Iwasawa Theory

John Coates

Cambridge
Introduction

It grew out of the work of Kummer and Iwasawa on cyclotomic fields. It has at least four main ingredients.

A The fundamental arithmetic problems. (rational points on curves, class numbers of cyclotomic fields, \ldots).

B Zeta and $L$ functions (Complex and $p$-adic avatars)

C Purely algebraic problems about modules over Iwasawa algebras of complex $p$-adic Lie groups.

D As a tool for number-theoretic calculations.

The link between (A) and (B) via the $p$-adic world is given by so called ”Main conjectures” of Iwasawa theory.
Iwasawa theory grew out of the theory of cyclotomic fields, and it always seems to be the first place where we can prove examples of general new phenomena in Iwasawa theory.

Notation. Let $p$ be a prime number, define

$$\mu_{p^\infty} := \text{group of all } p\text{-power roots of unity}.$$ 

**Definition**

$$Q^{\text{cyc}} := \text{unique subfield of } Q(\mu_{p^\infty}) \text{ with Galois group } \mathbb{Z}_p,$$

$$B_n := \text{unique subfield of } Q^{\text{cyc}} \text{ of degree } p^n \text{ over } Q,$$

$$h_n := \text{class number of } B_n.$$
1 If $n \leq m$, $h_n|h_m$. (Since $p$ is totally ramified).
2 $(h_n, p) = 1$ for all $n \geq 1$. (Iwasawa theory)
Web’s Conjecture. If $p = 2$, $h_n = 1$ for all $n \geq 1$. If true, it would prove at last that there are infinitely many number fields with class number 1. Interesting recent progress on this conjecture by K. Horie, and T. Fukuda and K. Komatsu.

**Theorem (Horie)**

*If $l$ is a prime with $l \equiv 3, 5, 7, 9, 11, 13 \pmod{16}$, then $(h_n, l) = 1$ for all $n \geq 1$."

**Theorem (Fukuda and Komatsu)**

*Let $N$ be the product of all primes $< 11 \times 10^7$. Then $(h_n, N) = 1$ for all $n \geq 1$. Only possible divisors of $h_n$ are $l \equiv 1, 15 \pmod{16}$ with $l > 11 \times 10^7$."

Very little seems to be known. Presumably there are $p$ for which $h_n > 1$. We mention one other interesting result about class numbers of cyclotomic fields.

$\mathcal{F} :=$ maximal real subfield of $\mathbb{Q}(\mu_m : m = 3, 4, \cdots )$

$$\text{Gal}(\mathcal{F}/\mathbb{Q}) = \prod_q \mathbb{Z}_q^\times /\{\pm 1\}.$$ 

**Theorem (Kurihara)**

*The ideal class group of $\mathcal{F}$ is trivial.*

In other words, every ideal class of $\mathbb{Q}(\mu_m)^+(m = 3, 4, \cdots)$ must capitulate in $\mathcal{F}$. 
We briefly recall it as it appears to be the first example of a vastly general phenomena.
From now on $p > 2$

**Definition**

\[ F_\infty := \mathbb{Q}(\mu_{p\infty})^+ = \mathbb{Q}(\mu_p)^+\mathbb{Q}^{\text{cyc}}, \]

\[ G := \text{Gal}(F_\infty/\mathbb{Q}), \]

\[ \chi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_p^\times \quad \text{--- character giving action on } \mu_{p\infty}. \]

**Definition**

\[ \lambda(G) := \lim_{\leftarrow U} \mathbb{Z}_p. \]
Iwaswawa’s main conjecture

Mazur: we can view elements of $\Lambda(G)$ as $\mathbb{Z}_p$-valued measures on $G$. We need two ingredients to make a "main conjecture":

1. a $p$-adic zeta or $L$-function
2. a $\Lambda(G)$-module arising from arithmetic.

**Definition**

A pseudo-measure on $G$ is an element of the ring of fractions of $\Lambda(G)$ such that $(\epsilon - 1)\mu$ is in $\Lambda(G)$ for any $\sigma$ in $G$.

**Theorem (Kummer, Iwasawa)**

There exists a unique pseudo-measure $\zeta_{F_\infty/\mathbb{Q}}$ on $G$ such that for all even integers $n > 0$, we have

$$(*) \int_G \chi(\sigma)^n d\zeta_{F_\infty/\mathbb{Q}} = (1 - p^{n-1})\zeta(1 - n).$$
Iwaswawa’s main conjecture

\( \zeta_{F_\infty/Q} \) is the \( p \)-adic analogue of the Riemann zeta function \( \zeta(s) \). But we still understand only a little about the relationship between them. Here is a simple example. If \( n \) is an even negative integer, the integral on the left is well-defined, and we expect it to be a \( p \)-adic analogue of 
\[
(1 - p^{n-1}) \zeta(1 - n) \neq 0.
\]
But

**Problem.**

Prove that \( \int_G \chi(\sigma)^n d\zeta_{F_\infty/Q} \neq 0 \) for all but even integers \( n < 0 \).
Iwaswawa’s main conjecture: algebraic facts

\[ \zeta^* = \text{set of all non-zero divisors in } \Lambda(G). \]
\[ \Lambda(G)_{S^*} = \text{localization of } \Lambda(G) \text{ at } S^*. \]
\[ \mathcal{M}_e(G) = \text{category of all f.g. } S^*-\text{torsion } \Lambda(G) \text{ modules.} \]
\[ K_1(\Lambda(G)_{S^*}) = \Lambda(G)_{S^*}. \]
\[ K_0(\mathcal{M}_e(G)) = \text{Grothendieck group of category } \mathcal{M}_e(G). \]

Fact (follow from classical structure theory for modules in \( \mathcal{M}_e(G) \)). We have a canonical exact sequence

\[ K_1(\Lambda(G)) \rightarrow K_1(\Lambda(G)_{S^*}) \rightarrow \partial \ K_0(\mathcal{M}_e(G)) \rightarrow 0. \]

Definition

Given \( M \) in \( \mathcal{M}_e(G) \), a characteristic element for \( M \) is any \( f \) in \( K_1(\Lambda(G)_{S^*}) \) with \( \partial(f) = [M] \).

Key fact.

We can recover \( \chi(G, M) \) from \( f \).
Iwasawa’s main conjecture: Return to arithmetic

\[ R_\infty = \text{maximal abelian } p\text{-extension of } F_\infty, \text{ unramified outside } p. \]

\[ X_\infty = \text{Gal}(R_\infty)/F_\infty. \]

As \( R_\infty \) is Galois over \( \mathbb{Q} \), \( G \) acts on \( X_\infty \) via inner automorphisms \( \Rightarrow X_\infty \) is a \( \Lambda(G) \)-module.

**Theorem (Iwasawa)**

\( X_\infty \) is a f.g. \( S^* - \text{torsion} \) \( \Lambda(G) \)-module.
We can now state Iwasawa’s revolutionary ”main conjecture”:-

**Theorem (Iwasawa, Mazur-Wiles)**

*We have*

\[ \partial(\zeta_{F_{\infty}/\mathbb{Q}}) = [X_{\infty}] - [\mathbb{Z}_p]. \]

This provides a deep link between the $p$-adic zeta function and arithmetic.
Vast generalization of Iwasawa’s main conjecture

We will mainly discuss it for elliptic curves defined over $\mathbb{Q}$, but we could replace the elliptic curve by any motive.

$E$ - an elliptic curve defined over $\mathbb{Q}$.

$F_\infty/\mathbb{Q}$ - a Galois extension of $\mathbb{Q}$ satisfying
- $G = \text{Gal}(G_\infty/\mathbb{Q})$ is a $p$-adic Lie group with no element of order $p$;
- $F_\infty \supset \mathbb{Q}^{\text{cyc}}$;
- $F_\infty/\mathbb{Q}$ is unramified outside a finite set of primes of $\mathbb{Q}$.

Examples.

$F_\infty = \mathbb{Q}(E_p^\infty), F_\infty = \mathbb{Q}(\mu_p^\infty, p^\infty\sqrt{m})$.

Definition

$H = \text{Gal}(F_\infty/\mathbb{Q}^{\text{cyc}}), \Gamma = \text{Gal}(\mathbb{Q}^{\text{cyc}}/\mathbb{Q}), G/H = \Gamma$.

$$\Lambda(G) = \lim_{\longrightarrow} \mathbb{Z}_p(G/U),$$

$U$ runs over open normal subgroup of $G$. 13
**Algebraic facts, 5 author paper**

**Definition**

\[ S := \{ f \in \Lambda(G) : \Lambda(G)/\Lambda(G)f \text{ is a f.g. } \Lambda(H)\text{-module} \}, \]

\[ S^* = \bigcup_{n \geq 0} p^n S. \]

**Elementary fact.**

\[ S^* \text{ is a left and right Ore set of non-zero divisors in } \Lambda(G). \]

**Definition**

\[ \mathcal{M}_H(G) := \text{category of all f.g. } S^*\text{-torsion } \Lambda(G)\text{-module}. \]

**Fact.**

\[ M \in \mathcal{M}_H(G) \iff M/M(p) \text{ is a f.g. over } \Lambda(H). \]
Remark.
When \( \dim G > 1 \), it is no longer true that every f.g. torsion \( \Lambda(G) \) module is \( S^* \)-torsion.

\[ K_0(M_H(G)) = \text{Grothendieck group of category } M_H(G). \]
\[ S^* \text{ Ore } \Rightarrow \text{Localization } \Lambda(G)_{S^*} \text{ exists.} \]

Fact. We have a localization exact sequence

\[
K_1(\Lambda(G)) \to K_1(\Lambda(G)_{S^*}) \to \partial K_0(M_H(G)) \to 0.
\]

Definition
Given \( M \) in \( M_H(G) \), a characteristic element for \( M \) is any \( f \) in \( K_1(\Lambda(G)_{S^*}) \) with \( \partial(f) = [M] \).

Key Fact.
We can recover \( \chi(G, M) \) from \( f \).
What is the relevant arithmetic $\Lambda(G)$-module? We have known since Fermat it is the Selmer group:-

**Definition**

$$\text{Sel}(E/F_\infty) = \text{Ker}(H^1(F_\infty, E_p\infty) \to \prod_\nu H^1(F_\infty, \nu, E),$$

$$X(E/F_\infty) = \text{Hom}(\text{Sel}(E/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p).$$

Both have continuous left actions of $G = \text{Gal}(F_\infty/\mathbb{Q})$, which extends to a left action of $\lambda(G)$.

Easy to see that $X(E/F_\infty)$ is a f.g. $\Lambda(G)$-module.

**Question.**

When is $X(E/F_\infty) \in \mathfrak{M}_H(G)$?
Fact.

If $E$ has potential supersingular reduction at $p$, $X(E/F_\infty)$ is not $\Lambda(G)$-torsion, and so is certainly not in $\mathfrak{M}_H(G)$.

Problem.

How can we formulate a "main conjecture" in the supersingular case when $G$ has dimension $>1$.

Do not know the answer in simplest case:-
$E$ has CM, $F_\infty = \mathbb{Q}(E_{p\infty})$, $p$ supersingular.
Fact.
If $E$ has potential supersingular reduction at $p$, $X(E/F_\infty)$ is not $\Lambda(G)$-torsion, and so is certainly not in $\mathcal{M}_H(G)$.

Problem.
How can we formulate a "main conjecture" in the supersingular case when $G$ has dimension $> 1$.

Do not know the answer in simplest case:-
$E$ has CM, $F_\infty = \mathbb{Q}(E_p\infty)$, $p$ supersingular.

Returning to the potentially ordinary or multiplicative case we have
If $E$ has potential ordinary or multiplicative reduction at $p$, we always have $X(E/F_{\infty})$ is in $\mathcal{M}_H(G)$.

When $\dim G = 1$, this is precisely Mazur’s celebrated conjecture, which is now known if $F_{\infty}$ is abelian over $\mathbb{Q}(\text{Kato})$. But it seems subtle and difficult to attack Conjecture $\mathcal{M}_H(G)$ is general because of the problem of positive $\mu$-invariants occuring in these Iwasawa modules.

**Proof.**

Once $X(E/F_{\infty})$ is in $\mathcal{M}_H(G)$, it has a characteristic element $\xi_{E/F_{\infty}}$ in $K_1(\Lambda(G)_{S^*})$. Idea of main conjecture is that we can choose $\xi_{E/F_{\infty}}$ to be a $p$-adic $L$-function for $E/F_{\infty}$.
Description of $p$-adic $L$ function in good ordinary case

$A(G) =$ set consisting of all irreducible Artin representations of $G$. $L(G, \rho, s)$ for $\rho \in A(G)$.

$S =$ set consisting of $p$ and all $q \neq p$ with infinite inertial subgroup in $G$. $d^+(\rho), d^-(\rho)$-as usual. $\Omega^+, \Omega^-$-periods of Néron differential.

$e_p(\rho)$-\(\epsilon\)-factor of $\rho$ at $p$, $R_p(\rho, X)$-Euler factor at $p$,

$a - a_pX + pX^2 = (1 - \mu X)(1 - wX), \mu \in \mathbb{Z}_p^\times$.

Conjecture.

There exists a unique $\zeta_{E/F\infty}$ in $K_1(\Lambda(G)_{S^*})$ such that, for all $\rho$ in $A(G)$, we have

$$\zeta_{E/F\infty}(\rho) = \frac{L_S(E, \rho, 1)}{(\Omega^+_E)^{d^+(\rho)}(\Omega^-_E)^{d^-(\rho)}} e_p(\rho) \frac{R_p(\hat{\rho}, u^{-1})}{R_p(\rho, w^{-1})} u^{-f_{\rho,p}}$$

where $f_{\rho,p} =$ exponent of $p$ in conductor of $\rho$. 

\(\square\)
No theoretical results so far, but it works beautifully numerically! T. and V. Dokchitser have calculated $L(E, \rho, 1)$ when $F_\infty = \mathbb{Q}(E_{p^\infty})$ and $F_\infty = \mathbb{Q}(\mu_{p^\infty}, p^\infty \sqrt{m})$.

When $G$ has dimension $> 1$, only theoretical results so far are found by M. kakde in his Cambridge phD thesis. When $G$ is non-commutative of dimension 1, there also has been interesting work by J.Ritter, A. Weiss and T.Hara. All replace $E$ by TAte motive.
Kakde’s extension

Kakde brilliantly extended Iwasawa’s main conjecture.

\[
\begin{align*}
R_\infty & \quad H \\
G & \quad \mathbb{Q}(\mu_{p^\infty})^+ \\
\mathbb{Q} & \quad \Phi = \Delta \times \Gamma
\end{align*}
\]

\[R_\infty = \text{max abelian } p\text{-extension of } \mathbb{Q}(\mu_{p^\infty})^+, \text{ unramified outside } p\]

\[H = \mathbb{Z}_p^\lambda.\]

\[0 \rightarrow H \rightarrow G \rightarrow \Phi \rightarrow 0.\]
Kakde’s extension

**Definition**

\[ W_\infty = \text{max. abelian } p\text{-extension of } R_\infty, \text{ unram outside } p. \]

**Definition**

\[ X(W_\infty) = \text{Gal}(W_\infty/R_\infty). \]
Kakde’s extension

It is a f.g. $\Lambda(G)$-module.
Ferrero-Washington $\Rightarrow X(W_\infty) \in \mathcal{M}_H(G)$.

**Theorem (Kakde)**

Assume $\Gamma$ acts diagonally on $H$ (true for all $p < 30,000$). Then there exists $\zeta_{R_\infty}/Q$ in $K_1(\Lambda(G))_{S^*}$ such that

$$\zeta_{R_\infty}/Q(\rho \chi^n) = L\{p\}(\rho, 1 - n)$$

for all $\rho \in A(G)$ and all even integers $n > 1$. Moreover, we have

$$\partial_G(\zeta_{R_\infty}/Q) = [X(W_\infty)] - [\mathbb{Z}_p].$$

Method is to use Kato’s congruence, modified by Kakde. Very interesting question to formulate Kato’s congruences for a general $G$. 
Another possible application

$E$-runs over all elliptic curve over $\mathbb{Q}$.

$N(E) = \text{conductor of } E \text{ over } \mathbb{Q}$.

**Definition**

$r_E = \text{ord}_{s=1} L(E, s), \quad g_E = \text{rank } E(\mathbb{Q})$.

Mestre made the following remark.

**Theorem**

$r_E \leq c \log N(E)$ for some absolute constant $C$. 
Another possible application

Question.
Prove a similar upper bound for $g_E$?

Remark.
Follows from a classical 2-decent when $E$ has a rational point of order 2. But what if $E$ does not have a rational point of order 2?

One should be able to use the main conjectures of Iwasawa for a suitably chosen prime $p$ to attack this conjecture.
A conjectural generalization of Rohrlich’s Theorem

\[ \mathcal{X} = \text{set of all } 1\text{-dimensional characters of } \text{Gal}(\mathbb{Q}(\mu_{p^{\infty}})/\mathbb{Q}). \]

**Theorem (Rohrlich)**

There exists a constant \( C(E, p) \) such that

\[
\sum_{\chi \in \mathcal{X}} \text{ord}_{s=1} L(E, \chi, s) \leq C(E, p). 
\]

When combined with Kato’s work, it has many deep consequences, e.g.

**Corollary**

\( E(\mathbb{Q}(\mu_{p^{\infty}})) \) is a f.g. abelian group.
A conjectural generalization of Rohrlich’s Theorem

There is a possible vast generalization of Rohrlich’s theorem to all the $p$-adic Lie extensions discussed earlier. Note that

$$\mathcal{X}' \subset A(G),$$

where $\mathcal{X}'$ consists of all elements of $\mathcal{X}$ of $p$-power order.

**Conjecture.**

There exists a constant $C(E, F_\infty)$ such that, for all $\rho \in A(G)$, we have

$$\sum_{\chi \in \mathcal{X} \, \text{ord}_s = 1} L(E, \rho \chi, s) \leq C(E, F_\infty).$$

**Evidence.** When $F_\infty = \mathbb{Q}(\mu_{p^\infty}, p^\infty \sqrt{m})$, we show that this would follow from the $\mathcal{M}_H(G)$-Conjecture combined with a refinement of the Birch-Swinnerton-Dyer conjecture. (see paper by Fukaya, Kato, Sujatha, and C. in Journal of Algebraic Geometry).
Thank you!