Overview of some Iwasawa theory

Christian Wuthrich

23rd — 27th of July 2012

Contents

0 Introduction

This is the draft version of the notes to my lectures at Heidelberg in July 2012. The intention is to give an overview of some topics in Iwasawa theory. These lectures will contain a lot of definitions and results, but hardly any proofs and details. Especially I would like to emphasise that the word "proof" should actually be replaced by "sketch of proof" in all cases below.

Also I have no claim at making this a complete introduction to the subject, nor is the list of references at the end. For this the reader might find [14] a better source.

All computations were done in [46]. Any comments and corrections are very welcome.

It is my pleasure to thank Thanasis Bouganis, Sylvia Guibert, Chern-Yang Lee, Birgit Schmoetten-Jonas and Otmar Venjakob.

1 Iwasawa theory of the class group

Let F be a number field and let p be an **odd** prime. Suppose we are given a tower of Galois extensions $F = {}^0F \subset {}^1F \subset {}^2F \subset \cdots$ such that the Galois group of ${}^nF/F$ is cyclic of order p^n for all $n \geqslant 1$. Write ${}^nC$ for the p-primary part of the class group of ${}^nF$ and write p^{e_n} for its order.

Theorem 1 (Iwasawa 56 [15]). *There exist integers μ, λ, ν, and n_0 such that*

$$e_n = \mu\, p^n + \lambda\, n + \nu \qquad \text{for all } n \geqslant n_0.$$

1.1 $\mathbb{Z}_p$-extensions

Let me first describe the tower of extensions that we are talking about. Set ${}^\infty F = \bigcup {}^n F$. The extension ${}^\infty F/F$ is called a $\mathbb{Z}_p$-extension as its Galois group Γ is isomorphic to the additive group of p-adic integers since it is the projective limit of cyclic groups of order p^n. The most important example is the cyclotomic $\mathbb{Z}_p$-extension: If $F = \mathbb{Q}$, then the Galois group of $\mathbb{Q}(\mu_{p^n})/\mathbb{Q}$ is $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$, which is cyclic of order $(p-1)p^{n-1}$. So there is an extension ${}^{n-1}\mathbb{Q}/\mathbb{Q}$ contained in $\mathbb{Q}(\mu_{p^n})$ such that ${}^\infty\mathbb{Q}$ is a $\mathbb{Z}_p$-extension of $\mathbb{Q}$. For a general F, the cyclotomic $\mathbb{Z}_p$-extension is ${}^\infty F = {}^\infty\mathbb{Q} \cdot F$.

It follows from the Kronecker-Weber theorem that ${}^\infty\mathbb{Q}$ is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. It would be a consequence of Leopoldt's conjecture that the cyclotomic $\mathbb{Z}_p$-extension is the only one for any totally real number field, see [29, Theorem 11.1.2]. For a general number field F, the composition of all $\mathbb{Z}_p$-extension contains at least $\mathbb{Z}_p^{r_2+1}$ in its Galois group where r_2 denotes the number of complex places in F. For a imaginary quadratic number field F, for instance, the theory of elliptic curves with complex multiplication provides us with another interesting $\mathbb{Z}_p$-extension, the anti-cyclotomic $\mathbb{Z}_p$-extension. It can be characterised as the only $\mathbb{Z}_p$-extension ${}^\infty F/F$ such that ${}^\infty F/\mathbb{Q}$ is a non-abelian Galois extension.

Lemma 2 (Proposition 11.1.1 in [29]). *The only places that can ramify in ${}^\infty F/F$ divide p and at least one of them must ramify.*

In the cyclotomic $\mathbb{Z}_p$-extension of F, all places above p are ramified and there are only finitely many places above all other places.

1.2 The Iwasawa algebra and its modules

Let $\mathcal{O}$ be a "coefficient ring", for us this will always be the ring of integers in a p-adic field; so $\mathcal{O} = \mathbb{Z}_p$ is typical. There is a natural morphism between the group rings $\mathcal{O}\left[\mathrm{Gal}({}^n F/F)\right]$, which allows us to form the limit

$$\Lambda = \varprojlim_n \mathcal{O}\left[\mathrm{Gal}({}^n F/F)\right].$$

This completed topological group ring, called the Iwasawa algebra and also denoted by $\mathcal{O}[\![\Gamma]\!]$, is far better to work with than the huge group ring $\mathcal{O}[\Gamma]$.

Proposition 3. *To a choice of a topological generator γ of Γ, there is an isomorphism from Λ to the ring of formal power series $\mathcal{O}[\![T]\!]$ sending γ to $T+1$.*

The proof is given in Theorem 5.3.5 of [29]. By the Weierstrass preparation theorem, an element $f(T) \in \mathcal{O}[\![T]\!]$ can be written as a product of a power of the uniformiser of $\mathcal{O}$ times a unit of $\mathcal{O}[\![T]\!]$ and times a distinguished polynomial, which, by definition, is a monic polynomial whose non-leading coefficients belong to the maximal ideal.

Let ${}^n X$ be a system of abelian groups with an action by $\mathrm{Gal}({}^n F/F)$. If there is a naturally defined norm map ${}^{n+1}X \to {}^n X$, then we can form $X = \varprojlim {}^n X$ and consider it as a compact Λ-module. For instance the class groups ${}^n C$ above have a natural norm map between them. Also lots of naturally defined cohomology groups will have such a map, too. Suppose now $\mathcal{O}/\mathbb{Z}_p$ is unramified, otherwise the power of p below must be replaced by a power of the uniformiser of $\mathcal{O}$.

Proposition 4. *Let X be a finitely generated Λ-module. Then there exist integers r, s, t, $m_1, m_2, \ldots, m_s, n_1, n_2, \ldots n_t$, irreducible distinguished polynomials $f_1, f_2, \ldots f_t$, and a morphism of Λ-modules*

$$X \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda / p^{m_i}\Lambda \oplus \bigoplus_{j=1}^{t} \Lambda / f_j^{n_j}\Lambda$$

whose kernel and cokernel are finite.

Proofs can be found in [43], [29, Theorem 5.3.8] or quite different in [50, Theorem 13.12] and [20, Theorem 5.3.1]. The main reason is that Λ is a 2-dimensional local, unique factorisation domain.

As the ideals $f_j\Lambda$ and the integers $r,\ldots, n_t$ are uniquely determined by X, we can define the following invariants attached to X. The rank of X is $\mathrm{rank}_\Lambda(X) = r$. The μ-invariant is $\mu(X) = \sum_{i=1}^{s} m_i$ and the λ-invariant is $\lambda(X) = \sum_{j=1}^{t} n_j \cdot \deg(f_j)$. Finally, if $r = 0$,

$$\mathrm{char}(X) = p^{\mu(X)} \cdot \prod_{j=1}^{t} f_j^{n_j}\,\Lambda$$

is called the characteristic ideal of X. If $r = 0$, $s \leqslant 1$ and all f_j are pairwise coprime, then $X \to \Lambda/\mathrm{char}(X)$ has finite kernel and cokernel.

Let us summarise the useful properties of Λ-modules in a lemma. Write $X_{^n\Gamma}$ for the largest quotient of X on which ${}^n\Gamma = \mathrm{Gal}({}^\infty F/{}^n F)$ acts trivially.

Lemma 5. *Let X be a Λ-module.*

a). X is finitely generated if and only if X is compact and X_Γ is a finitely generated $\mathbb{Z}_p$-module.

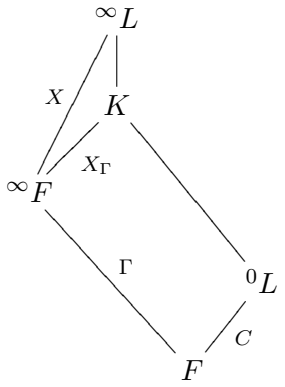
b). Suppose X is a finitely generated Λ-module. Then X is Λ-torsion, i.e., the Λ-rank of X is 0, if and only if $X_{^n\Gamma}$ has bounded $\mathbb{Z}_p$-rank.

c). If $X_{^n\Gamma}$ is finite for all n, then there are constants ν and n_0 such that $|X_{^n\Gamma}| = p^{e_n}$ with $e_n = \mu(X)\cdot p^n + \lambda(X)\cdot n + \nu$ for all $n \geqslant n_0$.

Proofs can be found in §5.3. of [29]. Note that if $X = \Lambda/f$ for an irreducible f, then $X_{^n\Gamma}$ is finite, unless f is a factor of the distinguished polynomial ${}^n\omega = (1+T)^{p^n} - 1$ corresponding to a topological generator of ${}^n\Gamma$.

1.3 Proof of Iwasawa's theorem

I will sketch the proof of theorem 1 only in the simplified case when F has a single prime $\mathfrak{p}$ above p and that this prime is totally ramified in ${}^\infty F/F$. Let ${}^n L$ be the p-Hilbert class field of ${}^n F$, i.e. the largest unramified extension of ${}^n F$ whose Galois group is abelian and a p-group. By class field theory the Galois group of ${}^n L/{}^n F$ is isomorphic to ${}^n C$.



Set $^\infty L = \bigcup {}^n L$, which is a Galois extension of $^\infty F$ with Galois group $X = \varprojlim {}^n C$. The action of ${}^n\Gamma$ on ${}^n C$ translates to an action of Γ on X given by the following. Let $\gamma \in \Gamma$ and $x \in X$. Choose a lift g of γ to the Galois group of $^\infty L/F$ and set $x^\gamma = gxg^{-1}$. So X is a compact Λ-module.

Define K to be the largest abelian extension of F inside $^\infty L$. Then $^0 L$ and $^\infty F$ are contained in K. The maximality of K shows that the Galois group of $K/^\infty F$ must be equal to X_Γ.

Since $K/^\infty F$ is unramified and $^\infty F/F$ is totally ramified at $\mathfrak{p}$, the inertia group I at a prime above $\mathfrak{p}$ in K gives a section of the map from $\mathrm{Gal}(K/F) \to \Gamma$. Since $K^I = {}^0 L$, we have $\mathrm{Gal}(K/^\infty F) = {}^0 C =: C$ and it has a trivial action of Γ on it. Hence C is isomorphic to X_Γ. Replacing in this argument F by ${}^n F$, we can also conclude that $X_{{}^n\Gamma} \cong {}^n C$.

In particular, it is always finite. Hence X is a finitely generated torsion Λ-module and lemma 5 c) implies the theorem. □

Iwasawa has given an example in [16] of a $\mathbb{Z}_p$-extension with $\mu(X) > 0$, however he conjectured that $\mu(X) = 0$ whenever the tower is the cyclotomic $\mathbb{Z}_p$-extension. This was shown to be true by Ferrero–Washington [11] when $F/\mathbb{Q}$ is abelian.

The above proof can also be used to show that if $F = \mathbb{Q}$ then the class group of ${}^n\mathbb{Q}$ has no p-torsion. Conjecturally this may even be true for $F = \mathbb{Q}(\mu_p)^+$, see §1.8.

1.4 Stickelberger elements

Let K be an abelian extension of $\mathbb{Q}$. By the Kronecker-Weber theorem, there is a smallest integer m such that $K \subset \mathbb{Q}(\mu_m)$ called the conductor of K. For each $a \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ write σ_a for the image of a under the map $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times \cong \mathrm{Gal}\big(\mathbb{Q}(\mu_m)/\mathbb{Q}\big) \to \mathrm{Gal}(K/\mathbb{Q}) = G$. The Stickelberger element for K is defined to be

$$\theta_K = -\frac{1}{m} \sum_{\substack{1 \leqslant a < m \\ (a,m)=1}} a \cdot \sigma_a^{-1} \ \in \mathbb{Q}[G]$$

and the Stickelberger ideal is $I = \mathbb{Z}[G] \cap \theta_K\, \mathbb{Z}[G]$. It is not difficult to show that $I = I'\theta_K$ with I' being the ideal in $\mathbb{Z}[G]$ generated by all $c - \sigma_c$ with $(c, m) = 1$, see [50, Lemma 6.9].

Stickelberger's theorem 6. *The Stickelberger ideal I annihilates the class group of K.*

This means that for any fractional ideal $\mathfrak{a}$ and any integer c coprime to m, the ideal $(c - \sigma_c)\,\theta_K(\mathfrak{a})$ is principal. It is important to note that this theorem does not say anything interesting when K is totally real as then θ_K is a multiple of the norm $N_{K/\mathbb{Q}}$. Hence it will not give us information about the class number of $\mathbb{Q}(\mu_p)^+$. For a quadratic imaginary field K, this is an algebraic version of the analytic class number formula for K, see the remark (b) after theorem 6.10 in [50].

Here is the idea of the proof, for details see [50, Theorem 6.10] or [20, Theorem 2.4].

Proof. We consider only the case $K = \mathbb{Q}(\mu_p)$ for some odd prime p. In each ideal class there is a prime ideal $\mathfrak{q}$ of degree 1, i.e. it is split above some prime $\ell \equiv 1 \pmod p$. Take

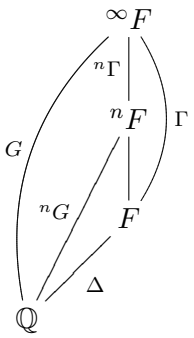
the Dirichlet character χ modulo ℓ of order p such that $\chi(a) \equiv a^{(\ell-1)/p} \pmod{\mathfrak{q}}$ for all a. Fix a primitive ℓ-th root of unity ξ. The Gauss sum of χ is defined to be

$$\mathrm{Ga}(\chi) = -\sum_{u \bmod \ell} \chi(u)\, \xi^u \ \in \mathbb{Q}(\mu_p, \mu_\ell).$$

One can show that $\mathrm{Ga}(\chi) \cdot \overline{\mathrm{Ga}(\chi)} = \ell$ and that we have $(c - \sigma_c)\,\mathrm{Ga}(\chi) \in \mathbb{Q}(\mu_p)$ for all c coprime to p. Finally a detailed analysis of the valuation of this Gauss sum at all primes above ℓ reveals that for any $\beta \in \mathbb{Z}[G]$ such that $\beta\theta_K \in \mathbb{Z}[G]$, we have that $\beta\theta_K(\mathfrak{q}) = \beta\big(\mathrm{Ga}(\chi)\big)\,\mathcal{O}_K$ is a principal ideal in the ring of integers $\mathcal{O}_K$ of K. □

1.5 p-adic L-functions

Consider the cyclotomic $\mathbb{Z}_p$-extension ${}^\infty F$ of $F = \mathbb{Q}(\mu_p)$ for some odd prime p. Write ${}^nG$ for the Galois group of ${}^nF = \mathbb{Q}(\mu_{p^{n+1}})$ over $\mathbb{Q}$ and $G = \varprojlim {}^nG = \mathrm{Gal}({}^\infty F/\mathbb{Q})$. Then $G \cong \Delta \times \Gamma$ with $\Delta = {}^0G$ and $\Gamma = \mathrm{Gal}({}^\infty F/F)$. We write γ_a for the image of σ_a in Γ. The cyclotomic character $\chi\colon G \to \mathbb{Z}_p^\times$ splits accordingly into the Teichmüller character $\omega\colon \Delta \to \mathbb{Z}_p^\times$ and $\kappa\colon \Gamma \to 1 + p\mathbb{Z}_p$. So for any $a \in \mathbb{Z}_p^\times$, the character ω sends σ_a to a $(p-1)$-st root of unity with $\omega(a) - a \in p\mathbb{Z}_p$ and $\kappa(\gamma_a) = \langle a \rangle = a/\omega(a)$.



For $i \in {}^{\mathbb{Z}}/_{(p-1)\mathbb{Z}}$, consider the projector

$$\varepsilon_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a)\, \sigma_a^{-1} \ \in \mathbb{Z}_p[\Delta]$$

to the ω^i-eigenspaces. We split up the Stickelberger element ${}^n\theta = \theta_{{}^nF} \in \mathbb{Q}[{}^nG]$ for the field ${}^nF$ into $p-1$ elements ${}^n\theta_i \in \mathbb{Q}_p[\mathrm{Gal}({}^nF/F)]$ defined by $\varepsilon_i \cdot {}^n\theta = {}^n\theta_i \cdot \varepsilon_i$; explicitly

$${}^n\theta_i = -\frac{1}{p^{n+1}} \sum_{\substack{1 \leqslant a < p^{n+1} \\ p \nmid a}} a \cdot \omega^{-i}(a) \cdot \gamma_a^{-1} \ \in \mathbb{Q}_p[\mathrm{Gal}({}^nF/F)]\,.$$

Lemma 7. *If $i \neq 1$ then ${}^n\theta_i \in \mathbb{Z}_p[\mathrm{Gal}({}^nF/F)]$ and if $i \neq 0, 1$, then $\theta_i = \big({}^n\theta_i\big)_{n \geqslant 1}$ belongs to $\varprojlim \mathbb{Z}_p[\mathrm{Gal}({}^nF/F)] = \Lambda$. If $i \neq 0$ is even then $\theta_i = 0$.*

Recall that the generalised Bernoulli numbers for a Dirichlet character χ of conductor m are defined by

$$\sum_{a=1}^{m} \chi(a) \frac{t\, e^{at}}{e^{mt} - 1} = \sum_{r=0}^{\infty} B_{r,\chi}\, \frac{t^r}{r!}.$$

An explicit computation [50, Theorem 7.10] links the elements θ_i to these Bernoulli numbers and the traditional Bernoulli numbers B_r. Recall that the $B_{r,\chi}$ and B_r also turn up as values of the complex L-function $L(s, \chi)$ and the Riemann zeta-function [50, Theorem 4.2]. Hence we find the interpolation property.

Theorem 8. *For any even integer $r \geqslant 1$, we have*

$$\kappa^{1-r}(\theta_{1-r}) = -(1-p^{r-1})\,\frac{B_r}{r} = (1-p^{r-1})\,\zeta(1-r).$$

Furthermore, for any $r \geqslant 1$ and any even $j \not\equiv r \pmod{p-1}$, we have

$$\kappa^{1-r}(\theta_{1-j}) = -\frac{B_{r,\omega^{j-r}}}{r} = L(1-r,\omega^j).$$

For any $s \in \mathbb{Z}_p$ we can extend $\kappa^s\colon \Gamma \to 1+p\mathbb{Z}_p$ linearly to $\kappa^s\colon \Lambda \to \mathbb{Z}_p$. The p-adic L-functions are defined to be $L_p(s,\omega^j) = \kappa^s(\theta_{1-j})$. To represent the p-adic L-function as a map $\chi \mapsto \chi(\theta_{1-j})$ is analogue to Tate's description of complex L-functions in his thesis; often these maps are written as measures on the Galois group Γ.

Now $L_p(s,\omega^j)$ is an analytic function in s and the existence of such a function satisfying the above theorem is equivalent to strong congruences between the values of $L(s,\omega^j)$ for negative integers s. For instance, one can deduce the Kummer congruences [50, Corollary 5.14] from the theorem.

Leopoldt showed that $L_p(1,\omega^j)$ satisfies a p-adic analytic class number formula involving the p-adic regulator, see [50, Theorems 5.18 and 5.24]. The p-adic L-function for $j=0$ corresponding to θ_1 is not in Λ, instead it has a simple pole at $s=1$.

The above L-functions are in fact the branches of the p-adic zeta-function discovered by Kubota and Leopoldt. There are generalisations to a much larger class of L-functions: Suppose K is a totally real number field and F/K an abelian extension of degree prime to p. Let χ be a character of the Galois group of F/K into the algebraic closure of $\mathbb{Q}_p$ and suppose that F is still totally real. Take $\mathcal{O}$ to be the ring $\mathbb{Z}_p[\chi]$ generated by the values of χ. Then there is a p-adic L-function $L_\chi \in \mathcal{O}[\![\Gamma]\!]$ such that $\kappa^s(L_\chi) = L_p(s,\chi)$ satisfies $L_p(1-r,\chi) = L(1-r,\chi\omega^{-r}) \cdot \prod_{\mathfrak{p}|p}(1-\chi\omega^{-r}(\mathfrak{p})N(\mathfrak{p})^{r-1})$ for all $r \geqslant 1$. See for instance [51].

1.6 The main conjecture

Let $3 \leqslant i \leqslant p-2$ be an odd integer. Consider the projective limit X of the p-primary parts of the class groups of ${}^nF = \mathbb{Q}(\mu_{p^{n+1}})$. Since Δ acts on this $\mathbb{Z}_p$-module, we can decompose it into eigenspaces for this action. Let $X_i = \varepsilon_i X$, which is now a finitely generated torsion $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$-module. Hence it makes sense to talk about its characteristic ideal.

Theorem 9 (Main conjecture)**.** *The ideal* $\mathrm{char}(X_i)$ *is generated by θ_i for all odd $3 \leqslant i \leqslant p-2$.*

This was first proven by Mazur-Wiles in [27], then generalised to totally real fields by Wiles in [51]. These proofs use crucially the arithmetic of modular forms. Later a proof was found using the Euler system of cyclotomic units, see [8] and the appendix in [20].

This theorem has many implications (some of which were known before the conjecture was proved). We can split up the p-primary part C of the class group of $\mathbb{Q}(\mu_p)$ into eigenspaces $C_i = \varepsilon_i C$

Theorem 10. *For every odd $3 \leqslant i \leqslant p-2$, the order of C_i is equal to the order of $\mathbb{Z}_p/B_{1,\omega^{-i}}$.*

Theorem 11 (Herbrand-Ribet [35]). *For any odd $3 \leqslant i \leqslant p-2$, the character ω^i appears in C/C^p if and only if p divides the numerator of B_{p-i}.*

1.7 Cyclotomic units

The p-adic L-function can also be constructed out of the following units. For each c coprime to m, the element $(\zeta_m^c - 1)/(\zeta_m - 1)$ is a unit in $\mathbb{Z}[\zeta_m]$ where ζ_m a primitive m-th root of unity, called a cyclotomic unit. On the one hand they are linked to the p-adic L-function as m varies in the powers of p; in fact the p-adic L-functions can be obtained as a logarithmic derivatives of the Coleman series associated to the cyclotomic unit. See Propositions 2.6.3 and 4.2.4 in [8]. On the other hand they are linked to the class group: When m is a power of p, the index of the group generated by the cyclotomic units and the roots of unity in $\mathbb{Q}(\mu_m)$ is equal to the class group order of $\mathbb{Q}(\mu_m)^+$ within the group of units in $\mathbb{Z}[\zeta_m]$.

The cyclotomic p-units $\zeta_m^c - 1$ form an Euler system, see §3.2 in [38], the appendix in [20] and §5.2 in [8], due to the fact that they make the Euler factors of the L-function appear in their compatibility with respect to the norm map:

$$N_{\mathbb{Q}(\mu_{m\ell})/\mathbb{Q}(\mu_m)}(\zeta_{m\ell} - 1) = (1 - \sigma_\ell^{-1})(\zeta_m - 1)$$

for any prime $\ell \nmid m$. These special elements provides a powerful way of bounding the class group in terms of values of the p-adic L-function and yield a proof of the main conjecture.

1.8 Vandiver's conjecture

The theory so far only covered the minus part of the class group, i.e., C_i for odd i. Note that $\oplus_{i \text{ even}} C_i$ is the p-primary part of the class group of $\mathbb{Q}(\mu_p)^+$.

Vandiver's conjecture 1. *The class number of $\mathbb{Q}(\mu_p)^+$ is not divisible by p.*

Although one may argue (see end of §5.4 in [50]) that it is not likely to hold for all p, it is known to hold for all primes $p \leqslant 39 \cdot 2^{22}$ see [5]. Moreover for all these 9163831 primes, the components C_i are always cyclic of order p and there are at most 7 non-trivial components. However, probably there are primes with C_i of order larger than p and probably the λ-invariant can get arbitrarily large.

It is known since Kummer that if p divides the class number of $\mathbb{Q}(\mu_p)^+$ then p divides $|C_i|$ for some odd i, see Corollary 8.17 in [50].

Proposition 12. *If Vandiver's conjecture holds for p, then C_i is isomorphic to $\mathbb{Z}_p/B_{1,\omega^{-i}}$ for all odd i. Moreover ${}^nC_i$ is a cyclic $\mathbb{Z}_p[\mathrm{Gal}(F_n/F)]$-module for all n.*

This is shown in Corollary 10.15 in [50].

Greenberg's conjecture 2 ([14]). *If F is totally real, then $X = \varprojlim {}^nC$ is finite.*

1.9 Examples

Let us first take $p = 5$ and so $i = 3$ is the only interesting value. We take γ_{1+p} to be the generator of Γ corresponding to $T + 1$. Then

$$\begin{aligned}{}^4\theta_3 =& 2 + 2\cdot 5 + 5^2 + 3\cdot 5^3 + 4\cdot 5^4 + \mathbf{O}(5^5) + \big(4 + 4\cdot 5 + 5^2 + 4\cdot 5^3 + \mathbf{O}(5^4)\big)\cdot T \\ &+ \big(1 + 5 + 4\cdot 5^2 + \mathbf{O}(5^4)\big)\cdot T^2 + \mathbf{O}(T^3)\end{aligned}$$

which is congruent to θ_3 modulo ${}^4\omega = (1+T)^{5^4} - 1$; in particular the above expression is the correct approximation for the 5-adic L-function θ_3. It is a unit in Λ as the leading term $-B_{1,\omega^2} = 2 + 2\cdot 5 + \cdots$ is a 5-adic unit. Of course this is not surprising as the class group of $\mathbb{Q}(\mu_5)$ is trivial. So here $X = 0$ and $e_n = 0$ for all n.

Now to the first irregular prime $p = 37$. Here the Bernoulli number B_{32} is divisible by 37. Accordingly, we expect a non-trivial ω^5 part in the class group of $\mathbb{Q}(\mu_{37})$. Indeed the approximation to the 37-adic L-function is

$$\begin{aligned}{}^3\theta_5 =& 14\cdot 37 + 33\cdot 37^2 + 13\cdot 37^3 + \mathbf{O}(37^4) + \big(16 + 6\cdot 37 + 32\cdot 37^2 + \mathbf{O}(37^3)\big)\cdot T \\ &+ \big(29 + 9\cdot 37 + 13\cdot 37^2 + \mathbf{O}(37^3)\big)\cdot T^2 + \mathbf{O}(T^3).\end{aligned}$$

This is not a unit as $-B_{1,\omega^{-5}}$ is divisible by 37. From the fact that the second coefficient is a unit, we conclude that θ_5 is a unit times a linear factor. Hence X is a free $\mathbb{Z}_{37}$-module of rank 1 and $e_n = n + 1$ for all n. The fact which underlies the proof of Ribet's theorem is that the Eisenstein series

$$\begin{aligned}G &= -\frac{B_{32}}{2\cdot 32} + \sum_{n\geqslant 1}\sum_{d|n} d^{31}q^n \\ &= \tfrac{7709321041217}{32640} + q + 2147483649\,q^2 + 617673396283948\,q^3 + 4611686020574871553\,q^4 + \cdots\end{aligned}$$

of weight 32 is congruent modulo one of the primes above 37 in $\mathbb{Q}(\mu_{12})$ to the cuspform

$$f = q + \zeta_{12}\,q^2 + \big(-\zeta_{12}^3 + \zeta_{12}^2 - \zeta_{12}\big)\,q^3 - \zeta_{12}^2\,q^4 + \big(2\,\zeta_{12}^3 + \zeta_{12}^2 - 2\,\zeta_{12}^2 - 2\big)\,q^5 + \cdots$$

of weight 2 for the group $\Gamma_1(37)$ and character ω^{30}.

2 Iwasawa theory for elliptic curves

2.1 Examples

Let ${}^\infty\mathbb{Q}/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and let $E/\mathbb{Q}$ be an elliptic curve. The theorem of Mordell-Weil shows that the group $E({}^n\mathbb{Q})$ is finitely generated for all n. Is this still true for $E({}^\infty\mathbb{Q})$? In particular is the rank of $E({}^n\mathbb{Q})$ bounded as n grows? The analogy with the case of global function fields suggests that this should be the case.

There is a second interesting group attached to E. For any elliptic curve E over a number field F, the Tate-Shafarevich group $Ш(E/{}^nF)$ is a certain torsion abelian group whose definition we give in §2.2. We write ${}^nШ$ for its p-primary part which is conjectured to be finite for all n. The first four examples were computed with the methods in [45].

2.1.1 Example 1

Let E be the elliptic curve given by

$$E: \qquad y^2 \,+\, x\,y \;=\; x^3 \;-\; 6511\,x \;-\; 203353$$

which has $E(\mathbb{Q}) = Ш(E/\mathbb{Q}) = 0$ and it is labelled 174b2 in Cremona's table [10]. It has bad reduction at 2 (additive), 3, and 29 (both split multiplicative).

If $p = 5$ then the rank of $E({}^n\mathbb{Q})$ is zero for all n and the group ${}^nШ$ is trivial, too. Since a p-torsion group can not act with a single fixed point on a p-primary group, we have that $E({}^n\mathbb{Q})$ has no p-torsion for all n.

2.1.2 Example 2

Let us take the same curve but now with $p = 7$. Then the rank will still be zero for all n. However if $|{}^nШ| = p^{e_n}$, then $e_n = p^n + 2n - 1$ for all $n \geqslant 0$. So the Tate-Shafarevich group will explode in this case. Note that this curve has a 7-isogeny defined over $\mathbb{Q}$ and one Tamagawa number is 7 and the number of points in the reduction over $\mathbb{F}_7$ has 7 points. So $p = 7$ appears in various places. In fact ${}^nШ$ is formed of $p^n - 1$ copies of $\mathbb{Z}/p\mathbb{Z}$ and two copies of $\mathbb{Z}/p^n\mathbb{Z}$.

2.1.3 Example 3

Again with the same curve, but this time for the prime $p = 13$. Once more the rank remains 0 in the tower, however the p-primary part of $Ш(E/{}^n\mathbb{Q})$ grows with

$$e_n = \Big\lfloor \frac{p}{p^2-1}\, p^n - \frac{n}{2} \Big\rfloor$$

for all n. This formula is shown in [18]. For instance $e_0 = e_1 = 0$, $e_2 = 12$, $e_3 = 168$, $e_4 = 2208$, ... Visibly the growth does not obey the same type of regularity as in the previous examples. The difference is that E has supersingular reduction at $p = 13$.

2.1.4 Example 4

Let us consider now the curve 5692a1

$$E: \qquad y^2 \;=\; x^3 \,+\, x^2 \;-\; 18\,x \;+\; 25$$

which has $E(\mathbb{Q}) = \mathbb{Z}\,(0,5) \oplus \mathbb{Z}(1,3)$. For $p = 3$, one can show that the rank is 6 over ${}^1\mathbb{Q}$ and it is 12 for all ${}^n\mathbb{Q}$ with $n \geqslant 2$. The 3-primary part of $Ш(E/{}^n\mathbb{Q})$ is trivial for all n. Note however that we do not know if $Ш(E/\mathbb{Q})$ is finite or not.

2.1.5 Example 5

Finally, consider the curve 11a3

$$E: \qquad y^2 \,+\, y \;=\; x^3 \;-\; x^2$$

and consider the anti-cyclotomic $\mathbb{Z}_3$-extension above $F = \mathbb{Q}\big(\sqrt{-7}\big)$. The construction of Heegner points allows us to produce points of infinite order ${}^nP \in E({}^nF)$. The tower of

points is compatible in the sense that the trace of ${}^nP$ to the layer below is $(-1)\cdot {}^{n-1}P$. It can be shown that these points and their Galois conjugates generate a group of rank p^n in $E({}^nF)$. Hence this is an example in which the rank is not bounded. See [1].

2.2 Selmer groups

Let E/F be an elliptic curve over a number field F. Set Σ to be the finite set of places in F consisting of all places above p, all places of bad reduction for E and all infinite places.

For any field K, we write $H^i(K,\cdot)$ for the group cohomology of continuous cochains for the profinite absolute Galois group $\mathrm{Gal}(\bar{K}/K)$. The notation $H^i_\Sigma(F,\cdot)$ will stand for the cohomology for the Galois group $G_\Sigma(F)$ of the maximal extension of F that is unramified outside F, see [29, §8.3]; it can also be described as the étale cohomology group $H^i_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_F)\setminus\Sigma,\cdot)$ for the corresponding étale group scheme. If the Galois module M is finite p-primary, then $H^i_\Sigma(F,M)$ is finite, see [29, Theorem 8.3.19]. If M is a finitely generated $\mathbb{Z}_p$-module then so is $H^i_\Sigma(F,M)$, see [38, Proposition B.2.7]. For any abelian group A, we will denote the Pontryagin dual $\mathrm{Hom}_{\mathbb{Z}}(A,{}^{\mathbb{Q}}\!/_{\mathbb{Z}})$ by $\hat{A}$.

For any finite extension K/F, we define the Tate-Shafarevich group $Ш(E/K)$ to be the kernel of the localisation map

$$H^1(K,E)\to\prod_v H^1(K_v,E)$$

where the product runs over all places v of K and K_v denotes the completion at v. The non-trivial elements in $Ш(E/K)$ have an interpretation as curves of genus 1 defined over K with Jacobian isomorphic to E and which are counter-examples to the Hasse principle, see [28, §17]. It is known that $Ш(E/K)$ is a torsion abelian group such that the Pontryagin dual of the p-primary part is a finitely generated $\mathbb{Z}_p$-module for every prime p. It is conjectured that $Ш(E/K)$ is finite.

Let m be a power of p. For any extension K of F, the long exact sequence of cohomology for $E[m]$ gives the Kummer exact sequence

$$0\longrightarrow {}^{E(K)}\!/_{mE(K)}\xrightarrow{\kappa} H^1\big(K,E[m]\big)\longrightarrow H^1(K,E)[m]\longrightarrow 0.$$

For any finite extension K of F, we define the m-Selmer group $\mathrm{Sel}^m(E/K)$ as the elements in $H^1(K,E[m])$ that restrict to elements in the image of the local Kummer map $\kappa_v\colon E(K_v)/p^kE(K_v)\to H^1(K_v,E[m])$ for all places v of K. This contains naturally $E(K)/mE(K)$ as a subgroup whose quotient is $Ш(E/K)[m]$. Since all cocycles in the Selmer group are unramified outside Σ, we get an exact sequence

$$0\longrightarrow \mathrm{Sel}^m(E/K)\longrightarrow H^1_\Sigma\big(K,E[m]\big)\longrightarrow\bigoplus_{v\in\Sigma}H^1(K_v,E)[m].$$

In particular, this shows that $\mathrm{Sel}^m(E/K)$ is finite. We can now form the two limits, induced by the inclusion and the multiplication by p map between $E[p^k]$ and $E[p^{k+1}]$. We set

$$\begin{aligned}\mathfrak{S}(E/K) &= \varinjlim_k \mathrm{Sel}^{p^k}(E/K)\ \subset H^1_\Sigma(K,W) \qquad \text{and}\\ \mathfrak{S}(E/K) &= \varprojlim_k \mathrm{Sel}^{p^k}(E/K)\ \subset H^1_\Sigma(K,T)\end{aligned}$$

where $T = \varprojlim_k E[p^k]$ is the (compact) p-adic Tate module and $W = \varinjlim_k E[p^k] = E[p^\infty]$ is the (discrete) p-primary torsion of E. It is true that $\varprojlim H^1_\Sigma\big(K, E[p^k]\big) = H^1_\Sigma(K, T)$ by an argument of Tate, see [29, Corollary 2.3.5].

The corresponding limit version of the Mordell-Weil group are $\varinjlim E(K)/p^k E(K)$ and $\varprojlim E(K)/p^k E(K)$. The first can be seen to be equal to $E(K) \otimes_{\mathbb{Z}} {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}$, which is isomorphic to a direct sum of $\mathrm{rank}(E(K))$ copies of ${}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}$. The latter is equal to $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p$, which is equal to the sum of $\mathrm{rank}(E(K))$ copies of $\mathbb{Z}_p$ plus the finite group $E(K)[p^\infty]$. By passing to the limits, we find the exact sequences

$$0 \longrightarrow E(K) \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} \longrightarrow Ш(E/K) \longrightarrow Ш(E/K)[p^\infty] \longrightarrow 0$$

$$0 \longrightarrow E(K) \otimes \mathbb{Z}_p \longrightarrow \mathfrak{S}(E/K) \longrightarrow \varprojlim_k Ш(E/K)[p^k] \longrightarrow 0$$

where the lower sequence remains exact because we have taken projective limits of finite groups. The group on the right hand side of the second line is a free $\mathbb{Z}_p$-module which is conjecturally trivial. The first line combines nicely the rank information with the Tate-Shafarevich group. The Pontryagin duals of the first line and all the groups in the second line are finitely generated $\mathbb{Z}_p$-modules.

Later in §4, we will give another description of $Ш(E/K)$ which does not use the Kummer map, but uses the modules W and T only.

2.3 Iwasawa theory for the Selmer group

Given a $\mathbb{Z}_p$-extension ${}^\infty F/F$, we consider the limit $Ш(E/{}^\infty F) = \varinjlim_n Ш(E/{}^n F)$ and its dual

$$X = Ш(\widehat{E/{}^\infty F}) = \varprojlim_n Ш(\widehat{E/{}^n F}) \tag{1}$$

which is naturally a compact Λ-module. The maps are induced by the natural inclusion $E({}^n F) \to E({}^{n+1} F)$ and the restriction map on the Tate-Shafarevich groups. Hence, if the Mordell-Weil group stabilises after a few steps, as in all but the last example above, then X will contain a $\mathbb{Z}_p$-module of this rank. The other natural limit $\varprojlim_n \mathfrak{S}(E/{}^n F)$ with respect to the corestriction map is less interesting: If the Mordell-Weil group stabilises, meaning that $E({}^\infty F) = E({}^n F)$ for some n, and the Tate-Shafarevich groups are finite, then this limit is trivial.

Lemma 13. *The Selmer group X is a finitely generated Λ-module for any $\mathbb{Z}_p$-extension.*

Proof. We should show by lemma 5 that X_Γ is a finitely generated $\mathbb{Z}_p$-module; this is the dual of the Γ-fixed part of $Ш(E/{}^\infty F)$. Later in theorem 20, we will show that this is not too far from the dual of $Ш(E/F)$, which is a finitely generated $\mathbb{Z}_p$-module. □

Conjecture 3 (Mazur [23])**.** *If E has good ordinary reduction at all places in F above p and ${}^\infty F/F$ is the cyclotomic $\mathbb{Z}_p$-extension, then the Selmer group X is a torsion Λ-module.*

Note that this conjecture implies, by proposition 4, that the largest free $\mathbb{Z}_p$-module in X has finite rank $\lambda(X)$, so by the above this will imply that the rank of $E({}^n F)$ stabilises. Moreover we have:

Proposition 14. *If the conjecture holds then $E(^\infty F)$ is a finitely generated $\mathbb{Z}$-module. Suppose that $Ш(E/^nF)[p^\infty]$ is finite for all n, then there are constants μ, λ, ν, n_0 such that if $\big|Ш(E/^nF)[p^\infty]\big| = p^{e_n}$, then $e_n = \mu\, p^n + \lambda\, n + \nu$ for all $n \geqslant n_0$.*

Proof. The first part is Theorem I.5 in [12]. For the second part, we will have to show that $X_{^n\Gamma}$ is very close to the dual of $\mathcal{S}(E/^nF)$ for all n. This is done in the control theorem 21 below. □

As shown by the examples 2.1.4 and 2.1.5, none of the two assumptions in Mazur's conjecture can be removed. Here are two important result in support of the conjecture.

Theorem 15 (Mazur [23])**.** *If $E(F)$ and $Ш(E/F)[p^\infty]$ are finite, then the conjecture holds.*

The main result of Kato in [17] implies the following.

Theorem 16. *Let E be an elliptic curve defined over $\mathbb{Q}$ and let F be an abelian extension of $\mathbb{Q}$. Suppose that E has good ordinary reduction at p, then the Selmer group for the cyclotomic $\mathbb{Z}_p$-extension is a torsion Λ-module.*

2.4 Mazur-Stickelberger elements

Let $E/\mathbb{Q}$ be an elliptic curve. We will suppose that E has good reduction at p. Let ω_E be a Néron differential on E; this is just $\frac{dx}{2y}$ when E is given by a global minimal model. The canonical lattice Z_E for E is the image of $\int : H_1\big(E(\mathbb{C}), \mathbb{Z}\big) \to \mathbb{C}$ sending a closed path γ on $E(\mathbb{C})$ to $\int_\gamma \omega_E$. We define Ω_E to be the smallest positive element of Z_E.

The theorem of modularity [4] shows that there exists a morphism φ_E of curves $X_0(N) \to E$ defined over $\mathbb{Q}$. We take one of minimal degree. If f is the newform corresponding to the isogeny class of E, then there is a natural number c_E, called the Manin constant, such that $c_E \cdot \varphi_E^*(\omega_E)$ is equal to the differential $2\pi i f(z)dz$ on $X_0(N)$ corresponding to f, written here as a differential in the variable z on the upper half plane $\mathcal{H}$. For the so-called optimal curve in the isogeny class one expects $c_E = 1$.

For any rational number $r = \frac{a}{m}$, consider the ray from r to $i\,\infty$ in the upper half plane. Its image in $X_0(N)(\mathbb{C})$ is a (not necessarily closed) path $\{r, \infty\}$ between two cusps.

Proposition 17 (Manin [22])**.** *There is a natural number $t \geqslant 1$ such that, for all $r \in \mathbb{Q}$, the value of $\lambda_f(r) = 2\pi i \int_{i\infty}^r f(z)\, dz$ belongs to $\frac{1}{t}\, Z_E$.*

This is clear for the closed paths, i.e., when r is $\Gamma_0(N)$-equivalent to $i\infty$. The proof for general r uses the Hecke operators T_ℓ on $X_0(N)$.

We define the (plus) modular symbol $[r]^+$ by

$$[r]^+ = \frac{1}{\Omega_E} \cdot \mathrm{Re}\Big(2\pi i \int_{i\infty}^r f(z)\, dz\Big) \ \in \mathbb{Q},$$

see [10] for more details. For an abelian field K of conductor m, we define the Stickelberger element for E to be

$$\Theta_{E/K} = \sum_{\substack{1 \leqslant a < m \\ (a,m)=1}} \Big[\frac{a}{m}\Big]^+ \sigma_a \ \in \mathbb{Q}\big[\mathrm{Gal}(K/\mathbb{Q})\big].$$

Let ℓ be a prime of good reduction. The ℓ-th coefficient a_ℓ of f satisfies $\ell - a_\ell + 1 = \#E(\mathbb{F}_\ell)$. If ℓ does not divide m, then

$$N_{\mathbb{Q}(\mu_{m\ell})/\mathbb{Q}(\mu_m)}\big(\Theta_{E/\mathbb{Q}(\mu_{m\ell})}\big) = (-\sigma_\ell)\big(1 - a_\ell\,\sigma_\ell^{-1} + \sigma_\ell^{-2}\big)\big(\Theta_{E/\mathbb{Q}(\mu_m)}\big),$$

which can be deduced from the action of the Hecke operator T_ℓ on $X_0(N)$.

2.5 The p-adic L-function

Let p be a prime of good reduction for E. Write now ${}^n\Theta_E$ for the Stickelberger element for the field ${}^n\mathbb{Q}$ and write ${}^nG = \mathrm{Gal}({}^n\mathbb{Q}/\mathbb{Q})$. We define the map $j\colon \mathbb{Q}[{}^nG] \to \mathbb{Q}[{}^{n+1}G]$ to send an element of ${}^nG$ to the sum over all its preimages in ${}^{n+1}G$. Then the norm $N\colon \mathbb{Q}[{}^{n+1}G] \to \mathbb{Q}[{}^nG]$ sends ${}^{n+1}\Theta_E$ to

$$N\big({}^{n+1}\Theta_E\big) = a_p \cdot {}^n\Theta_E - j\big({}^{n-1}\Theta_E\big).$$

This is shown using the Hecke operator T_p. Let α be a root of the polynomial $X^2 - a_p\,X + p$. We set

$$ {}^n\mathfrak{L}_E = \frac{1}{\alpha^{n+1}} \cdot {}^n\Theta_E - \frac{1}{\alpha^{n+2}}\, j\big({}^{n-1}\Theta_E\big) \tag{2}$$

for all $n \geqslant 1$. Then $\mathfrak{L}_E = ({}^n\mathfrak{L}_E)_{n\geqslant 1}$ belongs to $\varprojlim \mathbb{Q}[\mathrm{Gal}({}^n\mathbb{Q}/\mathbb{Q})]$ and it is called the p-adic L-function of E. Explicitly, we have

$${}^n\mathfrak{L}_E = \sum_{\substack{1\leqslant a<p^{n+1}\\ p\nmid a}} \left(\frac{1}{\alpha^{n+1}}\left[\frac{a}{p^{n+1}}\right]^+ - \frac{1}{\alpha^{n+2}}\left[\frac{a}{p^n}\right]^+\right)\cdot \gamma_a.$$

Suppose now that E has good ordinary reduction at p. Then a_p is a p-adic unit and hence we can find one root α which belongs to $\mathbb{Z}_p^\times$. Because the denominator of $[\frac{a}{m}]$ is uniformly bounded, $\mathfrak{L}_E$ actually belongs to $\mathbb{Q}_p \otimes \Lambda$ and in many cases it is known that $\mathfrak{L}_E \in \Lambda$. For the supersingular case there is no unit root α and $\mathfrak{L}_E$ will never belong to Λ, see [34].

Theorem 18. *The p-adic L-function satisfies the interpolation properties*

$$\mathbb{1}(\mathfrak{L}_E) = \left(1 - \frac{1}{\alpha}\right)^2 \cdot \frac{L(E,1)}{\Omega_E} \tag{3}$$

and

$$\chi(\mathfrak{L}_E) = \frac{\mathrm{Ga}(\chi)}{\alpha^{n+1}} \cdot \frac{L(E,\bar{\chi},1)}{\Omega_E} \tag{4}$$

for all character χ of conductor p^{n+1} on Γ, i.e, that factor through $\mathrm{Gal}({}^n\mathbb{Q}/\mathbb{Q})$ but not through $\mathrm{Gal}({}^{n-1}\mathbb{Q}/\mathbb{Q})$.

The proof connecting the corresponding finite sums of modular symbols to the Mellin transform of the modular form can be found in formula (8.6) and §14 of [26].

Theorem 19 (Rohrlich [36])**.** *Only finitely many of the values $\chi(\mathfrak{L}_E)$ in equation (4) are zero. In particular $\mathfrak{L}_E \neq 0$.*

Again, we can define the analytic function $L_p(E,s) = \kappa^{s-1}(\mathcal{L}_E)$. If $L(E,1) \neq 0$, we know that $E(\mathbb{Q})$ is finite. As a consequence of the above theorem, we see that $L_p(E,1) \neq 0$ as $\alpha \neq 1$. Moreover the value $L_p(E,1)$ is then predicted by the Birch and Swinnerton-Dyer conjecture.

Conjecture 4 (p-adic version of the Birch and Swinnerton-Dyer conjecture [26])**.** *The order of vanishing of $L_p(E,s)$ at $s=1$ is equal to the rank of $E(\mathbb{Q})$. The leading term of its series at $s=1$ is equal to*

$$\left(1-\frac{1}{\alpha}\right)^2 \cdot \frac{\mathrm{Reg}_p(E/\mathbb{Q}) \cdot \#Ш(E/\mathbb{Q}) \cdot \prod_v c_v}{\left(\#E(\mathbb{Q})_{\mathrm{tors}}\right)^2}$$

where c_v are the Tamagawa numbers and $\mathrm{Reg}_p(E/\mathbb{Q})$ is the p-adic regulator, see §3.2.

It would be very interesting to know that the order of vanishing of $L_p(E,s)$ is equal to the order of vanishing of $L(E,s)$. However this is only known when the p-adic L-function vanishes to order at most 1 by [30].

2.6 The main conjecture

Let $E/\mathbb{Q}$ and suppose E has good ordinary reduction at p. By theorem 16, we can associate to E the characteristic ideal $\mathrm{char}(X)$ of the dual of the Selmer group in (1). Under the same hypothesis, we have constructed a p-adic L-function (2).

Conjecture 5 (Main conjecture)**.** *The p-adic L-function $\mathcal{L}_E$ is a generator for the characteristic ideal $\mathrm{char}(X)$.*

The other series of lectures will talk about the main result by Skinner and Urban on this conjecture.

The generalisations to higher weight modular forms for $\Gamma_0(N)$ with $p \nmid N$ and $p \nmid a_p$ is fairly straight forward, see [26]. For the extensions to $p \mid N$, but $p^2 \nmid N$, one has to be a bit careful as the case of split multiplicative reduction behaves differently due to the presence of exceptional zeroes because $\alpha = 1$. Finally the generalisation to the supersingular case is clearly much more complicated. To my knowledge the generalisation to additive reduction, i.e., when $p^2 \mid N$, is not yet fully done.

3 The leading term formula

3.1 Control theorem

As before let E/F be an elliptic curve and let ${}^\infty F/F$ be a $\mathbb{Z}_p$-extension. Recall that X is the dual of the limit Selmer group $Ш(E/{}^\infty F)$ as defined in (1) and we are interested in comparing X_Γ with the dual of $Ш(E/F)$. For a place $v \in \Sigma$, write ${}^\infty J_v = \prod_{v|w} H^1({}^\infty F_w, E)[p^\infty]$. We have the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ш(E/{}^\infty F)^\Gamma & \longrightarrow & H^1_\Sigma({}^\infty F, W)^\Gamma & \longrightarrow & \bigoplus_{v\in\Sigma} \left({}^\infty J_v\right)^\Gamma \\ & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \oplus_v \gamma_v} \\ 0 & \longrightarrow & Ш(E/F) & \longrightarrow & H^1_\Sigma(F, W) & \longrightarrow & \bigoplus_{v\in\Sigma} H^1(F_v, E)[p^\infty]. \end{array} \tag{5}$$

We want to bound the kernel and cokernel of α. Even if it is clear that $E({}^{\infty}F)^{\Gamma} = E(F)$, it is not obvious what happens to the map $E(F) \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} \to \big(E({}^{\infty}F) \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\big)^{\Gamma}$ as a non-divisible point in $E(F)$ can become divisible by p in $E({}^{n}F)$.

Theorem 20. *The kernel of α is finite and the dual of the cokernel is a finitely generated $\mathbb{Z}_p$-module.*

Proof. The inflation-restriction sequence [29, Proposition 1.6.6] for the H^i_Σ-cohomology of $W = E[p^\infty]$ gives that the kernel of β is $H^1\big(\Gamma, H^0_\Sigma({}^{\infty}F, W)\big)$ and the cokernel lies in $H^2\big(\Gamma, H^0_\Sigma({}^{\infty}F, W)\big)$. Now the dual of $D = H^0({}^{\infty}F, W) = E({}^{\infty}F)[p^\infty]$ has $\mathbb{Z}_p$-rank at most 2. Hence the dual of the exact sequence

$$0 \longrightarrow D^{\Gamma} \longrightarrow D \xrightarrow{\gamma-1} D \longrightarrow D_{\Gamma} \longrightarrow 0$$

shows that $H^1(\Gamma, D) = D_\Gamma$ has the same corank as $D^\Gamma = E(F)[p^\infty]$, which is finite. Hence the kernel of β and α are finite. In fact, if D is finite as in almost all cases, then the kernel of β has the same order as $E(F)[p^\infty]$.

The cokernel of β is trivial, because $H^2(\Gamma, D) = \varinjlim_k H^2\big(\Gamma, E({}^{\infty}F)[p^k]\big)$ and the latter groups are trivial because Γ has cohomological dimension 1, see [29, Proposition 1.6.13]. Since β is surjective we see that the duals of $H^1_\Sigma({}^{\infty}F, W)^\Gamma$ and $Ш(E/{}^{\infty}F)^\Gamma$ are finitely generated $\mathbb{Z}_p$-modules. □

Note that this proves lemma 13 saying that X is a finitely generated Λ-module.

Theorem 21 (Control theorem)**.** *Suppose that E has good ordinary reduction at all primes that ramify in ${}^{\infty}F/F$. Then the map α has finite kernel and cokernel.*

Proof. From the previous proof, we see that we are left to show that the cokernel of α is finite. By the snake lemma applied to (5), it suffices to show that the kernel of $\oplus\gamma_v$ is finite under our hypothesis.

Let $v \in \Sigma$. By local Tate duality [49], the group $H^1(F_v, E)[p^\infty]$ is the Pontryagin dual of the p-adic completion $E(F_v)^\star = \varprojlim E(F_v)/p^k E(F_v)$ of the local points. The structure of elliptic curves over local fields, see chapter 7 in [44], can be used to show that $E(F_v)^\star$ is finite if $v \nmid p$ and it is a finitely generated $\mathbb{Z}_p$-module of rank $[F_v : \mathbb{Q}_p]$ if $v \mid p$. Choose a place w above v in ${}^{\infty}F$. We wish to show that the kernel of

$$\gamma_v \colon H^1(F_v, E)[p^\infty] \longrightarrow H^1({}^{\infty}F_w, E)[p^\infty]$$

is finite. Again by Tate duality this map is dual to the norm map

$$\widehat{\gamma_v} \colon E({}^{\infty}F)^\star \longrightarrow E(F_v)^\star.$$

The following lemmas will conclude this proof. □

We will write $x \overset{\times}{=} y$ if there is a p-adic unit u such that $x = u \cdot y$.

Lemma 22. *If v splits completely in ${}^{\infty}F/F$, then $\ker \gamma_v = 0$. Otherwise, if v is unramified, then $\#\ker \gamma_v \overset{\times}{=} c_v$, the Tamagawa number of E/F_v. In particular $\ker \gamma_v$ is non-zero for only finitely many v.*

Proof. If v splits completely, then ${}^{\infty}F_w = F_v$ and the "norm" map is clearly surjective.

First assume $v \nmid p$. The local extension ${}^{\infty}F_w/F_v$ is unramified and so the Néron model of E will not change in this extension. Let Φ be its group of components and write E_v^0 for the connected component of the special fibre. Then we have that

$$0 \longrightarrow E_v^0(\mathbb{F}_v)^\star \longrightarrow E(F_v)^\star \longrightarrow \Phi(\mathbb{F}_v)^\star \longrightarrow 0$$

because the points in the formal group $\hat{E}$ are divisible by p when $v \nmid p$. Now the norm map on the left hand side is surjective because of Lang's theorem [19]. On the right hand side instead the norm map will be the zero map for sufficiently large n. Hence $\ker \gamma_v$ is dual to $\Phi(\mathbb{F}_v)^\star$.

Now assume $v \mid p$, but the extension ${}^{\infty}F/F$ is unramified at v. The argument is the same as above, except that we now have to show that the norm is surjective on the formal groups. That is done in the part a) of the following lemma. □

Lemma 23. *Let E be an elliptic curve over a p-adic field K and let L/K be a cyclic extension of degree a power of p. Let $\mathfrak{m}_L$ and $\mathfrak{m}_K$ be the maximal ideals of L and K respectively.*

a). If L/K is unramified then the norm map on the formal group $\hat{E}(\mathfrak{m}_L) \to \hat{E}(\mathfrak{m}_K)$ is surjective.

b). If L/K is ramified and E has good ordinary reduction. Then the cokernel of the norm map on the formal groups is finite.

c). If $v \mid p$ is totally ramified and E has good ordinary reduction, then $\#\ker \gamma_v \overset{\times}{=} N_v^2$ where N_v is the number of points in the reduction $E(\mathbb{F}_v)$.

Proof. For the proof of the first point uses the filtration by $\hat{E}(\mathfrak{m}^k)$, the formal logarithm that gives an isomorphism $\hat{E}(\mathfrak{m}_L^k) \cong 1 + \mathfrak{m}_L^k$ for large enough k, the fact that $H^1(\mathbb{F}_L/\mathbb{F}_K, \mathbb{F}_L) = 0$ for the residue fields, and the surjectivity of the norm map on units [42, Proposition V.3].

The proof of the latter two can be found in [21]. It relies on the fact that the formal group of E becomes isomorphic to the multiplicative formal group over the ring of integers of the completion of the maximal unramified extension of F_v. □

A different and more accessible proof of item c) in the above lemma is explained in Lemma 4.6 in [12]. It should be noted that the both item b) and c) are no longer valid when the reduction is supersingular. The theory in the case of good supersingular reduction at primes above p is quite different.

One can now add a proof for theorem 15. If $E(F)$ and $Ш(E/F)[p^\infty]$ are both finite, then so is $\mathcal{S}(E/F)$. By the control theorem 21, this implies that X_Γ is finite. Since the Γ-coinvariants $\Lambda_\Gamma \cong \mathbb{Z}_p$ of Λ are not finite, we see that X is a torsion Λ-module. In fact, we see that this holds for all $\mathbb{Z}_p$-extensions, not just the cyclotomic. In example 2.1.5, the rank of $E(F)$ is 1.

3.2 p-adic heights

We will now construct an analogue to the real-valued Néron-Tate height. We present a version inspired by [2]. Let E/F be an elliptic curve and we suppose that E has good ordinary reduction at all places above p that are ramified. To each cohomology class in $H^1(F,T)$ represented by a cocycle $\xi\colon G_F = \mathrm{Gal}(\bar{F}/F) \to T = T_p(E)$, we associate an extension

$$0 \longrightarrow T_p\mu \longrightarrow T_\xi \longrightarrow T \longrightarrow 0$$

where $T_p\mu = \varprojlim \mu[p^k]$, also denoted by $\mathbb{Z}_p(1)$, is a free $\mathbb{Z}_p$-module of rank 1 on which G_F acts via the cyclotomic character. As a $\mathbb{Z}_p$-module $T_\xi = T_p\mu \oplus T$, but the G_F-action is given by

$$\sigma(\zeta, P) = \Big(\sigma(\zeta) \cdot e\big(\xi_\sigma,\, \sigma(P)\big),\ \sigma(P)\Big) \qquad \text{for } \zeta \in T_p\mu \text{ and } P \in T,$$

with $e\colon T \times T \to T_p\mu$ denoting the Weil-pairing [44, §3.8]. It is not hard to show that the class of the extension T_ξ does not depend on the chosen cocycle and that the boundary maps $\partial\colon H^i(F,T) \to H^{i+1}(F, T_p\mu)$ are given by applying the Weil-pairing to the cup-product with ξ, at least up to sign.

Consider now the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(F,T_p\mu) & \longrightarrow & H^1(F,T_\xi) & \longrightarrow & H^1(F,T) & \longrightarrow & H^2(F,T_p\mu) \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \prod_v H^1(F_v,T_p\mu) & \longrightarrow & \prod_v H^1(F_v,T_\xi) & \longrightarrow & \prod_v H^1(F_v,T) & \xrightarrow{\prod \partial_v} & \prod_v H^2(F_v,T_p\mu) \end{array} \tag{6}$$

with the product running over all places in F. It follows from global class field theory that the downwards arrow on the right is injective [29, Corollary 9.1.8.ii] if T is replaced by μ_{p^k}; that the limit is still surjective needs an additional argument [47, Corollary to Proposition 2.2]. On the left we have the map from the p-adic completion $(F^\times)^\star$ of $F^\times$ to $\prod_v (F_v^\times)^\star$.

Choose an topological generator γ. Let $l\colon \Gamma \to \mathbb{Z}_p$ be the map that send γ to 1. For each place v consider the composition

$$\lambda_v\colon F_v^\times \longrightarrow \mathbb{A}_F^\times \longrightarrow \Gamma \xrightarrow{\ l\ } \mathbb{Z}_p$$

where $\mathbb{A}_F^\times$ is the idèle group of F and the map that follows it is the reciprocity map. This map extends to the completion $\lambda_v\colon (F_v^\times)^\star \to \mathbb{Z}_p$. In case ${}^\infty F/F$ is the cyclotomic $\mathbb{Z}_p$-extension, then l is a multiple of $\log_p \circ \kappa$. For finite places v away from p, the map is simply $\lambda_v(x) = (\log_p(\kappa(\gamma))^{-1} \cdot \log(\#\mathbb{F}_v) \cdot v(x)$ where $\mathbb{F}_v$ is the residue field. For places above p, we get $\lambda_v(x) = -(\log_p(\kappa(\gamma))^{-1} \cdot \log_p(N_{K_v/\mathbb{Q}_p}(x))$.

Suppose now ξ belongs to $\mathfrak{S}(E/F)$. Let $\mathfrak{S}(E/F)^0$ be the subgroup of $\mathfrak{S}(E/F)$ of all elements η such that $\mathrm{res}_v(\eta) \in E(F_v)^\star$ lies in the image of the norm from $E({}^\infty F_w)^\star$ for all places v. By lemma 22 and 23, this subgroup has finite index in $\mathfrak{S}(E/F)$. Let $\eta \in \mathfrak{S}(E/F)^0$. Since both $\mathrm{res}_v(\eta)$ and $\mathrm{res}_v(\xi)$ belong to the image of $E(F_v)^\star$ inside $H^1(F_v,T)$, their cup-pairing is trivial. This is again a consequence of local Tate duality [49]. Hence $\mathrm{res}_v(\eta)$ is sent to 0 by ∂_v. By the injectivity of the right arrow in (6), we conclude that there is an element ζ in $H^1(F,T_\xi)$ that maps to η in $H^1(F,T)$.

For each place v, we will define a local lift $\zeta_v \in H^1(F_v, T_\xi)$. Since $\eta \in \text{Ш}(E/F)^0$, there is an element $\tilde{\eta}_v \in H^1({}^\infty F_w, T)$ whose norm is $\text{res}_v(\eta)$. Pick any lift of $\tilde{\eta}_v$ to $H^1({}^\infty F_w, T_\xi)$ and define ζ_v to be its norm in $H^1(F_v, T_\xi)$.

By construction $\text{res}_v(\zeta) - \zeta_v \in H^1(F_v, T_\xi)$ maps to 0 in $H^1(F_v, T)$ and hence we can viewed it as an element in $H^1(F_v, T_p\mu) = (F_v^\times)^\star$. We set

$$\langle \xi, \eta \rangle = \sum_v \lambda_v\big(\text{res}_v(\zeta) - \zeta_v\big) \ \in \mathbb{Z}_p.$$

It is not hard to check that this element is independent of the choices made, because both $(F^\times)^\star$ and the norms from $H^1({}^\infty F_w, T_p\mu)$ lie in the kernel of $\sum_v \lambda_v$.

Since $\text{Ш}(E/F)^0$ has finite index, we can linearly extend this to a pairing on $\text{Ш}(E/F)$ with values in $\mathbb{Q}_p$. This is called the canonical p-adic height pairing corresponding to the $\mathbb{Z}_p$-extension and the choice of γ. Note that this construction only works under the assumption that E has good ordinary reduction at the ramified places. For the generalisation to any Galois representation, which is de Rham at places above p, see [33, §3.1.2].

There is a variant of this construction: Let $\xi \in \text{Ш}(E/F)^0$ and $\eta = ({}^n\eta)_n \in \text{Ш}(E/{}^\infty F)$, then one can construct in a similar way an element of ${}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}$. This time one lifts $\text{res}_w({}^n\eta) \in H^1({}^n F_w, W)$ to $H^1({}^n F_w, T_\xi \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p})$ etc. It turns out that the map $\hat{\delta}\colon \text{Ш}(E/F)^0 \to \text{Hom}\big(\text{Ш}(E/{}^\infty F), {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\big) = X$ has its image in X^Γ. Now the p-adic height pairing can be described involving the map $\pi\colon X^\Gamma \to X \to X_\Gamma$.

Proposition 24 (Proposition 3.4.5. in [31]). *There is a commutative diagram*

$$\begin{array}{ccccc} X_\Gamma & & \xleftarrow{\quad\pi\quad} & & X^\Gamma \\ {\scriptstyle\alpha}\downarrow & & & & \uparrow{\scriptstyle\hat{\delta}} \\ \widehat{\text{Ш}(E/F)} & \xrightarrow[\iota]{} & \text{Hom}_{\mathbb{Z}_p}\big(\text{Ш}(E/F), \mathbb{Z}_p\big) & \xleftarrow[h_p]{} & \text{Ш}(E/F)^0 \end{array} \tag{7}$$

where h_p is the p-adic height pairing and ι is a naturally defined surjective $\mathbb{Z}_p$-morphism with finite kernel.

Finally one should mention that the p-adic height pairing has also an analytic description using canonical p-adic sigma-functions σ_v for all ramified places. These are well-explained in [25] and a fast algorithm for computing them was found in [24] using Kedlaya's algorithm. For instance, if $E/\mathbb{Q}$ and $P = (x, y) \in E(\mathbb{Q})$ is a point that has good reduction everywhere and reduces to 0 at p, then $h_p(P) = \log_p(\sigma_p(P)) - \log_p(e)$ where e is the square root of the denominator of x. In general the formula allows one to compute the p-adic height with only the information of E over F together with the explicit maps λ_v.

Conjecture 6 (Schneider [39]). *The canonical p-adic height pairing for the cyclotomic $\mathbb{Z}_p$-extension on an elliptic curve with good ordinary reduction at all places above p is non-degenerate.*

Suppose $\text{Ш}(E/F)[p^\infty]$ is finite. Choose a basis of $E(F)$ modulo torsion and let $\text{Reg}_\gamma(E/F) \in \mathbb{Q}_p$ be the determinant of the p-adic height pairing on this basis. The number $\text{Reg}_p(E/F) = \text{Reg}_\gamma(E/F) \cdot \log_p(\kappa(\gamma))^{\text{rank}\, E(F)}$ is independent of the choice of γ. The above conjecture then says that $\text{Reg}_\gamma(E/F) \neq 0$ in the cyclotomic case. For the anti-cyclotomic $\mathbb{Z}_p$-extension it can well be that the p-adic height is degenerate.

3.3 Leading term

The following theorem was proved by Perrin-Riou for curves with complex multiplication then in general by Schneider [40]. See [32] for the details to complete our sketch of proof.

Let ${}^{\infty}F/F$ be a $\mathbb{Z}_p$-extension such that all ramified places are totally ramified. Write $\Sigma(\mathrm{ram})$ for the set of all the ramified places in F and denote by S the set of all places that split completely in ${}^{\infty}F$.

As before, identify Λ with $\mathbb{Z}_p[\![T]\!]$ via the choice of a topological generator γ. Let $F_X(T) \in \mathbb{Z}_p[\![T]\!]$ be a generator of the characteristic ideal for X.

Theorem 25. *Suppose E has good ordinary reduction at all ramified places above p and suppose that the canonical p-adic height for ${}^{\infty}F/F$ is non-degenerate. Then*

a). X is Λ-torsion;

b). the characteristic series $F_X(T)$ has a zero of order $\mathrm{rank}_{\mathbb{Z}_p}\big(\mathfrak{S}(E/F)\big)$ at $T=0$;

c). if $Ш(E/F)[p^\infty]$ is finite then the leading term $F_X^*(0)$ of $F_X(T)$ at $T=0$ satisfies

$$F_X^*(0) \overset{\times}{=} \prod_{v\in\Sigma(\mathrm{ram})} N_v^2 \cdot \frac{\mathrm{Reg}_p(E/F)\cdot \#Ш(E/F)[p^\infty]\cdot \prod_{v\notin S} c_v\cdot}{\big(\#E(F)_{\mathrm{tors}}\big)^2}.$$

If the main conjecture holds for a curve $E/\mathbb{Q}$, then the finiteness of $Ш(E/\mathbb{Q})[p^\infty]$ and the non-degeneracy of the p-adic height pairing imply the p-adic BSD conjecture, up to a p-adic unit in the leading term. This is because $1-1/\alpha \overset{\times}{=} N_v$. Theorem 25 together with Kato's theorem 29 can be used to give a new efficient algorithm [45] for the determination of the rank of $E(\mathbb{Q})$ and upper bounds of $Ш(E/\mathbb{Q})[p^\infty]$ for almost all p.

The proof of this theorem follows surprisingly closely what Tate [48] did in the function field case to reduce BSD to the finiteness of the p-primary part of the Tate-Shafarevich group. The algebraic part relies on the following lemma which can be deduced from proposition 4.

Lemma 26. *Let X be a finitely generated Λ-module and suppose the cokernel of $\pi\colon X^\Gamma \to X_\Gamma$ is finite. Then*

a). X is Λ-torsion;

b). π has finite kernel;

c). the leading term of its characteristic series satisfies $F_X^*(0) \overset{\times}{=} \frac{\#\mathrm{coker}(\pi)}{\#\ker(\pi)} =: q(\pi)$.

If X_Γ is finite, then $q(\pi)$ is the Euler-characteristic $\prod_{i=0}^{1} \#H^i\big(\Gamma, \mathfrak{S}(E/{}^{\infty}F)\big)^{(-1)^i}$. For a proof in this case see §3 of [7] or in §4 of Greenberg's part in [6].

Proof of theorem 25. From diagram (7) and the assumption that h_p has finite kernel and cokernel, we find that π must have finite cokernel. Hence the lemma applies and we are left to determine the value of $q(\pi)$. Note that δ has now also finite kernel and cokernel.

Global duality [29, Theorem 8.6.13] gives us a long exact sequence.

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ш(E/F) & \longrightarrow & H^1_\Sigma(F,W) & & \\ & & & & & \searrow & \\ & & & & & & \bigoplus_{v\in\Sigma} H^1(F_v,E)[p^\infty] \\ & & & & & \swarrow & \\ 0 & \longleftarrow & H^2_\Sigma(F,W) & \longleftarrow & \widehat{\mathfrak{S}(E/F)} & & \end{array}$$

Because X is Λ-torsion we have that $\varprojlim \mathfrak{S}(E/^nF) = 0$ as shown in [31, §3.1.7]. When taking the limit of these above sequence over n, the resulting exact sequence is

$$0 \longrightarrow Ш(E/^\infty F) \longrightarrow H^1_\Sigma({}^\infty F, W) \longrightarrow \bigoplus_{v\in\Sigma} {}^\infty J_v \longrightarrow 0$$

where ${}^\infty J_v = \prod_{w|v} H^1({}^\infty F_w, E)[p^\infty]$.

Now we can produce a big diagram with exact rows:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & Ш(E/^\infty F)^\Gamma & \longrightarrow & H^1_\Sigma({}^\infty F,W)^\Gamma & \longrightarrow & \bigoplus_{v\in\Sigma} ({}^\infty J_v)^\Gamma & \longrightarrow & Ш(E/^\infty F)_\Gamma & \longrightarrow & H^1_\Sigma({}^\infty F,W)_\Gamma & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \oplus\gamma_v} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \varepsilon} & & \\ 0 & \longrightarrow & Ш(E/F) & \longrightarrow & H^1_\Sigma(F,W) & \longrightarrow & \bigoplus_{v\in\Sigma} H^1(F_v,E)[p^\infty] & \longrightarrow & \widehat{\mathfrak{S}(E/F)} & \longrightarrow & H^2_\Sigma(F,W) & \longrightarrow & 0 \end{array}$$

To show that the two right squares commute requires some work [31, §4.4 and 4.5]. By the way, I am cheating slightly as in fact the term $\mathfrak{S}(E/F)$ should be replaced by $\mathfrak{S}(E/F)^0$ and other terms should be modified accordingly. Also one has to show that $({}^\infty J_v)_\Gamma = 0$ to get the exactness in the top right corner; this follows from the triviality of $H^2(F_v,E)[p^\infty]$, again by local Tate duality.

Next, the transgression map ε is part of the short exact sequences from the degenerating Hochschild-Serre spectral sequence. It is injective and the cokernel is equal to $H^2_\Sigma({}^\infty F,W)^\Gamma$. However the group $H^2_\Sigma({}^\infty F,W)$ is trivial as shown in §3.4.1 in [31]. This shows that ε is an isomorphism. So the big diagram gives the equality

$$q(\alpha)\cdot q(\beta)^{-1}\cdot q\Big(\bigoplus \gamma_v\Big)\cdot q(\delta) = 1.$$

On the other hand the diagram (7) gives the equation

$$q(\hat{\delta})\cdot q(\pi)\cdot q(\alpha)\cdot q(\iota) = q(h_p)$$

In the proof of theorem 20 we have seen that $q(\beta) \stackrel{\times}{=} \big(\#E(F)_{\mathrm{tors}}\big)^{-1}$ if $E({}^\infty F)[p^\infty]$ is finite, which follows without too much difficulty from [21] under our assumptions. In lemma 22 and 23 we found that

$$q\Big(\bigoplus \gamma_v\Big) \stackrel{\times}{=} \Big(\prod_{v\notin S} c_v \cdot \prod_{v\in\Sigma(\mathrm{ram})} N_v^2\Big)^{-1}.$$

Finally, we know that $E(F)\otimes\mathbb{Z}_p$ has index $\#E(F)[p^\infty]$ in $\mathfrak{S}(E/F)$ if the Tate-Shafarevich group is finite. Hence

$$q(h_p) \stackrel{\times}{=} \frac{\mathrm{Reg}_p(E/F)}{\#E(F)_{\mathrm{tors}}.}$$

It is not difficult to see that $q(\iota) = \#Ш(E/F)[p^\infty]$ under our hypothesis. The neglected index of $[\mathfrak{S}(E/F) : \mathfrak{S}(E/F)^0]$ would have cancelled. □

4 Selmer groups for general Galois representations

Let T be a free $\mathbb{Z}_p$-module of finite rank with an action of $G_F = \mathrm{Gal}(\bar{F}/F)$. We will suppose that only finitely many places ramify in T; so T has an action of $G_\Sigma(K)$ for a finite set Σ containing the places above p and ∞. Let $V = T \otimes \mathbb{Q}_p$ and $W = V/T = T \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}$. So far we were dealing with the example $T_E = T_pE$ and $W_E = E[p^\infty]$ and V_E is then a 2-dimensional Galois representation. But of course there are lots of other examples, such as more general subquotients of étale cohomology groups of varieties defined over F with $\mathbb{Q}_p$-coefficients or Galois representation attached to modular forms.

We wish to define the Selmer group but we have no longer a Kummer map $\kappa :? \to H^1(F_v, W)$ or $? \to H^1(F_v, T)$. In order to understand how to define it in the general case, we look at how we could describe the image of κ in the case of an elliptic curve.

4.1 Local conditions at places away from p

Let $v \in \Sigma$ be a prime not dividing p. Then the Kummer maps are $E(F_v) \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} \to H^1(F_v, W_E)$ and $E(F_v)^\star \to H^1(F_v, T_E)$. Recall that $E(F_v)$ contains with finite index a group isomorphic to $\mathfrak{m}_v$, the maximal ideal of F_v. Hence $E(F_v) \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} = 0$ and $E(F_v)^\star = E(F_v)[p^\infty] = W_E^{G_{F_v}}$ is finite.

Here is the general definition for $v \nmid p$. Define the subgroup $H^1_f(F_v, V)$ by the exact sequence

$$0 \longrightarrow H^1_f(F_v, V) \longrightarrow H^1(F_v, V) \longrightarrow H^1(I, V) \tag{8}$$

where $I = I_v$ is the inertia subgroup in $\mathrm{Gal}(\bar{F}_v/F_v)$. By the restriction-inflation sequence, $H^1_f(F_v, V)$ is isomorphic to $H^1(F_v^{\mathrm{ur}}/F_v, V^I)$ where F_v^{ur} is the maximal unramified extension of F_v. Then we define $H^1_f(F_v, W)$ as the image of $H^1_f(F_v, V)$ under the map $H^1(F_v, V) \to H^1(F_v, W)$. Also $H^1_f(F_v, T)$ is the preimage of $H^1_f(F_v, V)$ from the map $H^1(F_v, T) \to H^1(F_v, V)$.

For the case of the elliptic curve, we find $H^1_f(F_v, V_E) = 0$ for all $v \nmid p$: In fact, we have in general that $H^1_f(F_v, V) = V^I/(\mathrm{Fr}_v - 1)V^I$ by Lemma 1.3.2 in [38]. If the reduction is good then $V_E^I = V_E$ by the Néron–Ogg–Shafarevich criterion [44, Theorem 7.7.1] and Fr_v, the Frobenius of $\mathrm{Gal}(F_v^{\mathrm{ur}}/F_v)$, acts with eigenvalues different from 1. If the reduction is multiplicative, then $V_E^I \cong \mathbb{Q}_p(1)$ and the group $H^1_f(F_v, V_E)$ is again trivial. Finally if the reduction is additive, then $V_E^I = 0$. Since we have the exact sequence

$$0 = V_E^{G_{F_v}} \longrightarrow W_E^{G_{F_v}} \longrightarrow H^1(F_v, T_E) \longrightarrow H^1(F_v, V_E) \longrightarrow H^1(F_v, W_E)$$

we obtain that $H^1_f(F_v, W_E) = 0 = E(F_v) \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}$ and $H^1_f(F_v, T_E) = E(F_v)[p^\infty] = E(F_v)^\star$.

It would be tempting to define in general $H^1_f(F_v, W)$ without passing through V by replacing V with W in (8). However the elliptic curve example explains that this does not work. In general, we have that $H^1_f(F_v, W)$ is the divisible part of the kernel of $H^1(F_v, W) \to H^1(I_v, W)$ and $H^1_f(F_v, T)$ has finite index in the corresponding kernel for T; see [38, Lemma 1.3.5].

4.2 Local conditions at places above p

Let now v be a place above p. The definition of the group $H^1_f(F_v, V)$ is given by Bloch-Kato [3] by asking that

$$0 \longrightarrow H^1_f(F_v, V) \longrightarrow H^1(F_v, V) \longrightarrow H^1(F_v, V \otimes B_{\text{cris}}) \tag{9}$$

is an exact sequence, where B_{cris} is a certain period ring of Fontaine.

Now, if V is ordinary, one can give an easier definition. Here a general representation V is called ordinary if there is a decreasing filtration $\text{Fil}^i V$ of $\text{Gal}(\bar{F}_v/F_v)$-stable subspaces of V such that the inertia group I acts like the i-th power of the cyclotomic character on the quotient $\text{Fil}^i V/\text{Fil}^{i+1} V$. For an ordinary elliptic curve, we consider the kernel of the reduction on $E[p^k]$ which is the p^k-torsion $\widehat{E}[p^k]$ of the formal group. Then $\text{Fil}^1 V_E = T_p\widehat{E} \otimes \mathbb{Q}_p$ sits in the middle between $\text{Fil}^2 V_E = 0$ and $\text{Fil}^0 V_E = V_E$.

We set $F^+V = \text{Fil}^1 V$ and then [13] shows that

$$0 \longrightarrow H^1_f(F_v, V) \longrightarrow H^1(F_v, V) \longrightarrow H^1\left(I, {}^{V}\big/_{F^+V}\right) \tag{10}$$

is exact. The subgroups $H^1_f(F_v, W)$ and $H^1_f(F_v, T)$ are again defined as the image and preimage of $H^1_f(F_v, V)$, respectively.

4.3 The Selmer groups

The Selmer groups are now defined as the following kernels. They are often denoted by $H^1_f(F, W)$ and $H^1_f(F, T)$.

$$0 \longrightarrow \text{Ш}(W) \longrightarrow H^1_\Sigma(F, W) \longrightarrow \bigoplus_{v\in\Sigma} {H^1(F_v, W)}\big/{H^1_f(F_v, W)}, .$$

$$0 \longrightarrow \text{Ш}(T) \longrightarrow H^1_\Sigma(F, T) \longrightarrow \bigoplus_{v\in\Sigma} {H^1(F_v, T)}\big/{H^1_f(F_v, T)}$$

They are now defined only in terms of T and equal to the previously defined Selmer group for elliptic curves. If $\text{Ш}(E/F)$ is finite, then we have a way to determine the rank and the order of the Tate-Shafarevich group from the Galois representation V_E only. Note that the L-function $L(E, s)$ is also constructed from V_E only.

For instance, if $T = \mathbb{Z}_p$ has a trivial G_F-action on it, then $\text{Ш}({}^{\mathbb{Q}_p}/_{\mathbb{Z}_p})$ is the dual of the p-primary part of the class group. If $T = \mathbb{Z}_p(1)$ is of rank 1 with the action by G_F given by the cyclotomic character, then $\text{Ш}\big({}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}(1)\big)$ sits in a short exact sequence between $\mathcal{O}_F^\times \otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$ and the p-primary part of the class group.

5 Kato's Euler system

In this section we give a quick and very imprecise overview of the work of Kato in [17] where he proves one divisibility in the main conjecture for elliptic curves (and modular forms of higher weight). See also [41] and [9].

Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime at which E has good reduction. Let N be the conductor of E. We assume that $E[p]$ is an irreducible $G_{\mathbb{Q}}$-module and hence all $G_{\mathbb{Q}}$-stable lattices in V_pE are equal up to a scaling factor.

5.1 Construction of the Euler system

Let M be an integer. Pick an integer $m \geqslant 5$ coprime to $6M$. For any elliptic curve A over a field $k/\mathbb{Q}$, we can construct a division polynomial $f_m \in k(A)^\times$, which is a function of divisor $\mathrm{div}(f_m) = -m^2(O) + \sum_{P\in A[m]}(P)$ normalised such that $[a]^* f_m = f_m$ for all a coprime to m. Consider the maps $g_i^{(m)}$ for $i = 1$ or 2 that sends a point in the modular curve $Y(M)$ represented by (A, Q_1, Q_2) to $f_m(Q_i)$. It is a rational function on $Y(M)$ without zero, i.e., $g_i \in \mathcal{O}(Y(M))^\times$, called a Siegel unit. It can be shown that the function $g_i = g_i^{(m)} \otimes \frac{1}{m^2-1}$ in $\mathcal{O}(Y(M)) \otimes \mathbb{Q}$ is independent of the choice of m. They give rise to Beilinson element in $K_2\big(\mathcal{O}(Y(M))^\times\big) \otimes \mathbb{Q}$, defined as the Steinberg symbol $\{g_1, g_2\}$.

Such pairs of modular units can now be sent through a chain of maps. For a square-free r coprime to pN, we take $M = N\,p^{n+1}\,r$ and consider the map

$$X(M) \longrightarrow X(N) \otimes {}^n\mathbb{Q}(\mu_r) \xrightarrow{\varphi_E} E \otimes {}^n\mathbb{Q}(\mu_r).$$

We chase the pair of modular units through the maps (see §8.4 in [17])

$$\begin{array}{ccc}
\mathcal{O}\big(Y(M)\big)^\times \times \mathcal{O}\big(Y(M)\big)^\times & \xrightarrow{\cup} & H^2_{\text{ét}}\Big(Y(N)/{}^n\mathbb{Q}(\mu_r),\ \mathbb{Z}_p(2)\Big) \\
 & & \Big\downarrow \text{twist à la Soulé} \\
 & & H^2_{\text{ét}}\Big(Y(N)/{}^n\mathbb{Q}(\mu_r),\ \mathbb{Z}_p(1)\Big) \\
 & & \Big\downarrow \\
 & & H^1\Big({}^n\mathbb{Q}(\mu_r), H^1_{\text{ét}}\big(\overline{Y(N)},\ \mathbb{Z}_p(1)\big)\Big) \\
 & & \Big\downarrow \\
 & & H^1\big({}^n\mathbb{Q}(\mu_r),\ T_E\big) \otimes \mathbb{Q}
\end{array}$$

where we used that $H^1_{\text{ét}}\big(\overline{E}, \mathbb{Z}_p(1)\big) = T_E$. Poincaré duality relates $H^1_{\text{ét}}\big(\overline{Y_0(N)}, \mathbb{Q}_p\big)$ to modular symbols as it is equal to the homology $H_1\big(\overline{X_0(N)}(\mathbb{C}), \{\text{cusps}\}, \mathbb{Z}\big) \otimes \mathbb{Q}_p$ of paths between cusps. See §4.7 and §8.3 in [17].

The image of the Siegel units produce now elements ${}^n c_r$ in $H^1_\Sigma\big({}^n\mathbb{Q}(\mu_r), T\big)$ that form an Euler system for a certain lattice T in $T_E \otimes \mathbb{Q}_p$. See example 13.3 in [17] for details. In particular, $({}^n c_r)_n$ belongs to $\varprojlim_n H^1({}^n\mathbb{Q}(\mu_r), T)$. If ℓ is a prime not dividing rpN then they satisfy the norm relations

$$\mathrm{cor}\big({}^n c_{r\ell}\big) = \Big(1 - \frac{a_\ell}{\ell}\,\sigma_\ell^{-1} + \frac{1}{\ell}\,\sigma_\ell^{-2}\Big)({}^n c_r).$$

See proposition 8.12 in [17] for the precise statement deduced from the Hecke operators on the modular curves.

5.2 Relation to p-adic L-function

Suppose E has good ordinary reduction at p and let $\alpha \in \mathbb{Z}_p$ be the unit root of Frobenius. We continue to assume that $E[p]$ is irreducible. The general "dual of exponential" à la

Bloch-Kato has a very explicit description for elliptic curves. It is the map

$$\exp^*\colon E({}^n\mathbb{Q}_p)^\star \to \left(E({}^n\mathbb{Q}_p)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\right)^\wedge \to {}^n\mathbb{Q}_p$$

which is a linear extension of the formal logarithm on the formal group with respect to the invariant differential ω_E. Based on the work of Coleman, Perrin-Riou has constructed an Iwasawa theoretic version which interpolates these maps:

$$\mathrm{Col}\colon \mathbb{H}^1_s := \left(E({}^\infty\mathbb{Q}_p)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\right)^\wedge \to \Lambda.$$

It is an injective Λ-morphism with finite cokernel such that for all character χ of Γ of conductor p^{n+1}, we have

$$\chi\big(\mathrm{Col}(z)\big) = \frac{\mathrm{Ga}(\chi)}{\alpha^{n+1}} \sum_{\sigma\in \mathrm{Gal}({}^n\mathbb{Q}/\mathbb{Q})} \bar{\chi}(\sigma)\exp^*\big(\sigma({}^n z)\big).$$

See the appendix of [37] for details of the construction.

One of the main theorems of Kato is

Theorem 27. *There is an element ${}^\infty c \in \varprojlim H^1_\Sigma({}^n\mathbb{Q}, T)\otimes\mathbb{Q}$ closely related to the ones constructed above such that $\mathrm{Col}({}^\infty c) = \mathcal{L}_E$*

This is theorem 16.6 in [17] with the "good choice" of γ^+ as in 17.5. This is the technically most difficult part of [17]. It implies that the Euler system is non-trivial by theorem 19. If the representation $\bar{\rho}\colon G_\mathbb{Q} \to \mathrm{Gl}(T_E)$ is surjective, then ${}^\infty c$ is integral by his theorem 12.5.4.

5.3 Euler system method

For each i, the limit $\mathbb{H}^i = \varprojlim_n H^i_\Sigma({}^n\mathbb{Q}, T_E)$ is a finitely generated Λ-module, which does not depend on Σ as long as it contains p. The existence of a non-trivial Euler system ${}^\infty c_r \in \varprojlim H^1({}^n\mathbb{Q}(\mu_r), T_E)$ proves the following.

Theorem 28 (Theorem 12.4 in [17])**.** *a). $\mathbb{H}^2$ is Λ-torsion.*

b). $\mathbb{H}^1$ is a torsion-free Λ-module of rank 1.

c). If $E[p]$ is an irreducible $G_\mathbb{Q}$-module, then $\mathbb{H}^1$ is free of rank 1.

See also [38]. The statement that $\mathbb{H}^2$ is Λ-torsion is called the weak Leopoldt conjecture and it is believed to hold for many Galois representations T. Global duality together with basic results deduced from the above theorem provides us with an exact sequence

$$0 \longrightarrow \mathbb{H}^1 \big/ {}^\infty c\,\Lambda \longrightarrow \mathbb{H}^1_s \big/ {}^\infty c\,\Lambda \longrightarrow X \longrightarrow \mathbb{H}^2 \longrightarrow 0.$$

Here ${}^\infty c \in \mathbb{H}^1\otimes\mathbb{Q}$ is the part of the Euler system that is sent to the p-adic L-function $\mathcal{L}_E$ by the Coleman map; therefore Col sends the second term into $\Lambda/\mathcal{L}_E\Lambda$ with finite cokernel. Hence the main conjecture is equivalent to

Conjecture 7. *The characteristic ideal of* $\mathbb{H}^2$ *and of* $\mathbb{H}^1/^\infty c\Lambda$ *are equal.*

The advantage of this formulation is that it does not involve the p-adic L-function and makes sense in the supersingular case as well.

Theorem 29 (Theorem 17.4 in [17])**.** *Suppose E has good ordinary reduction at p. Then*

a). X is a torsion Λ-module;

b). there is an integer $t \geqslant 0$ such that the characteristic ideal $\mathrm{char}(X)$ *divides $p^t \mathcal{L}_E \Lambda$;*

c). if the representation $\bar{\rho}\colon G_{\mathbb{Q}} \to \mathrm{Gl}(T_E)$ is surjective, then $\mathrm{char}(X)$ *divides $\mathcal{L}_E \Lambda$.*

References

[1] Massimo Bertolini, *Iwasawa theory for elliptic curves over imaginary quadratic fields*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 1–25, 21st Journées Arithmétiques (Rome, 2001).

[2] Spencer Bloch, *A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture*, Invent. Math. **58** (1980), no. 1, 65–76.

[3] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[4] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[5] Joe P. Buhler and David Harvey, *Irregular primes to 163 million*, Math. Comp. **80** (2011), no. 276, 2435–2444.

[6] John Coates, Ralph Greenberg, Kenneth A. Ribet, and Karl Rubin, *Arithmetic theory of elliptic curves*, Lecture Notes in Mathematics, vol. 1716, Springer, 1999, Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12–19, 1997, Edited by C. Viola.

[7] John Coates and Ramdorai Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Mathematics, vol. 88, Narosa Publishing House, 2000.

[8] ———, *Cyclotomic fields and zeta values*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006.

[9] Pierre Colmez, *La conjecture de Birch et Swinnerton-Dyer p-adique*, Astérisque (2004), no. 294, ix, 251–319.

[10] John E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[11] Bruce Ferrero and Lawrence C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), no. 2, 377–395.

[12] Ralph Greenberg, *Introduction to Iwasawa theory for elliptic curves*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, pp. 407–464.

[13] ———, *Iwasawa theory for p-adic representations*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 97–137.

[14] ———, *Iwasawa theory—past and present*, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 335–385.

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

[16] ———, *On the μ-invariants of $\mathbb{Z}_l$-extensions*, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo, 1973, pp. 1–11.

[17] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque (2004), no. 295, ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III.

[18] Masato Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I*, Invent. Math. **149** (2002), no. 1, 195–224.

[19] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

[20] ———, *Cyclotomic fields I and II*, second ed., Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990, With an appendix by Karl Rubin.

[21] Jonathan Lubin and Michael I. Rosen, *The norm map for ordinary abelian varieties*, J. Algebra **52** (1978), no. 1, 236–240.

[22] Juri I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[23] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[24] Barry Mazur, William Stein, and John Tate, *Computation of p-adic heights and log convergence*, Doc. Math. (2006), no. Extra Vol., 577–614.

[25] Barry Mazur and John Tate, *The p-adic sigma function*, Duke Math. J. **62** (1991), no. 3, 663–688.

[26] Barry Mazur, John Tate, and Jeremy Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.

[27] Barry Mazur and Andrew Wiles, *Class fields of abelian extensions of $\mathbb{Q}$*, Invent. Math. **76** (1984), no. 2, 179–330.

[28] James S. Milne, *Elliptic curves*, BookSurge Publishers, Charleston, SC, 2006.

[29] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2000.

[30] Bernadette Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math. **89** (1987), no. 3, 455–510.

[31] ———, *Théorie d'Iwasawa et hauteurs p-adiques*, Invent. Math. **109** (1992), no. 1, 137–185.

[32] ———, *Théorie d'Iwasawa et hauteurs p-adiques (cas des variétés abéliennes)*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser, 1993, pp. 203–220.

[33] ———, *Fonctions L p-adiques des représentations p-adiques*, Astérisque (1995), no. 229.

[34] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.

[35] Kenneth A. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. **34** (1976), no. 3, 151–162.

[36] David E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423.

[37] Karl Rubin, *Euler systems and modular elliptic curves*, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge Univ. Press, Cambridge, 1998, pp. 351–367.

[38] ———, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.

[39] Peter Schneider, *p-adic height pairings. I*, Invent. Math. **69** (1982), no. 3, 401–409.

[40] ———, *p-adic height pairings. II*, Invent. Math. **79** (1985), no. 2, 329–374.

[41] Anthony J. Scholl, *An introduction to Kato's Euler systems*, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge Univ. Press, Cambridge, 1998, pp. 379–460.

[42] Jean-Pierre Serre, *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[43] ———, *Classes des corps cyclotomiques (d'après K. Iwasawa)*, Séminaire Bourbaki, Vol. 5, Soc. Math. France, Paris, 1995, pp. Exp. No. 174, 83–93.

[44] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[45] William Stein and Christian Wuthrich, *Algorithms for the arithmetic of elliptic curves using Iwasawa theory*, Math. Comp. **82** (2013), no. 283, 1757–1792.

[46] William A. Stein et al., *Sage Mathematics Software (Version 5.1)*, The Sage Development Team, 2012, available from `http://www.sagemath.org`.

[47] John Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274.

[48] ———, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, 1995, pp. Exp. No. 306, 415–440.

[49] ———, *WC-groups over p-adic fields*, Séminaire Bourbaki, Vol. 4, Soc. Math. France, 1995, pp. Exp. No. 156, 265–277.

[50] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[51] Andrew Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. (2) **131** (1990), no. 3, 493–540.