Journal of Number Theory 132 (2012) 1483–1506

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Iwasawa theory for elliptic curves at supersingular primes: A pair of main conjectures

Florian E. Ito Sprung

151 Thayer Street, Box #1917, Providence, RI 02912, United States

ARTICLE INFO

Article history:
Received 8 December 2009
Revised 18 May 2011
Accepted 20 November 2011
Available online 5 March 2012
Communicated by Christopher Skinner

Keywords:
Elliptic curves
Iwasawa theory
Supersingular primes

ABSTRACT

Text. We extend Kobayashi's formulation of Iwasawa theory for elliptic curves at supersingular primes to include the case $a_p \neq 0$, where a_p is the trace of Frobenius. To do this, we algebraically construct p-adic L-functions $L_p^\sharp$ and $L_p^\flat$ with the good growth properties of the classical Pollack p-adic L-functions that in fact match them exactly when $a_p = 0$ and p is odd. We then generalize Kobayashi's methods to define two Selmer groups $\mathrm{Sel}^\sharp$ and $\mathrm{Sel}^\flat$ and formulate a main conjecture, stating that each characteristic ideal of the duals of these Selmer groups is generated by our p-adic L-functions $L_p^\sharp$ and $L_p^\flat$. We then use results by Kato to prove a divisibility statement.

Video. For a video summary of this paper, please click here or visit http://www.youtube.com/watch?v=Y7gPQsBZo6s.

1. Introduction

In the early 1970s, B. Mazur and P. Swinnerton-Dyer constructed a p-adic L-function for an elliptic curve $E/\mathbb{Q}$ when p is good ordinary. Their L-function is an Iwasawa function, i.e. a p-adic analytic function convergent on the closed p-adic unit disc, and interpolates special values of the complex L-series of E twisted by various characters. Later that decade, Mazur formulated the Iwasawa theory for elliptic curves at these good ordinary primes, relating the p-adic L-function to the Selmer group over the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$. The good supersingular case (the one for which the trace of Frobenius a_p is divisible by p) has not been in as good a shape yet. Thanks to the work of R. Pollack from the early 2000s, we now have a *pair* of Iwasawa functions in the case $a_p = 0$, for which S. Kobayshi was able to formulate a pair of Iwasawa main conjectures by relating each of Pollack's Iwasawa functions to a modified Selmer group. However, the general supersingular case has so far

E-mail address: ian.sprung@gmail.com.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2011.11.003

seemed less amenable to analysis. The main theorems of this article obtain an appropriate pair of Iwasawa functions and relate them to a new pair of modified Selmer groups via a pair of main conjectures. Our pairs of Iwasawa functions and Selmer groups compare favorably with the works of Pollack and Kobayashi when reduced to the case $a_p = 0$.

More precisely, let $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. We can identify the ring of power series $\mathbb{Z}_p[\![X]\!]$ with $\mathbb{Z}_p[\![\Gamma]\!]$. In the good ordinary case, Mazur's and Swinnerton-Dyer's p-adic L-function (see [MSD], but also [Ma1]) is an element of $\mathbb{Q}_p \otimes \mathbb{Z}_p[\![X]\!]$ and thus an Iwasawa function, but conjecturally should live in the simpler ring $\mathbb{Z}_p[\![X]\!]$. Mazur conjectured in [Ma2] that the Selmer group is $\mathbb{Z}_p[\![X]\!]$-cotorsion (i.e. the Pontryagin dual is $\mathbb{Z}_p[\![X]\!]$-torsion – Kato proved this in [Ka]), and conjectured that the p-adic L-function generates its characteristic ideal. This is the main conjecture, a proof of which has been announced by Skinner and Urban [SU].

In the 1980s, Mazur, Tate, and Teitelbaum constructed more general p-adic L-functions in [MTT], among others for the supersingular (a.k.a. extraordinary) case, reconstructing p-adic L-functions of Višik [Vi], and Amice and Vélu [AV]. This case contains infinitely many primes p by a theorem of Elkies [El], but the p-adic L-functions are no longer elements of $\mathbb{Z}_p[\![X]\!] \otimes \overline{\mathbb{Q}_p}$, and correspondingly, the Selmer group is no longer $\mathbb{Z}_p[\![X]\!]$-cotorsion. In fact, there are two p-adic L-functions, one for each root α of the Hecke polynomial $Y^2 - a_p Y + p$, denoted $L_p(E, \alpha, X)$.

In the last decade, Pollack noticed in [Pollack] that if $a_p = 0$, one may get far by constructing auxiliary functions $\log_p^\pm$ vanishing at all p^nth roots of unity for n even $(+)$ or n odd $(-)$. Using *analytic* methods, he expressed each of these two p-adic L-functions as a certain sum, e.g. for p odd,

$$L_p(E, \alpha, X) = L_p^+(E, X) \log_p^+(1 + X) + L_p^-(E, X) \log_p^-(1 + X)\alpha,$$

where $L_p^\pm \in \mathbb{Z}_p[\![X]\!]$. Kobayashi then constructed two $\mathbb{Z}_p[\![X]\!]$-cotorsion subgroups of the Selmer group $\mathrm{Sel}^\pm$ in [Kobayashi] and formulated a pair of Iwasawa main conjectures in the spirit of Mazur's ordinary one: Each of Pollack's $L_p^\pm$-functions should generate the characteristic ideal of the Pontryagin duals of $\mathrm{Sel}^\pm$. He used *algebraic* arguments to reconstruct Pollack's $L_p^\pm$-functions and to define his Selmer groups, and proved a divisibility statement of his main conjecture via work of Kato, but still assumed $a_p = 0$.

What makes the case $a_p = 0$ so much more convenient than the case $a_p \neq 0$ is that it allowed Pollack and Kobayashi to give *separate* constructions for their appropriate objects $L_p^\pm$, $\log^\pm$, and $\mathrm{Sel}^\pm$, which break down for $a_p \neq 0$. For example, Pollack worked his observation that the sum $L_p(E, \alpha, X) + L_p(E, \overline{\alpha}, X)$ vanishes at $X = \zeta_{p^n} - 1$ for even n into the definition of $\log^+$. What makes Pollack's observation work is that $\alpha^2 = -p$ is an easy integer, since it is 1 modulo powers of p and signs! This *two-periodicity* of α and related objects was the crucial ingredient that made the arguments in Kobayashi's paper work as well. In this paper, we give a method that is independent of any periodicity, constructing the essential objects *simultaneously*. For example, there are four appropriate generalizations of $\log^\pm$ which we define as entries of a limit of an infinite product of 2×2 matrices. In general, we can't know just one of the four entries without knowing the other three since its definition involves information coming from every factor in the matrix product.

We then formulate a main conjecture in the spirit of Mazur's that relates our p-adic L-functions to subgroups of the Selmer group when p is odd, and prove a divisibility statement.

We note that the Hasse–Weil bound $|a_p| \leqslant 2\sqrt{p}$ (see e.g. [Si, Chapter 5]) forces $p = 2$ or $p = 3$ when $a_p \neq 0$. But we have worked out our methods so that they should generalize to general modular forms of weight two (with larger relevant primes). For elliptic curves, appropriate examples include any curve of conductor 11 ($a_2 = -2$) and a classical curve of Mordell given by $y^2 + y = x^3 - x$ ($a_2 = -2$, $a_3 = -3$). A look at the Cremona tables reveals that 70 out of the 471 curves of conductor $\leqslant 299$ have $a_p \neq 0$ for some supersingular p. The first curve with $a_2 = 2$ is $67A$, that with $a_3 = 3$ is $140B$, and the first curve with $a_2 = 2$, $a_3 = 3$ is $319A$. The two curves $245A$ and $245B$ both have $a_2 = -2$, while $a_3 = -3$ for the first, and $a_3 = 3$ for the latter.

There has been much work in the direction of extending the theory presented in this paper. Antonio Lei [Le] has generalized Kobayashi's methods to modular forms of higher weight, assuming $a_p = 0$. Lei, Loeffler, and Zerbes have given one generalization to any odd prime of good reduction in [LLZ]

for modular forms of higher weight using the theory of Wach modules. They show the existence of pairs of p-adic L-functions which live in (a ring analogous to[1]) $\mathbb{Z}_p[\![X]\!]\otimes\mathbb{Q}$, and a matrix that relates them to the p-adic L-functions of Amice and Vélu, and Višik. It would be nice to see if these matrices could be expressed *explicitly*, and to construct p-adic L-functions in (the ring analogous to) $\mathbb{Z}_p[\![X]\!]$, as in this paper. Their paper suggests that this is possible and is thus a huge hint for this question!

Overview. We now give a sketch of our methods in the case of an odd prime p. Denote by $\Phi_n(X)=\sum_{t=0}^{p-1}X^{p^{n-1}t}$ the p^nth cyclotomic polynomial, which is the irreducible polynomial for any primitive p^nth root of unity ζ_{p^n}. Put $k_n=\mathbb{Q}_p(\zeta_{p^{n+1}})$, and let $\mathcal{G}_n=\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})\cong\mathrm{Gal}(k_n/\mathbb{Q})$. Let $\Lambda_n=\mathbb{Z}_p[\mathcal{G}_n]$. Taking inverse limits, put $\mathcal{G}_\infty=\varprojlim_n\mathcal{G}_n$, and let $\Lambda=\mathbb{Z}_p[\![\mathcal{G}_\infty]\!]$.

The key construction in this paper is that of two Coleman maps $\mathrm{Col}^\sharp$ and $\mathrm{Col}^\flat$. They are generalizations of Kobayashi's $\mathrm{Col}^\pm$ (since for $a_p=0$, p odd, we have $\mathrm{Col}^\sharp=\mathrm{Col}^-$, $\mathrm{Col}^\flat=\mathrm{Col}^+$). As such, they are Λ-valued and just as (the trivial character-components of) $\mathrm{Col}^\pm$ sent Kato's zeta element to Pollack's p-adic L-functions, (the trivial character-components of) $\mathrm{Col}^\sharp$ and $\mathrm{Col}^\flat$ send Kato's zeta elements to new p-adic L-functions $L_p^\sharp(E,X)$ and $L_p^\flat(E,X)$, which are natural generalizations of Pollack's p-adic L-functions: They are in the trivial character-component $\mathbb{Z}_p[\![X]\!]$ of Λ and satisfy the following relation with the classical p-adic L-function $L_p(E,\alpha,X)$:

Theorem 1.1. *Let $L_p^\sharp(E,X)\in\mathbb{Z}_p[\![X]\!]$, $L_p^\flat(E,X)\in\mathbb{Z}_p[\![X]\!]$, and $L_p(E,\alpha,X)$ be as above. Then we have $L_p(E,\alpha,X)=L_p^\sharp(E,X)\log_\alpha^\sharp(1+X)+L_p^\flat(E,X)\log_\alpha^\flat(1+X)$.*

Here, $\log_\alpha^\sharp$ and $\log_\alpha^\flat$ are generalizations of Pollack's half-logarithms $\log_p^\pm$, which we construct together with the Coleman maps $\mathrm{Col}^\sharp$ and $\mathrm{Col}^\flat$ by looking at Kurihara's P_n-pairing (see [Ku]): Denote by T the p-adic Tate module. From Honda's theory of formal groups, there is a system of elements $(c_n)_n$, $c_n\in E(k_n)\otimes\mathbb{Z}_p\subseteq H^1(k_n,T)$ satisfying $\mathrm{Tr}_{n+1/n}(c_{n+1})=a_pc_n-c_{n-1}$. By using the essential assumption $a_p=0$, Kobayashi proved that the image of $P_{n,c_{n-1}}:H^1(k_n,T)\to\Lambda_n$ vanished at all $X=\zeta_{p^m}-1$ for $m\leqslant n$ with the same parity as n. In this way, he recovered the zeros of $\log_p^\pm$ (the sign depends on the parity of n). Dividing the image of $P_{n,c_{n-1}}$ by the minimal polynomial of these zeroes, he constructed maps $\mathrm{Col}_n^\pm$ whose inverse limits would be $\mathrm{Col}^\pm$.

To treat the excluded case $a_p\neq0$, these methods do not have to be modified quite that significantly. In Section 2, we define certain linear combinations δ_n^i of c_n and c_{n-1}. These δ_n^i are periodic with respect to i, and if one ignores the sign, the periods are $2p$ for $a_p\neq0$ and 2 for $a_p=0$ (for $a_p=0$, we just have $\delta_n^i=\pm c_n$ or $=\pm c_{n-1}$). Kobayashi's key accomplishment was to exhibit new zeroes (the primitive p^nth roots of unity) for $P_{n,c_{n-1}}$ each time n was increased by 2. If we followed his method naïvely for $a_p\neq0$, the periodicity of δ_n^i would only allow us to discover new zeroes each time n increased by $2p$, which is too few, since the image would then not have the right growth properties. *Rather than relying on any periodicity*, we let linear algebra come to the rescue. We look at certain linear combinations of $P_{n,\delta_n^{i+1}}$ and P_{n,δ_n^i} and show their images vanish at $X=\zeta_{p^n}-1$. In this way, we are able to write the function $(P_{n,c_n},P_{n,c_{n-1}}):H^1(k_n,T)\to\Lambda_n^{\oplus2}$ as a product of a function Col_n times a product $\mathcal{H}_n$ involving n matrices of the form $\left(\begin{smallmatrix}a_p&\Phi_m\\-1&0\end{smallmatrix}\right)$. Then we prove that $(\mathrm{Col}^\sharp,\mathrm{Col}^\flat)=\varprojlim_n\mathrm{Col}_n$ is a well-defined map from $\mathbf{H}^1_{\mathrm{Iw}}=\varprojlim_n H^1(k_n,T)$ to $\Lambda^{\oplus2}$.

The outline of the paper is as follows: In Section 2, we construct the generators δ_n^i and prove some basic properties. In Section 3, we construct the product of matrices $\mathcal{H}_n$ that we just mentioned, and relate it to the pair of functions $(P_{n,c_n},P_{n,c_{n-1}})$. Then in Section 4, we construct a limit matrix $\mathcal{H}$ and prove that its entries are in $O(\log_p(1+X)^{\frac12})$, as are Pollack's half-logarithms $\log_p^\pm(1+X)$. In Section 5, we construct the Coleman maps $\mathrm{Col}^\sharp$ and $\mathrm{Col}^\flat$ and in Section 6, we construct $\log_\alpha^\sharp$ and $\log_\alpha^\flat$ from $\mathcal{H}$ and prove our main theorem.

[1] Instead of $\mathbb{Z}_p$, they work with the ring of integers of the completion at p of the number field generated by the eigenvalues of the Hecke operators and the values of the nebencharacter.

In Section 7, we give a formulation of a pair of main conjectures for *any* odd supersingular prime, each in the spirit of Mazur's. Each is equivalent to Kato's [Ka], Perrin-Riou's [PR], or Kurihara's [Ku] main conjecture. Let $\mathfrak{p}$ be the prime ideal of $\mathbb{Q}_\infty$ above p, and

$$\mathrm{Sel}^\sharp(E/\mathbb{Q}_\infty) := \mathrm{Ker}\left(\mathrm{Sel}(E/\mathbb{Q}_\infty) \to \frac{E(\mathbb{Q}_{\infty,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^\sharp_{\infty,\mathfrak{p}}}\right),$$

where the local condition $E^\sharp_{\infty,\mathfrak{p}}$ is the exact annihilator under the local Tate pairing of $\mathrm{Ker}\,\mathrm{Col}^\sharp$, and similarly define $\mathrm{Sel}^\flat(E/\mathbb{Q}_\infty)$. The idea of choosing a new local condition to get amenable modified Selmer groups goes back to Kurihara, who chose the trivial group for his main conjecture, but did not have an Iwasawa function yet for the analytic side. Now at least one of $L_p^\flat(E,X)$ and $L_p^\sharp(E,X)$ is nonzero, and conjecturally both are. The theorem below is the key to our main conjecture:

Theorem 1.2. *Choose $* \in \{\sharp, \flat\}$ so that $L_p^*(E,X)$ is nonzero. The Pontryagin dual $\mathcal{X}^*(E/\mathbb{Q}_\infty) = \mathrm{Hom}(\mathrm{Sel}^*(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ of this $*$-Selmer group is a finitely generated torsion $\mathbb{Z}_p[\![X]\!]$-module.*

Main Conjecture 1.3. *Let p be odd, and $* \in \{\sharp, \flat\}$ so that $L_p^*(E,X)$ is nonzero. The characteristic ideal of the Pontryagin dual of $\mathrm{Sel}^*(E/\mathbb{Q}_\infty)$ is then generated by the p-adic L-function $L_p^*(E,X)$:*

$$\mathrm{Char}\big(\mathcal{X}^*(E/\mathbb{Q}_\infty)\big) = \big(L_p^*(E,X)\big).$$

We then use a theorem of Kato concerning his Euler systems to prove the following theorem:

Theorem 1.4. *Suppose $E/\mathbb{Q}$ does not have complex multiplication. Choose $* \in \{\sharp, \flat\}$ so that $L_p^*(E,X)$ is nonzero. Then if the p-adic representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{\mathbb{Z}_p}(T)$ on the automorphism group of the p-adic Tate module T is surjective, we have*

$$\mathrm{Char}\big(\mathcal{X}^*(E/\mathbb{Q}_\infty)\big) \supseteq \big(L_p^*(E,X)\big).$$

The statements here correspond to the $\eta = 1$ case in the more precise statements of Section 7. In fact, we will work with the Iwasawa algebra $\mathbb{Z}_p[\Delta][\![X]\!]$ rather than $\mathbb{Z}_p[\![X]\!]$. The smart reader will notice that some of our methods can (almost word-for-word) be applied to the setting of [IP], where the authors work with a number field for which p (assumed to be odd) splits completely. Since the applications of the results there are however not generalizable to the case $a_p \neq 0$ at present and we included the prime $p = 2$ in our paper, we have decided to stick with Kobayashi's setting for convenience of the reader and simplicity.

2. The generators δ_n^i

Notation. We attempt to keep the notation of [Kobayashi]. Thus, E is an elliptic curve over $\mathbb{Q}$ and p a prime so that E has good supersingular reduction at p, $[\frac{a}{b}]$ is the greatest integer not greater than $\frac{a}{b}$, I the identity matrix, and $\Phi_n(X) = \sum_{t=0}^{p-1} X^{p^{n-1}t}$ the p^nth cyclotomic polynomial, which is the irreducible polynomial for any primitive p^nth root of unity ζ_{p^n}. Let $N = n+1$ if p is odd, and $N = n+2$ if $p = 2$. Put $k_n = \mathbb{Q}_p(\zeta_{p^N})$, and let $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^N})/\mathbb{Q}) \cong \mathrm{Gal}(k_n/\mathbb{Q})$. We then have a decomposition $\mathcal{G}_n \cong (\mathbb{Z}/p^N\mathbb{Z})^\times \cong \Delta \times \Gamma_n$, where $\Gamma_n \cong \mathbb{Z}/p^n\mathbb{Z}$, and $\Delta \cong \mathbb{Z}/(p-1)\mathbb{Z}$ if p is odd. For $p = 2$, $\Delta = \{\pm 1\} \subset \mathcal{G}_n$. Taking inverse limits, put $\mathcal{G}_\infty = \varprojlim_n \mathcal{G}_n \cong \Delta \times \Gamma$, where $\Gamma \cong \mathbb{Z}_p$. Now fix a topological generator γ of Γ. By sending γ to $(1+X)$, we can identify $\Lambda = \mathbb{Z}_p[\![\mathcal{G}_\infty]\!]$ with $\mathbb{Z}_p[\Delta][\![X]\!]$. Denoting the image of γ under the projection $\mathcal{G}_\infty \to \mathcal{G}_n$ by γ_n, we can similarly identify $\Lambda_n = \mathbb{Z}_p[\mathcal{G}_n]$ with $\mathbb{Z}_p[\Delta][\![X]\!]/(\omega_n(X))$, where $\omega_n(X) = (1+X)^{p^n} - 1$. See [Wa, Chapter 7]. We denote by $\mathfrak{m}_n$ the maximal ideal of $\mathbb{Z}_p[\zeta_{p^N}]$.

Definition 2.1.

$$A := \begin{pmatrix} a_p & p \\ -1 & 0 \end{pmatrix}.$$

Kobayashi constructed a power series $\log_{\mathcal{F}_{ss}}(X) \in \mathbb{Z}_p[\![X]\!]$ that can be interpreted as the logarithm of a formal group $\mathcal{F}_{ss}$ isomorphic to the formal group $\hat{E}$ of the elliptic curve via Honda theory [Ho]. Although Kobayashi assumed $a_p = 0$, Pollack has pointed out in [Po1] that this could be done for $a_p \neq 0$ as well. Both [Kobayashi] and [Po1] also assume p is odd, but Honda's theorems hold for $p = 2$ as well [Ho], so we make no special assumption on a_p or p in this paper until Section 7. We denote the trace map from $\mathcal{F}_{ss}(\mathfrak{m}_{n+1})$ to $\mathcal{F}_{ss}(\mathfrak{m}_n)$ by $\mathrm{Tr}_{n+1/n}$. The power series $\log_{\mathcal{F}_{ss}}$ can be used to show the following result of Kobayashi:

Theorem 2.2. *There exist $c_n \in \mathcal{F}_{ss}(\mathfrak{m}_n) \cong \hat{E}(\mathfrak{m}_n)$ so that as a $\mathbb{Z}_p[\mathcal{G}_n]$-module, $\mathcal{F}_{ss}(\mathfrak{m}_n)$ is generated by c_n and c_{n-1} when $n \geqslant 0$. $\mathcal{F}_{ss}(\mathfrak{m}_{-1})$ is generated by c_{-1} when p is odd, and $\mathcal{F}_{ss}(\mathfrak{m}_{-2}) = \mathcal{F}_{ss}(\mathfrak{m}_{-1})$ by c_{-2} when $p = 2$. They satisfy the relations*:

(1) $\mathrm{Tr}_{n+1/n} c_{n+1} = a_p c_n - c_{n-1}$ *if* $n \geqslant 0$,
(2) $\mathrm{Tr}_{0/-1} c_0 = (a_p - 2)c_{-1}$ *when p is odd,*
(2′) $\mathrm{Tr}_{0/-1} c_0 = (\frac{a_p}{p} - 1)c_{-1} + 2c_{-2}$ *when* $p = 2$.

Proof. This is essentially [Kobayashi, Proposition 8.12] and [Kobayashi, Lemma 8.9]. See also the discussion in [Po1, Theorem 3.1] for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ with odd p. To allow arbitrary supersingular primes, we must modify Kobayashi's arguments, but not too much: What we need is a formal group whose logarithm is of Honda type $t^2 - a_p t + p$. We thus look at the sequence $\{x_k\}$ given by

$$(x_k, x_{k-1}) := (1, 0)A^k \times \frac{1}{p^k} \quad \text{for } k \geqslant 0.$$

The logarithm giving rise to our formal group via Honda theory [Kobayashi, Theorem 8.3 iii)] is then the power series

$$\log_{\mathcal{F}_{ss}}(X) = \sum_{k=0}^{\infty} x_k\big((1+X)^{p^k} - 1\big).$$

Note that to make Kobayshi's arguments work, we choose $\varepsilon \in p\mathbb{Z}$ so that $\log_{\mathcal{F}_{ss}}(\varepsilon) = \frac{p}{p+1-a_p}$. Addition in our formal group then allows us to construct $c_n = \varepsilon[+]_{\mathcal{F}_{ss}}(\zeta_{p^N} - 1)$. □

Lemma 2.3. *$\mathcal{F}_{ss}(k_n)$ has no p-torsion.*

Proof. Multiplication by p is given by a power series $[p](X) = pX + (\textit{higher order terms}) \in \mathbb{Z}_p[\![X]\!]$ on the formal group. We have $[p](X) = f(X)u(X)$ for a distinguished polynomial $f(X)$ of degree p^2 and a unit $u(X)$ by the p-adic Weierstraß preparation theorem. Now $\frac{f(X)}{X}$ has constant term $p \times (\textit{unit})$, and is thus an Eisenstein polynomial of degree $p^2 - 1$. It follows that the nontrivial torsion points live in a totally ramified extension of degree $p^2 - 1$, which does not divide $\deg(k_n/\mathbb{Q}_p)$: For odd p, this degree is $p^{n+1} - p^n$, while for $p = 2$, we have $\deg(k_n/\mathbb{Q}_p) = p^{n+1}$. Thus the only p-torsion point in $\mathcal{F}_{ss}(k_n)$ is zero itself. □

For the case $a_p = 0$, Kobayashi used a certain trace-compatibility of these generators [Kobayashi, Lemma 8.9] to define elements $c_n^{\pm} \in \mathcal{F}_{ss}(\mathfrak{m}_n)$, from which he was able to reconstruct Pollack's $L_p^{\pm}$-functions. We will now give a more general construction that includes the case $a_p \neq 0$.

Definition 2.4. Let $i \in \mathbb{Z}$. Put

$$B_i := B_+ = \begin{pmatrix} \frac{1}{p} & 0 \\ 0 & 1 \end{pmatrix} \quad \text{if } i \text{ is even}, \quad \text{and} \quad B_i := B_- = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{p} \end{pmatrix} \quad \text{if } i \text{ is odd}, \quad \text{and} \quad \text{let } Y_0 := I.$$

For general $i \in \mathbb{Z}$, we define Y_i by putting $AY_{i-1}B_i = Y_i$ and using two-way induction. Equivalently, $Y_i := A^i B_1 \cdots B_i$ for $i > 0$ and $Y_i := A^i B_0^{-1} B_{-1}^{-1} \cdots B_{i+1}^{-1}$ for $i < 0$. We prove below (Integrality Lemma 2.9) that Y_i has integral entries. Now put

$$\left(\delta_n^{i+1}, \delta_n^i\right) := (c_n, c_{n-1})Y_i \quad \text{for any } i \in \mathbb{Z}.$$

For the reader's convenience, we include a table of the δ_n^is.

	$a_p = 2$	$a_p = -2$	$a_p = 3$	$a_p = -3$	$a_p = 0$
δ_n^{-1}	$-c_n + c_{n-1}$	$-c_n - c_{n-1}$	$-c_n + c_{n-1}$	$-c_n - c_{n-1}$	$-c_n$
δ_n^0	c_{n-1}	c_{n-1}	c_{n-1}	c_{n-1}	c_{n-1}
δ_n^1	c_n	c_n	c_n	c_n	c_n
δ_n^2	$2c_n - c_{n-1}$	$-2c_n - c_{n-1}$	$3c_n - c_{n-1}$	$-3c_n - c_{n-1}$	$-c_{n-1}$
δ_n^3	$c_n - c_{n-1}$	$c_n + c_{n-1}$	$2c_n - c_{n-1}$	$2c_n + c_{n-1}$	$-c_n$
δ_n^4	$-c_{n-1}$	$-c_{n-1}$	$3c_n - 2c_{n-1}$	$-3c_n - 2c_{n-1}$	c_{n-1}
δ_n^5	$-c_n$	$-c_n$	$c_n - c_{n-1}$	$c_n + c_{n-1}$	c_n
δ_n^6	$-2c_n + c_{n-1}$	$2c_n + c_{n-1}$	$-c_{n-1}$	$-c_{n-1}$	$-c_{n-1}$
δ_n^7	$-c_n + c_{n-1}$	$-c_n - c_{n-1}$	$-c_n$	$-c_n$	$-c_n$
δ_n^8	c_{n-1}	c_{n-1}	$-3c_n + c_{n-1}$	$3c_n + c_{n-1}$	c_{n-1}

Remark 2.5. When $a_p = 0$, the δ_n^i are periodic in i with period 4, or 2 if one ignores signs, which was essential in the work of [Kobayashi]. The period is $4p$ (or $2p$ modulo signs) for $a_p \neq 0$, but in this paper, no argument needs this periodicity.

Proposition 2.6. *Let $n \geqslant 0$ and $i \in \mathbb{Z}$. Then*

$$\delta_n^{i+1} = \begin{cases} \operatorname{Tr}_{n+1/n}(\delta_{n+1}^i) & \text{if } i \text{ is odd, and} \\ \frac{1}{p} \operatorname{Tr}_{n+1/n}(\delta_{n+1}^i) & \text{if } i \text{ is even.} \end{cases}$$

Note that the sums of the upper and lower indices of δ_n^{i+1} and δ_{n+1}^i are the same.

Proof. From Theorem 2.2, we have $\operatorname{Tr}_{n+1/n}(c_{n+1}) = a_p c_n - c_{n-1}$, so the trace of $yc_{n+1} + y'c_n \in \hat{E}(\mathfrak{m}_{n+1})$ can be computed with the matrix A:

$$\operatorname{Tr}_{n+1/n}(c_{n+1}, c_n) \begin{pmatrix} y \\ y' \end{pmatrix} = (c_n, c_{n-1}) A \begin{pmatrix} y \\ y' \end{pmatrix} \in \hat{E}(\mathfrak{m}_n). \tag{1}$$

Thus $(\delta_n^{i+1}, \delta_n^i) = (c_n, c_{n-1})AY_{i-1}B_i = \operatorname{Tr}_{n+1/n}(c_{n+1}, c_n)Y_{i-1}B_i = \operatorname{Tr}_{n+1/n}(\delta_{n+1}^i, \delta_{n+1}^{i-1})B_i$. □

Lemma 2.7.

$$Y_i = \begin{cases} Y_{i-1}B_+A & \text{if } i \text{ is even,} \\ Y_{i-1}AB_- & \text{if } i \text{ is odd.} \end{cases}$$

Proof. We do the proof for odd i by two-way induction (if necessary, just read backwards):

$$Y_i = Y_{i-1}AB_- \quad \Leftrightarrow \quad Y_{i+1} = AY_iB_+ = AY_{i-1}AB_-B_+$$
$$\Leftrightarrow \quad Y_{i+1} = AY_{i-1}B_-B_+A = Y_iB_+A. \qquad \square$$

Lemma 2.8. *$Y_i = p^{-\frac{i}{2}} \times A^i$ for i even, and $Y_iB_+A = p^{-\frac{i+1}{2}} \times A^{i+1}$ for i odd.*

Proof. Two-way induction as in the above proof. Note that $(AB_-B_+A) = p^{-1} \times A^2$. $\square$

Lemma 2.9 *(Integrality Lemma). $Y_i \in \mathrm{GL}_2(\mathbb{Z})$, i.e. Y_i has integral coefficients and is invertible.*

Proof. Since $\frac{a_p}{p} \in \mathbb{Z}$, this is true for $i = \pm 1$. Now note that A^2 is an element of $\mathrm{GL}_2(\mathbb{Z})$ multiplied by p. Now use Lemma 2.8 and Lemma 2.7, noting that $AB_- \in \mathrm{GL}_2(\mathbb{Z})$ and $\det(Y_i) = \pm 1$. $\square$

Corollary 2.10. *δ_n^{i+1} and δ_n^i generate $\hat{E}(\mathfrak{m}_n)$ as a $\mathbb{Z}_p[\mathcal{G}_n]$-module for $n \geqslant 0$.*

Proof. This follows from c_n and c_{n-1} being generators for $\hat{E}(\mathfrak{m}_n)$ and $\det(Y_i) = \pm 1$. $\square$

3. Construction of the zero-finding matrices $\mathcal{H}_n(X)$

Definition 3.1. Let $P_{n,x} : H_1(k_n, T) \to \mathbb{Z}_p[\mathcal{G}_n]$ be defined by

$$z \mapsto \sum_{\sigma \in \mathcal{G}_n} \left(x^\sigma, z\right)_n \sigma \quad \text{for } x \in \mathcal{F}_{ss}(\mathfrak{m}_n),$$

where $(\,,\,)_n : \mathcal{F}_{ss}(\mathfrak{m}_n) \times H^1(k_n, T) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$ is the pairing coming from the cup product. Here, we have put $\mathcal{F}_{ss}(\mathfrak{m}_n) \subseteq H^1(k_n, T)$ (see [Kobayashi, Section 8.5]).

Definition 3.2. We let $P_n^i := P_{n,\delta_n^i}$.

By linearity, the periodicity of δ_n^i carries over to P_n^i, and we also have

$$\left(P_n^{i+1}, P_n^i\right) = \left(P_n^1, P_n^0\right)Y_i. \tag{2}$$

The main result of this section is the following proposition.

Proposition 3.3. *Let $z \in H^1(k_n, T)$. Then for some $f'_\sharp(z), f'_\flat(z) \in \Lambda_n$,*

$$\left(P_n^1(z), P_n^0(z)\right) = \left(f'_\sharp(z), f'_\flat(z)\right)\mathcal{A}_1 \cdots \mathcal{A}_n, \quad \text{where } \mathcal{A}_i = \mathcal{A}_i(X) := \begin{pmatrix} a_p & \Phi_i(1+X) \\ -1 & 0 \end{pmatrix}.$$

The proof of this proposition will occupy the rest of this section.

Observation 3.4. Let $k < m$ be integers. Since $\Phi_m(\zeta_{p^k}) = 1 + (\zeta_{p^k})^{p^{m-1}} + \cdots + (\zeta_{p^k})^{p^{m-1}(p-1)} = p$, we have

$$\mathcal{A}_m(\zeta_{p^k} - 1) = \begin{pmatrix} a_p & p \\ -1 & 0 \end{pmatrix} = A.$$

Lemma 3.5 *(Tandem Lemma). Fix an integer $n \geqslant 0$. Assume that for any $i \in \mathbb{N}$, we are given functions $Q_i = Q_i(X)$ so that $Q_i \in \Phi_i(1+X)\Lambda_n$ whenever $i \leqslant n$, and $(Q_{n+1}, Q_n)Y_{n'-n} = (Q_{n'+1}, Q_{n'})$ for any $n' \in \mathbb{N}$.*

Then $(Q_{n+1}, Q_n) = (\tilde{q}_1, q_0)\mathcal{A}_1\mathcal{A}_2\cdots\mathcal{A}_n$ with $\tilde{q}_1 = \tilde{q}_1(X) \in \Lambda_n$, $q_0 = q_0(X) \in \Lambda_n$.

Proof. We prove that $(Q_{n+1}, Q_n) = (\tilde{q}_{n-l+1}, q_{n-l})\mathcal{A}_{n-l+1}\mathcal{A}_{n-l+2}\cdots\mathcal{A}_n$ for $\tilde{q}_{n-l+1}, q_{n-l} \in \Lambda_n$ by induction on l. For $l = 0$, we put $Q_{n+1} = \tilde{q}_{n+1}$, $Q_n = q_n$. Now assume this holds for $l \geqslant 0$. We first show $\Phi_{n-l}(1+X) | q_{n-l}(X)$: By Observation 3.4 and the inductive hypothesis,

$$(Q_{n+1}, Q_n) = (\tilde{q}_{n+1-l}, q_{n-l})A^l \quad \text{at } X = \zeta_{p^{n-l}} - 1,$$

and

$$(Q_{n+1}, Q_n)Y_{-l} = (Q_{n+1-l}, Q_{n-l}) \quad \text{by assumption.}$$

But $Q_{n-l}(\zeta_{p^{n-l}} - 1) = 0$, so $(\tilde{q}_{n+1-l}, q_{n-l})A^lY_{-l} = (Q_{n+1-l}, 0)$ at $X = \zeta_{p^{n-l}} - 1$.

From Corollary 2.8, $A^lY_{-l} = p^{\frac{l-1}{2}} \times B_+^{-1}$ for l odd, and $A^lY_{-l} = p^{\frac{l}{2}} \times I$ for l even.

Therefore, $q_{n-l} \times$ (some power of p) $= 0$ at $\zeta_{p^{n-l}} - 1$. But $\mathbb{Z}_p[\Delta][\zeta_{p^{n-l}}]$ has no p-torsion, so we have $q_{n-l}(\zeta_{p^{n-l}} - 1) = 0$. Thus, we can indeed write $q_{n-l}(X) = \Phi_{n-l}(1+X)\tilde{q}_{n-l}(X)$. Since $AB_- \in \mathrm{GL}_2(\mathbb{Z})$, we now define

$$(\tilde{q}_{n-l}, q_{n-1-l}) := (\tilde{q}_{n-l+1}, \tilde{q}_{n-l})(AB_-)^{-1}.$$

Then $(\tilde{q}_{n-l}, q_{n-l-1})\mathcal{A}_{n-l} = (\tilde{q}_{n-l}, q_{n-l-1})AB_-\left(\begin{smallmatrix} 1 & 0 \\ 0 & \Phi_{n-l} \end{smallmatrix}\right) = (\tilde{q}_{n-l+1}, \tilde{q}_{n-l})\left(\begin{smallmatrix} 1 & 0 \\ 0 & \Phi_{n-l} \end{smallmatrix}\right) = (\tilde{q}_{n-l+1}, q_{n-l})$. Thus, $(Q_{n+1}, Q_n) = (\tilde{q}_{n-l}, q_{n-l-1})\mathcal{A}_{n-l}\cdots\mathcal{A}_n$, as desired. □

Lemma 3.6. *Let $i \leqslant n$ with $i > 0$. Then $\mathrm{Im}(P_n^{i-n}) \subset \Phi_i(1+X)\Lambda_n$.*

Proof. Consider the ring morphism

$$\Lambda_i = \mathbb{Z}_p[\Delta][X]/\big(\omega_i(X)\big) = \mathbb{Z}_p[\mathcal{G}_i] \xrightarrow{\prod \psi} \prod_{\psi} \overline{\mathbb{Q}_p},$$

where $\mathcal{G}_i \xrightarrow{\psi} \overline{\mathbb{Q}_p}^{\times}$ are all the characters of $\mathcal{G}_i$ of conductor p^{i+1} (or 2^{i+2} if $p = 2$), so that $\psi(\gamma_i)$ is a primitive p^ith root of unity, and thus $\mathrm{Ker}\prod \psi = \Phi_i(1+X)\Lambda_i$.

Denote by $\overline{\sigma}$ the image of σ by the natural projection $\mathcal{G}_i \to \mathcal{G}_{i-1}$. Since $\delta_i^0 = c_{i-1} = \delta_{i-1}^1$,

$$\psi \circ P_i^0(z) = \sum_{\sigma \in \mathcal{G}_i} \big(\big(\delta_i^0\big)^{\sigma}, z\big)_i \psi(\sigma) = \sum_{\tau \in \mathcal{G}_{i-1}} \big(\big(\delta_{i-1}^1\big)^{\tau}, z\big)_i \sum_{\sigma \in \mathcal{G}_i,\, \overline{\sigma} \equiv \tau} \psi(\sigma) = 0,$$

so $\mathrm{Im}(P_i^0) \subset \mathrm{Ker}\,\psi = \Phi_i(1+X)\Lambda_i$.

From [Kobayashi, Lemma 8.15] and the definition of the δ_n^i,

$$\begin{array}{ccc} H^1(k_n, T) & \xrightarrow{P_n^i} & \Lambda_n \\ \big\downarrow \mathrm{cor} & & \big\downarrow \mathrm{proj} \\ H^1(k_{n-1}, T) & \xrightarrow{p^* P_{n-1}^{i+1}} & \Lambda_{n-1} \end{array}$$

commutes, where $p^* = 1$ for odd i and $p^* = p$ for even i. The following thus commutes as well:

$$\begin{array}{ccc} H^1(k_n, T) & \xrightarrow{P_n^{i-n}} & \Lambda_n \\ \Big\downarrow \text{cor} & & \Big\downarrow \text{proj} \\ H^1(k_i, T) & \xrightarrow{p^* P_i^0} & \Phi_i(1+X)\Lambda_i, \end{array}$$

for an appropriate p-power p^*. This implies that P_n^{i-n} maps into $\Phi_i(1+X)\Lambda_n$. □

Proof of Proposition 3.3. For any $i \in \mathbb{N}$, put $Q_i := P_n^{i-n}(z)$ and apply the Tandem Lemma 3.5. We know that $Q_i \in \Phi_i(1+X)\Lambda_n$ from Lemma 3.6 for $i \leqslant n$, so by Eq. (2),

$$\begin{aligned}(Q_{n+1}, Q_n)Y_{n'-n} &= \big(P_n^1(z), P_n^0(z)\big)Y_{n'-n} = \big(P_n^{n'-n+1}(z), P_n^{n'-n}(z)\big) \\ &= (Q_{n'+1}, Q_{n'}). \qquad \square\end{aligned}$$

Notation 3.7. We define matrices $\mathcal{H}_n$ with entries in Λ_n by

$$\mathcal{H}_n = \mathcal{H}_n(X) := \tilde{Y}\mathcal{A}_1 \cdots \mathcal{A}_n, \quad \text{where } \tilde{Y} := -(AB_-)^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & -a_p \end{pmatrix}.$$

Definition 3.8. We now put $(f_\sharp(z), f_\flat(z)) := (f'_\sharp(z), f'_\flat(z))\tilde{Y}^{-1}$. This might seem unnatural at first, since in Sections 4, 5, and 6, there are no problems if you formally replace $(f_\sharp(z), f_\flat(z))$ by $(f'_\sharp(z), f'_\flat(z))$ while ignoring $\tilde{Y}$. We need this definition to match a sign convention of Kobayashi (Remark 6.16), and because we need this setup in Section 7. The main proposition then becomes:

Proposition 3.9. *For $z \in H^1(k_n, T)$, there are $(f_\sharp(z), f_\flat(z)) \in \Lambda_n^{\oplus 2}$ so that we have*

$$\big(P_n^1(z), P_n^0(z)\big) = \big(f_\sharp(z), f_\flat(z)\big)\mathcal{H}_n.$$

4. Construction and growth properties of $\mathcal{H}$

We now scrutinize the growth properties of $\mathcal{H}_n$:

Definition 4.1. Fix $0 < r < 1$. For $f(X) \in \mathbb{C}_p[\![X]\!]$ convergent on the open unit disc of $\mathbb{C}_p$, let

$$\big|f(X)\big|_r := \sup_{|z|_p < r} \big|f(z)\big|_p$$

with normalization $|p|_p = \frac{1}{p}$, and for a matrix with such entries, define its norm $|\ |_r$ by

$$\left|\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right|_r := \max\big\{|a|_r, |b|_r, |c|_r, |d|_r\big\}.$$

Example 4.2. [2]

$$\left|\Phi_n(1+X)\right|_r = \begin{cases} \frac{1}{p} & \text{when } r \leqslant p^{-\frac{1}{p^{n-1}(p-1)}}, \\ r^{p^{n-1}(p-1)} & \text{when } r \geqslant p^{-\frac{1}{p^{n-1}(p-1)}}. \end{cases}$$

Example 4.3. $|\frac{1}{p}\mathcal{A}_n(X)\mathcal{A}_{n+1}(X)|_r = |\frac{\Phi_n(1+X)}{p}|_r = 1$ for n big enough so that $p^n \geqslant \frac{p}{p-1}\frac{\log p}{\log r^{-1}}$.

Proof. For appropriately big n,

$$\left|\frac{1}{p}\mathcal{A}_n\mathcal{A}_{n+1}\right|_r = \left|\begin{pmatrix} \frac{a_p^2-\Phi_n(1+X)}{p} & \frac{a_p\Phi_{n+1}(1+X)}{p} \\ -\frac{a_p}{p} & -\frac{\Phi_{n+1}(1+X)}{p} \end{pmatrix}\right|_r = \left|\frac{\Phi_n(1+X)}{p}\right|_r = 1. \qquad \square$$

Lemma 4.4 *(Convergence Lemma).* $\lim_{n\to\infty}\mathcal{H}_nA^{-n}$ *exists and converges on the open unit disc of* $\mathbb{C}_p$.

Proof. Using the norm $|\ |_r$,

$$R := \left|\mathcal{H}_nA^{-n} - \mathcal{H}_{n+1}A^{-(n+1)}\right|_r = \left|\mathcal{H}_nA^{-n} - \mathcal{H}_n\mathcal{A}_{n+1}A^{-(n+1)}\right|_r$$

satisfies

$$R \leqslant \left|p^{-\frac{n}{2}}\mathcal{H}_n\right|_r\left|p^{\frac{n}{2}}\left(A^{-n} - \mathcal{A}_{n+1}A^{-(n+1)}\right)\right|_r \leqslant \left|p^{-\frac{n}{2}}\mathcal{H}_n\right|_r\left|I - \mathcal{A}_{n+1}A^{-1}\right|_r\left|p^{\frac{n}{2}}A^{-n}\right|_r.$$

As $n\to\infty$, the first term $|p^{-\frac{n}{2}}\mathcal{H}_n|_r$ is bounded by Example 4.3, and analogous calculations as in its proof yield $|pA^{-2}|_r = 1$, so the last term $|p^{\frac{n}{2}}A^{-n}|_r$ is bounded, too. Finally, from [Pollack, proof of Lemma 4.1], we have $|\frac{\Phi_{n+1}(1+X)}{p} - 1|_r \to 0$ as $n\to\infty$, so the middle term $|I - \mathcal{A}_{n+1}A^{-1}|_r \to 0$ as $n\to\infty$. It follows that $|\mathcal{H}_nA^{-n} - \mathcal{H}_{n+1}A^{-(n+1)}|_r \to 0$ as $n\to\infty$, whence the lemma. $\square$

Definition 4.5. Recall that $N = n+1$ for p odd and $N = n+2$ for p even. Now let us put

$$\mathcal{H} := \lim_{n\to\infty}\mathcal{H}_nA^{-N}.$$

Definition 4.6. Let $f(X), g(X) \in \mathbb{C}_p[\![X]\!]$ converge on the open unit disc of $\mathbb{C}_p$. Then we say that $f(X)$ is $O(g(X))$ if

$$\left|f(X)\right|_r \text{ is } O\left(\left|g(X)\right|_r\right) \text{ as } r\to 1^-.$$

If in addition, $g(X)$ is $O(f(X))$, then we say that $f(X)\sim g(X)$.

Example 4.7. $1\sim X$. Since $\log_p(1+X) = X\prod_n\frac{\det\mathcal{A}_n}{\det A}$, we have $\det\mathcal{H}\sim\log_p(1+X)$.

Lemma 4.8 *(Growth Lemma). The entries of* $\mathcal{H}$ *are* $O(\log_p(1+X)^{\frac{1}{2}})$.

[2] This appears in the proof of [Pollack, Lemma 4.5]. There seems to be a typo. He meant to write $|\Phi_n(1+X)|_r = r^{p^{n-1}(p-1)}$ for sufficiently large r.

Proof. We give the proof for $N = n+1$, since it is very similar for $N = n+2$. Note that

$$\mathcal{H}_n A^{-N} = \tilde{Y}\mathcal{A}_1 \cdots \mathcal{A}_n A^{-N} = \begin{cases} \tilde{Y}\mathcal{A}_1 \cdots \mathcal{A}_n Y_{-N} \times p^{-\frac{n+1}{2}} & \text{for } n \text{ odd,} \\ \tilde{Y}\mathcal{A}_1 \cdots \mathcal{A}_n Y_{-N} B_+ \times p^{-\frac{n}{2}} & \text{for } n \text{ even (cf. Corollary 2.8).} \end{cases}$$

Thus,

$$\left|\mathcal{H}_n A^{-N}\right|_r \leqslant \begin{cases} |\tilde{Y}\mathcal{A}_1|_r |\frac{1}{p}\mathcal{A}_2\mathcal{A}_3|_r \cdots |\frac{1}{p}\mathcal{A}_{n-1}\mathcal{A}_n|_r |Y_{-N} \times p^{-1}|_r & \text{for } n \text{ odd,} \\ |\tilde{Y}|_r |\frac{1}{p}\mathcal{A}_1\mathcal{A}_2|_r \cdots |\frac{1}{p}\mathcal{A}_{n-1}\mathcal{A}_n|_r |Y_{-N} B_+|_r & \text{for } n \text{ even.} \end{cases}$$

From Example 4.3, $|\frac{1}{p}\mathcal{A}_k\mathcal{A}_{k+1}|_r = |\frac{\Phi_k(1+X)}{p}|_r$, so

$$\left|\mathcal{H}_n A^{-N}\right|_r \leqslant \left| \prod_{1 \leqslant k < n,\, k \not\equiv n (2)} \frac{\Phi_k(1+X)}{p} \right|_r \times c$$

for some constant c independent from r. From [Pollack, Lemma 4.5], we have

$$\log_p(1+X)^{\frac{1}{2}} \sim \frac{1}{p} \prod_{k \text{ odd}} \frac{\Phi_k(1+X)}{p} \sim \frac{1}{p} \prod_{k \text{ even}} \frac{\Phi_k(1+X)}{p},$$

so the entries of $\mathcal{H}$ are all $O(\log_p(1+X)^{\frac{1}{2}})$, as desired. □

5. Construction of the Coleman maps

In this section, we construct a map $\mathrm{Col} : \mathbf{H}^1_{\mathrm{Iw}}(T) \to \Lambda \oplus \Lambda$, where $\mathbf{H}^1_{\mathrm{Iw}}(T) = \varprojlim_n H^1(k_n, T)$.

Definition 5.1. Let h^i_n be the $\mathbb{Z}_p[\Delta][X]$-module morphisms given by

$$\begin{aligned} \Lambda_n \oplus \Lambda_n &\xrightarrow{h^i_n} (\Lambda_n \oplus \Lambda_n)\mathcal{H}_n Y_i \subset \Lambda_n \oplus \Lambda_n, \\ (a, b) &\mapsto (a, b)\mathcal{H}_n Y_i. \end{aligned}$$

Observation 5.2. $\operatorname{Ker} h^i_n$ is independent from i, and we henceforth denote it by $\operatorname{Ker} h_n$.

Proof. Right multiplication by Y_i is a $\mathbb{Z}_p[\Delta][X]$-module isomorphism, because $\det Y_i = 1$. □

Proposition 5.3. *There is a unique homomorphism* Col_n *so that the following commutes*

$$\begin{array}{ccccc} & & \exists!\, \mathrm{Col}_n & & \\ & \overset{(P^{i+1}_n, P^i_n)}{\nearrow} & & \overset{h^i_n}{\nwarrow} & \\ H^1(k_n, T) & \xrightarrow{\qquad} & \Lambda_n \oplus \Lambda_n & \xleftarrow{\qquad} & \frac{\Lambda_n \oplus \Lambda_n}{\operatorname{Ker} h_n}. \end{array}$$

Proof. For $z \in H^1(k_n, T)$, $(P^{i+1}_n(z), P^i_n(z)) = (f_\sharp(z), f_\flat(z))\mathcal{H}_n Y_i = h^i_n(f_\sharp(z), f_\flat(z))$. Thus, we can put $\mathrm{Col}_n(z) = (f_\sharp(z), f_\flat(z)) \in \frac{\Lambda_n \oplus \Lambda_n}{\operatorname{Ker} h_n}$, independent from i. □

Lemma 5.4. $\mathrm{proj} : \Lambda_{n+1} \oplus \Lambda_{n+1} \to \Lambda_n \oplus \Lambda_n$ *satisfies* $\mathrm{proj}(\operatorname{Ker} h_{n+1}) \subset \operatorname{Ker} h_n$.

Proof. For $(a,b) \in \operatorname{Ker} h_{n+1} \subset \Lambda_{n+1}^{\oplus 2}$, we know that $(a,b)\mathcal{H}_{n+1} = (0,0)$ in $\in \Lambda_{n+1}^{\oplus 2}$.

Now $\Phi_{n+1}(1+X) \equiv p \pmod{\omega_n(X)}$ implies $(a,b)\mathcal{H}_{n+1} \equiv (a,b)\mathcal{H}_n A \equiv (0,0) \pmod{\omega_n}$, so

$$p(a,b)\mathcal{H}_n \equiv (0,0) \pmod{\omega_n},$$

since pA^{-1} has integral coefficients. But $\Lambda_{n+1}/\omega_n \cong \Lambda_n$ has no p-torsion, so $(a,b)\mathcal{H}_n \in \Lambda_n^{\oplus 2}$. Thus, $\operatorname{proj}((a,b)) \in \operatorname{Ker} h_n$. □

Now we can define $\beta_i : \operatorname{Im}(h_{n+1}^{i-1}) \to \operatorname{Im}(h_n^i)$ (cf. diagram (8.27) in [Kobayashi]) as

$$\beta_i = \begin{cases} (\operatorname{proj}, \frac{1}{p}\operatorname{proj}) & \text{for } i \text{ odd}, \\ (\frac{1}{p}\operatorname{proj}, \operatorname{proj}) & \text{for } i \text{ even}. \end{cases}$$

Proposition 5.5. *The following diagram commutes*

$$\begin{array}{ccccc} H^1(k_{n+1}, T) & \xrightarrow{P_{n+1}^i, P_{n+1}^{i-1}} & \operatorname{Im}(h_{n+1}^{i-1}) & \xleftarrow[h_{n+1}^{i-1}]{} & \frac{\Lambda_{n+1}\oplus\Lambda_{n+1}}{\operatorname{Ker} h_{n+1}} \\ \downarrow \operatorname{cor} & & \downarrow \beta_i & & \downarrow \operatorname{proj} \\ H^1(k_n, T) & \xrightarrow{P_n^{i+1}, P_n^i} & \operatorname{Im}(h_n^i) & \xleftarrow[h_n^i]{} & \frac{\Lambda_n\oplus\Lambda_n}{\operatorname{Ker} h_n}. \end{array}$$

Proof. As for the left square, commutativity follows from the trace compatibility of the P_n^i (see [Kobayashi, Lemma 8.15]). The map β_i ensures that we divide by the appropriate power of p in accordance with Definition 2.4 of δ_n^i.

As for the right square, the map $\beta_i \circ h_{n+1}^{i-1}$ is given by multiplying by the matrix $\mathcal{H}_{n+1}Y_{i-1}B_i \equiv \mathcal{H}_n A Y_{i-1} B_i \pmod{\omega_n(X)}$. But $AY_{i-1}B_i = Y_i$ by construction, so we are done. □

Combining Propositions 5.3 and 5.5, we obtain the following corollary.

Corollary 5.6. *The Coleman maps are compatible*:

$$\begin{array}{ccc} H^1(k_{n+1}, T) & \xrightarrow{\operatorname{Col}_{n+1}} & \frac{\Lambda_{n+1}\oplus\Lambda_{n+1}}{\operatorname{Ker} h_{n+1}} \\ \downarrow \operatorname{cor} & \circlearrowleft & \downarrow \operatorname{proj} \\ H^1(k_n, T) & \xrightarrow{\operatorname{Col}_n} & \frac{\Lambda_n\oplus\Lambda_n}{\operatorname{Ker} h_n}. \end{array}$$

Proposition 5.7 *(Limit Proposition).*

$$\varprojlim_n \frac{\Lambda_n \oplus \Lambda_n}{\operatorname{Ker} h_n} \cong \Lambda \oplus \Lambda.$$

Proof. The map h_n^i can be defined on $\Lambda^{\oplus 2}$ as well, as multiplication by the matrix $\mathcal{H}_n Y_i$. Let π_n be the projection $\Lambda \to \Lambda_n$ and put $M_n := \operatorname{Ker} \pi_n^{\oplus 2} \circ h_n^i$ (which is independent of i, cf. Observation 5.2). By definition, $\omega_n(X)\Lambda^{\oplus 2} \subset M_n$, from which $\frac{\Lambda\oplus\Lambda}{M_n} \cong \frac{\Lambda_n\oplus\Lambda_n}{\operatorname{Ker} h_n}$ as Λ-modules. Now

$$\Lambda^{\oplus 2}/M_n \cong \varprojlim_m \Lambda^{\oplus 2}/\big(M_n + p^m\Lambda^{\oplus 2}\big),$$

since M_n is a free finitely generated $\mathbb{Z}_p$-module. We have $M_n \supset \omega_n\Lambda^{\oplus 2}$, so $M_n + p^m\Lambda^{\oplus 2} \supset \omega_n\Lambda^{\oplus 2} + p^m\Lambda^{\oplus 2}$. Assume for the moment that we also have $M_{2m+\nu} + p^m\Lambda^{\oplus 2} \subset \omega_\nu\Lambda^{\oplus 2} + p^m\Lambda^{\oplus 2}$. These two inclusions would induce module morphisms

$$\varprojlim_{(\nu,m)} \Lambda^{\oplus 2}/\big(\omega_\nu\Lambda^{\oplus 2} + p^m\Lambda^{\oplus 2}\big) \to \varprojlim_{(n,m)} \Lambda^{\oplus 2}/\big(M_n + p^m\Lambda^{\oplus 2}\big),$$

$$\varprojlim_{(n,m)} \Lambda^{\oplus 2}/\big(M_n + p^m\Lambda^{\oplus 2}\big) \to \varprojlim_{(\nu,m)} \Lambda^{\oplus 2}/\big(\omega_\nu\Lambda^{\oplus 2} + p^m\Lambda^{\oplus 2}\big),$$

which are inverses of each other, from which $\varprojlim_n \Lambda^{\oplus 2}/M_n = \Lambda \oplus \Lambda$ would follow. Let us thus prove this second inclusion. It suffices to prove that $M_{2m+\nu} = 0$ inside $\Lambda_\nu^{\oplus 2}/p^m$.

Lemma 5.8. *$\mathcal{H}_n^{-1} \times \omega_n(X)$ has coefficients in $\mathbb{Z}_p[\Delta][X]$, and $M_n = (\Lambda_n \oplus \Lambda_n)\mathcal{H}_n^{-1} \times \omega_n(X)$.*

Proof. Choose $(a,b) \in M_n \subset \Lambda^{\oplus 2}$. This says that $(a,b)\mathcal{H}_n = (c,d)\omega_n$ for some $(c,d) \in \Lambda^{\oplus 2}$. Conversely, for a fixed $(c,d) \in \Lambda^{\oplus 2}$, any such (a,b) is unique, since $\det \mathcal{H}_n = \frac{\omega(X)}{X} \neq 0$ in $\mathbb{Z}_p[X]$, and this is not a zero-divisor in $\mathbb{Z}_p[\Delta][X]$. Thus, $(a,b) = (c,d)\mathcal{H}_n^{-1}\omega_n$. □

Now $\mathcal{H}_{2m+\nu}^{-1} \times \omega_{2m+\nu} \equiv (\mathcal{H}_\nu\mathcal{A}_{1+\nu}\cdots\mathcal{A}_{2m+\nu})^{-1}\omega_\nu\Phi_{1+\nu}\cdots\Phi_{2m+\nu} \equiv A^{-2m}\mathcal{H}_\nu^{-1}\omega_\nu \times p^{2m} \pmod{\omega_\nu}$ by Observation 3.4. But $pA^{-2} \in \mathbb{M}_2(\mathbb{Z})$, so $\mathcal{H}_{2m+\nu}^{-1} \times \omega_{2m+\nu} \in p^m\Lambda_\nu^{\oplus 2}$ and thus $M_{2m+\nu} = 0$ in $\Lambda_\nu^{\oplus 2}/p^m$. □

In view of the Limit Proposition 5.7 and Corollary 5.6, we can make the following definition:

Definition 5.9. Let the Coleman map $\mathrm{Col} : \mathbf{H}^1_{\mathrm{Iw}}(T) \to \Lambda \oplus \Lambda$ be the projective limit of $\mathrm{Col}_n : H^1(k_n, T) \to \frac{\Lambda_n \oplus \Lambda_n}{\mathrm{Ker}\, h_n}$, where $\Lambda = \mathbb{Z}_p[\Delta][\![X]\!]$.

6. The p-adic L-functions $L_p^\sharp(E,X)$ and $L_p^\flat(E,X)$

Recall (e.g. from [Wa, 6.3]) that for a character $\eta : \Delta \to \mathbb{Z}_p^\times$, a $\mathbb{Z}_p[\Delta]$-module M, and an odd prime p, the η-component M^η is simply given by $\varepsilon_\eta M$, where $\varepsilon_\eta = \frac{1}{\#\Delta}\sum_{\tau\in\Delta}\eta(\tau)\tau^{-1}$.

Definition 6.1. For p odd, let $\mathbf{z}^\pm = (z_n^\pm)_n \in \mathbf{H}^1_{\mathrm{Iw}}(T) = \varprojlim H^1(k_n, T)$ be Kato's zeta elements (see [Kobayashi, Theorem 5.2 i] and [Ka, Theorem 12.5]). Write

$$\big(L_p^\sharp(E,\eta,X), L_p^\flat(E,\eta,X)\big)$$

for the η-component of the image of $\eta(-1)\,\mathrm{Col}(\mathbf{z}^{\eta(-1)})$ in Λ^2, which we naturally view as an element of $\mathbb{Z}_p[\![X]\!]^2 \cong (\Lambda^\eta)^2$. If $p = 2$, we have $\mathbf{z}^\pm = (z_n^\pm)_n \in \mathbf{H}^1_{\mathrm{Iw}}(T) \otimes \mathbb{Q} = \varprojlim H^1(k_n, T) \otimes \mathbb{Q}$, and we extend our Coleman map naturally to $\mathrm{Col}_\mathbb{Q} : \mathbf{H}^1_{\mathrm{Iw}}(T) \otimes \mathbb{Q} \to (\Lambda \oplus \Lambda) \otimes \mathbb{Q}$. Now define

$$\big(L_2^\sharp(E,\eta,X), L_2^\flat(E,\eta,X)\big)$$

as the image of $(\eta(-1)\,\mathrm{Col}_\mathbb{Q}(\mathbf{z}^{\eta(-1)}))$ in the quotient $\mathbb{Q} \otimes \mathbb{Z}_2[\![X]\!]^2$ of $\mathbb{Q} \otimes \mathbb{Z}_2[\Delta][\![X]\!]^2 = \mathbb{Q} \otimes \Lambda^{\oplus 2}$ induced by the map $\Lambda \to \mathbb{Z}_2[\![X]\!]$, $g \in \Delta \mapsto \eta(g)$.

Let $\psi = \eta\chi$ be a nontrivial character of $\mathcal{G}_n$ of conductor N, so that $\chi(\gamma_n)$ is a primitive p^nth root of unity. We also let α and $\overline{\alpha}$ be the two roots of $X^2 - a_p X + p$. Recall that $N = n+1$ for p odd, and $N = n+2$ if $p = 2$. Let $L(E,\psi,s)$ be the Hasse–Weil L-function with Dirichlet character ψ, and denote by $\Omega_E^{\pm}$ the real and imaginary Néron periods, obtained by integrating an invariant differential[3] ω_E. We can compare $L(E,\psi,s)$ with its p-adic counterpart $L_p(E,\alpha,\eta,X)$ of Mazur, Tate, and Teitelbaum originally due to Amice and Vélu [AV], and Višik [Vi]:

Theorem 6.2. *Let the notation be as above. For the p-adic L-function $L_p(E,\alpha,\eta,X)$ of* [MTT],

$$\alpha^N L_p\big(E,\alpha,\eta,\chi(\gamma_n)-1\big) = \frac{p^N}{\tau(\overline{\psi})}\frac{L(E,\overline{\psi},1)}{\Omega_E^{\eta(-1)}},$$

where $\tau(\overline{\psi})$ is the Gauß sum $\sum_{\sigma\in\mathcal{G}_n}\overline{\psi}(\sigma)\zeta_{p^N}^{\sigma}$.

For $\psi = 1$, we have

$$L_p(E,\alpha,0) = \big(1-\alpha^{-1}\big)^2\frac{L(E,1)}{\Omega_E^{+}}.$$

The statement of this theorem only makes sense after fixing an embedding of an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ inside the completion of an algebraic closure of $\mathbb{Q}_p$: We fix an embedding $\overline{\mathbb{Q}}\to\mathbb{C}_p$. We also fix an embedding $\overline{\mathbb{Q}}\to\mathbb{C}$. We would like to go further and compare both of these very classical p-adic L-functions to our p-adic L-functions $L_p^{\sharp}$ and $L_p^{\flat}$.

There is a map $\exp^*_{\omega_E}: H^1(k_n,V)\to\operatorname{cotan}(E/k_n)$, where $V = T\otimes\mathbb{Q}_p$ and $\operatorname{cotan}(E/k_n)$ is the cotangent space of E/k_n at the origin (see [Kobayashi, Section 8.7]) with the following properties:

Proposition 6.3. *The morphism $P_{n,x}$ in Definition* 3.1 *is given by*

$$P_{n,x}(z) = \Bigg(\sum_{\sigma\in\mathcal{G}_n}\log_{\mathcal{F}_{ss}}\big(x^{\sigma}\big)\sigma\Bigg)\Bigg(\sum_{\sigma\in\mathcal{G}_n}\exp^*_{\omega_E}\big(z^{\sigma}\big)\sigma^{-1}\Bigg).$$

This is [Kobayashi, Proposition 8.25]. The following theorem is [Ka, Theorem 12.5]:

Theorem 6.4 *(Kato). With notation as above,*

$$\psi\Bigg(\sum_{\sigma\in\mathcal{G}_n}\exp^*_{\omega_E}\big(\mathbf{z}^{\eta(-1)\sigma}\big)\sigma^{-1}\Bigg) = \frac{L(E,\overline{\psi},1)}{\Omega_E^{\eta(-1)}}.$$

Proposition 6.5. *Let ζ_{p^n} be any primitive p^nth root of unity. With notation as above,*

$$\big(\alpha^N L_p(E,\alpha,\eta,\zeta_{p^n}-1),0\big) = \big(L_p^{\sharp}(E,\eta,\zeta_{p^n}-1),L_p^{\flat}(E,\eta,\zeta_{p^n}-1)\big)\mathcal{H}_n(\zeta_{p^n}-1).$$

Proof. Let $\pi_\psi:\Lambda_n\to\overline{\mathbb{Q}_p}$ be induced by a character $\psi:\mathcal{G}_n\to\overline{\mathbb{Q}}^{\times}\subset\overline{\mathbb{Q}_p}^{\times}$ which sends X to $\zeta_{p^n}-1$. Then by definition, the right-hand side equals

$$\pi_\psi^{\oplus 2}\big(h_n^0\big(\eta(-1)\operatorname{Col}_n\big(z_n^{\eta(-1)}\big)\big)\big) = \big(\psi\circ P_n^1\big(z_n^{\eta(-1)}\big),\psi\circ P_n^0\big(z_n^{\eta(-1)}\big)\big)\times\psi(-1).$$

[3] Which is defined up to multiplication by ±1. We use the same ω_E for constructing $\Omega^{\pm}$ and $\exp^*_{\omega_E}$.

But by Proposition 6.3,

$$\psi \circ P_n^i\big(z_n^{\eta(-1)}\big) = \psi\Bigg(\sum_{\sigma\in\mathcal{G}_n} \log_{\mathcal{F}_{ss}}\big(\delta_n^i\big)^\sigma \sigma\Bigg)\psi\Bigg(\sum_{\sigma\in\mathcal{G}_n} \exp^*_{\omega_E}\big(z_n{}^{\eta(-1)\sigma}\big)\sigma^{-1}\Bigg), \quad \text{so}$$

$$\big(\psi \circ P_n^1\big(z_n^{\eta(-1)}\big),\, \psi \circ P_n^0\big(z_n^{\eta(-1)}\big)\big) = \left(\tau(\psi)\frac{L(E,\overline{\psi},1)}{\Omega_E^{\eta(-1)}}, 0\right)$$

by Theorem 6.4 and trace computations, which equals

$$= \left(\frac{\psi(-1)p^N}{\tau(\overline{\psi})}\frac{L(E,\overline{\psi},1)}{\Omega_E^{\eta(-1)}}, 0\right) = \big(\psi(-1)\alpha^N L_p(E,\alpha,\eta,\zeta_{p^n}-1), 0\big) \quad \text{by Theorem 6.2.} \qquad \square$$

Corollary 6.6. $(L_p^\sharp(E,\eta,\zeta_{p^n}-1), L_p^\flat(E,\eta,\zeta_{p^n}-1))\mathcal{H}(\zeta_{p^n}-1) = (\alpha^N L_p(E,\eta,\alpha,\zeta_{p^n}-1),0)A^{-N}$.

Proof. We have $\mathcal{H}(\zeta_{p^n}-1) = \lim_{m\to\infty}\mathcal{H}_n\mathcal{A}_{n+1}\cdots\mathcal{A}_{n+m}A^{-m}A^{-N}(\zeta_{p^n}-1)$. But $\mathcal{A}_{n+m}(\zeta_{p^n}-1) = A$ for $m>0$ from Observation 3.4, so $\mathcal{H}(\zeta_{p^n}-1) = \mathcal{H}_n(\zeta_{p^n}-1)A^{-N}$. $\square$

Lemma 6.7. *We have the matrix identity* $A^{-N}\left(\begin{smallmatrix}1 & 1\\ -\alpha^{-1} & -\overline{\alpha}^{-1}\end{smallmatrix}\right) = \left(\begin{smallmatrix}\alpha^{-N} & \overline{\alpha}^{-N}\\ -\alpha^{-N-1} & -\overline{\alpha}^{-N-1}\end{smallmatrix}\right)$.

Proof. We obtain this by diagonalization or by induction. Note that $1 = \frac{a_p}{p}\alpha - \frac{1}{p}\alpha^2$. $\square$

Definition 6.8. Put $\left(\begin{smallmatrix}\log_\alpha^\sharp(1+X) & \log_{\overline{\alpha}}^\sharp(1+X)\\ \log_\alpha^\flat(1+X) & \log_{\overline{\alpha}}^\flat(1+X)\end{smallmatrix}\right) := \mathcal{H}(X)\left(\begin{smallmatrix}1 & 1\\ -\alpha^{-1} & -\overline{\alpha}^{-1}\end{smallmatrix}\right)$.

Lemma 6.9. *We have*

$$\log_\alpha^\sharp(1+X) \sim \log_{\overline{\alpha}}^\flat(1+X) \sim \log_p(1+X)^{\frac{1}{2}} \quad \textit{or} \quad \log_\alpha^\flat(1+X) \sim \log_{\overline{\alpha}}^\sharp(1+X) \sim \log_p(1+X)^{\frac{1}{2}}.$$

Proof. From the Growth Lemma 4.8, $\log_\alpha^* = \log_\alpha^*(1+X) \in O(\log_p(1+X)^{\frac{1}{2}})$ for $* \in \{\sharp,\flat\}$.

$$\det\begin{pmatrix}\log_\alpha^\sharp & \log_{\overline{\alpha}}^\sharp\\ \log_\alpha^\flat & \log_{\overline{\alpha}}^\flat\end{pmatrix} = \det(\mathcal{H})\det\begin{pmatrix}1 & 1\\ -\alpha^{-1} & -\overline{\alpha}^{-1}\end{pmatrix} \sim \log_p(1+X), \quad \text{cf. Example 4.7,}$$

so $\log_\alpha^\sharp(1+X)\log_{\overline{\alpha}}^\flat(1+X) - \log_{\overline{\alpha}}^\sharp(1+X)\log_\alpha^\flat(1+X) \sim \log_p(1+X)$. $\square$

Definition 6.10. Let K be a finite extension of $\mathbb{Q}_p$. We let

$$\mathcal{A}(K) := \big\{ f \in K[\![X]\!] \;\big|\; f \text{ is convergent on the open unit disc of } \mathbb{C}_p \big\}.$$

Lemma 6.11 *(Interpolation Lemma). Let* $0 \leqslant h < 1$ *be a real number, and let* $f(X), g(X) \in \mathcal{A}(K)$. *If* $f(X) \in O(\log_p(1+X)^h)$ *and* $g(X) \in O(\log_p(1+X)^h)$ *satisfy* $f(\zeta_{p^n}-1) = g(\zeta_{p^n}-1)$ *for all primitive* p^n*th roots of unity with* $n \geqslant 1$, *then* $g(X) = f(X)$.

Proof. Put $h(X) := f(X) - g(X) \in O(\log_p(1+X)^h)$. Then $h(\zeta_{p^n}-1) = 0$, so by [La, Lemma 4.7], $\frac{\log_p(1+X)}{X} | h(X)$ in $\mathcal{A}(K)$. If $h(X) \neq 0$, this would yield $\frac{\log_p(1+X)}{X} \sim \log_p(1+X) \in O(h(X))$ (cf. [Pollack,

discussion before Proposition 2.11], [Co, Proposition I.4.5]), and thus $\log_p(1+X) \in O(\log_p(1+X)^h)$, which would be a contradiction. □

We are now ready to state the main theorem:

Main Theorem 6.12.

$$\log_\alpha^\sharp(1+X)L_p^\sharp(E,\eta,X) + \log_\alpha^\flat(1+X)L_p^\flat(E,\eta,X) = L_p(E,\alpha,\eta,X).$$

Proof. Put $L_p^* = L_p^*(E,\eta,\zeta_{p^n}-1)$, $\log_\alpha^* = \log_\alpha^*(\zeta_{p^n})$ for $* \in \{\sharp,\flat\}$, and $L_p(\alpha) = L_p(E,\alpha,\eta,\zeta_{p^n}-1)$. From Corollary 6.6 and Lemma 6.7, we have

$$\left(L_p^\sharp, L_p^\flat\right)\begin{pmatrix}\log_\alpha^\sharp & \log_{\overline{\alpha}}^\sharp \\ \log_\alpha^\flat & \log_{\overline{\alpha}}^\flat\end{pmatrix} = \left(\alpha^N L_p(\alpha), 0\right)\begin{pmatrix}\alpha^{-N} & \overline{\alpha}^{-N} \\ -\alpha^{-N-1} & \overline{\alpha}^{-N-1}\end{pmatrix} = \left(L_p(\alpha), L_p(\overline{\alpha})\right),$$

since by Theorem 6.2, $\alpha^N L_p(\alpha) = \overline{\alpha}^N L_p(\overline{\alpha})$. Because this holds for all primitive p^nth roots of unity ζ_{p^n} and both sides are $O(\log_p(1+X)^{\frac{1}{2}})$, they agree by the Interpolation Lemma 6.11 above with $h = \frac{1}{2}$. □

Remark 6.13. By convention (e.g. [Pollack]), we suppress the character η from the notation if it is trivial. Thus for the trivial character, we have

$$\log_\alpha^\sharp(1+X)L_p^\sharp(E,X) + \log_\alpha^\flat(1+X)L_p^\flat(E,X) = L_p(E,\alpha,X)$$

as in the introduction.

Now for general supersingular $p|a_p$, we can evaluate $L_p^\sharp(E,\eta,X)$ and $L_p^\flat(E,\eta,X)$ at $X=0$:

	$L_p^\sharp(E,\eta,0)$	$L_p^\flat(E,\eta,0)$
p odd, $\eta=1$	$\left(-a_p^2+2a_p+p-1\right)\frac{L(E,1)}{\Omega_E^+}$	$(2-a_p)\frac{L(E,1)}{\Omega_E^+}$
p odd, $\eta\neq 1$	$-pa_p\frac{L(E,\overline{\eta},1)}{\tau(\overline{\eta})\Omega_E^{\eta(-1)}}$	$-p\frac{L(E,\overline{\eta},1)}{\tau(\overline{\eta})\Omega_E^{\eta(-1)}}$
$p=2$, $\eta=1$	$\left(-a_p^3+2a_p^2+2pa_p-a_p-2p\right)\frac{L(E,1)}{\Omega_E^+}$	$\left(-a_p^2+2a_p+p-1\right)\frac{L(E,1)}{\Omega_E^+}$
$p=2$, $\eta\neq 1$	$-p^2a_p\frac{L(E,\overline{\eta},1)}{\tau(\overline{\eta})\Omega_E^{\eta(-1)}}$	$-p^2\frac{L(E,\overline{\eta},1)}{\tau(\overline{\eta})\Omega_E^{\eta(-1)}}$

Proposition 6.14. *Let $\eta:\Delta\to\mathbb{Z}_p^\times$ be any character. Then at least one of $L_p^\sharp(E,\eta,X)$ and $L_p^\flat(E,\eta,X)$ is a nonzero function. If $L(E,\overline{\eta},1)\neq 0$, then they are both nonzero.*

Proof. By a theorem of Rohrlich [Ro], $L_p(E,\alpha,\eta,\zeta_{p^n}-1)\neq 0$ for $n\gg 0$. Thus, the vector $(L_p^\sharp(E,\eta,X), L_p^\flat(E,\eta,X))$ can't be zero. Further, if $L(E,\overline{\eta},1)\neq 0$, then the assertion follows from the table above. □

In view of Mazur's and Swinnerton-Dyer's conjecture in the ordinary case [MSD, Conjecture 1] and the fact that neither $L_p^\sharp(E,\eta,X)$ nor $L_p^\flat(E,\eta,X)$ vanish when $a_p=0$ (cf. [Pollack, Corollary 5.11]), it seems reasonable to conjecture the following:

Conjecture 6.15. *Let E be an elliptic curve, p be a prime of good supersingular reduction, and $\eta:\Delta\to\mathbb{Z}_p^\times$ be any character. Then $L_p^\sharp(E,\eta,X)$ and $L_p^\flat(E,\eta,X)$ are both nonzero functions.*

Proposition 6.14 gives even more evidence for this conjecture via the fact that a positive proportion of elliptic curves has rank zero, cf. [BS].

Remark 6.16. We can recover Kobayashi's and Pollack's results concerning $a_p = 0$. We have

$$\mathcal{H}(X) = \begin{pmatrix} \log_p^+(1+X) & 0 \\ 0 & p\log_p^-(1+X) \end{pmatrix} \quad \text{for odd } p,$$
$$\mathcal{H}(X) = \begin{pmatrix} 0 & -\log_p^+(1+X) \\ \log_p^-(1+X) & 0 \end{pmatrix} \quad \text{for } p = 2.$$

Thus we find that

$$\begin{pmatrix} \log_\alpha^\sharp(1+X) \\ \log_\alpha^\flat(1+X) \end{pmatrix} = \begin{pmatrix} \log_p^+(1+X) \\ \alpha\log_p^-(1+X) \end{pmatrix} \quad \text{if } p \text{ is odd},$$
$$\begin{pmatrix} \log_\alpha^\sharp(1+X) \\ \log_\alpha^\flat(1+X) \end{pmatrix} = \begin{pmatrix} -\frac{1}{2}\log_2^+(1+X)\alpha \\ \log_2^-(1+X) \end{pmatrix} \quad \text{if } p = 2.$$

This shows that the extra factor of $\frac{1}{2}$ in [Pollack, Theorem 5.6] comes from an extra factor of A^{-1} in Definition 4.5 of $\mathcal{H}$ because the conductor N is one larger than usual if $p = 2$.

$$\left(L_2^\sharp, L_2^\flat\right) = \left(-L_2^-, L_2^+\right) \quad \text{in Pollack's notation},$$
$$\left(L_p^\sharp, L_p^\flat\right) = \begin{cases} (L_p^+, L_p^-) & \text{in Pollack's notation}, \\ (L_p^-, L_p^+) & \text{in Kobayashi's notation} \end{cases} \quad \text{if } p \text{ is odd}.$$

The matrix $\tilde{Y}$ was inserted so as to match Kobayashi's construction for $a_p = 0$. He constructed his $L_p^\pm$ from elements $(c_n^-, c_n^+) = (\delta_n^{-N+1}, \delta_n^{-N})$. This is why $c_0^+ = -c_0$ rather than $c_0^+ = c_0$ in [Kobayashi]. Let $\widetilde{\omega_n}^- := \prod_{m\in\mathbb{N}} \Phi_{2m-1}(1+X)$, $\widetilde{\omega_n}^+ := \prod_{m\in\mathbb{N}} \Phi_{2m}(1+X)$. Denoting the projection $\Lambda \to \Lambda_n$ by an overline,

$$\begin{array}{ccccc} \left(P_n^-\varepsilon_\eta, P_n^+\varepsilon_\eta\right) & = \left(\overline{L_p^-(E,\eta,X)}, \overline{L_p^+(E,\eta,X)}\right)\begin{pmatrix} \widetilde{\omega_n}^+ & 0 \\ 0 & \widetilde{\omega_n}^- \end{pmatrix} & = \left(\overline{L_p^-(E,\eta,X)}, \overline{L_p^+(E,\eta,X)}\right)\mathcal{H}_n Y_{-N} \\ \| & & \\ \left(P_n^{-N+1}\varepsilon_\eta, P_n^{-N}\varepsilon_\eta\right) & = \varepsilon_\eta \operatorname{Col}_n\left(\mathbf{z}^{\eta(-1)}\right)\mathcal{H}_n Y_{-N} & = \left(\overline{L_p^\sharp(E,\eta,X)}, \overline{L_p^\flat(E,\eta,X)}\right)\mathcal{H}_n Y_{-N}. \end{array}$$

7. The two Selmer groups

From now on, assume p is odd.

7.1. The image of the Coleman map

Recall that the map Col_n from Proposition 5.3 was defined by

$$\begin{array}{ccc} H^1(k_n, T) & \xrightarrow{\operatorname{Col}_n} & \frac{\Lambda_n \oplus \Lambda_n}{\operatorname{Ker} h_n} \\ & \searrow^{P_n^{i+1}, P_n^i} & \downarrow h_n^i \\ & & \Lambda_n \oplus \Lambda_n. \end{array}$$

We can split the limit of these maps $\operatorname{Col} = \varprojlim_n \operatorname{Col}_n$ and define $\sharp/\flat$-Coleman maps:

Definition 7.1. $\mathrm{Col} =: (\mathrm{Col}^\sharp, \mathrm{Col}^\flat)$.

However, we cannot split Col_n in general, since $\mathrm{Ker}\, h_n$ lives in $\Lambda_n \oplus \Lambda_n$. If $n = 0$, we have $\mathrm{Ker}\, h_0 = 0$ and thus we can put:

Definition 7.2. $\mathrm{Col}_0 =: (\mathrm{Col}_0^\sharp, \mathrm{Col}_0^\flat) = (-a_p P_0^1 + P_0^0, -P_0^1)$.

Thanks[4] to $\tilde{Y}$, $\mathrm{Ker}\, h_1 = 0 \oplus X\Lambda_1$, so we can write $\mathrm{Col}_1 = (\mathrm{Col}_1^\sharp, \mathrm{Col}_1^\flat)$ and $\mathrm{Col}_1^\sharp = -P_1^1$.

Proposition 7.3. $\mathrm{Col}^\flat$ *is surjective.*

Lemma 7.4. $\mathcal{F}_{ss}(\mathfrak{m}_0)$ *is generated by* $(c_0^\sigma)_{\sigma\in\mathcal{G}_0}$ *as a* $\mathbb{Z}_p$*-module.*

Proof. We have $\mathrm{Tr}_{k_0/\mathbb{Q}_p}(c_0) = (a_p - 2)c_{-1}$ by Theorem 2.2(2), and we know that $\mathcal{F}_{ss}(\mathfrak{m}_0)$ is generated by (c_0^σ) and (c_{-1}^σ). □

Lemma 7.5. $(c_0^\sigma)_{\sigma\in\mathcal{G}_0}$ *are a basis for* $\mathcal{F}_{ss}(\mathfrak{m}_0)$ *as a* $\mathbb{Z}_p$*-module.*

Proof. $\mathrm{rank}_{\mathbb{Z}_p}(\mathcal{F}_{ss}(\mathfrak{m}_0)^\eta) = 1$ for any character $\eta : \Delta \to \mathbb{Z}_p^\times$. □

Proof of Proposition 7.3. We can prove the surjectivity of $\mathrm{Col}_0^\flat = -P_0^1$ as in [Kobayashi, Proposition 8.23]: $P_0^1(z) = \sum_{\sigma\in\Delta}(c_0^\sigma, z)_0\sigma$, so from Lemma 7.5, P_0^1 is given by

$$H^1(k_0, T) \to \mathrm{Hom}\big(\mathcal{F}_{ss}(\mathfrak{m}_0), \mathbb{Z}_p\big) \cong \Lambda_0,$$

where the first map comes from the pairing given by the cup product $(\,,\,)_0 : \mathcal{F}_{ss}(\mathfrak{m}_0) \times H^1(k_0, T) \to \mathbb{Z}_p$ (see [Kobayashi, (8.23) on p. 18]), and the last identification is $f \mapsto \sum_{\sigma\in\Delta} f(c_0^\sigma)\sigma$.

Now $H^1(k_0, T) \to \Lambda_0$ is surjective since its Pontryagin dual is the injection

$$\mathcal{F}_{ss}(\mathfrak{m}_0) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \hat{E}(k_0) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(k_0, V/T),$$

where $V = T \otimes \mathbb{Q}_p$. In fact, $E(k_0) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(k_0, V/T)$ is always an injection, so we want $\hat{E}(k_0) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to E(k_0) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ to be one as well. Now this follows from the cokernel $\tilde{E}(\mathbb{F}_p)$ of $\hat{E}(k_0) \hookrightarrow E(k_0)$ having no p-torsion, since p is supersingular.

Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
\varprojlim_n H^1(k_n, T) & \xrightarrow{\mathrm{Col}^\flat} & \Lambda & \longrightarrow & \mathrm{Coker}(\mathrm{Col}^\flat) & \longrightarrow & 0 \\
\big\downarrow{\scriptstyle \mathrm{cor}} & & \big\downarrow & & \big\downarrow & & \\
H^1(k_0, T) & \xrightarrow{\mathrm{Col}_0^\flat} & \Lambda_0 = \mathbb{Z}_p[\Delta] & \longrightarrow & \mathrm{Coker}(\mathrm{Col}_0^\flat) & \longrightarrow & 0.
\end{array}$$

The surjectivity of $\mathrm{Col}^\flat$ follows from Nakayama's lemma if we know that the corestriction cor is surjective, which is indeed the case since this is true at finite levels: $H^1(k_n, T) \to H^1(k_m, T)$ is surjective if $n \geqslant m$. This can be seen as follows: The kernel of the restriction map $H^1(k_m, V/T) \to H^1(k_n, V/T)$

[4] It would have been more natural to choose $-\tilde{Y} = (AB_-)^{-1}$, but then we would have been off by a factor of -1 from Kobayashi's sign convention (cf. Remark 6.16) in the case $a_p = 0$.

is $H^1(\mathrm{Gal}(k_n/k_m), H^0(k_n, V/T))$ by the inflation–restriction sequence. But the formal group $\mathcal{F}_{ss}$ has no p-power torsion in k_n by Lemma 2.3, so $H^0(k_n, V/T) = 0$. Thus the kernel is zero, so we are done after using Tate duality. □

Proposition 7.6. *If η is trivial, then $\varepsilon_\eta \operatorname{Col}^\sharp$ is surjective. If η is nontrivial, then $\operatorname{Im}(\varepsilon_\eta \operatorname{Col}^\sharp) = J^\eta$. Here, $J = (a_p + a_p X + \frac{a_p}{p} X^2, X) \subset \Lambda$.*

Lemma 7.7. *We have an exact sequence*

$$0 \to \mathcal{F}_{ss}(\mathfrak{m}_{-1}) \xrightarrow{\Delta} \mathcal{F}_{ss}(\mathfrak{m}_0) \oplus \mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1) \xrightarrow{[-]} \mathcal{F}_{ss}(\mathfrak{m}_1) \to 0,$$

where $\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)$ is the $\mathbb{Z}_p$-submodule of $\mathcal{F}_{ss}(\mathfrak{m}_1)$ generated by $\{(\delta_1^{-1})^\sigma\}_{\sigma\in\mathcal{G}_1}$, Δ the diagonal map, and $[-] : (a, b) \mapsto (a - b)$.

Proof. $\{(\delta_1^{-1})^\sigma\}_{\sigma\in\mathcal{G}_1}$ and $\{(\delta_1^0)^\sigma\}_{\sigma\in\mathcal{G}_1} = \{c_0^\sigma\}_{\sigma\in\mathcal{G}_1}$ generate $\mathcal{F}_{ss}(\mathfrak{m}_1)$ as a $\mathbb{Z}_p$-module, so we have to prove that $\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1) \cap \mathcal{F}_{ss}(\mathfrak{m}_0) = \mathcal{F}_{ss}(\mathfrak{m}_{-1})$. Let $P \in \mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1) \cap \mathcal{F}_{ss}(\mathfrak{m}_0)$. Then $\operatorname{Tr}_{1/0} P \in \mathcal{F}_{ss}(\mathfrak{m}_{-1})$, since this holds for all elements of $\mathcal{C}_{ss}^{\delta_1^{-1}}$. But since we also have $P \in \mathcal{F}_{ss}(\mathfrak{m}_0)$, $\operatorname{Tr}_{1/0} P = pP$. Thus, $p(P^\sigma - P) = 0$ for all $\sigma \in \mathrm{Gal}(k_0/\mathbb{Q}_p)$. But $\mathcal{F}_{ss}(\mathfrak{m}_0)$ has no p-torsion, so P is invariant under $\mathrm{Gal}(k_0/\mathbb{Q}_p)$, whence $P \in \mathcal{F}_{ss}(\mathfrak{m}_{-1})$. Also, $\mathcal{F}_{ss}(\mathfrak{m}_{-1}) \subset \mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)$ since $\operatorname{Tr}_{1/0} \delta_1^{-1} = \delta_0^0 = c_{-1}$ and $\{c_{-1}^\sigma\}_{\sigma\in\Delta}$ generate $\mathcal{F}_{ss}(\mathfrak{m}_{-1})$ as a $\mathbb{Z}_p$-module (see e.g. [Po1]). □

Corollary 7.8. *If $\eta : \Delta \to \mathbb{Z}_p^\times$ is the trivial character, then* $\operatorname{rank}_{\mathbb{Z}_p}(\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1))^\eta = p$.

Proof. $\operatorname{rank}_{\mathbb{Z}_p} \mathcal{F}_{ss}(\mathfrak{m}_{-1})^\eta = 1$, $\operatorname{rank}_{\mathbb{Z}_p} \mathcal{F}_{ss}(\mathfrak{m}_0)^\eta = 1$, and $\operatorname{rank}_{\mathbb{Z}_p} \mathcal{F}_{ss}(\mathfrak{m}_1)^\eta = p$. □

Proof of Proposition 7.6. The idea is to use the map $\operatorname{Col}_1^\sharp$ in the way we used $\operatorname{Col}_0^\flat$ in the proof of Proposition 7.3. For η trivial, $(\varepsilon_\eta \delta_1^{-1^\sigma})_{\sigma\in\Gamma_1}$ is a basis for $\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)^\eta$ by the above Corollary 7.8. Here, we have written $\mathcal{G}_1 = \Delta \times \Gamma_1$, and the proof can now proceed as in the $\operatorname{Col}^\flat$-case, since from Lemma 7.7, $\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)^\eta \cong \mathcal{F}_{ss}(\mathfrak{m}_1)^\eta$, so that $\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)^\eta \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(k_1, V/T)$ is an injection.

For η nontrivial, we prove that $\operatorname{Im}(\varepsilon_\eta \operatorname{Col}_1^\sharp) = \varepsilon_\eta(a_p + a_p X + \frac{a_p}{p} X^2, X)\Lambda_1$. Then we use Nakayama's lemma as above.

We have that $\operatorname{Col}_1^\sharp = -P_1^1 = -\frac{a_p}{p} P_1^0 + P_1^{-1}$, and from the previous Lemma 7.7 that $\mathcal{F}_{ss}(\mathfrak{m}_1)^{\eta^{-1}} \cong \mathcal{F}_{ss}(\mathfrak{m}_0)^{\eta^{-1}} \oplus \mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)^{\eta^{-1}}$. Thus we can describe $-\varepsilon_\eta \operatorname{Col}_1^\sharp$ by

$$\begin{array}{ccccc} H^1(k_1, T)^\eta & \longrightarrow & \mathrm{Hom}(\mathcal{F}_{ss}(\mathfrak{m}_1)^{\eta^{-1}}, \mathbb{Z}_p) & \longrightarrow & \Lambda_1^\eta \\ & & \| \text{ Lemma 7.7} & \nearrow & \\ & & \mathrm{Hom}(\mathcal{F}_{ss}(\mathfrak{m}_0)^{\eta^{-1}} \oplus \mathcal{C}^{\delta_1^{-1}}(\mathfrak{m}_1)^{\eta^{-1}}, \mathbb{Z}_p). & & \end{array}$$

The first (surjective) map is induced by the pairing in Definition 3.1, and the second map is

$$f \mapsto \varepsilon_\eta \sum_{\sigma\in\mathcal{G}_1} f\big(\varepsilon_{\eta^{-1}} \delta_1^{1^\sigma}\big)\sigma = |\Delta|\varepsilon_\eta \sum_{\sigma\in\Gamma_1} f\big(\varepsilon_{\eta^{-1}} \delta_1^{1^\sigma}\big)\sigma \in \mathbb{Z}_p[\Delta][\Gamma_1]^\eta = \Lambda_1^\eta.$$

From $\delta_1^1 = \frac{a_p}{p}\delta_1^0 - \delta_1^{-1}$,

$$\varepsilon_\eta \sum_{\sigma\in\Gamma_1} f\big(\varepsilon_{\eta^{-1}}\delta_1^{1^\sigma}\big)\sigma = \varepsilon_\eta \sum_{\sigma\in\Gamma_1}\left(\frac{a_p}{p} f\big(\varepsilon_{\eta^{-1}}\delta_1^0\big) - f\big(\varepsilon_{\eta^{-1}}\delta_1^{-1^\sigma}\big)\right)\sigma.$$

$\varepsilon_{\eta^{-1}}\delta_1^0 = \varepsilon_{\eta^{-1}} c_0$ and $(\varepsilon_\eta\delta_1^{-1})_{\sigma\in\Gamma_1}^\sigma$ are each a basis for $\mathcal{F}_{ss}(\mathfrak{m}_0)^{\eta^{-1}}$ and generators for $\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)^{\eta^{-1}}$. From Lemma 7.7,

$$\begin{aligned}\operatorname{rank}_{\mathbb{Z}_p}\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)^{\eta^{-1}} &= \operatorname{rank}_{\mathbb{Z}_p}\mathcal{F}_{ss}(\mathfrak{m}_1)^{\eta^{-1}} + \operatorname{rank}_{\mathbb{Z}_p}\mathcal{F}_{ss}(\mathfrak{m}_{-1})^{\eta^{-1}} - \operatorname{rank}_{\mathbb{Z}_p}\mathcal{F}_{ss}(\mathfrak{m}_0)^{\eta^{-1}}\\ &= p-1, \quad \text{since } \operatorname{rank}_{\mathbb{Z}_p}\mathcal{F}_{ss}\big(\mathfrak{m}_{-1}^{\eta^{-1}}\big) = 0 \text{ for } \eta^{-1} \text{ nontrivial.}\end{aligned}$$

But note that $\sum_{\sigma\in\Gamma_1}(\varepsilon_{\eta^{-1}}\delta_1^{-1})^\sigma\sigma = \varepsilon_{\eta^{-1}}\operatorname{Tr}_{1/0}\delta_1^{-1} = \varepsilon_{\eta^{-1}}\delta_0^0 = 0$. Thus, $(\varepsilon_{\eta^{-1}}\delta_1^{-1^\sigma})_{\sigma\in\Gamma_1-\{1\}}$ is a basis for $\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)^{\eta^{-1}}$, so

$$\operatorname{Hom}\big(\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)^{\eta^{-1}}, \mathbb{Z}_p\big) \cong \varepsilon_\eta X\Lambda_1$$

by $f\mapsto \varepsilon_\eta\sum_{\sigma\in\Gamma_1} f(\varepsilon_{\eta^{-1}}\delta_1^{-1^\sigma})\sigma$. Note that $X\Lambda_1 = \operatorname{Ker}(\mathbb{Z}_p[\Delta][\Gamma_1]\to\mathbb{Z}_p[\Delta])$.

Since $|\Delta| = p-1$ is a unit and the dual basis of the basis $\{\varepsilon_\eta^{-1}(\delta_1^{-1})^\sigma\}_{\sigma\in\Gamma_1-\{1\}}$ for $\mathcal{C}_{ss}^{\delta_1^{-1}}(\mathfrak{m}_1)^{\eta^{-1}}$ has image $\{\varepsilon_\eta(\sigma-1)\}_{\sigma\in\Gamma_1-\{1\}}$ in $\varepsilon_\eta\Lambda_1$,

$$\operatorname{Im}\big(\varepsilon_\eta \operatorname{Col}_1^\sharp\big) = \varepsilon_\eta\left(\frac{a_p}{p}\mathbb{Z}_p\sum_{\sigma\in\Gamma_1}\sigma - \sum_{\sigma\in\Gamma-\{1\}}\mathbb{Z}_p(\sigma-1)\right).$$

For $p\geqslant 5, a_p = 0$, so $\operatorname{Im}(\varepsilon_\eta\operatorname{Col}_1^\sharp) = \varepsilon_\eta\sum_{\sigma\in\Gamma-\{1\}}\mathbb{Z}_p(\sigma-1) = \varepsilon_\eta X\Lambda_1$.

If $p=3$, then

$$\operatorname{Im}\big(\varepsilon_\eta\operatorname{Col}_1^\sharp\big) = \varepsilon_\eta\left(\left(\frac{a_p}{p}+\frac{a_p}{p}(1+X)+\frac{a_p}{p}(1+X)^2\right)\Lambda_1 + X\Lambda_1\right),$$

since

$$\mathbb{Z}_p\left(\frac{a_p}{p}+\frac{a_p}{p}(1+X)+\frac{a_p}{p}(1+X)^2\right) \cong \Lambda_1\left(\frac{a_p}{p}+\frac{a_p}{p}(1+X)+\frac{a_p}{p}(1+X)^2\right).$$

Thus, $\operatorname{Im}(\varepsilon_\eta\operatorname{Col}_1^\sharp) = \varepsilon_\eta(a_p + a_pX + \frac{a_p}{p}X^2, X)\Lambda_1$. Now we can apply the arguments as in the proof of Proposition 7.3 to show $\operatorname{Im}(\varepsilon_\eta\operatorname{Col}^\sharp) = J^\eta$. Note that $\omega_1(X) = (1+X)^p - 1 \in p\Lambda + X\Lambda$. □

7.2. The main conjecture

We keep the notation of [Kobayashi]: $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$, $K_{-1} = \mathbb{Q}$, and $K_\infty = \bigcup_n K_n$. Let $\mathfrak{p}_n$ be the place in K_n and $\mathfrak{p}$ the place in K_∞ above p. Kobayashi constructed the two $\pm$-Selmer groups

$$\operatorname{Sel}^\pm(E/K_n) = \operatorname{Ker}\left(\operatorname{Sel}(E/K_n)\to\frac{E(K_{n,\mathfrak{p}_n})\otimes\mathbb{Q}_p/\mathbb{Z}_p}{E^\pm(K_{n,\mathfrak{p}_n})\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right),$$

and put

$$\mathrm{Sel}^{\pm}(E/K_\infty) = \varinjlim_n \mathrm{Sel}^{\pm}(E/K_n).$$

Thus, we could also write

$$\mathrm{Sel}^{\pm}(E/K_\infty) = \mathrm{Ker}\left(\mathrm{Sel}(E/K_\infty) \to \frac{E(K_{\infty,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^{\pm}(K_{\infty,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right),$$

where

$$\mathrm{Sel}(E/K_\infty) = \varinjlim_n \mathrm{Sel}(E/K_n),\ E(K_{\infty,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \varinjlim_n E(K_{n,\mathfrak{p}_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p,$$

and

$$E^{\pm}(K_{\infty,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \varinjlim_n E^{\pm}(K_{n,\mathfrak{p}_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

The essential property is that $E^{\pm}(K_{\infty,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is the exact annihilator of $\mathrm{Ker}(\mathrm{Col}^{\pm})$ under the local Tate pairing

$$\varprojlim_n H^1(K_{n,\mathfrak{p}_n}, T) \times \varinjlim_n H^1(K_{n,\mathfrak{p}_n}, V/T) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Thus, we make the following definition:

Definition 7.9. We let $E^{\sharp}_{\infty,\mathfrak{p}}$ (resp. $E^{\flat}_{\infty,\mathfrak{p}}$) be the exact annihilator of $\mathrm{Ker}\,\mathrm{Col}^{\sharp}$ (resp. $\mathrm{Ker}\,\mathrm{Col}^{\flat}$) under the local Tate pairing.

Lemma 7.10. *We have* $E(K_{\infty,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \varinjlim_n H^1(K_{n,\mathfrak{p}_n}, V/T)$.

Proof. $E(K_{n,\mathfrak{p}_n}) \otimes \mathbb{Z}_p$ and $E(K_{n,\mathfrak{p}_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ are exact annihilators of each other, and we have $\varprojlim_n E(K_{n,\mathfrak{p}_n}) \hat{\otimes} \mathbb{Z}_p = 0$ since p is supersingular (by [CG] or [Ha]). □

Definition 7.11. We now define our two Selmer groups:

$$\mathrm{Sel}^{\sharp}(E/K_\infty) := \mathrm{Ker}\left(\mathrm{Sel}(E/K_\infty) \to \frac{E(K_{\infty,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^{\sharp}_{\infty,\mathfrak{p}}}\right),$$

$$\mathrm{Sel}^{\flat}(E/K_\infty) := \mathrm{Ker}\left(\mathrm{Sel}(E/K_\infty) \to \frac{E(K_{\infty,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^{\flat}_{\infty,\mathfrak{p}}}\right).$$

We also define their Pontryagin duals $\mathcal{X}^*(E/K_\infty) := \mathrm{Hom}(\mathrm{Sel}^*(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ for $* \in \{\sharp, \flat\}$.

Definition 7.12. Let j be the natural morphism $\mathrm{Spec}\, K_n \to \mathrm{Spec}\, O_{K_n}[\frac{1}{p}]$, and let $H^q(\mathrm{Spec}\ O_{K_n}[\frac{1}{p}], j_*T)$ be the qth étale cohomology group. We define $\mathbf{H}^1(T) := \varprojlim_n H^q(\mathrm{Spec}\ O_{K_n}[\frac{1}{p}], j_*T)$. We let $\mathbf{Z}(T)$ be the Λ-submodule of $\mathbf{H}^1(T)$ generated by Kato's zeta elements $\mathbf{z}^+$ and $\mathbf{z}^-$. (We can make this definition since p is supersingular. See [Kobayashi, Section 5] or [Ka] for more details.)

Definition 7.13. $\mathcal{X}^0(E/K_\infty)$ is the Pontryagin dual to Kurihara's Selmer group (see [Ku]), which is

$$\mathrm{Sel}^0(E/K_\infty) := \mathrm{Ker}\big(\mathrm{Sel}(E/K_\infty) \to E(K_{\infty,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\big).$$

Theorem 7.14. *Let p be an odd supersingular prime, $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character, and $* \in \{\sharp, \flat\}$ be chosen so that $L_p^*(E, \eta, X) \neq 0$. Then $\mathcal{X}^*(E/K_\infty)^\eta$ is $\mathbb{Z}_p[\![X]\!]$-torsion.*

Proof. From [Kobayashi, Proposition 7.1 and the limit of (7.18)], we have the exact sequence

$$\mathbf{H}^1(T)^\eta \to \mathbf{H}^1_{\mathrm{Iw}}(T)^\eta \to \mathcal{X}(E/K_\infty)^\eta \to \mathcal{X}^0(E/K_\infty)^\eta \to 0,$$

noting that $\varprojlim_n E(K_{n,\mathfrak{p}_n})\hat{\otimes}\mathbb{Z}_p = 0$. Since $L_p^*(E, \eta, X) \neq 0$ by assumption, the arguments in the proof of [Kobayashi, Theorem 7.3 i] provide us with an injection ι in the exact sequence of $\mathbb{Z}_p[\![X]\!]$-modules

$$0 \to \mathbf{H}^1(T)^\eta \xrightarrow{\iota} \big(\mathbf{H}^1_{\mathrm{Iw}}(T)^\eta / \operatorname{Ker} \varepsilon_\eta \operatorname{Col}^*\big) \to \mathcal{X}^*(E/K_\infty)^\eta \to \mathcal{X}^0(E/K_\infty)^\eta \to 0. \tag{3}$$

To see that the entire sequence is exact, we can use the Cassels–Poitou–Tate exact sequence (cf. [PR, Appendix A.3.2] or [CS, Theorem 1.5]) and the discussion in [Kobayashi] preceding (7.16). But $\mathrm{Coker}(\iota)$ is killed by $L_p^*(E, \eta, X) \neq 0$ and is thus $\mathbb{Z}_p[\![X]\!]$-torsion. Now $\mathcal{X}^0(E/K_\infty)^\eta$ is a torsion $\mathbb{Z}_p[\![X]\!]$-module [Kobayashi, Corollary 7.2], so we are done. □

A consequence of Conjecture 6.15 would then be the following conjecture.

Conjecture 7.15. *Both $\mathcal{X}^\sharp(E/K_\infty)$ and $\mathcal{X}^\flat(E/K_\infty)$ are Λ-torsion.*

Using work of Kato in an analogous way to Kobayashi, we now prove the following theorem:

Theorem 7.16. *Let p be an odd supersingular prime, and $* \in \{\sharp, \flat\}$ so that $L_p^*(E, \eta, X) \neq 0$. Then for some integer $n \geqslant 0$,*

$$\mathrm{Char}\big(\mathcal{X}^*(E/K_\infty)^\eta\big) \supseteq \left(p^n \frac{1}{X} L_p^*(E, \eta, X)\right) \quad \text{if } * = \sharp,\ \eta \neq 1,\ \text{and } a_p = 0,$$

$$\mathrm{Char}\big(\mathcal{X}^*(E/K_\infty)^\eta\big) \supseteq \big(p^n L_p^*(E, \eta, X)\big) \quad \text{for all other cases.}$$

Further, if the p-adic representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{\mathbb{Z}_p}(T)$ on the automorphism group of the p-adic Tate module T is surjective, we can take $n = 0$.

To prove this, we need a proposition by Kurihara [Kobayashi, Proposition 7.1 ii] and a theorem by Kato [Ka, Theorem 12.5]:

Proposition 7.17 *(Kurihara).* $\mathbf{H}^2(T)$ *and* $\mathcal{X}^0(E/K_\infty)$ *are isomorphic as Λ-modules.*

Theorem 7.18 *(Kato). Suppose that* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{\mathbb{Z}_p}(T)$ *is surjective. Then*

$$\mathrm{Char}\big(\mathbf{H}^2(T)^\eta\big) \supseteq \mathrm{Char}\big(\mathbf{H}^1(T)^\eta/\mathbf{Z}(T)^\eta\big).$$

Theorem 7.16 then follows from the following exact sequences:

Proposition 7.19. *Choose $* \in \{\sharp, \flat\}$ so that $L_p^*(E, \eta, X) \neq 0$. Then there are exact sequences*

$$0 \to \mathbf{H}^1(T)^\eta/\mathbf{Z}(T)^\eta \to J^\eta/\big(L_p^*(E,\eta,X)\big) \to \mathcal{X}^*(E/K_\infty)^\eta \to \mathcal{X}^0(E/K_\infty)^\eta \to 0 \quad \text{if } * = \sharp,\ \eta \neq 1,$$

$$0 \to \mathbf{H}^1(T)^\eta/\mathbf{Z}(T)^\eta \to \Lambda^\eta/\big(L_p^*(E,\eta,X)\big) \to \mathcal{X}^*(E/K_\infty)^\eta \to \mathcal{X}^0(E/K_\infty)^\eta \to 0 \quad \text{if not.}$$

Proof. This follows from the exact sequence (3) in the proof of Theorem 7.14, Proposition 7.3, and Proposition 7.6. □

Since p is odd supersingular, Kato's main conjecture [Ka, Conjecture 12.10] reads:

Conjecture 7.20 *(Kato). For a character $\eta : \Delta \to \mathbb{Z}_p^\times$, $\mathrm{Char}(\mathcal{X}^0(E/K_\infty)^\eta) = \mathrm{Char}(\mathbf{H}^1(T)^\eta/\mathbf{Z}(T)^\eta)$.*

In view of Proposition 7.19, the following conjecture is equivalent to the main conjecture of Kato, and to that of Perrin-Riou [PR]:

Main Conjecture 7.21. *Let p be an odd supersingular prime, and choose $* \in \{\sharp, \flat\}$ so that $L_p^*(E, \eta, X) \neq 0$. In Theorem 7.16, $n = 0$ and the three inclusions are three equalities*:

$$\mathrm{Char}\big(\mathcal{X}^*(E/K_\infty)^\eta\big) = \left(\frac{1}{X} L_p^*(E,\eta,X)\right) \quad \text{if } * = \sharp,\ \eta \neq 1,\ \text{and } a_p = 0,$$

$$\mathrm{Char}\big(\mathcal{X}^*(E/K_\infty)^\eta\big) = \big(L_p^*(E,\eta,X)\big) \quad \text{for all other cases.}$$

Theorem 7.16 then follows from Kato's divisibility statement in [Ka]. Note that for $a_3 \neq 0$, $\mathrm{Char}(J^\eta/L_3^\sharp(E,\eta,X)) = (L_3^\sharp(E,\eta,X))$. (If $a_3 \neq 0$ and η nontrivial, $\Lambda^\eta/J^\eta \cong \mathbb{F}_3$ is pseudo-null.)

Open Problem 7.22. *One of the insights in [Kobayashi] was to describe the $E^\pm(K_{n,\mathfrak{p}})$ explicitly using trace maps. If one could explicitly write $E_{\infty,\mathfrak{p}}^{\sharp/\flat} = \varinjlim_n E^{\sharp/\flat}(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ for some easily defined $E^{\sharp/\flat}(K_{n,\mathfrak{p}})$, this should lead to some interesting applications.*

Remark 7.23. We also remark that the techniques of Pollack and Rubin [P&R] cannot be extended, since for an elliptic curve with complex multiplication supersingular at p, we always have $a_p = 0$.

Acknowledgments

Our thanks go to everybody who deserves them, in particular Takeshi Tsuji, both for his initial bit of skepticism for this topic and relentless encouragement later, improvements of various proofs, and a very valuable suggestion that went into Lemma 3.5; to Shinichi Kobayashi, Robert Pollack, and Antonio Lei for helpful comments and emails, and to the buoyant, cheerful atmosphere of room 406 at Todai Math. For helpful suggestions on the exposition and for pointing out mistakes, we thank Barry Mazur, Robert Pollack, Joseph Silverman, and the anonymous referee.

Supplementary material

The online version of this article contains additional supplementary material.
Please visit doi:10.1016/j.jnt.2011.11.003.

References

[AV] Y. Amice, J. Vélu, Distributions p-adiques associées aux séries de Hecke, in: Journées Arithmétiques de Bordeaux, Bordeaux, 1974, Astérisque 24–25 (1975) 119–131.

[BS] M. Bhargava, A. Shankar, Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, arXiv:1007.0052 [math.NT].

[CG] J. Coates, R. Greenberg, Kummer theory for abelian varieties over local fields, Invent. Math. 124 (1–3) (1996) 129–174.

[CS] J. Coates, R. Sujatha, Galois Cohomology of Elliptic Curves, Tata Inst. Fund. Res. Stud. Math., vol. 88, Narosa Publishing House, New Delhi, 2000.

[Co] P. Colmez, Théorie d'Iwasawa des représentations de de Rham d'un corps local, Ann. of Math. 148 (2) (1998) 485–571.

[El] N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, Invent. Math. 89 (3) (1987) 561–567.

[Ha] M. Hazewinkel, On norm maps for one dimensional formal groups I: The cyclotomic Γ-extension, J. Algebra 32 (1974) 89–108.

[Ho] T. Honda, On the theory of commutative formal groups, J. Math. Soc. Japan 22 (1970) 213–246.

[IP] A. Iovita, R. Pollack, Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields, J. Reine Angew. Math. 598 (2006) 71–103.

[Ka] K. Kato, p-Adic Hodge theory and values of zeta functions of modular forms, Astérisque 295 (2004) 117–290.

[Kobayashi] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. 152 (1) (2003) 1–36.

[Ku] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, Invent. Math. 149 (2002) 195–224.

[La] M. Lazard, Les zéros des fonctions analytiques d'une variable sur un corps valué complet, Publ. Math. Inst. Hautes Etudes Sci. 14 (1962) 47–75.

[Le] A. Lei, Iwasawa theory for modular forms at supersingular primes, Compos. Math. 147 (3) (May 2011) 803–838.

[LLZ] A. Lei, D. Loeffler, S. Zerbes, Wach modules and Iwasawa theory for modular forms, Asian J. Math. 14 (4) (December 2010) 475–528.

[Ma1] B. Mazur, Courbes elliptiques et symboles modulaires, in: Séminaire Bourbaki 414, 1971/1972, in: Lecture Notes in Math., vol. 317, Springer, 1972.

[Ma2] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math. 18 (1972) 183–266.

[MSD] B. Mazur, P. Swinnerton-Dyer, Arithmetic of Weil curves, Invent. Math. 25 (1974) 1–61.

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

[PR] B. Perrin-Riou, Fonctions L p-adiques des représentations p-adiques, Astérisque 229 (1995), 198 pp.

[Pollack] R. Pollack, The p-adic L-function of a modular form at a supersingular prime, Duke Math. J. 118 (3) (2003) 523–558.

[Po1] R. Pollack, An algebraic version of a theorem of Kurihara, J. Number Theory 110 (2005) 164–177.

[P&R] R. Pollack, K. Rubin, The main conjecture for CM elliptic curves at supersingular primes, Ann. of Math. 159 (1) (2004) 447–464.

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

[Si] J.H. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 106, Springer, New York, 1992.

[SU] C. Skinner, E. Urban, The Iwasawa main conjectures for GL_2, preprint.

[Vi] M.M. Višik, Nonarchimedean measures associated with Dirichlet series, Mat. Sb. 99 (141) (2) (1976) 248–260, 296.

[Wa] L. Washington, Introduction to Cyclotomic Fields, Grad. Texts in Math., vol. 83, Springer, New York, 1980.