The Langlands Program

B. Sury

24.04.2018

Automorphic functions - introduced by Henri Poincaré.

In view of their symmetry properties, Automorphic functions often give rise to relations between different objects and even explain why various classical results hold.

Langlands's perspective - an extended definition of these functions via harmonic analysis and group representations.

Riemann Zeta function

C F Gauss (1777-1855) conjectured the 'Prime Number Theorem' in 1794:

$\pi(x)$ is asymptotic to the function $Li(x) := \int_1^x \frac{dt}{\log t}$.

$\frac{\pi(x)}{x/\log x} \to 1$ as $x \to \infty$ or, equivalently, the n-th prime p_n asymptotically grows like $n \log(n)$.

Infinitude of primes in every arithmetic progression of the form $an + b$ with $(a, b) = 1$ was proved in 1837 by Lejeune Dirichlet.

Unlike Euclid's proof, Dirichlet's proof requires more sophisticated, *analytic* techniques.

Bernhard Riemann's 1859 memoir gave totally new impetus to prime number theory, introducing novel techniques and giving birth to the subject of analytic number theory.

Riemann lived less than 40 years (September 17, 1826 - July 20, 1866) and wrote just one paper on number theory and it was 7 pages long.

Key difference between earlier workers and Riemann's paper:

Considered the series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ as a function of a complex variable s which varies over the right half-plane $\mathrm{Re}\,(s) > 1$.

Riemann proved meromorphic continuation and functional equation for this Riemann zeta function.

The key point of viewing the zeta function as a function of a complex variable s allowed Riemann to prove an 'explicit formula' connecting the complex zeroes of the zeta function and the set of prime numbers!

Riemann also made 5 conjectures, four of which were solved in the next 40 years; the one-unproved conjecture is the Riemann Hypothesis.

Riemann's memoir

The Riemann zeta function defined by the infinite series $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ for $\mathrm{Re}\,(s) > 1$ satisfies:

(I) Meromorphic continuation: $\zeta(s)$ can be defined for all $s \in \mathbf{C}$ as a holomorphic function except for the single point $s = 1$ where it has a simple pole with residue 1:

For (I), Riemann uses Jacobi's theta function

$$\theta(z) = \sum_{n=-\infty}^{\infty} e^{-n^2 \pi z}$$

which has the transformation property $\theta(1/z) = \sqrt{z}\theta(z)$ for $Re(z) > 0$ (here, $\sqrt{z}$ is chosen with argument in $(-\pi/4, \pi/4)$).

(II) Functional equation: The continued function (again denoted $\zeta(s)$) satisfies

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).$$

The mysterious appearance of the Gamma function was explained very satisfactorily as the "factor corresponding to the infinite prime" by Tate using adeles; will mention this later but one part of the explanation is:

$\pi^{-s/2}\Gamma(s/2)$ is the Mellin transform (a multiplicative version of the Fourier transform) of $e^{-\pi x^2}$ which is its own Fourier transform; the Poisson summation formula applies.

As the Gamma function has poles at all negative integers, the zeta function has zeroes at all $-2n$ for natural numbers n.

$s = 1$ simple pole of $\zeta(s)$ and $s = 0$ simple pole of $\Gamma(s/2)$, we obtain $\zeta(0) = -1/2$.

$1 + 1 + 1 + \cdots\cdots = -\frac{1}{2}$

$1 + 2 + 3 + \cdots\cdots = -\frac{1}{12}$

$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}$ where B_r are the Bernoulli numbers; note that $B_{odd>1} = 0$ which is related to $\zeta(-even < 0) = 0$.

Riemann's five conjectures in his 8-page paper:

(i) $\zeta(s)$ has infinitely many zeroes in $0 \leq \mathrm{Re}\,(s) \leq 1$.

(ii) The number of zeroes of $\zeta(s)$ in a rectangle of the form $0 \leq \mathrm{Re}\,(s) \leq 1$, $0 \leq \mathrm{Im}\,(s) \leq T$ equals

$$\frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T)$$

(iii) The function

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s)$$

has an infinite product expansion of the form

$$e^{A+Bs} \prod_{\rho} (1 - \frac{s}{\rho} e^{s/\rho})$$

for some constants A, B where the product runs over the zeroes of $\zeta(s)$ in the infinite strip $0 \leq \mathrm{Re}\,(s) \leq 1$.

(iv) If $\Lambda(n)$ is the von Mangoldt arithmetical function defined to be $\log p$ if n is a power of a single prime p and zero otherwise, and if $\psi(x) = \sum_{n \leq x} \Lambda(n)$, then

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{\log(1 - x^{-2})}{2}.$$

The value $\frac{\zeta'}{\zeta}(0)$ can be seen to be $\log(2\pi)$ on using the functional equation; note that the sum over the zeroes is to be interpreted as

$$\lim_{T \to \infty} \sum_{|\rho| \leq T} \frac{x^{\rho}}{\rho}$$

and is not absolutely convergent.

(v) (**Riemann hypothesis**) All the zeroes of $\zeta(s)$ in the so-called critical strip $0 \leq \mathrm{Re}\,(s) \leq 1$ lie on the vertical line $\mathrm{Re}\,(s) = \frac{1}{2}$.

The conjectures (i), (ii), and (iv) were proved in 1895 by von Mangoldt and (iii) was proved by Hadamard in 1893.

(iv) gives an explicit relation between prime numbers and *zeroes* of $\zeta(s)$.

In 1893, Hadamard and de la vallé Poussin independently proved that

$$\zeta(s) \neq 0 \ \ \forall \ \ \mathrm{Re}\,(s) = 1.$$

This non-vanishing on the vertical line $Re(s) = 1$ implies immediately that the ratio $\frac{\psi(x)}{x} \to 1$ as $x \to \infty$ and this is just a rephrasing of the Prime number theorem.

Indeed, looking at (iv), we see that $|x^\rho| = x^{\mathrm{Re}\,(\rho)}$ and, therefore, the prime number theorem ($\psi(x) \sim x$) is equivalent to the assertion $\mathrm{Re}\,(\rho) < 1$.

Not difficult to show that the **RH** gives

$$\frac{Li(x) - \pi(x)}{\sqrt{x}\log(x)} \simeq 1 + 2\sum_{\gamma} \frac{\sin(\gamma \log(x)}{\gamma}$$

where the sum is over all positive real γ such that $\frac{1}{2} + i\gamma$ is a zero of $\zeta(s)$.

As the right side is a sum of periodic functions, one may think of **RH** as saying that 'the primes have music in them'!

Weil's explicit formula

Let $\rho = \frac{1}{2} + i\gamma$ vary over the zeroes of $\zeta(s)$ - here, γ is complex, and the **RH** would imply that γ is real.

Consider any analytic function $h(z)$ on $|\mathrm{Im}\,(z)| \leq \frac{1}{2} + \delta$ satisfying

$h(-z) = h(z), |h(z)| \leq A(1+|z|)^{-2-\delta}$ for some $A, \delta > 0$.

Suppose g is the Fourier transform of h:

$$g(u) = \frac{1}{2\pi} \int_{\mathbf{R}} h(z) e^{-izu}\, dz.$$

$\sum_\gamma h(\gamma) =$
$\frac{1}{2\pi}\int_{-\infty}^{\infty} h(z)\frac{\Gamma'}{\Gamma}(\frac{1}{4}+\frac{iz}{2})\,dz + 2h(\frac{i}{2}) - g(0)\log\pi - 2\sum_{n=1}^{\infty}\frac{\Lambda(n)}{\sqrt{n}}g(\log n).$

So, the set of prime numbers and the nontrivial zeroes of $\zeta(s)$ are in duality!

As Weil observed, the Riemann Hypothesis is true if and only if $\sum_{\gamma} h(\gamma) > 0$ for all h of the form $h(z) = h_0(z)\overline{h_0(\bar{z})}$.

This Fourier-theoretic statement is remarkably similar to Selberg's trace formula (which itself can be thought of as a non-abelian generalization of Poisson's summation formula).

If X is a compact hyperbolic surface, the spectrum of the Laplace-Bertrami operator is discrete

$$0 = \mu_0 < \mu_1 \leq \mu_2 \leq \cdots$$

Label eigenvalues as $\mu_n = \frac{1}{4} + r_n^2$ for $n > 0$.

Selberg's trace formula relates the sum $\sum_n h(r_n)$ (the trace) for a 'nice' test function h to a sum over conjugacy classes $[x]$ of Γ:

$\sum_n h(r_n) =$
$\frac{Vol(X)}{4\pi} \int_{-\infty}^{\infty} zh(z) tanh(\pi z) dz + \sum_{[x]} \frac{\log N(x)}{N(x)^{1/2} - N(x)^{-1/2}} g(\log N(x))$
where g is the Fourier transform of h.

Riemann. $\psi(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{\log(1-x^{-2})}{2}$.

Weil. $\sum_\gamma h(\gamma) =$
$\frac{1}{2\pi}\int_{-\infty}^{\infty} h(z)\frac{\Gamma'}{\Gamma}(\frac{1}{4}+\frac{iz}{2})\,dz + 2h(\frac{i}{2}) - g(0)\log\pi - 2\sum_{n=1}^{\infty}\frac{\Lambda(n)}{\sqrt{n}}g(\log n)$.

Selberg. $\sum_n h(r_n) =$
$\frac{Vol(X)}{4\pi}\int_{-\infty}^{\infty} zh(z)tanh(\pi z)dz + \sum_{[x]}\frac{\log N(x)}{N(x)^{1/2}-N(x)^{-1/2}}g(\log N(x))$
where g is the Fourier transform of h.

Weil's explicit formula can also be interpreted as a trace formula for the trace of an operator on a suitable space.

The space is the semidirect product of the ideles of norm one and the adeles (to be defined later) quotiented by the discrete subgroup $\mathbb{Q}^* \propto \mathbb{Q}$.

For a suitable kernel function on this space, the conjugacy class side of the Selberg trace formula is precisely the sum over the primes occurring in Weil's explicit formula.

In the Langlands Program, one development is a very general trace formula due to James Arthur and his collaborators.

Reciprocity laws

Let p be a prime number $\equiv 1$ modulo 4.
The roots of the polynomials $f = X^2 - p$ and $g = X^p - 1$ generate fields $K_f = \mathbb{Q}(\sqrt{p})$ and $K_g = \mathbb{Q}(\zeta_p)$ where ζ_p is a primitive p-th root of unity.

Look at the set $Spl(K_f)$ of prime numbers q which 'split completely' in K_f (i.e. f, considered modulo p, splits into linear factors).

$Spl(K_f)$ consists of all primes q that are squares modulo p and $Spl(K_g)$ consists of prime numbers q for which $q \equiv 1$ modulo p; in particular, $Spl(K_g) \subset Spl(K_f)$.

More generally:
Theorem. Let $f, g \in \mathbb{Z}[X]$ be irreducible polynomials and denote by K_f and K_g, the fields generated by their roots. Then, $K_f \subset K_g$ if and only if $Spl(K_f) \supset^* Spl(K_g)$.

The "if" part is a deep theorem of Chebotarev.
The notation $Spl(K_f)$ is intended to show that its elements are the prime numbers p which "split into" n "prime ideal" factors in K_f, where n is the degree of K_f - by a beautiful result of Dedekind and Kummer.

Thus, $Spl(K_f)$ characterizes the field K_f; one would like to describe $Spl(K_f)$ in terms of the base field $\mathbb{Q}$ only.

One calls *a reciprocity law*, any rule or description (in terms of $\mathbb{Q}$) of the set $Spl(f)$ of primes modulo which f splits into linear factors; the example above captures the quadratic reciprocity law of Gauss.

As we saw, for $g = X^n - 1$, $Spl(g)$ consists of primes $p \equiv 1 \bmod n$ (for $n = 4$, we have Fermat's sum of two squares theorem).

For $f = X^2 - p$, $Spl(f)$ is described by a set of congruences modulo p via the quadratic reciprocity law.

Can $Spl(f)$ always be so described for any f?

Too ambitious but the ambit of abelian class field theory is to show:

If K is a number field, and the roots of $f \in K[X]$ generate a field extension whose Galois group over K is abelian, then $Spl(f)$ can be described via a finite set of generalized congruences.

In 1853, Kronecker announced the remarkable theorem that every abelian extension of $\mathbb{Q}$ lies in a cyclotomic field - the Kronecker-Weber theorem.

The proof by Weber which attempts to correct Kronecker's proof also had errors and the first correct proof is due to Hilbert in 1896 (the year when PNT was proved!).

Kronecker used a notion of density of primes as early as 1880 and proved that for a polynomial with d irreducible factors over $\mathbb{Z}$, the average number of roots modulo p as p varies over primes, is d. A corollary of this is:

For a polynomial $f \in \mathbb{Z}[X]$, the set $Spl(f)$ has density $1/[K:\mathbb{Q}]$, where K is the splitting field of f.

Interestingly, Kronecker used this to give a proof of irreducibility of the cyclotomic polynomial; the above statement on density carries over to number fields with the same proof.

Analogous to Kronecker-Weber theorem, the abelian extensions of all imaginary quadratic fields were also described by Kronecker using special values of the j-function, elliptic functions and roots of unity; this is a consequence of the theory of complex multiplication.

For instance, Abel had already shown that any abelian extension of $\mathbb{Q}(i)$ lies in the field obtained by attaching the values of the lemniscatic elliptic function sl at ω/n where ω is the lemniscatic analogue of π.

The general expectation of describing abelian extensions of any number field by attaching special values of some transcendental function is the 12th problem of Hilbert - it is still open.

The 9th problem of Hilbert asks for general reciprocity laws for non-abelian extensions - the Langlands Program concerns this.

Abelian class field theory

Let us look at $\mathbb{Q}$ first - if $K \subseteq \mathbb{Q}(\zeta_n)$ is an abelian extension, one calls n, an admissible modulus for K; the smallest possible n called the conductor of K.

If n is an admissible modulus for K, each integer a coprime to n defines an element of the Galois group of K over $\mathbb{Q}$ (simply, the restriction to K of the map $\zeta_n \mapsto \zeta_n^a$ on the cyclotomic field); this is denoted by $\left(\frac{K}{a}\right)$ and is called the Artin symbol.

In this manner, we have the *Artin homomorphism*

$$\left(\frac{K}{*}\right) : (\mathbb{Z}/n\mathbb{Z})^* \to Gal(K/\mathbb{Q}).$$

This is onto and therefore, gives $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*/I_{K,n}$ in terms of the arithmetic of $\mathbb{Q}$ (where $I_{K,n}$ is the kernel of the Artin map) - the Artin reciprocity isomorphism over $\mathbb{Q}$.

For instance, if $K = \mathbb{Q}(\sqrt{p})$ with $p \equiv 1 \bmod 4$, then its conductor is p and the Artin map is simply $a \mapsto \left(\frac{a}{p}\right)$ and the kernel is the subgroup of squares; so, $Gal(K/\mathbb{Q}) = \{\pm 1\}$.

If n is a modulus for K and p does not divide n, then the order of the coset of $pI_{K,n}$ in $(\mathbb{Z}/n\mathbb{Z})^*$ is the so-called residue class degree at p - this is the number $[K : \mathbb{Q}]/g$ where g is the number of prime ideal factors that p has in K.

In particular, for $K = \mathbb{Q}(\zeta_n)$, since the kernel is trivial, we are talking about the order of p mod n.

p splits completely in it if and only if $p \equiv 1 \bmod n$.

Generalizing to a general number field K:

A modulus m of K is a formal product of a non-zero ideal of O_K and real embeddings.

The fractional ideals prime to m form a group I_m with a subgroup P_m consisting of principal fractional ideals αO_K for $\alpha \equiv 1 \bmod m$ (this means also that $\alpha - 1 > 0$ at the real embeddings in m).

The quotient $C_m := I_m/P_m$ is called the ray class group; for the trivial modulus, we get the ideal class group of K.

For a Galois extension L of K, the norms of ideals of O_L over m give rise to a subgroup $N_m(L/K)$ of the ray class group C_m.

The index of this subgroup is at the most the degree $[L : K]$ and Takagi showed in 1920 that for certain moduli (called admissible), the index is equal to the degree.

For each modulus m of K and each subgroup H_m/P_m of the ray class group, there is a unique abelian extension L/K so that m is admissible for L, the norm subgroup $N_m(L/K)$ equals H_m modulo P_m and $I_m/H_m \cong Gal(L/K)$.

When the subgroup considered is trivial, the corresponding field is called the *ray class field* of K for the modulus m.

Conversely, every abelian extension L is contained in the ray class field for some modulus m.

The ray class field corresponding to the trivial modulus is called the Hilbert class field of K.

It has the property that its Galois group over K is isomorphic to the class group of K and every prime in K is unramified in it; it is the maximal abelian, unramified extension of K.

The analogue of Dirichlet's theorem on primes in arithmetic progressions is the statement that for a subgroup H_m/P_m of the ray class group, the primes in any coset of I_m/H_m have density $1/[I_m : H_m]$.

Takagi's result is made completely explicit by Artin through a natural map in the following manner.

For an abelian extension L/K and a modulus m of K containing the bad primes, Artin's reciprocity theorem (stated as a theorem in 1927 but proved only later!) gives an explicit homomorphism - the Artin map - from I_m to $Gal(L/K)$ (which maps P to $Frob_P(L/K)$) whose kernel contains $P_m N_m(L/K)$ (when the modulus is 'admissible', this is the whole kernel).

The surjectivity is proved analytically; the most difficult part of the theorem is to show that P_m is contained in the kernel of the Artin map.

The quadratic reciprocity law can easily be recovered from Artin's theorem.

Idelic formulation - shape of things to come

As we mentioned, splitting of primes in abelian extensions of a number field K are given by generalized congruence conditions.

The ideles are a device to capture ALL congruence conditions.

The ideles of K are the locally compact ring formed by the product of completions of K^* at all 'primes' of K with the restriction that in an idele, the factors at all but finitely many primes P are from the maximal compact subring of the completion K_P.

The open compact subgroups of the idele ring I_K are defined by congruence conditions.

The theorems of class field theory show that there is a bijection between continuous homomorphisms from I_K/K^* to $\mathbb{C}^*$ and continuous homomorphisms from the absolute Galois group $Gal(\bar{K}/K)$ to $\mathbb{C}^*$.

From Langlands's perspective, instead of the idele class group or the absolute Galois group, it is better to consider their character groups (one-dimensional representations).

In this manner, higher dimensional generalizations will consider irreducible n-dimensional representations of the Galois group and certain types of representations (called cuspidal automorphic representations) of ' $\prod_P' GL_n(K_P)$.

Classical L-functions

Dedekind zeta functions:

For an algebraic number field K, one has the Dedekind zeta function

$$\zeta_K(s) = \sum_{I \neq 0} N(I)^{-s} = \prod_P (1 - N(P)^{-s})^{-1}.$$

The series and the product are absolutely convergent for $\mathrm{Re}\,(s) > 1$.

Unlike the Riemann zeta function, the residue of $\zeta_K(s)$ at $s = 1$ carries subtle information on K like its class number etc.

$\zeta_K(s)$ admits a meromorphic continuation to $\mathrm{Re}\,(s) > 1 - 1/d$ and is holomorphic except for a simple pole at $s = 1$ with residue given by 'the analytic class number formula':

$\lim_{s \to 1^+}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h(K) \mathrm{Re}\, g(K)}{|\mu(K)|\sqrt{|disc(K)|}}$.

There is also a functional equation of the form $\Lambda(s) = |disc(K)|^{1/2-s}\Lambda(1-s)$ which gives in particular the location of the 'trivial zeroes' of $\zeta_K(s)$; for example, $\zeta_K(-n) = 0$ for all non-negative integers n if $K \not\subset \mathbf{R}$.

Extended Riemann hypothesis: *All the 'nontrivial' zeroes of* $\zeta_K(s)$ *lie on* $\mathrm{Re}\,(s) = \frac{1}{2}$.

Dirichlet L-functions

Dirichlet proved the infinitude of primes in progressions several years before Riemann's work and so, did not think in terms of analytic continuation etc.

To investigate the prime distribution in residue classes modulo q, Dirichlet considered the finite, abelian group $\mathbf{Z}_q^*$ and the dual group of homomorphisms from this group to $\mathbf{C}^*$.

Extending it to the whole of $\mathbf{Z}$ (taking 0 on non-units) so as to be periodic mod q, leads to Dirichlet characters mod q.

For any such Dirichlet character χ mod q, one has a Dirichlet L-function

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \ prime} (1 - \frac{\chi(p)}{p^s})^{-1}.$$

For example, if $q = 4$, the group has two elements and the nontrivial character is the map which takes the value $(\frac{-1}{p})$ - the Legendre symbol - at any odd prime p.

For any $a \geq 1$ which is relatively prime to q, using the Schur's orthogonality property for characters:

$\sum\{\frac{1}{p} : p \leq x, p \equiv a \ mod \ q\} =$
$\frac{1}{\phi(q)} \sum_{p \leq x} \frac{1}{p} + \frac{1}{\phi(q)} \sum_{\chi \neq 1} \bar{\chi}(a) \sum_{p \leq x} \frac{\chi(p)}{p}.$
Therefore, the assertion that

$$L(1, \chi) \neq 0 \ \ \forall \ \ \chi \neq 1$$

is equivalent to Dirichlet's theorem:

$\sum\{\frac{1}{p} : p \leq x, p \equiv a \ mod \ q\} = \frac{1}{\phi(q)} \log \log x + O(1).$

Generalized Riemann hypothesis: *All the 'nontrivial' zeroes of* $L(s,\chi)$ *lie on* $\mathrm{Re}\,(s) = \frac{1}{2}$ *for any Dirichlet character* χ.

For the quadratic field $K = \mathbf{Q}(\sqrt{\pm q})$ where the sign is the value $\chi(-1)$, one has:

$$\zeta_K(s) = \zeta(s)L(s,\chi).$$

This statement contains in it the quadratic reciprocity law of Gauss.

The theorem of Kronecker-Weber asserting that K is contained in a field of the form $\mathbf{Q}(e^{2i\pi/m})$ is equivalent to writing $\zeta_K(s)$ as a product of $L(s,\chi)$ for certain Dirichlet characters χ's and of $\zeta(s)$.

A point to be noted : the RHS is defined essentially in terms of $\mathbf{Q}$.

Generalizing Dirichlet characters, associated to a number field K, there are Hecke characters defined on the ray class groups of K.

In order to generalize Dirichlet's theorem on primes in arithmetic progression to a number field, Weber followed Dirichlet's idea from 1837.

Weber defined the L-function of characters χ of the generalized ideal class groups H_m/P_m by $L(s,\chi) = \sum_{(m,I)=1} \frac{\chi(I)}{N(I)^s}$ which converges absolutely for $Re(s) > 1$.

He could obtain analytic continuation only in the half-plane $Re(s) > 1 - 1/d$ where d is the degree of the field.

This does NOT suffice to prove the generalization of Dirichlet's theorem; one would need analytic continuation to $Re(s) > 0$ to deduce that $L(1, \chi) \neq 0$.

This is accomplished much later in 1918 by Hecke, who showed these L-functions analytically continue to entire functions except for the trivial character.

The next step is the introduction of nonabelian L-functions by Artin which ultimately leads us to a representation-theoretic point of view.

Other L-functions

A definition of the zeta function of an algebraic curve over a finite field was given by Emil Artin in his 1924 thesis.

He also proved the analogue of the **RH** for some 40 curves.

In 1934, Helmut Hasse established that the analogue of **RH** holds for the class of zeta functions associated to elliptic curves (nonsingular cubic curves $y^2 = f(x)$) over finite fields.

André Weil proved the **RH** for *all* nonsingular curves over finite fields in 1948 by deep methods from algebraic geometry - now simplified by Enrico Bombieri in 1972 using the Riemann-Roch theorem to a 5-page proof!

In 1949, Weil defined a zeta function for any algebraic variety over a finite field and made several conjectures.

One of these conjectures is an analogue of the **RH**.

Amazingly a prototype already occurs in the work of Gauss - the Last entry in his famous mathematical diary is a special case of Weil's **RH**:

Let $p \equiv 1 \bmod 4$ be a prime. Then, the number of solutions of the congruence $x^2 + y^2 + x^2y^2 \equiv 1 \bmod p$ equals $p - 1 - 2a$, where $p = a^2 + b^2$ and $a + ib \equiv 1 \bmod 2(1 + i)$.

After tremendous progress in algebraic geometry, Pierre Deligne proved the Weil conjectures in general in 1973.

Deligne's journey takes him through the theory of modular forms and a beautiful conjecture due to Ramanujan turns out to be the analogue of the **RH**.

For C - a nonsingular projective curve over a finite field $\mathbf{F}_q$ - one considers:

Div(C), the formal finite sums of the form $D = \sum a_i P_i$ where a_i are integers and the points P_i in C are defined over some finite extensions of $\mathbf{F}_q$ where $Frob_q(D) = D$.

Say $D = \sum a_i P_i$ effective $(D > 0)$ if $a_i \geq 0$ for all i.

Prime divisor - one which is not expressible as a sum of effective divisors.

Homomorphism $deg : \sum a_i P_i \to \sum a_i$.

Artin-Hasse-Schmidt zeta function of C is:

$$\zeta(C, s) := \sum_{D>0} (q^{deg(D)})^{-s} = \prod_P (1 - q^{deg(P)})^{-s}.$$

Satisfies the functional equation

$$q^{(g-1)s}\zeta(C, s) = q^{(g-1)(1-s)}\zeta(C, 1-s)$$

where g is the genus of C.

The Riemann-Roch theorem implies that $\zeta(C, s)$ is a rational function of q^{-s}; write $\zeta(C, s) = Z(C, t)$ where $t = q^{-s}$ and Z is a rational function of t.

Here **RH** is the statement that all zeroes of $\zeta(C, s)$ lie on $\mathrm{Re}\,(s) = \frac{1}{2}$; this is equivalent to the assertion that the numerator polynomial of Z has all zeroes of absolute value $q^{-1/2}$.

Easy for $g = 0$; Hasse's theorem when $g = 1$ - the case of elliptic curves.

In the Weil conjectures for general algebraic varieties X, the **RH** corresponds to the statement that the zeroes and poles of the corresponding rational function have absolute values $q^{\pm d/2}$ for some integer d.

Roots are viewed as eigenvalues of the Frobenius automorphism of $\mathbf{F}_q$ acting on the cohomology of the variety X.

L-functions of modular forms

For a positive integer N and a Dirichlet character χ mod N, a *modular form* of type (k, χ) on $\Gamma_0(N)$ is a function f on the upper half-plane which is holomorphic at all points including the cusps such that it satisfies the transformation formula

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z) \text{ for all } \begin{matrix} a & b \\ c & d \end{matrix} \in \Gamma_0(N).$$

In particular, $f(z+1) = f(z)$ and thus, at $i\infty$, it has a Fourier expansion $f(z) = \sum_{n=1}^{\infty} a_n q^n$ where $q = e^{2i\pi z}$.

The subspace of cusp forms is defined as those f for which $a_0 = 0$; the orthogonal complement of this subspace (with respect to the Petersen inner product) is spanned by Eisenstein series.

We look at the vector space $S_k(\Gamma_0(N), \chi)$ of cusp forms of type (k, χ). One defines the L-function of f as

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Using the theory of Hecke operators, Hecke proved that for any $f \in S_k(\Gamma_0(N), \chi)$, the L-function $L(s, f)$ extends to an entire function and satisfies a functional equation with a symmetry $s \leftrightarrow k - s$.

He also proved that the L-function has an Euler product

$$L(s, f) = \prod_{p|N} \left(1 - \frac{a_p}{p^s}\right)^{-1} \prod_{p\nmid N} \left(1 - \frac{a_p}{p^s} + \frac{\chi(p)}{p^{2s+1-k}}\right)^{-1}$$

which converges for $\mathrm{Re}\,(s) > (k+2)/2$, if and only if, f is a (normalized) common eigenform for all the Hecke operators.

Ramanujan-Petersson and Selberg conjectures

In its simplest form, the RP conjecture says that the Fourier coefficients $a_n(f)$ of a normalized Hecke eigenform of weight k for $SL_2(\mathbf{Z})$ satisfies

$$|a_p(f)| \leq 2p^{\frac{k-1}{2}} \quad \text{for every prime } p.$$

Hecke's work shows that the Fourier coefficients $a_n(f)$ are just the eigenvalues for the Hecke operators T_n.

This conjecture is therefore an analogue of the **RH**, and was proved by Deligne in the work on Weil conjectures alluded to earlier.

The analogue of the Ramanujan-Petersson conjecture for Maass forms - forms where the holomorphy assumption is dropped - is the assertion that $a_n(f) = O(n^{\epsilon})$ for each $\epsilon > 0$; this is still open.

The adelic formulation of the Ramanujan-Petersson conjecture used by Satake shows that the above Ramanujan-Petersson conjecture and the Selberg conjecture on eigenvalues are two sides of the same coin - the latter may be thought of as an archimedean analogue of the former.

Eichler-Shimura correspondence and Taniyama-Shimura-Weil conjecture

If $f \in S_2(\Gamma_0(N))$, it is clear that the differential form $f(z)\,dz$ is invariant under $\Gamma_0(N)$.

Then, for any fixed point z_0 on the upper half-plane, the integral $\int_{z_0}^{z} f(z)\,dz$ is independent of the path joining z_0 to z.

Thus, for any $\gamma \in \Gamma_0(N)$, there is a well-defined function $\gamma \mapsto \Phi_f(\gamma) = \int_{z_0}^{\gamma(z_0)} f(z)\,dz$ - this function does not depend on the choice of z_0.

Eichler-Shimura: When f is a normalized new form with integer coefficients, the set $\{\Phi_f(\gamma)\}$ as γ varies, forms a lattice Λ_f in $\mathbf{C}$. There is an elliptic curve E_f defined over $\mathbf{Q}$ which becomes isomorphic to the complex torus $\mathbf{C}/\Lambda_f$ over $\mathbf{C}$. Moreover

$$L(s, E_f) = L(s, f).$$

The converse result that every elliptic curve E over $\mathbf{Q}$ comes from a modular form of weight 2 for $\Gamma_0(N_E)$ as above was conjectured by Taniyama-Shimura-Weil and is now a famous theorem of Taylor and Wiles for square-free N and of Breuil, Conrad, Diamond & Taylor for other N.

Artin L-functions

Let L/K be a Galois extension of number fields with Gal $(L/K) = G$.

For a prime ideal P of $\mathcal{O}_K$, write

$$P\mathcal{O}_L = (P_1 P_2 \cdots P_g)^e$$

with P_i prime ideals.

The decomposition groups $D_{P_i} = \{\sigma \in G : \sigma(P_i) = P_i\}$ are all conjugate, and there is a surjective natural homomorphism to the Galois group of the residue field extension

$$D_{P_i} \to Gal\left(\frac{\mathcal{O}_L/P_i}{\mathcal{O}_K/P}\right)$$

Kernel is trivial for all but finitely many prime ideals P.

As the Galois group of an extension of finite fields is cyclic with a distinguished generator, the Frobenius automorphism, there is a conjugacy class σ_P in G corresponding to any unramified prime ideal P - this class is called the Artin symbol of P.

For a finite-dimensional complex representation of G, $\rho : G \to GL(V)$, Artin attached an L-function defined by

$L(s, \rho; L/K) = \prod_P det(1 - \rho(\sigma_P)N(P)^{-s}|V^{I_P})^{-1}$ where V^{I_P}, the subspace fixed by I_P is acted on by the conjugacy class σ_P.

Artin showed that these L-functions have nice properties like invariance under the induction of representations and posed:

Artin's Conjecture: $L(s, \rho; L/K)$ *extends to an entire function when the character of* ρ *does not contain the trivial character.*

Thus, the pole of a Dedekind zeta function ought to come from that of the Riemann zeta function.

Artin's conjecture is still open; a consequence of Artin's reciprocity law is the statement that these L-functions extend to meromorphic functions for any s.

Automorphic L-functions and Langlands program

The whole point of view ever since Artin defined his L-functions shifted to viewing everything in the powerful language of representation theory.

Classical modular form theory for subgroups of $SL_2(\mathbf{Z})$ can be viewed in terms of representations of $SL_2(\mathbf{R})$.

More generally, representations of adele groups surfaced as the principal objects of study as we will see.

A natural way to arrive at the adeles is via harmonic analysis; for example, a generalization of the duality between $\mathbf{Z}$ and $\mathbf{R}/\mathbf{Z}$, viewing $\mathbf{Q}$ as a discrete group, the compact abelian dual group turns out to be the quotient group $\mathbf{A_Q}/\mathbf{Q}$.

The adele ring $\mathbb{A}_K$ of a number field K is defined as the set of all tuples $(x_v)_v$ with $x_v \in K_v$ where all but finitely many of the x_v are in $\mathcal{O}_v$.

To define the topology on adeles, consider any finite set S of places of K containing all the archimedean ones; the product ring $\prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v$ is locally compact as S is finite.

As S varies, these products form a basis of neighbourhoods of zero for a unique topology on $\mathbb{A}_K$ for which it is a locally compact ring.

Tate's thesis made a single Fourier-analytic computation "adelically" to recover the functional equation of the Riemann zeta function, explain the Gamma factor as the term corresponding to the "infinite prime" and pave the way to obtain functional equations for more general L-functions.

Indeed, the Gaussian function $f_\infty(x) = e^{-\pi x^2}$ is its Fourier tranform, and its Mellin transform is $\pi^{-s/2}\Gamma(s/2)$.

Similarly, in the p-adic ring $\mathbb{Z}_p$, the characteristic function χ_p is its own Fourier transform and its Mellin transform turns out to be $(1 - 1/p^s)^{-1}$.

Thus, taking the "Schwartz" function $f = f_\infty \prod_p \chi_p$ on the adele ring, the corresponding Poisson summation formula (for the lattice $\mathbb{Q}$ in $\mathbb{A}_\mathbb{Q}$) is

$$\sum_{a \in \mathbb{Q}} f(at) = \sum_{a \in \mathbb{Q}} f(t/a)$$

whose Mellin transform gives the functional equation for ζ and also explains that the Gamma factor is the contribution at the infinite prime of $\mathbb{Q}$.

The above was generalized to ideles also by Tate.

More generally, for a matrix group like $GL_n(K)$ (or an algebraic subgroup $G \subset GL_n$ defined over K), one can naturally consider the groups $G(K_v)$ and $G(\mathcal{O}_v)$ for all places v of K.

The groups $GL_n(K_v)$ are locally compact.

One has the 'adelic group' $G(\mathbf{A}_K)$ which has a basis of neighbourhoods of the identity given by $GL_n(\mathbb{A}_S) = \prod_{v \in S} G(K_v) \times \prod_{v \notin S} G(\mathcal{O}_v)$ as S varies over finite sets of places containing all the archimedean places of K - for $n = 1$ this is the idele group of K.

The diagonal embedding of $G(K)$ in $G(\mathbf{A}_K)$ embeds it as a discrete subgroup.

Unlike $\mathbf{A}_K/K$ which is compact, the quotient space $GL_n(\mathbf{A}_K)/GL_n(K)$ (this is not a group) is not compact; it does not even have finite 'measure' for a Haar measure of the adele group.

However, the finiteness of measure holds modulo the group Z of scalar matrices.

In fact, the double coset space $GL_n(\mathbb{A}_\infty)\backslash GL_n(\mathbb{A})/GL_n(K)$ can be identified with the class group of the number field K.

For a Grossencharacter ω (a character of $GL_1(\mathbf{A}_K)/GL_1(K)$), it makes sense to consider the following Hilbert space consisting of measurable functions on the quotient space $GL_n(\mathbf{A}_K)/GL_n(K)$ with certain properties which remind us of transformation properties of modular forms.

This is the Hilbert space $L^2(GL_n(\mathbf{A}_K)/GL_n(K), \omega)$ of those measurable functions ϕ which satisfy:

(i) $\phi(zg) = \omega(z)\phi(g), z \in Z$;

(ii) $\int_{GL_n(\mathbf{A}_K)/Z.GL_n(K)} |\phi(g)|^2 dg < \infty$.

The subspace $L_0^2(GL_n(\mathbf{A}_K)/GL_n(K), \omega)$ of cusp forms is defined by the additional conditions corresponding to any parabolic subgroup.

The latter are conjugates in GL_n of 'ladder' groups

$$P_{n_1,\cdots,n_r} = \left\{\begin{pmatrix} g_1 & \cdots & \cdots & \\ 0 & g_2 & \cdots & \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_r \end{pmatrix}\right\}$$

The standard parabolic $P_{n_1,\cdots,n_r}$ is a semidirect product of its unipotent radical

$$U = \left\{\begin{pmatrix} I_{n_1} & \cdots & \cdots & \\ 0 & I_{n_2} & \cdots & \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & I_{n_r} \end{pmatrix}\right\}$$

and $GL_{n_1} \times \cdots \times GL_{n_r}$.

Any parabolic subgroup P has a similar semidirect product decomposition $P = M \propto U$.

The parabolic subgroups are characterized by the condition that they are closed subgroups such that $GL_n(\mathbf{C})/P(\mathbf{C})$ is compact.

The additional 'cuspidality' condition for a parabolic subgroup P is

$$\int_{U_P(\mathbf{A}_K)/U_P(K)} \phi(ug)du = 0 \ \ \forall \ \ g \in GL_n(\mathbf{A}_K).$$

The adele group acts as unitary operators by right multiplication on the Hilbert space $L^2(GL_n(\mathbf{A}_K)/GL_n(K), \omega)$ and leaves the space of cusp forms invariant.

By definition, a subquotient of this representation is called *an automorphic representation* of $GL_n(\mathbf{A}_K)$.

Moreover, a sub-representation of the representation on cusp forms is said to be a *cuspidal automorphic representation*.

One further notion is that of an *admissible* representation of the adele group - this is one which can contain any irreducible representation of a maximal compact subgroup of the adele group only finitely many times.

A theorem of D.Flath tells us: Any irreducible, admissible representation of the adele group is a 'restricted' tensor product of unique irreducible representations of $GL_n(K_v)$.

Further, for an admissible automorphic representation $\pi = \otimes_v \pi_v$, the representation π_v belongs to a special class known as the unramified principal series for all but finitely many v.

An unramified principal series representation π_v is one whose restriction to $GL_n(\mathcal{O}_v)$ contains the trivial representation; a certain isomorphism theorem due to Satake shows that corresponding to π_v, there is a conjugacy class in $GL_n(\mathbf{C})$ of a diagonal matrix of the form

$$A_v = diag(N(v)^{-z_1}, \cdots, N(v)^{-z_n})$$

for some n-tuple $(z_1, \cdots, z_n) \in \mathbf{C}^n$.

Corresponding to an admissible, automorphic representation $\pi = \otimes_v \pi_v$, Langlands defined an L-function.

If S is the finite set of places outside of which π_v is unramified principal series, define for $v \notin S$,

$$L(s, \pi_v) = det(1 - A_v N(v)^{-s})^{-1}.$$

If $L_S(s, \pi) := \prod_{v \notin S} L(s, \pi_v)$, then Langlands proved that this product has a meromorphic extension to the whole complex plane.

Defining $L(s, \pi_v)$ for $v \in S$ in a suitable manner, it also follows that $L(s, \pi) = \prod_v L(s, \pi_v)$ has meromorphic continuation, and a functional equation.

If π is cuspidal automorphic also, Godement & Jacquet showed:

$L(s, \pi)$ is an entire function unless $n = 1$ and $\pi = |.|^t$ for some $t \in \mathbf{C}$.

Generalized Ramanujan-Petersson conjecture: *If π is cuspidal automorphic, then the eigenvalues of A_v have absolute value 1 for all v. Equivalently, for such a π, the matrix coefficients of π_v, for each prime p, belongs to $L^{2+\epsilon}(GL_n(\mathbf{Q}_p)/Z(\mathbf{Q}_p))$ for any $\epsilon > 0$.*

Selberg's $(1/4)$-eigenvalue conjecture can be interpreted as asserting that π_∞ is a tempered representation of $GL_n(\mathbf{R})$.

Langlands Reciprocity conjecture: *Let L/K be a Galois extension of number fields and let G be the Galois group. Let (ρ, V) be an n-dimensional complex representation of G. Then, there is a cuspidal automorphic representation π of $GL_n(\mathbf{A}_K)$ such that $L(s, \rho; L/K) = L(s, \pi)$.*

This is just Artin's reciprocity law when ρ is 1-dimensional.

Grand Riemann Hypothesis: *All the zeroes of $L(s, \pi)$ for a cuspidal automorphic representation π, lie on $\mathrm{Re}\,(s) = 1/2$.*

The Grand Riemann Hypothesis has several concrete number-theoretic consequences; for instance, it implies the Artin primitive root conjecture which asserts that any non-square $a \neq -1$ is a primitive root for infinitely many primes.

Langlands Functoriality Conjecture

Let G be a reductive algebraic group over a global field K.

The complex group $\hat{G}$ defined by the Dynkin diagram dual to that defined by G plays the role of a parameter space for representations of G; this information has to be augmented by another piece as G is not always split.

Given an isomorphism ϕ of a maximal torus with the product of GL_1's that is defined over the algebraic closure of $\mathbb{Q}$, for elements σ in the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$, $\sigma(\phi)\phi^{-1}$ give the obstruction to ϕ being defined over $\mathbb{Q}$.

This map determines a homomorphism from $G_{\mathbb{Q}}$ to the group $Out(G)$ of outer automorphisms of G (which is also $Out(\hat{G})$).

Langlands introduced the semidirect product group ${}^LG := G_{\mathbb{Q}} \propto \hat{G}$ - called the Langlands dual group of G.

For instance, for $G = GL_n$, $\hat{G} = GL(n, \mathbb{C})$ and so,
${}^LG = Gal(\bar{K}/K) \times GL(n, \mathbb{C})$.

For $G = SO_{2n+1}$, $\hat{G} = Sp(2n, \mathbb{C})$ and so,
${}^LG = Gal(\bar{K}/K) \times GL(n, \mathbb{C})$.

For $G = Sp_{2n}$, $\hat{G} = SO(2n+1, \mathbb{C})$ and so,
${}^LG = Gal(\bar{K}/K) \times SO(2n+1, \mathbb{C})$.

If G is a unitary group defined by a quadratic extension of K, the group $\hat{G}$ is $GL(n, \mathbb{C})$ but the action of the Galois group is nontrivial and the group ${}^LG$ is a semidirect product $Gal(\bar{K}/K) \propto GL(n, \mathbb{C})$ now.

For general G, the action of $G_{\mathbb{Q}}$ factors through a finite quotient $Gal(K/\mathbb{Q})$.

Similar to the GL_n case, unramified representations π_p can be defined on $G(\mathbb{Q}_p)$ if G is quasi-split (which happens for almost all primes p).

Therefore, one has semisimple conjugacy classes $c(\pi_p)$ in $Gal(K/\mathbb{Q}) \propto \hat{G}$ for almost all p.

Thus, for an automorphic representation $\pi = \otimes_p \pi_p$ of $G(\mathbb{A})$, one has the data of the family of conjugacy classes $c(\pi_p)$ for almost all p; say $p \notin S(\pi)$.

This is viewed as analytic data.

The conjugacy classes $c(\pi_p)$ are to be viewed as eigenvalues of (general) Hecke operators.

The principle of functoriality describes deep (conjectural) relationships among automorphic representations of different groups by means of the corresponding families of semisimple conjugacy classes:

Langlands Functoriality Conjecture: Suppose G, G' are reductive with G quasi-split, and suppose $\rho :^L G' \to^L G$ is an algebraic homomorphism. Then, for any automorphic representation π' of G', there is a corresponding automorphic representation π of G such that $c(\pi_p) = \rho(c(\pi'_p))$ for $p \not\in S(\pi) \cup S(\pi')$.

When G' is trivial, $G = GL_n$ and $\rho : Gal(K/\mathbb{Q}) \to GL_n(\mathbb{C})$, the functoriality conjecture is quite concrete and asserts that there is an automorphic representation π of GL_n such that $c(\pi_p) = \rho(Frob_p)$ for all $p \not\in S$.

Thus, for a faithful ρ, one obtains a "nonabelian reciprocity law":

$$Spl(K) = \{p \not\in S : c(\pi_p) = 1\}.$$

For $n = 1$, this reduces to the theorem of Kronecker-Weber.

For $n = 2$, when K is a solvable extension, this was proved by Langlands and Tunnel; this was an important ingredient of Wiles's proof of FLT.

For general n, when K is a nilpotent extension, this was proved by Arthur and Clozel using something called Base Change.

We saw that functoriality entails producing an automorphic representation form a Galois representation but the converse is not true!

There are more automorphic representations than those which correspond to Galois representations.

Langlands conjectured the existence of a universal group $L_{\mathbb{Q}}$ whose n-dimensional representations parametrize automorphic representations of GL_n.

Local Langlands Correspondence

Langlands himself proved the LLC over $\mathbb{R}$ and $\mathbb{C}$ via his Langlands classification.

For GL_n over a local field of positive characteristic, it was proved by Laumon, Rapoport and Stuhler in 1993.

Later, in 2000, Harris, Taylor and Henniart proved the LLC for GL_n over nonarchimedean local fields of characteristic 0.

One feature of representation theory over local fields is the complication coming from L-indistinguishability (two groups having the same L-functions) and one studies L-packets (finite sets of representations of one group corresponding to each representation of the other).

Langlands conjectures for function fields

A geometric Langlands Program - analogue of the Langlands functoriality conjecture over global function field - was formulated by Drinfeld and Laumon. Due to the efforts of Drinfeld, Laumon, Lafforgue and Lomeli, these have been proved for classical groups.

THANK YOU!