Iwasawa Theory—Past and Present

Ralph Greenberg

University of Washington

Dedicated to the memory of Kenkichi Iwasawa.

Let F be a finite extension of $\mathbb{Q}$. Let p be a prime number. Suppose that F_∞ is a Galois extension of F and that $\Gamma = \mathrm{Gal}\,(F_\infty/F)$ is isomorphic to $\mathbb{Z}_p$, the additive group of p-adic integers. The nontrivial closed subgroups of Γ are of the form $\Gamma_n = \Gamma^{p^n}$ for $n \geq 0$. They form a descending sequence and Γ/Γ_n is cyclic of order p^n. If we let $F_n = F_\infty^{\Gamma_n}$, then we obtain a tower of number fields

$$F = F_0 \subset F_1 \subset \cdots \subset F_n \subset \cdots$$

such that F_n/F is a cyclic extension of degree p^n and $F_\infty = \bigcup_n F_n$. In 1956, at the summer meeting of the American Mathematical Society in Seattle, Iwasawa gave an invited address entitled *A theorem on Abelian groups and its application to algebraic number theory.* The application which he discussed is the following now famous theorem.

Theorem. *Let p^{e_n} be the highest power of p dividing the class number of F_n. Then there exist integers λ, μ, and ν such that $e_n = \lambda n + \mu p^n + \nu$ for all sufficiently large n.*

Iwasawa's proof of this theorem is based on studying the Galois group $X = \mathrm{Gal}\,(L_\infty/F_\infty)$, where $L_\infty = \bigcup_n L_n$ and L_n is the p-Hilbert class field of F_n. (That is, L_n is the maximal abelian p-extension of F_n which is unramified at all primes of F_n. By class field theory, L_n is a finite extension of F_n and $[L_n\!:\!F_n] = p^{e_n}$.) The extension L_∞/F is Galois and one has an exact sequence

$$0 \to X \to \mathrm{Gal}\,(L_\infty/F) \to \Gamma \to 0.$$

Since X is a projective limit of finite abelian p-groups, we can regard X as a compact $\mathbb{Z}_p$-module. ($\mathbb{Z}_p$ denotes the ring of p-adic integers.) But there is also a natural action of Γ on X. If $\gamma \in \Gamma$ and $x \in X$, one defines $\gamma(x) = \widetilde{\gamma}x\widetilde{\gamma}^{-1}$, where $\widetilde{\gamma} \in \mathrm{Gal}\,(L_\infty/F)$ is such that $\widetilde{\gamma}|_{F_\infty} = \gamma$. All of this structure allows Iwasawa to study the growth of $[L_n\!:\!F_n]$ which, as we mentioned, is equal to p^{e_n}.

The details of the proof of the above theorem were published in 1959 in [Iw3]. Iwasawa has written more than twenty papers about the theory of $\mathbb{Z}_p$-extensions. (He referred to extensions F_∞/F as described above as Γ-extensions until the late 1960's, when he switched to calling them $\mathbb{Z}_p$-extensions.) These papers introduced many new ideas which have really blossomed over the years. Several hundred papers have been written pursuing various aspects of these ideas, which have turned out to be fruitful in a number of different ways. In this article we will give a somewhat sketchy and personal account of these ideas and how they have developed. Along the way we will mention some of the many open questions which this topic has provided.

1. The relationship between the structure of X (together with the action of Γ) and the groups $\mathrm{Gal}\,(L_n/F_n)$ is rather easy to establish if we assume that F has just one prime $\mathfrak{p}$ lying over p and that this prime is totally ramified in F_∞/F. The prime $\mathfrak{p}$ would then be the only prime of F which is ramified in F_∞/F. For if $\mathfrak{q}$ is any prime of F not lying over p, then $\mathfrak{q}$ could be at most tamely ramified in the abelian extension F_n/F for any n. As is well-known, the ramification index for $\mathfrak{q}$ in F_n/F must then divide $N(\mathfrak{q})-1$, where $N(\mathfrak{q})$ denotes the cardinality of the residue field for $\mathfrak{q}$. It follows that the inertia subgroup of Γ for $\mathfrak{q}$ would be finite, which implies that it must be trivial since Γ is torsion-free. This argument shows in general that only primes of F lying over p can be ramified in a $\mathbb{Z}_p$-extension F_∞/F.

Let L_n^* denote the maximal abelian extension of F_n contained in L_∞. Obviously, $F_\infty \subset L_n^*$ and $L_n \subset L_n^*$. Let $\mathfrak{p}_n$ denote the unique prime of F_n lying over $\mathfrak{p}$, which is the only prime of F_n ramified in L_n^*/F_n. Clearly $L_n = (L_n^*)^{I_n}$, where I_n denotes the inertia subgroup of $\mathrm{Gal}\,(L_n^*/F_n)$ for $\mathfrak{p}_n$. Now $I_n \cap \mathrm{Gal}\,(L_n^*/F_\infty) = 0$ since L_n^*/F_∞ is unramified. Therefore $L_n^* = L_n F_\infty$ and, since $L_n \cap F_\infty = F_n$, we have $\mathrm{Gal}\,(L_n/F_n) \cong \mathrm{Gal}\,(L_n^*/F_\infty)$. On the other hand, $\mathrm{Gal}\,(L_\infty/L_n^*)$ is precisely the derived subgroup of $G_n = \mathrm{Gal}\,(L_\infty/F_n)$. We have an exact sequence

$$0 \to X \to G_n \to \Gamma_n \to 0.$$

Let γ_0 be a fixed topological generator of Γ. (This means that the subgroup generated by γ_0 is dense in Γ. It suffices to choose $\gamma_0 \in \Gamma$ such that $\gamma_0|_{F_1}$ is nontrivial.) Then $\gamma_n = \gamma_0^{p^n}$ is a topological generator of Γ_n. Since Γ_n acts on X by inner automorphisms, one can see that $\gamma_n(x)x^{-1}$ is a commutator in G_n for any $x \in X$. It is not hard to show that the derived subgroup of G_n is precisely $\{\gamma_n(x)x^{-1} \mid x \in X\}$. Changing to an additive notation for X, we write this as $\omega_n X$, where $\omega_n = \gamma_n - 1$. Therefore, $\mathrm{Gal}\,(L_n^*/F_\infty) \cong X/\omega_n X$, giving the result that

$$\mathrm{Gal}\,(L_n/F_n) \cong X/\omega_n X \tag{1}$$

for all $n \geq 0$. This isomorphism is induced by the restriction map from X to $\mathrm{Gal}\,(L_n/F_n)$.

Let A be a discrete, p-primary, abelian group on which Γ acts continuously (as automorphisms). Assume that $A^{\Gamma_n} = \{a \mid a \in A,\ \gamma_n(a) = a\}$ is finite for all $n \geq 0$. (Iwasawa uses the term "strictly Γ-finite" for such an A.) The structure theory which Iwasawa develops in [Iw3] then allows him to prove that $|A^{\Gamma_n}| = p^{\lambda n + \mu p^n + \nu}$ for all sufficiently large n, where the integers λ and μ are described in terms of the structure of A and where $\nu \in \mathbb{Z}$. He applies this to $A = \mathrm{Hom}_{\mathrm{cont}}(X, \mathbb{Q}_p/\mathbb{Z}_p)$. The action of Γ on this group is induced by the action of Γ on X. Note that $X/\omega_n X$ is the maximal quotient of X on which Γ_n acts trivially. Hence $A^{\Gamma_n} = \mathrm{Hom}(X/\omega_n X, \mathbb{Q}_p/\mathbb{Z}_p)$ is finite and has the same order as $X/\omega_n X$. Iwasawa's theorem would then follow (in the special case where F has just one prime above p, totally ramified in F_∞/F).

Serre gave a Seminaire Bourbaki lecture on Iwasawa's results in 1959. There he introduced a somewhat different approach which Iwasawa soon adopted. The idea is to view X as a module over the ring $\Lambda = \mathbb{Z}_p[[T]]$ by letting T act on the $\mathbb{Z}_p$-module X as $\omega_0 = \gamma_0 - 1$. This makes X into a $\mathbb{Z}_p[T]$-module. One can easily show that the action of T on X is "topologically nilpotent", i.e., any open subgroup of X contains $T^n X$ for $n \gg 0$. Then X does become a Λ-module. It turns out to be a finitely generated, torsion Λ-module. (This is true without any assumption about the primes of F over p. In the special case that we have been considering, it follows easily from the fact that $X/TX \cong \mathrm{Gal}\,(L_0/F_0)$ is finite, together with a version of Nakayama's Lemma for compact Λ-modules.) Serre then derives Iwasawa's structure theorem from a classification theorem for such Λ-modules.

This classification theorem is quite easy to state:

Theorem. *If X is any finitely generated, torsion Λ-module, then there exists a Λ-module homomorphism*

$$X \to \bigoplus_{i=1}^{t} \Lambda/(f_i(T)^{a_i}),$$

with finite kernel and cokernel, where each $f_i(T)$ is an irreducible element of Λ and each a_i is a positive integer for $1 \le i \le t$. The value of t, the prime ideals $(f_i(T))$, and the corresponding a_i's are uniquely determined by X, up to their order.

A Λ-module homomorphism with finite kernel and cokernel is often called a pseudo-isomorphism. The ring Λ is a UFD, but not a PID. Furthermore, Λ is a complete, Noetherian local ring (with maximal ideal $\mathfrak{m} = (p, T)$) and is regular of dimension 2. The prime ideals of height 1 are principal. One of them is $(p) = p\Lambda$. The others have a unique generator of the form $f(T) = T^l + a_{l-1}T^{l-1} + \cdots + a_0$, where $l \ge 1$, $a_0, a_1, \ldots, a_{l-1} \in p\mathbb{Z}_p$, and $f(T)$ is irreducible as an element of $\mathbb{Q}_p[T]$. (A polynomial of this form, irreducible or not, is called a "distinguished" polynomial.) We will assume that each $f_i(T)$ is either p or an irreducible, distinguished polynomial. Then we define

$$f_X(T) = \prod_{i=1}^{t} f_i(T)^{a_i}.$$

One refers to $f_X(T)$ as the characteristic polynomial of X. The invariants λ and μ which occur in Iwasawa's theorem can be described just in terms of $f_X(T)$. (No hypothesis on the primes of F lying over p is needed.) It turns out that $\lambda = \deg(f_X(T))$ and that μ is just the largest integer such that p^μ divides

$f_X(T)$ in Λ (or $\mathbb{Z}_p[T]$). One can also describe λ and μ in terms of the Λ-module X. We have $X/X_{\mathbb{Z}_p\text{-tors}} \cong \mathbb{Z}_p^{\lambda}$. This determines λ just in terms of the structure of X as a $\mathbb{Z}_p$-module. As for μ, let $Y = X_{\mathbb{Z}_p\text{-tors}}$. Since Λ is Noetherian, Y is finitely generated as a Λ-module. It therefore has finite exponent p^c as a group. For $i \geq 0$, $p^iY/p^{i+1}Y$ is a module over the ring $\overline{\Lambda} = \Lambda/p\Lambda$, which is simply $\mathbb{F}_p[[T]]$, with $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then μ is just the sum of the $\overline{\Lambda}$-ranks of the modules $p^iY/p^{i+1}Y$, where $0 \leq i \leq c-1$. It is often better to think of Λ in a more intrinsic way as $\mathbb{Z}_p[[\Gamma]]$, which by definition is $\varprojlim \mathbb{Z}_p[\mathrm{Gal}(F_n/F)]$. This inverse limit is defined by the $\mathbb{Z}_p$-algebra homomorphisms $\mathbb{Z}_p[\mathrm{Gal}(F_m/F)] \to \mathbb{Z}_p[\mathrm{Gal}(F_n/F)]$ (for $m \geq n$) induced by the restriction maps $\sigma \to \sigma|_{F_n}$ for $\sigma \in \mathrm{Gal}(F_m/F)$. The identification of $\mathbb{Z}_p[[\Gamma]]$ with $\mathbb{Z}_p[[T]]$ depends on the choice of topological generator γ_0 for Γ. One identifies γ_0 with $1+T$.

We continue with the special case where only one prime $\mathfrak{p}$ of F lies over p and F_∞/F is totally ramified at $\mathfrak{p}$. Then $p^{e_n} = |X/\omega_nX|$ for $n \geq 0$. To study how these orders grow, one reduces to the case of a Λ-module of the form $Y = \Lambda/(g(T))$, where $g(T)$ is one of the $f_i(T)^{a_i}$'s. Then Y/ω_nY will also be finite and we have

$$|Y/\omega_nY| \approx \Big(\prod_{\zeta^{p^n}=1} g(\zeta-1)\Big) \tag{2}$$

where we write $a \approx b$ to mean that two nonzero p-adic integers a and b satisfy $ab^{-1} \in \mathbb{Z}_p^{\times}$. This is not hard to verify. The quotient ring $\Lambda/\omega_n\Lambda$ can be identified with the group ring $\mathbb{Z}_p[\mathrm{Gal}(F_n/F)]$. (Thinking of Λ more intrinsically as $\Lambda = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(F_n/F)]$, one has a surjective homomorphism $\Lambda \to \mathbb{Z}_p[\mathrm{Gal}(F_n/F)]$ defined by sending $T = \gamma_0 - 1$ to the element $\gamma_0|_{F_n} - 1$. The kernel of this homomorphism is generated by ω_n.) Thus, $\Lambda/\omega_n\Lambda$ is a free $\mathbb{Z}_p$-module of rank p^n. Multiplication by T on $\Lambda/\omega_n\Lambda$ is $\mathbb{Z}_p$-linear and has eigenvalues $\zeta-1$, where $\zeta^{p^n} = 1$. Now Y/ω_nY is the cokernel of multiplication by $g(T)$ on $\Lambda/\omega_n\Lambda$. This map is $\mathbb{Z}_p$-linear and has determinant $\prod_\zeta g(\zeta-1)$, where $\zeta^{p^n} = 1$. This implies (2). If $g(T) = p^m$, then one gets $|Y/\omega_nY| = p^{mp^n}$. If $g(T) = T^l + a_{l-1}T^{l-1} + \cdots + a_0$, where $p|a_i$ for $0 \leq i < l$, then the valuation of $g(\zeta-1)$ is the same as that of $(\zeta-1)^l$ when ζ has sufficiently large order. One then finds that $|Y/\omega_nY| = p^{ln+v}$ when $n \gg 0$, where v is a constant. Putting all of this together, and taking into account the finite kernel and cokernel, one obtains that $|X/\omega_nX| = p^{\lambda n + \mu p^n + \nu}$ for $n \gg 0$, where ν is a constant.

A more detailed account of the proof of Iwasawa's theorem (including the general case where one must keep careful track of the inertia groups for primes above p in $\mathrm{Gal}(L_n^*/F_n)$) can be found in [Iw3], [Se1], or perhaps more conveniently in Washington's book [Wa]. In the general case, it sometimes happens that X/ω_nX is infinite. This happens precisely when $f_X(\zeta-1) = 0$ for some p^n-th root of unity ζ.

2. We know very little about the Iwasawa invariants λ and μ associated to an arbitrary $\mathbb{Z}_p$-extension F_∞/F. We will just mention two rather special results.

Proposition (2.1) *Assume that the class number of F is not divisible by p and that F has only one prime lying over p. Let F_∞/F be any $\mathbb{Z}_p$-extension. Then $\lambda = \mu = \nu = 0$.*

Proposition (2.2) *Assume that p splits completely in $F/\mathbb{Q}$. Let F_∞/F be a $\mathbb{Z}_p$-extension in which every prime of F lying over p is ramified. Then $\lambda(F_\infty/F) \geq r_2$, where r_2 denotes the number of complex primes of F.*

Proposition 2.1 is stated in [Iw3], and follows easily from a result proved in his earlier paper [Iw1]. We can prove it as follows. First note that the unique prime $\mathfrak{p}$ of F lying over p must be ramified in F_1/F. Otherwise F_1 would be contained in the p-Hilbert class field L_0 of $F = F_0$, contradicting the assumption that p doesn't divide the class number of F. This implies that $\mathfrak{p}$ is totally ramified in F_∞/F. Using the notation described before, we have $X/TX \cong \mathrm{Gal}\,(L_0/F_0) = 0$. Hence $TX = X$ and therefore $X = 0$ (because the action of T on X is topologically nilpotent). But then $\mathrm{Gal}\,(L_n/F_n) = X/\omega_n X = 0$ for all n, which clearly means that $\lambda = \mu = \nu = 0$, as stated.

To prove proposition 2.2, we need the following existence theorem for $\mathbb{Z}_p$-extensions.

Theorem. *Let $\widetilde{F}$ denote the compositum of all $\mathbb{Z}_p$-extensions of F. Then*

$$\mathrm{Gal}\,(\widetilde{F}/F) \cong \mathbb{Z}_p^d,$$

where $r_2 + 1 \leq d \leq [F : \mathbb{Q}]$.

One consequence of this theorem is that F will have infinitely many distinct $\mathbb{Z}_p$-extensions when F is not totally real. The proof of the theorem is a straightforward application of the idelic form of class field theory. Let

$$U^0 = \prod_{\mathfrak{p}|p} U^0_{\mathfrak{p}},$$

where $U^0_{\mathfrak{p}}$ denotes the group of principal units in the completion $F_{\mathfrak{p}}$ of F at $\mathfrak{p}$. Then U^0 can be considered as a $\mathbb{Z}_p$-module and

$$\mathrm{rank}_{\mathbb{Z}_p}(U^0) = \sum_{\mathfrak{p}|p} [F_{\mathfrak{p}} : \mathbb{Q}_p] = [F : \mathbb{Q}].$$

The Artin map defines a homomorphism from U^0 to $\mathrm{Gal}\,(\widetilde{F}/F)$ with finite cokernel (isomorphic to $\mathrm{Gal}\,(L_0 \cap \widetilde{F}/F)$). To describe the kernel of this homomorphism, let E denote the group of units in F and let E^0 denote the subgroup of units $\epsilon \equiv 1 \pmod{\mathfrak{p}}$ for all $\mathfrak{p}|p$, which has finite index in E. We can consider E^0 as a subgroup of U^0 by using the natural injection $F \to \prod_{\mathfrak{p}|p} F_{\mathfrak{p}}$. Then the topological closure $\overline{E^0}$ of E^0 in U^0 is a $\mathbb{Z}_p$-submodule; it is the image of $E^0 \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and thus has $\mathbb{Z}_p$-rank bounded above by $\mathrm{rank}_{\mathbb{Z}}(E^0)$. Let H denote the kernel of the Artin map $U^0 \to \mathrm{Gal}(\widetilde{F}/F)$. Then H can be characterized as the smallest $\mathbb{Z}_p$-submodule of U^0 containing $\overline{E^0}$ and such that U^0/H is torsion-free. Clearly $[H:\overline{E^0}] < \infty$. The theorem follows from this because U^0/H has $\mathbb{Z}_p$-rank equal to $[F:\mathbb{Q}] - \mathrm{rank}_{\mathbb{Z}_p}(\overline{E^0})$ and $\mathrm{rank}_{\mathbb{Z}_p}(\overline{E^0}) \leq \mathrm{rank}_{\mathbb{Z}}(E) = r_1 + r_2 - 1$, where $r_1 = [F:\mathbb{Q}] - 2r_2$ is the number of real primes of F.

It is extremely likely that we have the equality $d = r_2 + 1$ in the above theorem. This is known as Leopoldt's Conjecture. It is clearly equivalent to the assertion that

$$\mathrm{rank}_{\mathbb{Z}_p}(\overline{E^0}) = \mathrm{rank}_{\mathbb{Z}}(E^0),$$

the second quantity being $r = r_1 + r_2 - 1$. More concretely, it can be stated as follows. Let $\sigma_1, \ldots, \sigma_n$ denote the distinct embeddings of F into $\overline{\mathbb{Q}}_p$, where $n = [F:\mathbb{Q}]$. Suppose that $\epsilon_1, \ldots, \epsilon_r$ are generators of E^0 (modulo the subgroup of roots of unity). Then the conjecture asserts that the $n \times r$ matrix $[\log_p(\sigma_s(\epsilon_t))]_{1 \leq s \leq n, 1 \leq t \leq r}$ has rank r. Leopoldt considered just the case where F is totally real. Then he conjectured the nonvanishing of the so-called p-adic regulator for F, the determinant of the $r \times r$ submatrix obtained by omitting any row (well-defined up to ± 1). The above formulation in terms of $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}(\widetilde{F}/F))$ is due to Iwasawa and has been proven when F is an abelian extension of $\mathbb{Q}$ or of an imaginary quadratic field. In these cases, it follows from Brumer's p-adic version of a famous theorem of Baker concerning linear forms in logarithms of algebraic numbers.

Obviously $F_\infty \subset \widetilde{F}$. But it is also true that $\widetilde{F} \subset L_\infty$ under the stated assumption that $F_{\mathfrak{p}} = \mathbb{Q}_p$ for all $\mathfrak{p}|p$. This is because the inertia subgroup $I_{\mathfrak{p}}$ of $\mathrm{Gal}(\widetilde{F}/F)$ for each such $\mathfrak{p}$ is precisely the image of $U^0_{\mathfrak{p}}$ (contained in U^0 as a direct factor) under the Artin map $U^0 \to \mathrm{Gal}(\widetilde{F}/F)$. Thus $I_{\mathfrak{p}} \cong \mathbb{Z}_p$. But the image of $I_{\mathfrak{p}}$ in $\mathrm{Gal}(F_\infty/F)$ under the restriction homomorphism is also isomorphic to $\mathbb{Z}_p$ since $\mathfrak{p}$ is ramified in F_∞/F. Therefore, $I_{\mathfrak{p}} \cap \mathrm{Gal}(\widetilde{F}/F_\infty) = 0$, which implies that the primes of F_∞ lying over any such $\mathfrak{p}$ are unramified in $\widetilde{F}/F_\infty$. Since primes not dividing p are unramified in every $\mathbb{Z}_p$-extension of F, and hence in $\widetilde{F}/F$, it follows that $\widetilde{F} \subset L_\infty$. Thus $X = \mathrm{Gal}(L_\infty/F_\infty)$ has $\mathrm{Gal}(\widetilde{F}/F_\infty) \cong \mathbb{Z}_p^{d-1}$ as a quotient. This implies that indeed $\lambda = \mathrm{rank}_{\mathbb{Z}_p}(X) \geq d - 1 \geq r_2$. In fact, Γ acts trivially on the quotient $\mathrm{Gal}(\widetilde{F}/F_\infty)$ and consequently $f_X(T)$ is divisible by T^{r_2}. If $r_2 > 0$, we obtain examples where $X/\omega_0 X$ is infinite, since $\omega_0 = T$.

Several of Iwasawa's papers discuss the values of λ and μ in the important case where $F = \mathbb{Q}(\zeta_p)$, $F_1 = \mathbb{Q}(\zeta_{p^2}), \ldots, F_n = \mathbb{Q}(\zeta_{p^{n+1}}), \ldots$, where, for any $m \geq 1$, we let ζ_m denote a primitive m-th root of unity. Then $F_\infty = \bigcup_n F_n$ is the so-called cyclotomic $\mathbb{Z}_p$-extension of F. If p is a regular prime (i.e., a prime such that the class number of $F = \mathbb{Q}(\zeta_p)$ is not divisible by p), then proposition 2.1 immediately implies that $\lambda = \mu = \nu = 0$ for this (and any) $\mathbb{Z}_p$-extension of F. We will denote the Iwasawa invariants for F_∞/F by λ_p, μ_p, and ν_p. How can one compute them for irregular primes p?

It is customary to factor the class number h_p of F as $h_p = h_p^- h_p^+$, where h_p^+ denotes the class number of the maximal real subfield $F^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ of F. There is, of course, a similar factorization of the class number of F_n. The maximal real subfields form a $\mathbb{Z}_p$-extension $F_\infty^+ = \bigcup_n F_n^+$ of F^+. The Iwasawa invariants can then be written as $\lambda_p = \lambda_p^- + \lambda_p^+$, $\mu_p = \mu_p^- + \mu_p^+$, $\nu_p = \nu_p^- + \nu_p^+$, where $\lambda_p^+, \mu_p^+, \nu_p^+$ are the invariants for F_∞^+/F^+. If $X = \mathrm{Gal}\,(L_\infty/F_\infty)$ as before, then $\mathrm{Gal}\,(F_\infty/F_\infty^+) \cong \mathbb{Z}/2\mathbb{Z}$ acts on X (by inner automorphisms). Assuming that p is odd, we then get a decomposition $X = X^- \oplus X^+$. We have $f_X(T) = f_{X^-}(T) f_{X^+}(T)$. The invariants λ_p^+, μ_p^+, and ν_p^+ can be recovered from $f_{X^+}(T)$ (or from X^+) just as described earlier, and similarly for λ_p^-, μ_p^-, and ν_p^-. For example, $\lambda_p^- = \deg(f_{X^-}(T)) = \mathrm{rank}_{\mathbb{Z}_p}(X^-)$. Let S_0 denote the p-primary subgroup of the ideal class group of $F = F_0$. Then, by class field theory, $S_0 \cong \mathrm{Gal}\,(L_0/F_0)$. Now $\mathrm{Gal}\,(F/F^+)$ acts on S_0 in an obvious way and on $\mathrm{Gal}\,(L_0/F_0)$ by inner automorphisms. The isomorphism is compatible with these actions (and even for the actions of $\varDelta = \mathrm{Gal}\,(F/\mathbb{Q})$ on both groups, which we will consider later). Correspondingly, we can write $S_0 = S_0^- \oplus S_0^+$ and the power of p dividing h_p^- (respectively, h_p^+) is just the order of S_0^- (respectively, S_0^+). Our earlier arguments show that

$$X^-/TX^- \cong S_0^-, \qquad\qquad X^+/TX^+ \cong S_0^+.$$

A well-known conjecture of Vandiver states that $p \nmid h_p^+$. That is, $S_0^+ = 0$. This would imply that $X^+ = 0$, and hence $\lambda_p^+ = \mu_p^+ = \nu_p^+ = 0$. As we will mention later, there is considerable numerical support for Vandiver's conjecture.

Iwasawa's paper *On some invariants of cyclotomic fields*, published in 1958, is devoted to finding criteria for the nonvanishing of μ_p. One such criterion is an infinite sequence of congruences involving Bernoulli numbers. We will state the first two of these congruences below. It is in fact sufficient to consider μ_p^-. To justify this, Iwasawa refers to a theorem of Takagi [T] which states that

$$\dim_{\mathbb{Z}/p\mathbb{Z}}(S_n^-/pS_n^-) \geq \dim_{\mathbb{Z}/p\mathbb{Z}}(S_n^+/pS_n^+) \tag{3}$$

for all $n \geq 0$. Here we let S_n denote the p-primary subgroup of the ideal class group of F_n, which can be decomposed as $S_n = S_n^- \oplus S_n^+$ by the action of $\mathrm{Gal}\,(F_n/F_n^+)$. The proof of (3) is based on the Spiegelungssatz (the Reflection Principle). It then follows that:

$$\mu_p^+ > 0 \Rightarrow \mu_p^- > 0, \textit{ and hence, } \mu_p > 0 \Leftrightarrow \mu_p^- > 0.$$

(This is reminiscent of a theorem of Kummer stating that: $p|h_p^+ \Rightarrow p|h_p^-$. That result can also be proved by using the Reflection Principle.) The fields

F_n are abelian over $\mathbb{Q}$. Iwasawa transforms the classical formula for the first factor of the class number of F_n, and also uses Stickelberger's theorem giving a nontrivial annihilator in $\mathbb{Z}[\mathrm{Gal}(F_n/\mathbb{Q})]$ for S_n^-, to obtain necessary and sufficient conditions for the nonvanishing of μ_p^-. We will just state here one necessary condition which turns out to be quite effective. (Iwasawa uses it to show that $\mu_p^- = 0$ for $p = 37, 59, 67$—the three irregular primes < 100. This condition actually suffices to prove the vanishing of μ_p^- for all $p < 8,000,000$.)

If $\mu_p^- > 0$*, then there exists an even integer* j*,* $2 \le j \le p-3$*, such that*

$$B_j \equiv 0 \pmod{p\mathbb{Z}_p} \quad \textit{and} \quad \frac{B_{j+p-1}}{j+p-1} \equiv \frac{B_j}{j} \pmod{p^2\mathbb{Z}_p}. \tag{4}$$

Here B_j denotes the j-th Bernoulli number, which we recall is defined by the generating function

$$\frac{xe^x}{e^x - 1} = \sum_{j=0}^{\infty} B_j \frac{x^j}{j!}.$$

The B_j's are clearly rational numbers and are nonzero precisely when j is even or $j = 1$. If $j \not\equiv 0 \pmod{p-1}$, then $B_j/j \in \mathbb{Z}_p$ and so the congruences in (4) just involve elements of $\mathbb{Z}_p$. Kummer's famous criterion for regularity states that: $p|h_p \Leftrightarrow B_j \equiv 0 \pmod{p\mathbb{Z}_p}$ *for some even* j*,* $2 \le j \le p-3$. The first congruence in (4) then follows because $\mu_p^- > 0$ certainly implies that $p|h_p$. The second congruence is stronger than the well-known Kummer congruence:

$$\frac{B_{j'}}{j'} \equiv \frac{B_j}{j} \pmod{p\mathbb{Z}_p} \quad \textit{if} \quad j' \equiv j \not\equiv 0 \pmod{p-1}, \tag{5}$$

but it can sometimes hold. For example, $(B_{16}/16) - (B_4/4) = -7\cdot 13^2/2^5\cdot 5\cdot 17$, which implies the second congruence in (4) for the pair $(p, j) = (13, 4)$.

A subsequent paper *On the theory of cyclotomic fields* (published in 1959) continues with the case $F = \mathbb{Q}(\zeta_p)$, $F_\infty = \mathbb{Q}(\zeta_p, \zeta_{p^2}, \dots)$, introducing several new Galois groups into the topic. Let M_∞ denote the maximal, abelian extension of F_∞ which is pro-p (i.e., $Y = \mathrm{Gal}(M_\infty/F_\infty)$ is a projective limit of finite p-groups) and in which only the prime of F_∞ lying over p is ramified. If L_∞ is as before, then obviously $L_\infty \subset M_\infty$, and so $X = \mathrm{Gal}(L_\infty/F_\infty)$ is a quotient of $Y = \mathrm{Gal}(M_\infty/F_\infty)$, as Λ-modules. In contrast to X, Y is not Λ-torsion. Iwasawa shows that $\mathrm{rank}_\Lambda(Y) = \frac{1}{2}(p-1)$, although he doesn't use the terminology of Λ-modules. Let N_∞ be the field obtained by adjoining to F_∞ all p-power roots of units of F_∞. Then $N_\infty \subset M_\infty$ and $\mathrm{Gal}(M_\infty/N_\infty)$ is shown to be Λ-torsion. Let $S_\infty = \varinjlim S_n$, where the maps $S_n \to S_m$ for $m > n$ defining this direct limit are as follows: if $c \in S_n$ is the class of the ideal $\mathfrak{a}$ of the ring of integers $\mathcal{O}_n$ of F_n, then c is mapped to the class of $\mathfrak{a}\mathcal{O}_m$

in S_m. Then S_∞ can be regarded as a discrete Λ-module, which Iwasawa shows is isomorphic to $\mathrm{Hom}(\mathrm{Gal}\,(M_\infty/N_\infty), \mu_{p^\infty})$. (Here μ_{p^∞} is the group of p-power roots of unity. The isomorphism preserves the action of $\mathrm{Gal}\,(F_\infty/\mathbb{Q})$, and in particular the action of Γ, on both groups.)

We will state several important results from this paper. The Galois action on μ_{p^∞} gives a canonical isomorphism $\mathrm{Gal}\,(F_\infty/\mathbb{Q}) \cong \mathbb{Z}_p^\times = \mu_{p-1} \times (1+p\mathbb{Z}_p)$ for any odd prime p. Here μ_{p-1} denotes the $(p-1)$st roots of unity in $\mathbb{Z}_p^\times$. We write $\mathrm{Gal}\,(F_\infty/\mathbb{Q}) = \Delta \times \Gamma$, where $\Gamma = \mathrm{Gal}\,(F_\infty/F)$ as before. We regard Δ as $\mathrm{Gal}\,(F_\infty/\mathbb{Q}_\infty)$, where $\mathbb{Q}_\infty$ is the unique subfield of F_∞ such that $\mathrm{Gal}\,(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. (In fact, $\mathbb{Q}_\infty$ is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$.) There is also a canonical isomorphism $\omega : \Delta \to \mu_{p-1} \subset \mathbb{Z}_p^\times$ defined by the action of Δ on μ_{p^∞}. If A is any $\mathbb{Z}_p$-module on which Δ acts, then we have a canonical decomposition $A = \bigoplus\limits_{k=0}^{p-2} A^{\omega^k}$, where $A^{\omega^k} = \{a | a \in A, \delta(a) = \omega^k(\delta)a \ \forall\ \delta \in \Delta\}$. We consider this decomposition for $A = X$, Y, and S_∞. Iwasawa refers to this as the Δ-decomposition. Since $\mathrm{Gal}\,(F_\infty/\mathbb{Q})$ acts on these groups, the corresponding actions of Δ and Γ commute and so we can regard X^{ω^k}, Y^{ω^k}, and $S_\infty^{\omega^k}$ as Λ-modules. For each k, $0 \le k \le p-2$, let $\lambda_p^{(k)}$ and $\mu_p^{(k)}$ denote the Iwasawa invariants for X^{ω^k}, which are determined by the polynomial $f_{X^{\omega^k}}(T)$. Then $\lambda_p = \sum\limits_{k=0}^{p-2} \lambda_p^{(k)}$, $\mu_p = \sum\limits_{k=0}^{p-2} \mu_p^{(k)}$. The results we want to mention are the following.

Proposition (2.3) *Suppose that $0 \le i$, $j \le p-2$ are integers such that $i + j \equiv 1 \pmod{p-1}$ and i is odd (so that j is even). Then $\lambda_p^{(i)} \ge \lambda_p^{(j)}$ and $\mu_p^{(i)} \ge \mu_p^{(j)}$. Consequently, $\lambda_p^- \ge \lambda_p^+$ and $\mu_p^- \ge \mu_p^+$.*

Proposition (2.4) *Assume that i and j are as in the previous proposition. Then there exists a perfect pairing*

$$S_\infty^{\omega^i} \times Y^{\omega^j} \to \mu_{p^\infty}$$

which is compatible with the action of Γ.

(Note: This means that $Y^{\omega^j} \cong \mathrm{Hom}(S_\infty^{\omega^i}, \mu_{p^\infty})$ as Λ-modules. The pairing is also compatible with the action of Δ because $\omega^i\omega^j = \omega$.)

Proposition (2.5) *For odd i, X^{ω^i} has no nonzero, finite Λ-submodules. For all k, Y^{ω^k} has no nonzero, finite Λ-submodules.*

Proposition 2.4 is a refined version of the Reflection Principle. The pairing is defined roughly as follows. Let $s \in S_\infty^-$ have order p^m. Suppose that s is the class of an ideal $\mathfrak{a}$ (coming from some level $F_{m'}$ of F_∞) such that $\overline{\mathfrak{a}} = \mathfrak{a}^{-1}$ and $\mathfrak{a}^{p^m} = (\alpha)$, $\alpha \in F_{m'}^\times$. One can choose α so that $\overline{\alpha} = \alpha^{-1}$. Let $y \in Y$.

Define $(s,y) \in \mu_{p^\infty}$ by $(s,y) = y(\beta)/\beta$, where $\beta^{p^m} = \alpha$. (One checks easily that $\beta \in M_\infty^\times$.) This can be verified to induce a well-defined perfect pairing

$$S_\infty^- \times Y^+ \to \mu_{p^\infty}$$

and one obtains proposition 2.4 by studying the action of Δ. Proposition 2.3 is a consequence of proposition 2.4. First note that

$$F_\infty \subset L_\infty \subset M_\infty$$

and so one has a surjective Λ-module homomorphism $Y^{\omega^k} \to X^{\omega^k}$ for all k. Hence, for even j, we see that $f_{X^{\omega^j}}(T)$ divides $f_{Y^{\omega^j}}(T)$ in Λ. Therefore $\lambda_p^{(j)}$ and $\mu_p^{(j)}$ are bounded above by the λ- and μ-invariants of Y^{ω^j}, which the above pairing shows are actually equal to $\lambda_p^{(i)}$ and $\mu_p^{(i)}$, respectively. This equality follows from Iwasawa's theory of adjoints, which allows one to relate the structure of the discrete Λ-module $S_\infty^{\omega^i}$ to that of the compact Λ-module X^{ω^i}. In particular, the invariant $\lambda_p^{(i)}$ can be identified as the $\mathbb{Z}_p$-rank of X^{ω^i} or as the $\mathbb{Z}_p$-corank of $S_\infty^{\omega^i}$. (That is, the maximal divisible subgroup of $S_\infty^{\omega^i}$ is $(S_\infty^{\omega^i})_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_p^{(i)}}$.) As we will mention below, proposition 2.4 and the theory of adjoints gives an important relationship between X^{ω^i} and Y^{ω^j}.

Now we discuss briefly the proof of proposition 2.5. The first part asserts that X^- has no nonzero finite Λ-submodules. Iwasawa shows that this assertion is equivalent to the fact that the maps $S_n^- \to S_m^-$ for $m > n$ are injective, which he verifies using properties of the units of F_∞, interpreted in terms of Galois cohomology. In a footnote, Iwasawa states that the injectivity of the map $S_0^- \to S_1^-$ was proved by F. Pollaczek in [Po] where, Iwasawa writes, one may trace the germ of other results proved in the present paper. Iwasawa also refers to Pollaczek's paper in [Iw2]. As for the second part, one crucial ingredient is the fact that S_∞ has no proper Λ-submodules of finite index. (The pairing in proposition 2.4 would then immediately give the result for even values of k.) Actually, it is true for any $\mathbb{Z}_p$-extension F_∞/F (with F arbitrary) that $S_\infty = \varinjlim S_n$ has no proper Λ-submodules of finite index. This is not hard to deduce from the fact that the norm map $N_{m,n} : S_m \to S_n$ is surjective for $m > n > n_0$, where n_0 is large enough so that at least one prime (over p) is totally ramified in F_∞/F_{n_0}. The surjectivity of the norm maps follows from class field theory together with the surjectivity of the restriction maps $\mathrm{Gal}(L_m/F_m) \to \mathrm{Gal}(L_n/F_n)$ for $m > n > n_0$.

One more result that was already alluded to above relates X^{ω^i} and Y^{ω^j} when i, j are as in propositions 2.3, 2.4. Let $\kappa : \Gamma \xrightarrow{\sim} 1 + p\mathbb{Z}_p$ denote the canonical isomorphism giving the action of Γ on μ_{p^∞}. There is an involution of Λ defined by sending $\gamma \in \Gamma$ to $\kappa(\gamma)\gamma^{-1} \in \Lambda^\times$. If γ_0 is a fixed topological generator of Γ, then $T = \gamma_0 - 1$ is sent to $\dot{T} = \kappa(\gamma_0)(1+T)^{-1} - 1$. Now if Z is any Λ-module, we define a new Λ-module $\dot{Z}$ by letting $\theta \in \Lambda$ act on $z \in Z$ just as $\dot{\theta}z$, where $\dot{\theta}$ is the image of θ under the above involution. Then combining the theory of adjoints in [Iw4] with proposition 2.4 (and the fact that $S_\infty^{\omega^i}$ is the adjoint of X^{ω^i}), Iwasawa obtains the following theorem.

Proposition (2.6) *With the above notation, Y^{ω^j} is pseudo-isomorphic to $\dot{X}^{\omega^i}$. Hence $f_{Y^{\omega^j}}(T)$ generates the same ideal as $f_{X^{\omega^i}}(\kappa(\gamma_0)(1+T)^{-1}-1)$ in Λ.*

3. Returning to the question of determining λ_p, μ_p, and ν_p, Iwasawa shows in [Iw2] that $\mu_p = 0$ and $\lambda_p = 1$ for $p = 37, 59$, and 67. We've already discussed the vanishing of μ_p. Now it is known that $p \| h_p$ for these three primes. Hence $p \| h_p^-$ and so $S_0 = S_0^-$ is cyclic of order p. Recall that $X/TX \cong S_0$. Therefore, X is a cyclic Λ-module (by Nakayama's Lemma). Since $X = X^-$ has no nonzero, finite Λ-submodules by proposition 2.5, it follows easily that X is isomorphic to $\Lambda/(g(T))$, where $g(T) = f_X(T)$. By (2), we have $g(0) \approx p$, but it is also known that $|S_1| = p^2$ for the above three primes, and so we have $\prod g(\zeta - 1) \approx p^2$, where ζ runs over all p-th roots of 1. By (2), it follows that $\mu_p = 0$ and that $\lambda_p = \nu_p = 1$, for $p = 37$, 59, and 67.

More generally, suppose that S_0 is cyclic as a $\mathbb{Z}[\Delta]$-module. Equivalently this means that $S_0^{\omega^k}$ is a cyclic group for all k. Nakayama's Lemma then implies that X^{ω^k} is a cyclic Λ-module. We obtain the following result, again using proposition 2.5.

Proposition (3.1) *Suppose that S_0 is cyclic as a $\mathbb{Z}[\Delta]$-module. Then, for any odd integer i, $1 \le i \le p-2$, we have*

$$X^{\omega^i} \cong \Lambda/I,$$

where I is the principal ideal $(f_{X^{\omega^i}}(T))$ of Λ.

The ideal I is called the characteristic ideal of X^{ω^i}. Under the hypotheses of proposition 3.1, Iwasawa proves in [Iw7] that a certain generator $g_i(T)$ of I can be chosen in a completely explicit way, which can be used quite effectively for computation. Write

$$g_i(T) = \sum_{m=0}^{\infty} b_m^{(i)} T^m$$

where $b_m \in \mathbb{Z}_p$ for $m \ge 0$. It is clear (since $g_i(T)$ and $f_{X^{\omega^i}}(T)$ differ by multiplication by an element of $\Lambda^\times$) that $\mu_p^{(i)} = 0$ if and only if $p \nmid b_m^{(i)}$ for some $m \ge 0$. In this case, $\lambda_p^{(i)}$ is equal to the smallest such value of m. The constant term of $g_i(T)$ is given by $b_0^{(i)} = -B_{1,\omega^{-i}}$ where, for any Dirichlet character χ of conductor f, one defines

$$B_{1,\chi} = \frac{1}{f}\sum_{a=1}^{f} \chi(a)a.$$

One thinks of $\chi = \omega^{-i}$ as a Dirichlet character of conductor p by the canonical isomorphism $\Delta \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times$. A congruence argument shows that $p|b_0^{(i)} \Leftrightarrow p|B_j$, where $i + j \equiv 1 \pmod{p-1}$ as before. Therefore, if $p \nmid B_j$, then $g_i(T) \in \Lambda^\times$ and $\lambda_p^{(i)} = \mu_p^{(i)} = v_p^{(i)} = 0$. On the other hand, if $p|B_j$, then either $\lambda_p^{(i)}$ or $\mu_p^{(i)}$ must be positive. If Vandiver's Conjecture (that $p \nmid h_p^+$) is valid for the prime p, then it follows from the Reflection Principle that $S_0^{\omega^i}$ is cyclic for each odd i, and so the hypothesis in proposition 3.1 holds. In [I-S], Iwasawa and Sims find that for all primes $p \leq 4001$ and for all even j $(2 \leq j \leq p-3)$ such that $p|B_j$, the coefficient $b_1^{(i)}$ turns out to be in $\mathbb{Z}_p^\times$. Vandiver's conjecture was known to hold for these primes. Thus $\mu_p^{(i)} = 0$ and $\lambda_p^{(i)} = 1$ (i.e., $X^{\omega^i} \cong \mathbb{Z}_p$) for those pairs (p, i). One also finds that $S_0^{\omega^i} \cong \mathbb{Z}/p\mathbb{Z}$ and $v_p^{(i)} = 1$, both following from the fact that $p^2 \nmid b_0^{(i)}$ for $p \leq 4001$.

Similar computations have been carried out by many others, extending to date up to $p < 8,000,000$. (We refer the reader to [BCEM] and to the references given there.) But so far nothing essentially different has been found. That is, for $p < 8,000,000$, one has: (i) $p \nmid h_p^+$, (ii) $\mu_p = 0$, (iii) $\lambda_p^{(i)} = v_p^{(i)} = 1$ when $p|B_j$, and (iv) S_0 has exponent p. Concerning (ii), Ferrero and Washington succeeded in proving in 1978 that $\mu_p = 0$ for all primes p. Their proof is based on a careful study of the explicit expressions for the $b_m^{(i)}$'s. As for (iii) and (iv), this amounts to verifying that $p \| b_0^{(i)}$ and $p \nmid b_1^{(i)}$ for the pairs (p, i) where $p|B_j$. One then has the equality

$$\lambda_p = \dim_{\mathbb{Z}/p\mathbb{Z}}(S_0) \tag{6}$$

However, it seems reasonable to conjecture (on probabilistic grounds) that $\lambda_p^{(i)} \geq 2$ holds for infinitely many pairs (p, i), i.e., $p|b_0^{(i)}$ and $p|b_1^{(i)}$. But no such pair has yet been found. We have already mentioned that $p|b_0^{(i)}$ if and only if $B_j \equiv 0 \pmod{p\mathbb{Z}_p}$, which is the first congruence in (4). As we will explain later (by using p-adic L-functions), $p|b_1^{(i)}$ if and only if the second congruence in (4) holds. It also seems reasonable to conjecture that $p^2|b_0^{(i)}$ holds for infinitely many pairs (p, i). Assuming that $p \nmid h_p^+$, that would mean that S_0 is not of exponent p.

Suppose now that F is any finite extension of $\mathbb{Q}$. Let p be any prime. We will consider the λ- and μ-invariants associated to the cyclotomic $\mathbb{Z}_p$-extension F_∞/F, which is defined by $F_\infty = F\mathbb{Q}_\infty$. Concerning the μ-invariant, Iwasawa made the following well-known conjecture.

Conjecture (3.2) *Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension. Then $\mu(F_\infty/F)$ is equal to* 0.

We mentioned earlier that $S_\infty = \varinjlim S_n$ has no proper Λ-submodules of finite index. If $\mu(F_\infty/F) = 0$, then it would follow that

$$S_\infty \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda \tag{7}$$

as a $\mathbb{Z}_p$-module, where $\lambda = \lambda(F_\infty/F)$. This is an illustration of an interesting analogy with the theory of algebraic function fields of one variable. Iwasawa discusses this analogy in several places and it seems to have been an important source of motivation from the start. (It is already mentioned in [Iw2].) Suppose that $K = k(x,y)$ is the function field of an absolutely irreducible curve C over a finite field k. Let g be the genus of C. Let $\overline{k}$ denote an algebraic closure of k. Then it is known that the p-primary subgroup of the divisor class group (of degree 0) for $\overline{k}(x,y)$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$, assuming that $p \neq \mathrm{char}(k)$. (One can identify this divisor class group with $J(\overline{k})$, where J denotes the Jacobian of C. If $p = \mathrm{char}(k)$, then the p-primary subgroup is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^a$, where $0 \le a \le g$.) Now K does have a $\mathbb{Z}_p$-extension $K_\infty = k_\infty(x,y)$, where k_∞ denotes the unique subfield of $\overline{k}$ containing k such that $\mathrm{Gal}\,(k_\infty/k) \cong \mathbb{Z}_p$. (Recall that $\mathrm{Gal}\,(\overline{k}/k) \cong \widehat{\mathbb{Z}}$.) The divisor class group (of degree 0) can be identified with $J(k_\infty) = J(\overline{k})^{\mathrm{Gal}\,(\overline{k}/k_\infty)}$. Its p-primary subgroup is easily seen to be divisible and hence isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$, where $0 \le \lambda \le 2g$ (or $0 \le \lambda \le a$ if $p = \mathrm{char}(k)$).

The only general result to date concerning conjecture 3.2 is the following theorem of Ferrero and Washington which we already alluded to above in the special case $F = \mathbb{Q}(\zeta_p)$.

Theorem (3.3) *Assume that $F/\mathbb{Q}$ is abelian and that F_∞/F is the cyclotomic $\mathbb{Z}_p$-extensions. Then $\mu(F_\infty/F) = 0$.*

The proof for $F = \mathbb{Q}(\zeta_p)$ is based on one of the criteria given in [Iw2], together with results about normality of the p-adic expansion of p-adic integers. A rather different proof was discovered by Sinnott [Si]. If q is a prime and $q \neq p$, then, under the same hypotheses as in theorem (3.3), Washington proves in [Wa1] that the number of elements of order q in the ideal class group of F_n is bounded as $n \to \infty$. (The vanishing of $\mu(F_\infty/F)$ is just this same statement when $q = p$.) It is not hard to deduce that the power of q dividing the class number of F_n must then be bounded as $n \to \infty$.

It is interesting to speculate about the behavior of $\lambda(F_\infty/F)$, but quite hard to prove anything of a general nature. The analogy with function fields suggests the following possibility: *if F is a fixed number field, but the prime p is allowed to vary, then $\lambda(F_\infty/F)$ is bounded.* For $F = \mathbb{Q}$, this is certainly true since proposition 2.1 implies that $\lambda(\mathbb{Q}_\infty/\mathbb{Q}) = 0$ for all p. But it has not been verified for any other number field F. The equality (6) suggests the question of how $\lambda(F_\infty/F)$ and $\dim_{\mathbb{Z}/p\mathbb{Z}}(S_0/pS_0)$ might be related. These quantities are certainly not necessarily equal. For example, there are many real quadratic fields F such that $\lambda(F_\infty/F) = 0$, but $S_0 \neq 0$, where p is either 2 or 3. We will mention some examples later. On the other hand, suppose that F is an imaginary quadratic field and that p is an odd prime. Then one has the inequality

$$\lambda(F_\infty/F) \ge \dim_{\mathbb{Z}/p\mathbb{Z}}(S_0/pS_0).$$

This is because $S_0 = S_0^-$, $S_\infty = S_\infty^-$, and the map $S_0^- \to S_\infty^-$ is injective. Since $S_\infty \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda(F_\infty/F)}$, the inequality is obvious. It is often a strict inequality. For example, suppose that $S_0 = 0$ and that p splits in the field F. By proposition 2.2, we have $\lambda(F_\infty/F) \geq 1$. There are infinitely many such primes p. T. Fukuda [Fu] has done extensive and systematic calculations of $\lambda(F_\infty/F)$ when F is imaginary quadratic and p is 3, 5, or 7. It seems reasonable to believe that: *if p is a fixed prime and F varies over all imaginary quadratic fields, then $\lambda(F_\infty/F)$ is unbounded.* For $p = 2$, this is not difficult to prove. For $p \geq 3$, it is an open question. The record to date is due to Fukuda, namely $\lambda = 14$ for $p = 3$. He found three such fields, one of which is $F = \mathbb{Q}(\sqrt{-956238})$ which has class number 3.

The following conjecture was proposed and studied in [Gr1].

Conjecture (3.4) *Assume that F is a totally real number field and that F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension. Then $\lambda(F_\infty/F) = \mu(F_\infty/F) = 0$. That is, the power of p dividing the class number of F_n is bounded as $n \to \infty$.*

According to Leopoldt's conjecture, L_∞/F_∞ should be the only $\mathbb{Z}_p$-extension of F. The above conjecture states that $X = \mathrm{Gal}\,(L_\infty/F_\infty)$ should be finite. In [Gr1], several sufficient conditions for this to be true are proved and a few examples are given where one can verify that X is finite, but nontrivial. (That is, $\lambda = \mu = 0$, but $\nu > 0$.) An expanded version of [Gr1] was published in 1976 [Gr3], including many more examples. Since then this conjecture has been studied by T. Fukuda, K. Komatsu, H. Taya and many others. If F has just one prime lying over p, totally ramified in F_∞/F, then a necessary and sufficient condition for conjecture 3.4 to hold is that $\ker(S_0 \to S_m) = S_0$ for some $m \geq 0$. This is proved in [Gr1, 3], but we will now give a simpler proof using the fact that $X/\omega_n X \cong S_n$ for all n. This isomorphism is equivariant for the action of $\mathrm{Gal}\,(F_n/F)$. By class field theory, the norm map $N_{F_n/F} : S_n \to S_0$ is surjective. Let $\eta_n = \omega_n/\omega_0 \in \Lambda$. The image of η_n in $\Lambda/\omega_n\Lambda = \mathbb{Z}_p[\Gamma/\Gamma_n]$ is just the norm element and so it follows that $Im(S_0 \to S_n) = \eta_n S_n$. If $\ker(S_0 \to S_m) = S_0$, then $\eta_m S_m = 0$ and therefore $\eta_m X \subseteq \omega_m X$. Since $\eta_m | \omega_m$ in Λ, we must have $\eta_m X = \omega_m X$. Letting $Y = \omega_m X$, it follows that $\omega_0 Y = Y$ and Nakayama's lemma then implies that $Y = 0$. Thus, we see that $X \cong S_m$ if $\ker(S_0 \to S_m) = S_0$. For the necessity, we just remark that, for an arbitrary $\mathbb{Z}_p$-extension, S_∞ has no proper Λ-submodules of finite index. If X is finite, then S_∞ would also be finite, and therefore $S_\infty = 0$. It would follow that, for any $n \geq 0$, there exists an $m \geq n$ such that $\ker(S_n \to S_m) = S_n$. An interesting example illustrating the above criterion is $F = \mathbb{Q}(\sqrt{254})$ and $p = 3$. Then $S_0 \cong \mathbb{Z}/3\mathbb{Z}$. In this case, Kurihara, Ichimura-Sumida, and Kraft-Schoof independently found that $\ker(S_0 \to S_m) = S_0$ holds for $m = 5$, but not for $m = 4$. Thus, $X \cong S_5$, which is cyclic of order 3^5. For more on this general topic, we refer the reader to [F-K] and also to [Ic-S], [O-T] and the numerous references which are given there.

Suppose now that F is an arbitrary Galois extension of $\mathbb{Q}$. We suppose also that $F \cap \mathbb{Q}_\infty = \mathbb{Q}$. Then $F_\infty = F\mathbb{Q}_\infty$ is Galois over $\mathbb{Q}$ and $\mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \Delta \times \Gamma$, where $\Delta = \mathrm{Gal}(F_\infty/\mathbb{Q}_\infty)$ can be identified with $\mathrm{Gal}(F/\mathbb{Q})$. Let χ be the character of an irreducible representation of Δ over $\overline{\mathbb{Q}}_p$, with underlying representation space V_χ. Let $d_\chi = \dim_{\overline{\mathbb{Q}}_p}(V_\chi)$. Let $X = \mathrm{Gal}(L_\infty/F_\infty)$ as before. Then $V_F = X \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$ is a finite-dimensional representation space for Δ over $\overline{\mathbb{Q}}_p$. Its dimension is $\lambda(F_\infty/F)$. We define λ_χ to be the multiplicity of V_χ in V_F. That is, $\lambda_\chi = \dim_{\overline{\mathbb{Q}}_p}(\mathrm{Hom}_\Delta(V_F, V_\chi))$. Then we have

$$\lambda(F_\infty/F) = \sum_\chi d_\chi \lambda_\chi,$$

where χ runs over all irreducible characters of Δ. (Note that in defining each λ_χ, one can assume that χ is faithful, changing F if necessary.) Now we can write $d_\chi = d_\chi^+ + d_\chi^-$, where $d_\chi^\pm$ denote the dimensions of the (± 1)-eigenspaces for the action of a complex conjugation $\delta_0 \in \Delta$. (One fixes an embedding of F into $\mathbb{C}$ to define δ_0. The dimensions $d_\chi^\pm$ are independent of this choice.) If $d_\chi = d_\chi^+$, then one can assume that F is totally real. Conjecture 3.4 then implies that $\lambda_\chi = 0$ for all such χ. If $d_\chi = d_\chi^-$, then one can assume that F is a totally complex quadratic extension of a totally real number field F^+. (That is, F is a so-called CM field.) In this case, λ_χ is often nonzero. As we will mention later, the value of λ_χ is related to the number of zeros of a p-adic Artin L-function which can be associated to χ. The simplest case is when F is an imaginary quadratic field (i.e. $F^+ = \mathbb{Q}$ and χ is an odd Dirichlet character of order 2). Then $\lambda_\chi = \lambda_F$.

The "mixed" case (where d_χ^+ and d_χ^- are both positive) seems quite mysterious. Virtually nothing is known. One can use proposition 2.2 to give examples where λ_χ is nonzero. To explain this, note that $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ acts on $\mathrm{Gal}(\widetilde{F}/F)$ by inner automorphisms and so $\mathrm{Gal}(\widetilde{F}/F) \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$ becomes a representation space for Δ. One can verify that V_χ occurs in this representation space with multiplicity at least d_χ^-. (That's the exact multiplicity if Leopoldt's conjecture is valid for F and p.) If p splits completely in $F/\mathbb{Q}$, the proof of proposition 2.2 then shows that $\lambda_\chi \geq d_\chi^-$. More generally, let $\Delta_\mathfrak{p}$ denote the decomposition subgroup of Δ corresponding to a prime $\mathfrak{p}$ of F lying over p. Then one can show that

$$\lambda_\chi \geq \max(\dim_{\overline{\mathbb{Q}}_p}(V_\chi^{\Delta_\mathfrak{p}}) - d_\chi^+, \quad 0).$$

It would be interesting to find examples where this inequality is strict. Are there such examples if one requires that $p \nmid [F:\mathbb{Q}]$?

Consider the case where F is a totally complex field and $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ is dihedral of order $2m$, where m is odd. If $m > 1$, any faithful irreducible representation of Δ is 2-dimensional and of mixed type. Also F contains a unique imaginary quadratic subfield K. If $\widetilde{K}$ denotes the compositum of all $\mathbb{Z}_p$-extensions of K, then $\mathrm{Gal}(\widetilde{K}/K) \cong \mathbb{Z}_p^2$. Considering the action of

$\mathrm{Gal}(K/\mathbb{Q})$ on this group, one can find a unique $\mathbb{Z}_p$-extension K_∞^{ac}/K such that $K_\infty^{ac}/\mathbb{Q}$ is Galois and the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ acts by -1 on $\mathrm{Gal}(K_\infty^{ac}/K)$. One often refers to K_∞^{ac} as the "anti-cyclotomic" $\mathbb{Z}_p$-extension of K. Assume that p is a fixed odd prime and that K is also fixed. For any positive n, let $F = K_n^{ac}$, the n-th level in the $\mathbb{Z}_p$-extension K_∞^{ac}/K. Then $F \cap \mathbb{Q}_\infty = \mathbb{Q}$ and $\mathrm{Gal}(F/\mathbb{Q})$ is dihedral of order $2p^n$. It seems reasonable to believe that $\lambda_\chi = 0$ if χ is a faithful character of $\mathrm{Gal}(F/\mathbb{Q})$ and $n \gg 0$. Equivalently, this means that $\lambda(K_n^{ac}\mathbb{Q}_\infty/K_n^{ac})$ is bounded as $n \to \infty$. There is another interesting interpretation. Let $K_\infty^c = K\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of K. Then $\widetilde{K} = K_\infty^{ac}K_\infty^c$ and $\mathrm{Gal}(\widetilde{K}/K) = \Gamma^- \times \Gamma^+$, reflecting the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{Gal}(\widetilde{K}/K)$. Here $\Gamma^- = \mathrm{Gal}(\widetilde{K}/K_\infty^c)$, $\Gamma^+ = \mathrm{Gal}(\widetilde{K}/K_\infty^{ac})$. Let $\widetilde{L}$ denote the maximal, abelian, unramified, pro-p extension of $\widetilde{K}$ (or, more briefly, the pro-p Hilbert class field of $\widetilde{K}$). Let $\widetilde{X} = \mathrm{Gal}(\widetilde{L}/\widetilde{K})$, which can be viewed as a module over the ring $\widetilde{\Lambda} = \mathbb{Z}_p[[\mathrm{Gal}(\widetilde{K}/K)]]$. This ring can be identified with a formal power series ring over $\mathbb{Z}_p$ in two variables. It is known that $\widetilde{X}$ is a finitely generated, torsion $\widetilde{\Lambda}$-module. It might in fact be pseudo-null, which means that it has two relatively prime annihilators in $\widetilde{\Lambda}$ (which is a UFD). (Note: The finitely generated pseudo-null modules over $\Lambda = \mathbb{Z}_p[[T]]$ are simply the finite Λ-modules. But over $\widetilde{\Lambda} = \mathbb{Z}_p[[T_1, T_2]]$, pseudo-null modules can be infinite.) Now we have the following equivalence:

$$\lambda_\chi = 0 \textit{ for all } n \gg 0 \Longleftrightarrow \widetilde{X} \textit{ is a pseudo-null } \widetilde{\Lambda}\textit{-module.}$$

We will just sketch the reason for this. As a module over $\Lambda^- = \mathbb{Z}_p[[\Gamma^-]]$, one can show that $\widetilde{X}$ is still finitely generated. (The crucial ingredient is to show that $\widetilde{X}/(\gamma_0^- - 1)\widetilde{X}$ is finitely generated as a $\mathbb{Z}_p$-module, where γ_0^- is a topological generator of Γ^-. This follows from the fact that $\mu(K_\infty^c/K) = 0$.) Let $\omega_n^- = (\gamma_0^-)^{p^n} - 1$. Now $K_n^-\mathbb{Q}_\infty = \widetilde{K}^{\Gamma_n^-}$ and one can show that $\lambda(K_n^-\mathbb{Q}_\infty/K_n^-) = \mathrm{rank}_{\mathbb{Z}_p}(\widetilde{X}/\omega_n^-\widetilde{X}) + O(1)$ as $n \to \infty$. But it is easy to see that $\mathrm{rank}_{\mathbb{Z}_p}(\widetilde{X}/\omega_n^-\widetilde{X})$ is bounded if and only if $\mathrm{rank}_{\Lambda^-}(\widetilde{X}) = 0$, and that this will be true precisely when $\widetilde{X}$ is pseudo-null as a $\widetilde{\Lambda}$-module.

For several different reasons, including the remarks in the previous paragraph, we have been tempted to make the following conjecture.

Conjecture (3.5) *Suppose that F is any number field and that p is any prime. Let $\widetilde{F}$ denote the compositum of all $\mathbb{Z}_p$-extensions of F. Let $\widetilde{L}$ denote the pro-p Hilbert class field of $\widetilde{F}$ and let $\widetilde{X} = \mathrm{Gal}(\widetilde{L}/\widetilde{F})$, regarded as a module over the ring $\widetilde{\Lambda} = \mathbb{Z}_p[[\mathrm{Gal}(\widetilde{F}/F)]]$. Then $\widetilde{X}$ is a pseudo-null $\widetilde{\Lambda}$-module.*

We refer to [L-N] for some equivalent versions of this conjecture and some additional references.

4. In *On some modules in the theory of cyclotomic fields* (published in 1964), two versions of what would later be known as Iwasawa's "Main Conjecture" are proven under a certain hypothesis. This paper concentrates on the case $F = \mathbb{Q}(\zeta_p)$, $F_\infty = \mathbb{Q}(\zeta_p, \zeta_{p^2}, \dots)$. The hypothesis that he makes is the following.

Cyclicity Hypothesis: S_0 *is a cyclic* $\mathbb{Z}[\Delta]$*-module.*

Under this same hypothesis, one version of the Main Conjecture is already proven (in essence) in the earlier paper *A class number formula for cyclotomic fields*. We will discuss this first. Under the cyclicity hypothesis, it follows that S_n is cyclic as a module for $\mathbb{Z}_p[\mathrm{Gal}\,(F_n/\mathbb{Q})]$ for any $n \geq 0$, and then Iwasawa proves that, for any odd i, $3 \leq i \leq p-2$, one has

$$S_n^{\omega^i} \cong \mathbb{Z}_p[\mathrm{Gal}\,(F_n/F)]/(\theta_n^{(i)}), \ \textit{where}\ \theta_n^{(i)} = -\frac{1}{p^{n+1}} \sum_{a=1}^{p^{n+1}} a\omega^{-i}(a)\langle\sigma_a\rangle^{-1} \quad (8)$$

Here $\sigma_a \in \mathrm{Gal}\,(F_n/\mathbb{Q})$ is determined by $\sigma_a(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}^a$, $\langle\sigma_a\rangle$ is the projection of σ_a to $\mathrm{Gal}\,(F_n/F)$ in the decomposition $\mathrm{Gal}\,(F_n/\mathbb{Q}) = \Delta \times \mathrm{Gal}\,(F_n/F)$, and $\omega^{-i}(\sigma_a)$ is determined by the projection of σ_a to Δ, regarding ω^{-i} as a character of that group. It is not hard to verify that $\theta_n^{(i)} \in \mathbb{Z}_p[\mathrm{Gal}\,(F_n/F)]$. (For $i=1$, this isn't true, but it is shown that $S_n^{\omega^1} = 0$.) The fact that $\theta_n^{(i)}$ annihilates $S_n^{\omega^i}$ is a consequence of Stickelberger's Theorem.

A crucial observation is that $\theta_m^{(i)}$ is mapped to $\theta_n^{(i)}$ under the $\mathbb{Z}_p$-algebra homomorphism $\mathbb{Z}_p[\mathrm{Gal}\,(F_m/F)] \to \mathbb{Z}_p[\mathrm{Gal}\,(F_n/F)]$ for $m \geq n \geq 0$. We let $\theta^{(i)} = \varprojlim \theta_n^{(i)} \in \Lambda = \mathbb{Z}_p[[\Gamma]]$. Iwasawa proves the following result in [Iw7].

Theorem (4.1) *Suppose that the cyclicity hypothesis holds. Let i be odd, $3 \leq i \leq p-2$. Then $X^{\omega^i} \cong \Lambda/(\theta^{(i)})$ as a Λ-module.*

Here is a sketch of the proof. If one identifies Λ with $\mathbb{Z}_p[[T]]$ as before, then $\theta^{(i)}$ is identified with a power series $g_i(T)$. This is the power series which we referred to in section 3. Note that $g_i(0) = b_0^{(i)} = -B_{1,\omega^{-i}}$. Now proposition 3.1 asserts that $X^{\omega^i} \cong \Lambda/I$, where I is the principal ideal generated by $f_i(T) = f_{X^{\omega^i}}(T)$. Stickelberger's Theorem implies that $\theta^{(i)}$ annihilates $X^{\omega^i} \cong \varprojlim S_n^{\omega^i}$. This means that $g_i(T) \in I$. That is,

$$f_i(T) | g_i(T) \quad (9)$$

in the ring Λ. Using (1) and (2) for $n=0$, it follows that $f_i(0) \approx |S_0^{\omega^i}|$. Using (8) for $n=0$, one has $S_0^{\omega^i} \cong \mathbb{Z}_p/B_{1,\omega^{-i}}\mathbb{Z}_p$ and so $g_i(0) \approx |S_0^{\omega^i}|$ too. It then follows from (9) that $g_i(T)/f_i(T) \in \Lambda^\times$, which implies theorem 4.1.

Without the cyclicity hypothesis, there seems to be no simple way to prove the divisibility (9). However, Iwasawa later (in Chapter 7 of [Iw10]) proves the following proposition by using the formulas for the first factor of the class number of the fields F_n for $n \geq 0$. Let $\lambda_{p,\mathrm{anal}}^{(i)}$ and $\mu_{p,\mathrm{anal}}^{(i)}$ denote the

λ- and μ-invariants for $\Lambda/(g_i(T))$, which can be easily described in terms of the coefficients $b_m^{(i)}$ of $g_i(T)$. Let $\lambda_{p,\mathrm{alg}}^{(i)}$ and $\mu_{p,\mathrm{alg}}^{(i)}$ be the λ- and μ-invariants of X^{ω^i}, which we previously denoted more simply by $\lambda_p^{(i)}$ and $\mu_p^{(i)}$.

Proposition (4.2) *For any odd prime p, we have the following equalities:*

$$\sum_{\substack{i=3\\ i \text{ odd}}}^{p-1} \lambda_{p,\mathrm{alg}}^{(i)} = \sum_{\substack{i=3\\ i \text{ odd}}}^{p-2} \lambda_{p,\mathrm{anal}}^{(i)} \qquad \textit{and} \qquad \sum_{\substack{i=3\\ i \text{ odd}}}^{p-2} \mu_{p,\mathrm{alg}}^{(i)} = \sum_{\substack{i=3\\ i \text{ odd}}}^{p-2} \mu_{p,\mathrm{anal}}^{(i)}.$$

Thus, if we somehow know that (9) holds for all odd i, $3 \le i \le p-2$, then it would still follow that the ideals $(f_i(T))$ and $(g_i(T))$ are equal. This is of course weaker than theorem 4.1 in that one does not obtain the precise structure of X^{ω^i}. On the other hand, if one could prove the divisibility $g_i(T)|f_i(T)$ for all these i's, then one would again obtain $(f_i(T)) = (g_i(T))$. In 1981, Mazur and Wiles succeeded in proving this divisibility, as we will discuss below.

Several years later Iwasawa discovered that the power series $g_i(T)$ is intimately connected to the p-adic L-function $L_p(s, \omega^j)$ which was constructed by Kubota and Leopoldt in [K-L] (also published in 1964). Here i and j are related as before: $i + j \equiv 1 \pmod{p-1}$ and p is an odd prime. This p-adic L-function can be characterized as the unique continuous function from $\mathbb{Z}_p$ to $\mathbb{Q}_p$ such that

$$L_p(1-m, \omega^j) = (1 - p^{m-1})\zeta(1-m)$$

for all $m \ge 1$ with $m \equiv j \pmod{p-1}$. Here $\zeta(z)$ denotes the Riemann zeta function. It is known that $\zeta(1-m) = -B_m/m$ for all $m \ge 1$, where B_m denotes the m-th Bernoulli number. Kubota and Leopoldt prove that $L_p(s, \omega^j)$ is actually analytic for all $s \in \mathbb{Z}_p$, except for a simple pole at $s = 1$ when $j = 0$ (which corresponds to $i = 1$). They also give the values $L_p(1-m, \omega^j)$ for all $m \ge 1$, and in particular one has $L_p(0, \omega^j) = -B_{1,\omega^{-i}}$.

We will state Iwasawa's result in terms of $\theta^{(i)}$. We assume that $i \ne 1$, and hence $j \ne 0$. Let $\kappa : \Gamma \to 1 + p\mathbb{Z}_p$ be the isomorphism giving the action of Γ on μ_{p^∞}. That is, $\kappa = \chi|_\Gamma$, where χ is the usual cyclotomic character. For any $s \in \mathbb{Z}_p$, we have a continuous homomorphism $\kappa^s : \Gamma \to 1 + p\mathbb{Z}_p$ defined by $\kappa^s(\gamma) = \kappa(\gamma)^s$ for $\gamma \in \Gamma$. One can extend κ^s to a continuous $\mathbb{Z}_p$-algebra homomorphism φ_s: $\Lambda \to \mathbb{Z}_p$. (If one identifies Λ with $\mathbb{Z}_p[[T]]$ by setting $T = \gamma_0 - 1$, then φ_s can be defined as follows: $\varphi_s(g(T)) = g(\kappa(\gamma_0)^s - 1)$ for any $g(T) \in \Lambda$.) Iwasawa proves the following result in [Iw9].

Theorem (4.3) *Suppose that j is an even integer, $2 \le j \le p-3$. Then $L_p(s, \omega^j) = \varphi_s(\theta^{(i)})$ for all $s \in \mathbb{Z}_p$. Equivalently, $g_i(T)$ satisfies the following interpolation property: $g_i(\kappa(\gamma_0)^{1-m} - 1) = -(1 - p^{m-1})B_m/m$ for all $m \ge 1$ such that $m \equiv j \pmod{p-1}$.*

A nonzero element of Λ has only finitely many zeros and so the above interpolation property determines $g_i(T)$ uniquely. The Kubota-Leopoldt p-adic L-function $L_p(s,\omega^j)$ is obtained from $g_i(T)$ by the substitution $T=\kappa(\gamma_0)^s-1$.

This may be a good place to discuss the congruences in (4) again. Writing $g_i(T)=\sum_{n=0}^{\infty} b_n^{(i)}T^n$ as before, it is clear that

$$g_i(t)\equiv g_i(0)=b_0^{(i)} \pmod{p\mathbb{Z}_p}$$

for all $t\in p\mathbb{Z}_p$. It follows that $B_m/m\equiv -b_0^{(i)} \pmod{p\mathbb{Z}_p}$ for all $m\equiv j \pmod{p-1}$, taking $t=\kappa(\gamma_0)^{1-m}-1$, and so we have

$$B_j\equiv 0 \pmod{p\mathbb{Z}_p} \Longleftrightarrow p|b_0^{(i)}. \tag{10}$$

Here, as before, i and j are related by $i+j\equiv 1 \pmod{p-1}$, $2\le i,j\le p-2$ with i odd, j even. (Thus, $\omega^i\omega^j=\omega$, where ω^i is an odd character, ω^j is an even character.) On the other hand, if $t_1,t_2\in p\mathbb{Z}_p$, then

$$g_i(t_1)-g_i(t_2)\equiv b_1^{(i)}(t_1-t_2) \pmod{p^2\mathbb{Z}_p}.$$

It follows that if $B_{j'}/j'\equiv B_j/j \pmod{p^2\mathbb{Z}_p}$ for some $j'\equiv j \pmod{p-1}$ where $j',j\ge 4$ and $j'\not\equiv j \pmod{p}$, then $p|b_1^{(i)}$. Conversely, if $p|b_1^{(i)}$, then $g_i(t)\equiv g_i(0) \pmod{p^2\mathbb{Z}_p}$ for all $t\in p\mathbb{Z}_p$. Thus, we have

$$\frac{B_{j+p-1}}{j+p-1}\equiv\frac{B_j}{j} \pmod{p^2\mathbb{Z}_p} \Longleftrightarrow p|b_1^{(i)}$$

provided that $j\ge 4$. In summary, the two congruences in (4) hold if and only if $\lambda_{p,\mathrm{anal}}^{(i)}\ge 2$ (since we know that $\mu_{p,\mathrm{anal}}^{(i)}=0$). As we have mentioned, this does not happen for $p<8,000,000$.

The first version of Iwasawa's Main Conjecture can be stated as follows. For each odd i, $3\le i\le p-3$, let $f_i(T)$ be the characteristic polynomial for the Λ-module X^{ω^i}. Let $g_i(T)$ be the power series which is characterized by the interpolation property in theorem 4.3. (It is related to $L_p(s,\omega^j)$ by a simple change of variable.)

Conjecture (4.4) *The ideals $(f_i(T))$ and $(g_i(T))$ of Λ are equal.*

As Iwasawa discusses in another article [Iw8], one can view this conjectural relationship between $f_i(T)$ and $g_i(T)$ (which Iwasawa proved under the cyclicity hypothesis) as another aspect of the analogy between algebraic function fields and algebraic number fields mentioned earlier. There is an important theorem of Weil which states that the zeta function of a curve C over a finite field k is closely related to the action of the Frobenius automorphism in $\mathrm{Gal}(\overline{k}/k)$ on the p-power torsion points of the Jacobian variety for C, where p is any prime such that $p\neq\mathrm{char}(k)$. The analogy arises from the fact that $g_i(T)$ is related to values of the Riemann zeta function $\zeta(z)$ by an interpolation property. This analogy can in fact be made quite precise.

Theorem 2.6 shows that conjecture (4.4) can be formulated in the following equivalent form.

Conjecture (4.5) *The characteristic ideal $(f_{Y^{\omega^j}}(T))$ for the Λ-module Y^{ω^j} can be generated by $\dot{g}_i(T) = g_i(\kappa(\gamma_0)(1+T)^{-1} - 1)$.*

Later we will point out that the power series $\dot{g}_i(T)$ can also be characterized by a nice interpolation property. We want to discuss a third version of conjecture (4.4), which Iwasawa also proves is equivalent. We first observe that there is a natural factorization of the polynomial $f_{Y^{\omega^j}}(T)$. Recall that $F_\infty \subset L_\infty \subset M_\infty$ and one therefore has an exact sequence

$$0 \to Z^{\omega^j} \to Y^{\omega^j} \to X^{\omega^j} \to 0 \qquad (11)$$

of finitely generated, torsion Λ-modules. (Torsion because j is even.) Here $Z = \mathrm{Gal}(M_\infty/L_\infty)$. It follows that

$$f_{Y^{\omega^j}}(T) = f_{X^{\omega^j}}(T) f_{Z^{\omega^j}}(T). \qquad (12)$$

Iwasawa proves that $\dot{g}_i(T)$ has a factorization parallel to (12). If $n \geq 0$, let U_n denote the group of units in the completion $(F_n)_{\mathfrak{p}_n}$, where $\mathfrak{p}_n$ is the unique prime of F_n above p. Let E_n and C_n denote the group of units and the subgroup of cyclotomic units for the field F_n. Let $\overline{E}_n$ and $\overline{C}_n$ denote the closures of E_n and C_n respectively in the topological group U_n. Let $\mathfrak{Y} = \varprojlim U_n/\overline{C}_n$, where the maps defining the inverse limit are induced by the norm maps $N_{m,n} : U_m \to U_n$ for $m \geq n$. Note that $N_{m,n}(\overline{C}_m) \subseteq \overline{C}_n$ (in fact, equal) and $N_{m,n}(\overline{E}_m) \subseteq \overline{E}_n$. Also, note that $U_n/\overline{C}_n$ is a $\mathbb{Z}_p$-module since all nonzero residue classes modulo $\mathfrak{p}_n$ have representatives in C_n. (The residue field is just $\mathbb{F}_p$.) Let $\mathfrak{X} = \varprojlim \overline{E}_n/\overline{C}_n$ and $\mathfrak{Z} = \varprojlim U_n/\overline{E}_n$. Then Iwasawa shows that one has an exact sequence

$$0 \to \mathfrak{X}^{\omega^j} \to \mathfrak{Y}^{\omega^j} \to \mathfrak{Z}^{\omega^j} \to 0 \qquad (13)$$

of finitely generated, torsion Λ-modules and furthermore one has the following theorem.

Theorem (4.6) *For even j, $2 \leq j \leq p-3$, there is a Λ-isomorphism*

$$\mathfrak{Y}^{\omega^j} \cong \Lambda/(\dot{g}_i(T)),$$

where $i + j \equiv 1 \pmod{p-1}$.

Consequently, one does have a natural factorization of $\dot{g}_i(T)$, namely

$$\dot{g}_i(T) = f_{\mathfrak{X}^{\omega^j}}(T) f_{\mathfrak{Z}^{\omega^j}}(T) u(T), \qquad (14)$$

where $u(T) \in \Lambda^\times$.

Iwasawa also proves that $\mathfrak{Z}^{\omega^j} \cong Z^{\omega^j}$ as Λ-modules, the isomorphism coming from class field theory: one identifies $\varprojlim U_n/\overline{E}_n$ with the inertia subgroup for p in $\mathrm{Gal}(M_\infty/F_\infty)$, which of course coincides with $\mathrm{Gal}(M_\infty/L_\infty)$. Comparing (12) and (14), one is then led to a third equivalent formulation of conjecture 4.4.

Conjecture (4.7) *For even j, $2 \le j \le p-3$, the characteristic ideals of X^{ω^j} and $\mathfrak{X}^{\omega^j}$ are equal.*

We should mention that, under the assumption of Vandiver's conjecture, one has $X^{\omega^j} = 0$. But Iwasawa shows that $\mathfrak{X}^{\omega^j}/T\mathfrak{X}^{\omega^j} \cong \overline{E}_0^{\omega^j}/\overline{C}_0^{\omega^j}$, which is also trivial. It would follow that $\mathfrak{X}^{\omega^j} = 0$ too. Thus, conjecture 4.7 is then obvious and conjecture 4.4 holds. One could also deduce theorem 4.1 again.

These conjectures can be formulated in a more general setting. Let F be a finite, abelian extension of $\mathbb{Q}$. For simplicity of exposition, we will assume that p is an odd prime, that $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ has exponent dividing $p-1$ (so that irreducible characters of Δ will have values in $\mathbb{Z}_p^\times$), and that F contains a primitive p-th root of unity. These assumptions are not at all essential. Let χ and ψ be two irreducible characters of Δ such that $\chi\psi = \omega$ and χ is odd (so that ψ is even). Let $F_\infty = F\mathbb{Q}_\infty$ and let $X = \mathrm{Gal}(L_\infty/F_\infty)$, $Y = \mathrm{Gal}(M_\infty/F_\infty)$ where L_∞, M_∞ are defined as before. We can define X^χ and Y^ψ which turn out to be related just as in proposition 2.6 (which is the special case $\chi = \omega^i, \psi = \omega^j$). Propositions 2.3–2.5 are also true. There is also a p-adic L-function $L_p(s,\psi)$ defined by a certain interpolation property and which corresponds to a power series $g_\chi(T) \in \Lambda$. (We use χ as a subscript to be closer to the previous notation $g_i(T)$ corresponding to $\chi = \omega^i$.) One can easily state the analogues of conjectures 4.4, 4.5, and 4.7, which again turn out to be equivalent. We refer the reader to [Co2] or [Gr2] for more details. In this generality, the conjectures were proved by Mazur and Wiles in [M-W1]. We should mention that Iwasawa's arguments work quite well (and describe X^χ or Y^ψ up to pseudoisomorphism) if one makes a certain hypothesis which is slightly weaker than the cyclicity hypothesis (which is false in general). We will state it in a form which makes sense whenever $F/\mathbb{Q}$ is Galois and $F_\infty = F\mathbb{Q}_\infty$. Then $F_\infty/\mathbb{Q}$ is Galois. We can define $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$ as $\varprojlim \mathbb{Z}_p[\mathrm{Gal}(F_n/\mathbb{Q})]$.

Pseudo-cyclicity Hypothesis. *There is a cyclic $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$-submodule Z of $X = \mathrm{Gal}(L_\infty/F_\infty)$ such that X/Z is finite.*

We do not know of any examples where this hypothesis fails to be true. If $F/\mathbb{Q}$ is abelian, then conjecture 3.4 (applied to the maximal real subfield of $F(\zeta_p)$) would imply the pseudo-cyclicity hypothesis. (See [Gr3].) It also would be true if we somehow knew that all the roots of $g_\chi(T)$ were simple for all odd characters χ of $\Delta = \mathrm{Gal}(F(\zeta_p)/\mathbb{Q})$, an assertion which is quite likely to be valid.

Even more generally, one can formulate the analogues of conjectures 4.4 or 4.5 for abelian characters χ or ψ of any totally real number field K under the assumption that χ is totally odd or ψ is totally even. If $\chi\psi = \omega_K$, where $\omega_K = \omega|_{G_K}$, then the two conjectures are again equivalent, as one shows by using the Reflection Principle. The p-adic L-functions $L_p(s, \psi)$, which satisfy an interpolation property involving the numbers $L(1-m, \psi\omega_K^{-m})$ for $m \geq 1$, were constructed by Deligne and Ribet using Hilbert modular forms for K and independently by D. Barsky and by P. Cassou-Noguès using explicit formulas of Shintani. In this generality, Wiles succeeded in proving these "Main Conjectures" in 1988. The proof appeared in [Wi2]. The approach uses 2-dimensional p-adic representations associated to Hilbert modular forms for K. As a consequence of this result of Wiles, an analogous main conjecture for p-adic Artin L-functions can be deduced. These functions are associated to representations of $\mathrm{Gal}\,(F/\mathbb{Q})$, where F is any finite, totally real, Galois extension of $\mathbb{Q}$, and can be characterized by an interpolation property involving values of the corresponding complex Artin L-function. The invariant λ_χ discussed in section 3 (for an irreducible χ which is not of "mixed" type) then has an "analytic" interpretation as the number of zeros of a certain p-adic Artin L-function.

Iwasawa gave a course at Princeton University during the academic year 1968–69 in which he explained many of the ideas that have been mentioned so far. That course was my first introduction to the subject. Iwasawa's lectures were beautiful, and usually given without consulting any notes. I recall that the notes that I took of his lectures were quite in demand and circulated for many years afterwards. The results in the course were proved in complete generality and eventually became incorporated in Iwasawa's 1973 paper *On $\mathbb{Z}_l$-extensions of algebraic number fields.* The course and this paper included the study of a skew-symmetric pairing which was inspired by the analogy with algebraic function fields and the Weil pairing.

5. Barry Mazur gave a series of lectures in Paris during the Spring of 1970, where he developed a theory aimed at proving the following kind of result.

Conjecture (5.1) *Suppose that A is an abelian variety defined over a number field F. Assume that p is a prime such that A has good, ordinary reduction at all primes of F lying above p. Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension. Then $A(F_\infty)$ is finitely generated.*

The details of his theory were published in [Maz1]. One case in which Mazur succeeded in proving this conjecture is under the following assumption:

$$A(F) \text{ and } Ш_A(F)_p \text{ are both finite.} \tag{15}$$

Here $Ш_A(F)_p$ denotes the p-primary subgroup of the Tate-Shafarevich group for A over F. We will formulate several of Mazur's results and conjectures in terms of the classical Selmer group, although he uses a certain variation of this group. Recall that if K is any algebraic extension of F, then the p-primary subgroup $\mathrm{Sel}_A(K)_p$ of the Selmer group fits into an exact sequence

$$0 \to A(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Sel}_A(K)_p \to Ш_A(K)_p \to 0.$$

Thus (15) means that $\mathrm{Sel}_A(F)_p$ is finite.

One of the main results of [Maz1] is the following.

Theorem (5.2) *Assume that A/F has good, ordinary reduction at all primes of F lying over p. Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension. Then the kernel and cokernel of the natural maps*

$$\mathrm{Sel}_A(F_n)_p \to \mathrm{Sel}_A(F_\infty)_p^{\mathrm{Gal}\,(F_\infty/F_n)}$$

are finite and have bounded order as $n \to \infty$.

This is often referred to as Mazur's "Control Theorem" and is valid for any $\mathbb{Z}_p$-extension F_∞/F. Now assume that $\mathrm{Sel}_A(F)_p$ is finite. $\mathrm{Sel}_A(F_\infty)_p$ is a discrete, p-primary group on which $\Gamma = \mathrm{Gal}\,(F_\infty/F)$ acts. We can regard $\mathrm{Sel}_A(F_\infty)_p$ as a discrete Λ-module and its Pontryagin dual $X_A(F_\infty)$ as a compact Λ-module. Since we are assuming that $\mathrm{Sel}_A(F)_p$ is finite, theorem 5.2 implies that $X_A(F_\infty)/TX_A(F_\infty)$ is finite. Thus $X_A(F_\infty)$ is a finitely generated, torsion Λ-module. The classification theorem then implies that $X_A(F_\infty)$ has finite $\mathbb{Z}_p$-corank, which we denote by $\lambda_A(F_\infty/F)$. Therefore, the maximal divisible subgroup $(\mathrm{Sel}_A(F_\infty)_p)_{\mathrm{div}}$ of $\mathrm{Sel}_A(F_\infty)_p$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_A(F_\infty/F)}$ from which it follows that $A(F_\infty)\otimes(\mathbb{Q}_p/\mathbb{Z}_p) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ where $0 \le r \le \lambda_A(F_\infty/F)$. On the other hand, if F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension, then it is known that $A(F_\infty)_{\mathrm{tors}}$ is finite. Mazur proves this in [Maz1] under certain hypotheses. By a simple argument given in Mazur's paper, it then follows that $A(F_\infty)$ is indeed a finitely generated group, provided that (15) holds.

More generally, the same conclusion (i.e., conjecture 5.1) follows from the following conjecture.

Conjecture (5.3) *Under the same assumptions as in conjecture 5.1, the Λ-module be $X_A(F_\infty) = \widehat{\mathrm{Sel}_A(F_\infty)_p}$ is finitely generated and torsion.*

We would then say that $\mathrm{Sel}_A(F_\infty)_p$ is cofinitely generated and cotorsion as a Λ-module. In fact, for any $\mathbb{Z}_p$-extension F_∞/F and for any abelian variety A (with no restriction on the reduction-type at p), $\mathrm{Sel}_A(F_\infty)_p$ is always a cofinitely generated Λ-module, but can fail to be Λ-cotorsion. For example, let F be an imaginary quadratic field. Let A be an elliptic curve/$\mathbb{Q}$. Suppose that F_∞ is the anti-cyclotomic $\mathbb{Z}_p$-extension of F. Then it often happens that $\mathrm{rank}_{\mathbb{Z}}(A(F_n))$ is unbounded as $n \to \infty$. This interesting phenomenon is discussed in [Maz2]. In such a case, it is clear that $\mathrm{Sel}_A(F_\infty)_p$ cannot be Λ-cotorsion.

Mazur also states a Main Conjecture somewhat analogous to conjecture 4.4 or 4.5. It is for the case where A is an elliptic curve $E/\mathbb{Q}$ which is modular and where F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of a subfield F of $\mathbb{Q}(\zeta_p)$. The prime p is assumed to be odd and such that E has good, ordinary reduction at p. For simplicity, we will discuss $F = \mathbb{Q}$. For such a prime p, Mazur and Swinnerton-Dyer constructed a p-adic L-function $L_p(s, E)$ in [M-SwD]. If $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ and $\Lambda = \mathbb{Z}_p[[\Gamma]]$, then $L_p(s, E) = \varphi_{s-1}(\theta_E)$ for all $s \in \mathbb{Z}_p$, where θ_E is an element of $\frac{1}{p^t}\Lambda$ for some $t \geq 0$. Here $\varphi_s : \Lambda \to \mathbb{Z}_p$ is just as in theorem 4.3. The element θ_E is characterized by a certain interpolation property involving the values at $z = 1$ of the twisted Hasse-Weil L-series $L(z, E, \rho)$ for $E/\mathbb{Q}$, where ρ varies over all Dirichlet characters of p-power order and conductor. (They can be regarded as characters of Γ.) It is now known under very mild assumptions that $\theta_E \in \Lambda$. This should be true in general. One important idea in [M-SwD] is that θ_E can be identified with a $\mathbb{Q}_p$-valued measure on the Galois group Γ. The measure of any open subset of Γ is in $\frac{1}{p^t}\mathbb{Z}_p$, and presumably should be in $\mathbb{Z}_p$ itself. If μ_E is this measure, then

$$L_p(s, E) = \int_\Gamma \kappa^{s-1} d\mu_E$$

where κ^{s-1} is viewed as a function on Γ.

Mazur's Main Conjecture is the following statement.

Conjecture (5.4) *The characteristic ideal of $X_E(\mathbb{Q}_\infty) = \mathrm{Sel}_E(\mathbb{Q}_\infty)\widehat{\ }_p$ is generated by θ_E.*

Even without assuming conjecture 5.3, this conjecture makes sense. It could be interpreted as asserting that $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ is Λ-cotorsion if and only if $\theta_E \neq 0$. It is now known that indeed $\theta_E \neq 0$, a consequence of a theorem of Rohrlich [Ro] which states that $L(1, E, \rho) \neq 0$ for all but finitely many characters ρ of Γ. Just to give a simple illustration of how conjecture 5.4 can be applied, we will mention one corollary, namely the following piece of the Birch and Swinnerton-Dyer conjecture:

$$L(1, E) \neq 0 \iff E(Q) \textit{ and } \text{Ш}_E(\mathbb{Q})_p \textit{ are both finite.} \tag{16}$$

This would follow because the interpolation property implies that

$$L(1, E) \neq 0 \iff L_p(1, E) \neq 0 \iff T \nmid \theta_E$$

where $T = \gamma_0 - 1 \in \Lambda$ as before. If conjecture 5.4 is valid, then $T \nmid \theta_E$ is equivalent to the assertion that $X_E(\mathbb{Q}_\infty)/TX_E(\mathbb{Q}_\infty)$ is finite. Mazur's Control Theorem (theorem 5.2) shows that this last assertion is indeed equivalent to the finiteness of $\mathrm{Sel}_E(\mathbb{Q})_p$. We should also add that, if $L(1, E) \neq 0$, then conjecture 5.4 would imply the p-part of the Birch and Swinnerton-Dyer conjecture. (See chapter 4 of [Gr5] for an exposition of this result.)

If $E(\mathbb{Q})$ is infinite, then conjecture 5.4 implies the following inequality:

$$\mathrm{ord}_{s=1}(L_p(s,E)) \geq \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})).$$

This is because $X_E(\mathbb{Q}_\infty)/TX_E(\mathbb{Q}_\infty)$ has $\mathbb{Z}_p$-rank equal to the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_E(\mathbb{Q})_p$. This is at least $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ (with equality if $Ш_E(\mathbb{Q})_p$ is finite). The Birch and Swinnerton-Dyer conjecture asserts that $\mathrm{ord}_{z=1}(L(z,E)) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. In order to deduce this from conjecture 5.4 one would need to prove three results:

(i) $Ш_E(\mathbb{Q})$ *is finite.*
(ii) $TX_E(\mathbb{Q}_\infty)/T^2X_E(\mathbb{Q}_\infty)$ *is finite.*
(iii) $\mathrm{ord}_{z=1}(L(z,E)) = \mathrm{ord}_{s=1}(L_p(s,E))$

The first result is of course a well-known conjecture, proved by Kolyvagin if $\mathrm{ord}_{z=1}(L(z,E)) \leq 1$. In this case, Kolyvagin also proves the equality of $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ and $\mathrm{ord}_{z=1}(L(z,E))$. The second result is an easy consequence of theorem 5.2 if $\mathrm{Sel}_E(\mathbb{Q})_p$ is finite. (For then $X_E(\mathbb{Q}_\infty)/TX_E(\mathbb{Q}_\infty)$ is finite and this implies (ii).) More generally, it is equivalent to the nondegeneracy of a certain p-adic height pairing. This equivalence is proved in [Pe1] for elliptic curves with complex multiplication and in [Sch2] in a more general context. The nondegeneracy is trivial if $\mathrm{Sel}_E(\mathbb{Q})_p$ is finite. It has been proven by D. Bertrand if E has complex multiplication, $E(\mathbb{Q})$ has rank 1, and $Ш_E(\mathbb{Q})_p$ is finite. B. Perrin-Riou [Pe2] has also proven it if $\mathrm{ord}_{s=1}(L_p(s,E)) = 1$. But nothing is known about the nondegeneracy if $\mathrm{ord}_{z=1}(L(z,E)) > 1$.

As for the equality in (iii), it is obvious if $L(1,E) \neq 0$ and would follow from the Gross-Zagier theorem together with Perrin-Riou's p-adic analogue [Pe2] if $\mathrm{ord}_{s=1}(L_p(s,E)) = 1$. It is also known that $\mathrm{ord}_{z=1}(L(z,E))$ and $\mathrm{ord}_{s=1}(L_p(s,E))$ have the same parity since one can compare the signs in the functional equation for $L(z,E)$ and its analogue for $L_p(s,E)$. Beyond this, we know nothing about the relationship between these orders of vanishing.

We should also mention the interesting case where E has split, multiplicative reduction at p. The corresponding p-adic L-function $L_p(s,E)$ has been constructed in [M-T-T]. But it has a "trivial zero". That is, the natural interpolation property given in [M-T-T] implies that $L_p(1,E) = 0$, and it is conjectured there that $\mathrm{ord}_{s=1}(L_p(s,E)) = 1 + \mathrm{ord}_{z=1}(L(z,E))$. The functional equation proved in [M-T-T] show that these orders have opposite parities.

Conjectures 5.3 and 5.4 have been proven by Rubin [Ru2] when $E/\mathbb{Q}$ has complex multiplication and p is any odd prime where E has good, ordinary reduction. For a modular elliptic curve E, Kato has proven conjectures 5.3 and has also proven that θ_E is at least contained in the characteristic ideal of $X_E(\mathbb{Q}_\infty)$, up to multiplication by a power of p.

If E is a modular elliptic curve/$\mathbb{Q}$ having good, supersingular reduction at p, then a p-adic L-function $L_p(s,E)$ still exists, but now corresponds to an unbounded $\mathbb{Q}_p$-valued measure μ_E on Γ. (This means that the measures of open subsets have unbounded denominators.) Also, the Selmer group $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ will definitely not be Λ-cotorsion. This topic has been studied by Perrin-Riou and by Schneider. We refer the reader to [Pe3], where one can even find a formulation of a Main Conjecture in the supersingular case. We want to mention just one specific question, which seems to still be open. Assume that $\text{Ш}_E(\mathbb{Q}_n)_p$ is finite for all n. What can one then say about the growth of $|\text{Ш}_E(\mathbb{Q}_n)_p|$ as $n \to \infty$? If E has good, ordinary reduction at p and if conjecture 5.3 holds for $A = E$ and the $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$, then one can prove that $|\text{Ш}_E(\mathbb{Q}_n)_p| = p^{\lambda n + \mu p^n + \nu}$ for $n \gg 0$, where λ, μ, and ν are suitable integers. But if E has supersingular reduction, we do not even have a good guess. More generally, one can consider the analogous question for an arbitrary abelian variety A/F and an arbitrary $\mathbb{Z}_p$-extension F_∞/F.

In 1976, Coates and Wiles proved the following theorem.

Theorem (5.5) *Assume that E is an elliptic curve defined over $\mathbb{Q}$ with complex multiplication and that $L(1, E) \neq 0$. Then $E(\mathbb{Q})$ is finite.*

The proof involves a beautiful argument based on adapting some of the results in Iwasawa's paper [Iw7] to a different, but quite analogous, situation. We will outline this argument and also take the opportunity to state another main conjecture which Coates and Wiles formulated.

Suppose that E is an elliptic curve defined over $\mathbb{Q}$ such that $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$, the ring of integers of an imaginary quadratic field K. We will assume that p is an odd prime and that E has good, ordinary reduction at p. Then p splits completely in K. Since K must have class number 1, we can write that $p = \pi\bar{\pi}$, where $\pi, \bar{\pi} \in \mathcal{O}$ (complex conjugates). Let $E[\pi^\infty]$ denote the group of π-power torsion points on $E(\overline{\mathbb{Q}}) : E[\pi^\infty] = \bigcup_n E[\pi^{n+1}]$, where $E[\pi^{n+1}]$ is the kernel of the endomorphism π^{n+1} of $E(\overline{\mathbb{Q}})$. Adjoining coordinates to K, we obtain the fields $F_\infty = K(E[\pi^\infty]) = \bigcup_n F_n$, where $F_n = K(E[\pi^{n+1}])$. Considering the action of $\mathrm{Gal}\,(F_\infty/K)$ on $E[\pi^\infty]$ (which is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as a group), one obtains an isomorphism

$$\psi_E : \mathrm{Gal}\,(F_\infty/K) \xrightarrow{\sim} \mathbb{Z}_p^\times .$$

Therefore, $\mathrm{Gal}\,(F_\infty/K) \cong \Delta \times \Gamma$, where $\Gamma = \mathrm{Gal}\,(F_\infty/F_0)$ is isomorphic to $1 + p\mathbb{Z}_p$ and $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times$. The situation is quite analogous to that for $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$, where μ_{p^∞} denotes the group of p-power roots of unity. The prime π is totally ramified in F_∞/K. (But $\bar{\pi}$ is unramified.) If $F = F_0$, then Δ can be identified with $\mathrm{Gal}\,(F/K)$ and there is a canonical isomorphism

$$\omega_E : \Delta \to (\mathbb{Z}/p\mathbb{Z})^\times$$

which gives the action of Δ on $E[\pi]$. (We also regard ω_E as having values in $\mathbb{Z}_p^\times$.) The extension F_∞/F is a $\mathbb{Z}_p$-extension, and only the prime of F lying above π is ramified. (Note: In F/K, the primes of K where E has bad reduction are also ramified.)

Now suppose that $E(\mathbb{Q})$ is infinite and that P is a $\mathbb{Q}$-rational point on E of infinite order. We will assume that $P \notin \pi E(K)$. For each $n \geq 0$, let $P_n \in E(\overline{\mathbb{Q}})$ be such that $\pi^{n+1} P_n = P$. Then $P_0 \notin E(K)$. Let $T_n = F_n(P_n)$, $T_\infty = \bigcup_n T_n$. It turns out that T_n/F_n is cyclic of order p^{n+1} and is unramified except at the unique prime of F_n above π. The extension T_∞/K is Galois, $\mathrm{Gal}\,(T_\infty/F_\infty) \cong \mathbb{Z}_p$, and the action of $\mathrm{Gal}\,(F_\infty/K)$ on $\mathrm{Gal}\,(T_\infty/F_\infty)$ by inner automorphisms is given by ψ_E. This can be seen by considering the 1-cocycles $\sigma_n : G_K \to E[\pi^{n+1}]$ defined by $\sigma_n(g) = g(P_n) - P_n$ for all $g \in G_K$. One can check that $\sigma_n|_{G_{F_\infty}}$ induces a compatible set of isomorphisms $\mathrm{Gal}\,(F_\infty(P_n)/F_\infty) \xrightarrow{\sim} E[\pi^{n+1}]$ for $n \geq 0$, equivariant for the actions of $\mathrm{Gal}\,(F_\infty/K)$. This implies that $\mathrm{Gal}\,(T_\infty/F_\infty) \cong T_\pi(E)$, the π-adic Tate module for E, as $\mathrm{Gal}\,(F_\infty/K)$-modules. Since T_∞/F_∞ is ramified only at π, we have $T_\infty \subset M_\infty$, where M_∞ denotes the maximal, abelian pro-p extension of F_∞ which is unramified everywhere except at π.

Let $X = \mathrm{Gal}\,(L_\infty/F_\infty)$, where L_∞ is the pro-p Hilbert class field of F_∞. Let $Y = \mathrm{Gal}\,(M_\infty/F_\infty)$ and $Z = \mathrm{Gal}\,(M_\infty/L_\infty)$, noting that $L_\infty \subset M_\infty$. Then X, Y, and Z are Λ-modules, where $\Lambda = \mathbb{Z}_p[[\Gamma]]$. Since Δ acts on them too (because M_∞ and L_∞ are Galois over K), we can consider the Δ-components corresponding to ω_E and obtain an exact sequence

$$0 \to Z^{\omega_E} \to Y^{\omega_E} \to X^{\omega_E} \to 0$$

of Λ-modules. Coates and Wiles verify that T_∞/F_∞ is ramified at π, a crucial fact for their proof. It then follows that $T_\infty \not\subset L_\infty$ and so $T_\infty \cap L_\infty$ is a finite extension of F_∞ since all nontrivial subgroups of $\mathrm{Gal}\,(T_\infty/F_\infty)$ have finite index. Therefore Z has a quotient $\mathrm{Gal}\,(T_\infty/T_\infty \cap L_\infty)$ which is isomorphic to $\mathbb{Z}_p$ and on which $\mathrm{Gal}\,(F_\infty/K)$ acts by ψ_E. Let $\kappa_E = \psi_E|_\Gamma$. Then it follows that Z^{ω_E} has a quotient which is isomorphic to $\Lambda/(\gamma_0 - \kappa_E(\gamma_0))$, as a Λ-module where γ_0 denotes any topological generator of Γ.

If F' is any algebraic extension of K, then the Selmer group for E over F' is an $\mathcal{O}$-module. One can consider its π-primary subgroup $\mathrm{Sel}_E(F')_\pi$, which is a subgroup of $H^1(G_{F'}, E[\pi^\infty])$. Let $F' = F_\infty$. Since G_{F_∞} acts trivially on $E[\pi^\infty]$, $\mathrm{Sel}_E(F_\infty)_\pi$ is a subgroup of $\mathrm{Hom}(\mathrm{Gal}\,(F_\infty^{\mathrm{ab}}/F_\infty), E[\pi^\infty])$. Coates proves that

$$\mathrm{Sel}_E(F_\infty)_\pi = \mathrm{Hom}(\mathrm{Gal}\,(M_\infty/F_\infty), E[\pi^\infty]).$$

Thus $\mathrm{Sel}_E(F_\infty)_\pi$ is closely related to the Pontryagin dual $\mathrm{Hom}(Y, \mathbb{Q}_p/\mathbb{Z}_p)$ of the Galois group Y. They are isomorphic as groups, but the action of $\mathrm{Gal}\,(F_\infty/K)$ is twisted by ψ_E. Now let $r = \mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}_{\mathcal{O}}(E(K))$. Then $\mathrm{Sel}_E(K)_\pi$ has a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$ and the restriction map $\mathrm{Sel}_E(K)_\pi \to \mathrm{Sel}_E(F_\infty)_\pi^{\mathrm{Gal}\,(F_\infty/K)}$ can be shown to have finite kernel and cokernel. This means that $\mathrm{Hom}_\Gamma(Y^{\omega_E}, E[\pi^\infty])$ has $\mathbb{Z}_p$-corank at least r. If $r > 0$, then the fact that T_∞/F_∞ is ramified at π implies that the image of $\mathrm{Sel}_E(K)_\pi$ in $\mathrm{Hom}_\Gamma(Z^{\omega_E}, E[\pi^\infty])$ has $\mathbb{Z}_p$-corank at least 1. It is possible to show that this image then has $\mathbb{Z}_p$-corank exactly 1 and hence

$\mathrm{Hom}_\Gamma(X^{\omega_E}, E[\pi^\infty])$ has $\mathbb{Z}_p$-corank at least $r-1$. Therefore it follows that $\lambda(F_\infty/F) \geq r-1$. That is, if $r > 1$, then Iwasawa's λ-invariant for the noncyclotomic $\mathbb{Z}_p$-extension F_∞/F will be positive. Letting $S = T - (\kappa_E(\gamma_0)-1)$, we see that $S^r | f_{Y^{\omega_E}}(T)$, $S | f_{Z^{\omega_E}}(T)$, and $S^{r-1} | f_{X^{\omega_E}}(T)$. These divisibilities should conjecturally be exact. Perrin-Riou proves in her thesis [Pe1] that this is so precisely when $\text{Ш}_E(K)_\pi$ is finite and a certain p-adic height pairing on $E(K) \otimes_{\mathcal{O}} K_\pi$ is nondegenerate. The finiteness of $\text{Ш}_E(K)_\pi$ implies that $Y^{\omega_E}/SY^{\omega_E}$ has $\mathbb{Z}_p$-rank exactly r. The nondegeneracy is shown to imply that $SY^{\omega_E}/S^2Y^{\omega_E}$ is finite, i.e., in the classification theorem applied to the Λ-module Y^{ω_E}, there is no factor of the form $\Lambda/(S^a)$ with $a \geq 2$.

In their paper [C-W1], Coates and Wiles show that if $E(Q)$ is infinite, then the rational number $L(1, E/\mathbb{Q})/\Omega_E$ (where Ω_E denotes the real period of E) is divisible by all primes in a certain infinite set, concluding that $L(1, E/\mathbb{Q}) = 0$. In another paper [C-W2] they prove a perfect analogue of theorem 4.6 (which Iwasawa proved in [Iw7]). This result gives another proof of theorem 5.5, which is the one we will briefly explain. Let U_n denote the group of principal units in the $\mathfrak{p}_n$-adic completion of F_n, where $\mathfrak{p}_n$ is the unique prime of F_n lying over π. Let E_n and C_n denote respectively the groups of global units and elliptic units in F_n which are congruent to 1 modulo $\mathfrak{p}_n$. Let $\overline{E}_n$, $\overline{C}_n$ denote the corresponding closures in U_n. Let $\mathfrak{X} = \varprojlim \overline{E}_n/\overline{C}_n$, $\mathfrak{Y} = \varprojlim U_n/\overline{C}_n$, and $\mathfrak{Z} = \varprojlim U_n/\overline{E}_n$. Then $\mathfrak{X}$, $\mathfrak{Y}$, and $\mathfrak{Z}$ are torsion Λ-modules on which $\Delta = \mathrm{Gal}(F/K)$ acts. To state the result of Coates and Wiles, we must mention the p-adic L-functions that they consider, which were first constructed by Manin-Vishik [M-V] and, in a much more precise form, by Katz [Ka]. Let ψ_E denote the grossencharacter of K associated to the elliptic curve E by Deuring. It has the property that $L(z, E/\mathbb{Q}) = L(z, \psi_E)$. Suppose that $1 \leq j \leq p-2$. For each such j, there is a power series $G_E^{(j)}(T)$ with the property that

$$G_E^{(j)}(u_0^k - 1) = A_k \left(1 - \psi_E^k(\mathfrak{p})/N(\mathfrak{p})\right) L(1, \psi_E^k) \tag{17}$$

for all positive integers k such that $k \equiv j \pmod{p-1}$. Here $u_0 = \kappa_E(\gamma_0)$ and A_k is a certain explicit, nonzero factor which involves the real period Ω_E and a certain "p-adic period" $\Omega_E^{(p)}$. The coefficients of $G_E^{(j)}(T)$ as well as $\Omega_E^{(p)}$ belong to the ring of integers $\mathbf{I}$ in the completion of the maximal unramified extension $\mathbb{Q}_p^{\mathrm{unr}}$ of $\mathbb{Q}_p$. Furthermore, there is a power series $g_E^{(j)}(T)$ with coefficients in $\mathbb{Z}_p$ such that $G_E^{(j)}(T)/g_E^{(j)}(T)$ is an invertible element in the formal power series ring $\mathbf{I}[[T]]$. Only the ideal $(g_E^{(j)}(T))$ of Λ is uniquely determined. The result of Coates and Wiles can be stated as follows.

Theorem (5.6) *Suppose that $1 \leq j \leq p-2$ and that p is a prime such that $p \geq 5$, E has good, ordinary reduction at p, and $\psi_E(\mathfrak{p})/N(\mathfrak{p}) \not\equiv 1 \pmod{\mathfrak{p}}$. Then*

$$\mathfrak{Y}^{\omega_E^j} \cong \Lambda/(g_E^{(j)}(T))$$

as Λ-modules.

If $\psi_E(\mathfrak{p})/N(\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}}$, then p is called an anomalous prime for E. (Equivalently, $\widetilde{E}(\mathbb{F}_p)$ has an element of order p, where $\widetilde{E}$ is the reduction of E modulo p.) Then some modification of theorem 5.6 holds. There are infinitely many primes satisfying the hypotheses of theorem 5.6. One deduces theorem 5.5 as follows. If $E(\mathbb{Q})$ is infinite, then, as we have discussed, one obtains that $S = T - (u_0 - 1)$ divides $f_{Z^{\omega_E}}(T)$. But class field theory shows that $Z \cong \mathfrak{Z}$ as $\mathrm{Gal}\,(F_\infty/K)$-modules. Thus S also divides $f_{\mathfrak{Z}^{\omega_E}}(T)$ and therefore divides $f_{\mathfrak{Y}^{\omega_E}}(T)$. By theorem 5.6, it is then clear that $S|g_E^{(1)}(T)$ and so $g_E^{(1)}(u_0 - 1) = 0$ since $S = T - (u_0 - 1)$. Therefore, by the interpolation property (17), $L(1, \psi_E) = L(1, E/\mathbb{Q})$ is indeed zero.

In [C-W2], Coates and Wiles state the following conjecture, which is often referred to as the one-variable main conjecture for elliptic curves with complex multiplication.

Conjecture (5.7) *With the above notation and assumptions, the characteristic ideal of $Y^{\omega_E^j}$ is generated by $g_E^{(j)}(T)$. Equivalently, the Λ-modules $X^{\omega_E^j}$ and $\mathfrak{X}^{\omega_E^j}$ have the same characteristic ideal.*

Later on, Yager [Y] proved a two-variable analogue of theorem 5.6 and formulated an analogous conjecture, referred to as the two-variable main conjecture. The corresponding two-variable p-adic L-function was constructed by Katz and has an interpolation property involving the numbers $L(1, \psi_E^k \overline{\psi}_E^l)$ where k and l are in fixed residue classes modulo $p-1$ and $k \geq 1$, $l \leq 0$.

6. In their paper *Class fields of abelian extensions of* $\mathbb{Q}$ published in 1984, Mazur and Wiles gave a proof of conjecture 4.4. They also prove the more general version for any finite abelian extension $F/\mathbb{Q}$. If ψ is any even Dirichlet character, their result gives an interpretation of the Kubota-Leopoldt p-adic L-function $L_p(s, \psi)$ (or more precisely its zeros) in terms of the χ-component of $\mathrm{Gal}\,(L_\infty/F_\infty)$, where $\chi = \omega\psi^{-1}$ (which is an odd Dirichlet character) and F is chosen so that χ can be identified in the usual way with a character of $\Delta = \mathrm{Gal}\,(F/\mathbb{Q})$. Their approach was inspired by Ribet's proof of the converse of a theorem of Kummer-Herbrand in that they use the structure of certain finite groups of torsion points on abelian varieties arising as quotients of the Jacobian varieties of some modular curves. An important role is played by the cuspidal group whose structure is related to Stickelberger ideals, and hence to Bernoulli numbers, by results of Kubert and Lang. By using the fields generated by these groups of torsion points, Mazur and Wiles construct a sequence of finite extensions of F_∞ contained in L_∞. A crucial part of their proof depends on the theory of Fitting ideals to prove the divisibility statement that they need. In the special case where $F = \mathbb{Q}(\zeta_p)$, it states that $g_i(T)|f_i(T)$. (This corresponds to the case $\chi = \omega^i$, where i is odd.) As we mentioned earlier, such a divisibility result would be sufficient because of proposition 4.2. One can find a good outline of their proof in the introduction of their paper, and also a good expository account in the Seminaire Bourbaki lecture on this topic given by Coates [Co3].

We would like to give some idea of why modular Jacobian varieties and modular forms provide a natural approach to such questions. For this we will just discuss a proof of the converse to the result of Kummer-Herbrand alluded to above. Let $F = \mathbb{Q}(\zeta_p)$. Suppose that $2 \leq i,\ j \leq p-2$, that $i+j \equiv 1 \pmod{p-1}$, and that i is odd (so that j is even). The Kummer-Herbrand result asserts that if $S_0^{\omega^i} \neq 0$, then $p|B_j$. As the discussion in section 4 shows, this follows easily from Stickelberger's theorem giving an annihilator in $\mathbb{Z}[\Delta]$ of S_0. Ribet proves the converse by showing that if $p|B_j$, then $\mathrm{Gal}\,(L_0/F_0)^{\omega^i} \neq 0$, where L_0 denotes the p-Hilbert class field of $F_0 = F$. To do this, he constructs a nontrivial, unramified p-extension L/F such that $\mathrm{Gal}\,(L/F)$ is abelian, $L/\mathbb{Q}$ is Galois, and $\Delta = \mathrm{Gal}\,(F/\mathbb{Q})$ acts on $\mathrm{Gal}\,(L/F)$ by the character ω^i.

An idea which had been proposed by various people in the 1970s was to construct such a field L by using the p-adic representations associated to modular forms. The existence of these representations had been conjectured by Serre and proved by Deligne. The motivation for approaching the question in this way was suggested by one of the famous congruences proved by Ramanujan, namely that $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$ for all $n \geq 1$, where $\tau(n)$ denotes the n-th coefficient in the q-expansion (or Fourier expansion) of $f_{12} = q \prod_{m=1}^{\infty} (1-q^m)^{24}$, the unique normalized cusp form of level 1 and weight 12, and $\sigma_{11}(n) = \Sigma d^{11}$, where d runs over the positive divisors of n. The above congruence is derived directly from the fact that $691|B_{12}$. One then obtains a congruence between the Eisenstein series of weight 12 which has $\sigma_{11}(n)$ as its n-th Fourier coefficient and a cusp form which must be f_{12}. In general, if $p|B_j$, then a similar congruence must exist involving some cusp form of level 1 and weight j.

Let p be any prime. Let $\Sigma = \{p, \infty\}$ and let $\mathbb{Q}_\Sigma$ denote the maximal extension of $\mathbb{Q}$ unramified outside Σ. Deligne constructs a 2-dimensional representation space V_p of $\mathrm{Gal}\,(\mathbb{Q}_\Sigma/\mathbb{Q})$ associated to f_{12} such that $Tr_{V_p}(\mathrm{Frob}_l) = \tau(l)$ for all primes $l \neq p$. Here $\mathrm{Frob}_l \in \mathrm{Gal}\,(\mathbb{Q}_\Sigma/\mathbb{Q})$ is the Frobenius automorphism for any prime of $\mathbb{Q}_\Sigma$ lying above l and Tr_{V_p} is the trace. Now let $p = 691$. Choose a $\mathrm{Gal}\,(\mathbb{Q}_\Sigma/\mathbb{Q})$-invariant $\mathbb{Z}_p$-lattice T_p in V_p. Then one obtains a 2-dimensional representation space T_p/pT_p for $\mathrm{Gal}\,(\mathbb{Q}_\Sigma/\mathbb{Q})$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ such that Frob_l has trace equal to $1 + l^{11} \pmod{p}$, i.e., equal to $1 + \omega^{11}(l) \pmod{p\mathbb{Z}_p}$. The Chebotarev Density Theorem then implies that T_p/pT_p is reducible and has composition factors $\mathbb{F}_p = \mathbb{F}_p(\omega^0)$ (on which $\mathrm{Gal}\,(\mathbb{Q}_\Sigma/\mathbb{Q})$ acts trivially) and $\mathbb{F}_p(\omega^{11})$ (on which $\mathrm{Gal}\,(\mathbb{Q}_\Sigma/\mathbb{Q})$ acts by ω^{11}). If one knew that V_p were irreducible, then it would be easy to show that T_p could be chosen so that one has a nonsplit exact sequence

$$0 \to \mathbb{F}_p(\omega^0) \to T_p/pT_p \to \mathbb{F}_p(\omega^{11}) \to 0$$

of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$-modules. (But in this specific case, it is possible to verify this directly.) In matrix form, the corresponding $\mathbb{F}_p$-representation looks like $\begin{bmatrix} 1 & * \\ 0 & \omega^{11} \end{bmatrix}$, where $*$ is nontrivial. It follows that there is a cyclic extension L of F of degree p such that this $\mathbb{F}_p$-representation factors through $\mathrm{Gal}(L/\mathbb{Q})$ and its restriction to $\mathrm{Gal}(L/F)$ gives a Δ-equivariant isomorphism

$$\mathrm{Gal}(L/F) \xrightarrow{\sim} \mathrm{Hom}(\mathbb{F}_p(\omega^{11}), \mathbb{F}_p) = \mathbb{F}_p(\omega^{-11}).$$

Thus, starting from the fact that $p|B_j$ for $j = 12$ and $p = 691$, one obtains a field L as above such that $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ acts on $\mathrm{Gal}(L/F)$ by $\chi = \omega^{1-j} = \omega^i$ where i, j are related as before. In this case, $i = 679$.

It turns out that the extension L/F is automatically unramified. The easiest way to explain this is to use a later result of Wiles which (in a much more general formulation) actually plays an important role in his proof of the Main Conjecture over totally real number fields. The prime $p = 691$ is a so-called "ordinary" prime for f_{12}. This means that $p \nmid \tau(p)$, as Ramanujan's congruence shows. Wiles' result implies that for any such prime p, if one regards V_p as a representation space for $G_{\mathbb{Q}_p}$, then it is reducible. More precisely, there is an exact sequence

$$0 \to W_p \to V_p \to U_p \to 0$$

where W_p and U_p are 1-dimensional representation spaces for $G_{\mathbb{Q}_p}$ such that

$$W_p \cong \mathbb{Q}_p(11) \quad \text{and} \quad U_p \cong \mathbb{Q}_p(0)$$

as representation spaces for the inertia subgroup $I_p = G_{\mathbb{Q}_p^{\mathrm{unr}}}$. Here we use the notation $\mathbb{Q}_p(k)$ for the 1-dimensional space on which any Galois group acts by the k-th power of the p-power cyclotomic character. Thus U_p is unramified as a $G_{\mathbb{Q}_p}$-module. This implies that T_p/pT_p has a $G_{\mathbb{Q}_p}$-submodule isomorphic to $\mathbb{F}_p(\omega^{11})$. Since it also has $\mathbb{F}_p(\omega^0)$ as a $G_{\mathbb{Q}_p}$-submodule, we have

$$T_p/pT_p \cong \mathbb{F}_p(\omega^0) \times \mathbb{F}_p(\omega^{11})$$

as $G_{\mathbb{Q}_p}$-modules. Therefore $G_{\mathbb{Q}_p(\zeta_p)}$ acts trivially on T_p/pT_p which means that the unique prime of F lying over p splits completely in L/F. Since $L \subset \mathbb{Q}_\Sigma$ and $\Sigma = \{p, \infty\}$, L is indeed a subfield of the p-Hilbert class field of F.

Vandiver's conjecture is true for $p = 691$. Hence the cyclicity hypothesis of section 4 is valid for this prime and so the Main Conjecture has been proven by Iwasawa in this case. The Ribet-Kummer-Herbrand theorem is an easy consequence and can be viewed as a first approximation to the conjecture 4.4. This is because $S_0^{\omega^i} \neq 0 \iff f_i(T) \notin \Lambda^\times$, whereas $p|B_j \iff g_i(T) \notin \Lambda^\times$, following the notation of section 4. Ribet proves the converse of the Kummer-Herbrand theorem for all p and j by pursuing the idea of finding unramified extensions L/F in the 2-dimensional representations associated to modular forms. He succeeds in making this work by using modular forms of weight

2 which have the advantage that the associated l-adic representations arise from abelian varieties. He then still obtains a congruence between an Eisenstein series and a cusp form if $p|B_j$. He can prove the irreducibility of the associated 2-dimensional representation, and then the existence of a suitable $G_{\mathbb{Q}}$-invariant lattice. To prove that L/F is unramified, he reduces the necessary splitting for $G_{\mathbb{Q}_p}$-modules to a theorem of Raynaud concerning finite commutative group schemes. In the work of Wiles proving the Main Conjecture for p-adic L-functions attached to totally real number fields, unramified extensions are constructed in the 2-dimensional representations associated to Hilbert modular forms. Under the assumption of ordinariness, he proves the reducibility as a $G_{\mathbb{Q}_p}$-representation space, just as we mentioned for f_{12}. The argument adapts ideas of Hida and again somehow reduces to the case of 2-dimensional representations obtained from abelian varieties (i.e., from weight 2).

There are now other proofs of conjecture 4.4 which proceed by using Kolyvagin's Euler systems. This approach was first inspired by Thaine's discovery of a method to relate the order of $(E_0/C_0)_p^{\omega^j}$ to the order of $S_0^{\omega^j}$ for every j, where $F = F_0 = \mathbb{Q}(\zeta_p)$ and the notation is just as in section 4. Thaine's technique involves studying the cyclotomic units in certain abelian extensions of $\mathbb{Q}$ containing F. In retrospect, Thaine uses the first step in an Euler system. Rubin carries this method through in [Ru3], proving the equivalent conjecture 4.7. Rubin also gives an Euler system proof of conjecture 4.4 in [Ru4]. In his paper *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Rubin proves the conjectures formulated by Coates and Yager mentioned at the end of section 5. The approach is to study Euler systems formed from elliptic units in abelian extensions of an imaginary quadratic field. As a consequence, Rubin obtains the best results to date concerning the Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication.

The method of Wiles using systematically 2-dimensional representations associated to ordinary modular forms (for a prime p) allows him to prove the main conjecture corresponding to abelian characters of totally real number fields. The method of Euler systems has given the same result only for abelian characters (i.e., Dirichlet characters) of $\mathbb{Q}$. Rubin has succeeded in making the Euler system method work for abelian characters of imaginary quadratic fields, as we mentioned in the previous paragraph, obtaining the conjectures of Coates and of Yager. One wonders if these conjectures can also be obtained from a modular form approach.

7. There is now a large literature concerning p-adic L-functions. The p-adic analogues of various classical complex L-functions have been constructed. We refer to [Co4], [C-P], [C-S], [H] and to their references as a guide to this topic. We have already described in some detail the conjectural interpretation for the Kubota-Leopoldt p-adic L-functions which was proposed by Iwasawa and proved by Mazur and Wiles. We have described more briefly the conjecture of Mazur which gives an interpretation of the p-adic L-function associated to a modular elliptic curve/$\mathbb{Q}$ with good, ordinary reduction at p. This p-adic L-function is the p-adic analogue of $L(z, f_E)$, where f_E is the modular form corresponding to E, a newform of weight 2 and level equal to the conductor of E. But a p-adic analogue of the L-function $L(z, f)$ associated to a newform f of weight $k \geq 2$ and any level not divisible by p had also been constructed in the 1970s by Manin-Vishik, and Amice-Vèlu. Under an "ordinariness" hypothesis, this p-adic L-function corresponds to an element in the Iwasawa algebra $\Lambda = \mathcal{O}[[T]]$, where $\mathcal{O}$ denotes the integers in the finite extension of $\mathbb{Q}_p$ generated by the coefficients of f. The hypothesis is that the p-th Fourier coefficient is a unit in $\mathcal{O}$. At the time it seemed quite mysterious how to interpret this p-adic L-function when $k > 2$. That is, could one formulate an appropriate Main Conjecture?

In 1987 I gave two lectures on this topic at the conference *Iwasawa Theory and Special Values of L-functions* which took place at M.S.R.I.. I then described a rather simple, general, and natural way to formulate such a conjecture under a certain "ordinariness" hypothesis. This conjecture gave a possible interpretation for the p-adic analogue $L_p(s, V)$ of the complex L-function $L(z, V)$ attached to a compatible system $V = \{V_l\}$ of l-adic representations of $G_{\mathbb{Q}}$. The ordinariness hypothesis for V and p is that there should exist a filtration F^iV_p of $\mathbb{Q}_p$-subspaces of V_p (for $i \in \mathbb{Z}$) with the properties:

(a) $F^{i+1}V_p \subset F^iV_p$; $\quad F^iV_p = V_p$ if $i \ll 0$, $\quad F^iV_p = 0$ if $i \gg 0$.
(b) F^iV_p is invariant for the action of $G_{\mathbb{Q}_p}$ and the inertia subgroup I_p of $G_{\mathbb{Q}_p}$ acts on $F^iV_p/F^{i+1}V_p$ by χ_p^i.

Here $\chi_p : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ is th p-power cyclotomic character. Let $A = V_p/T_p$, where T_p is a $G_{\mathbb{Q}}$-invariant $\mathbb{Z}_p$-lattice in V_p. Then A is a discrete $G_{\mathbb{Q}}$-module isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^d$ as a group, where $d = \dim_{\mathbb{Q}_p}(V_p)$. We define F^+V_p to be F^1V_p and F^+A to be the image of F^+V_p in A. Thus F^+A is a divisible subgroup of A invariant under the action of $G_{\mathbb{Q}_p}$.

We can now define a certain Λ-module $S_A(\mathbb{Q}_\infty)$, which we refer to as the Selmer group for A over $\mathbb{Q}_\infty$. It is defined by

$$S_A(\mathbb{Q}_\infty) = \ker\big(H^1(\mathbb{Q}_\infty, A) \to H^1(I_\pi, A/F^+A) \times \prod_{v\nmid p} H^1(I_v, A)\big)$$

where π denotes the unique prime of $\mathbb{Q}_\infty$ lying over p, I_π denotes the inertia subgroup of $G_{\mathbb{Q}_\infty}$ for a fixed prime of $\overline{\mathbb{Q}}$ over π, v varies over all primes of $\mathbb{Q}_\infty$ except π, and I_v denotes the inertia subgroup of $G_{\mathbb{Q}_\infty}$ for any prime of $\overline{\mathbb{Q}}$ over v. Also, as usual, $H^1(K, *)$ denotes $H^1(G_K, *)$ for any field K. $S_A(\mathbb{Q}_\infty)$ is a p-primary group on which Γ acts naturally, and hence it is a discrete Λ-module, where $\Lambda = \mathbb{Z}_p[[\Gamma]]$. It is always cofinitely generated as a Λ-module, but not always Λ-cotorsion. We let $X_A(\mathbb{Q}_\infty)$ denote the Pontryagin dual of $S_A(\mathbb{Q}_\infty)$.

The gamma-factors in the conjectural functional equation for $L(z, V)$ have a pole at $z = 1$ with order r_V, say. Then one would expect that $L(z, V, \rho)$ will have a zero at $z = 1$ of order exactly r_V for all but finitely many characters ρ of Γ, where $L(z, V, \rho)$ is the L-function for V twisted by the character ρ. The natural conjecture is that:

$$X_A(\mathbb{Q}_\infty) \textit{ has } \Lambda\textit{-rank equal to } r_V.$$

Let $V^* = \{V_l^*\}$, where $V_l^* = \mathrm{Hom}(V_l, \mathbb{Q}_l(1))$. Then V^* is another compatible system of l-adic representations of $G_{\mathbb{Q}}$. Assume now that $r_V = r_{V^*} = 0$. This means that $L(1, V)$ is a "critical value" of $L(z, V)$ in the sense defined by Deligne. (And so is $L(1, V^*)$.) Under this assumption, as well as the ordinariness assumption, Coates and Perrin-Riou [C-P] formulate a precise conjecture about the existence and the interpolation property of a p-adic analogue $L_p(s, V)$. It should correspond to an element θ_V in Λ (which is unfortunately only defined up to multiplication by an element of $\mathbb{Q}^\times$). The interpolation property involves the numbers $L(1, V, \rho)$ with $\rho \in \widehat{\Gamma}$ and one would expect that $\theta_V \neq 0$. Here then is the Main Conjecture.

Conjecture (7.1) *The characteristic ideal of $X_A(\mathbb{Q}_\infty)$ is generated by θ_V.*

There is an ambiguity in this conjecture. In addition to the fact that θ_V and hence the ideal (θ_V) are not well-defined, the Selmer group $S_A(\mathbb{Q}_\infty)$ depends on the choice of the $\mathbb{Z}_p$-lattice T_p. Both ambiguities involve only the μ-invariant. The μ-invariant of $S_A(\mathbb{Q}_\infty)$ can indeed be positive, but it is possible to make a precise conjecture about its value.

An obvious question to ask (and which stumped us for quite a while) was whether the above conjecture is consistent with the functional equation for the corresponding L-functions, which relates the values $L(1, V, \rho)$ to $L(1, V^*, \rho^{-1})$. For the p-adic L-function one obtains a functional equation which can be expressed as $\theta_{V^*} = \theta_V^\iota$, where $\iota : \Lambda \to \Lambda$ is the involution of Λ induced by $\iota(\gamma) = \gamma^{-1}$ for all $\gamma \in \Gamma$. For the Selmer groups, the question was then whether the characteristic ideals of $X_A(\mathbb{Q}_\infty)$ and $X_{A^*}(\mathbb{Q}_\infty)$ are also related by the involution ι. Here $A^* = V_p^*/T_p^*$ where $T_p^* = \mathrm{Hom}(T_p, \mathbb{Z}_p(1))$, which is a $G_{\mathbb{Q}}$-invariant $\mathbb{Z}_p$-lattice in V_p^*. Our first attempts to prove this were based on the Reflection Principle (which works in the case where V is a compatible system of 1-dimensional representations), but then we found that the Duality Theorems of Poitou and Tate were just the right tool. In *Iwasawa theory for p-adic representations*, one can find a detailed description of the conjectures, results about the structure of Galois cohomology groups and Selmer groups as Λ-modules, various examples, and the proof of the compatibility with the functional equation.

Consider the compatible system $\mathbb{Q}(k) = \{\mathbb{Q}_l(k)\}$ for $k \in \mathbb{Z}$, where $\mathbb{Q}_l(k)$ is the 1-dimensional $\mathbb{Q}_l$-vector space on which $G_{\mathbb{Q}}$ acts by χ_l^k, χ_l being the l-power cyclotomic character. Then $\mathbb{Q}_p(k)$ satisfies the ordinariness condition and $F^+\mathbb{Q}_p(k) = \mathbb{Q}_p(k)$ if $k \geq 1$, $F^+\mathbb{Q}_p(k) = 0$ if $k \leq 0$. Let $\Sigma = \{p, \infty\}$ and let $A = \mathbb{Q}_p(k)/\mathbb{Z}_p(k)$. Then

$$S_A(\mathbb{Q}_\infty) = H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, A) \qquad \text{if } k \geq 1$$
$$S_A(\mathbb{Q}_\infty) = H^1_{\text{unr}}(\mathbb{Q}_\infty, A) \qquad \text{if } k \leq 0$$

where $H^1_{\text{unr}}(\mathbb{Q}_\infty, A) = \ker(H^1(\mathbb{Q}_\infty, A) \to \prod_v H^1(I_v, A))$, where v varies over all primes of $\mathbb{Q}_\infty$. This is the group of everywhere unramified cocycle classes. Assuming that p is odd, the restriction map $H^1(\mathbb{Q}_\infty, A) \to H^1(F_\infty, A)^\Delta$ is an isomorphism, where $F_\infty = \mathbb{Q}(\mu_{p^\infty})$ and $\Delta = \mathrm{Gal}(F_\infty/\mathbb{Q}_\infty)$. Now $H^1(F_\infty, A)^\Delta = \mathrm{Hom}_\Delta(\mathrm{Gal}(F_\infty^{\text{ab}}/F_\infty), A)$. The action of Δ on A is by the character ω^k. Using the notation of section 1, we have

$$S_A(\mathbb{Q}_\infty) \cong \mathrm{Hom}(Y^{\omega^k}, A) \qquad \text{if } k \geq 1,$$
$$S_A(\mathbb{Q}_\infty) \cong \mathrm{Hom}(X^{\omega^k}, A) \qquad \text{if } k \leq 0,$$

where the isomorphisms are Λ-module isomorphisms and come from the natural restriction maps.

If $k \geq 1$ and is odd, then $S_A(\mathbb{Q}_\infty)$ has Λ-corank 1 since it is just the Pontryagin dual of Y^{ω^k} with the Λ-module structure twisted in a simple way (by κ^{-k}). For all other $k \in \mathbb{Z}$, $S_A(\mathbb{Q}_\infty)$ is Λ-cotorsion. (Vandiver's conjecture implies that $S_A(\mathbb{Q}_\infty) = 0$ if $k \leq 0$ and is even. Conjecture 3.4 would imply that $S_A(\mathbb{Q}_\infty)$ is finite in this case.)

Now $L(z, \mathbb{Q}(k)) = \zeta(z-k)$. The corresponding gamma-factor is $\Gamma(\frac{z-k}{2})$ and we see that $r_V = 1$ if $k \geq 1$ and is odd, but that $r_V = 0$ otherwise. Also, $\mathbb{Q}(k)^* = \mathbb{Q}(1-k)$. Thus $L(1, \mathbb{Q}(k))$ is a critical value if and only if k is either a positive even integer or a negative odd integer. In either case one can use the Kubota-Leopoldt p-adic L-function to define both $L_p(s, \mathbb{Q}(k))$ and the corresponding element $\theta_{\mathbb{Q}(k)}$ (which is in Λ if $\omega^k \neq \omega^0$ or ω^1) in a precise way. One also finds that Conjecture 7.1 is then equivalent to conjecture 4.4 when $k \leq 0$ and to conjecture 4.5 when $k \geq 1$. For more details about this equivalence we refer the reader to section 1 of [Gr4].

Let E be a modular elliptic curve/$\mathbb{Q}$ with good, ordinary reduction at p. This means equivalently that $p \nmid a_p$, where $a_p = a_p(E)$ denotes the p-th Fourier coefficient for the newform f_E attached to E. Consider the compatible system $V(E) = \{V_l(E)\}$, where $V_l(E) = T_l(E) \otimes \mathbb{Q}_l$ and $T_l(E)$ is the l-adic Tate module for E. As a $G_{\mathbb{Q}_p}$-representation space, $V_p(E)$ does have a natural filtration. If $\widetilde{E}$ is the reduction of E modulo p, then $T_p(\widetilde{E}) \cong \mathbb{Z}_p$ since $\widetilde{E}$ is ordinary. The map $V_p(E) \to V_p(\widetilde{E})$ is surjective and the inertia group I_p acts trivially on $V_p(\widetilde{E})$. If $F^1V_p(E)$ denotes the kernel of this map, then I_p acts by χ_p on F^1V_p (because of the Weil pairing). Thus one can take $F^0V_p(E) = V_p(E)$, $F^2V_p(E) = 0$, and so p is indeed an ordinary prime for $V(E)$. We have $A = V_p(E)/T_p(E) \cong E[p^\infty]$, the p-power torsion on E, and $S_{E[p^\infty]}(\mathbb{Q}_\infty)$ is a certain Λ-module. It turns out that

$$\mathrm{Sel}_E(\mathbb{Q}_\infty)_p = S_{E[p^\infty]}(\mathbb{Q}_\infty).$$

This will be explained later. On the other hand, $L(1, V(E), \rho) = L(1, E, \rho)$ for all $\rho \in \widehat{\Gamma}$, and hence we can just define $L_p(s, V(E))$ to be $L_p(s, E)$, the p-adic L-function constructed by Mazur and Swinnerton-Dyer. This also gives the right normalization: the period involved in the interpolation property defining $L_p(s, V(E))$ should be the real Neron period Ω_E for E (which also occurs in the precise formulation of the Birch and Swinnerton-Dyer conjecture). Therefore, Mazur's conjecture is equivalent to conjecture 7.1 when $V = V(E)$ and the p-adic L-function is as defined in [M-SwD].

Now consider $V = V(f_{12}) = \{V_l(f_{12})\}$, the compatible system of l-adic representations defined by Deligne for the unique newform f_{12} of weight 12 and level 1. The corresponding complex L-function is

$$L(z, V) = L(z, V(f_{12})) = L(z, f_{12}) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^z}$$

where $\tau(n)$ is Ramanujan's tau-function and where the Dirichlet series expression is valid for $\mathcal{R}e(z) > \frac{13}{2}$. The functional equation relates the values $L(z, V)$ and $L(12 - z, V)$. The gamma-factor is simply $\Gamma(z)$. The critical values of $L(z, V)$ are therefore $L(j, V)$ for integral j, $1 \leq j \leq 11$. For each such j and for any prime p, there is a p-adic L-function defined by an interpolation property involving the values $L(j, V, \rho)$ for $\rho \in \widehat{\Gamma}$. But one can view these values as $L(1, V(1-j), \rho)$, where $V(t) = \{V_l(t)\}$ denotes the t-th Tate twist. (That is, $V_l(t) = V_l \otimes \chi_l^t$). The functional equation then relates $L(1, V(1-j), \rho)$ to $L(1, V(1-j'), \rho^{-1})$ for $j + j' = 12$, reflecting the fact that $V(1-j)^* = V(1-j')$ because the determinant of V_l is χ_l^{11}. Manin and Vishik found that the corresponding p-adic L-functions $L_p(s, V(1-j))$, $1 \leq j \leq 11$, are associated to a bounded measure on Γ and hence to an element of Λ (choosing a suitable period) precisely when $p \nmid \tau(p)$. Thus if $p \nmid \tau(p)$, one can define elements $\theta_{V(1-j)}$ in Λ for each such j.

In early 1986 I asked Ken Ribet the following question: if p is a prime such that $p \nmid \tau(p)$, then does $V_p = V_p(f_{12})$ have a 1-dimensional unramified quotient when considered as a $\mathbb{Q}_p$-representation space for $G_{\mathbb{Q}_p}$, just as is the case for $V_p(E) = V_p(f_E)$ when E is a modular elliptic curve and $p \nmid a_p(E)$? He told me that Mazur and Wiles had just recently proved such a result. (It can be found in [M-W2] and also in a more explicit and general form in [Wi1].) This result was crucial to my speculations at the time because it would then follow that $V_p(1-j)$ had a 1-dimensional quotient on which I_p acts by χ_p^{1-j}. That is, if $V = V(f_{12})$ and $p \nmid \tau(p)$, then V is ordinary in the sense defined earlier. Furthermore, since the determinant for V_p is χ_p^{11}, it would follow that $F^+V_p(1-j)$ is 1-dimensional precisely when $1 \leq j \leq 11$ (because I_p acts on the composition factors for $V_p(1-j)$ (as a representation space for $G_{\mathbb{Q}_p}$) by χ_p^{1-j} and χ_p^{12-j}. If T_p is a $G_{\mathbb{Q}}$-invariant $\mathbb{Z}_p$-lattice in V_p, then we let $A(1-j) = V_p(1-j)/T_p(1-j)$. We then have $A(1-j)^* \cong A(1-j')$ where $j + j' = 12$. If $j \leq 0$, then $F^+A(1-j) = A(1-j)$ and it is not hard to show that $S_{A(1-j)}(\mathbb{Q}_\infty)$ cannot be Λ-cotorsion. On the other hand, if $j \geq 12$, then

$j' \leq 0$ and $S_{A(j-1)^*}(\mathbb{Q}_\infty)$ cannot be Λ-cotorsion. Both of these Selmer groups could possibly be Λ-cotorsion if $1 \leq j \leq 11$. This seemed quite encouraging.

It may be worthwhile to recount some of the considerations which led me to ask Ribet that question about $V_p(f_{12})$. During the academic year 1985–86 I was visiting l'Université de Paris-Sud. In the Fall of that year, John Coates described to me his recent work with Claus Schmidt in which they construct a p-adic analogue of $L(z, \mathrm{Sym}^2(E))$ and formulate a corresponding main conjecture under the assumption that E is a modular elliptic curve with good, ordinary reduction at p. They could verify that if E is an elliptic curve/$\mathbb{Q}$ with complex multiplication, then the two-variable main conjecture (mentioned at the end of section 5) would imply their conjecture. Their formulation involved an Iwasawa module defined in terms of the Selmer group for E over the field $\mathbb{Q}(E[p^\infty])$ and did not suggest a way to formulate a main conjecture for $L_p(s, f_{12})$, an example which especially interested me. But that Winter I recall looking at some numerical data given in Manin's paper [Man]; namely, he writes

$$(r_0 : r_2 : r_4) = (1 : -\frac{691}{2^2 \cdot 3^4 \cdot 5} : \frac{691}{2^3 \cdot 3^2 \cdot 5 \cdot 7})$$

where $r_{j-1} = \frac{(j-1)! i^j}{(2\pi)^j} L(j, f_{12})$ and the expression indicates ratios of these numbers. What did those 691s mean? Were they related to the fact that T_p/pT_p is a reducible $\mathbb{F}_p$-representation of $G_\mathbb{Q}$ if $p = 691$? Manin also gives similar data for the other newforms f_{16}, f_{18}, f_{20}, f_{22} and f_{26} of level 1 with rational Fourier coefficients and the same pattern continued. It seemed reasonable to guess that the corresponding p-adic L-functions might have a positive μ-invariant, i.e., $\theta_{V(1-j)} \in p\Lambda$ for $j = 3$ and 5. This would assume that one chose a period Ω so that $L(1, f_{12})/\Omega = 1$, but even then the interpolation property defining $L_p(s, f_{12})$ would imply that $p | L_p(1, f_{12})$ for $p = 691$ because $(1 - \alpha_p^{-1})$ would be a factor. Here $\alpha_p \in \mathbb{Z}_p^\times$ is the p-adic unit root of $x^2 - \tau(p)x + p^{11}$ and so $\alpha_p \equiv \tau(p) \equiv 1 \pmod{p\mathbb{Z}_p}$ for $p = 691$. Thus, perhaps $\theta_{V(1-j)} \in p\Lambda$ for $j = 1$ too. For an elliptic curve $E/\mathbb{Q}$ with good, ordinary reduction at p, Mazur had given many examples where the Λ-module $\widehat{\mathrm{Sel}_E(\mathbb{Q}_\infty)_p}$ has a positive μ-invariant. In those examples, $E[p] = T_p(E)/pT_p(E)$ is always $G_\mathbb{Q}$-reducible and, more precisely, possesses a $G_\mathbb{Q}$-invariant subgroup isomorphic to μ_p. It occurred to me that there would then be a natural map with finite kernel from $H^1(\mathbb{Q}_\infty, \mu_p)$ to a subgroup of $H^1(\mathbb{Q}_\infty, E[p^\infty])$ and perhaps that might be the source of the positive μ-invariant. The fact that $T_p(f_{12})/pT_p(f_{12})$ would have a $G_\mathbb{Q}$-invariant subgroup isomorphic to $\mu_p^{\otimes 11}$ if the $\mathbb{Z}_p$-lattice $T_p(f_{12})$ was chosen suitably and that this might also account for a positive μ-invariant turned out to be another helpful clue.

These hints led me to look closely at the definition of the Selmer group for an elliptic curve E over $\mathbb{Q}_\infty$. Its p-primary subgroup is defined by

$$\mathrm{Sel}_E(\mathbb{Q}_\infty)_p = \ker\big(H^1(\mathbb{Q}_\infty, E[p^\infty]) \to \prod_v H^1((\mathbb{Q}_\infty)_v, E[p^\infty])/Im(\kappa_v)\big)$$

where $\kappa_v : E((\mathbb{Q}_\infty)_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1((\mathbb{Q}_\infty)_v, E[p^\infty])$ is the local Kummer homomorphism for E over $(\mathbb{Q}_\infty)_v$. If $v|l$ where $l \neq p$, then it turns out that $Im(\kappa_v) = 0$. This is quite easy to prove. For if L is any finite extension of $\mathbb{Q}_l$, then $E(L)$ contains a subgroup of finite index isomorphic to $\mathbb{Z}_l^{[L:\mathbb{Q}_l]}$. This subgroup is divisible by p and so it follows that $E(L) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. This immediately implies that $E((\mathbb{Q}_\infty)_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ and hence $Im(\kappa_v) = 0$ for $v \nmid p$. Let π be the unique prime of $\mathbb{Q}_\infty$ lying over p. Let I_π denote the inertia subgroup of $G_{(\mathbb{Q}_\infty)_\pi}$. Then it turns out that

$$\begin{aligned} Im(\kappa_\pi) &= \ker\big(H^1((\mathbb{Q}_\infty)_\pi, E[p^\infty]) \to H^1((\mathbb{Q}_\infty)_\pi, \widetilde{E}[p^\infty])\big) \\ &= \ker\big(H^1((\mathbb{Q}_\infty)_\pi, E[p^\infty]) \to H^1(I_\pi, \widetilde{E}[p^\infty])\big). \end{aligned}$$

The equivalence of these descriptions follows from the easily verified fact that the map $H^1((\mathbb{Q}_\infty)_\pi, \widetilde{E}[p^\infty]) \to H^1(I_\pi, \widetilde{E}[p^\infty])$ is injective. One inclusion can be proved by observing that if $g \in I_p = G_{\mathbb{Q}_p^{\mathrm{unr}}}$ and if $P \in E(\overline{\mathbb{Q}}_p)$, the $g(P) - P$ must be in the kernel of the reduction map $E(\overline{\mathbb{Q}}_p) \to \widetilde{E}(\overline{\mathbb{F}}_p)$. It then follows that any element of $Im(\kappa_\pi)$ becomes trivial in $H^1(I_\pi, \widetilde{E}[p^\infty])$. Coates and I managed to prove the equality. For a complete proof see [Gr5], or [C-G] where the local Kummer maps are studied in a more general context. The fact that $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p = S_{E[p^\infty]}(\mathbb{Q}_\infty)$ follows from these considerations. In particular, if $E[p]$ contains a $G_\mathbb{Q}$-invariant subgroup isomorphic to μ_p, then it becomes rather clear that the image of $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p)$ (where $\Sigma = \{p, \infty\}$) in $H^1(\mathbb{Q}_\infty, E[p^\infty])$ is contained in $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$. Elements of this image are unramified at all $v \nmid p$ and are also contained in $Im(\kappa_\pi)$ because of the above description. But it is quite easy to see that $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p)$ is isomorphic to the Λ-module $\mathrm{Hom}(X^{\omega^1}/pX^{\omega^1}, \mu_p)$ and therefore has $(\Lambda/p\Lambda)$-corank equal to 1. This shows that $\widehat{\mathrm{Sel}_E(\mathbb{Q}_\infty)_p}$ has positive μ-invariant. Similarly, $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_p^{\otimes 11})$ is isomorphic to $\mathrm{Hom}(X^{\omega^{11}}/pX^{\omega^{11}}, \mu_p^{\otimes 11})$ and this also has $(\Lambda/p\Lambda)$-corank equal to 1. Since, as Ribet informed me, $V_p(f_{12})$ does have a suitable filtration and we would clearly have $\mu_p^{\otimes 11} \subset F^+A$ (when $A = V_p(f_{12})/T_p(f_{12})$ and $T_p(f_{21})$ is chosen as before), it again follows that the μ-invariant of $\widehat{S_A(\mathbb{Q}_\infty)}$ is positive.

8. In the past decade Perrin-Riou has made considerable progress in developing Iwasawa theory in the "non-ordinary" case. The first example to consider is $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ when E is an elliptic curve/$\mathbb{Q}$ with good, supersingular reduction at p. It was realized in the early 1970s that $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ is not Λ-cotorsion, and so $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p^{\Gamma_n}$ has unbounded $\mathbb{Z}_p$-corank as $n \to \infty$. In contrast, it is reasonable to conjecture that $\mathrm{Sel}_E(\mathbb{Q}_n)_p$ has bounded $\mathbb{Z}_p$-corank for $n \geq 0$. In [Pe3], Perrin-Riou proves this under the hypothesis that $\mathrm{Sel}_E(\mathbb{Q})_p$ is finite and $p \geq 5$. If E is modular, the boundedness of $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_E(\mathbb{Q}_n)_p)$ has been proven by Kato. In either case, it is clear that the analogue of theorem 5.2 would be false. On the analytic side, a p-adic L-function $L_p(s, E)$ for E was also constructed in the early 1970s. (Vishik, Manin, and Amice-Vela studied the existence of p-adic analogues of the complex L-functions attached to new forms of arbitrary weight. See [Man] and [M-T-T].) But $L_p(s, E)$ is not an Iwasawa function if E has supersingular reduction at p. (That is, $L_p(s, E)$ does not correspond to an element $\theta_E \in \Lambda$ as it does in the ordinary case.) In fact, Vishik proved that $L_p(s, E)$ must have infinitely many zeros for $s \in \overline{\mathbb{Q}}_p$, $|s|_p < 1$, and Rohrlich's nonvanishing theorem [Ro] shows that $L_p(s, E)$ is not identically zero.

Let α and β denote the two inverse roots of the zeta function for $\widetilde{E}$, the reduction of E modulo p. Since $\widetilde{E}$ is supersingular, α and β both have p-adic valuation $\frac{1}{2}$. There are actually two distinct p-adic L-functions, $L_p^{(\alpha)}(s, E)$ and $L_p^{(\beta)}(s, E)$. Perrin-Riou constructs algebraic analogues for these p-adic L-functions in [Pe3] and formulates a main conjecture. There are numerous unsolved questions. It is not clear what the zeros of these p-adic L-functions or their algebraic analogues really mean, except for those zeros corresponding to a character of $\Gamma = \mathrm{Gal}\,(\mathbb{Q}_\infty/\mathbb{Q})$ of finite order. What do the common zeros mean? (They should conjecturally be a finite set.) It would be important to verify some special cases of the main conjecture. (For example, if E has complex multiplication, then Rubin has proven some deep results in [Ru1, 2] which would seem to be closely related. Also, recent work of Kato connecting these p-adic L-functions to certain Euler systems should be helpful.) In Perrin-Riou's subsequent papers, she refines and extends her theory, developing a rather elegant formulation in terms of the Bloch-Kato logarithms which map Galois cohomology groups to Dieudonné modules. The details are difficult and we refer the reader to [Pe4], [Pe5], and the references to be found in those articles.

We have neglected to discuss the link between algebraic K-theory for rings of integers of number fields and Iwasawa theory. This was discovered by Tate for K_2 in the early 1970s. More generally, the relationship arises from the Chern maps

$$ch_{i,1} : K_{2i-1}(\mathcal{O}_F) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to H^1(F_\Sigma/F, \mathbb{Z}_p(i))$$
$$ch_{i,2} : K_{2i-2}(\mathcal{O}_F) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to H^2(F_\Sigma/F, \mathbb{Z}_p(i))$$

for $i \geq 2$. Here $\mathcal{O}_F$ denotes the ring of integers of a number field F, F_Σ denotes the maximal extension of F unramified outside $\Sigma = \{p, \infty\}$, p is any odd prime, and $\mathbb{Z}_p(i)$ denotes a free $\mathbb{Z}_p$-module of rank 1 on which $\mathrm{Gal}\,(F_\Sigma/F)$ acts by χ^i, where χ is the p-power cyclotomic character. It has been proven that the Chern maps are surjective. (Soulé for $i \leq p$, Dwyer-Friedlander for arbitrary i.) This means that theorems about the K-groups will give results about the above Galois cohomology groups which can then be interpreted in terms of Iwasawa theory. We will mention two specific results which I believe have never been proven in any other way. Assume for simplicity that $\mu_p \subset F$. Then $F_\infty = F(\mu_{p^\infty})$ is the cyclotomic $\mathbb{Z}_p$-extension of F. Let $X = \mathrm{Gal}\,(L_\infty/F_\infty)$, just as at the beginning of this article. Let $f_X(T)$ be the characteristic polynomial of X (with $T = \gamma_0 - 1$) and let $\chi(\gamma_0) = u_0$. As a consequence of a theorem of Borel asserting that $K_m(\mathcal{O}_F)$ is finite for even $m \geq 2$, it follows that $H^2(F_\Sigma/F, \mathbb{Z}_p(i))$ is finite, and Soulé proves in [So] that this implies that $f_X(u_0^{1-i} - 1) \neq 0$ for all $i \geq 2$. Secondly, Lee and Szczarba proved in 1978 that the order of $K_4(\mathbb{Z})$ was not divisible by any prime $p > 3$. Thus, $H^2(F_\Sigma/F, \mathbb{Z}_p(3)) = 0$ for $p \geq 5$. In [Ku1], Kurihara deduces from this the useful result that $S_0^{\omega^{p-3}} = 0$. Here the notation is the same as in section 2, where $F = \mathbb{Q}(\mu_p)$.

There are many other topics which have been overlooked in this article. The literature in Iwasawa theory has become quite vast over the years. The following list of references includes just a sampling of this literature. In addition to papers cited in the text, we have included various others which provide an introduction to important topics and also include many valuable references themselves. Thus, indirectly, we hope that this list will be rather comprehensive.

References

[BCEM] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, Irregular primes and cyclotomic invariants to four million, *Math. of Comp.* **61** (1993), 151–153.

[Ca] P. Cassou-Nogués, Valeurs aux entiers negatifs des fonctions zeta et fonctions zeta p-adiques, *Inv. Math.* **51** (1979), 29–59.

[Co1] J. Coates, On K_2 and some classical conjectures in algebraic number theory, *Ann. of Math.* **95** (1972), 99–116.

[Co2] J. Coates, p-adic L-functions and Iwasawa's theory, in *Algebraic Number Fields*, Academic Press (1977), 264–353.

[Co3] J. Coates, The work of Mazur and Wiles on cyclotomic fields, *Seminaire Bourbaki*, Lecture Notes in Math. **901** (1981), 220–242.

[Co4] J. Coates, On p-adic L-functions, *Seminaire Bourbaki* no. 701 (1988), Astérisque 177–178 (1989), 33–59.

[C-G] J. Coates, R. Greenberg, Kummer theory for abelian varieties over local fields, *Inv. Math.* **124** (1996), 129–174.

[C-L] J. Coates, S. Lichtenbaum, On l-adic zeta functions, *Ann. of Math.* **98** (1973), 498–550.

[C-P] J. Coates, B. Perrin-Riou, On p-adic L-functions attached to motives over $\mathbb{Q}$, in Algebraic Number Theory—in honor of K. Iwasawa, *Adv. Stud. in Pure Math.* **17** (1989), 23–54.

[C-S] J. Coates, C-G. Schmidt, Iwasawa theory for the symmetric square of an elliptic curve, *Jour. reine angew. Math.* **375** (1987), 104–156.

[C-W1] J. Coates, A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Inv. Math.* **39** (1977), 223–251.

[C-W2] J. Coates, A. Wiles, On p-adic L-functions and elliptic units, *J. Austral. Math. Soc.* **26** (1978), 1–25.

[Col1] R. Coleman, Division values in local fields, *Inv. Math.* **53** (1979), 91–116.

[Col2] R. Coleman, Dilogarithms, regulations, and p-adic L-functions, *Inv. Math.* **69** (1982), 171–208.

[Colm] P. Colmez, Résidu en $s = 1$ des fonctions zeta p-adiques, *Inv. Math.* **91** (1988), 371–389.

[Cu-M] A. Cuoco, P. Monsky, Class numbers in $\mathbb{Z}_p^d$-extensions, *Math. Ann.* **225** (1981), 235–258.

[DFKS] D. Dummit, D. Ford, H. Kisilevsky, J. Sands, Computation of Iwasawa lambda invariants for imaginary quadratic fields, *J. Number Theory* **37** (1991), 100–121.

[deS] E. de Shalit, Iwasawa Theory of Elliptic Curves with Complex Multiplication, in *Perspectives in Math. 3*, Academic Press (1987).

[F-W] B. Ferrero, L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377–395.

[Fu] T. Fukuda, Iwasawa λ-invariants of imaginary quadratic fields I, II, III, *J. College of Industrial Technology* **27** (1994).

[F-K] T. Fukuda, K. Komatsu, On $\mathbb{Z}_p$-extensions of real quadratic fields, *J. Math. Soc. Japan* **38** (1986), 95–102.

[Gi] R. Gillard, Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abéliennes, *J. reine angew. Math.* **327** (1985), 76–91.

[G-K] R. Gold, H. Kisilevsky, On geometric $\mathbb{Z}_p$-extensions of function fields, *Manuscripta Math.* **62** (1988), 145–161.

[Gr1] R. Greenberg, On some questions concerning the Iwasawa invariants, Princeton University thesis (1971).

[Gr2] R. Greenberg, On p-adic L-functions and cyclotomic fields I, II, *Nagoya Math. J.* **56** (1974), 61–77, **67** (1977), 138–158.

[Gr3] R. Greenberg, On the Iwasawa invariants of totally real number fields, *Amer. J. of Math.* **98** (1976), 263–284.

[Gr4] R. Greenberg, Iwasawa theory for p-adic representations, in *Algebraic Number Theory—in honor of K. Iwasawa*, *Adv. Stud. in Pure Math.* **17** (1989), 97–137.

[Gr5] R. Greenberg, Iwasawa theory for elliptic curves, to appear in *Lect. Notes in Math.*

[Gr6] R. Greenberg, Iwasawa theory and p-adic deformations of motives, *Symposia in Pure Math.* **55** (1994), part 2, 193–223.

[Gr7] R. Greenberg, Trivial zeros of p-adic L-functions, *Contemporary Math.* **165** (1994), 149–179.

[H] H. Hida, Elementary theory of L-functions and Eisenstein Series, *London Mathematical Society Student Texts* **26** (1993), Cambridge University Press.

[H-T] H. Hida, J. Tilouine, On the anticyclotomic main conjecture for CM fields, *Inv. Math.* **117** (1994), 89–147.

[Ic-S] H. Ichimura, H. Sumida, On the Iwasawa invariants of certain real abelian fields, *Tôhoku Math. J.* **49** (1997), 203–215.

[Iw1] K. Iwasawa, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Hamburg* **20** (1956), 257–258.

[Iw2] K. Iwasawa, On some invariants of cyclotomic fields, *Amer. J. of Math.* **80** (1958), 773–783.

[Iw3] K. Iwasawa, On Γ-extensions of algebraic number fields, *Bull. Amer. Math. Soc.* **65** (1959), 183–226.

[Iw4] K. Iwasawa, On some properties of Γ-finite modules, *Ann. of Math.* **70** (1959), 291–312.

[Iw5] K. Iwasawa, On the theory of cyclotomic fields, *Ann. of Math.* **70** (1959), 530–561.

[Iw6] K. Iwasawa, A class number formula for cyclotomic fields, *Ann. of Math.* **76** (1962), 171–179.

[Iw7] K. Iwasawa, On some modules in the theory of cyclotomic fields, *J. Math. Soc. Japan* **16** (1964), 42–82.

[Iw8] K. Iwasawa, Analogies between number fields and function fields, in *Some Recent Advances in the Basic Sciences* **2** (1969), 203–208, Yeshiva University.

[Iw9] K. Iwasawa, On p-adic L-functions, *Ann. of Math.* **89** (1969), 198–205.

[Iw10] K. Iwasawa, Lectures on p-adic L-functions, *Ann. of Math. Stud.* **74**, Princeton University Press (1972).

[Iw11] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields, *Ann. of Math.* **98** (1973), 246–326.

[Iw12] K. Iwasawa, On the μ-invariants of $\mathbb{Z}_l$-extensions, *Number Theory, Algebraic Geometry, and Commutative Algebra*, in honor of Y. Akizuki, Kinokuniga, Tokyo (1973), 1–11.

[Iw13] K. Iwasawa, Riemann-Hurwitz formula and p-adic Galois representations for number fields, *Tôhoko Math. J.* **33** (1981), 263–288.

[Iw-S] K. Iwasawa, C. Sims, Computation of invariants in the theory of cyclotomic fields, *J. Math. Soc. Japan* **18** (1966), 86–96.

[K] K. Kato, Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR} in Arithmetic Algebraic Geometry, *Lecture Notes in Math.* **1553** (1994), 50–163.

[Ka] N. Katz, p-adic L-functions for CM fields, *Inv. Math.* **49** (1978), 199–297.

[Ki] Y. Kida, l-extensions of CM-fields and cyclotomic invariants, *J. Number Theory* **12** (1980), 519–528.

[Kis] H. Kisilevsky, Some non-semisimple Iwasawa modules, *Comp. Math.* **49** (1983), 399–404.

[K-N] M. Kolster, T. Nguyen Quang Do, Syntomic regulators and special values of p-adic L-functions, *Inv. Math.* **133** (1998), 417–447.

[K-L] T. Kubota, H. W. Leopoldt, Eine p-adische Theorie der Zetawerte, *J. reine angew. Math.* **214** (1964), 328–339.

[K-S] J. Kraft, R. Schoof, Computing Iwasawa modules of real quadratic fields, *Comp. Math.* **97** (1995), 135–155.

[Ku1] M. Kurihara, Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbb{Z}$, *Comp. Math.* **81** (1992), 223–236.

[Ku2] M. Kurihara, The Iwasawa λ-invariants of real abelian fields and the cyclotomic elements, to appear in *Tokyo Jour. of Math.*

[L-N] A. Lannuzel, T. Nguyen Quang Do, Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres, in this volume.

[Man] J. I. Manin, Periods of parabolic forms and p-adic Hecke series, *Math. USSR Sbornik* **21** (1973), 371–393.

[M-V] J. Manin, M. Visik, p-adic Hecke series of imaginary quadratic fields, *Math. USSR-Sbornik* **24** (1974), 345–371.

[Maz1] B. Mazur, Rational points of abelian varieties with values in tower of number fields, *Inv. Math.* **18** (1972), 183–266.

[Maz2] B. Mazur, Modular Curves and Arithmetic, *Proceedings of the International Conference of Mathematicians*, Warszawa (1983).

[M-SwD] B. Mazur, H. Swinnerton-Dyer, Arithmetic of Weil curves, *Inv. Math.* **25** (1974), 1-61.

[M-T] B. Mazur, J. Tilouine, Représentations galoisiennes, différentielles de Kähler et conjectures principales, *Publ. Math., IHES* **71** (1990), 65–103.

[M-T-T] B. Mazur, J. Tate, J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Inv. Math.* **84** (1986), 1–48.

[M-W1] B. Mazur, A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Inv. Math.* **76** (1984), 179–330.

[M-W2] B. Mazur, A. Wiles, On p-adic analytic families of Galois representations, *Comp. Math.* **59** (1986), 231–264.

[N] T. Nguyen Quang Do, Galois module structure of p-class formations, this volume.

[O-T] M. Ozaki, H. Taya, A note on Greenberg's conjecture for real abelian number fields, *Manuscripta Math.* **88** (1995), 311–320.

[Pe1] B. Perrin-Riou,Arithmetique des courbes elliptiques et théorie d'Iwasawa, *Bull. Soc. Math. Fr.* **17** (1984).

[Pe2] B. Perrin-Riou, Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner, *Bull. Soc. Math. France* **115** (1987), 399–456.

[Pe3] B. Perrin-Riou, Théorie d'Iwasawa p-adique locale et globale, *Inv. Math.* **99** (1990), 247–292.

[Pe4] B. Perrin-Riou, Fonctions L p-adiques des representations p-adiques, *Astérisque* **229** (1995).

[Pe5] B. Perrin-Riou, Fonctions L p-adiques, *Proceedings of the International Conference of Mathematics*, Zurich (1994), 400–410.

[Po] F. Pollaczek, Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswurzeln, *Math. Zeit.* **21** (1924), 1–38.

[Ro] D. Rohrlich, On L-functions of elliptic curves and cyclotomic towers, *Inv. Math.* **75** (1984), 409–423.

[Ru1] K. Rubin, Elliptic Curves and $\mathbb{Z}_p$-extensions, *Comp. Math.* **56** (1985), 237–250.

[Ru2] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Inv. Math.* **103** (1991), 25–68.

[Ru3] K. Rubin, The main conjecture. Appendix to: *Cyclotomic Fields I–II* by S. Lang, Graduate Texts in Math 121, Springer-Verlag (1990).

[Ru4] K. Rubin, Euler Systems, Hermann Weyl Lectures, to appear.

[Sc] L. Schneps, On the μ-invariant of p-adic L-functions attached to elliptic curves with complex multiplication, *J. Number Theory* **25** (1987), 20–33.

[Sch1] P. Schneider, Iwasawa L-functions of varieties over algebraic number fields, A first approach, *Inv. Math.* **71** (1983), 251–293.

[Sch2] P. Schneider, p-adic height pairings II, *Inv. Math.* **79** (1985), 329–374.

[Se1] J. P. Serre, Classes des corps cyclotomique (d'après K. Iwasawa), *Seminaire Bourbaki* no. 174 (1959).

[Se2] J. P. Serre, Une interpretation des congruences relatives à la fonction τ de Ramanujan, *Seminaire Delange-Pisot-Poitou*, 1967.

[Si] W. Sinnott, On the μ-invariant of the Γ-transform of a rational function, *Inv. Math.* **75** (1984), 273–282.

[So] C. Soulé, Elements cyclotomiques en K-théorie, *Astérisque* **147–148** (1987), 225–257.

[T] T. Takagi, Zur Theorie der Kreiskörpers, *Jour. reine angew. Math.* **157** (1927), 230–238.

[Ti] J. Tilouine, Théorie d'Iwasawa classique et de l'algèbre de Hecke ordinaire, *Comp. Math.* **65** (1988), 265–320.

[Wa1] L. Washington, The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension, *Inv. Math.* **49** (1978), 87–97.

[Wa2] L. Washington, Introduction to Cyclotomic Fields, *Grad. Texts in Math.* **83** (1980), Springer-Verlag.

[Wi1] A. Wiles, On ordinary λ-adic representations associated to modular forms, *Inv. Math.* **94** (1988), 529–573.

[Wi2] A. Wiles, The Iwasawa conjecture for totally real fields, *Ann. of Math.* **131** (1990), 493–540.

[Win] K. Wingberg, Duality theorems for Γ-extensions of algebraic number fields, *Comp. Math.* **55** (1985), 333–381.

[Y] R. Yager, On two-variable p-adic L-functions, *Ann. of Math.* **115** (1982), 411–449.