The Sato-Tate conjecture and its generalizations

Kiran S. Kedlaya 

Department of Mathematics, University of California, San Diego
kedlaya@ucsd.edu
http://kskedlaya.org/slides/

VaNTAGe virtual seminar
March 24, 2020

Contents

Counting roots of polynomials

Let $f(x) \in \mathbb{Z}[x]$ be a primitive squarefree polynomial of degree $d > 0$. For p prime, define

$$N_f(p) := \#\{x \in \{0, \dots, p-1\} : f(x) \equiv 0 \pmod{p}\}.$$

Clearly $N_f(p) \in \{0, \dots, d\}$. But for fixed f and i, what is the probability that $N_f(p) = i$ when p is a "random" prime?

In other words, if we define $\pi(N) := \#\{p \text{ prime}, p \leq N\}$, does the limit

$$\lim_{N \to \infty} \frac{1}{\pi(N)} \#\{p \text{ prime}, p \leq N, N_f(p) = i\}$$

exist, and if so what is it?

Trivial example: if f splits as a product of linear factors, then $N_f(p) = d$ for all but finitely many p.

Counting roots of polynomials

Let $f(x) \in \mathbb{Z}[x]$ be a primitive squarefree polynomial of degree $d > 0$. For p prime, define

$$N_f(p) := \#\{x \in \{0, \dots, p-1\} : f(x) \equiv 0 \pmod{p}\}.$$

Clearly $N_f(p) \in \{0, \dots, d\}$. But for fixed f and i, what is the probability that $N_f(p) = i$ when p is a "random" prime?

In other words, if we define $\pi(N) := \#\{p \text{ prime}, p \leq N\}$, does the limit

$$\lim_{N \to \infty} \frac{1}{\pi(N)} \#\{p \text{ prime}, p \leq N, N_f(p) = i\}$$

exist, and if so what is it?

Trivial example: if f splits as a product of linear factors, then $N_f(p) = d$ for all but finitely many p.

Counting roots of polynomials

Let $f(x) \in \mathbb{Z}[x]$ be a primitive squarefree polynomial of degree $d > 0$. For p prime, define

$$N_f(p) := \#\{x \in \{0, \dots, p-1\} : f(x) \equiv 0 \pmod{p}\}.$$

Clearly $N_f(p) \in \{0, \dots, d\}$. But for fixed f and i, what is the probability that $N_f(p) = i$ when p is a "random" prime?

In other words, if we define $\pi(N) := \#\{p \text{ prime}, p \leq N\}$, does the limit

$$\lim_{N \to \infty} \frac{1}{\pi(N)} \#\{p \text{ prime}, p \leq N, N_f(p) = i\}$$

exist, and if so what is it?

Trivial example: if f splits as a product of linear factors, then $N_f(p) = d$ for all but finitely many p.

Example: quadratic polynomials

Take $f(x) = ax^2 + bx + c$. Let $\Delta = b^2 - 4ac$ be the discriminant. Then

$$N_f(p) = \begin{cases} 0 & \text{if } \Delta \not\equiv \square \pmod{p} \\ 1 & \text{if } \Delta \equiv 0 \pmod{p} \\ 2 & \text{if } \Delta \equiv \square \not\equiv 0 \pmod{p} \end{cases} \qquad (\text{for } p > 2).$$

If $\Delta \neq \square$, then $N_f(p)$ takes the values 0 and 2 each with probability $\frac{1}{2}$.

The proof of this combines Dirichlet's  theorem* with the fact that quadratic reciprocity implies a clean formula for $N_f(p)$. For example, in case $\Delta = 5$, one has

$$N_f(p) = \begin{cases} 0 & \text{if } p \equiv 2, 3 \pmod{5} \\ 1 & \text{if } p = 5 \\ 2 & \text{if } p \equiv 1, 4 \pmod{5} \end{cases} \qquad (\text{for } p > 2).$$

*I really mean the prime number theorem in arithmetic progressions, but never mind.

Example: quadratic polynomials

Take $f(x) = ax^2 + bx + c$. Let $\Delta = b^2 - 4ac$ be the discriminant. Then

$$N_f(p) = \begin{cases} 0 & \text{if } \Delta \not\equiv \square \pmod{p} \\ 1 & \text{if } \Delta \equiv 0 \pmod{p} \\ 2 & \text{if } \Delta \equiv \square \not\equiv 0 \pmod{p} \end{cases} \qquad \text{(for } p > 2\text{)}.$$

If $\Delta \neq \square$, then $N_f(p)$ takes the values 0 and 2 each with probability $\frac{1}{2}$.

The proof of this combines Dirichlet's  theorem* with the fact that quadratic reciprocity implies a clean formula for $N_f(p)$. For example, in case $\Delta = 5$, one has

$$N_f(p) = \begin{cases} 0 & \text{if } p \equiv 2, 3 \pmod{5} \\ 1 & \text{if } p = 5 \\ 2 & \text{if } p \equiv 1, 4 \pmod{5} \end{cases} \qquad \text{(for } p > 2\text{)}.$$

*I really mean the prime number theorem in arithmetic progressions, but never mind.

Example: quadratic polynomials

Take $f(x) = ax^2 + bx + c$. Let $\Delta = b^2 - 4ac$ be the discriminant. Then

$$N_f(p) = \begin{cases} 0 & \text{if } \Delta \not\equiv \square \pmod{p} \\ 1 & \text{if } \Delta \equiv 0 \pmod{p} \\ 2 & \text{if } \Delta \equiv \square \not\equiv 0 \pmod{p} \end{cases} \qquad (\text{for } p > 2).$$

If $\Delta \neq \square$, then $N_f(p)$ takes the values 0 and 2 each with probability $\frac{1}{2}$.

The proof of this combines Dirichlet's  theorem* with the fact that quadratic reciprocity implies a clean formula for $N_f(p)$. For example, in case $\Delta = 5$, one has

$$N_f(p) = \begin{cases} 0 & \text{if } p \equiv 2, 3 \pmod{5} \\ 1 & \text{if } p = 5 \\ 2 & \text{if } p \equiv 1, 4 \pmod{5} \end{cases} \qquad (\text{for } p > 2).$$

*I really mean the prime number theorem in arithmetic progressions, but never mind.

The Chebotarëv  density theorem: first version

Let L be a splitting field of f, with Galois  group G. One only has a congruence formula for $N_f(p)$ when G is abelian, by Artin*  reciprocity.

But we can answer the probability question as follows. Let $\alpha_1, \dots, \alpha_d$ be the roots of f in L, on which G acts by permutations. Let c_i denote the probability that a random element of G has exactly i fixed points.

Theorem (Chebotarëv, early 1920s)

For $i = 0, \dots, d$, $N_f(p) = i$ with probability c_i.

Consistency check: $N_f(p)$ can never equal $d-1$, and $c_{d-1} = 0$.

Example: if d is large and $G = S_d$, then the probability that $N_f(p) = 0$ is roughly $1/e \cong 0.368$ by counting derangements.

---

*Not to be confused with his son .

The Chebotarëv  density theorem: first version

Let L be a splitting field of f, with Galois  group G. One only has a congruence formula for $N_f(p)$ when G is abelian, by Artin*  reciprocity.

But we can answer the probability question as follows. Let $\alpha_1, \dots, \alpha_d$ be the roots of f in L, on which G acts by permutations. Let c_i denote the probability that a random element of G has exactly i fixed points.

Theorem (Chebotarëv, early 1920s)

For $i = 0, \dots, d$, $N_f(p) = i$ with probability c_i.

Consistency check: $N_f(p)$ can never equal $d-1$, and $c_{d-1} = 0$.

Example: if d is large and $G = S_d$, then the probability that $N_f(p) = 0$ is roughly $1/e \cong 0.368$ by counting derangements.

*Not to be confused with his son .

The Chebotarëv  density theorem: first version

Let L be a splitting field of f, with Galois  group G. One only has a congruence formula for $N_f(p)$ when G is abelian, by Artin*  reciprocity.

But we can answer the probability question as follows. Let $\alpha_1, \dots, \alpha_d$ be the roots of f in L, on which G acts by permutations. Let c_i denote the probability that a random element of G has exactly i fixed points.

Theorem (Chebotarëv, early 1920s)

For $i = 0, \dots, d$, $N_f(p) = i$ with probability c_i.

Consistency check: $N_f(p)$ can never equal $d-1$, and $c_{d-1} = 0$.

Example: if d is large and $G = S_d$, then the probability that $N_f(p) = 0$ is roughly $1/e \cong 0.368$ by counting derangements.

*Not to be confused with his son .

The Chebotarëv  density theorem: first version

Let L be a splitting field of f, with Galois  group G. One only has a congruence formula for $N_f(p)$ when G is abelian, by Artin*  reciprocity.

But we can answer the probability question as follows. Let $\alpha_1, \dots, \alpha_d$ be the roots of f in L, on which G acts by permutations. Let c_i denote the probability that a random element of G has exactly i fixed points.

Theorem (Chebotarëv, early 1920s)

For $i = 0, \dots, d$, $N_f(p) = i$ with probability c_i.

Consistency check: $N_f(p)$ can never equal $d - 1$, and $c_{d-1} = 0$.

Example: if d is large and $G = S_d$, then the probability that $N_f(p) = 0$ is roughly $1/e \cong 0.368$ by counting derangements.

---

*Not to be confused with his son .

The Chebotarëv  density theorem: first version

Let L be a splitting field of f, with Galois  group G. One only has a congruence formula for $N_f(p)$ when G is abelian, by Artin*  reciprocity.

But we can answer the probability question as follows. Let $\alpha_1, \dots, \alpha_d$ be the roots of f in L, on which G acts by permutations. Let c_i denote the probability that a random element of G has exactly i fixed points.

Theorem (Chebotarëv, early 1920s)

For $i = 0, \dots, d$, $N_f(p) = i$ with probability c_i.

Consistency check: $N_f(p)$ can never equal $d-1$, and $c_{d-1} = 0$.

Example: if d is large and $G = S_d$, then the probability that $N_f(p) = 0$ is roughly $1/e \cong 0.368$ by counting derangements.

*Not to be confused with his son .

The Chebotarëv density theorem: second version

For q a prime power, we may also define

$$N_f(q) = \#\{x \in \mathbb{F}_q : f(x) = 0\};$$

this agrees with the previous definition when q is prime.

Theorem (Chebotarëv, early 1920s)

For any $c_1, c_2, \ldots \in \{0, \ldots, d\}$, the probability that $N_f(p) = c_1, N_f(p^2) = c_2, \ldots$ equals the probability that a random element g of G has c_1 fixed points, g^2 has c_2 fixed points, and so on.

This theorem asserts strictly more than the previous version. For example, if $G = S_5$, (12345) and (123)(45) were previously counted in the same category (no fixed points) but are now separated.

The Chebotarëv density theorem: second version

For q a prime power, we may also define

$$N_f(q) = \#\{x \in \mathbb{F}_q : f(x) = 0\};$$

this agrees with the previous definition when q is prime.

Theorem (Chebotarëv, early 1920s)

For any $c_1, c_2, \ldots \in \{0, \ldots, d\}$, the probability that $N_f(p) = c_1, N_f(p^2) = c_2, \ldots$ equals the probability that a random element g of G has c_1 fixed points, g^2 has c_2 fixed points, and so on.

This theorem asserts strictly more than the previous version. For example, if $G = S_5$, (12345) and (123)(45) were previously counted in the same category (no fixed points) but are now separated.

The Chebotarëv density theorem: second version

For q a prime power, we may also define

$$N_f(q) = \#\{x \in \mathbb{F}_q : f(x) = 0\};$$

this agrees with the previous definition when q is prime.

Theorem (Chebotarëv, early 1920s)

For any $c_1, c_2, \ldots \in \{0, \ldots, d\}$, the probability that $N_f(p) = c_1, N_f(p^2) = c_2, \ldots$ equals the probability that a random element g of G has c_1 fixed points, g^2 has c_2 fixed points, and so on.

This theorem asserts strictly more than the previous version. For example, if $G = S_5$, (12345) and (123)(45) were previously counted in the same category (no fixed points) but are now separated.

The Chebotarëv density theorem: final version

View G as a probability space for the uniform distribution. View the set $\mathrm{Conj}(G)$ of conjugacy classes of G as a probability space for the image distribution (i.e., each class is weighted proportionally to its size).

With finitely many exceptions (the divisors of the discriminant of L), to each prime p we may associate a **Frobenius**  **class** $\mathrm{Frob}_p \in \mathrm{Conj}(G)$.

Theorem (Chebotarëv, early 1920s)

The Frob_p *are equidistributed for the image distribution on* $\mathrm{Conj}(G)$.

That is, for any function $g : \mathrm{Conj}(G) \to \mathbb{R}$,

$$\lim_{N\to\infty} \frac{1}{\pi(N)} \sum_{p \leq N} g(\mathrm{Frob}_p) = \int_{\mathrm{Conj}(G)} g \, d\mu.$$

Taking g to be the characteristic function of a singleton set, we recover the usual statement: each class occurs in proportion to its cardinality.

The Chebotarëv density theorem: final version

View G as a probability space for the uniform distribution. View the set Conj(G) of conjugacy classes of G as a probability space for the image distribution (i.e., each class is weighted proportionally to its size).

With finitely many exceptions (the divisors of the discriminant of L), to each prime p we may associate a **Frobenius**  **class** $\mathrm{Frob}_p \in \mathrm{Conj}(G)$.

Theorem (Chebotarëv, early 1920s)

The Frob_p *are equidistributed for the image distribution on* Conj(G).

That is, for any function $g : \mathrm{Conj}(G) \to \mathbb{R}$,

$$\lim_{N\to\infty} \frac{1}{\pi(N)} \sum_{p\leq N} g(\mathrm{Frob}_p) = \int_{\mathrm{Conj}(G)} g\, d\mu.$$

Taking g to be the characteristic function of a singleton set, we recover the usual statement: each class occurs in proportion to its cardinality.

The Chebotarëv density theorem: final version

View G as a probability space for the uniform distribution. View the set $\mathrm{Conj}(G)$ of conjugacy classes of G as a probability space for the image distribution (i.e., each class is weighted proportionally to its size).

With finitely many exceptions (the divisors of the discriminant of L), to each prime p we may associate a **Frobenius**  **class** $\mathrm{Frob}_p \in \mathrm{Conj}(G)$.

Theorem (Chebotarëv, early 1920s)

The Frob_p *are equidistributed for the image distribution on* $\mathrm{Conj}(G)$.

That is, for any function $g : \mathrm{Conj}(G) \to \mathbb{R}$,

$$\lim_{N\to\infty} \frac{1}{\pi(N)} \sum_{p \le N} g(\mathrm{Frob}_p) = \int_{\mathrm{Conj}(G)} g \, d\mu.$$

Taking g to be the characteristic function of a singleton set, we recover the usual statement: each class occurs in proportion to its cardinality.

The Chebotarëv density theorem: final version

View G as a probability space for the uniform distribution. View the set $\mathrm{Conj}(G)$ of conjugacy classes of G as a probability space for the image distribution (i.e., each class is weighted proportionally to its size).

With finitely many exceptions (the divisors of the discriminant of L), to each prime p we may associate a **Frobenius**  **class** $\mathrm{Frob}_p \in \mathrm{Conj}(G)$.

Theorem (Chebotarëv, early 1920s)

The Frob_p *are equidistributed for the image distribution on* $\mathrm{Conj}(G)$*.*

That is, for any function $g : \mathrm{Conj}(G) \to \mathbb{R}$,

$$\lim_{N\to\infty} \frac{1}{\pi(N)} \sum_{p \leq N} g(\mathrm{Frob}_p) = \int_{\mathrm{Conj}(G)} g \, d\mu.$$

Taking g to be the characteristic function of a singleton set, we recover the usual statement: each class occurs in proportion to its cardinality.

The Chebotarëv density theorem: final version

View G as a probability space for the uniform distribution. View the set Conj(G) of conjugacy classes of G as a probability space for the image distribution (i.e., each class is weighted proportionally to its size).

With finitely many exceptions (the divisors of the discriminant of L), to each prime p we may associate a **Frobenius**  **class** $\mathrm{Frob}_p \in \mathrm{Conj}(G)$.

Theorem (Chebotarëv, early 1920s)

The Frob_p *are equidistributed for the image distribution on* Conj(G).

That is, for any function $g : \mathrm{Conj}(G) \to \mathbb{R}$,

$$\lim_{N\to\infty} \frac{1}{\pi(N)} \sum_{p \leq N} g(\mathrm{Frob}_p) = \int_{\mathrm{Conj}(G)} g \, d\mu.$$

Taking g to be the characteristic function of a singleton set, we recover the usual statement: each class occurs in proportion to its cardinality.

One final note

For an element g of S_d, the data of the numbers of fixed points of $g, g^2, \ldots$ is equivalent to the cycle structure, and hence in turn to the conjugacy class. Thus when $G = S_d$, the second and third versions of Chebotarëv density are equivalent.

However, for a general (even transitive) subgroup G of S_d, the map $\mathrm{Conj}(G) \to \mathrm{Conj}(S_d)$ is not injective, so the final version of Chebotarëv density carries strictly more information. For example, if G is cyclic, then $\mathrm{Conj}(G) = G$ but any two generators are conjugate in S_d.

One final note

For an element g of S_d, the data of the numbers of fixed points of $g, g^2, \dots$ is equivalent to the cycle structure, and hence in turn to the conjugacy class. Thus when $G = S_d$, the second and third versions of Chebotarëv density are equivalent.

However, for a general (even transitive) subgroup G of S_d, the map $\mathrm{Conj}(G) \to \mathrm{Conj}(S_d)$ is not injective, so the final version of Chebotarëv density carries strictly more information. For example, if G is cyclic, then $\mathrm{Conj}(G) = G$ but any two generators are conjugate in S_d.

Contents

L-polynomials of an elliptic curve

For E an elliptic curve over a number field K, and $\mathfrak{p}$ a prime ideal of $\mathfrak{o}_K$ at which E has good reduction, the L-**polynomial** of E at $\mathfrak{p}$ is

$$L(E_{\mathfrak{p}}, T) := 1 - a_{\mathfrak{p}}(E)T + qT^2 \qquad (q = \mathrm{Norm}(\mathfrak{p}))$$

where $a_{\mathfrak{p}}(E) = q + 1 - \#E(\mathfrak{o}_K/\mathfrak{p})$ is the trace of Frobenius.

In some key examples, one can give an explicit formula for $L(E_{\mathfrak{p}}, T)$. E.g., the final entry of Gauss's  notebooks is a formula for $L(E_{\mathfrak{p}}, T)$ for the curve $y^2 = x^3 - x$ over $\mathbb{Q}(i)$, later generalized by Hecke  to any elliptic curve with **complex multiplication** (CM).

One key point: if E has CM by the imaginary quadratic field M and $M \not\subseteq K$, then $a_{\mathfrak{p}}(E) = 0$ for all primes $\mathfrak{p}$ that remain inert in KM.

L-polynomials of an elliptic curve

For E an elliptic curve over a number field K, and $\mathfrak{p}$ a prime ideal of $\mathfrak{o}_K$ at which E has good reduction, the L-**polynomial** of E at $\mathfrak{p}$ is

$$L(E_{\mathfrak{p}}, T) := 1 - a_{\mathfrak{p}}(E)T + qT^2 \qquad (q = \mathrm{Norm}(\mathfrak{p}))$$

where $a_{\mathfrak{p}}(E) = q + 1 - \#E(\mathfrak{o}_K/\mathfrak{p})$ is the trace of Frobenius.

In some key examples, one can give an explicit formula for $L(E_{\mathfrak{p}}, T)$. E.g., the final entry of Gauss's  notebooks is a formula for $L(E_{\mathfrak{p}}, T)$ for the curve $y^2 = x^3 - x$ over $\mathbb{Q}(i)$, later generalized by Hecke  to any elliptic curve with **complex multiplication** (CM).

One key point: if E has CM by the imaginary quadratic field M and $M \not\subseteq K$, then $a_{\mathfrak{p}}(E) = 0$ for all primes $\mathfrak{p}$ that remain inert in KM.

L-polynomials of an elliptic curve

For E an elliptic curve over a number field K, and $\mathfrak{p}$ a prime ideal of $\mathfrak{o}_K$ at which E has good reduction, the L-**polynomial** of E at $\mathfrak{p}$ is

$$L(E_\mathfrak{p}, T) := 1 - a_\mathfrak{p}(E)T + qT^2 \qquad (q = \mathrm{Norm}(\mathfrak{p}))$$

where $a_\mathfrak{p}(E) = q + 1 - \#E(\mathfrak{o}_K/\mathfrak{p})$ is the trace of Frobenius.

In some key examples, one can give an explicit formula for $L(E_\mathfrak{p}, T)$. E.g., the final entry of Gauss's  notebooks is a formula for $L(E_\mathfrak{p}, T)$ for the curve $y^2 = x^3 - x$ over $\mathbb{Q}(i)$, later generalized by Hecke  to any elliptic curve with **complex multiplication** (CM).

One key point: if E has CM by the imaginary quadratic field M and $M \not\subseteq K$, then $a_\mathfrak{p}(E) = 0$ for all primes $\mathfrak{p}$ that remain inert in KM.

The Sato-Tate conjecture

Suppose E does *not* have CM. Then $a_{\mathfrak{p}}(E)$ depends on $\mathfrak{p}$ in an apparently mysterious fashion, though modularity puts some method in it (see below).

However, Hasse  showed that $|a_{\mathfrak{p}}(E)| \leq 2q^{1/2}$. We then ask how $q^{-1/2}a_{\mathfrak{p}}(E)$ is distributed in $[-2, 2]$ as $\mathfrak{p}$ varies.

Conjecture (Sato  and Tate , early 1960s)

The quantities $q^{-1/2}a_{\mathfrak{p}}(E)$ are equidistributed in $[-2, 2]$ for the "semicircular" measure $\mu(x) = \frac{1}{2\pi}\sqrt{4 - x^2}$.

Sato and Tate arrived at this by different combinations of theoretical and numerical evidence (the latter for primes up to 15000; see this pdf, pp. 41–42). Sutherland  has much stronger numerical evidence.

The Sato-Tate conjecture

Suppose E does *not* have CM. Then $a_{\mathfrak{p}}(E)$ depends on $\mathfrak{p}$ in an apparently mysterious fashion, though modularity puts some method in it (see below).

However, Hasse  showed that $|a_{\mathfrak{p}}(E)| \leq 2q^{1/2}$. We then ask how $q^{-1/2}a_{\mathfrak{p}}(E)$ is distributed in $[-2,2]$ as $\mathfrak{p}$ varies.

Conjecture (Sato  and Tate , early 1960s)

The quantities $q^{-1/2}a_{\mathfrak{p}}(E)$ are equidistributed in $[-2,2]$ for the "semicircular" measure $\mu(x) = \frac{1}{2\pi}\sqrt{4-x^2}$.

Sato and Tate arrived at this by different combinations of theoretical and numerical evidence (the latter for primes up to 15000; see this pdf, pp. 41–42). Sutherland  has much stronger numerical evidence.

The Sato-Tate conjecture

Suppose E does *not* have CM. Then $a_{\mathfrak{p}}(E)$ depends on $\mathfrak{p}$ in an apparently mysterious fashion, though modularity puts some method in it (see below).

However, Hasse  showed that $|a_{\mathfrak{p}}(E)| \leq 2q^{1/2}$. We then ask how $q^{-1/2}a_{\mathfrak{p}}(E)$ is distributed in $[-2, 2]$ as $\mathfrak{p}$ varies.

Conjecture (Sato  and Tate , early 1960s)

The quantities $q^{-1/2}a_{\mathfrak{p}}(E)$ are equidistributed in $[-2, 2]$ for the "semicircular" measure $\mu(x) = \frac{1}{2\pi}\sqrt{4 - x^2}$.

Sato and Tate arrived at this by different combinations of theoretical and numerical evidence (the latter for primes up to 15000; see this pdf, pp. 41–42). Sutherland  has much stronger numerical evidence.

The Sato-Tate conjecture

Suppose E does *not* have CM. Then $a_{\mathfrak{p}}(E)$ depends on $\mathfrak{p}$ in an apparently mysterious fashion, though modularity puts some method in it (see below).

However, Hasse  showed that $|a_{\mathfrak{p}}(E)| \leq 2q^{1/2}$. We then ask how $q^{-1/2}a_{\mathfrak{p}}(E)$ is distributed in $[-2, 2]$ as $\mathfrak{p}$ varies.

Conjecture (Sato  and Tate , early 1960s)

The quantities $q^{-1/2}a_{\mathfrak{p}}(E)$ *are equidistributed in* $[-2, 2]$ *for the "semicircular" measure* $\mu(x) = \frac{1}{2\pi}\sqrt{4 - x^2}$.

Sato and Tate arrived at this by different combinations of theoretical and numerical evidence (the latter for primes up to 15000; see this pdf, pp. 41–42). Sutherland  has much stronger numerical evidence.

Progress on the Sato-Tate conjecture

The Sato-Tate conjecture is known:

- for $K = \mathbb{Q}$ by Clozel , Harris , Shepherd-Barron* , and Taylor ;
- for K totally real by Barnet-Lamb , Geraghty , and Gee ;
- for K a CM field† by Allen , Calegari , Caraiani , Gee, Helm , Le Hung , Newton , Scholze , Taylor, and Thorne .

These are all results on (potential) modularity/automorphy of Galois representations, of the sort pioneered by Wiles  (mid 1990s). More on the connection later.

---

*Not to be confused with his father .

†A **CM field** is a totally imaginary quadratic extension of a totally real number field. E.g., any imaginary quadratic field.

Progress on the Sato-Tate conjecture

The Sato-Tate conjecture is known:

- for $K = \mathbb{Q}$ by Clozel , Harris , Shepherd-Barron[*] , and Taylor ;
- for K totally real by Barnet-Lamb , Geraghty , and Gee ;
- for K a CM field[†] by Allen , Calegari , Caraiani , Gee, Helm , Le Hung , Newton , Scholze , Taylor, and Thorne .

These are all results on (potential) modularity/automorphy of Galois representations, of the sort pioneered by Wiles  (mid 1990s). More on the connection later.

---

[*]Not to be confused with his father .

[†]A **CM field** is a totally imaginary quadratic extension of a totally real number field. E.g., any imaginary quadratic field.

Progress on the Sato-Tate conjecture

The Sato-Tate conjecture is known:

- for $K = \mathbb{Q}$ by Clozel , Harris , Shepherd-Barron* , and Taylor ;
- for K totally real by Barnet-Lamb , Geraghty , and Gee ;
- for K a CM field† by Allen , Calegari , Caraiani , Gee, Helm , Le Hung , Newton , Scholze , Taylor, and Thorne .

These are all results on (potential) modularity/automorphy of Galois representations, of the sort pioneered by Wiles  (mid 1990s). More on the connection later.

---

*Not to be confused with his father .

†A **CM field** is a totally imaginary quadratic extension of a totally real number field. E.g., any imaginary quadratic field.

Progress on the Sato-Tate conjecture

The Sato-Tate conjecture is known:

- for $K = \mathbb{Q}$ by Clozel , Harris , Shepherd-Barron* , and Taylor ;
- for K totally real by Barnet-Lamb , Geraghty , and Gee ;
- for K a CM field† by Allen , Calegari , Caraiani , Gee, Helm , Le Hung , Newton , Scholze , Taylor, and Thorne .

These are all results on (potential) modularity/automorphy of Galois representations, of the sort pioneered by Wiles  (mid 1990s). More on the connection later.

---

*Not to be confused with his father .

†A **CM field** is a totally imaginary quadratic extension of a totally real number field. E.g., any imaginary quadratic field.

Averaging in the other direction

One can also average in the other direction: fix a finite field $\mathbb{F}_q$, average over all elliptic curves over that field, then take the limit as $q \to \infty$. In this direction, a statement about convergence to the Sato-Tate distribution was proved by Birch .

For this type of averaging, one can go much further; various examples can be found in the book of Katz  and Sarnak , based on Deligne's  equidistribution theorem (part of his second proof of the **Weil**  **conjectures**).

Averaging in the other direction

One can also average in the other direction: fix a finite field $\mathbb{F}_q$, average over all elliptic curves over that field, then take the limit as $q \to \infty$. In this direction, a statement about convergence to the Sato-Tate distribution was proved by Birch .

For this type of averaging, one can go much further; various examples can be found in the book of Katz  and Sarnak , based on Deligne's  equidistribution theorem (part of his second proof of the **Weil**  **conjectures**).

Contents

L-polynomials of algebraic varieties

Let X be a smooth proper variety over K. For each $\mathfrak{p}$ at which X has good reduction, the zeta function of the reduction $X_{\mathfrak{p}}$ factors* as

$$Z(X_{\mathfrak{p}}, T) = \frac{L_1(X_{\mathfrak{p}}, T) \cdots L_{2d-1}(X_{\mathfrak{p}}, T)}{L_0(X_{\mathfrak{p}}, T) \cdots L_{2d}(X_{\mathfrak{p}}, T)} \qquad (d = \dim X)$$

where $L_i \in \mathbb{Z}[T]$ has degree b_i (the i-th Betti  number of $X_{\mathbb{C}}$), constant term 1, and all $\mathbb{C}$-roots on the circle $|T| = q^{-i/2}$.

E.g., for X an abelian variety, for L the reverse charpoly of Frobenius,

$$L_i(X_{\mathfrak{p}}, T) = \wedge^i L(X_{\mathfrak{p}}, T)$$

i.e., the roots of L_i are i-fold products of roots of L.

*These properties follow from the Weil conjectures, as resolved by the work of Dwork , Grothendieck , Deligne, etc.

L-polynomials of algebraic varieties

Let X be a smooth proper variety over K. For each $\mathfrak{p}$ at which X has good reduction, the zeta function of the reduction $X_{\mathfrak{p}}$ factors* as

$$Z(X_{\mathfrak{p}}, T) = \frac{L_1(X_{\mathfrak{p}}, T) \cdots L_{2d-1}(X_{\mathfrak{p}}, T)}{L_0(X_{\mathfrak{p}}, T) \cdots L_{2d}(X_{\mathfrak{p}}, T)} \qquad (d = \dim X)$$

where $L_i \in \mathbb{Z}[T]$ has degree b_i (the i-th Betti  number of $X_{\mathbb{C}}$), constant term 1, and all $\mathbb{C}$-roots on the circle $|T| = q^{-i/2}$.

E.g., for X an abelian variety, for L the reverse charpoly of Frobenius,

$$L_i(X_{\mathfrak{p}}, T) = \wedge^i L(X_{\mathfrak{p}}, T)$$

i.e., the roots of L_i are i-fold products of roots of L.

---

*These properties follow from the Weil conjectures, as resolved by the work of Dwork , Grothendieck , Deligne, etc.

A generalized Sato-Tate conjecture

Fix X and i. The renormalized polynomials $\overline{L}_i(X_\mathfrak{p}, T) = L_i(X_\mathfrak{p}, q^{-i/2}T)$ have $\mathbb{C}$-roots of norm 1, so they sit in a compact subset of $\mathbb{R}^d$.

Conjecture (Serre , mid-1990s)

There exists a compact Lie  group $G \subseteq \mathrm{U}(b_i)$ such that the $\overline{L}_i(X_\mathfrak{p}, T)$ are equidistributed for the image of Haar  measure on G via charpoly.

That is, the $\overline{L}_i(X_\mathfrak{p}, T)$ "look statistically like random matrices in G." Such models have a long history in number theory, starting with Montgomery's  use of eigenvalues of random matrices to model ζ-zeroes.

In case* $K = \mathbb{Q}$ and $X = \operatorname{Spec} L$, for $L'/\mathbb{Q}$ the Galois closure, Chebotarëv density implies Serre's conjecture for $G = \mathrm{Gal}(L'/\mathbb{Q})$ embedded in $\mathrm{U}([L : \mathbb{Q}])$ via the permutation representation.

*I never said X had to be geometrically irreducible!

A generalized Sato-Tate conjecture

Fix X and i. The renormalized polynomials $\overline{L}_i(X_{\mathfrak{p}}, T) = L_i(X_{\mathfrak{p}}, q^{-i/2}T)$ have $\mathbb{C}$-roots of norm 1, so they sit in a compact subset of $\mathbb{R}^d$.

Conjecture (Serre , mid-1990s)

There exists a compact Lie  group $G \subseteq \mathrm{U}(b_i)$ such that the $\overline{L}_i(X_{\mathfrak{p}}, T)$ are equidistributed for the image of Haar  measure on G via charpoly.

That is, the $\overline{L}_i(X_{\mathfrak{p}}, T)$ "look statistically like random matrices in G." Such models have a long history in number theory, starting with Montgomery's  use of eigenvalues of random matrices to model ζ-zeroes.

In case* $K = \mathbb{Q}$ and $X = \operatorname{Spec} L$, for $L'/\mathbb{Q}$ the Galois closure, Chebotarëv density implies Serre's conjecture for $G = \mathrm{Gal}(L'/\mathbb{Q})$ embedded in $\mathrm{U}([L:\mathbb{Q}])$ via the permutation representation.

*I never said X had to be geometrically irreducible!

A generalized Sato-Tate conjecture

Fix X and i. The renormalized polynomials $\overline{L}_i(X_{\mathfrak{p}}, T) = L_i(X_{\mathfrak{p}}, q^{-i/2}T)$ have $\mathbb{C}$-roots of norm 1, so they sit in a compact subset of $\mathbb{R}^d$.

Conjecture (Serre , mid-1990s)

There exists a compact Lie  *group* $G \subseteq \mathrm{U}(b_i)$ *such that the* $\overline{L}_i(X_{\mathfrak{p}}, T)$ *are equidistributed for the image of Haar*  *measure on* G *via charpoly.*

That is, the $\overline{L}_i(X_{\mathfrak{p}}, T)$ "look statistically like random matrices in G." Such models have a long history in number theory, starting with Montgomery's  use of eigenvalues of random matrices to model ζ-zeroes.

In case* $K = \mathbb{Q}$ and $X = \operatorname{Spec} L$, for $L'/\mathbb{Q}$ the Galois closure, Chebotarëv density implies Serre's conjecture for $G = \mathrm{Gal}(L'/\mathbb{Q})$ embedded in $\mathrm{U}([L : \mathbb{Q}])$ via the permutation representation.

*I never said X had to be geometrically irreducible!

A generalized Sato-Tate conjecture

Fix X and i. The renormalized polynomials $\overline{L}_i(X_{\mathfrak{p}}, T) = L_i(X_{\mathfrak{p}}, q^{-i/2}T)$ have $\mathbb{C}$-roots of norm 1, so they sit in a compact subset of $\mathbb{R}^d$.

Conjecture (Serre , mid-1990s)

There exists a compact Lie  *group* $G \subseteq \mathrm{U}(b_i)$ *such that the* $\overline{L}_i(X_{\mathfrak{p}}, T)$ *are equidistributed for the image of Haar*  *measure on* G *via charpoly.*

That is, the $\overline{L}_i(X_{\mathfrak{p}}, T)$ "look statistically like random matrices in G." Such models have a long history in number theory, starting with Montgomery's  use of eigenvalues of random matrices to model ζ-zeroes.

In case* $K = \mathbb{Q}$ and $X = \operatorname{Spec} L$, for $L'/\mathbb{Q}$ the Galois closure, Chebotarëv density implies Serre's conjecture for $G = \mathrm{Gal}(L'/\mathbb{Q})$ embedded in $\mathrm{U}([L:\mathbb{Q}])$ via the permutation representation.

*I never said X had to be geometrically irreducible!

Example: elliptic curves

Let X be an elliptic curve and take $i = 1$.

- If X has no CM, then the Sato-Tate conjecture is equivalent to Serre's conjecture with $G = \mathrm{SU}(2)$.
- If X has CM by a subfield of K, then Hecke's formula implies Serre's conjecture for $G = \mathrm{SO}(2)$.
- If X has CM by a quadratic field not contained in K, then Hecke's formula implies Serre's conjecture with G equal to the normalizer of $\mathrm{SO}(2)$ in $\mathrm{SU}(2)$. This group has two connected components; on the non-identity component, the trace is identically 0.

See here for animated examples.

Example: elliptic curves

Let X be an elliptic curve and take $i = 1$.

- If X has no CM, then the Sato-Tate conjecture is equivalent to Serre's conjecture with $G = \mathrm{SU}(2)$.
- If X has CM by a subfield of K, then Hecke's formula implies Serre's conjecture for $G = \mathrm{SO}(2)$.
- If X has CM by a quadratic field not contained in K, then Hecke's formula implies Serre's conjecture with G equal to the normalizer of $\mathrm{SO}(2)$ in $\mathrm{SU}(2)$. This group has two connected components; on the non-identity component, the trace is identically 0.

See here for animated examples.

Example: elliptic curves

Let X be an elliptic curve and take $i = 1$.

- If X has no CM, then the Sato-Tate conjecture is equivalent to Serre's conjecture with $G = \mathrm{SU}(2)$.
- If X has CM by a subfield of K, then Hecke's formula implies Serre's conjecture for $G = \mathrm{SO}(2)$.
- If X has CM by a quadratic field not contained in K, then Hecke's formula implies Serre's conjecture with G equal to the normalizer of $\mathrm{SO}(2)$ in $\mathrm{SU}(2)$. This group has two connected components; on the non-identity component, the trace is identically 0.

See here for animated examples.

Example: elliptic curves

Let X be an elliptic curve and take $i = 1$.

- If X has no CM, then the Sato-Tate conjecture is equivalent to Serre's conjecture with $G = \mathrm{SU}(2)$.
- If X has CM by a subfield of K, then Hecke's formula implies Serre's conjecture for $G = \mathrm{SO}(2)$.
- If X has CM by a quadratic field not contained in K, then Hecke's formula implies Serre's conjecture with G equal to the normalizer of $\mathrm{SO}(2)$ in $\mathrm{SU}(2)$. This group has two connected components; on the non-identity component, the trace is identically 0.

See here for animated examples.

Example: elliptic curves

Let X be an elliptic curve and take $i = 1$.

- If X has no CM, then the Sato-Tate conjecture is equivalent to Serre's conjecture with $G = \mathrm{SU}(2)$.
- If X has CM by a subfield of K, then Hecke's formula implies Serre's conjecture for $G = \mathrm{SO}(2)$.
- If X has CM by a quadratic field not contained in K, then Hecke's formula implies Serre's conjecture with G equal to the normalizer of $\mathrm{SO}(2)$ in $\mathrm{SU}(2)$. This group has two connected components; on the non-identity component, the trace is identically 0.

See here for animated examples.

Equidistribution for conjugacy classes

As with Chebotarëv density, the true conjecture of Serre is more precise.

- One can give a specific* candidate for G, which we call the **Sato-Tate group** associated to the **motive**† of X in degree i.
- For each prime $\mathfrak{p}$ of good reduction for X, we get a class $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Conj}(G)$ with charpoly $\overline{L}_i(X_{\mathfrak{p}}, T)$. The precise conjecture is that these classes are equidistributed for the image of Haar measure.

Again, equidistribution on $\mathrm{Conj}(G)$ is stronger than equidistribution of charpolys. For example, two abelian threefolds can have the same distribution without having isomorphic Sato-Tate groups.

---

*Serre's description is conditional on various "standard conjectures" about motives. It can be made unconditional in various cases, such as for abelian varieties satisfying the Mumford -Tate conjecture; this has done by Banaszak  and K.

†Never mind what this, except that any decomposition of G as a linear group corresponds to a factorization of the motive. And for orthogonal motives of even weight, the whole story lifts to a suitable double cover group.

Equidistribution for conjugacy classes

As with Chebotarëv density, the true conjecture of Serre is more precise.

- One can give a specific* candidate for G, which we call the **Sato-Tate group** associated to the **motive**† of X in degree i.
- For each prime $\mathfrak{p}$ of good reduction for X, we get a class $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Conj}(G)$ with charpoly $\overline{L}_i(X_{\mathfrak{p}}, T)$. The precise conjecture is that these classes are equidistributed for the image of Haar measure.

Again, equidistribution on $\mathrm{Conj}(G)$ is stronger than equidistribution of charpolys. For example, two abelian threefolds can have the same distribution without having isomorphic Sato-Tate groups.

---

*Serre's description is conditional on various "standard conjectures" about motives. It can be made unconditional in various cases, such as for abelian varieties satisfying the Mumford  -Tate conjecture; this has done by Banaszak  and K.

†Never mind what this, except that any decomposition of G as a linear group corresponds to a factorization of the motive. And for orthogonal motives of even weight, the whole story lifts to a suitable double cover group.

Equidistribution for conjugacy classes

As with Chebotarëv density, the true conjecture of Serre is more precise.

- One can give a specific* candidate for G, which we call the **Sato-Tate group** associated to the **motive**† of X in degree i.
- For each prime $\mathfrak{p}$ of good reduction for X, we get a class $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Conj}(G)$ with charpoly $\overline{L}_i(X_{\mathfrak{p}}, T)$. The precise conjecture is that these classes are equidistributed for the image of Haar measure.

Again, equidistribution on $\mathrm{Conj}(G)$ is stronger than equidistribution of charpolys. For example, two abelian threefolds can have the same distribution without having isomorphic Sato-Tate groups.

---

*Serre's description is conditional on various "standard conjectures" about motives. It can be made unconditional in various cases, such as for abelian varieties satisfying the Mumford -Tate conjecture; this has done by Banaszak  and K.

†Never mind what this, except that any decomposition of G as a linear group corresponds to a factorization of the motive. And for orthogonal motives of even weight, the whole story lifts to a suitable double cover group.

Equidistribution for conjugacy classes

As with Chebotarëv density, the true conjecture of Serre is more precise.

- One can give a specific* candidate for G, which we call the **Sato-Tate group** associated to the **motive**† of X in degree i.
- For each prime $\mathfrak{p}$ of good reduction for X, we get a class $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Conj}(G)$ with charpoly $\overline{L}_i(X_{\mathfrak{p}}, T)$. The precise conjecture is that these classes are equidistributed for the image of Haar measure.

Again, equidistribution on $\mathrm{Conj}(G)$ is stronger than equidistribution of charpolys. For example, two abelian threefolds can have the same distribution without having isomorphic Sato-Tate groups.

---

*Serre's description is conditional on various "standard conjectures" about motives. It can be made unconditional in various cases, such as for abelian varieties satisfying the Mumford  -Tate conjecture; this has done by Banaszak  and K.

†Never mind what this, except that any decomposition of G as a linear group corresponds to a factorization of the motive. And for orthogonal motives of even weight, the whole story lifts to a suitable double cover group.

The connected part of the Sato-Tate group

There is a canonical exact sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1$$

where G° is the identity component (and hence connected) and $\pi_0(G)$ is the component group (and hence finite).

The group G° depends only on $X_{\overline{\mathbb{Q}}}$. It can be read from the Hodge  structure of X or the **Mumford-Tate group**, which conjecturally controls the action of Galois on étale cohomology.

The connected part of the Sato-Tate group

There is a canonical exact sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1$$

where G° is the identity component (and hence connected) and $\pi_0(G)$ is the component group (and hence finite).

The group G° depends only on $X_{\overline{\mathbb{Q}}}$. It can be read from the Hodge  structure of X or the **Mumford-Tate group**, which conjecturally controls the action of Galois on étale cohomology.

The finite part of the Sato-Tate group

In the canonical exact sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1$$

the group $\pi_0(G)$ is naturally identified with $\mathrm{Gal}(L/K)$ for some number field. This description is compatible with base extension: if K' is a number field containing K, then the Sato-Tate group of $X_{K'}$ is the preimage of $\mathrm{Gal}(LK'/K') \subseteq \mathrm{Gal}(L/K) \cong \pi_0(G)$ in G.

For $X = A$ an abelian variety, L contains* the **endomorphism field** of A (the minimal number field F with $\mathrm{End}(A_F) = \mathrm{End}(A_{\overline{\mathbb{Q}}})$).

E.g., for an elliptic curve with CM by M, $F = L = MK$.

---

*The containment gives an upper bound on $[F : K]$ which is optimal with respect to divisibility. This was shown by Guralnick  and K, building on work of Silverberg . Equality holds in many cases, including all of dimension ≤ 3.

The finite part of the Sato-Tate group

In the canonical exact sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1$$

the group $\pi_0(G)$ is naturally identified with $\mathrm{Gal}(L/K)$ for some number field. This description is compatible with base extension: if K' is a number field containing K, then the Sato-Tate group of $X_{K'}$ is the preimage of $\mathrm{Gal}(LK'/K') \subseteq \mathrm{Gal}(L/K) \cong \pi_0(G)$ in G.

For $X = A$ an abelian variety, L contains* the **endomorphism field** of A (the minimal number field F with $\mathrm{End}(A_F) = \mathrm{End}(A_{\overline{\mathbb{Q}}})$).

E.g., for an elliptic curve with CM by M, $F = L = MK$.

*The containment gives an upper bound on $[F : K]$ which is optimal with respect to divisibility. This was shown by Guralnick  and K, building on work of Silverberg . Equality holds in many cases, including all of dimension ≤ 3.

The finite part of the Sato-Tate group

In the canonical exact sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1$$

the group $\pi_0(G)$ is naturally identified with $\mathrm{Gal}(L/K)$ for some number field. This description is compatible with base extension: if K' is a number field containing K, then the Sato-Tate group of $X_{K'}$ is the preimage of $\mathrm{Gal}(LK'/K') \subseteq \mathrm{Gal}(L/K) \cong \pi_0(G)$ in G.

For $X = A$ an abelian variety, L contains* the **endomorphism field** of A (the minimal number field F with $\mathrm{End}(A_F) = \mathrm{End}(A_{\overline{\mathbb{Q}}})$).

E.g., for an elliptic curve with CM by M, $F = L = MK$.

---

*The containment gives an upper bound on $[F : K]$ which is optimal with respect to divisibility. This was shown by Guralnick  and K, building on work of Silverberg . Equality holds in many cases, including all of dimension ≤ 3.

Contents

Reminder: the prime number theorem

Theorem (Hadamard  and de la Vallée Poussin , around 1900)

We have

$$\sum_{p \leq N} \log p \sim N.$$

The proof uses that in the region $\mathrm{Re}(s) \geq 1$, the Riemann  zeta function

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}$$

has a simple pole at $s = 1$ with residue 1 and no other zeroes or poles.

Establishing an error term of the form $O(N^{1-\epsilon})$ amounts to proving that ζ has no more zeroes or poles in $\mathrm{Re}(s) \geq 1 - \epsilon$. In particular, the Riemann hypothesis (RH) predicts an error bound of $O(N^{1/2+\epsilon})$.

Reminder: the prime number theorem

Theorem (Hadamard  and de la Vallée Poussin , around 1900)

We have

$$\sum_{p \leq N} \log p \sim N.$$

The proof uses that in the region $\mathrm{Re}(s) \geq 1$, the Riemann  zeta function

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}$$

has a simple pole at $s = 1$ with residue 1 and no other zeroes or poles.

Establishing an error term of the form $O(N^{1-\epsilon})$ amounts to proving that ζ has no more zeroes or poles in $\mathrm{Re}(s) \geq 1 - \epsilon$. In particular, the Riemann hypothesis (RH) predicts an error bound of $O(N^{1/2+\epsilon})$.

Reminder: the prime number theorem

Theorem (Hadamard  and de la Vallée Poussin , around 1900)

We have

$$\sum_{p \leq N} \log p \sim N.$$

The proof uses that in the region $\mathrm{Re}(s) \geq 1$, the Riemann  zeta function

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}$$

has a simple pole at $s = 1$ with residue 1 and no other zeroes or poles.

Establishing an error term of the form $O(N^{1-\epsilon})$ amounts to proving that ζ has no more zeroes or poles in $\mathrm{Re}(s) \geq 1 - \epsilon$. In particular, the Riemann hypothesis (RH) predicts an error bound of $O(N^{1/2+\epsilon})$.

L-functions and the Sato-Tate conjecture

Serre observed that similar logic applies to the generalized Sato-Tate conjecture: for G a compact Lie group and $g_{\mathfrak{p}} \in \mathrm{Conj}(G)$, if for each nontrivial irreducible $\mathbb{C}$-linear representation ρ of G, the "L-function"

$$\prod_{\mathfrak{p}} \det(1 - \rho(g_{\mathfrak{p}}) \,\mathrm{Norm}(\mathfrak{p})^{-s})^{-1}$$

is holomorphic and nonvanishing on $\mathrm{Re}(s) \geq 1$, then the $g_{\mathfrak{p}}$ are equidistributed for the image of Haar measure.

This gives one of the standard approaches to Chebotarëv density, using Dirichlet L-functions. It is also the approach used to prove Sato-Tate in the known cases, using potential automorphy of the symmetric power L-functions (these corresponding to the irreps of SU(2)).

L-functions and the Sato-Tate conjecture

Serre observed that similar logic applies to the generalized Sato-Tate conjecture: for G a compact Lie group and $g_{\mathfrak{p}} \in \mathrm{Conj}(G)$, if for each nontrivial irreducible $\mathbb{C}$-linear representation ρ of G, the "L-function"

$$\prod_{\mathfrak{p}} \det(1 - \rho(g_{\mathfrak{p}})\,\mathrm{Norm}(\mathfrak{p})^{-s})^{-1}$$

is holomorphic and nonvanishing on $\mathrm{Re}(s) \geq 1$, then the $g_{\mathfrak{p}}$ are equidistributed for the image of Haar measure.

This gives one of the standard approaches to Chebotarëv density, using Dirichlet L-functions. It is also the approach used to prove Sato-Tate in the known cases, using potential automorphy of the symmetric power L-functions (these corresponding to the irreps of SU(2)).

Effective bounds under GRH

Using Serre's approach, if one is willing to assume both analytic continuation *and* the analogue of RH for the appropriate L-functions, one obtains an error bound as for the prime number theorem.

- For Chebotarëv density, this is due to Lagarias  and Odlyzko .
- For Sato-Tate, this is due to (Kumar)* Murty .
- In the general case, this is due to Bucur  and K, and in a more refined form to Bucur, Fité , and K.

---

*Not to be confused with his brother .

Effective bounds under GRH

Using Serre's approach, if one is willing to assume both analytic continuation *and* the analogue of RH for the appropriate L-functions, one obtains an error bound as for the prime number theorem.

- For Chebotarëv density, this is due to Lagarias  and Odlyzko .
- For Sato-Tate, this is due to (Kumar)* Murty .
- In the general case, this is due to Bucur  and K, and in a more refined form to Bucur, Fité , and K.

*Not to be confused with his brother .

Effective bounds under GRH

Using Serre's approach, if one is willing to assume both analytic continuation *and* the analogue of RH for the appropriate L-functions, one obtains an error bound as for the prime number theorem.

- For Chebotarëv density, this is due to Lagarias  and Odlyzko .
- For Sato-Tate, this is due to (Kumar)* Murty .
- In the general case, this is due to Bucur  and K, and in a more refined form to Bucur, Fité , and K.

*Not to be confused with his brother .

Effective bounds under GRH

Using Serre's approach, if one is willing to assume both analytic continuation *and* the analogue of RH for the appropriate L-functions, one obtains an error bound as for the prime number theorem.

- For Chebotarëv density, this is due to Lagarias  and Odlyzko .
- For Sato-Tate, this is due to (Kumar)* Murty .
- In the general case, this is due to Bucur  and K, and in a more refined form to Bucur, Fité , and K.

*Not to be confused with his brother .

Contents

Abelian varieties of low dimension

The classification of Sato-Tate groups is known for abelian varieties of dimension ≤ 3.

- In dimension 1, we have seen the three cases already (no CM, CM within the base field, CM not within the base field).
- In dimension 2, there are 52 groups as shown by Fité, K, Rotger , and Sutherland; there are 6 options for the identity component. These all occur for genus 2 curves as well.
- In dimension 3, there are 410 groups as shown by Fité, K, and Sutherland; there are 14 options for the connected component. It is not yet known which of these occur for genus 3 curves.

Abelian varieties of low dimension

The classification of Sato-Tate groups is known for abelian varieties of dimension ≤ 3.

- In dimension 1, we have seen the three cases already (no CM, CM within the base field, CM not within the base field).
- In dimension 2, there are 52 groups as shown by Fité, K, Rotger , and Sutherland; there are 6 options for the identity component. These all occur for genus 2 curves as well.
- In dimension 3, there are 410 groups as shown by Fité, K, and Sutherland; there are 14 options for the connected component. It is not yet known which of these occur for genus 3 curves.

Abelian varieties of low dimension

The classification of Sato-Tate groups is known for abelian varieties of dimension ≤ 3.

- In dimension 1, we have seen the three cases already (no CM, CM within the base field, CM not within the base field).
- In dimension 2, there are 52 groups as shown by Fité, K, Rotger , and Sutherland; there are 6 options for the identity component. These all occur for genus 2 curves as well.
- In dimension 3, there are 410 groups as shown by Fité, K, and Sutherland; there are 14 options for the connected component. It is not yet known which of these occur for genus 3 curves.

Abelian varieties of low dimension

The classification of Sato-Tate groups is known for abelian varieties of dimension ≤ 3.

- In dimension 1, we have seen the three cases already (no CM, CM within the base field, CM not within the base field).
- In dimension 2, there are 52 groups as shown by Fité, K, Rotger , and Sutherland; there are 6 options for the identity component. These all occur for genus 2 curves as well.
- In dimension 3, there are 410 groups as shown by Fité, K, and Sutherland; there are 14 options for the connected component. It is not yet known which of these occur for genus 3 curves.

Other classification problems of interest

Other cases for which the classification of Sato-Tate groups is potentially of interest.

- Abelian varieties of dimension 4. These include cases where the group is not determined by endomorphisms alone, as shown by examples of Mumford and Shioda .
- K3 surfaces. The Mumford-Tate groups are understood by work of Tankeev  and Zarhin .

Other classification problems of interest

Other cases for which the classification of Sato-Tate groups is potentially of interest.

- Abelian varieties of dimension 4. These include cases where the group is not determined by endomorphisms alone, as shown by examples of Mumford and Shioda .
- K3 surfaces. The Mumford-Tate groups are understood by work of Tankeev  and Zarhin .

Other classification problems of interest

Other cases for which the classification of Sato-Tate groups is potentially of interest.

- Abelian varieties of dimension 4. These include cases where the group is not determined by endomorphisms alone, as shown by examples of Mumford and Shioda .
- K3 surfaces. The Mumford-Tate groups are understood by work of Tankeev  and Zarhin .

Heuristic vs. rigorous computation of Sato-Tate groups

For any given X, if one can compute L-polynomials efficiently (a topic for a separate talk!), one can match the empirically measured Sato-Tate distribution with a candidate Sato-Tate group by comparing moments. However, this depends on having a classification, and even then can only give rigorous results for "large" groups. (Also, in rare cases distinct groups give rise to identical distributions.)

For abelian varieties of dimension ≤ 3, one can compute the Sato-Tate group rigorously via the rational endomorphism algebra. This has been made practical by Costa , Mascot , Sijsling , and Voight .

There is also a new group-theoretic approach by Zywina  that does not depend on a classification (and so applies to higher-dimensonal abelian varieties), and can give rigorous results in many more cases.

Heuristic vs. rigorous computation of Sato-Tate groups

For any given X, if one can compute L-polynomials efficiently (a topic for a separate talk!), one can match the empirically measured Sato-Tate distribution with a candidate Sato-Tate group by comparing moments. However, this depends on having a classification, and even then can only give rigorous results for "large" groups. (Also, in rare cases distinct groups give rise to identical distributions.)

For abelian varieties of dimension ≤ 3, one can compute the Sato-Tate group rigorously via the rational endomorphism algebra. This has been made practical by Costa , Mascot , Sijsling , and Voight .

There is also a new group-theoretic approach by Zywina  that does not depend on a classification (and so applies to higher-dimensonal abelian varieties), and can give rigorous results in many more cases.

Heuristic vs. rigorous computation of Sato-Tate groups

For any given X, if one can compute L-polynomials efficiently (a topic for a separate talk!), one can match the empirically measured Sato-Tate distribution with a candidate Sato-Tate group by comparing moments. However, this depends on having a classification, and even then can only give rigorous results for "large" groups. (Also, in rare cases distinct groups give rise to identical distributions.)

For abelian varieties of dimension ≤ 3, one can compute the Sato-Tate group rigorously via the rational endomorphism algebra. This has been made practical by Costa , Mascot , Sijsling , and Voight .

There is also a new group-theoretic approach by Zywina  that does not depend on a classification (and so applies to higher-dimensonal abelian varieties), and can give rigorous results in many more cases.

Contents

About the references

References are listed in the order in which they are alluded to in the text. To save space on the slides, I didn't give explicit citations (hopefully you can figure this out from context) or include anything about the papers besides their titles (the Internet can help).

Some references are included which were not explicitly mentioned, but are closely related to references which were mentioned.

References (part 1)

Lenstra–Stevenhagen, Chebotarëv and his density theorem
Ito, On the history of the Sato-Tate conjecture (slides)
Clozel–Harris–Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations
Harris–Shepherd-Barron–Taylor, A family of Calabi-Yau varieties and potential automorphy
Barnet-Lamb–Geraghty–Gee, The Sato-Tate conjecture for Hilbert modular forms
Allen–Calegari–Caraiani–Gee–Helm–Le Hung–Newton–Scholze–Taylor–Thorne, Potential automorphy over CM fields
Birch, How the number of points of an elliptic curves over a fixed prime field varies
Katz–Sarnak, *Random Matrices, Frobenius Eigenvalues, and Monodromy*
Serre, Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques

References (part 2)

Serre, *Lectures on $N_X(p)$*
Banaszak–K, An algebraic Sato-Tate group and Sato-Tate conjecture
Banaszak–K, Motivic Serre group, algebraic Sato-Tate group, and Sato-Tate conjecture
Cantoral-Farfán–Commelin, The Mumford-Tate conjecture implies the algebraic Sato-Tate conjecture
Guralnick–K, Endomorphism fields of abelian varieties
Serre, *Abelian l-adic Representations and Elliptic Curves* (the appendix to chapter 1 discusses equidistribution in a compact Lie group)
Fité–K–Rotger–Sutherland, Sato-Tate distributions and Galois endomorphism modules in genus 2
Fité–K–Sutherland, Sato-Tate groups of abelian threefolds: a preview of the classification
Lagarias–Odlyzko, Effective Chebotarev
Serre, Quelques applications du théorème de densité de Chebotarev

References (part 3)

Murty, Explicit formulae and the Lang–Trotter conjecture
Bucur–K, An application of the effective Sato-Tate conjecture
Chen–Park–Swaminathan, Elliptic curve variants of the least quadratic nonresidue problem and Linnik's theorem
Rouse–Thorner, The explicit Sato-Tate conjecture and densities pertaining to Lehmer-type questions
Thorner, Effective forms of the Sato-Tate conjecture
Bucur–Fité–K, Effective Sato-Tate conjecture for abelian varieties and applications
Mumford, A note of Shimura's paper "Discontinuous groups and abelian varieties"
Shioda, Algebraic cycles on abelian varieties of Fermat type
Tankeev, On algebraic cycles on surfaces and abelian varieties
Zarhin, Hodge groups of K3 surfaces
Costa–Mascot–Sijsling–Voight, Rigorous computation of the endomorphism ring of a Jacobian