# The work of R. P. Langlands

E. Kowalski

ETH Zürich

Abel Prize Day
September 25, 2020

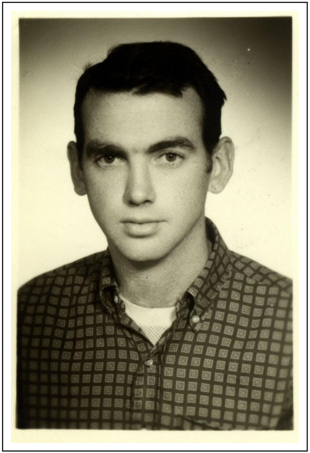
# Citation

The Norwegian Academy of Sciences and Letters has decided to award the Abel Prize for 2018 to

**Robert P. Langlands**

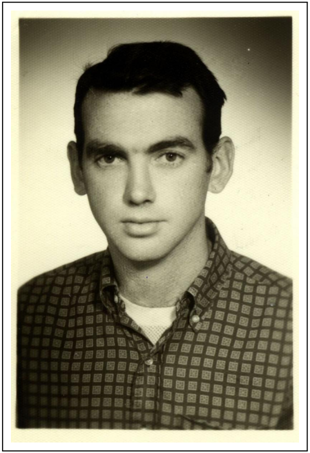
"for his visionary program connecting representation theory to number theory."

# Biography



- Born 1936 in British Columbia.

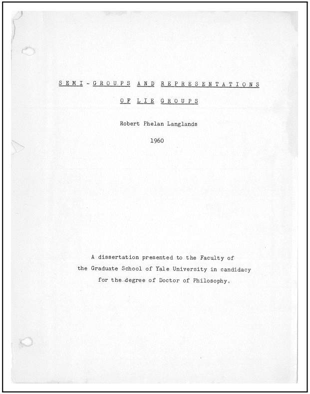
# Biography



- Born 1936 in British Columbia.
- MSc, University of British Columbia, 1958

"The thesis was undoubtedly not well-written and could be understood by no-one. Moreover, I myself discovered very soon after submission an error in the arguments."

# Biography


SEMI-GROUPS AND REPRESENTATIONS

OF LIE GROUPS

Robert Phelan Langlands

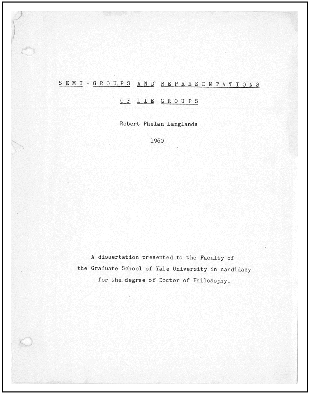
1960

A dissertation presented to the Faculty of
the Graduate School of Yale University in candidacy
for the degree of Doctor of Philosophy.

- Born 1936 in British Columbia.
- MSc, University of British Columbia, 1958
- PhD, Yale University, 1960; "Semi-groups and representations of Lie groups".

"Once again, there was, oddly enough, no-one to understand it, but as I know from a conversation overheard in a stairway, Browder was quite firm in defending me and my thesis in the face of another faculty member, whose stated grounds for rejecting it were solely that no-one could read it."

# Biography



SEMI-GROUPS AND REPRESENTATIONS

OF LIE GROUPS

Robert Phelan Langlands

1960

A dissertation presented to the Faculty of
the Graduate School of Yale University in candidacy
for the degree of Doctor of Philosophy.

http://publications.ias.edu/rpl/

- Born 1936 in British Columbia.
- MSc, University of British Columbia, 1958
- PhD, Yale University, 1960; "Semi-groups and representations of Lie groups".
- Positions at Princeton, Yale and IAS.

# Cold open: Representations

*Three sentences on representation theory*

- A representation of a group $G$ on a $k$-vector space $E$ is a homomorphism $\varrho\colon G \to \mathrm{GL}(E)$.
- If $E$ is a Hilbert space and $\varrho(g)$ is always unitary, one says that $\varrho$ is a unitary representation.
- If $E \neq \{0\}$ and no (closed) proper subspace is stable, then $\varrho$ is called irreducible.

# The birth of algebraic number theory: quadratic reciprocity

For a prime $p$ and an integer $n \in \mathbf{Z}$, define the *Legendre symbol*

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \equiv m^2 \bmod p \text{ for some } m \text{ coprime to } p \\ 0 & \text{if } p \text{ divides } n \\ -1 & \text{otherwise.} \end{cases}$$

It is elementary that $(n/p)(m/p) = (nm/p)$.

# The birth of algebraic number theory: quadratic reciprocity

For a prime $p$ and an integer $n \in \mathbf{Z}$, define the *Legendre symbol*

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \equiv m^2 \bmod p \text{ for some } m \text{ coprime to } p \\ 0 & \text{if } p \text{ divides } n \\ -1 & \text{otherwise.} \end{cases}$$

It is elementary that $(n/p)(m/p) = (nm/p)$.

**Theorem.** (Gauss) For any distinct odd primes $p$ and $q$, we have

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/2}.$$

# An application

How quickly can you compute

$$\left(\frac{5}{196561}\right) \quad ?$$

Note that by quadratic reciprocity

$$\left(\frac{5}{196561}\right) = \left(\frac{196561}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

# An application

How quickly can you compute

$$\left(\frac{5}{196561}\right) \quad ?$$

Note that by quadratic reciprocity

$$\left(\frac{5}{196561}\right) = \left(\frac{196561}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

So there is some integer $m \geqslant 1$ such that $m^2 - 5 \equiv 0 \bmod 196561$. The smallest of them is 87909.

# An application

How quickly can you compute

$$\left(\frac{5}{196561}\right) \quad ?$$

Note that by quadratic reciprocity

$$\left(\frac{5}{196561}\right) = \left(\frac{196561}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

So there is some integer $m \geqslant 1$ such that $m^2 - 5 \equiv 0 \bmod 196561$. The smallest of them is 87909.

Gödel was apparently fascinated by this example of transforming a seemingly exponential-time computation into a logarithmic-time one.

# A first interpretation

The condition

$$\left(\frac{q}{p}\right) = 1$$

means that the polynomial $X^2 - q \in \mathbf{Z}[X]$ has two roots modulo $p$: it *splits* in linear factors in $(\mathbf{Z}/p\mathbf{Z})[X]$.

# A first interpretation

The condition

$$\left(\frac{q}{p}\right) = 1$$

means that the polynomial $X^2 - q \in \mathbf{Z}[X]$ has two roots modulo $p$: it *splits* in linear factors in $(\mathbf{Z}/p\mathbf{Z})[X]$.

Quadratic Reciprocity means that the set of primes where this happens (and also the set of those where $X^2 - q$ remains irreducible modulo $p$) can be described explicitly as the set of primes satisfying certain congruence relations.

# A first interpretation

The condition

$$\left(\frac{q}{p}\right) = 1$$

means that the polynomial $X^2 - q \in \mathbf{Z}[X]$ has two roots modulo $p$: it *splits* in linear factors in $(\mathbf{Z}/p\mathbf{Z})[X]$.

Quadratic Reciprocity means that the set of primes where this happens (and also the set of those where $X^2 - q$ remains irreducible modulo $p$) can be described explicitly as the set of primes satisfying certain congruence relations.

**First general question.** Given a fixed irreducible $f \in \mathbf{Z}[X]$, can one describe the primes $p$ such that $f$ splits modulo $p$? Can one describe more generally the factorization of $f$ modulo $p$?

# A second interpretation

Suppose that $q \equiv 1 \bmod 4$. Observe the following identity

$$\prod_p \left(1 - \left(\frac{q}{p}\right) p^{-s}\right)^{-1} = \prod_p \left(1 - \left(\frac{p}{q}\right) p^{-s}\right)^{-1} = \sum_{n \geqslant 1} \left(\frac{n}{q}\right) n^{-s},$$

where the second step follows from

$$\left(\frac{p_1^{n_1}}{q}\right) \cdots \left(\frac{p_k^{n_k}}{q}\right) = \left(\frac{p_1^{n_1} \cdots p_k^{n_k}}{q}\right).$$

# A second interpretation

Suppose that $q \equiv 1 \bmod 4$. Observe the following identity

$$\prod_p \left(1 - \left(\frac{q}{p}\right) p^{-s}\right)^{-1} = \prod_p \left(1 - \left(\frac{p}{q}\right) p^{-s}\right)^{-1} = \sum_{n \geqslant 1} \left(\frac{n}{q}\right) n^{-s},$$

where the second step follows from

$$\left(\frac{p_1^{n_1}}{q}\right) \cdots \left(\frac{p_k^{n_k}}{q}\right) = \left(\frac{p_1^{n_1} \cdots p_k^{n_k}}{q}\right).$$

The right-hand side can be studied by analytic means, because $(n/q)$ is periodic modulo $q$. For instance, it extends to an entire function.

# A second interpretation

Suppose that $q \equiv 1 \bmod 4$. Observe the following identity

$$\prod_p \left(1 - \left(\frac{q}{p}\right) p^{-s}\right)^{-1} = \prod_p \left(1 - \left(\frac{p}{q}\right) p^{-s}\right)^{-1} = \sum_{n \geqslant 1} \left(\frac{n}{q}\right) n^{-s},$$

where the second step follows from

$$\left(\frac{p_1^{n_1}}{q}\right) \cdots \left(\frac{p_k^{n_k}}{q}\right) = \left(\frac{p_1^{n_1} \cdots p_k^{n_k}}{q}\right).$$

The right-hand side can be studied by analytic means, because $(n/q)$ is periodic modulo $q$. For instance, it extends to an entire function.

The left-hand side would otherwise be a complete mystery.

# A second interpretation

Suppose that $q \equiv 1 \bmod 4$. Observe the following identity

$$\prod_p \left(1 - \left(\frac{q}{p}\right) p^{-s}\right)^{-1} = \prod_p \left(1 - \left(\frac{p}{q}\right) p^{-s}\right)^{-1} = \sum_{n \geqslant 1} \left(\frac{n}{q}\right) n^{-s},$$

where the second step follows from

$$\left(\frac{p_1^{n_1}}{q}\right) \cdots \left(\frac{p_k^{n_k}}{q}\right) = \left(\frac{p_1^{n_1} \cdots p_k^{n_k}}{q}\right).$$

The right-hand side can be studied by analytic means, because $(n/q)$ is periodic modulo $q$. For instance, it extends to an entire function.

The left-hand side would otherwise be a complete mystery.

Both (equal) sides are examples of so-called $L$-functions; an achievement of Langlands was to predict (and sometimes prove) that $L$-functions of both types are sometimes equal.

# A second interpretation

Suppose that $q \equiv 1 \bmod 4$. Observe the following identity

$$\prod_p \left(1 - \left(\frac{q}{p}\right)p^{-s}\right)^{-1} = \prod_p \left(1 - \left(\frac{p}{q}\right)p^{-s}\right)^{-1} = \sum_{n \geqslant 1} \left(\frac{n}{q}\right) n^{-s},$$

where the second step follows from

$$\left(\frac{p_1^{n_1}}{q}\right) \cdots \left(\frac{p_k^{n_k}}{q}\right) = \left(\frac{p_1^{n_1} \cdots p_k^{n_k}}{q}\right).$$

The right-hand side can be studied by analytic means, because $(n/q)$ is periodic modulo $q$. For instance, it extends to an entire function.

The left-hand side would otherwise be a complete mystery.

Both (equal) sides are examples of so-called $L$-functions; an achievement of Langlands was to predict (and sometimes prove) that $L$-functions of both types are sometimes equal.

One such equality, first conjectured by Shimura, Taniyama and Weil is the essential step in the proof of Fermat's Great Theorem by Wiles.

# And a third...

The set $\mathbf{Q}(\sqrt{q})$ of all complex numbers of the form

$$a + b\sqrt{q}, \qquad a,\ b \text{ rational numbers},$$

is a field (one can add, multiply, divide by non-zero elements). The map $\sigma\colon a + b\sqrt{q} \mapsto a - b\sqrt{q}$ is an automorphism of this field.

# And a third...

The set $\mathbf{Q}(\sqrt{q})$ of all complex numbers of the form

$$a + b\sqrt{q}, \qquad a,\ b \text{ rational numbers,}$$

is a field (one can add, multiply, divide by non-zero elements). The map $\sigma\colon a + b\sqrt{q} \mapsto a - b\sqrt{q}$ is an automorphism of this field.
The group $G$ of all automorphisms of $\mathbf{Q}(\sqrt{q})$ is equal to $\{1, \sigma\}$. There is an obvious homomorphism

$$\eta\colon G \to \{-1, 1\} \subset \mathrm{GL}_1(\mathbf{C}).$$

# And a third...

The set $\mathbf{Q}(\sqrt{q})$ of all complex numbers of the form

$$a + b\sqrt{q}, \qquad a,\ b \ \text{ rational numbers,}$$

is a field (one can add, multiply, divide by non-zero elements). The map $\sigma\colon a + b\sqrt{q} \mapsto a - b\sqrt{q}$ is an automorphism of this field.

The group $G$ of all automorphisms of $\mathbf{Q}(\sqrt{q})$ is equal to $\{1, \sigma\}$. There is an obvious homomorphism

$$\eta\colon G \to \{-1, 1\} \subset \mathrm{GL}_1(\mathbf{C}).$$

This is an example of a *Galois representation*.

# Frobenius

For any prime $p$ different from $q$, the *Frobenius automorphism* $x \mapsto x^p$ modulo $p$ permutes the two roots of $X^2 - q$ in an algebraic closure of the finite field $\mathbf{Z}/p\mathbf{Z}$.

# Frobenius

For any prime $p$ different from $q$, the *Frobenius automorphism* $x \mapsto x^p$ modulo $p$ permutes the two roots of $X^2 - q$ in an algebraic closure of the finite field $\mathbf{Z}/p\mathbf{Z}$.

This permutation $F_p$ is either the identity, if the roots belong to $\mathbf{Z}/p\mathbf{Z}$ (namely when $X^2 - q$ splits modulo $p$) or it exchanges the two roots. So $F_p$ may be identified with an element of $G$, which is $\sigma$ if $F_p$ exchanges the two roots.

# Frobenius

For any prime $p$ different from $q$, the *Frobenius automorphism* $x \mapsto x^p$ modulo $p$ permutes the two roots of $X^2 - q$ in an algebraic closure of the finite field $\mathbf{Z}/p\mathbf{Z}$.

This permutation $F_p$ is either the identity, if the roots belong to $\mathbf{Z}/p\mathbf{Z}$ (namely when $X^2 - q$ splits modulo $p$) or it exchanges the two roots. So $F_p$ may be identified with an element of $G$, which is $\sigma$ if $F_p$ exchanges the two roots.

Quadratic Reciprocity means that, with these identifications, we have

$$\eta(F_p) = \left(\frac{q}{p}\right) = \chi(p),$$

where $\chi\colon \mathbf{Z} \to \mathrm{GL}_1(\mathbf{C})$ is defined by $\chi(n) = (n/q)$, and satisfies $\chi(nm) = \chi(n)\chi(m)$; it is a "Dirichlet character".

# Class Field Theory

Class Field Theory was the major purpose and achievement of algebraic number theory from the time of Gauss to roughly 1940.

# Class Field Theory

Class Field Theory was the major purpose and achievement of algebraic number theory from the time of Gauss to roughly 1940.

It gave an answer to the question of splitting of polynomials, even with coefficients in "number fields" instead of $\mathbf{Q}$, under the condition that their splitting field should have abelian Galois group.

# Class Field Theory

Class Field Theory was the major purpose and achievement of algebraic number theory from the time of Gauss to roughly 1940.

It gave an answer to the question of splitting of polynomials, even with coefficients in "number fields" instead of $\mathbf{Q}$, under the condition that their splitting field should have abelian Galois group.

For polynomials with integer coefficients, this means (by a theorem of Kronecker and Weber) that the roots of $f$ are integral linear combinations of roots of unity. This is obviously extremely restrictive.

# Class Field Theory

Class Field Theory was the major purpose and achievement of algebraic number theory from the time of Gauss to roughly 1940.

It gave an answer to the question of splitting of polynomials, even with coefficients in "number fields" instead of $\mathbf{Q}$, under the condition that their splitting field should have abelian Galois group.

For polynomials with integer coefficients, this means (by a theorem of Kronecker and Weber) that the roots of $f$ are integral linear combinations of roots of unity. This is obviously extremely restrictive.

A major problem in number theory when Langlands entered the scene was to extend this beyond the abelian case.

# Galois representations

Artin had begun to study representations of the Galois group $G$ of an arbitrary Galois extension of $\mathbf{Q}$ in finite-dimensional vector spaces:

$$\varrho\colon G \to \mathrm{GL}_d(\mathbf{C}),$$

and associated to them their $L$-function

$$L(\varrho, s) = \prod_p \det(1 - \varrho(F_p)p^{-s})^{-1}.$$

# Galois representations

Artin had begun to study representations of the Galois group $G$ of an arbitrary Galois extension of $\mathbf{Q}$ in finite-dimensional vector spaces:

$$\varrho\colon G \to \mathrm{GL}_d(\mathbf{C}),$$

and associated to them their $L$-function

$$L(\varrho, s) = \prod_p \det(1 - \varrho(F_p)p^{-s})^{-1}.$$

He couldn't prove their expected properties, except in very special cases, in the absence of a convenient expression for the corresponding series expansion (no reciprocity law).

# Galois representations

Artin had begun to study representations of the Galois group $G$ of an arbitrary Galois extension of $\mathbf{Q}$ in finite-dimensional vector spaces:

$$\varrho\colon G \to \mathrm{GL}_d(\mathbf{C}),$$

and associated to them their $L$-function

$$L(\varrho, s) = \prod_p \det(1 - \varrho(F_p)p^{-s})^{-1}.$$

He couldn't prove their expected properties, except in very special cases, in the absence of a convenient expression for the corresponding series expansion (no reciprocity law).

Langlands identified what should be the analogue of the Dirichlet characters in that setting: generalizations of the modular forms which were also classically studied by many 19th century mathematicians.

# A modular form

For $z \in \mathbf{C}$ with positive imaginary part, define

$$\Delta(z) = e^{2i\pi z} \prod_{n \geqslant 1} (1 - e^{2i\pi nz})^{24}.$$

We have

$$\Delta\Big(\frac{az+b}{cz+d}\Big) = (cz+d)^{12}\Delta(z), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}).$$

# A modular form

For $z \in \mathbf{C}$ with positive imaginary part, define

$$\Delta(z) = e^{2i\pi z} \prod_{n \geqslant 1} (1 - e^{2i\pi nz})^{24}.$$

We have

$$\Delta\Big(\frac{az+b}{cz+d}\Big) = (cz+d)^{12}\Delta(z), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}).$$

Ramanujan observed, and Hecke proved, the remarkable fact that if we expand

$$\Delta(z) = \sum_{n \geqslant 1} \tau(n) e^{2i\pi nz},$$

then the arithmetic coefficients $\tau(n) \in \mathbf{Z}$ satisfy

$$\sum_{n \geqslant 1} \tau(n) n^{-s} = \prod_p (1 - \tau(p)p^{-s} + p^{11-2s})^{-1}.$$

# Automorphic representations

There is a locally compact topological ring $\mathbf{A}$, obtained by combining all the completions of $\mathbf{Q}$ with respect to the $p$-adic and ordinary metrics. It contains $\mathbf{Q}$ as a discrete subring.

# Automorphic representations

There is a locally compact topological ring $\mathbf{A}$, obtained by combining all the completions of $\mathbf{Q}$ with respect to the $p$-adic and ordinary metrics. It contains $\mathbf{Q}$ as a discrete subring.

Langlands indicated that Artin representations

$$\varrho\colon G \to \mathrm{GL}_d(\mathbf{C})$$

should "correspond" to certain *infinite-dimensional* irreducible unitary representations

$$\pi\colon \mathrm{GL}_d(\mathbf{A}) \to \mathrm{U}(H)$$

# Automorphic representations

There is a locally compact topological ring $\mathbf{A}$, obtained by combining all the completions of $\mathbf{Q}$ with respect to the $p$-adic and ordinary metrics. It contains $\mathbf{Q}$ as a discrete subring.

Langlands indicated that Artin representations

$$\varrho\colon G \to \mathrm{GL}_d(\mathbf{C})$$

should "correspond" to certain *infinite-dimensional* irreducible unitary representations

$$\pi\colon \mathrm{GL}_d(\mathbf{A}) \to \mathrm{U}(H)$$

that can be embedded in the natural representation $\mathrm{reg}$ on

$$L^2(\mathrm{GL}_d(\mathbf{Q})\backslash \mathrm{GL}_d(\mathbf{A}))$$

which is defined by

$$(\mathrm{reg}(g)f)(x) = f(xg).$$

# The Langlands correspondance

The correspondance between

$$\varrho\colon G \to \mathsf{GL}_d(\mathbf{C})$$

and

$$\pi\colon \mathsf{GL}_d(\mathbf{A}) \to \mathrm{U}(H)$$

should be such that

$$L(\varrho, s) = L(\pi, s).$$

The $L$-function on the right-hand side is a generalization of the Dirichlet and Hecke $L$-functions; it can be studied and analytically continued by similar analytic means.

# The Langlands correspondance

The correspondance between

$$\varrho\colon G \to \mathrm{GL}_d(\mathbf{C})$$

and

$$\pi\colon \mathrm{GL}_d(\mathbf{A}) \to \mathrm{U}(H)$$

should be such that

$$L(\varrho, s) = L(\pi, s).$$

The $L$-function on the right-hand side is a generalization of the Dirichlet and Hecke $L$-functions; it can be studied and analytically continued by similar analytic means.

Even for $d = 2$, this is not yet proved (when the projective image of $\varrho$ is $A_5$).

# The Langlands correspondance

The correspondance between

$$\varrho\colon G \to \mathsf{GL}_d(\mathbf{C})$$

and

$$\pi\colon \mathsf{GL}_d(\mathbf{A}) \to \mathrm{U}(H)$$

should be such that

$$L(\varrho, s) = L(\pi, s).$$

The $L$-function on the right-hand side is a generalization of the Dirichlet and Hecke $L$-functions; it can be studied and analytically continued by similar analytic means.

Even for $d = 2$, this is not yet proved (when the projective image of $\varrho$ is $A_5$). If the image is $S_4$, this was proved by Langlands and Tunnell; it is one of the starting points of the work of Wiles.

# Functoriality

If we have an Artin representation

$$\varrho\colon G \to \mathrm{GL}_d(\mathbf{C}),$$

with image $H$, we can compose with other representations $H \to \mathrm{GL}_e(\mathbf{C})$ to get a new one

$$\varrho'\colon G \to \mathrm{GL}_e(\mathbf{C}).$$

# Functoriality

If we have an Artin representation

$$\varrho\colon G \to \mathsf{GL}_d(\mathbf{C}),$$

with image $H$, we can compose with other representations $H \to \mathsf{GL}_e(\mathbf{C})$ to get a new one

$$\varrho'\colon G \to \mathsf{GL}_e(\mathbf{C}).$$

This means that from an automorphic representation

$$\pi\colon \mathsf{GL}_d(\mathbf{A}) \to \mathrm{U}(E),$$

we should be able to construct

$$\pi'\colon \mathsf{GL}_e(\mathbf{A}) \to \mathrm{U}(F),$$

with equality of $L$-functions.

# Equidistribution

This prediction of Langlands contains an immense amount of arithmetic information. It is very far from being proved or really understood...

# Equidistribution

This prediction of Langlands contains an immense amount of arithmetic information. It is very far from being proved or really understood...

For instance, Serre noticed that the existence of this functoriality in sufficient generality leads to a very concrete statement conjectured by Sato and Tate:

# Equidistribution

This prediction of Langlands contains an immense amount of arithmetic information. It is very far from being proved or really understood...

For instance, Serre noticed that the existence of this functoriality in sufficient generality leads to a very concrete statement conjectured by Sato and Tate:

**Theorem.** For any real numbers $-2 \leqslant a < b \leqslant 2$, we have

$$\frac{1}{\pi(x)}\mathrm{Card}\{p \leqslant x \mid a < \frac{\tau(p)}{p^{11/2}} < b\} \longrightarrow \frac{1}{\pi}\int_a^b \sqrt{1 - x^2/4}\, dx$$

as $x \to +\infty$.

# Equidistribution

This prediction of Langlands contains an immense amount of arithmetic information. It is very far from being proved or really understood...

For instance, Serre noticed that the existence of this functoriality in sufficient generality leads to a very concrete statement conjectured by Sato and Tate:

**Theorem.** For any real numbers $-2 \leqslant a < b \leqslant 2$, we have

$$\frac{1}{\pi(x)} \mathrm{Card}\{p \leqslant x \mid a < \frac{\tau(p)}{p^{11/2}} < b\} \longrightarrow \frac{1}{\pi} \int_a^b \sqrt{1 - x^2/4}\, dx$$

as $x \to +\infty$.

(This was proved by Clozel, Harris and Taylor in 2008.)