2] Added after the talk: As J. Achter pointed out to me during the JMM2020, this has been proven by K. James and and P. Pollack. Thus Corollary 3 only recovers a weaker and conditional form of James' and Pollack's result!

Frobenius traces attaining the Weil bound

- On this slide, let A be an elliptic curve with CM (defined over k).
- Consider the set of "record primes"

$$R(x) = \{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \text{ and } a_{\mathfrak{p}} = \lfloor 2\sqrt{\mathrm{Nm}(\mathfrak{p})} \rfloor\}.$$

- Serre has conjectured[2]

$$\#R(x) \sim \frac{4}{3\pi} \frac{x^{3/4}}{\log(x)} \qquad \text{as } x \to \infty.$$

Corollary 3

Suppose that GRH holds for the Hecke L-function attached to any integral power of the Hecke character of A. Then

$$\#R(x) \asymp \frac{x^{3/4}}{\log(x)} \qquad \text{for } x \gg 0.$$

[2] Added after the talk: As J. Achter pointed out to me during the JMM2020, this has been proven by K. James and and P. Pollack. Thus Corollary 3 only recovers a weaker and conditional form of James' and Pollack's result!

Frobenius traces attaining the Weil bound

- On this slide, let A be an elliptic curve with CM (defined over k).
- Consider the set of "record primes"

$$R(x) = \{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \text{ and } a_{\mathfrak{p}} = \lfloor 2\sqrt{\mathrm{Nm}(\mathfrak{p})} \rfloor\}\,.$$

- Serre has conjectured[2]

$$\#R(x) \sim \frac{4}{3\pi}\frac{x^{3/4}}{\log(x)} \qquad \text{as } x \to \infty.$$

Corollary 3

Suppose that GRH holds for the Hecke L-function attached to any integral power of the Hecke character of A. Then

$$\#R(x) \asymp \frac{x^{3/4}}{\log(x)} \qquad \text{for } x \gg 0\,.$$

[2] Added after the talk: As J. Achter pointed out to me during the JMM2020, this has been proven by K. James and and P. Pollack. Thus Corollary 3 only recovers a weaker and conditional form of James' and Pollack's result!

Frobenius traces attaining the Weil bound

- On this slide, let A be an elliptic curve with CM (defined over k).
- Consider the set of "record primes"

$$R(x) = \{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \text{ and } a_{\mathfrak{p}} = \lfloor 2\sqrt{\mathrm{Nm}(\mathfrak{p})} \rfloor\}.$$

- Serre has conjectured[2]

$$\#R(x) \sim \frac{4}{3\pi}\frac{x^{3/4}}{\log(x)} \qquad \text{as } x \to \infty.$$

Corollary 3

Suppose that GRH holds for the Hecke L-function attached to any integral power of the Hecke character of A. Then

$$\#R(x) \asymp \frac{x^{3/4}}{\log(x)} \qquad \text{for } x \gg 0\,.$$

[2] Added after the talk: As J. Achter pointed out to me during the JMM2020, this has been proven by K. James and and P. Pollack. Thus Corollary 3 only recovers a weaker and conditional form of James' and Pollack's result!

Frobenius traces attaining the Weil bound

- A simple idea:

  If $\mathrm{Nm}(\mathfrak{p}) \leq x$ and $\overline{a}_{\mathfrak{p}} \in I_x := (2 - x^{-1/2}, 2)$, then $a_{\mathfrak{p}} = \lfloor 2\sqrt{\mathrm{Nm}(\mathfrak{p})} \rfloor$.

- Therefore

$$\#R(x) \geq \sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_{I_x}(\overline{a}_{\mathfrak{p}}) = \mu(I_x)\,\mathrm{Li}(x) + O(x^{1/2}\log(Nx)\log(x)).$$

- Using that $\mu(I_x) = \frac{1}{\pi}x^{-1/4} + O(x^{-3/4})$, we find that

$$\#R(x) \geq \frac{1}{\pi}\frac{x^{3/4}}{\log(x)} \qquad \text{as } x \to \infty.$$

- If A is a non CM elliptic curve, then $\mu(I_x)$ is tiny and the error term bigger. No hope for such an approach to count record primes!

Frobenius traces attaining the Weil bound

- A simple idea:

  If $\mathrm{Nm}(\mathfrak{p}) \leq x$ and $\overline{a}_\mathfrak{p} \in I_x := (2 - x^{-1/2}, 2)$, then $a_\mathfrak{p} = \lfloor 2\sqrt{\mathrm{Nm}(\mathfrak{p})} \rfloor$.

- Therefore

$$\#R(x) \geq \sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_{I_x}(\overline{a}_\mathfrak{p}) = \mu(I_x)\,\mathrm{Li}(x) + O(x^{1/2}\log(Nx)\log(x)).$$

- Using that $\mu(I_x) = \frac{1}{\pi} x^{-1/4} + O(x^{-3/4})$, we find that

$$\#R(x) \geq \frac{1}{\pi}\frac{x^{3/4}}{\log(x)} \qquad \text{as } x \to \infty.$$

- If A is a non CM elliptic curve, then $\mu(I_x)$ is tiny and the error term bigger. No hope for such an approach to count record primes! Nonetheless, Serre still conjectures:

$$\#R(x) \sim \frac{8}{3\pi}\frac{x^{1/4}}{\log(x)} \qquad \text{as } x \to \infty.$$

Frobenius traces attaining the Weil bound

- A simple idea:

  If $\mathrm{Nm}(\mathfrak{p}) \leq x$ and $\overline{a}_\mathfrak{p} \in I_x := (2 - x^{-1/2}, 2)$, then $a_\mathfrak{p} = \lfloor 2\sqrt{\mathrm{Nm}(\mathfrak{p})} \rfloor$.

- Therefore

$$\#R(x) \geq \sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_{I_x}(\overline{a}_\mathfrak{p}) = \mu(I_x)\,\mathrm{Li}(x) + O(x^{1/2}\log(Nx)\log(x))\,.$$

- Using that $\mu(I_x) = \frac{1}{\pi}x^{-1/4} + O(x^{-3/4})$, we find that

$$\#R(x) \geq \frac{1}{\pi}\frac{x^{3/4}}{\log(x)} \qquad \text{as } x \to \infty\,.$$

- If A is a non CM elliptic curve, then $\mu(I_x)$ is tiny and the error term bigger. No hope for such an approach to count record primes! Nonetheless, Serre still conjectures:

$$\#R(x) \sim \frac{8}{3\pi}\frac{x^{1/4}}{\log(x)} \qquad \text{as } x \to \infty\,.$$

Frobenius traces attaining the Weil bound

- A simple idea:

  If $\mathrm{Nm}(\mathfrak{p}) \leq x$ and $\overline{a}_\mathfrak{p} \in I_x := (2 - x^{-1/2}, 2)$, then $a_\mathfrak{p} = \lfloor 2\sqrt{\mathrm{Nm}(\mathfrak{p})} \rfloor$.

- Therefore

$$\#R(x) \geq \sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_{I_x}(\overline{a}_\mathfrak{p}) = \mu(I_x)\,\mathrm{Li}(x) + O(x^{1/2}\log(Nx)\log(x))\,.$$

- Using that $\mu(I_x) = \frac{1}{\pi} x^{-1/4} + O(x^{-3/4})$, we find that

$$\#R(x) \geq \frac{1}{\pi}\frac{x^{3/4}}{\log(x)} \qquad \text{as } x \to \infty\,.$$

- If A is a non CM elliptic curve, then $\mu(I_x)$ is tiny and the error term bigger. No hope for such an approach to count record primes!

  Nonetheless, Serre still conjectures:

$$\#R(x) \sim \frac{8}{3\pi}\frac{x^{1/4}}{\log(x)} \qquad \text{as } x \to \infty\,.$$

Frobenius traces attaining the Weil bound

- A simple idea:

  If $\mathrm{Nm}(\mathfrak{p}) \leq x$ and $\overline{a}_{\mathfrak{p}} \in I_x := (2 - x^{-1/2}, 2)$, then $a_{\mathfrak{p}} = \lfloor 2\sqrt{\mathrm{Nm}(\mathfrak{p})} \rfloor$.

- Therefore

$$\#R(x) \geq \sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_{I_x}(\overline{a}_{\mathfrak{p}}) = \mu(I_x)\,\mathrm{Li}(x) + O(x^{1/2}\log(Nx)\log(x)) .$$

- Using that $\mu(I_x) = \frac{1}{\pi}x^{-1/4} + O(x^{-3/4})$, we find that

$$\#R(x) \geq \frac{1}{\pi}\frac{x^{3/4}}{\log(x)} \qquad \text{as } x \to \infty .$$

- If A is a non CM elliptic curve, then $\mu(I_x)$ is tiny and the error term bigger. No hope for such an approach to count record primes! Nonetheless, Serre still conjectures:

$$\#R(x) \sim \frac{8}{3\pi}\frac{x^{1/4}}{\log(x)} \qquad \text{as } x \to \infty .$$