Iwasawa theory report

August 3, 2025

In writing this report, I relied heavily on the following sources: 'An introduction to cyclotomic fields' by Lawrence Washington and 'Iwasawa Theory - Past and Present' by Ralph Greenberg.

Introduction

Cyclotomic extensions $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$, where ζ_n is a primitive n^{th} root of unity, (or more generally, extensions of a number field obtained by adjoining a root of unity) play a very important role in number theory. For example, in the proofs of class field theory, many statements are first proved in the case of finite, cyclic extensions and then deduced the more general case. Cyclic extensions can also be used as a testing ground for theorems since they are well understood and relatively easy to work with.

The study of such fields led to Kummer's proof of Fermat's last theorem in the following special case.

Theorem 0.1. *If p is an odd, regular prime (i.e. p does not divide the class number of $\mathbb{Q}(\zeta_p)$), then $x^p + y^p = z^p$ has no solution with $(xyz, p) = 1$ and $x, y, z \in \mathbb{Z}$.*

While working on Fermat's last theorem, Kummer discovered that there is a connection between the arithmetic of the field $\mathbb{Q}(\zeta_p)$ and the values of the Riemann Zeta function $\zeta(s)$ for s taking values that are odd, negative integers. He discovered that that p is a regular prime if and only if it does not divide the numerator of any of the values $\zeta(-1), \zeta(-3), \ldots, \zeta(4-p)$.

The Riemann Zeta function is a special case of an L-function. There is also a theory of p-adic L functions. In the 60s, Iwasawa developed the theory of $\mathbb{Z}_p$-extensions. He related such extensions to p-adic L-functions. In 1979, Mazur and Wiles proved Iwasawa's main conjecture, showing that p-adic L-functions are essentially characteristic power series arising from Galois actions on $\mathbb{Z}_p$-extensions.

Aside from this, there are strong analogues between the theory of function fields of curves and $\mathbb{Z}_p$-extensions, which Iwasawa often emphasised. Iwasawa theory has become an important tool in modern number theory. In particular, much of the progress towards the Birch-Swinnerton Dyer conjecture to date can be attributed to tools from Iwasawa theory.

$\mathbb{Z}_p$-extensions and the Iwasawa Algebra

A $\mathbb{Z}_p$-extension of a number field F is a Galois extension F_∞/F with $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$.

Let Γ be the multiplicative topological group isomorphic to the additive group $\mathbb{Z}_p$ with γ being a fixed topological generator corresponding to 1 in $\mathbb{Z}_p$. Closed subgroups of $\mathbb{Z}_p$ are precisely those of the form $p^n\mathbb{Z}_p$, corresponding to closed subgroups of Γ of the form Γ^{p^n}. Let $\Gamma_n = \Gamma/\Gamma^{p^n}$ = cyclic group of order p^n.

Let O be the ring of integers of a finite extension of $\mathbb{Q}_p$. There is a natural isomorphism $O[\Gamma_n] \cong O[T]/((1+T)^{p^n}-1)$ via $\gamma \bmod T^{p^n} \longmapsto 1+T \bmod \left((1+T)^{p^n}-1\right)$. Moreover, using the fact that $(1+T)^{p^n}-1$ divides $(1+T)^{p^m}-1$ for $m \geq n \geq 0$, we have natural maps $\phi_{m,n} : O[\Gamma_m] \to O[\Gamma_n]$ induced by the natural maps $\Gamma_m \to \Gamma_n$.

Taking the inverse limit with respect to the $\phi_{m,n}$, we get the profinite group ring $O[T]$ of T. We obtain $O[T] \subseteq O[[T]]$ since $\alpha \in O[T]$ gives rinse to a sequence $\alpha_n \in O[\Gamma_n]$ such that $\phi_{m,n}(\alpha_m) = \alpha_n$.

Let $f, g \in O[[T]]$ where $Q[T]$ in with $a_i \in \mathfrak{p}$ (the unique maximal ideal of O) for $0 \leq i \leq n-1, a_n \in O^\times$. Then we can write $g = qf + r$ uniquely where $q \in O[[T]]$, $r \in O[T]$ is a polynomial of degree at most $n-1$.

Theorem 0.2 (Division algorithm)**.** *Let $f, g \in O[[T]]$ where $Q[T]$ in with $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1, a_n \in O^\times$. Then we can write $g = qf + r$ uniquely where $q \in O[[T]]$, $r \in O[T]$ is a polynomial of degree at most $n-1$.*

$P(T) \in O[T]$ is called distinguished if $P(T) = T^n + a_{n-1}T^{n-1} + \ldots a_0$ with $a_i \in \mathfrak{p}$ for $0 \leqslant i \leqslant n-1$.
(This is almost the definition of an Eisenstein polynomial).

Theorem 0.3 (p-adic Weierstrass preparation theorem)**.** *Let $f(T) = \sum_{i=0}^{\infty} a_i T^i \in O[[T]]$. Then assume $a_i \in \mathfrak{p}$ for $0 \leq i \leqslant n-1$ but $a_n \notin \mathfrak{p}$ so $a_n \in O^\times$. Then f can be written uniquely in the form $f(T) = P(T)U(T)$ where $U(T) \in O[[T]]$ is a unit and $P(T)$ is a distinguished polynomial of degree n.*

More generally, if $f(T) \in O[[T]]$ is nonzero, we can write it uniquely as $f(T) = \pi^\mu P(T)U(T)$ where $\mu \in \mathbb{Z}_{\geq 0}$ (where π is a uniformizer for O).

As a consequence of the division algorithm and the Weierstrass preparation theorem, we obtain:

Theorem 0.4. *There is an isomorphism* $O[[\Gamma]] \cong O[[T]]$ *via* $\gamma \mapsto 1+T$.

We shall be particularly interested in the case $O = \mathbb{Z}_p$ and we write $\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$ and call it the Iwasawa algebra. Its structure as a topological ring is of great importance in Iwasawa theory. We will now state some properties of Λ and its modules.

By the p-adic Weierstrass preparation theorem, if $f(T) \in \Lambda$ is nonzero and $P(T)$ is distinguished, we can write $P(T) = q(T)P(T) + r(T) \in \mathbb{Z}_p[[T]]$ where $\deg(r(T)) < \deg(P(T))$. This gives a division algorithm $\Rightarrow \Lambda$ is a UFD whose irreducibles are P and distinguished polynomials. Additionally, Λ is noetherian, using the fact that if A is a noetherian ring, then so is $A[[X]]$.

If $f, g \in \Lambda$ are relatively prime, then (f, g) has finite index in Λ. The proof of this reduces to showing that (f, g) must contain some (f', p^s) where f' is distinguished and that such an ideal has finite index.

Let $f \in \Lambda$ with $f \notin \Lambda^\times$. Then $\Lambda/(f)$ is infinite.

Proof: We may assume $f \neq 0$. It suffices to consider $f = p$ and f distinguished. If $f = p$, $\Lambda/(f) \cong \mathbb{Z}/p\mathbb{Z}[[T]]$. If f is distinguished, use the division algorithm.

These facts are used to show that the prime ideals of Λ are $(0), (p, T), (p)$ and the ideals $(P(T))$ where $P(T)$ is irreducible and distinguished. The ideal (p, T) is the unique maximal ideal.

We now shift our attention to Λ-modules. M and M' (Λ-modules) are pseudo-isomorphic $M \sim M'$ if there is a homomorphism $M \longrightarrow M'$ with finite kernel and finite cokernel.

$M \sim M'$ does not necessarily imply that $M' \sim M$, even if we assume both modules are finitely generated. E.g. $(p, T) \sim \Lambda$ but $\Lambda \not\sim (p, T)$ since for $\Lambda \to (p, T)$, f the image of 1 in (p, T), $\Lambda/(f)$ is infinite since f is not a unit in $\Lambda \Rightarrow (p, T)/(f)$ is infinite. It is true if M and M' are both finitely generated and torsion.

The following theorem is a classification of pseudo-isomorphism classes of finitely generated Λ-modules. The proof is similar to the classification theorem of finitely generated modules over a principal ideal domain. This is perhaps not surprising given the form of these modules and the fact that every localization of Λ at a height 1 prime ideal is a principal ideal domain.

Theorem 0.5 (Classification of finitely generated Λ-modules)**.** *If M is a finitely generated Λ-module, then $M \sim \Lambda^r \oplus (\oplus_{i=1}^s \Lambda/(p^{n_i})) \oplus (\oplus_{i=1}^t \Lambda/(f_j(T)^{m_j}))$ for $r, s, t, n_i, m_j \in \mathbb{Z}$, f_j distinguished and irreducible.*

If M is finitely, torsion generated Λ-module pseudo isomorphic to a module of the form given in Theorem 0.5, then its characteristic polynomial is $p^{\sum_{i=1}^{s} n_i} \prod_{j=1}^{t} f_j$. Its characteristic ideal in Λ is the ideal generated by the characteristic polynomial.

Finally, we have Nakayama's lemma for Λ-modules:

Theorem 0.6 (Nakayama's lemma)**.** *Let X be a compact Λ-module. Then X is finitely generated over $\Lambda \Leftrightarrow X/(p,T)X$ is finite. If $x_1, \ldots, x_n$ generate $X/(p,T)X$ over $\mathbb{Z}$, then they also generate X as a Λ-module. Special case: $X/(p,T)X = 0 \Leftrightarrow X = 0$.*

Some easy consequences of class field theory

Class field theory is our main tool for transferring information about the topology of $\mathbb{Z}_p$ to obtain information about $\mathbb{Z}_p$-extensions and about Λ-modules.

We will not state the full theorems of class field theory. We only quote the required statements as needed and show how this can be applied to the study of Iwasawa theory.

The Hilbert class field and the Hilbert p-class field

Let F be a number field. Class field theory tells us that there is a maximal unramified abelian extension of F, called the Hilbert class field of F (and which we will denote by F_H) such that $\mathrm{Gal}(F_H/F) \cong Cl(F)$. In particular, F_H is a finite extension of F. Furthermore, every unramified abelian extension of F has Galois group isomorphic to a quotient of $Cl(F)$.

Since $Cl(F)$ is abelian, it has a unique sylow p-subgroup $Cl(F)^{(p)}$ for every prime p dividing $\#Cl(F)$. If p does not divide $\#Cl(F)$, let $Cl(F)^{(p)}$ be the trivial subgroup. Then we have $Cl(F) = Cl(F)^{(p)} \oplus \left(\oplus_{p' \nmid p} Cl(F)^{(p')}\right)$, then letting $H^{(p)} = \oplus_{p' \nmid p} Cl(F)^{(p')}$, we have $Cl(F)^{(p)} \cong Cl(F)/H^{(p)}$. Therefore, by global class field theory, there is a unique extension $F_H^{(p)}$ of F satisfying $Cl(F_H^{(p)}) \cong Cl(F)^{(p)}$ and $F_H \supseteq F_H^{(p)} \supseteq F$. It is called the Hilbert p-class field of F and by definition, it is the maximal unramified abelian extension of F with a pro-p Galois group.

Which primes ramify in $\mathbb{Z}_p$-extensions

Every number field has at least one $\mathbb{Z}_p$-extension, namely the cyclotomic $\mathbb{Z}_p$-extension. It is obtained by letting F_∞ be an appropriate subfield of $F(\zeta_{p^\infty})$.

Lemma 0.1. *Let F_∞/F be a $\mathbb{Z}_p$-extension. Then, for each $n \geq 0$, there is a unique field F_n of degree p^n over F, and these F_n, plus F_∞, are the only fields between F and F_∞.*

Proof: The intermediate fields correspond to the closed subgroups of $\mathbb{Z}_p$. Let $S \neq 0$ be a closed subgroup and let $x \in S$ be such that $v_p(x)$ is minimal. Then $x\mathbb{Z}$, hence $x\mathbb{Z}_p$, is in S. By the choice of x, we must have $S = x\mathbb{Z}_p = p^n\mathbb{Z}_p$ for some n. $\square$

Theorem 0.7. *If F is a number field and F_∞/F is a $\mathbb{Z}_p$-extension, then the only primes of F that can ramify in the extension F_∞/F are the primes lying over p.*

The proof is a clever application of local class field theory to study the inertia group at a prime $l \neq p$. A cdvr (complete discrete valuation ring) containing this inertia subgroup is constructed and the study of the local units of this cdvr gives us the conclusion we want.

Proof: Let $\widetilde{l}$ be a prime of F, possibly archimedean, not lying over p. Let $I \subset \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$ be its inertia subgroup. We will show that this is zero. Suppose not, then since I is closed, it must be of the form $p^n\mathbb{Z}_p$ for some n.

We can immediately exclude $\widetilde{l}$ being archimedean since in this case, I has order 1 or 2. For each n, inductively choose a prime $\widetilde{l_n}$ of F_n lying over $\widetilde{l}_{n-1}$ with $\widetilde{l}_0 = \widetilde{l}$. Let $\widetilde{F}_n$ be the completion of F_n at the prime $\widetilde{l_n}$, and let $\widetilde{F}_\infty = \cup_n \widetilde{F}_n$. This is a cdvr with a unique maximal ideal, corresponding to a prime ideal $\widetilde{l}_\infty$ of F_∞ lying over each $\widetilde{l_n}$. Setting k_n and k_∞ to be the residue fields of $\widetilde{F}_n$ and $\widetilde{F}_\infty$ respectively, and

$$\begin{aligned} I_n &= \ker(\mathrm{Gal}((F_\infty)_{\widetilde{l}_\infty}/(F_n)_{\widetilde{l}_n}) \to \mathrm{Gal}(k_\infty/k_n)) \\ &= \ker(\mathrm{Gal}(\widetilde{F}_\infty/\widetilde{F}_n) \to \mathrm{Gal}(k_\infty/k_n)), \\ &\text{we obtain } I = \varprojlim_n I_n. \end{aligned}$$

Letting U be the units of $\widetilde{F}_\infty$, local class field theory says that there is some continuous, surjective homomorphism $U \to I \cong p^n\mathbb{Z}_p$. However, $U \cong (\text{finite group}) \times \mathbb{Z}_l^a$ for $\widetilde{l}$ lying over the prime integer l (can be proved by considering $\log_l : U \to l^{-N}O_{\widetilde{F}_\infty}$ for sufficiently large N). Since $p^n\mathbb{Z}_p$ has no torsion, there must be some continuous, surjective map $\mathbb{Z}_l^a \to p^n\mathbb{Z}_p \to p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$. However, $\mathbb{Z}_l^a$ has no closed subgroups of index a p-power, contradiction. $\square$

Theorem 0.8. *Let F be a number field. Let F_∞/F be a $\mathbb{Z}_p$-extension. At least one prime ramifies in this extension (by the above, such a prime is a prime of F over p), and there exists $n \geq 0$ such that every prime which ramifies in F_∞/F_n is totally ramified.*

The first claim follows from the existence and description of the Hilbert class field of F and the second follows from the topology of $\mathbb{Z}_p$ extensions.

Proof: Proof: Since the class number of F is finite, the maximal abelian unramified extension of F is finite, so some prime must ramify in F_∞/F since

$F_H \supseteq F_H \cap F_\infty$ (the maximal unramified subextension of F_∞/F). Therefore, $\mathrm{Gal}(F_H \cap F_\infty)$ is a quotient of $\mathrm{Gal}(F_H/F) \cong Cl(F)$ so is finite.

We know that only finitely many primes of K ramify in K_∞/K (we are restricted to considering primes of K over p). Call them $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, and let $I_1, \ldots, I_s$ be the corresponding inertia groups. Then $\cap I_j = p^n\mathbb{Z}_p$ for some n. The fixed field of $p^n\mathbb{Z}_p$ is K_n and $\mathrm{Gal}(K_\infty/K)$ is contained in each I_j (since it is a closed subgroup). Therefore, all primes above each $\mathfrak{p}_j$ in K_n are totally ramified in K_∞/K_n. This follows from the fact that for such primes $\mathcal{P}$, $\mathrm{Gal}(K_\infty/K_n)$ fix the residue field and since $D_{\mathcal{B}|\mathcal{P}} \subset \mathrm{Gal}(K_\infty/K_n)$, it must be equal to inertia. This completes the proof. $\square$

Iwasawa's theorem

The theorem and the idea of the proof

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 Λ are of the form $\Gamma_n = \Gamma^{p^n}$ for $n \geq 0$. They form a descending sequence and F_n/F is cyclic of order p^n. If we let $F_n = F_\infty^{\Gamma_n}$, then we obtain a tower of number fields

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

such that F_n/F is a cyclic extension of degree p^n and $F_\infty = \cup_n F_n$.

Theorem 0.9 (Iwasawa's 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.*

We explain the ideas and main steps of the proof. Iwasawa's proof of this theorem is based on studying the Galois group $X = \mathrm{Gal}(L_\infty/F_\infty)$, where $L_\infty = \cup_n L_n$ and L_n is the Hilbert p-class field of F_n. This is a natural approach in light of the fact that, by definition of L_n and e_n, we have $[L_n : F_n] = p^{e_n}$.

The extension L_∞/F is Galois and there is an exact sequence of topological groups

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

Since X is a projective limit of finite, abelian p-groups, we can regard X as a compact $\mathbb{Z}_p$-module.

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, is equal to p^{e_n}.

The relationship between the structure of X (together with the action of Γ) and the groups $\mathrm{Gal}(L_n/F_n)$ is 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. The general case is a bit more involved but we do not lose the idea of the structure of the argument if we work in this restricted setting. For a more general proof, see Washington's book.

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 (it is ramified using the fact that the inertia subgroup of a prime over $\mathfrak{p}_n$ in L_n^* contains the inertial subgroup of a prime of F_∞ over L_n as a subgroup). 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 (subextension of an unramified extension). Therefore $L_n^* = L_n F_\infty$ and, since $L_n^* \cap F_\infty = F_n$, we have $\mathrm{Gal}(L_n/F_n) \cong \mathrm{Gal}(L_n F_\infty/F_\infty) \cong \mathrm{Gal}(L_n^*/F_\infty)$. Considering the exact sequence

$$0 \to \mathrm{Gal}(L_\infty/L_n^*) \to \mathrm{Gal}(L_\infty/F_n) \to \mathrm{Gal}(L_\infty/F_n)^{ab} \to 0,$$

we see that $\mathrm{Gal}(L_\infty/L_n^*) = [\mathrm{Gal}(L_n^*/F_n), \mathrm{Gal}(L_n^*/F_n)]$.

We also have an exact sequence $0 \to X \to \mathrm{Gal}(L_n/F_n) \to \Gamma_n \to 0$. Let γ be a fixed topological generator of Γ. (It suffices to choose $\gamma \in \Gamma$ such that $\gamma|_{F_n}$ is nontrivial.) Then $\gamma_n = \gamma^{p^n}$ 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 $\mathrm{Gal}(L_n/F_n)$ for each $x \in X$. It is not hard to show that the derived subgroup of $\mathrm{Gal}(L_n/F_n)$ is precisely $\{\gamma_n(x)x^{-1} : x \in X\}$. Changing to an additive notation for X, we write this as $w_n X$, where $w_n = \gamma_n - 1$. Therefore, $\mathrm{Gal}(L_n^*/F_\infty) \cong X/w_n X$, giving the result that $\mathrm{Gal}(L_n/F_n) \cong X/w_n X$ 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 $A^{\Gamma_n} = \{a : a \in A, \gamma_n(a) = a\}$ is finite for all $n \geq 0$. The structure theory which Iwasawa develops then allows him to prove that $|A^{\Gamma_n}| = p^{\lambda n + \mu p^n + v}$ for all sufficiently large n, where the integers λ and μ are described in terms of the structure of A and where $v \in \mathbb{Z}$. 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 $X/w_n X$ is the maximal quotient of X on which Γ_n acts trivially. Hence $A^{\Gamma_n} = \mathrm{Hom}(X/w_n X, \mathbb{Q}_p/\mathbb{Z}_p)$ is finite and has the same order as $X/w_n X$. So as required result that $p^{e_n} = |\mathrm{Gal}(L_n/F_n)| = |X/w_n X| = p^{\lambda n + \mu p^n + v}$ for $n \gg 0$.

Serre introduced the approach, which was subsequently adopted by Iwasawa, of viewing X as a module over the ring $\Lambda = \mathbb{Z}_p[[T]]$ by letting T act on the

$\mathbb{Z}_p$-module X as $\gamma - 1$, making X into a $\mathbb{Z}_p[[T]]$ module in the way described in the previous section. In the case we have been considering, using the fact that $X/TX \cong \mathrm{Gal}(L_0/F_0)$ is finite, combined with Nakayama's lemma 0.6, we obtain $T^n X = 0$ for $n >> 0$. Moreover, from the stucture theorem 0.5 of finitely generated Λ-modules, we have some homomorphism $X \to \oplus_{i=1}^{t} \Lambda/(f_i(T)^{a_i})$ 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 $1 \leq i \leq t$. 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. Each $f_i(T)$ is either distinguished or p. We define the characteristic polynomial of X to be the polynomial $f_X(t) = \prod_{i=1}^{t} f_i(T)^{a_i}$.

The invariants λ and μ which occur in Iwasawa's theorem can be described just in terms of $f_X(T)$. 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 $i \geq 0, p^i Y/p^{i+1}Y$ 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 $p^i Y/p^{i+1}Y$, where $0 \leq i \leq c-1$.

We continue with the special case where only one prime $\mathfrak{p}$ of F lies over p and F_∞/F is totally ramified at p. Then $p^{e_n} = |X/w_n X|$ 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. Considering separately the 2 cases where g is a power of p and g is distincuished, and accounting for the finite kernel and cokernel, we obtain $p^{e_n} = |\mathrm{Gal}(L_n/F_n)| = |X/w_n X| = p^{\lambda n + \mu p^n + v}$ for $n \gg 0$ using Serre's approach.

Determining λ and μ

Iwasawa wanted to understand the invariants λ and μ associated to $\mathbb{Z}_p$-extensions. In general, the constants λ and μ are hard to determine.

Proposition 0.1. *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 $\lambda = \mu = \nu = 0$. (No power of p can divide $\#Cl(F_n)$).*

Proof: 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 $\mathrm{Gal}(L_n/F_n) = X/w_n X = 0$ for all n, which clearly means that $\lambda = \mu = v = 0$, as stated. $\square$

Proposition 0.2. *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 places of F.*

To prove this, we need the following theorem on $\mathbb{Z}_p$-extensions:

Theorem 0.10. *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 $r_2 + 1 \leq d \leq [F:\mathbb{Q}]$.*

Proof: Let $U^0 = \prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^0$ where $U_{\mathfrak{p}}^0$ is the group of principal units of the completion of F at $\mathfrak{p}$. Considered as a $\mathbb{Z}_p$-module,

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

The Artin map defines a homomorphism from U^0 to $\mathrm{Gal}(\widetilde{F}/F)$ with finite cokernel, isomorphic to $\mathrm{Gal}(L_0 \cap \widetilde{F}/F)$. Why? $\mathrm{Gal}(\tilde{F}/F) \leftrightarrow \widetilde{H} \leq J_F$ such that $k^\times N_{\tilde{F}/F}\left(J_{\tilde{F}}\right) = \tilde{H}$ and $H = k^\times N_{F_H/F}\left(J_{F_H}\right)$. Therefore, the Artin map (idelic version) induces a morphism $U^0 \longrightarrow \mathrm{Gal}(\tilde{F}/F)$. Letting $F_H = L_0 =$ maximal abelian extension unramified outside of H, the image of the Artin map is $\mathrm{Gal}(\widetilde{F}/L_0 \cap \widetilde{F})$. Therefore, the kernel is $\mathrm{Gal}(\tilde{F}/F)/\mathrm{Gal}(\widetilde{F}/L_0 \cap \widetilde{F}) = \mathrm{Gal}(L_0 \cap \widetilde{F}/F)$. It is finite because $L_0 \supset L_0 \cap \widetilde{F} \supset F$ so $\mathrm{Gal}(L_0 \cap \widetilde{G}/F)$ is isomorphic to a quotient of the ideal class group of F.

What is the kernel of this homomorphism? Let E be the group of units in F and E° be the subgroup of units $\epsilon \equiv 1 (\mathrm{mod}\, \mathfrak{p})$ for all $\mathfrak{p} \mid p$ (of finite index in E). We consider E^0 as a subgroup of U^0, using the natural injection $F \to \prod_{\mathfrak{p}|p} F_{\mathfrak{p}} = U^0$. The kernel H of the Artin map is characterized as the smallest $\mathbb{Z}_p$-submodule of U^0 containing $\overline{E^0}$ and such that U^0/H is torsion-free. ($[H : \overline{E^0}] < \infty$)

The theorem follows because U^0/H has $\mathbb{Z}_p$-rank equal to $[F:\mathbb{Q}] - \mathrm{rank}_{\mathbb{Z}_p}(\overline{E^0})$ and $\mathrm{rank}_{\mathbb{Z}_p}(\overline{E^0}) \leqslant \mathrm{rank}_{\mathbb{Z}}(E) = r_1 + r_2 - 1$ (Dirichlet's units theorem). $\square$

Proof of Proposition 0.2:Under the assumption of that F_∞/F is ramified over every $\mathfrak{p}|p$, the inertia subgroup $I_{\mathfrak{p}}$ of $\mathrm{Gal}(\widetilde{F}/F)$ is the image of $U_{\mathfrak{p}}$ under the Artin map $U^0 \to \mathrm{Gal}(\widetilde{F}/F) \implies I_{\mathfrak{p}} \cong \mathbb{Z}_p$ but the image of $I_{\mathfrak{p}}$ in $\mathrm{Gal}(F_\infty/F)$ under the restriction map must also be isomorphic to $\mathbb{Z}_p$ because $\mathfrak{p}$ is ramified in F_∞/F. Therefore, $I_{\mathfrak{p}} \cap \mathrm{Gal}(\widetilde{F}/F) = 0$, which implies primes of F_∞ lying over $\mathfrak{p}$ are unramified in $\widetilde{F}/F_\infty$.
(Why? If $\mathfrak{p}$ is ramified in $\widetilde{F}/F_\infty$, it must be totally ramified since it is contained in a $\mathbb{Z}_p$-extension).

Since primes not dividing p are unramified in every $\mathbb{Z}_p$-extension of F, we must have $\widetilde{F} \subset L_\infty$ (since $L_n \cap \widetilde{F}/F_n$ must be unramified for all n).

Therefore $\mathrm{Gal}(L_\infty/F_\infty)/\mathrm{Gal}(L_\infty/\widetilde{F}) \cong \mathrm{Gal}(\widetilde{F}/F_\infty) \cong \mathbb{Z}_p^{d-1}$ implies $\lambda = \mathrm{rank}_{\mathbb{Z}_p}(X) \geq d-1 \geq r_2$. $\square$

Iwasawa's main conjecture (now theorem)

It is also natural to consider the p-primary subgroups S_n of $Cl(F_n)$. We have $S_n \cong \mathrm{Gal}(L_n/F_n)$ for each $n \geq 0$. Letting $S_\infty = \varinjlim_n S_n$, Iwasawa shows that this is a discrete Λ-module, isomorphic to $\mathrm{Hom}(\mathrm{Gal}(M_\infty/N_\infty), \mu_{p^\infty})$ where M_∞ is the maximal abelian extension of F_∞ that is pro-p and N_∞ is obtained from F_∞ by adjoining app p-power roots of unity. This isomorphism preserves the action of $\mathrm{Gal}(F_\infty/\mathbb{Q})$, hence of Γ on both groups. We can identify $\mathrm{Gal}(F_\infty/\mathbb{Q}) = \Delta \times \Gamma$ where $\Delta = \mathrm{Gal}(F_\infty/\mathbb{Q}_\infty), \Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, where $\mathbb{Q}_\infty$ is the unique subfield of F_∞ such that $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. There is a canonical isomorphism $\omega : \Delta \to \mu_{p-1} \subset \mathbb{Z}_p^\times$ defined by the action of Δ on μ_{p^∞}. Explicitly, ω is the cyclotomic character, where for each $\sigma \in \Delta, \omega(\sigma)$ is determined by the property that for every $\zeta \in \mu_{p^\infty}, \sigma(\zeta) = \zeta^{\omega(\sigma)}$.

If A is any $\mathbb{Z}_p$-module on which Δ acts, there is a canonical decomposition $A = \oplus_{k=0}^{p-1} A^{\omega^k}$ where $A^{\omega^k} = \{a \in A : \delta(a) = \omega^k(\delta), \forall \delta \in A\}$. We are mainly interested in this decomposition for $A = X$ and S_∞. The actions of Δ and Γ commute and we can therefore regard X^{ω^k} and $S_\infty^{\omega^k}$ as Λ-modules.

Theorem 0.11 (Iwasawa's main conjecture (theorem))**.** *For each odd integer $1 \leq i \leq p-2$, we have $X^{\omega^i} \cong \Lambda/I$ where I is the principal ideal $(f_{X^{\omega^i}}(T))$ of Λ and in fact, $I = (g_i(T))$ where g_i is a power series attached to a Kubota-Leopoldt p-adic L-function $L_p(\omega^{1-i}, s)$. The power series is determined by interpolation by the values $g_i(\gamma^s - 1) = L_p(\omega^{1-i}, s)$ for all $s \in \mathbb{Z}_p$ where γ is a topological generator of $1 + p\mathbb{Z}_p$.*

This was eventually proved by Mazur and Wiles in 1984. Their approach was inspired by Ribet's proof of the converse of a theorem by Kummer- Herbrand in that they use the structure of certain finite groups of torsion on abelian varieties arising as quotients of Jacobian varieties of some modular curves. An important role is played by the cuspidal subgroup of this Jacobian, whose structure is related to Stickelberger ideals (these can be used to construct non-trivial annihilators of ideal class groups), which are in turn related to Bernoulli numbers. Using fields generated by the group of torsion points, Mazur and Wiles construct a finite sequence of extensions of F_∞ contained in L_∞. Another crucial part of their proof depends an the theory of fitting ideals to prove a certain divisibility statement they need.

An obvious question is the following: Why do Jacobian varieties and modular forms allow us to study such problems?

To discuss this, we first discuss Ribet's approach to proving the converse of the Kummer-Herbrand theorem. The Kummer-Herbrand result states that if $S_0^{\omega^i} \neq 0$, then $p \mid B_j$. As a reminder, $S_0 = Cl(F)^p \cong \mathrm{Gal}(L_0/F)$. The Kummer-Herbrand theorem is a result of Stickelberger's theorem, giving an annihilator in $\mathbb{Z}[\Delta]$ of S_0. Ribet proves the converse, showing that if $p \mid B_j$, then $\mathrm{Gal}\left(L_0/F\right)^{\omega^i} \neq 0$. To do this, he constructs a nontrivial, uramified 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. (L would correspond to a subfield extension in L_0).

An idea pursued by various people in the 70s was to construct such a field L using p-adic representation associated to modular forms. This approach was motivated by Ramanujan's congruence $\sigma_{11}(n) \equiv \tau(n)(\mathrm{mod}\ 691)$ for all $n \geqslant 1$ where $\tau(n) = n^{\text{th}}$ coefficient in the Fourier expansion of $f_{12} = q\prod_{m=1}^{\infty}(1-q^m)^{24}, \sigma_{11}(n) = \sum_{d|n} d^{11}$. This congruence arises from the fact that $691|B_{12}$. We then obtain 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 $p \mid B_j$, then there is a similar congruence involving a cusp form of level 1 and weight j.

If p is any prime, letting $\mathbb{Q}_\Sigma$ be the maximal extension of $\mathbb{Q}$ unramified outside of Σ, then Deligne constructs a 2-dimensional representation space V_p of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$ associated to f_{12} such that $\mathrm{Tr}_{V_p}\left(\mathrm{Frob}_l\right) = \tau(l)$ for all primes $l \neq p$, where $\mathrm{Frob}_l \in \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$ is the Frobenius of any prime of $\mathbb{Q}_\Sigma$ over l. For $p = 691$, choosing a $\mathrm{Gal}\left(\mathbb{Q}_\Sigma/\mathbb{Q}\right)$-invariant $\mathbb{Z}_p$-lattice T_p in V_p, we obtain a 2 -dimensional representation space T_p/pT_p for $\mathrm{Gal}\left(\mathbb{Q}_\Sigma/\mathbb{Q}\right)$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ such that Frob_l has trace $1 + l^{11}(\mathrm{mod}p)$ (equal to $1 + \omega^{11}(l)(\mathrm{mod}p\mathbb{Z})$).

The Chebotarev density theorem then implies that T_p/pT_p is reducible and has composition factors $\mathbb{F}_p = \mathbb{F}_p\left(\omega^0\right)$, on which $\mathrm{Gal}\left(\mathbb{Q}_\Sigma/\mathbb{Q}\right)$ acts trivially, and $\mathbb{F}_p\left(\omega^{11}\right)$, on which $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$ acts by ω^{11}. Why? We can define a semisimple representation $\bar{\rho}' : \mathrm{Gal}(\mathbb{Q}^E/\mathbb{Q}) \longrightarrow GL_2\left(\mathbb{F}_p\right)$ given by $\bar{\rho}' = \chi_0 \oplus \chi_{11}$ where χ_0 is the trivial character, χ_{11} is the mod p reduction of will so for $l \neq p$. This satisfies $\mathrm{Tr}\left(\overline{\rho}'\left(\mathrm{Frob}_l\right)\right) = 1 + l^{11}(\mathrm{mod}p)$, the same as for T_p. The Chebotarev density theoem says that $\{\mathrm{Frob}_l\}$ for all l unramified is dense in $\mathrm{Gal}(\mathbb{Q}^E/\mathbb{Q})$. Therefore, the traces on Frobenius elements determine the semisimplification of a representation, which implies that 2 semisimple representations over $\mathbb{F}_p$ having the same trace on all Frobenius elements are isomorphic.

If it were known that the V_p were irreducible, then T_p could be chosen so that there is a nonsplit exact sequence $0 \longrightarrow \mathbb{F}_p\left(\omega^0\right) \longrightarrow T_p/pT_p \longrightarrow \mathbb{F}_p(\omega^{11}) \to 0$ of $\mathrm{Gal}\left(\mathbb{Q}_\Sigma/\mathbb{Q}\right)$-modules. In matrix form, the corresponding $\mathbb{F}_p$-representation

looks like $\begin{pmatrix} 1 & * \\ 0 & \omega^{11} \end{pmatrix}$ where $*$ is nontrivial. It follows, since the kernel must have finite index, that there is a cyclic extension L of F of degree p such that the representation factors through $\mathrm{Gal}(L/\mathbb{Q})$. Why cyclic of degree p? $\mathrm{Gal}(L/F) \cong \mathrm{im}(\mathrm{rep}) \cong \mathbb{F}_p$ of degree p and abelian. Its restriction to $\mathrm{Gal}(L/F)$ gives a Δ-equivariant isomorphism $\mathrm{Gal}(L/F) \cong \mathrm{Hom}\left(\mathbb{F}_p(\omega^{11}), \mathbb{F}_p\right) = \mathbb{F}_p\left(\omega^{-11}\right)$. Starting from the fact that $p \mid B_j$ for $j = 12, p = 691$, we obtain a field extension L as above such that $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ acts on $\mathrm{Gal}(L/F)$ by $\chi = \omega^{1-j} = \omega^i$ $(i = 679)$. The extension L/F turns out to be automatically unramified.

In what follows, we write $G_K = \mathrm{Gal}(\overline{K}/K)$ for a field K. A result of Wiles shows that for the so called 'ordinary prime' $p = 691$ for f_{12}, V_p is a representation space for $G_{\mathbb{Q}_p}$ that is reducible. There is therefore an exact sequence $0 \longrightarrow W_p \to V_p \to U_p \to 0$ where W_p and U_p are 1 -dimensional representation spaces for $G_{\mathbb{Q}_p}$ such that $W_p \cong \mathbb{Q}_p(11), U_p \cong \mathbb{Q}_p(0)$ as representation spaces for the inertia subgroup $I_p = G_{\mathbb{Q}_p^{\mathrm{unr}}}$. Here $\mathbb{Q}_p(k)$ is defined to be the 1-dim space on which a Galois group acts by the k^{th} power of the p-power cyclotomic character. Therefore, U_p is an unramified $G_{\mathbb{Q}_p}$-module. This implies T_p/pT_p has a $G_{\mathbb{Q}_p}$-submodule isomorphic to $\mathbb{F}_p(\omega^{11})$. Since it also has $\mathbb{F}_p\left(\omega^0\right)$ as a submodule, we have $T_p/pT_p \cong \mathbb{F}_p\left(\omega^0\right) \times \mathbb{F}_p\left(\omega^{11}\right)$ as $G_{\mathbb{Q}_p}$-modules $\Rightarrow G_{\mathbb{Q}_p}\left(\zeta_p\right)$ acts trivially on $T_p/pT_p \Rightarrow$ there is a unique prime of F lying over p that splits completely in L/F. Since $L \subset \mathbb{Q}_\Sigma$, where $\Sigma = \{p, \infty\}$, L is a subfied of the p-Hilbert class of F.

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 uses modular forms of weight 2 with the property that the associated l-adic representations arise from abelian varieties. He then obtains a congruence between an Eisenstein series and a cusp form if $p \mid B_j$. He proves irreducibility of the associated 2-dim representation and then the existence of a suitable $G_{\mathbb{Q}}$-invariant lattice. To prove 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 ordinaryness, he proves the reducibility as a $G_{\mathbb{Q}_p}$-representation space, just as for f_{12}. The argument uses ideas of Hida and reduces to 2-dimensional representations obtained from abelian varieties (i.e. from modular forms of weight 2). Let $L(z, f)$ be the p-adic L-function associated to a newform f of weight $k \geqslant 2$ at any level, not divisible by p. Under an ordinariness hypothesis, this belongs to $\Lambda = O[[T]]$.

Elliptic curves and the BSD conjecture

The proof of Iwasawa's main conjecture provides a link to geometry. We explore this further by considering how the theory of $\mathbb{Z}_p$ extensions can be applied to the study of elliptic curves (and abelian varieties more generally).

0.1 A $\mathbb{Z}_p$-analogue of the Mordell-Weil theorem

Mazur aimed proving results of the following kind:

Conjecture 0.1. *Suppose A is an abelian vanity defined over a number field F. Assume p is a prime such that A has good 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.*

This is reminiscent of the Mordell-Weil theorem, which states that if A is an abelian variety over a number field F, then $A(F)$, the set of F-rational points, is finitely generated. The proof of the Mordell-Weil theorem has 2 main parts. First, the weak Mordell Weil theorem is proven. This is the statement that for any integer $m \geq 2$, $A(F)/mA(F)$ is finite. The second part uses a height function defined on A and the weak Mordell-Weil theorem to prove the (strong) Mordell-Weil theorem. The weak Mordell-Weil theorem is proved by showing that the Selmer group $S_A^{(m)}(F)$, into which $A(K)/mA(K)$ injects, is finite. We define Selmer groups and Tate Shafarevich groups below. These groups are important in considering this type of question.

Given an abelian variety A/F and an integer $n \geq 2$, the Selmer group $S^{(n)}(A/K)$ is defined to be:

$$S_A^{(n)}(F) = \{\gamma \in H^1(F, A[n]) : \text{for all places } \mathfrak{p} \text{ of } K, \gamma_\mathfrak{p} \text{ comes from } A(K_\mathfrak{p})\}$$

$= \mathrm{Ker}(H^1(K, A[n]) \longrightarrow \prod_\mathfrak{p} H^1(K_\mathfrak{p}, A))$ where $A[n]$ is the set of n torsion points of $A(\overline{F})$.

The Tate Shafarevich group of A is defined to be

$$SH_A(K) = \mathrm{Ker}\left(H^1(K, A) \to \prod_\mathfrak{p} H^1(K_\mathfrak{p}, A)\right).$$

These groups are related by the following exact sequence

$$0 \to A(F)/nA(F) \to S_A^{(n)}(F) \to SH_A(F)[n] \to 0.$$

Here $SH_A(F)[n]$ is the subgroup of elements in the kernel of the multiplication by n map on $SK_A(F)$.

Similarly, Selmer groups and the Tate Shafarevich group can be defined for any algebraic extension K/F of F. For a prime p, we define

$$S_A(F)_p = \cup_{n\geq 1} S_A^{p^n}(K) \text{ and } SH_A(K) = SH_A(F)_p = \bigcup_{n\geq 1} \text{Ker}\left(H^1(F, A[p^n]) \to \prod_v H^1(F_v, A)\right)$$

We then have an exact sequence

$$0 \to A(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to \text{S}_A(K)_p \to SH_A(K)_p \to 0.$$

Mazur proves his conjecture under the following assumption:

$$A(F) \text{ and } SH_A(F)_p \text{ are finite.}$$

Using the above exact sequence, this gives finiteness of $S_A(K)_p$.

Theorem 0.12 (Mazur's control theorem)**.** *Assume 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 $\text{Sel}_A(F_n)_p \longrightarrow \text{Sel}_A(F_\infty)_p^{\text{Gal}(F_\infty/F_n)}$ are finite and have bounded order as $n \to \infty$.*

Assuming $\text{S}_A(F)_p$ is finite, Mazur's control theorem implies that $\text{S}_A\left(F_\infty\right)_p$ is a discete, p-primary subgroup on which $\Gamma = \text{Gal}(F_\infty/F)$ acts.

We can regard $\text{Sel}_A(F_\infty)_p$ as a discrete Λ-module, from which it follows that its Pontryagin dual $X_A\left(F_\infty\right)$ as a compact Λ-module.

If we assure $S_A(F)_p$ is finite, then Mazur's control theorem implies that $X_A\left(F_\infty\right)/TX_A\left(F_\infty\right)$ is finite, which implies that $X_A\left(F_\infty\right)$ is a finitely-generated, torsion Λ-module. The classification theorem implies that $X_A(F_\infty)$ has finite $\mathbb{Z}_p$-corank, denoted by $\lambda_A(F_\infty/F)$. The maximal divisible subgroup $(\text{Sel}_A(F_\infty)_p)_{\text{div}}$ of $\text{Sel}_A(F_\infty)_p$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_A(F_\infty/F)}$. This implies that $A(F_\infty) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ for some $0 \leq r \leq \lambda_A(F_\infty/F)$.

If F_∞/F is the cyclic $\mathbb{Z}_p$-extension, then $A\left(F_\infty\right)_{\text{tors}}$ is known to be finite. Mazur proves that this, along with the previous hypotheses, imply that $A(F_\infty)$ is a finitely generated group.

This could be seen as vaguely analagous to the proof of the Mordell-Weil theorem from the weak Mordell-Weil theorem but instead of using height functions, Mazur uses Iwasawa theory and knowledge of Selmer groups.

The Birch and Swinnerton-Dyer conjecture

Conjecture 0.2 (BSD conjecture)**.** *Let E be an elliptic curve over a number field F and let $L(E, s)$ be its Hasse-Weil L function. This extends to an analytic function on $\mathbb{C}$ and conjecturally satisfies the following properties*

1. *Order of vanishing:* $\mathrm{ord}_{s=1}L(E,s) = \mathrm{rank}_{\mathbb{Z}}(E(F))$. *Here* $\mathrm{ord}_{s=1}$ *denotes the order of vanishing at* $s = 1$.

2. *Leading coefficient: It is additionally conjectured that the leading Taylor coefficient of* $L(E,s)$ *at* $s = 1$ *(for* L *having vanishing order* r *at* $s = 1$*) is given by*

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r} = \frac{\#SH_E(F)\cdot\Omega_E\cdot\prod c_v\cdot\mathrm{Reg}(E/F)}{(\#E(F)_{\mathrm{tors}})^2}$$

We now explain the terms in a little more detail. The most important definition is that of the Hasse-Weil L function. If p is a prime of good reduction, set $a_p = p + 1 - \#E(\mathbb{F}_p)$ and define $L_p(E,s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$. If p is a prime of bad reduction, define $L_p(E,s)$ as follows:

Case 1) If the reduction is split multiplicative, define $L_p(E,s) = (1-p^{-s})^{-1}$.

Case 2) If the reduction is non-split multiplicative $L_p(E,s) = (1+p^{-s})^{-1}$.

Case 3) If the reduction is additive, define $L_p(E,s) = 1$.

(For a discussion of the reduction of an elliptic curve modulo p, see Silverman's book 'The Arithmetic of Elliptic Curves'). In this way, $L_p(E,s)$ reflects the behavior of the reduction of E modulo p. Define $L(E,s) = \prod_p L_p(E,s)$. Initially, the infinite product is defined for $Re(s) > \frac{3}{2}$ so that it converges. However, $L(E,s)$ has an analytic continuation to all of $\mathbb{C}$ and satisfies a functional equation relating $L(E,s)$ and $L(E,2-s)$, involving the conductor of E.

Ω_E is the integral of a Néron differential over $E(\mathbb{R})$, $\prod_v c_v$ is the product of Tamagawa numbers at primes of bad reduction. $\mathrm{Reg}(E/K)$ is the regulator of the determinant of the height pairing on $E(K)/E(K)_{\mathrm{tors}}$.

Mazur's conjectures for elliptic curves

Mazur states a conjecture, similar in nature to Iwasawa's main conjecture for an elliptic curve $E/\mathbb{Q}$ which is modular and in the case where F_∞ is a $\mathbb{Z}_p$-extension of a subfield F of $\mathbb{Q}(\zeta_p)$ at a prime p at which E is assumed to have good reduction. For simplicity, assume $F = \mathbb{Q}$. For such a prime p, Mazur and Swinnerton-Dyer constructed a p-adic L-function $\widetilde{L}_p(s,E)$.

Note: An elliptic curve E being modular means that there is some non-constant morphism $X_0(N) \to E$ over $\mathbb{Q}$ where $X_0(N)$ is the elliptic curve whose points correspond to pairs consisting of elliptic curves and subgroups of order N (it is the moduli space for such data).

If $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ and $\Lambda = \mathbb{Z}_p[[\Gamma]]$, then $\widetilde{L}_p(s,E) = \varphi_{s-1}(\theta_E)$ 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 defined as follows: The action of Γ on μ_{p^∞} gives rise to an isomorphism $\kappa : \Gamma \to 1 + p\mathbb{Z}_p$

(via the cyclotomic character, for $\gamma \in \Gamma$, κ is given by the relation $\gamma(\zeta) = \zeta^{\kappa(\gamma)}$ for any $\zeta \in \mu_{p^\infty}$). Then

$$\varphi_s : \Lambda \to \mathbb{Z}_p \text{ is defined by } \varphi_s(g(t)) = g(\kappa(\gamma)^s - 1)$$

where under a fixed identification $\Lambda \cong \mathbb{Z}_p[[T]], \gamma - 1 \leftrightarrow T$.

The element θ_E is characterized by an interpolation property involving the values at $z = 1$ of the twisted Hasse-weil L-function $L(z, E, \rho)$ for $E/\mathbb{Q}$ where ρ varies over all Dirichlet characters of p-power order and conductor.

Under mild assumptions, $\theta_E \in \Lambda$. θ_E can be identified with a $\mathbb{Q}_p$-valued measure on the Galois group Γ. Then the measure or any open subset of Γ is in $\frac{1}{p^t}\mathbb{Z}_p$. If μ_E is this measure, then $\widetilde{L}_p(s, E) = \int_T \kappa^{s-1} d\mu_E$ where κ^{s-1} is viewed as a function on Γ.

Conjecture 0.3 (Elliptic curve analogue of Iwasawa's main conjecture)**.** *The characteristic ideal of* $X_E(\mathbb{Q}_\infty) = \widehat{\mathrm{Sel}_E(\mathbb{Q}_\infty)}_p$ *is generated by* θ_E*. In other words, as a* Λ*-module,* $X_E(\mathbb{Q}_\infty) \cong \Lambda/(\theta_E)$.

A piece of the BSD conjecture can be stated as

$$L(1, E) \neq 0 \Longleftrightarrow E(\mathbb{Q}) \text{ and } SH_E(\mathbb{Q})_p \text{ are finite.}$$

The interpolation property implies that

$$L(1, E) \neq 0 \Longleftrightarrow \widetilde{L}_p(1, E) \neq 0 \Longleftrightarrow T \nmid \theta_E$$

where $T = \gamma - 1 \in \Lambda$, as before.

Conjecture 0.3 is valid $\Rightarrow T \nmid \theta_E$ is equivalent to the assertion that $X_E(\mathbb{Q}_\infty)/TX_E(\mathbb{Q}_\infty)$ is finite. Then Mazur's control theorem implies that the last assertion is equivalent to the finteness of $\mathrm{Sel}_E(\mathbb{Q})_p$.

If $E(\mathbb{Q})$ as infinite, conjecture 0.3 implies that $\mathrm{ord}_{s=1}(\widetilde{L}_p(S, E)) \geq \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. This is because $X_E(Q_\infty)/TX_E(Q_\infty)$ has $\mathbb{Z}_p$-rank equal to the corank of $\mathrm{Sel}_E(\mathbb{Q})_p$ which is at least $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ (with equality if $SH_E(\mathbb{Q})_p$ is finite).

The first part of the BSD conjecture asserts that $\mathrm{ord}_{z=1}(L(z, E)) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. In order to deduce this from conjecture 0.3, we would need to prove the following results:

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

Mazur also made the following conjecture.

Conjecture 0.4. *Under the same assumtions as in Conjecture 0.1, the* Λ*-module* $X_A(F_\infty) := \widehat{\mathrm{Sel}_A(F_\infty)_p}$ *is finitely generated and torsion.*

Assume now that $SH_E(\mathbb{Q}_n)$ is finite for all n. What can we say about the growth of $|SH_E(\mathbb{Q}_n)_p|$ as $n \to \infty$? If E has good, ordinary reduction and conjecture 0.4 holds for $A = E$ and the $\mathbb{Z}_p$-extension is $\mathbb{Q}_\infty/\mathbb{Q}$, then it can be shown that $\left|SH\left(\mathbb{Q}_n\right)_p\right| = \rho^{\lambda n} + \mu\rho^n + v$ for $n \gg 0$.

Work of Coates and Wiles for CM elliptic curves

Coates and Wiles proved the following result in the direction of BSD in 1976:

Theorem 0.13. *Assume* E *is an elliptic curve over* $\mathbb{Q}$ *with CM and that* $L(1, E) \neq 0$*. Then* $E(\mathbb{Q})$ *is finite.*

We outline the techniques used in their proof.

Suppose E is an elliptic curve over $\mathbb{Q}$ such that $\mathrm{End}_{\mathbb{C}}(E) = O =$ ring of integers of an imaginary quadratic field K. We assume 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 (CM elliptic curves defined over $\mathbb{Q}$ can only exist when the CM field K has class number 1), we can write $p = \pi\bar{\pi}$ where $\pi, \bar{\pi} \in O$ are complex conjugate.

Let $E[\pi^\infty] = \cup_n E[\pi^{n+1}]$. Adjoining coordinates to K, we obtain the field $F_\infty = K(E[\pi^\infty]) = \cup_n F_n$ where $F_n = K(E[\pi^{n+1}])$. Considering the action of $\mathrm{Gal}(F_\infty/K)$ on $E[\pi^\infty]$, we obtain an identification $\psi_E : \mathrm{Gal}(F_\infty/K) \xrightarrow{\cong} \mathbb{Z}_p^\times$. We write $\mathrm{Gal}(F_\infty/K) \cong \Delta \times \Gamma$ where $\Gamma = \mathrm{Gal}(F_\infty/F_0)$ and $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times$. If $F = F_0, \Delta$ can be identified with $\mathrm{Gal}(F/K)$ and there is a cononical isomorphism $\omega_E : \Delta \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$, corresponding to the action on $E[\pi]$. The extension F_∞/F is $\mathbb{Z}_p$ and the only prime of F lying above π is is ramified.

Suppose $E(\mathbb{Q})$ is infinite and P is a $\mathbb{Q}$-rational point on E of infinite order. We assume that P is a $\mathbb{Q}$-rational point of E of infinite order. Assume $P \notin \pi E(K)$ and that for each $n \geqslant 0, P_n \in E(\overline{\mathbb{Q}})$ satisfies $\pi^{n+1}P_n = P$. Then $P_0 \notin E(K)$. (Note that we can always find such a sequence of points since $[\pi^{n+1}] : E \xrightarrow{\times\pi^{n+1}} E$ is not surjective.)

Let $T_n = F_n\left(P_n\right)$ (the field obtained by adjoining the coordinates of P_n to F_n), $T_\infty = \cup_n T_n$. Then T_n/F_n is cyclic of order p^{n+1} and is unramified except at the unique prime of F_n over π. T_∞/K is Galois and $\mathrm{Gal}(T_\infty/F_\infty) \cong \mathbb{Z}_p$.

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 $\sigma_n(g) = g(P_n) - P_n \; \forall g \in G_K$. We can check that $\sigma_n|_{G_\infty}$ induces a compatible system of isomorphisms $\mathrm{Gal}(F_\infty(P_n)/F_\infty) \xrightarrow{\cong} E\left[\pi^{n+1}\right] \; \forall n \geqslant 0$, equivariant for the $\mathrm{Gal}\left(F_\infty/K\right)$ actions. 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 Γ_∞/F_∞ is ramified only at π, we have $T_\infty \subset M_\infty$ where M_∞ is the maximal abelian pro-p extension of F_∞, unramified everywhere except π.

Let $X = \mathrm{Gal}(L_\infty/F_\infty)$ where L_∞ is the pro-p Hilbert class field of $F_\infty, Y = \mathrm{Gal}(M_\infty/F_\infty)$ and $Z = \mathrm{Gal}(M_\infty/L_\infty)$, noting $L_\infty \subset M_\infty$ by definition. Then X, Y and Z are Λ-modules where $\Lambda = \mathbb{Z}_p[[T]]$.

M_∞ and L_∞ are Galois over $K \Rightarrow \Delta$ acts on all these modules too. Considering the Δ-components corresponding to ω_E, we obtain the exact sequence $0 \longrightarrow Z^{\omega_E} \longrightarrow Y^{\omega_E} \longrightarrow X^{\omega_E} \longrightarrow 0$ of Λ-modules.

The action of $\mathrm{Gal}(F_\infty/K)$ on $\mathrm{Gal}(T_\infty/F_\infty)$ by inner automorphisms induces a compatible system of isomorphisms $\mathrm{Gal}(F_\infty(P_n)/F_\infty) \xrightarrow{\cong} E\left[\pi^{n+1}\right] \; \forall n \geqslant 0$, equivariant for the $\mathrm{Gal}\left(F_\infty/K\right)$ actions. 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 Γ_∞/F_∞ is ramified only at π, we have $T_\infty \subset M_\infty$ where M_∞ is the maximal abelian pro-p extension of F_∞, unramified everywhere except π.

A crucial part of the Coates and Wiles argument is showing that T_∞/F_∞ is ramified at π. It then follows that $T_\infty \not\subset L_\infty \Rightarrow T_\infty \cap L_\infty$ is a finite extension of F_∞ since all nontrivial subgroups of $\mathrm{Gal}\left(T_\infty/F_\infty\right) = Z$ have finite index $\Rightarrow Z$ has quotient $\mathrm{Gal}(T_\infty/T_\infty \cap L_\infty)$ isomorphic to $\mathbb{Z}_p$, on which $\mathrm{Gal}(F_\infty/K)$ acts by ψ_E. Let $K_E = \psi_E|_\Gamma$. Then Z^{ω_E} has quotient isomorphic to $\Lambda/(\gamma_0 - \kappa_E(\gamma_0))$ as a Λ-module share γ_0 is the topological generator of T.

If F' is an algebraic extension of K, $\mathrm{Sel}_E(F')$ is an O-module and we can consider its π-primary subgroup $\mathrm{S}_E(F')_\pi$, which is a subgroup of $H^1(G_{F'}, E[\pi^\infty])$. Let $F' = F_\infty$. Then G_{F_∞} acts trivially on $E[\pi^\infty] \Rightarrow \mathrm{S}_E\left(F_\infty\right)$ is a subgroup of $\mathrm{Hom}(\mathrm{Gal}(F_\infty^{ab}/F_\infty), E[\pi^\infty])$. Coates proves that $\mathrm{S}_E\left(F_\infty\right)_\pi = \mathrm{Hom}(\mathrm{Gal}(M_\infty/F_\alpha), E\left[\pi^\infty\right])$. Therefore, $\mathrm{S}_E(F_\infty)_\pi$ is related to the Pontryagin dual $\mathrm{Hom}(Y, \mathbb{Q}_p/\mathbb{Z}_p)$ (they are isomorphic as groups but the action of $\mathrm{Gal}(F_\infty/K)$ is twisted).

Letting $r = \mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}_O(E(K))$, $\mathrm{Sel}_E(K)_\pi$ has a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$. Then the 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. Therefore, $\mathrm{Hom}_\Gamma(X^{\omega_E}, E[\pi^\infty])$ has 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 $\mathrm{Hom}_{T1}\left(Z^\omega E, E[\pi^\infty]\right)$ has $\mathbb{Z}_p$-crank at least 1. It is passible to show that this image then has $\mathbb{Z}_p$-corank exactly 1 and hence $\mathrm{Hom}_\Gamma\left(X_E^\omega, E\left[\pi^\infty\right]\right)$ has $\mathbb{Z}_p$-corank at least $r - 1$.

Setting $S = T - (\kappa_E(\gamma_0) - 1)$, $S^r \mid f_{Y^{\omega_E}}(T)$, $S \mid f_{Z^{\omega_E}}(T)$ and $S^{r-1} \mid f_{X^{\omega_E}}(T)$.

The divisibility should be exact. This is the case when $SH_E(K)_\pi$ is finite + a certain p-adic height pairing $E(K) \otimes_O K_\pi$ is non-degerente. Finiteness of $SH_E(K)_\pi \Rightarrow Y^{\omega_E}/SY^{\omega_E}$ has $\mathbb{Z}_p$-rank r. The nondegeneracy is shown to imply that $SY^{\omega_E}/S^2Y^{\omega_E}$ is finite, i.e. in the classification of the Λ-module Y^{ω_E}, there is no factor of the form $\Lambda/(S^a)$ for $a \geqslant 2$.

Coates and Wiles show that if $E(\mathbb{Q})$ is infinite, then the rational number $L(1, E/\mathbb{Q})/\Omega_E$ where Ω_E = real period of E is divisible by all primes in an infinite set, concluding that $L(1, E/\mathbb{Q}) = 0$.