ABOUT MAIN CONJECTURES

I have been asked by Vasily Golyshev to give a short general lecture 'About Main Conjectures' (regarding L-functions) in this summer seminar (on motivic gamma functions). I'm delighted to do that!

Vasily wrote that the seminar is more of "a 'basic notions' seminar focusing on "grand design" so that "we understand what it all is about" (rather than technical reports, or reports about new work).

And he also mentioned that it should be no more than half an hour long or a bit more—to allow for questions.

Given such an assignment for this seminar I realized that I had better re-consider the scope of '*Main Conjectures*' viewing that notion as encompassing classical Iwasawa Main Conjectures but much broader, in hopes to learning whether motivic gamma functions—i.e., the topic of this seminar—might eventually fit into that framework .

Of course any mathematical field is entitled to designate one of its goals as its "Main Conjecture." At one time I was very much taken with issues related to a certain *Main Conjecture* usually referred to as the *Hauptvermutung*; but that was in geometric topology, and over six decades ago.

The Main Conjectures we will be concerned with here are of a different sort. They consist of the 'coming together' of two different mathematical structures or viewpoints, and are part of a trio consisting of these things:

The 'Trio':

  (i) "Analytic Formulas" **(AF)**
 (ii) "Main Conjectures" (per se) **(MC)**
(iii) "Explicit Formulas" **(EF)**.

I've listed them in what I think of as a natural ordering.

I won't have time today to discuss **(EF)** *and how Explicit Formulas tie in with the other two categories.*

Analytic Formulas

We'll organize the ingredients of an **Analytic Formula** so that its 'left-hand-side' (LHS) isolates *an interesting arithmetic quantity*; and its 'right-hand-side' (RHS) consists of the value of *an interesting analytic function* at a specified point (times some elementary factor $\mathcal{E}$).

arithmetic quantity $=$ *special value of analytic function* $\times$ $\mathcal{E}$

The Dirichlet Ideal Class Number Formula

The simplest example of such a formula is the Dirichlet Ideal Class Number Formula for Imaginary Quadratic Fields. So, take $F := \mathbb{Q}[\sqrt{-d}]$ where d is a square-free positive number, and let

- $h :=$ the class number of F—i.e., the order of the ideal class group of F,

    and

- $L(\chi_F, s) :=$ the L-function of $\chi_F : \mathbb{Z} \to \{\pm 1\}$ the Dirichlet character attached to F. I.e., the analytic continuation to the entire complex plane of the Dirichlet series:

$$\sum_{n \geq 1} \chi_F(n) n^{-s}.$$

The *Class Number Formula* cleanly connects the fundamental arithmetic invariant of F, namely the class number h, to a fundamental analytic invariant of F; namely the value of $L(\chi_F, s)$ at the point $s = 1$:

`cnf`   (0.1) $h \;=\; L(\chi_F, 1) \cdot \mathcal{E}$

Here $\mathcal{E}$ is a combination of relatively elementary factors:

$$\mathcal{E} := w \cdot \sqrt{|D_F|}/2\pi.$$

where

- $w :=$ the number of roots of unity in F (i.e., w=2; unless $d = 1$, or $d = 3$),

and

- $D_F :=$ the discriminant of F.

This picture of the nature of the analytic formula **(AF)** persists for any number field, but more generally the connection is not as simple as the relationship between:

the class number h on the (LHS) of the formula
and
some simple Dirichlet L-function on the (RHS)

but rather:
- the (LHS) will be the arithmetic invariant

$$\boxed{h \cdot \text{Reg}}$$

where Reg is the regulator of the field
and
- the(RHS) will have the value at the point $s = 1$ of

the ratio of the zeta-function of the field, divided by the Riemann zeta-function (times an elementary factor).

Synopsis: an analytic formula makes the arithmetic/analytic connection:

arithmetic quantity related to F
$\updownarrow$
value at $s = 1$ of an analytic function.

Question: what is the 'go-between' that ties the *arithmetic* to the *analytic* in the **(AF)**?

Answer: a volume computation that gives an asymptotic estimate for the number of ideals of norm $\leq X$.

The Birch-Swinnerton-Dyer Conjecture

The classical Birch-Swinnerton-Dyer Conjecture is perfectly in this "**(AF)**" form.

That is—first, if E is an elliptic curve over a number field K *such that is group of rational points $E(K)$ is finite* then the order of the Shafarevitch-Tate group $|Sha(E;K)|$ of E over K is the arithmetic quantity associated to $E_{/K}$ that will enter as the (LHS) of the conjecture.

This is the quantity corresponding to the ideal class group of a number field K.

The set $Sha(E;K)$ is defined to be the collection of isomorphism classes of curves of genus 1 whose jacobians are equal to E and which have rational points over any completion of K (and hence are isomorphic to E over those completions). It has a natural abelian group structure, and is conjectured to be finite.

Then *if $E(K)$—the (Mordell-Weil) group of K-rational points of E— is finite* the classical Birch-Swinnerton-Dyer Conjecture offers, for the arithmetic of $E_{/K}$, an analogue to Equation 0.1 above:

`bsc`   (0.2)
$$|Sha(E;K)| = L(E_{/K};1) \cdot \mathcal{E}$$

where, $L(E_K, s)$ is the Hasse-Weil L-function of E over the field K. And where, again, $\mathcal{E}$ is a combination of relatively elementary factors that includes the period of the elliptic curve E and the number of K-rational torsion points it has. Moreover, if $E(K)$ is not finite, but of rank $r > 0$, then the (LHS) of Equation 0.2 should be replaced by

$$\boxed{|Sha(E;K)| \cdot \mathrm{Reg}(E;K)}$$

where $\mathrm{Reg}(E;K)$ is the regulator of E over K (which is the determinant of an $r \times r$ matrix whose entries come from consideration of the heights of elements in the group $E(K)$); and the (RHS) should be replaced by

$$\boxed{L^{(r)}(E_{/K};1)}$$

times a certain concoction of elementary factors. Here $L^{(r)}(E_{/K}; 1)$ means the r-th derivative of $L(E_{/K}; s)$ evaluated at the point $s = 1$.

Main Conjectures

Conjectures that I want to include in this **(MC)** category will be proposing a similar arithmetic/analytic connection. Note that in the formulation of this category, I'll still keep the adjective "conjecture" even for such statements that have already been proved, or once they're proved. The apparatus needed for such an **(MC)** consists of:

A linear space and operator on it
related to the arithmetic of interest
$\updownarrow$
zeros of an analytic function.

More specifically:

The arithmetic side:

- **(A linear space and operator)** First, you have to be given some type of linear space **H** and some specified linear operator

$$\gamma : H \to H$$

 acting as endomorphism on it. Both **H** and γ should be of fundamental arithmetic interest—for example **H** might contain information classifying certain important arithmetic objects, the linear operator γ being a natural added feature of this classification.

The possible kinds of **H** : The 'linear space' **H** could be
- a finite dimensional p-adic (or complex) vector space;
- a graded vector space;
- or a Hilbert space,
- or Banach space,
- or simply a module over an appropriate ring containing γ, such as $\mathbf{Z}_p[[\gamma]]$ where the action of γ on **H** is via this module structure.

The analytic side:

- **(A meromorphic function)** Second, you should be given a specified meromorphic (but usually analytic) function,

$$\lambda(s),$$

  complex or p-adic—depending on the situation—of fundamental interest. It may come from some other mathematical program; it could be an L-function; and, at least sometimes if you're lucky, it could be more accessible than any construction of the $(\mathbf{H}, \gamma)$ above.

A "Main Conjecture" **(MC)** then posits a direct relationship between:

$$\text{the eigenvalues of } \gamma \quad \text{and} \quad \text{the zeros of } \lambda(s);$$

—or in the case where $\mathbf{H}$ is a $\mathbf{Z}_p[[\gamma]]$-module as alluded to above, the Main Conjecture might identify:

$$\text{locus of zeros of } \lambda(s) \quad \leftrightarrow \quad \text{support of the } \mathbf{Z}_p[[\gamma]]\text{-module } \mathbf{H}.$$

Ridiculously Broad

The program **MC** just sketched is so broad that it might ridiculously allow elementary theorems (such as the fact that *the zeros of the characteristic polynomial*

$$\lambda(X) := \det(X \cdot I_n - A)$$

are the eigenvalues of the $n \times n$ matrix A) to fit it's framework.

But ... **note:** Consider $\lambda(s) :=$ the characteristic series of $\gamma :=$ the Laplacian operator Δ acting on $\mathbf{H} = $ the space of L^2 functions on a Riemannian manifold—and this is already *interesting*, [and it has its connection, thanks to Selberg, to the lengths of closed geodesics].

Linnaean classification:

Here is a Linnaean classification of the various results that might, more appropriately, go under that rubric (even though they may not have been called **MC** traditionally). I will order them so that items further down in the list were (at least in some instances) inspired because they were analogous to items earlier in the list.

(i) **The Hilbert-Pólya dream** is that there is some Hilbert Space **H** and self-adjoint unbounded operator

$$\gamma : \mathbf{H} \to \mathbf{H},$$

this structure constructed in some essential way from 'arithmetic' in such a way that the classical Riemann zeta-function (after appropriate normalization) is equal to the characteristic series of this operator γ. *(If this 'dream' is true–and identifies the nontrivial zeros of the zeta function with the eigenvalues of the self-adjoint operator γ—the Riemann Hypothesis would follow.)*

Comments: The history behind this 'dream' is obscure. I'm not sure to what extent Hilbert himself had anything to do with it. See Andrew Odlyzko's correspondence trying to get closer to its history: `http://www.dtc.umn.edu/~odlyzko/polya/index.html`. The first published account of it seems to be:

Montgomery, Hugh L. (1973), "The pair correlation of zeros of the zeta function", Analytic number theory, Proc. Sympos. Pure Math., XXIV, Providence, R.I.: American Mathematical Society, pp. 181193, MR 0337821

Mention Alain Connes' work—and Don Zagier's.

(ii) **Cohomology of varieties over finite fields as an "(MC)"**

—Weil, Grothendieck, Deligne, . . .

Let k be a finite field of characteristic p—so $k \simeq \mathbf{F}_q$ for q a power of p. Denote by $\bar{k}$ its algebraic closure. The Frobenius automorphism (which we'll denote $\gamma : x \mapsto x^q$) is a topological generator of the profinite Galois group $\mathrm{Gal}(\bar{k}/k)$.

If V is a projective variety over k and ℓ a prime number different from p, we can take **H** to be the graded finite dimensional ℓ-adic vector space given by étale cohomology $H^{\cdot}_{et}(V_{\bar{k}}; \mathbb{Q}_\ell)$ and the operator γ on it given by Frobenius. Take $\lambda(s) :=$ the zeta-function of $V_{/k}$.

Appropriately normalized, the alternating product of the characteristic polynomials of the operator γ acting on the graded pieces of $H^{\cdot}_{et}(V_{\bar{k}}; \mathbb{Q}_\ell)$ *is equal to* $\lambda(s) :=$ the zeta-function of $V_{/k}$.

SO again we have the apparatus $(\mathbf{H}, \gamma; \lambda(s))$ with the structure that we've characterized above as a 'Main Conjecture.' The eigenvalues of γ on $\mathbf{H}$ give us, after suitable normalization the zeros of $\lambda(s)$.

In fact, André Weil himself seems to have been inspired by the Hilbert-Pólya dream described above, in conjecturing such a structure. This structure was later shown to exist by Grothendieck; and then shown by Deligne to satisfy the analogue of the Riemann Hypothesis.

(iii) **The classical Iwasawa Main Conjecture:**

Iwasawa, in turn, translated Weil's work—by analogy—into a fundamental project in arithmetic.

In analogy with the (algebraically closed) field extension $\bar{k}/k$ of the finite field k—where we took γ to be the topological generator of the Galois group $\mathrm{Gal}(\bar{k}/k)$ given by the Frobenius automorphism,

Iwasawa—fixed a (say: odd) prime number p and started with a number field K as his base field—

(for us, take the simplest such K in Iwasawa's consideration; namely $K = \mathbb{Q}[e^{2\pi i/p}]$).

p-cyclotomic tower as analogue of algebraic closure of a finite field Iwasawa then considered the infinite degree p-cyclotomic tower K_∞/K obtained by adjoining to K the p^n-th roots of unity $e^{2\pi i/p^n}$ for all n, noting that as in Weil's set-up the profinite group $\mathrm{Gal}(K_\infty/K)$ is again topologically cyclic and can be generated by the automorphism γ that sends any p^n-th roots of unity α to α^{1+p}. By the 'p-cyclotomic tower' is meant the sequence of fields:

(0.3)
$$K = K_1 \subset K_2 = K[e^{2\pi i/p^2}] \subset \cdots \subset K_n = K[e^{2\pi i/p^n}] \subset \cdots \subset K_\infty,$$

This already is a neat global arithmetic set-up that corresponds to Weil's set-up over finite fields.

Iwasawa defines his global arithmetic linear space $\mathbf{H}$—which turns out to be a finite-dimensional vector space over the field

of p-adic numbers $\mathbb{Q}_p$, admitting γ as a (naturally defined) linear operator—as follows:

Let $A_n :=$ the p-primary component of the ideal class group of the field K_n, i.e., of the n-th rung of the p-cyclotomic tower (0.3).

Let $\hat{A}_n = Hom(A_n, \mathbb{Q}/\mathbb{Z})$ be the dual group. These are all p-power abelian groups; so they can be thought of as (finite) modules over the ring of p-adic integers $\mathbb{Z}_p$.

Inductive sequence of ideal class groups ascending the tower For $m > n$ there is a natural mapping $A_n \to A_m$ given by assigning to (the class of) any ideal I of the ring of integers in K_n (the class of) the ideal generated by I in the ring of integers in K_m. So, passing to the duals, we get natural maps the other way: $\hat{A}_m \to \hat{A}_n$. The projective limit of this sequence,

$$\lim_{n \to \infty} \hat{A}_n$$

is then a natural $\mathbb{Z}_p[[\gamma]]$-module.

Our H:

Take:

(0.4)
$$\mathbf{H} := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \lim_{n \to \infty} \hat{A}_n$$

as our linear space; the automorphism γ acts naturally on $\mathbf{H}$. Iwasawa showed that $\mathbf{H}$ is a finite dimensional vector space (over $\mathbb{Q}_p$). Or... if we use class field theory Class field theory establishes a natural identification of the ideal class group, $Cl(K)$, of a number field K with the Galois group $\mathrm{Gal}(L/K)$ where L is the maximal (everywhere unramified) abelian extension of K,

$$Cl(K) \quad \overset{\sim}{\leftrightarrow} \quad \mathrm{Gal}(L/K),$$

so we can work out another description of $\mathbf{H}$ in terms of a projective limit of the p-primary components of these Galois groups, going up the p-cyclotomic tower. The *arithmetic side* of the Iwasawa Main Conjecture To give a slightly more precise picture one should note that there's also the cyclic group of order $p - 1$,

$$\Delta := \mathrm{Gal}(\mathbb{Q}[e^{2\pi i]/p}]/\mathbb{Q})$$

acting naturally on this $\mathbf{H}$ which breaks $\mathbf{H}$ up into components $\mathbf{H}^i$ dependent on the characters ω^i of Δ (where ω is the Teichmüller character, generating the group of characters of Δ and i is taken mod $p - 1$. Each of these components are considered separately.

This gives us the *arithmetic side* of the Iwasawa Main Conjecture. The *analytic side* is also neat:

Kubota and Leopoldt had produced p-adic analytic functions that are the "p-adic companions" of Dirichlet L-functions $L(\chi; s)$. By "companions" I mean, that these are p-adic analytic functions $L_p("\chi"; "s")$ that—with suitable normalizations—agree with the corresponding Dirichlet L-function in their values, at *enough* pairs $(\chi, 1)$—

Enough, that is, so that the p-adic L-function $L_p("\chi"; "s")$ is uniquely determined by this property. These $L_p("\chi"; "s")$ are, in a sense, the (p-adic) analytic continuations to the p-adic plane of the corresponding 'classical' Dirichlet L-function.

<p style="text-align:center"><i>Explain the quotation marks</i></p>

The *analytic side:*

I'll rename the p-adic L-function $L_p("\chi"; "s")$ that is the companion of the classical L-function $L(\omega^{1-i}, s)$:

$$\lambda(i; s)$$

(it isn't referred to this way elsewhere!)

In brief, then, the Iwasawa Main Conjecture makes a direct connection between our arithmetic object and our analytic function:

<p style="text-align:center">Eigenvalues of γ on $\mathbf{H}^i$ for <i>odd</i> values of i
$\updownarrow$
Zeros of $\lambda(i; s)$.</p>

Two questions might arise:

(a) The Iwasawa Main Conjecture, as described, asks about a connection between something built out of ideal class groups and something built out of Dirichlet L-functions. BUT... we already have available to us the classical analytic formula as described above which makes a neat connection between those mathematical objects... *so why is it difficult to make Iwasawa's conjectured connection as described above?*

(b) The format of the Iwasawa Main Conjecture is so much like the Hilbert-Pólya dream that one can't help wondering whether there is some p-adic analogue of the classical Riemann Hypothesis.
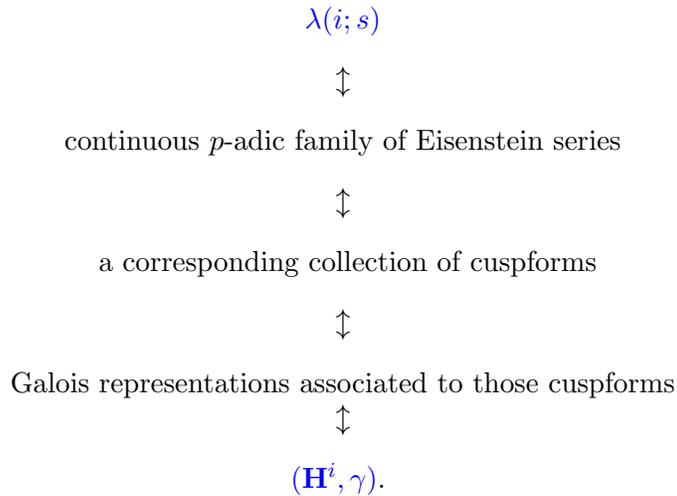
I have no idea about (ii). About (i): the reason is fundamentally that:

the analytic formula is a statement about the sizes of things, with nothing much about structure—even nothing directly usable about the way in which γ acts. To get information about the precise action of γ, it is helpful to actually have a controlled way of **constructing abelian unramified extensions**—or, more generally, abelian extensions with prescribed ramification—controlled in such a way that it and the action of γ **connects with the behavior of the relevant p-adic L-function**. The analytic formula is certainly helpful though: once you have constructed all the abelian extensions you need to construct, it 'guarantees' that you have don that: constructed all you need to construct.

The 'go-betweens'

In the original proof of Iwasawa's Main Conjecture, Andrew Wiles and I made use of a method begun by Ken Ribet (used in his proof of Herbrand's Conjecture). Wiles and I were guided by the wonderful fact that the p-adic Eisenstein series has—as constant term—the appropriate value of the p-adic L-function.

And the go-betweens between the $(\mathbf{H}^i, \gamma)$ and $\lambda(i; s)$ are:

$$\lambda(i; s)$$

$$\updownarrow$$

continuous p-adic family of Eisenstein series

$$\updownarrow$$

a corresponding collection of cuspforms

$$\updownarrow$$

Galois representations associated to those cuspforms

$$\updownarrow$$

$$(\mathbf{H}^i, \gamma).$$

The continuous p-adic family of Eisenstein series: This is a construction of Serre in *Formes modulaires et fonctions zêta p-adiques*: a p-adic interpolation of the Fourier coefficients of the classical family of Eisenstein series. More exactly we may form, for

every p-adic weight κ that projects to the even number $i \neq 0$ modulo $p - 1$, the p-adic continuous series of 'p-adic Hecke eigenforms on $\Gamma_0(p)$':

$$\mathrm{Eis}_\kappa^{\{p\}}(q) := -\frac{1}{2}L_p(\omega^i; 1 - \kappa) + \sum_n \Big\{ \sum_{d \,\mid\, n} d^{\{\kappa\}} \Big\} \cdot q^n \ \subset \mathbb{Z}_p[[q]].$$

Here ω is the Teichmüller character, and $L_p(s, \chi)$ is the Kubota-Leopoldt p-adic L-function. ... **And if this L-function value is p-adically close to** 0**,** the Fourier series of that Eisenstein series would (one shows) be equally close—p-adically—to that of a cuspidal newform.

Reading this the opposite way: there exists a cuspidal newform whose Fourier series is p-adically close to that of an Eisenstein series.

Connecting these cusp forms to the Galois representation on the torsion points of the jacobian of an appropriate modular curve: the Galois action on those torsion points constructs, for us, an abelian unramified extension of the sort we need.

Andrew Wiles extended the result to any totally real base field— a simpler proof of this Main Conjecture was later given by Karl Rubin.

(iv) **The Main Conjecture for elliptic curves and automorphic forms:**

These conjectures are, in turn, strict analogues or extensions of Iwasawa's classical Main Conjecture. They are conjectures concerning the arithmetic of an elliptic curve E over K or an automorphic form π for a reductive group over K.

- One makes a choice of a prime p and considers, exactly as before, the p-cyclotomic tower.

- What corresponds to the sequence of p-primary components of ideal class groups A_n of the ring of integers in K_n are—once on takes certain things into consideration—the p-primary components of Selmer groups $Selm(E; K_n)$, these being extensions of p-primary components of $Sha(E; K_n)$ by a contribution related to the size of $E(K_n)$.

- What corresponds to the p-adic L function $L_p(\chi, s)$ are the p-adic L-functions $L_p(E, \chi; s)$ or $L_p(\pi, \chi; s)$—at least in the cases where these have been constructed.

The corresponding "$(\mathbf{H}, \gamma, \lambda(s))$"-structure

Once one makes those corresponding changes one comes up with a $(\mathbf{H}, \gamma, \lambda(s))$ allowing us to formulate a "Main Conjecture." The role played by the classical analytic formula in our discussion of the classical Iwasawa Main Conjecture is comparable to the relationship between the Swinnerton-Dyer Conjecture and the Main Conjecture for elliptic curves.

A comment on variations of Main Conjectures:

Nowadays there is the broad project of considering classical modular eigenforms or more general automorphic forms π not singly, but rather as varying p-adically (i.e., their Fourier expansions are p-adically interpolated—two eigenforms π, π' being 'close' if the coefficients of their Fourier expansions are p-adically close.

Limits of these constitute 'p-adic automorphic forms—their Fourier expansion having p-adic coefficients.

Eigenvarieties:

The natural parameter spaces of variation are called *eigenvarieties* and have the structure of rigid-p-adic analytic spaces. It's natural to study, and conjecture about, corresponding variations of the apparatus $(\mathbf{H}, \gamma, \lambda(s))$ associated to such p-adic automorphic forms π, the variation being rigid p-adic analytic, parameterized over these eigenvarieties.

'Go-betweens'

Returning to the thought that a 'Main Conjecture' must bridge:

Eigenvalues of γ on an arithmetic object $\mathbf{H}$
$$\updownarrow$$
Zeros of an analytic object $\lambda(s)$,
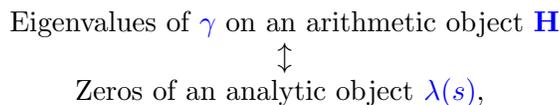
you might ask: what could possibly be the *go-between* that connect this arithmetic structure with this analytic structure? E.g., what sort of thing lives in both worlds at the same time?

Euler Systems as 'Go-betweens'

Euler Systems–very roughly—are a tightly connected system of algebraic cycles on a certain arithmetic scheme ascending a cyclotomic tower: they control,

- on the one hand: L-functions related to this situation, and
- on the other hand, by a 'Kummer construction" they also control relevant cohomology related to the associated Galois representation.

E.g., Very recently, David Loeffler and Sarah Livia Zerbes proved (under some hypotheses) the Iwasawa main conjecture for quadratic Hilbert modular forms over the p-cyclotomic tower using an Euler system in the cohomology of Siegel modular varieties (arXiv:2006.14491).