

Iwasawa theory: a climb up the tower

Romyar Sharifi

Iwasawa theory is an area of number theory that emerged from the foundational work of Kenkichi Iwasawa in the late 1950s and onward. It studies the growth of arithmetic objects, such as class groups, in towers of number fields. Its key observation is that a part of this growth exhibits a remarkable regularity, which it aims to describe in terms of values of meromorphic functions known as L -functions, such as the Riemann zeta function.

Through such descriptions, Iwasawa theory unveils intricate links between algebraic, geometric, and analytic objects of an arithmetic nature. The existence of such links is a common theme in many central areas within arithmetic geometry. So it is that Iwasawa theory has found itself a subject of continued great interest. This year's Arizona Winter School attracted nearly 300 students hoping to learn about it!

The literature on Iwasawa theory is vast and often technical, but the underlying ideas are possessing of an undeniable beauty. I hope to convey some of this, while explaining the original questions of Iwasawa theory and giving a sense of the directions in which the area is heading.

Algebraic number theory

To understand Iwasawa theory requires some knowledge of the background out of which it arose. We attempt to chart a course, beginning with a whirlwind tour of the elements of algebraic number theory. We make particular note of two algebraic objects, the class group and the unit group of a number field, that play central roles for us.

Algebraic numbers are the roots inside the complex numbers of nonzero polynomials in a single variable with rational coefficients. They lie in finite field extensions of \mathbb{Q} called number fields. The set

of algebraic numbers forms a subfield $\overline{\mathbb{Q}}$ of \mathbb{C} known as an algebraic closure of \mathbb{Q} . Inside $\overline{\mathbb{Q}}$ sits a subring $\overline{\mathbb{Z}}$ of algebraic integers, consisting of the roots of monic polynomials with integer coefficients.

The field automorphisms of $\overline{\mathbb{Q}}$ form a huge group called the absolute Galois group $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. These automorphisms permute the roots of each rational polynomial, and consequently this action preserves the algebraic integers.

We'll use F to denote a number field. The integer ring \mathcal{O}_F of F is the subring of algebraic integers in F . It is a PID if and only if it's a UFD, but unlike $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, it need not in general be either. Rather, \mathcal{O}_F is what is known as a Dedekind domain. As such, it has the property that every nonzero ideal factors uniquely up to ordering into a product of prime ideals. This property provides a replacement for unique factorization of elements. A "prime" of F is a nonzero prime ideal of \mathcal{O}_F .

A fractional ideal of F is a nonzero, finitely generated \mathcal{O}_F -submodule of F . In particular, nonzero ideals of \mathcal{O}_F are fractional ideals, but so for instance are all \mathcal{O}_F -multiples of $\frac{1}{2}$. The set I_F of fractional ideals is an abelian group under multiplication with identity \mathcal{O}_F . The class group Cl_F of F is the quotient of I_F by its subgroup of principal fractional ideals generated by nonzero elements of F . The group Cl_F is trivial if and only if \mathcal{O}_F is a PID.

Remarkably, Cl_F is finite. Its order h_F is known as the class number. Like the class group itself, it is the subject of many open questions. For instance, work of K. Heegner, A. Baker, and H. Stark in the 1950s and 60s solved a problem of Gauss by showing that there are exactly nine imaginary quadratic fields with class number one: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, On the other hand, Gauss' conjecture that there are infinitely many such real quadratic fields is still open.

Romyar Sharifi is professor of mathematics at UCLA. His email address is sharifi@math.ucla.edu.

This material is based upon work supported by the National Science Foundation under Grant Nos. 1661658 and 1801963.

A number field F can be viewed as a subfield of \mathbb{C} in multiple ways. That is, any $\sigma \in G_{\mathbb{Q}}$ gives an isomorphism $\sigma: F \rightarrow \sigma(F)$, and $\sigma(F)$ is a subfield of \mathbb{C} as well, so precomposition with σ yields a different “archimedean” embedding of F in \mathbb{C} . We may then place a metric on F by restricting the usual distance function. An embedding of F in \mathbb{C} is real if it has image in \mathbb{R} and complex if it is not real, in which case it has dense image in \mathbb{C} . The numbers of real and complex-conjugate pairs of complex embeddings are respectively denoted $r_1(F)$ and $r_2(F)$.

The unit group \mathcal{O}_F^\times of invertible elements in \mathcal{O}_F under multiplication is deeply intertwined with the class group Cl_F . In fact, these groups are the kernel and cokernel of the map $F^\times \rightarrow I_F$ taking an element to its principal fractional ideal. Dirichlet’s unit theorem says that \mathcal{O}_F^\times is a direct product of the group of roots of unity in F and a free abelian group of rank $r = r_1(F) + r_2(F) - 1$. This is proven using logarithms of absolute values of units with respect to archimedean embeddings. The regulator R_F of F is a nonzero real number defined as a determinant of a matrix formed out of such logarithms.

The prototypical example is $F = \mathbb{Q}(\sqrt{-5})$, for which $\mathcal{O}_F = \mathbb{Z}[\sqrt{-5}]$. One has $r_1(F) = 0$, $r_2(F) = 1$, and $\mathcal{O}_F^\times = \{\pm 1\}$. We have two factorizations of 6 into irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ that don’t differ up to units:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

The unique factorization into primes that resolves this for our purposes is

$$(6) = (2, 1 + \sqrt{-5})^2 (3, 1 + \sqrt{-5}) (3, 1 - \sqrt{-5}).$$

The class number of $\mathbb{Q}(\sqrt{-5})$ is 2, so the class group is generated by the class of any nonprincipal ideal, such as $(2, 1 + \sqrt{-5})$ or $(3, 1 \pm \sqrt{-5})$.

Ramification in an extension of number fields is akin to the phenomenon of branching in branched covers in topology. As we’ve implicitly noted, the factorization of (2) in $\mathbb{Z}[\sqrt{-5}]$ is $(2, 1 + \sqrt{-5})^2$. The square is telling us that the same prime is occurring (at least) twice in the factorization: this is the branching. Whenever this happens in an extension of number fields, we say that the prime of the base field ramifies in the extension. Only finitely many primes ramify in an extension of number fields.

The Dedekind zeta function of F is the unique meromorphic continuation to \mathbb{C} of the series

$$\zeta_F(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_F} (N\mathfrak{a})^{-s},$$

where \mathfrak{a} runs over the nonzero ideals of \mathcal{O}_F and $N\mathfrak{a}$ is the index of \mathfrak{a} in \mathcal{O}_F . It has a simple pole

at $s = 1$ and satisfies a functional equation relating $\zeta_F(s)$ and $\zeta_F(1 - s)$ that involves factors coming from the archimedean embeddings. The Dedekind zeta function of \mathbb{Q} is the ubiquitous Riemann zeta function $\zeta(s)$.

The functional equation tells us that $\zeta_F(s)$ vanishes to order the rank r of \mathcal{O}_F^\times at $s = 0$. The leading term in its Taylor expansion is given by the analytic class number formula

$$\frac{\zeta_F^{(r)}(0)}{r!} = -\frac{h_F R_F}{w_F}.$$

where w_F is the number of roots of unity in F . This provides an important instance of a meromorphic function intertwining the unit and class groups. More broadly, it’s a first fundamental example of the links between analytic and algebraic objects of arithmetic.

To a prime \mathfrak{p} of F , we can attach a \mathfrak{p} -adic metric under which elements are closer together if their difference lies in a higher power of \mathfrak{p} . We may complete F with respect to this metric to obtain a complete “local” field $F_{\mathfrak{p}}$ that has a markedly non-Euclidean topology. It has a compact valuation ring $\mathcal{O}_{\mathfrak{p}}$ equal to the open and closed unit ball about 0.

For example, the p -adic metric d_p on \mathbb{Q} is defined by $d_p(x, y) = p^{-n}$ for the largest $n \in \mathbb{Z}$ such that $x - y \in p^n \mathbb{Z}$. The completion of \mathbb{Q} with respect to d_p is called the p -adic numbers \mathbb{Q}_p , which has valuation ring the p -adic integers \mathbb{Z}_p . Alternatively, \mathbb{Z}_p is the inverse limit of the rings $\mathbb{Z}/p^n \mathbb{Z}$ under the reduction maps between them.

Every prime \mathfrak{p} of F is maximal in \mathcal{O}_F with finite residue field $\mathcal{O}_F/\mathfrak{p}$. The Galois group G of a finite Galois extension E/F acts transitively on the set of primes \mathfrak{q} of E containing \mathfrak{p} . The stabilizer of \mathfrak{q} in G is called its decomposition group $G_{\mathfrak{q}}$ and is isomorphic to $\text{Gal}(E_{\mathfrak{q}}/F_{\mathfrak{p}})$. The extension $\mathcal{O}_E/\mathfrak{q}$ of $\mathcal{O}_F/\mathfrak{p}$ has cyclic Galois group generated by $x \mapsto x^{N_{\mathfrak{p}}}$. This element lifts to an element of $G_{\mathfrak{q}}$ called a Frobenius element at \mathfrak{q} . The lift is unique if \mathfrak{p} is unramified in E/F . It is independent of \mathfrak{q} if G is also abelian, in which case we denote it by $\varphi_{\mathfrak{p}}$.

The Hilbert class field H_F of F is the largest unramified abelian extension of F . Here, “unramified” means that no prime ramifies and no real embedding becomes complex. The Artin map taking the class of a prime \mathfrak{p} to $\varphi_{\mathfrak{p}}$ provides an isomorphism

$$\text{Cl}_F \xrightarrow{\sim} \text{Gal}(H_F/F).$$

For example, the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Q}(\sqrt{5}, i)$, and the Artin isomorphism tells us whether or not a prime \mathfrak{p} of $\mathbb{Z}[\sqrt{-5}]$ is principal

via the sign in $\varphi_p(i) = \pm i$. Class field theory concerns “reciprocity maps” generalizing the Artin isomorphism by relaxing the ramification conditions. These in turn can be used to prove reciprocity laws generalizing Gauss’ law of quadratic reciprocity.

Cyclotomic fields

Iwasawa theory has its origins in the study of the arithmetic of cyclotomic fields, a classical area of number theory that dates back to attempts at proving Fermat’s last theorem in the mid-1800’s. This is a fascinating subject in its own right, not least for the connections it reveals between Bernoulli numbers and the structure of cyclotomic class groups.

For a positive integer N , the N th cyclotomic field $\mathbb{Q}(\zeta_N)$ is given by adjoining the primitive N th root of unity $\zeta_N = e^{2\pi i/N}$ to \mathbb{Q} . The Kronecker-Weber theorem states that every finite abelian extension of the rationals is contained in a cyclotomic field. If $N > 1$, the prime ideals that ramify in $\mathbb{Q}(\zeta_N)$ are exactly those dividing N . The integer ring of $\mathbb{Q}(\zeta_N)$ is $\mathbb{Z}[\zeta_N]$, so every cyclotomic integer is a \mathbb{Z} -linear combination of roots of unity.

Each element σ of $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ carries ζ_N to another primitive N th root of unity, which has the form ζ_N^i for some i prime to N . The map taking σ to the unit i modulo N provides an isomorphism

$$\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$$

known as the N th cyclotomic character.

For x , y , and z satisfying the Fermat equation in odd prime exponent p , we have a factorization

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y) = z^p$$

in $\mathbb{Z}[\zeta_p]$. Using this, Kummer proved in an 1850 paper that if p is regular, which is to say that $p \nmid h_{\mathbb{Q}(\zeta_p)}$, then Fermat’s last theorem holds in exponent p . (Its use lies in the fact that if p is regular, then $(x + \zeta_p^i y)$ cannot be the p th power of a nonprincipal ideal.) It’s known that there are infinitely many irregular primes but not that there are infinitely many regular primes, though over 60% of primes up to any given number are expected to be regular.

For $k \geq 0$, the k th Bernoulli number $B_k \in \mathbb{Q}$ is the k th derivative at 0 of the function $\frac{x}{e^x - 1}$. One has $B_k = 0$ for odd $k \geq 3$. Here’s a table of Bernoulli numbers for positive even indices:

k	2	4	6	8	10	12	14
B_k	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{7}{6}$

Kummer proved the following, which amounts to a special case of the class number formula.

Theorem (Kummer). *A prime p is irregular if and only if p divides the numerator of B_k for some positive even $k < p$.*

In particular, 691 is irregular as it divides B_{12} . Here’s a table of irregular primes $p < 150$ and the indices n of the Bernoulli numbers B_n they divide:

p	37	59	67	101	103	131	149
n	32	44	58	68	24	22	130

The prime 157 divides both B_{62} and B_{110} . The index of irregularity i_p of p is the number of Bernoulli numbers B_k with $k < p$ even that p divides. Its values up to an increasingly large bound are expected fit a Poisson distribution with parameter $\frac{1}{2}$. The latest in a long history of computations is due to Hart, Harvey, and Ong for $p < 2^{31} = 2147483648$. In this range, i_p attains a maximum value of 9.

Regularity of p is equivalent to the triviality of the Sylow p -subgroup A of $\text{Cl}_{\mathbb{Q}(\zeta_p)}$. We call A the p -part of the class group. So, what more does the fact an odd p divides a particular Bernoulli number tell us about A ? The answer is found in the action of

$$\Delta = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$$

on A induced by the Δ -action on field elements.

For each $\delta \in (\mathbb{Z}/p\mathbb{Z})^\times$, there is a unique element $\omega(\delta) \in \mathbb{Z}_p^\times$ of order dividing $p-1$ that reduces to δ . The resulting homomorphism

$$\omega: (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{Z}_p^\times$$

is a splitting of the reduction modulo p map. The group A breaks up as a direct sum

$$A = \bigoplus_{i \in \mathbb{Z}/(p-1)\mathbb{Z}} A^{(i)}$$

of subgroups

$$A^{(i)} = \{a \in A \mid \delta(a) = \omega(\delta)^i a \text{ for all } \delta \in \Delta\}$$

for integers i modulo $p-1$. For obvious reasons, these are often called Δ -eigenspaces of A . It is such eigenspaces that we shall seek to study, beginning with the following important theorem.

Theorem (Herbrand-Ribet). *If k is a positive even integer with $k < p$, then p divides B_k if and only if $A^{(p-k)} \neq 0$.*

Herbrand proved that $A^{(p-k)} = 0$ unless $p \mid B_k$ in 1932. Ken Ribet proved the converse in a 1976 paper [Ri]. The proof of Herbrand's theorem relies on a direct construction of an annihilator of the class group in $\mathbb{Z}[\Delta]$ due to Stickelberger. Ribet's proof is more delicate, involving a congruence between modular forms that occurs when $p \mid B_k$ and its consequences for a Galois representation. We'll explain his method later.

There is also a coarser decomposition of A as $A^+ \oplus A^-$, where A^\pm is the subgroup of elements on which complex conjugation acts as ± 1 . Then A^\pm is the direct sum of the Δ -eigenspaces of A for even/odd i . The Herbrand-Ribet theorem concerns A^- , but Kummer had already shown that $A^- = 0$ implies $A = 0$.

The order of A^+ is the highest power of p dividing the class number h^+ of the fixed field $\mathbb{Q}(\zeta_p)^+$ of complex conjugation. In 1920, H. Vandiver rediscovered and later popularized a conjecture of Kummer's that $A^+ = 0$. Hart, Harvey, and Ong have verified this conjecture for $p < 2^{31}$.

Vandiver's conjecture can be rephrased as a question about units. That is, the group of cyclotomic units in $\mathbb{Z}[\zeta_p]$ is generated by

$$1 + \zeta_p + \cdots + \zeta_p^{j-1} \quad \text{for } 1 < j < p.$$

The class number formula implies that the index of this subgroup of the unit group $\mathbb{Z}[\zeta_p]^\times$ is h^+ . Vandiver's conjecture asserts that p does not divide this index.

By a reflection principle of H.-W. Leopoldt, an even eigenspace $A^{(k)}$ vanishes if $A^{(p-k)} = 0$, while $A^{(k)} = 0$ implies that $A^{(p-k)}$ is cyclic. The proof of this uses class field theory and a general duality between Galois and field elements known as Kummer theory.

Classical Iwasawa theory

Iwasawa theory concerns the growth of arithmetic objects in towers of number fields. More precisely, it concerns the growth of p -parts of class groups, and more general objects called Selmer groups, in towers of number fields of p -power degree. This growth exhibits a certain regularity that in good circumstances can be partially described by a p -adic variant of a complex-valued L -function.

The simplest sort of tower consists of a sequence F_n of fields

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_\infty = \bigcup_{n=0}^{\infty} F_n$$

with F_n/F cyclic of degree p^n . The Galois group $\Gamma = \text{Gal}(F_\infty/F)$ of the tower is the inverse limit of the groups $\Gamma_n = \text{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$ and as such is isomorphic to the additive group of \mathbb{Z}_p . It is thus a compact group under the p -adic topology. Every number field F has a cyclotomic \mathbb{Z}_p -extension defined as the unique \mathbb{Z}_p -extension of F inside the union of the fields $F(\zeta_{p^n})$.

If F has more than one \mathbb{Z}_p -extension, it has infinitely many. Yet, the Galois group of the compositum of all \mathbb{Z}_p -extensions still has finite \mathbb{Z}_p -rank $t \geq r_2(F) + 1$. Leopoldt conjectured this to be an equality in 1962. This notoriously difficult conjecture can be phrased as the equality of the \mathbb{Z} -rank of the unit group \mathcal{O}_F^\times and the \mathbb{Z}_p -rank of the closure of its image inside the direct sum of its local completions at primes over p . Leopoldt's conjecture is known for abelian extensions of \mathbb{Q} and imaginary quadratic fields by 1967 work of Armand Brumer.

Let's fix a \mathbb{Z}_p -extension F_∞ of F in our discussion. In 1959, Iwasawa proved a result on the growth of the orders of the p -parts A_n of the class groups of the fields F_n [Iw1].

Theorem (Iwasawa). *There exist nonnegative integers λ and μ and an integer ν such that*

$$|A_n| = p^{p^n \mu + n\lambda + \nu}$$

for all sufficiently large n .

As a p -group, A_n is a module over \mathbb{Z}_p . Since it also has a commuting Γ_n -action, A_n is a module for the group ring $\mathbb{Z}_p[\Gamma_n]$, which consists of finite formal sums of elements of Γ_n with \mathbb{Z}_p -coefficients.

We can compare the A_n via norm maps $A_{n+1} \rightarrow A_n$ for every $n \geq 0$, as well as via maps $A_n \rightarrow A_{n+1}$ induced by the inclusion of F_n in F_{n+1} . These maps are compatible with the action of $\mathbb{Z}_p[\Gamma_{n+1}]$ on both sides, with the action on A_n arising through the restriction map $\Gamma_{n+1} \rightarrow \Gamma_n$. The Iwasawa algebra

$$\Lambda = \varprojlim_n \mathbb{Z}_p[\Gamma_n]$$

then acts on both the inverse limit $\varprojlim_n A_n$ and the direct limit $A_\infty = \varinjlim_n A_n$. The Iwasawa algebra is a completion of the usual group ring $\mathbb{Z}_p[\Gamma]$, and as such it is a compact topological ring. Modules over Λ are also known as Iwasawa modules.

The Artin isomorphism identifies A_n with the Galois group $\text{Gal}(L_n/F_n)$ of the maximal unramified abelian p -extension (i.e., of p -power degree) L_n of F_n . These maps are compatible with norms on class groups and restriction on Galois groups.

The inverse limit of Artin isomorphisms identifies $\varprojlim_n A_n$ with the Galois group

$$X_\infty = \text{Gal}(L_\infty/F_\infty),$$

where $L_\infty = \bigcup_n L_n$. As an inverse limit of finite p -groups, X_∞ is said to be pro- p , and L_∞ is the maximal unramified abelian pro- p extension of F_∞ .

The Γ -action on the inverse limit of the A_n is identified via the Artin isomorphisms with the conjugation action of Γ on X_∞ . For this, one lifts $\gamma \in \Gamma$ to $\tilde{\gamma} \in \text{Gal}(L_\infty/F)$ and allows γ to act on $\sigma \in X_\infty$ by

$$\gamma: \sigma \mapsto \tilde{\gamma}\sigma\tilde{\gamma}^{-1}.$$

This gives X_∞ the structure of a Λ -module, and we refer to X_∞ as the unramified Iwasawa module. In that each A_n is finite, X_∞ is finitely generated and torsion over Λ .

The Λ -module X_∞ is compact, while A_∞ is discrete. To obtain a compact Λ -module from A_∞ , we take its Pontryagin dual $A_\infty^\vee = \text{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$, which is again finitely generated and torsion. Its structure is very closely related to that of X_∞ .

In good circumstances, such as when F_∞ is the cyclotomic \mathbb{Z}_p -extension of $F = \mathbb{Q}(\zeta_p)$, we can recover A_n from X_∞ as the largest quotient of X_∞ upon which Γ^{p^n} acts trivially. Crucial to this is the fact that Γ is a pro- p group. Because of this, Λ is a local ring, and one can employ Nakayama's lemma. This stands in stark contrast to the case of finite Galois extensions of prime-to- p degree, for which one has far less control over the growth of p -parts of class groups. Nevertheless, Larry Washington showed in 1979 that the p -parts eventually stop growing in the cyclotomic \mathbb{Z}_ℓ -extension for $\ell \neq p$ of an abelian extension of \mathbb{Q} .

As observed by Jean-Pierre Serre, the Iwasawa algebra Λ is isomorphic to a power series ring $\mathbb{Z}_p[[T]]$ in a single variable T . For this, we fix a topological generator γ of Γ , which is to say an element generating a dense subgroup, or equivalently, an element that restricts to a generator of each Γ_n . There is then a unique continuous isomorphism of compact \mathbb{Z}_p -algebras that takes $\gamma - 1$ to T . We shall use such an isomorphism to identify Λ and $\mathbb{Z}_p[[T]]$.

The structure theory of finitely generated modules over Λ mimics the theory of finitely generated modules over a PID if one treats Λ -modules as being defined up to finite submodules and quotient modules. The idea is that Λ becomes a PID upon localization at any principal prime ideal, and there are no nonzero finite modules over the localization.

A homomorphism $f: M \rightarrow N$ of finitely generated Λ -modules is called a pseudo-isomorphism if it has finite kernel and cokernel. The notion of pseudo-isomorphism gives an equivalence relation on any set of finitely generated, torsion Λ -modules.

Theorem (Iwasawa, Serre). *For any finitely generated, torsion Λ -module M , there is a pseudo-*

isomorphism

$$M \rightarrow \bigoplus_{i=1}^r \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^s \Lambda/(p^{m_j}),$$

where $r, s \geq 0$, each f_i is a monic irreducible polynomial in $\mathbb{Z}_p[T]$ satisfying $f_i \equiv T^{\deg f_i} \pmod{p}$, and each k_i and m_j is a positive integer.

In the notation the theorem, we set

$$\lambda(M) = \sum_{i=1}^r k_i \deg f_i \quad \text{and} \quad \mu(M) = \sum_{j=1}^s m_j.$$

We can also associate to M its characteristic ideal $\text{char}(M)$ in Λ . That is, given the above pseudo-isomorphism, we define

$$\text{char}(M) = \left(p^{\mu(M)} \prod_{i=1}^r f_i^{k_i} \right).$$

The polynomial $\prod_{i=1}^r f_i^{k_i}$ is the usual characteristic polynomial of T acting on the finite-dimensional \mathbb{Q}_p -vector space $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

In the case of the unramified Iwasawa module X_∞ , the quantities $\lambda = \lambda(X_\infty)$ and $\mu = \mu(X_\infty)$ are those in Iwasawa's growth formula. In fact, we also have $\lambda = \lambda(A_\infty^\vee)$ and $\mu = \mu(A_\infty^\vee)$, with the characteristic ideals of X_∞ and A_∞^\vee differing by the change of variables $T \mapsto (1+T)^{-1} - 1$.

Iwasawa conjectured that $\mu = 0$ if F_∞ is the cyclotomic \mathbb{Z}_p -extension of F . Bruce Ferrero and Washington proved this when F/\mathbb{Q} is abelian [FW]. In this case, Iwasawa also showed that the (-1) -eigenspace X_∞^- for the action of complex conjugation has no finite Λ -submodule.

For F_∞ the cyclotomic \mathbb{Z}_p -extension of $F = \mathbb{Q}(\mu_p)$, the Iwasawa module X_∞ has an action of $\Delta = \text{Gal}(F/\mathbb{Q})$ that commutes with its Λ -action, so we can again break up X_∞ as a direct sum of Δ -eigenspaces. In the computations of Hart-Harvey-Ong, not a single Δ -eigenspace of X_∞ has λ -invariant greater than 1. Such an eigenspace $X_\infty^{(i)}$ is nonzero if and only if $A^{(i)}$ is nonzero, so these computations imply that $\lambda \leq 9$ for $p < 2^{31}$.

p -adic L -functions

For any positive integer n , the Riemann zeta function satisfies

$$\zeta(1-n) = -\frac{B_n}{n}.$$

The prime p divides the denominator of B_n in lowest form if and only if $p-1$ divides n by an 1840

result of Klausen and Von-Staudt. Let's assume $p - 1$ does not divide n , since otherwise it's known that the relevant eigenspace $A^{(1)} = A^{(p-n)}$ is 0.

For $m \equiv n \pmod{p-1}$, Kummer showed in 1851 that

$$\zeta(1 - m) \equiv \zeta(1 - n) \pmod{p}.$$

This explains why our criterion for regularity requires only indices $n < p$. Even better, if $m \equiv n \pmod{p^{j-1}(p-1)}$ for some $j \geq 1$, then we have

$$(1 - p^{m-1})\zeta(1 - m) \equiv (1 - p^{n-1})\zeta(1 - n) \pmod{p^j}.$$

Fixing an even integer k , these congruences imply the existence of a continuous \mathbb{Z}_p -valued function $L_p(\omega^k, s)$ of a p -adic variable $s \in \mathbb{Z}_p$ satisfying

$$L_p(\omega^k, 1 - n) = (1 - p^{n-1})\zeta(1 - n)$$

for all $n \equiv k \pmod{p-1}$. Here as before, ω denotes the p -adic character $\omega: (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{Z}_p^\times$.

The p -adic L -functions $L_p(\omega; \cdot; \cdot)$ were constructed by Kubota and Leopoldt. Their values at other nonnegative integers are similarly given by special values of Dirichlet L -functions of complex-valued characters of Δ . The Riemann zeta function is the Dirichlet L -function for the trivial character.

The Iwasawa main conjecture

The Iwasawa main conjecture describes the characteristic ideal of $X_\infty^{(p-k)}$ for an odd prime p and an even integer k in terms of the Kubota-Leopoldt p -adic L -function $L_p(\omega^k, s)$. As $X_\infty^{(1)}$ is trivial since $A^{(1)} = 0$, let us suppose that $k \not\equiv 0 \pmod{p-1}$.

Iwasawa showed that $L_p(\omega^k, s)$ is determined on $s \in \mathbb{Z}_p$ by a unique power series $f_k \in \Lambda$ satisfying

$$f_k((1 + p)^s - 1) = L_p(\omega^k, s).$$

Here, we've taken the variable T to correspond to $\gamma - 1$ for the topological generator γ of Γ that raises all roots of unity of p -power order to the power $1 + p$, and $(1 + p)^s$ is the limit of the sequence of $(1 + p)^{s_n}$ for $s_n \in \mathbb{Z}$ satisfying $s_n \equiv s \pmod{p^n \mathbb{Z}_p}$.

The following conjecture of Iwasawa's, formulated in the late 1960s, was given a proof by Barry Mazur and Andrew Wiles in a 1984 paper [MW].

Theorem (Iwasawa main conjecture, Mazur-Wiles). *For any even integer $k \not\equiv 0 \pmod{p-1}$, we have*

$$\text{char}(X_\infty^{(p-k)}) = (f_k).$$

The main conjecture implies that the highest power of p dividing $L_p(\omega^k, s)$ is also the order of the largest quotient of $X_\infty^{(p-k)}$ upon which T acts as $(1 + p)^s - 1$. Taking $s = 0$, the main conjecture gives the order of $A^{(p-k)}$; it does not, however, tell us the isomorphism class (though refinements do exist).

The main conjecture can also be formulated in terms of the p -ramified Iwasawa module $\mathfrak{X}_\infty = \text{Gal}(M_\infty/F_\infty)$ for M_∞ the union of the maximal abelian p -extensions of the F_n ramified only at the unique prime $(1 - \zeta_{p^{n+1}})$ over p . This version of the main conjecture asserts that

$$\text{char}(\mathfrak{X}_\infty^{(k)}) = (g_k),$$

where g_k is given by the change of variables $g_k(T) = f_k((1 + p)(1 + T)^{-1} - 1)$. The equivalence follows from an Iwasawa-theoretic version of Kummer duality.

In [Iw2], Iwasawa proved his main conjecture assuming that $A^{(k)} = 0$. In this case, the equality of characteristic ideals becomes an isomorphism

$$X_\infty^{(p-k)} \cong \Lambda/(f_k).$$

It's worth understanding how Iwasawa's argument goes, as through it one obtains a form of the main conjecture free from L -functions asserting an equality of characteristic ideals of Iwasawa modules coming from unit and class groups.

Iwasawa studied the image of the cyclotomic units inside the local units of the completion at the prime over p , working up the tower of completions at p of the fields F_n by considering sequences of elements compatible under norm maps. The Iwasawa module \mathcal{U}_∞ of norm compatible sequences of local units contains submodules \mathcal{E}_∞ and \mathcal{C}_∞ generated by the sequences of global units and cyclotomic units, respectively.

Class field theory provides an exact sequence

$$0 \rightarrow \mathcal{E}_\infty/\mathcal{C}_\infty \rightarrow \mathcal{U}_\infty/\mathcal{C}_\infty \rightarrow \mathfrak{X}_\infty \rightarrow X_\infty \rightarrow 0.$$

This in turn yields an exact sequence with each module replaced by its ω^k -eigenspace under Δ . If $X_\infty^{(k)} = 0$, then the class number formula can be used to see that $\mathcal{E}_\infty^{(k)} = \mathcal{C}_\infty^{(k)}$ as well. The four-term exact sequence therefore reduces to an isomorphism

$$\mathcal{U}_\infty^{(k)}/\mathcal{C}_\infty^{(k)} \cong \mathfrak{X}_\infty^{(k)}.$$

Iwasawa then obtains that $\mathfrak{X}_\infty^{(k)} \cong \Lambda/(g_k)$ from the following unconditional theorem, which amounts to a p -adic regulator computation on cyclotomic units.

Theorem (Iwasawa). *There is an isomorphism of Λ -modules*

$$\mathcal{U}_\infty^{(k)} / \mathcal{C}_\infty^{(k)} \cong \Lambda / (g_k).$$

As characteristic ideals are multiplicative in exact sequences of finitely generated, torsion Λ -modules, this also tells us unconditionally that the main conjecture is equivalent to the equality

$$\text{char}(\mathcal{E}_\infty^{(k)} / \mathcal{C}_\infty^{(k)}) = \text{char}(X_\infty^{(k)})$$

in which no L -functions appear.

Modular forms

One might say that the theme of the work of Ribet and Mazur-Wiles is that the study of the geometry of varieties over \mathbb{Q} can be used to solve arithmetic questions. Specifically, their work makes use of modular curves and congruences between modular forms. The Galois representations attached to modular forms are two-dimensional, presenting a natural next class of objects to study beyond the one-dimensional abelian characters of class field theory. We embark upon another brief tour.

The group of matrices in $\text{GL}_2(\mathbb{R})$ with positive determinant acts by Möbius transformations on the upper half-plane \mathbb{H} of complex numbers with positive imaginary part. A modular curve is a quotient of \mathbb{H} by the action of a subgroup of $\text{SL}_2(\mathbb{Z})$ that is determined by congruences among its entries. This quotient can be compactified by adding in the equivalence classes of the cusps, which are the rational numbers and infinity.

A modular form f is a holomorphic function of \mathbb{H} that transforms under a congruence subgroup Γ (in the standard notation, but not to be confused with the Galois group appearing in Iwasawa theory) in a manner prescribed by its “weight” k , and which is bounded and holomorphic at the cusps. Specifically, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, then

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$

A modular form is a cusp form if it is zero at all cusps.

If $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, then $f(z+1) = f(z)$, so f has a Fourier expansion about the cusp at ∞ of the form

$$f = \sum_{n=0}^{\infty} a_n(f) q^n$$

with $q = e^{2\pi iz}$ for $z \in \mathbb{H}$. If f is a cusp form, then $a_0(f) = 0$.

There are Hecke operators T_n for each $n \geq 1$ that act on modular forms by summing over the action of representatives of the double coset $\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma$ as a union of right cosets. A modular form is an eigenform if it is a simultaneous eigenform for all Hecke operators. If an eigenform is normalized so that $a_1(f) = 1$, then $T_n(f) = a_n(f)f$ for all $n \geq 1$. The Fourier coefficients $a_n(f)$ of a normalized eigenform f are algebraic numbers that are integral for $n \geq 1$, and the coefficient field they generate is a number field.

Eisenstein series form a class of modular forms that are not cusp forms. For instance, for a positive even integer $k \geq 4$, we have an Eisenstein series

$$E_k = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} q^n$$

which is an eigenform of weight k for $\Gamma = \text{SL}_2(\mathbb{Z})$ itself. When an odd prime p divides $\zeta(1-k) = -B_k/k$, the constant term of E_k is zero modulo p . In this case, the reduction of E_k modulo p may be lifted to a cuspidal eigenform with coefficients in the ring of integers of a number field. For example, E_{12} is congruent modulo $691\mathbb{Z}[[q]]$ to the unique normalized cusp form

$$q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

of weight 12 for $\text{SL}_2(\mathbb{Z})$.

To a normalized cuspidal eigenform f of weight $k \geq 2$, work of Shimura and Deligne attached a p -adic Galois representation $\rho_f: G_{\mathbb{Q}} \rightarrow \text{GL}_2(K_f)$, with K_f the field obtained by adjoining to \mathbb{Q}_p the Fourier coefficients of f . Equivalently, it is a two-dimensional K_f -vector space V_f with a commuting $G_{\mathbb{Q}}$ -action. This representation ρ_f is irreducible, it is odd (i.e., it has determinant -1 on complex conjugation), and it has the property that the trace of $\rho_f(\varphi_\ell)$ for a Frobenius element φ_ℓ of an unramified prime over a rational prime ℓ is equal to $a_\ell(f)$.

Inside V_f , there is a rank two module L_f for the valuation ring \mathcal{O}_f of K_f that is preserved by the $G_{\mathbb{Q}}$ -action. Roughly, this says that ρ_f can be viewed as taking values in $\text{GL}_2(\mathcal{O}_f)$. So, it makes sense to reduce ρ_f modulo the maximal ideal of \mathcal{O}_f and talk about the resulting representation $\bar{\rho}_f: G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{F}_q)$ over the residue field \mathbb{F}_q . This residual representation is unique up to isomorphism if and only if it is irreducible. Otherwise, its isomorphism class depends upon the choice of L_f .

The method of Ribet-Mazur-Wiles

Ribet and Mazur-Wiles employed congruences between cusp forms and Eisenstein series to construct unramified abelian extensions of cyclotomic fields. As we've noted, if $p \mid B_k$ for an even $k < p$, then there exists a cuspidal eigenform f congruent to E_k modulo the maximal ideal of \mathcal{O}_f . The fixed field of the kernel of the Galois representation ρ_f is ramified only at the prime p . Ribet used this to construct an unramified abelian p -extension of $F = \mathbb{Q}(\zeta_p)$ on which Δ acts through ω^{p-k} . By class field theory, if the extension is nontrivial, then $A^{(p-k)}$ is nonzero, which is Ribet's converse to Herbrand's theorem.

The method works by playing two facts forced by the congruence off of each other. The first is that f is ordinary in the sense that $a_p(f)$ is a p -adic unit. For ordinary forms, there exists a basis of V_f such that ρ_f restricted to a decomposition group at p is upper triangular as a map to $\mathrm{GL}_2(\mathcal{O}_f)$. If needed, one can rescale so that the map $\phi: G_{\mathbb{Q}} \rightarrow \mathbb{F}_q$ to the residue field \mathbb{F}_q given by the reduction of the lower-left hand corner of ρ_f modulo the maximal ideal of \mathcal{O}_f is nonzero on the larger group $G_{\mathbb{Q}}$.

The second fact is that the residual Galois representation $\bar{\rho}_f$ is reducible. The above basis can actually be chosen so that $\bar{\rho}_f$ has the form

$$\bar{\rho}_f(\sigma) = \begin{pmatrix} \omega^{k-1}(\sigma) & 0 \\ \phi(\sigma) & 1 \end{pmatrix}$$

on $\sigma \in G_{\mathbb{Q}}$, viewing ω as a character of $G_{\mathbb{Q}}$. The restriction of ϕ to $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ is then a homomorphism that is unramified at the prime over p by construction, so it factors through the Galois group of a nontrivial unramified abelian p -extension H of F that is Galois over \mathbb{Q} . The group Δ acts on $\mathrm{Gal}(H/F)$ compatibly with conjugation of matrices, which is to say that it acts by $\omega^{p-k} = (\omega^{k-1})^{-1}$.

Mazur and Wiles generalized and refined Ribet's method in the context of Iwasawa theory in order to prove the main conjecture and its generalization to arbitrary abelian extensions of \mathbb{Q} . By studying the Galois actions on Jacobians of modular curves, they construct an unramified abelian extension of the field F_{∞} of all p -power roots of unity with Galois group a Λ -module quotient of $X_{\infty}^{(p-k)}$ that has characteristic ideal (f_k) .

Having proven that $(f_k) \mid \mathrm{char}(X_{\infty}^{(p-k)})$, Mazur and Wiles apply a consequence of analytic class number formula to obtain the main conjecture. That is, Iwasawa had shown in 1972 that

$$\sum_{j=1}^{(p-3)/2} \lambda(X_{\infty}^{(p-2j)}) = \sum_{j=1}^{(p-3)/2} \deg f_{2j}.$$

From this, it follows that one divisibility for all odd eigenspaces implies the other.

Later work of Wiles gave a more streamlined perspective, casting the proof in terms of the theory of families of ordinary modular forms of Haruzo Hida. That is, Wiles employed the residual representation of a Galois representation $\rho_{\mathcal{F}}: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{I}_f)$ attached to a p -adically continuously varying family \mathcal{F} of ordinary cuspidal eigenforms congruent to a family of Eisenstein series, where \mathbb{I}_f is a finite local Λ -algebra.

The method of Euler systems

Work of Francisco Thaine and Victor Kolyvagin led to a new and more explicit, though technically complex, approach to the main conjecture, which Karl Rubin completed to a full proof. The method uses what Kolyvagin termed an Euler system, the first example of which consists of cyclotomic units in abelian extensions of \mathbb{Q} . This system of elements is used to bound the order of an even eigenspace of the p -part of the class group by the order of an eigenspace of the quotient of the global units by the cyclotomic units.

The key property is a norm compatibility from $\mathbb{Q}(\zeta_{N\ell})$ to $\mathbb{Q}(\zeta_N)$ for p dividing N and a prime ℓ . Explicitly, if $\ell \nmid N$, one has

$$N_{\mathbb{Q}(\zeta_{N\ell})/\mathbb{Q}(\zeta_N)}(1 - \zeta_{N\ell}) = \frac{1 - \zeta_N}{1 - \zeta_N^{\ell-1}}.$$

With this relation, one applies a Galois-theoretic derivative construction to elements $1 - \zeta_{N\ell}$ for good choices of primes ℓ congruent to ± 1 modulo a sufficiently high power of p to obtain field elements that are powers of chosen non-principal ideals.

Up the cyclotomic tower, the method of Euler systems shows that

$$\mathrm{char}(X_{\infty}^{(k)}) \mid \mathrm{char}(\mathcal{E}_{\infty}^{(k)} / \mathcal{C}_{\infty}^{(k)})$$

for even $k \in \mathbb{Z}$. This is equivalent to the opposite divisibility to that of Mazur-Wiles, and again the analytic class number formula yields equality.

Totally real and CM fields

The Iwasawa main conjecture generalizes directly from \mathbb{Q} to totally real fields, those number fields with only real archimedean embeddings. The relevant p -adic L -functions were separately constructed by P. Deligne and Ribet, P. Cassou-Noguès, and D. Barsky. Wiles proved a main conjecture for

odd eigenspaces of the unramified Iwasawa module X_∞ over the cyclotomic \mathbb{Z}_p -extension F_∞ of an abelian extension F of a totally real field using Galois representations attached to Hilbert modular forms [Wi]. Ralph Greenberg has conjectured that the even eigenspaces of X_∞ are finite.

The existence of an Euler system in abelian extensions of totally real fields was conjectured by Harold Stark and Rubin, but it is still unproven. This is related to Hilbert's 12th problem, or Kronecker's Jugendtraum, of an explicit class field theory over totally real fields. In contrast, abelian extensions of imaginary quadratic fields contain analogues of cyclotomic units called elliptic units that do form an Euler system. In this case, there is an explicit form of class field theory arising from the theory of complex multiplication (CM) of elliptic curves that we'll discuss. Elliptic units are generated by values at torsion points of a theta function that is a meromorphic function on a CM elliptic curve.

In 1977, John Coates and Wiles proved an analogue of Iwasawa's theorem on local units modulo cyclotomic units for an imaginary quadratic field K with $h_K = 1$ [CW]. Choosing a split prime p with $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, their theorem states that the quotient of the local units at \mathfrak{p} modulo elliptic units up a \mathbb{Z}_p -extension of K ramified only at \mathfrak{p} is isomorphic to the quotient of the one-variable Iwasawa algebra by a power series corresponding to a p -adic L -function constructed by Nick Katz.

The compositum of \mathbb{Z}_p -extensions of an imaginary quadratic field K has Galois group \mathbb{Z}_p^2 . Its Iwasawa algebra is a power series ring in two variables over \mathbb{Z}_p . The unramified Iwasawa module X_∞ over the corresponding \mathbb{Z}_p^2 -extension of an abelian extension of K is conjecturally small enough to have unit characteristic ideal. The main conjecture here compares X_∞ and the quotient of global units by elliptic units. It was proven by Rubin using the method of Euler systems in 1991 [Ru]. If p splits in K , one can instead replace X_∞ with a larger Iwasawa module that allows ramification at exactly one of the two primes over p . This gives an equivalent form involving a two-variable Katz p -adic L -function.

In 1994, Hida and Jacques Tilouine gave an alternate proof of the specialization of this conjecture to an anticyclotomic \mathbb{Z}_p -extension using an approach closer to that of Mazur-Wiles. Their work extends to analogues of imaginary quadratic fields over totally real fields known as CM fields for which one once again has no known Euler system to employ. More recently, progress has been made on a divisibility in a general main conjecture over CM fields, in particular by Ming-Lun Hsieh.

Elliptic curves and BSD

Elliptic curves over number fields provide a next step beyond the theory of multiplicative groups that we've been in effect describing. In this setting, the arithmetic objects that replace class groups are known as Selmer groups. We run quickly through the arithmetic theory of elliptic curves, from the basic theory to deep results and a famous conjecture, before we begin passing up towers.

A complex elliptic curve E is defined by an equation

$$y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{C}$ and $4a^3 + 27b^2 \neq 0$ to ensure smoothness. More precisely, it is the projective curve of genus one defined by the homogenization of the above polynomial. Effectively, this means adding a single point ∞ at infinity.

The set $E(\mathbb{C})$ of points of E with complex coordinates has an abelian group law with ∞ as its identity. It is given by drawing a line between two points P and Q and declaring the third point of the line in $E(\mathbb{C})$ to be $-P - Q$, taking multiplicity into account. We'll assume that $a, b \in \mathbb{Q}$, which is to say that E is rational. The Mordell-Weil group $E(F)$ of points with coordinates in a number field F is then a finitely generated subgroup of $E(\mathbb{C})$.

The group $E(\bar{\mathbb{Q}})$ has a canonical action of $G_{\bar{\mathbb{Q}}}$ via the action on coordinates. A point of $E(\mathbb{C}) \cong (\mathbb{R}/\mathbb{Z})^2$ is said to be n -torsion if it has order dividing n . The group $E[n]$ of all n -torsion points is a subgroup of $E(\bar{\mathbb{Q}})$ isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$.

A rational elliptic curve E has a ring \mathcal{O} of endomorphisms consisting of nonzero \mathbb{Q} -rational maps $E \rightarrow E$ taking ∞ to itself. Among these are the morphisms given by multiplication by integers using the group law of E . If $\mathcal{O} \neq \mathbb{Z}$, then \mathcal{O} is a finite index subring of the integer ring of an imaginary quadratic field. In this case, we say that E has complex multiplication, or CM, by \mathcal{O} .

The cohomology of a group G with coefficients in a module M for its group ring is a sequence of abelian groups $H^i(G, M)$ that allows one to study the group action using the tools of homological algebra. For Galois groups, the closely related theory of Galois cohomology is a crucial tool in Iwasawa theory. Many theorems of class field theory can be phrased in terms of duality in Galois cohomology, and abelian groups of arithmetic interest can be encoded in cohomology.

For a number field F , the group $E(F)/nE(F)$ is contained in $H^1(\text{Gal}(\bar{\mathbb{Q}}/F), E[n])$. In fact, it is contained in a smaller subgroup of cohomology classes that are unramified at all but finitely many

primes and partially vanish locally at the remaining primes. The direct limit over n of these subgroups of $H^1(\text{Gal}(\overline{\mathbb{Q}}/F), E[n])$ is the Selmer group $\text{Sel}_E(F)$ we wish to study.

The most important thing to know about the Selmer group is that it intertwines the Mordell-Weil group with a mysterious, conjecturally finite group called the Shafarevich-Tate group $\text{III}_E(F)$ of E . That is, there is an exact sequence:

$$0 \rightarrow E(F) \otimes \mathbb{Q}/\mathbb{Z} \rightarrow \text{Sel}_E(F) \rightarrow \text{III}_E(F) \rightarrow 0.$$

This is analogous to what happens with cohomology with coefficients in roots of unity: in that case, the unit and class groups get wrapped up together.

The intertwining of $E(\mathbb{Q})$ and $\text{III}_E(\mathbb{Q})$ is also reflected in analytic formulas. One can construct an L -series for E from the data of the number of \mathbb{F}_p -points of mod p reductions of a minimal equation for E . It has analytic continuation to \mathbb{C} by the modularity of rational elliptic curves proven by Wiles, Taylor-Wiles, and Breuil-Conrad-Diamond-Taylor, which tells one that E has an associated cuspidal eigenform with the same L -series.

The Birch and Swinnerton-Dyer conjecture, or BSD, was formulated in 1965 and is one of the Clay Math Institute's Millennium Problems.

Conjecture (Birch and Swinnerton-Dyer). *The order of vanishing of the L -function $L(E, s)$ at $s = 1$ is equal to the rank of $E(\mathbb{Q})$.*

The BSD conjecture has a refined form that links the leading term of $L(E, s)$ in its Taylor expansion about $s = 1$ to the orders of the torsion subgroup $E(\mathbb{Q})_{\text{tor}}$ of Mordell-Weil and of $\text{III}_E(\mathbb{Q})$. The conjectural BSD formula has the form

$$\frac{L^{(r)}(E, 1)}{r!} = \frac{|\text{III}_E(\mathbb{Q})| \Omega_E R_E \prod_{\ell} c_{\ell}}{|E(\mathbb{Q})_{\text{tor}}|^2}, \quad (1)$$

where r is the order of vanishing, R_E is a regulator related to the heights of rational points, the quantity Ω_E is a real period, and each c_{ℓ} for a prime ℓ is the number of components of a certain mod ℓ reduction of E , all but finitely many being 1.

Much of the progress on BSD to date employs Iwasawa theory. For instance, the first major result that serves as theoretical evidence for BSD was due to Coates-Wiles. As a consequence of their theorem on local units modulo elliptic units, they proved that if $r = 0$ and E has CM by a subring of \mathcal{O}_K for K with $h_K = 1$, then $E(\mathbb{Q})$ is finite.

Iwasawa theory of elliptic curves

We turn to the question of how Selmer groups of a rational elliptic curve E grow in the cyclotomic \mathbb{Z}_p -extension \mathbb{Q}_{∞} of \mathbb{Q} . This amounts to studying the finitely generated Λ -module

$$\mathfrak{X}_E = \text{Hom}(\text{Sel}_E(\mathbb{Q}_{\infty}), \mathbb{Q}_p/\mathbb{Z}_p)$$

that is the Pontryagin dual of the direct limit $\text{Sel}_E(\mathbb{Q}_{\infty})[p^{\infty}]$ of p -power torsion subgroups of the Selmer groups $\text{Sel}_E(\mathbb{Q}_n)$.

The elliptic curve E has good reduction at p if its mod p reduction E_p is nonsingular, and it is then ordinary if E_p has a point of order p . For such elliptic curves, Mazur and Swinnerton-Dyer constructed a p -adic L -function $L_p(E, s)$ interpolating values of $L(E, s)$ up to certain Euler factors, and again it is determined by a power series \mathcal{L}_E . Mazur then formulated the following main conjecture.

Conjecture (Main conjecture for elliptic curves). *Suppose that E has good ordinary reduction at p and that $E(\mathbb{Q})[p]$ is an irreducible $G_{\mathbb{Q}}$ -representation. Then \mathfrak{X}_E is Λ -torsion and*

$$\text{char}(\mathfrak{X}_E) = (\mathcal{L}_E).$$

For elliptic curves with complex multiplication, this is equivalent to the main conjecture for imaginary quadratic fields and split primes p proven by Rubin. The general divisibility $\text{char}(\mathfrak{X}_E) \mid (\mathcal{L}_E)$ was proven by Kazuya Kato via the method of Euler systems [Ka]. Kato's Euler system is constructed using cohomological products formed from pairs of Siegel units on a modular curve parameterizing E , first studied by A. Beilinson. The other divisibility was proven under fairly mild hypotheses by Chris Skinner and Eric Urban using Galois representations attached to automorphic forms on the unitary group $\text{GU}(2, 2)$ [SU]. With no analytic class number formula that can be used in this setting, one needs both methods.

We mention a bit of what's known for elliptic curves with good supersingular (i.e., non-ordinary) reduction. For $p \geq 5$, there are in this case not one but two Selmer groups constructed by Shinichi Kobayashi, and two p -adic L -functions constructed by Rob Pollack. The corresponding main conjecture was proven by Rubin and Pollack for CM curves in 2004. In this case, p does not split in K , and the main conjecture is closely related to Rubin's main conjecture without L -functions for imaginary quadratic fields. The main conjecture for non-CM curves has recently been proven by Xin Wan under a hypothesis on the congruence subgroup. F. Sprung

has additionally treated the prime 3, in particular employing work of B.D. Kim and A. Lei in the formulation.

The main conjecture for elliptic curves implies a p -adic analogue of BSD of Mazur-Tate-Teitelbaum that relates the rank of $E(\mathbb{Q})$ to the order of vanishing of $L_p(E, s)$ at 1. As $L(E, s)$ is complex analytic and $L_p(E, s)$ is p -adic analytic, the derivatives are not clearly related, and neither form of BSD obviously implies the other in the case of positive rank.

The order r of vanishing of $L(E, s)$ at $s = 1$ is known as the analytic rank of E , and the actual rank of $E(\mathbb{Q})$ is known as the algebraic rank. Kolyvagin used an Euler system of Heegner points and a theorem of B. Gross and D. Zagier to prove that if the analytic rank of E is $r \leq 1$, then the algebraic rank is r and $\text{III}_E(\mathbb{Q})$ is finite. Both the converse to this and the BSD formula follow from the main conjecture for $r = 0$. Recent work of Skinner and of Wei Zhang implies a converse for $r = 1$ under mild hypotheses, and for $r = 1$ significant progress has been made towards the BSD formula as well, particularly in work of D. Jetchev, Skinner, and Wan.

Recent directions

Iwasawa theory extends to study the growth of other arithmetic objects attached to Galois representations in towers of number fields. Beginning in the late 1980s, Greenberg proposed main conjectures for a whole host of ordinary motivic Galois representations, and even continuously p -adically varying families thereof. Since then, main conjectures have been extended to more general towers, to non-ordinary families, to finer-grained analogues, and even to characteristic p base fields. Recent developments have seen considerable progress on methods of proof of both divisibilities. Here's a sampling.

The early part of the new millennium saw the development of Iwasawa theory over towers of number fields with Galois groups that are isomorphic to subgroups of $\text{GL}_n(\mathbb{Z}_p)$ for some n . The breakthrough came in a paper of Coates, Fukaya, Kato, Sujatha, and Venjakob containing a noncommutative main conjecture for elliptic curves. Invariants playing the roles of characteristic ideals and p -adic L -functions lie in a first K -group of a localization of the noncommutative Iwasawa algebra. Soon after, Fukaya and Kato formulated a remarkably general noncommutative main conjecture that relates closely to the equivariant Tamagawa number conjecture of Burns and Flach which in turn generalized a conjecture of Bloch and Kato on special values of L -functions.

At the start of this decade, a noncommutative

main conjecture for totally real fields was proven through work of Ritter and Weiss, Burns, and Kakde, assuming Iwasawa's conjecture on the vanishing of the μ -invariant. The key step is the verification of congruences among Deligne-Ribet p -adic L -functions over different totally real fields to reduce to the main conjecture proven by Wiles.

The work of Skinner-Urban has inspired a rush of new theorems on divisibilities in main conjectures, with recent progress on the construction of Galois representations attached to automorphic forms in the sense of the Langlands program providing a boon for the area. The construction of p -adic L -functions that interpolate special values of complex L -functions is a whole industry unto itself and often proceeds via distributions formed out of modular symbols or computations of local integrals.

Euler systems have long had a reputation as difficult to construct that has only recently begun to soften. An approach to construct them via geometric methods starting from cycles on varieties was initiated in work of Bertolini, Darmon, Prasanna, and Rotger and carried further in work of Loeffler, Zerbes, Lei, Kings, and Skinner. One typically computes complex and p -adic regulators to prove nonvanishing of Euler systems and relate them with (p -adic) L -functions.

Beyond Mazur-Wiles

I end with a brief discussion of a deeper relationship between the geometry of modular curves and the arithmetic of cyclotomic fields. In a 2011 paper, I formulated a conjecture relating relative homology classes $\{\alpha \rightarrow \beta\}$ of paths between cusps on a modular curve, taken here to be $X_1(p)$, and cup products $x \cup y$ of cyclotomic units in a Galois cohomology group that agrees with A^- modulo p . In fact, there is a simple explicit map

$$\left\{ \frac{a}{c} \rightarrow \frac{b}{d} \right\} \mapsto (1 - \zeta_p^c) \cup (1 - \zeta_p^d)$$

taking one set of elements to the other (for $ad - bc = 1$ and $p \nmid cd$). On a certain Eisenstein quotient of the plus part of homology, I conjectured this to provide an inverse to a canonical version of the map that appeared in the proof of Ribet's theorem.

Up the cyclotomic tower, this yields what can be viewed as a refinement of the Iwasawa main conjecture. That is, it provides not only an equality of characteristic ideals, but an isomorphism given by a recipe on special elements. Fukaya and Kato proved a major result in this direction in which the derivative of the p -adic L -function plays a crucial

and potentially unavoidable intermediate role. Their result implies the conjecture for $p < 2^{31}$.

Fukaya, Kato, and I expect this to be a special case of a general phenomenon of the geometry and topology of locally symmetric spaces of higher dimension informing the arithmetic of Galois representations attached to lower-dimensional automorphic forms. This begs the question of its elliptic curve analogue, which is but one of a wealth of intriguing possibilities for future directions in Iwasawa theory.

References

- [CW] J. COATES, A. WILES, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 223–251. MR0463176
- [FW] B. FERRERO, L. WASHINGTON, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377–395. MR0528968
- [Iw1] K. IWASAWA, On Γ -extensions of algebraic number fields, *Bull. Amer. Math. Soc.* **65** (1959), 183–226. MR0124316
- [Iw2] K. IWASAWA, On p -adic L -functions, *Ann. of Math.* **89** (1969), 198–205. MR0269627
- [Ka] K. KATO, p -adic Hodge theory and values of zeta functions of modular forms, *Cohomologies p -adiques et applications arithmétiques, III, Astérisque* **295** (2004), 117–290. MR2104361
- [MW] B. MAZUR, A. WILES, Class fields of abelian extensions of \mathbb{Q} , *Invent. Math.* **76** (1984), 179–330. MR0742853
- [Ri] K. RIBET, A modular construction of unramified p -extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.* **34** (1976), 151–162. MR0419403
- [Ru] K. RUBIN, The “main conjectures” of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103** (1991), 25–68. MR1079839
- [SU] C. SKINNER, E. URBAN, The Iwasawa main conjectures for GL_2 , *Invent. Math.* **195** (2014), 1–227. MR3148103
- [Wi] A. WILES, The Iwasawa conjecture for totally real fields, *Ann. of Math.* **131** (1990), 493–540. MR1053488