On a conjecture of Perrin-Riou

KÂZIM BÜYÜKBODUK

Abstract. Our goal in this article is to give a proof of Perrin-Riou's conjecture (under very mild hypothesis) on the non-vanishing of the p-adic Beilinson-Kato class associated to an elliptic curve $E_{/\mathbb{Q}}$, when E has ordinary (i.e., good ordinary or multiplicative) or supersingular reduction at p. This generalizes the previous work of Bertolini and Darmon (for a good ordinary prime p) and Venerucci (for a split multiplicative prime p). Our method is based on the general theory Λ-adic Kolyvagin systems, as developed by the author previously (and enhanced slightly here) and it applies equally well to treat all these cases simultaneously.

Contents

1. Introduction 1
1.1. Notation and Background 4
1.2. Organization of the article 5
2. Selmer structures and Kolyvagin systems 5
2.1. Selmer structures 5
2.2. Module of Kolyvagin systems 7
3. Proof of Perrin-Riou's conjecture 9
3.1. Preliminaries 9
3.2. Main conjectures 11
3.3. The Λ-adic Beilinson-Kato Kolyvagin system and the conclusion of the proof 11
4. Logarithms of Heegner points and Beilinson-Kato classes 12
Acknowledgements 14
Appendix A. Proof of Theorem 2.10 14
1.1. An analysis of local cohomology groups 15
1.2. Patching Kolyvagin systems 18
References 20

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ and let N denote its conductor. Fix a prime $p > 3$ and let S denote the set consisting of all rational primes dividing Np and the archimedean place. In this set up, Kato [Kat04] has constructed an Euler system $\mathbf{c}^{\mathrm{BK}} = \{c_F^{\mathrm{BK}}\}$ where F runs through abelian extensions of $\mathbb{Q}$, $c_F^{\mathrm{BK}} \in H^1(F, T_p(E))$ is unramified away from the primes dividing Np and $T_p(E)$ is the p-adic Tate module of E. Kato's explicit reciprocity laws show that the class $c_{\mathbb{Q}}^{\mathrm{BK}} \in H^1(\mathbb{Q}, T_p(E))$ is non-crystalline

Key words and phrases. Kolyvagin systems, Iwasawa theory.

at p (and in particular, non-zero) precisely when $L(E/\mathbb{Q},1)\neq 0$, where $L(E/\mathbb{Q},s)$ is the Hasse-Weil L-function of E. Perrin-Riou in [PR93, §3.3.2] predicts the following assertion to hold true. Let $\mathrm{res}_p : H^1(G_{\mathbb{Q},S},T)\to H^1(\mathbb{Q}_p,T)$ denote the restriction map.

Conjecture 1.1. The class $\mathrm{res}_p\left(c_{\mathbb{Q}}^{\mathrm{BK}}\right)\in H^1(\mathbb{Q}_p,T_p(E))$ is non-torsion if and only if $L(E/\mathbb{Q},s)$ has at most a simple zero at $s=1$.

This is the conjecture we address in this article. Our main result is the following:

Theorem 1.2. *Suppose that E is an elliptic curve such that the residual representation*

$$\overline{\rho}_E : G_{\mathbb{Q},S}\longrightarrow \mathrm{Aut}(E[p])$$

is surjective. Assume further that p does not divide $\mathrm{ord}_\ell(j(E))$ whenever $\ell\mid N$ is a prime of split multiplicative reduction. Then the "if" part of Perrin-Riou's Conjecture 1.1 holds true in the following cases:

(a) *E has good ordinary reduction at p.*
(b) *E has good supersingular reduction at p and N is square-free.*
(c) *E has multiplicative reduction at p and there exists a prime $\ell \mid\mid N$ such that there $\overline{\rho}_E$ is ramified at ℓ.*

As per the "only if" direction, one may deduce the following as a rather straightforward consequence of the recent results due to Skinner, Skinner-Zhang and Venerucci in the case of p-ordinary reduction and due to Kobayashi and Wan in the case of p-supersingular reduction. We state it here for the sake of completeness.

Theorem 1.3. *In the situation of Theorem 1.2, the "only if" part of Perrin-Riou's conjecture holds true for all cases* (a), (b) *and* (c) *if we further assume:*

- *in the case of* (a)*, that N is square free and either E has non-split multiplicative reduction at one odd prime or split multiplicative reduction at two odd primes;*
- *in the case of* (c) *and when E non-split-multiplicative reduction at p that*
  - *p does not divide $\mathrm{ord}_p(\Delta_E)$,*
  - *for all primes $\ell \mid\mid N$ such that $\ell\equiv \pm 1 \mod p$, the prime p does not divide $\mathrm{ord}_\ell(\Delta_E)$,*
  - *there exists at least two prime factors $\ell \mid\mid N$ such that p does not divide $\mathrm{ord}_\ell(\Delta_E)$.*

We remark that in the situation of (a), the hypotheses in Theorem 1.3 may be slightly altered if we relied on the work of Zhang [Zha14, Theorem 1.3] on the converse of the Gross-Zagier-Kolyvagin theorem, in place of the work of Skinner. This on one hand would allow us to relax the condition on the conductor N, on the other hand would force us to introduce additional hypothesis (see Theorem 1.1 of loc.cit).

In a variety of cases, we will be able refine Theorem 1.2 and deduce that the square of the logarithm of a suitable Heegner point agrees with the logarithm of the Beilinson-Kato class $\mathbf{BK}_1$ up to an explicit non-zero algebraic factor. This will justify some of the hypothetical conclusions in [PR93, §3.3.3]. We record here the following result we are able to prove in order to provide an example. For a discussion covering other cases of interest the reader is referred to Section 4.

Theorem 1.4. *Suppose that E is an elliptic curve with non-split-multiplicative reduction at p and verifies the hypotheses of Theorem 1.2, also that there exists a prime $\ell \mid\mid N$ such that there $\overline{\rho}_E$ is ramified at ℓ. Assume that $r_{\mathrm{an}}=1$ and further that Nekovář's p-adic* *height pairing associated to the canonical splitting of the Hodge-filtration on the semi-stable Dieudonné module $D_{\mathrm{st}}(V)$ is non-vanishing. Then,*

$$\log_V\left(\mathrm{res}_p(\mathbf{BK}_1)\right)\cdot\log_V\left(\mathrm{res}_p(P)\right)^{-2}\in\overline{\mathbb{Q}}^{\times},$$

where $\log_V$ *stands for the Bloch-Kato logarithm associated to* E.

We may in fact prove similar results in the situations of (a) and (b) as well. We refer the reader to Section 4 (more particularly, to Theorem 4.1, Remark 4.3 and Theorem 4.4) below for further details.

Remark 1.5. Bertolini and Darmon have announced that in their future work [BD15], they will prove a result similar to Theorem 1.4 in the situation of (a). Also, using somewhat different techniques then those of [BD15], Venerucci [Ven15] gave a proof of the result above, when E has split multiplicative reduction at p. Our approach in this article not only offers a uniform treatment of Perrin-Riou's Conjecture in either of the settings (a)-(c) above, it also allows us to handle primes of non-split-multiplicative and supersingular reduction.

Concerning Theorem 1.4 and its other forms presented in Section 4, we would like to underline[1] a common key feature of the three approaches (in [BD15, Ven15] and here) towards it, despite their apparent differences: All three works make crucial use of a suitable p-adic Gross-Zagier formula, allowing the comparison of Heegner points with Beilinson-Kato elements. For the approach in [BD15], this formula is provided by [BDP13] (where the relevant p-adic Gross-Zagier formula is proved by exploiting Waldspurger's formula and it resembles Katz's proof of the p-adic Kronecker limit formula) and for Venerucci's approach in [Ven15], it is provided by [BD07] (where the authors use Hida deformations and the Čerednik-Drinfeld uniformization of Shimura curves). In our approach towards Theorem 1.4 here, we rely on the p-adic Gross-Zagier formulae of Perrin-Riou [PR87] in the situation of (a), of Kobayashi [Kob13] in the situation of (b) and the recent work of Disegni [Dis15] when E has non-split-multiplicative reduction at p.

Remark 1.6. Our methods here easily adapt to treat also higher weight eigenforms; however, our conclusion in that situation is not as satisfactory as in the case of elliptic curves. For this reason, here we shall only provide a brief overview of our results towards Perrin-Riou's conjecture in that level of generality. We say that a Galois representation V (with coefficients in a finite extension K of $\mathbb{Q}_p$) is *essentially self-dual* if it has a self-dual Tate-twist $V(r)$ and we say that an elliptic eigenform f (of even weight $2k$ and level N, with N coprime to p) is essentially self-dual if Deligne's representation W_f associated to f is. In this case, we set $V_f = W_f(k)$; this is necessarily the self-dual twist of W_f. Fix a Galois-stable $\mathfrak{o}_K$-lattice T_f contained in V_f and let $\mathtt{k}$ denote the residue field of $\mathfrak{o}_K$. We will set $\rho_f : G_{\mathbb{Q},S}\to\mathrm{GL}(T_f)$ (where S is the set consisting of all rational primes dividing Np and the archimedean place) and $\overline{\rho}_f := \rho_f\otimes\mathtt{k}$. If the conditions that

- $\overline{\rho}_f$ is absolutely irreducible,
- f is p-distinguished (namely, the semi-simplification of $\overline{\rho}_f\big|_{G_{\mathbb{Q}_p}}$ non-scalar),
- either
  - $H^0(\mathbb{Q}_p, V_f/T_f) = 0$, or
  - $H^0(\mathbb{Q}_p, V_f/T_f)$ is a finite cyclic group and $H^0(\mathbb{Q}_{\infty,p}, T_f) = 0$,

[1] We would like to thank Henri Darmon for an enlightening exchange regarding this point

- the Tamagawa factors $\#H^1\left(\langle \mathrm{Fr}_\ell\rangle, H^0\left(I_\ell, V_f/T_f\right)_{\mathrm{div}}\right)$ is prime to p.

simultaneously hold true, then

$$\begin{aligned}\mathrm{ord}_{s=k}\, L(f,s)=1 \implies &\text{ either } \log_{V_f} \mathbf{BK}_1 \neq 0\,,\\ &\text{ or else } \mathrm{res}_p : H^1_f(\mathbb{Q},V_f)\to H^1_f(\mathbb{Q}_p,V_f) \text{ is the zero map.}\end{aligned}$$

Here $H^1_f(\mathbb{Q}_p,V_f)\subset H^1(\mathbb{Q}_p,V_f)$ is the image of the Bloch-Kato exponential map and $H^1_f(\mathbb{Q},V_f)$ is the Bloch-Kato Selmer group.

Note in particular that the main result of [BB15] towards Perrin-Riou's conjecture for p-non-crystalline semistable modular forms escapes the methods of the current article.

1.1. **Notation and Background.** Let $\mathbb{Q}_S/\mathbb{Q}$ denote the maximal extension of $\mathbb{Q}$ unramified outside S and let $G_{\mathbb{Q},S} := \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$. For a general number field K, we likewise define K_S to be the maximal extension of K unramified at every place of K above those in S and set $G_{K,S} := \mathrm{Gal}(K_S/K)$.

Let $\boldsymbol{\mu}_{p^\infty}$ denote the p-power roots of unity. For a complete local noetherian $\mathbb{Z}_p$-algebra R and an $R[[G_{\mathbb{Q},S}]]$-module X which is free of finite rank over R, we define $X^* := \mathrm{Hom}(X,\boldsymbol{\mu}_{p^\infty})$ and refer to it as the Cartier dual of X. For any ideal I of R, we denote by $X[I]$ the R-submodule of X killed by all elements of I.

We let $T=T_p(E)$ denote the p-adic Tate-module of E; this is a free $\mathbb{Z}_p$-module of rank 2 which is endowed with a continuous $G_{\mathbb{Q},S}$-action. We define the *cyclotomic deformation* $\mathbb{T}$ of T by setting $\mathbb{T} := T\otimes\Lambda$ (where we let $G_{\mathbb{Q},S}$ act diagonally), where $\Lambda := \mathbb{Z}_p[[\Gamma]]$ (with $\Gamma=\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is the Galois group of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_\infty/\mathbb{Q}$) is the cyclotomic Iwasawa algebra. We finally let $\mathbb{Q}_n/\mathbb{Q}$ denote the unique subextension of $\mathbb{Q}_\infty/\mathbb{Q}$ of degree p^n (and Galois group $\Gamma/\Gamma^{p^n}\cong \mathbb{Z}/p^n\mathbb{Z}$).

It follows from [MR04, Theorems 3.2.4 & 5.3.3] that Kato's Euler system $\mathbf{c}^{\mathrm{BK}}$ maps under the *Euler systems to Kolyvagin systems map* of Mazur and Rubin to a Λ-adic Kolyvagin system $\mathbb{BK}\in\mathbf{KS}(\mathbb{T})$ and a Kolyvagin system $\mathbf{BK}\in\mathbf{KS}(T)$ for the canonical Selmer structure $\mathcal{F}_\Lambda$ on $\mathbb{T}$ and $\mathcal{F}_{\mathrm{can}}$ on T. Precise definitions of these objects will be recalled in the next section. The Kolyvagin system $\mathbf{BK}$ (respectively, the Λ-adic Kolyvagin system $\mathbb{BK}$) will be referred to as the Beilinson-Kato Kolyvagin system (respectively, the Λ-adic Beilinson-Kato Kolyvagin system). The initial terms $\mathbf{BK}_1\in H^1(G_{\mathbb{Q},S},T)$ of $\mathbf{BK}$ and $\mathbb{BK}_1\in H^1(\mathbb{Q},\mathbb{T})$ of $\mathbb{BK}$ have the following two properties:

$$\mathbf{BK}_1 = c_{\mathbb{Q}}^{\mathrm{BK}} \tag{1.1}$$

$$\mathbb{BK}_1 = \{c_{\mathbb{Q}_n}^{\mathrm{BK}}\}\in \varprojlim H^1(G_{\mathbb{Q}_n,S},T)=H^1(\mathbb{Q},\mathbb{T}) \tag{1.2}$$

where the latter equality in (1.2) follows from [MR04, Lemma 5.3.1(iii)].

It follows from the non-vanishing results of Rohrlich [Roh84] and Kato's explicit reciprocity laws for the Beilinson-Kato elements that $\mathbb{BK}_1$ never vanishes.

Fix a topological generator γ of Γ. In this article, will work with various quotients of Λ: For positive integers α and k, we set $R_\alpha := \Lambda/(\gamma-1)^\alpha$ and $R_{k,\alpha} := \Lambda/(p^k,(\gamma-1)^\alpha)$. We will consider $T_\alpha := \mathbb{T}\otimes R_\alpha$ and $T_{k,\alpha} := \mathbb{T}\otimes R_\alpha$. Note that $R_{1,1}=\mathbb{F}_p$ and we shall write $\overline{T}$ in place of $T_{1,1}$. Each of these modules are free of rank 2 over the respective ring R_α or $R_{k,\alpha}$. We will denote by pr_0 the augmentation map $\Lambda\to\mathbb{Z}_p$ and by slight abuse, also any map induced by it.

Throughout this article, we shall denote the order of vanishing of the Hasse-Weil L-function $L(E/\mathbb{Q}, s)$ by r_{an} and call it the *analytic rank of* E.

1.2. Organization of the article.

In Section 2.1, we recall basic notions from [MR04, Büy11], relevant to our study of Λ-adic Kolyvagin systems. In Section 2.2 we introduce the module of Kolyvagin systems and state our main result towards its structure (Theorem 2.10). We deduce Perrin-Riou's conjecture (which is stated as part of our principal result Theorem 1.2) in Section 3 based on this structure theorem. Section 4 is devoted to refinements of this result (still along Perrin-Riou's predictions) in a variety of cases, by relating the logarithm of the initial Beilinson-Kato element $\mathbf{BK}_1$ to the square of the logarithm of a suitable Heegner point. In Appendix A, we give a proof of Theorem 2.10.

We remark that under the additional hypothesis that $E(\mathbb{Q}_p)[p] = 0$, a much more precise version of Theorem 2.10 is readily available (Theorem 2.11, previously proved by the author in [Büy11]). As we explain in Remark 2.12, this hypothesis holds true in all cases that have not been considered in [BD15, Ven15] (but also covers the case of [Ven15] in full if $p > 7$) and it is expected to hold true for all sufficiently large p. The reader who is content with these set of results may safely skip Appendix A.

2. Selmer structures and Kolyvagin systems

In this section, we recall some basic notions and constructions from [MR04] and their Λ-adic versions from [Büy11]. We also state one of our main results in this article (Theorem 2.10), which is key to our proof of Perrin-Riou's conjecture.

2.1. Selmer structures.

In this work, we shall consider the following Selmer structures (in the sense of [MR04, Definition 2.1.1]) on the Galois module $\mathbb{T}$ and its various quotients.

Definition 2.1. Recall the Galois representations $\mathbb{T}$ and its quotients T_α.
i) Let $\mathcal{F}_\Lambda$ denote the *canonical Selmer structure* on $\mathbb{T}$ defined by setting $H^1_{\mathcal{F}_\Lambda}(\mathbb{Q}_\ell, \mathbb{T}) = H^1(\mathbb{Q}_\ell, \mathbb{T})$ for every rational prime ℓ.
ii) For every $\alpha \in \mathbb{Z}^+$, we define the *α-canonical Selmer structure* $\mathcal{F}_\alpha$ on T_α by setting

- $H^1_{\mathcal{F}_\alpha}(\mathbb{Q}_\ell, T_\alpha) = \ker\left(H^1(\mathbb{Q}_\ell, T_\alpha) \to H^1(\mathbb{Q}_\ell^{\text{ur}}/\mathbb{Q}_\ell, T_\alpha \otimes \mathbb{Q}_p)\right)$, if $\ell \nmid p$;
- $H^1_{\mathcal{F}_\alpha}(\mathbb{Q}_p, T_\alpha) = H^1(\mathbb{Q}_p, T_\alpha)$.

We every pair $k, \alpha \in \mathbb{Z}^+$, we therefore obtain the Selmer structures $\mathcal{F}_\Lambda$ and $\mathcal{F}_\beta$ $(\beta \geq \alpha)$ on $T_{k,\alpha}$ by propagating (in the sense of [MR04, Example 1.1.2]) $\mathcal{F}_\Lambda$ and $\mathcal{F}_\beta$, respectively via the canonical maps $\mathbb{T} \twoheadrightarrow T_{k,\alpha}$ and $T_\beta \twoheadrightarrow T_{k,\alpha}$. In place of $\mathcal{F}_1$, we shall write $\mathcal{F}_{\text{can}}$ for an easier comparison of our discussion here with [MR04].

In the notation of [MR04, Definition 2.1.1] we have $\Sigma(\mathcal{F}) = S$ for each of the Selmer structures above.

Remark 2.2. Under our hypothesis that p does not divide $\text{ord}_\ell(j(E))$ whenever $\ell \mid N$ is a prime of split multiplicative reduction, it follows from [Büy11, §2.3.1] that the local conditions determined by the Selmer structures $\mathcal{F}_\Lambda$ and $\mathcal{F}_\beta$ on the Galois modules T_α and $T_{k,\alpha}$ $(k, \alpha, \beta \in \mathbb{Z}^+$ and $\alpha \leq \beta)$ all agree (and they all equal to the unramified submodule $H^1_{\text{ur}}(\mathbb{Q}_\ell, T_{k,\alpha}) = \ker\left(H^1(\mathbb{Q}_\ell, T_{k,\alpha}) \to H^1(\mathbb{Q}_\ell^{\text{ur}}, T_{k,\alpha})\right)$).

When $E(\mathbb{Q}_p)[p] = 0$, Selmer structures $\mathcal{F}_\beta$ (for $\beta \geq \alpha$) and $\mathcal{F}_\Lambda$ also induce at p the same Selmer local condition for $T_{k,\alpha}$. In this case, $H^1_{\mathcal{F}_?}(\mathbb{Q}_p, T_{k,\alpha}) = H^1(\mathbb{Q}_p, T_{k,\alpha})$ for

$? = \Lambda, \beta \geq \alpha$. Even when $E(\mathbb{Q}_p)$ need not vanish, we have by [MR04, Lemma 3.7.1] a map

$$\varpi_{k,k'} : H^1_{\mathcal{F}_\alpha}(\mathbb{Q}_p, T_{k,\alpha}) \longrightarrow H^1_{\mathcal{F}_\alpha}(\mathbb{Q}_p, T_{k',\alpha})[p^k]$$

for $k' \geq k$, induced from multiplication by $p^{k'-k}$. However, for $\beta \geq \alpha$ the analogous map

$$\gamma_{\alpha,\beta} : H^1(\mathbb{Q}_p, T_{k,\alpha}) \longrightarrow H^1(\mathbb{Q}_p, T_{k,\beta})[(\gamma-1)^\alpha]$$

induced by the multiplication by $(\gamma-1)^{\beta-\alpha}$ does not necessarily map $H^1_{\mathcal{F}_\alpha}(\mathbb{Q}_p, T_{k,\alpha})$ to $H^1_{\mathcal{F}_\beta}(\mathbb{Q}_p, T_{k,\beta})[(\gamma-1)^\alpha]$. However, it turns out that we may control this failure to a reasonable degree; see Section A.1.1 below.

Besides those appeared in definitions of the canonical Selmer structures we have introduced above, we will also be interested in the following local conditions away from S, at certain *Kolyvagin primes*. The Selmer structures obtained suitably modifying the canonical Selmer structures of Definition 2.1 at these primes are central to our considerations.

Definition 2.3. Given positive integers α and k, we let $\mathcal{P}_{k,\alpha}$ (respectively, $\mathcal{P}_j$) denote the set of *Kolyvagin primes* for $T_{k,\alpha}$, as introduced in [Büy11, Section 2.4]. We define the set $\mathcal{N}_{k,m}$ to be the set of square-free products of primes in $\mathcal{P}_{k,\alpha}$; and the set $\mathcal{N}_j$ is defined likewise.

Given $\ell \in \mathcal{P}_{k,\alpha}$, we define the *transverse submodule* by setting

$$H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{k,\alpha}) := \ker\left(H^1(\mathbb{Q}_\ell, T_{k,\alpha}) \to H^1(\mathbb{Q}_\ell(\boldsymbol{\mu}_\ell), T_{k,\alpha})\right) .$$

For a positive integer $n \in \mathcal{N}_{k,\alpha}$, we define the Selmer structure $\mathcal{F}_?(n)$ (with $? = \alpha, \Lambda$) by setting

- $\Sigma(\mathcal{F}_?(n)) = S \cup \{\ell \mid n\}$,
- $H^1_{\mathcal{F}_?(n)}(\mathbb{Q}_\ell, T_{k,\alpha}) = H^1_{\mathcal{F}_?}(\mathbb{Q}_\ell, T_{k,\alpha})$ for $\ell \in S$,
- $H^1_{\mathcal{F}_?(n)}(\mathbb{Q}_\ell, T_{k,\alpha}) = H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{k,\alpha})$ for $\ell \mid n$.

Definition 2.4. For a rational prime ℓ, there is the perfect local Tate pairing

$$\langle\, , \,\rangle_{\ell,\mathrm{Tate}} : H^1(\mathbb{Q}_\ell, X) \times H^1(\mathbb{Q}_\ell, X^*) \to H^2(\mathbb{Q}_\ell, \boldsymbol{\mu}_{p^\infty}) \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p,$$

where. For a Selmer structure $\mathcal{F}$ on X, define the *dual Selmer structure* $\mathcal{F}^*$ on X^* by setting $H^1_{\mathcal{F}^*}(\mathbb{Q}_\ell, X^*) := H^1_{\mathcal{F}}(\mathbb{Q}_\ell, X)^\perp$, the orthogonal complement of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, X)$ with respect to the local Tate pairing.

Remark 2.5. It follows from [MR04, Proposition 1.3.2] (which applies thanks to [Büy11, Remark 2.15]) that the transverse condition is self-dual: $H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T^*_{k,\alpha}) = H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{k,\alpha})^\perp$. In particular, $\mathcal{F}_?(n)^* = \mathcal{F}^*_?(n)$ for every $n \in \mathcal{N}_{k,\alpha}$.

Definition 2.6. If $\mathcal{F}$ is a Selmer structure on X, we define the *Selmer module* by setting

$$H^1_{\mathcal{F}}(\mathbb{Q}, X) := \ker\left(H^1(G_{\mathbb{Q},\Sigma(\mathcal{F})}, X) \longrightarrow \bigoplus_{\ell\in\Sigma(\mathcal{F})} H^1(F_\ell, X)/H^1_{\mathcal{F}}(F_\ell, X)\right) .$$

Definition 2.7. We say that an integer $n \in \mathcal{N}_{k,\alpha}$ is a core vertex for the representation $T_{k,\alpha}$ if $H^1_{F_\alpha(n)}(\mathbb{Q}, T_{k,\alpha})$ is a cyclic $R_{k,\alpha}$-module.

Remark 2.8. Given positive integers k and α as above, it follows from the discussion in [MR04, Section 4.1] that there are core vertices $n \in \mathcal{N}_{k,\alpha}$ for the pair $(\mathcal{F}_{\rm can}, \overline{T})$. Furthermore, when n is a core vertex for $(\mathcal{F}_{\rm can}, \overline{T})$, the quantity $\chi_n(T) := \dim_{\mathbb{F}_p} H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, \overline{T})$ is independent of the choice of n. This common value $\chi(T) = \chi_n(T)$ is called the *core Selmer rank* of T. In fact, it follows from [MR04, Theorem 5.2.15] that $\chi(T) = 1$ in our set up.

It is also an easy consequence of [MR04, Theorem 5.2.15] that $H^1_{F_\alpha(n)^*}(\mathbb{Q}, T^*_{k,\alpha}) = 0$ at a core vertex n; see also the displayed equality (A6) below and its proof.

2.2. **Module of Kolyvagin systems.** We recall the definition of Kolyvagin systems for artinian and pro-artinian rings. Let $G_n = \otimes_{\ell | n} \mathbb{F}_\ell^\times$.

Definition 2.9. A Kolyvagin system for the Selmer structure $\mathcal{F}_\alpha$ on $T_{k,\alpha}$ is a collection $\{\kappa_n\}_{n \in \mathcal{N}_{k,m}}$ with the following properties:
i) $\kappa_n \in H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, T_{k,\alpha}) \otimes G_n$.
ii) For $n\ell \in \mathcal{N}_{k,m}$, we have $(\phi_\ell^{\rm fs} \otimes \mathbf{1})\,(\mathrm{res}_\ell(\kappa)) = \mathrm{res}_p^s(\kappa_{n\ell})$, where the equality takes place in the quotient $H^1_s(\mathbb{Q}_\ell, T_{k,\alpha}) := H^1(\mathbb{Q}_\ell, T_{k,\alpha})/H^1_{\rm ur}(\mathbb{Q}_\ell, T_{k,\alpha})$; the map res_ℓ^s is the compositum of the arrows

$$H^1(\mathbb{Q}, T_{k,\alpha}) \longrightarrow H^1(\mathbb{Q}_\ell, T_{k,\alpha}) \longrightarrow H^1_{\rm ur}(\mathbb{Q}_\ell, T_{k,\alpha})\,,$$

$\phi_\ell^{\rm fs}$ is the *finite-to-singular comparison map* of [MR04, Definition 1.2.2]; see also [Büy11, Lemma 2.19] and finally, $\mathbf{1} : G_n \to G_{n\ell}$ is the obvious map.

The collection of Kolyvagin systems for the Selmer structure $\mathcal{F}_\alpha$ on $T_{k,\alpha}$ is denoted by $\mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_{k+\alpha})$. This set comes equipped with a natural $R_{k,\alpha}$-module structure. Using the Selmer structure $\mathcal{F}_\Lambda$ in place of $\mathcal{F}_\alpha$ we also define $\mathbf{KS}(\mathcal{F}_\Lambda, T_{k,\alpha}, \mathcal{P}_{k+\alpha})$, which naturally is an $R_{k,\alpha}$-submodule of $\mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_{k+\alpha})$.

We may finally define

$$\mathbf{KS}(\mathbb{T}) := \varprojlim_{k,\alpha} \left(\varinjlim_{j \geq k+\alpha} \mathbf{KS}(\mathcal{F}_\Lambda, T_{k,\alpha}, \mathcal{P}_j) \right) \subset \varprojlim_{k,\alpha} \left(\varinjlim_{j \geq k+\alpha} \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \right).$$

Our main result on the structure of this object is as follows. This result is crucial for our proof of Perrin-Riou's conjecture.

Theorem 2.10. *Suppose that E is an elliptic curve such that the residual representation*

$$\overline{\rho}_E : G_{\mathbb{Q},S} \longrightarrow \mathrm{Aut}(E[p])$$

is surjective. Assume further that p does not divide $\mathrm{ord}_\ell(j(E))$ whenever $\ell \mid N$ is a prime of split multiplicative reduction. Then,

i) *the Λ-module $\mathbf{KS}(\mathbb{T})$ of Λ-adic Kolyvagin systems contains a free Λ-module of rank one with finite index;*
ii) *there exists a Λ-adic Kolyvagin system $\boldsymbol{\kappa} \in \mathbf{KS}(\mathbb{T})$ with the property that $\mathrm{pr}_0(\boldsymbol{\kappa}) \in \mathbf{KS}(T)$ is non-zero.*

The proof of this theorem will be given in Section A.1.2, which is based on the arguments in [Büy11] and the local analysis we shall carry out in Section 1.1. We note that loc. cit., the author in [Büy11, Theorem 3.23] has already given a proof of the following statement under more restrictive hypothesis (which is, however, more precise when it applies):

Theorem 2.11. *In addition to the hypotheses of Theorem 2.10, suppose that* $E(\mathbb{Q}_p)[p] = 0$*. Then the natural map* $\mathbf{KS}(\mathbb{T}) \to \mathbf{KS}(\overline{T})$ *is surjective, the* Λ*-module* $\mathbf{KS}(\mathbb{T})$ *is free of rank one and its generated by any* Λ*-adic Kolyvagin system whose projection to* $\mathbf{KS}(\overline{T})$ *is non-zero.*

In the set up of Theorem 2.11, there should be no confusion with the notation $\mathbf{KS}(\overline{T})$ (since we have not specified the Selmer structure on $\overline{T}$) thanks to Remark 2.2.

Remark 2.12. The requirement that $E(\mathbb{Q}_p)[p] = 0$ in Theorem 2.11 is the condition that the prime p be *non-anomalous* in the sense of Mazur [Maz72]. Mazur has explained that given an elliptic curve E these primes should be sparse.

David and Weston in [DW08] present a heuristic reasoning why this should be the case and they conjecture that given an elliptic curve E, there are at most finitely many anomalous primes. If $E(\mathbb{Q})_{\mathrm{tor}}$ is non-trivial, for example, it is easy to verify this conjecture; see Proposition 2.1 in loc. cit. When $p > 5$ is a prime of good reduction for E, one may easily check that $E(\mathbb{Q}_p)[p] \neq 0 \implies a_p(E) = 1$ and in particular, when $p > 5$ is a prime of supersingular reduction for E, it is non-anomalous. Likewise, when p is a prime of non-split-multiplicative reduction or when E has split-multiplicative reduction at p and $p > 7$, one may check that $E(\mathbb{Q}_p)$ does not have p-torsion using Tate uniformization.

In short, for primes $p > 5$ at which

- either E has supersingular reduction,
- or non-split-multiplicative reduction,
- or split-multiplicative reduction with $p > 7$,
- or good ordinary reduction with $a_p(E) \neq 1$,
- or for elliptic curves which possess a non-trivial $\mathbb{Q}$-rational torsion,

Theorem 2.11 is sufficient for our purposes. The reader who only has an eye towards the previously untouched cases of Perrin-Riou's conjecture may therefore be satisfied with the contents of Sections 3 and Section 4 alone and choose to skip the technical details in Appendix A (which are designed to upgrade Theorem 2.11 to Theorem 2.10 so as to cover the case when p might be an anomalous prime).

We briefly explain the proof of Theorem 2.11 (which consists of four steps) and indicate what further needs to be carried over in order to deduce Theorem 2.10.

1. One shows that a core vertex $n \in \mathcal{N}_j$ for the Selmer structure $\mathcal{F}_\alpha$ on $\overline{T}$ is also a core vertex for the Selmer structure $\mathcal{F}_\alpha$ on the quotient $T_{k,\alpha}$. This combined with an argument of Mazur and Rubin in [MR04, Section 4.1] supplies us with a wealth of core vertices in any of the sets $\mathcal{N}_j$.

2. For each core vertex $n \in \mathcal{N}_j$, one then proves that the natural map

$$\mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \longrightarrow H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, T_{k,\alpha}) \tag{2.1}$$

is injective.

3. One further proves that the map (2.1) is surjective, therefore an isomorphism.

4. As the final step, one verifies that the maps

$$\mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \longrightarrow \mathbf{KS}(\mathcal{F}_{\alpha'}, T_{k',\alpha'}, \mathcal{P}_j)$$

for $\alpha \geq \alpha'$, $k \geq k'$ and $j \geq k+\alpha$ are surjective. The key point in doing so is the following *patcing* diagrams,

$$\begin{tikzcd}
\mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \arrow[r] \arrow[dr, "\pi_{\alpha,\alpha'}"'] & \mathbf{KS}(\mathcal{F}_{\alpha'}, T_{k,\alpha'}, \mathcal{P}_j) \arrow[d, "\gamma_{\alpha',\alpha}"] \\
& \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j)[(\gamma-1)^\alpha]
\end{tikzcd} \tag{2.2}$$

(where $\pi_{\alpha,\alpha'}$ is the multiplication by $(\gamma-1)^{\alpha-\alpha'}$), and considering the multiplication-by-p-power maps in similar manner,

$$\begin{tikzcd}
\mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \arrow[r] \arrow[dr] & \mathbf{KS}(\mathcal{F}_\alpha, T_{k',\alpha}, \mathcal{P}_j) \arrow[d] \\
& \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j)
\end{tikzcd} \tag{2.3}$$

where in each diagram one makes use of the Steps 2 and 3 in order to verify that the diagonal map is a surjection, whereas the vertical map is an isomorphism. This concludes the proof that the horizontal maps are surjections.

The 2nd and the 3rd steps formally follow from Step 1, as in [Büy11, Section 3.1.2 and 3.1.3]; and Step 1 will go through easily as a consequence of our local analysis in Appendix A even when $E(\mathbb{Q}_p)[p] \neq 0$. The main difficulty lies in the patching argument: One may in fact show that the strategy above (which relies on patching diagrams) is bound to fail as is. However, we will see in Section A.1.2 that we may deal with this matter by considering a slightly smaller collection of Kolyvagin systems.

3. Proof of Perrin-Riou's conjecture

3.1. **Preliminaries.** We first explain the proof of the "only if" part of Perrin-Riou's conjecture (Theorem 1.3) (which should be already well-known to the experts prior to this work). Its proof involves some of the reduction steps we rely on for the proof of the "if" part of the conjecture and we pin these down also in this portion of our article.

Proof of Theorem 1.3. Suppose first that $\mathrm{res}_p^s(\mathbf{BK}_1) \neq 0$, where res_p^s is the singular projection given as the compositum of the arrows

$$H^1(\mathbb{Q}, T) \to H^1(\mathbb{Q}_p, T) \twoheadrightarrow H^1(\mathbb{Q}_p, T)/H^1_f(\mathbb{Q}_p, T) =: H^1_s(\mathbb{Q}_p, T)\,.$$

Kato's explicit reciprocity law shows that $r_{\mathrm{an}} = 0$. We may therefore assume without loss of generality that $\mathbf{BK}_1$ is crystalline at p, namely that $\mathbf{BK}_1 \in H^1_f(\mathbb{Q}, T)$.

Since $\mathbf{BK}_1 \neq 0$, it follows from [MR04, Corollary 5.2.13(i)] that $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, T^*)$ is finite. Recall that $\mathcal{F}_{\mathrm{str}}$ denotes the Selmer structure on T given by

- $H_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}_\ell, T) = H_{\mathcal{F}}(\mathbb{Q}_\ell, T)$, if $\ell \neq p$,
- $H_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}_p, T) = 0$.

We contend to verify that $H^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T) = 0$. Assume on the contrary that $H^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T)$ is non-trivial. Since module $H^1(G_{\mathbb{Q},S}, T)$ is torsion free under our running hypothesis on the image of $\overline{\rho}_E$, this amounts to saying that $H^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T)$ has positive rank.

Recall further that the propagation of the Selmer structure $\mathcal{F}_{\mathrm{str}}$ to the quotients T/p^nT (in the sense of [MR04]) is still denoted by $\mathcal{F}_{\mathrm{str}}$. Recall that $T^* \cong E[p^\infty]$ and note for any positive integer n that we may identify the quotient T/p^nT with $E[p^n]$. By [MR04, Lemma 3.7.1], we have an injection

$$H_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q},T)/p^nH_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q},T) \hookrightarrow H_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q},T/p^nT) = H_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q},E[p^n])$$

induced from the projection $T \to T/p^nT$. This shows that

$$\text{length}_{\mathbb{Z}_p}\left(H_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q},E[p^n])\right) \geq n. \tag{3.1}$$

As above, we let $\mathcal{F}_{\mathrm{can}} = \mathcal{F}_1$ denote the canonical Selmer structure on T, given by

- $H_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell,T) = H_{\mathcal{F}}(\mathbb{Q}_\ell,T)$, if $\ell \neq p$,
- $H_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_p,T) = H^1(\mathbb{Q}_p,T)$.

It follows from [Rub00, Lemma I.3.8(i)] (together with the discussion in [MR04, §6.2]) that we have an inclusion

$$H_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}_\ell,E[p^n]) \subset H_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}_\ell,E[p^n])$$

for every ℓ. Here, $E[p^n]$ is identified with T on the left and with $T^*[p^n]$ on the right and also viewed as a submodule of $T \otimes \mathbb{Q}_p/\mathbb{Z}_p$). Furthermore, the index of $H_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}_\ell,E[p^n])$ within $H_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}_\ell,E[p^n])$ is bounded independently of n (in fact, bounded by the order of $E(\mathbb{Q}_p)[p^\infty]$). This in turn shows that together with (3.1) that

$$\text{length}_{\mathbb{Z}_p}\left(H_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q},E[p^n])\right) \geq n. \tag{3.2}$$

However, $H_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q},E[p^\infty])$ is finite and therefore the length of

$$H_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q},E[p^n]) \cong H_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q},E[p^\infty])[p^n]$$

(where the isomorphism is thanks to [MR04, Lemma 3.5.3], which holds true here owing to our assumption on the image of $\overline{\rho}_E$) is bounded independently of n. This contradicts (3.2) and shows that $H^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q},T) = 0$. Thence, the map

$$\mathrm{res}_p : H^1_f(\mathbb{Q},T) \longrightarrow H^1_f(\mathbb{Q}_p,T)$$

is injective. The module $H^1_f(\mathbb{Q}_p,T)$ is free of rank one and we conclude that $H^1_f(\mathbb{Q},T)$ has also rank one. When we are in the situation of (a) or (c), the proof now follows from the converse of the Kolyvagin-Gross-Zagier theorem proved in [Ski14a, SZ14]. In the situation of (b), it follows from the works Kobayashi [Kob13] and Wan [Wan14] that a suitable Heegner point $P \in E(\mathbb{Q})$ is non-trivial. This in turn implies (relying on the classical Gross-Zagier formula) that $r_{\mathrm{an}} = 1$, as desired. □

Proposition 3.1. *If $r_{\mathrm{an}} \leq 1$, then $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q},T^*)$ is finite.*

Proof. If $r_{\mathrm{an}} = 0$, it follows that $\mathrm{res}^s_p(\mathbf{BK})$ and in particular that $\mathbf{BK}_1 \neq 0$. The conclusion of the proposition follows from [MR04, Corollary 5.2.13(i)]. Suppose now that $r_{\mathrm{an}} = 1$. In this case,

$$\begin{aligned} H^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q},T) &= \ker(H^1_f(\mathbb{Q},T) \longrightarrow H^1_f(\mathbb{Q}_p,T)) \\ &= \ker\left(E(\mathbb{Q})\,\widehat{\otimes}\,\mathbb{Z}_p \longrightarrow E(\mathbb{Q}_p)\,\widehat{\otimes}\,\mathbb{Z}_p\right) = 0 \end{aligned}$$

where the second equality follows from the finiteness of the Tate-Shafarevich group [Kol90] and the final equality by the Gross-Zagier theorem. As in the proof of Theorem 1.3, we may use this conclusion to deduce that the order of $H_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q},T^*)[p^n] \cong H_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q},E[p^n])$ is bounded independently of n. The proof follows. □

Corollary 3.2. *If $r_{\mathrm{an}} \leq 1$, then for every non-zero $\{\kappa_n\} \in \mathbf{KS}(T)$, the initial term κ_1 of the Kolyvagin system $\{\kappa_n\}$ is non-vanishing.*

Proof. This follows from [MR04, Corollary 5.2.13(i)]. □

3.2. **Main conjectures.** We recall in this section Kato's formulation of the Iwasawa main conjecture for the elliptic curve E and record results towards this conjecture. It follows from Kato's reciprocity laws and Rohrlich's [Roh84] non-vanishing theorems that the class $\mathbb{BK}_1$ is non-vanishing and the Λ-module $H^1(\mathbb{Q},\mathbb{T})$ is of rank one (as it was predicted by the weak Leopoldt conjecture for E).

For two ideals $I, J \subset \Lambda$, we write $I \doteqdot J$ to mean that $I = p^e J$ for some integer e.

Conjecture 3.3. $\mathrm{char}\left(H^1_{\mathcal{F}^*_\Lambda}(\mathbb{Q},\mathbb{T}^*)^\vee\right) \doteqdot \mathrm{char}\left(H^1(\mathbb{Q},\mathbb{T})/\Lambda\cdot\mathbb{BK}_1\right).$

This assertion is equivalent (via Kato's reciprocity laws, and up to powers of p) to the classical formulation of Iwasawa main conjecture for E.

Theorem 3.4. *In the setting of Theorem 1.2, Conjecture 3.3 holds true in the following cases:*

(a) *E has good ordinary reduction at p.*
(b) *E has good supersingular reduction at p and N is square-free.*
(c) *E has multiplicative reduction at p and there exists a prime $\ell \,||\, N$ such that there $\overline{\rho}_E$ is ramified at ℓ.*

Proof. In the setting of (a), see the works of Kato and Skinner-Urban [Kat04, SU14] (as well as the enhancement of the latter due to Wan [Wan15], that lifts certain local hypothesis of Skinner and Urban) and in the situation of (b), the works of Kobayashi and Wan [Kob03, Wan14]. In the setting of (c), the works of Skinner and Kato [Ski14b, Kat04] yields the desired conclusion. Note that Kato has stated his divisibility result towards Conjecture 3.3 only when E has good ordinary reduction at p. We refer the reader to [Rub98] for the slightly more general version of his theorem required to treat the non-crystalline semistable case as well. □

3.3. **The Λ-adic Beilinson-Kato Kolyvagin system and the conclusion of the proof.** We are now ready to put together all the discussion above and give a proof of our main result.

Proposition 3.5. *Suppose that E is an elliptic curve such that the residual representation $\overline{\rho}_E$ is surjective. Assume further that p does not divide $\mathrm{ord}_\ell(j(E))$ whenever $\ell \mid N$ is a prime of split multiplicative reduction.*
i) *Let $\boldsymbol{\kappa} \in \mathbf{KS}(\mathbb{T})$ be a generator of any free submodule of $\mathbf{KS}(\mathbb{T})$ that has finite index in $\mathbf{KS}(\mathbb{T})$. (The existence of such a submodule is guaranteed by Theorem 2.10.) Then there exists $c \in \mathbb{Z}_p$ so that $\mathbb{BK} = c\cdot\boldsymbol{\kappa}$.*
ii) *Let $\kappa_1 \in H^1(\mathbb{Q},\mathbb{T})$ denote the initial term of $\boldsymbol{\kappa}$ and suppose that $r_{\mathrm{an}} \leq 1$. Then the image $\mathrm{pr}_0(\kappa_1) \in H^1(G_{\mathbb{Q},S},T)$ of κ_1 under the natural projection map is non-trivial.*

Proof. It follows from Theorem 2.10 and Rohrlich's theorem (which guarantees the non-triviality of $\mathbb{BK}_1$ and therefore also the fact that Λ-adic Kolyvagin system $\mathbb{BK}$ is non-torsion) that one may find $f \in \Lambda\backslash\{0\}$ and $t \in \mathbb{Z}_p$ with the property that $t\cdot\mathbb{BK} = f\cdot\boldsymbol{\kappa}$, hence also that $t\cdot\mathbb{BK}_1 = f\cdot\kappa_1$.

On the other hand, [MR04, Theorem 5.3.10(i) and Remark 5.3.11] shows (since the Λ-module $H^1(\mathbb{Q},\mathbb{T})$ has rank one) that

$$\mathrm{char}\left(H^1_{\mathcal{F}^*_\Lambda}(\mathbb{Q},\mathbb{T}^*)^\vee\right) \Big| \,\mathrm{char}\left(H^1(\mathbb{Q},\mathbb{T})/\Lambda\cdot\kappa_1\right) . \tag{3.3}$$

Furthermore,

$$\operatorname{char}\left(H^1_{\mathcal{F}^*_\Lambda}(\mathbb{Q},\mathbb{T}^*)^\vee\right) \doteq t\cdot \operatorname{char}\left(H^1(\mathbb{Q},\mathbb{T})/\Lambda\cdot \mathbb{BK}_1\right) = f\cdot \operatorname{char}\left(H^1(\mathbb{Q},\mathbb{T})/\Lambda\cdot \kappa_1\right) \tag{3.4}$$

where the first equality (up to powers of p) is Theorem 3.4. Putting (3.3) and (3.4) together we conclude with i).

Since $\boldsymbol{\kappa}$ generates a free submodule of $\mathbf{KS}(\mathbb{T})$ of finite index, it follows using Theorem 2.10(ii) that $\mathrm{pr}_0(\boldsymbol{\kappa}) \in \mathbf{KS}(T)$ is non-trivial. ii) follows from Corollary 3.2. □

Proof of Theorem 1.2 (modulo Theorem 2.10). For $c \in \mathbb{Z}_p$, $\boldsymbol{\kappa}$ and κ_1 as in the statement of Proposition 3.5 we have

$$\mathbf{BK}_1 = \mathrm{pr}_0(\mathbb{BK}_1) = c\cdot \mathrm{pr}_0(\kappa_1) \neq 0\,. \tag{3.5}$$

As explained in [Büy14, Proposition 3.11], the non-vanishing of the class $\mathrm{res}_p(\mathbf{BK}_1)$ follows from (3.5). □

We therefore verified the validity of Theorem 1.2 (without the need of the full strength of Theorem 2.10 and the material in Appendix A) in the following additional hypothesis:

- E has supersingular reduction at p, or
- E has non-split-multiplicative reduction at p, or
- E has split-multiplicative reduction at p and $p > 7$, or
- E has good ordinary reduction at p and $a_p(E) \neq 1$, or
- $E(\mathbb{Q})_{\mathrm{tor}}$ is non-trivial.

Note that all these five conditions ensure that $E(\mathbb{Q}_p)[p] = 0$.

4. Logarithms of Heegner points and Beilinson-Kato classes

As before, we suppose that E is an elliptic curve such that the residual representation $\overline{\rho}_E$ is surjective. Assume further that p does not divide $\mathrm{ord}_\ell(j(E))$ whenever $\ell \mid N$ is a prime of split multiplicative reduction. Assume also that one of the following conditions hold true.

(a) E has good ordinary reduction at p.
(b) E has good supersingular reduction at p and N is square-free.
(c) E has multiplicative reduction at p and there exists a prime $\ell \mid\mid N$ such that there $\overline{\rho}_E$ is ramified at ℓ.

With this set up, we will be able refine the conclusion of Theorem 1.2 in a variety of cases and deduce that the square of the logarithm of a suitable Heegner point agrees with the logarithm of the Beilinson-Kato class $\mathbf{BK}_1$ up to an explicit non-zero algebraic factor. In these cases, we will therefore justify some of the hypothetical conclusions in [PR93, §3.3.3].

We fix a Weierstrass minimal model $\mathcal{E}_{/\mathbb{Z}}$ of E. Let $\omega_{\mathcal{E}}$ be a Néron differential that is normalized as in [PR95, §3.4] and is such that we have $\Omega_E^+ := \int_{E(\mathbb{C})^+}\omega_{\mathcal{E}} > 0$ for the real period Ω_E^+. Suppose till the end of this Introduction that $L(E,s)$ has a simple zero at $s=1$. In this situation, $E(\mathbb{Q})$ has rank one and the Néron-Tate height $\langle P,P\rangle_\infty$ of any generator P of the free part of $E(\mathbb{Q})$ is related via the Gross-Zagier theorem to the first derivative of $L(E,s)$ at $s=1$:

$$\frac{L'(E,1)}{\Omega_E^+} = C(E)\cdot \langle P,P\rangle_\infty \tag{4.1}$$

with $C(E) \in \mathbb{Q}^\times$.

Let $D_{\rm cris}(V)$ be the crystalline Dieudonné module of V and we define the element $\omega_{\rm cris} \in D_{\rm cris}(V)$ as that corresponds $\omega_{\mathcal{E}}$ under the comparison isomorphism. We let $\mathcal{H} \subset \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ denote Perrin-Riou's ring of distributions. Let

$$\mathfrak{Log}_V : H^1(\mathbb{Q}_p, \mathbb{T}) \otimes_\Lambda \mathcal{H} \longrightarrow \mathcal{H} \otimes D_{\rm cris}(V)$$

be Perrin-Riou's extended logarithm map and write $\boldsymbol{\mathcal{L}}_{\mathbf{BK}}$ as a shorthand for the element $\mathfrak{Log}_V\,(\mathrm{res}_p(\mathbb{BK}_1)) \in \mathcal{H} \otimes D_{\rm cris}(V)$. We also let

$$\log_V : H^1_f(\mathbb{Q}_p, V) \xrightarrow{\sim} D_{\rm dR}(V)/\mathrm{Fil}^0\, D_{\rm dR}(V)$$

denote Bloch-Kato logarithm.

Suppose first that E has good reduction at p. In this case, $D_{\rm cris}(V)$ is a two dimensional vector space. Let $\alpha, \beta \in \overline{\mathbb{Q}}_p$ be the eigenvalues of the crystalline Frobenius φ acting on $D_{\rm cris}(V)$. Extending the base field if necessary, let D_α and D_β denote corresponding eigenspaces. Set $\omega_{\rm cris} = \omega_\alpha + \omega_\beta$ with $\omega_\alpha \in D_\alpha$ and $\omega_\beta \in D_\beta$. On projecting $\boldsymbol{\mathcal{L}}_{\mathbf{BK}}$ onto either of these vector spaces we obtain $\boldsymbol{\mathcal{L}}_{\mathbf{BK},?} \in \mathcal{H}$ (so that $\boldsymbol{\mathcal{L}}_{\mathbf{BK},?} \cdot \omega_?$ is the projection of $\mathcal{L}_{BK}$ onto $\mathcal{H} \otimes D_?$) for $? = \alpha, \beta$.

Theorem 4.1. *Suppose that E has good supersingular reduction at p and N is square-free. For* $? = \alpha, \beta$,

(i) *the Amice transform of the distribution* $\boldsymbol{\mathcal{L}}_{\mathbf{BK},?}$ *is the Manin-Vishik, Amice-Velu p-adic L-function* $L_{p,?}(E/\mathbb{Q}, s)$ *associated to the pair* $(E, D_?)$*;*
(ii) *when* $r_{\rm an} = 1$*, one of the two p-adic L-functions vanishes at* $s = 1$ *to degree* 1*;*
(iii) *still when* $r_{\rm an} = 1$*, at least one of the associated p-adic height pairings* $\langle\, ,\, \rangle_{p,?}$ *is non-degenerate,*
(iv) $\log_V\,(\mathrm{res}_p(\mathbf{BK}_1)) = (1 - 1/\alpha)(1 - 1/\beta) \cdot C(E) \cdot \log_V\,(\mathrm{res}_p(P))^2\,.$

Note that the quantity $(1 - 1/\alpha)(1 - 1/\beta) = (1 + 1/p)$ in fact belongs to $\mathbb{Q}^\times$.

Proof. The first assertion is due to Kato[2], see [Kat04]. It follows from [PR93, Proposition 2.2.2] and Theorem 1.2 that $\boldsymbol{\mathcal{L}}'_{\mathbf{BK}}(\mathbb{1}) \neq 0$. Thence, for at least one of α or β (say it is α) we have

$$\mathrm{ord}_{s=1} L_{p,\alpha}(E/\mathbb{Q}, s) = 1\,.$$

This completes the proof of the second assertion. The third follows from the p-adic Gross-Zagier formula of Kobayashi in [Kob13] and the last portion from the discussion in [PR93, §3.3.3] combined with Kobayashi's p-adic Gross-Zagier formula. □

Remark 4.2. The content of Theorem 4.1 justifies some of the hypothetical statements in [PR93, §3.3.3] at a supersingular prime p. We note that the full strength of Kobayashi's work [Kob13] actually contains the results of this theorem; and we merely point out here that the knowledge alone of a p-adic Gross-Zagier formula for *both* p-adic L-functions associated to E along with our Theorem 1.2 yields the non-degeneracy of one of the height pairings and verifies (as in Theorem 4.1(iv)) Perrin-Riou's prediction.

Remark 4.3. Much of what we have recorded above for a supersingular prime p applies verbatim for a good ordinary prime as well. Suppose that α is the root of the Hecke

[2] This is accomplished after suitably normalizing $\mathbb{BK}_1$ and throughout this work, we implicitly assume that we have done so.

polynomial which is a p-adic unit, so that $v_p(\beta) = 1$. In this case, we again have two p-adic L-functions: The projection of $\mathcal{L}_{\mathbf{BK}}$ to D_α yields the Mazur-Tate-Teitelbaum p-adic L-function $L_{p,\alpha}(E/\mathbb{Q}, s)$, whereas its projection to D_β agrees[3] with the *critical slope* p-adic L-function $L_{p,\beta}(E/\mathbb{Q}, s)$ of Bellaïche and Pollack-Stevens. The analogous statements to those in Theorem 4.1 therefore reduces to check that one of the following holds true:

a) There exists a p-adic Gross-Zagier formula for the critical slope p-adic L-function $L_{p,\beta}(E/\mathbb{Q}, s)$.
b) $\mathrm{ord}_{s=1} L_{p,\beta}(f, s) \geq \mathrm{ord}_{s=1} L_{p,\alpha}(f, s)$.

We suspect that the latter statement may be studied through a *critical slope* main conjecture and its relation with the ordinary main conjecture. We will pursue this direction in a future work.

Suppose now that E has non-split-multiplicative reduction at p. In this case, $D_{\mathrm{cris}}(V)$ is one-dimensional and we have $\mathcal{L}_{\mathbf{BK}} = \mathcal{L}_{\mathrm{MTT}} \cdot \omega_{\mathrm{cris}}$, where $\mathcal{L}_{\mathrm{MTT}} \in \Lambda$ is the Mazur-Tate-Teitelbaum measure. The following is a consequence of the p-adic Gross-Zagier formula (c.f., [Dis15]), the Rubin-style formula proved in [Büy14] and our main Theorem 1.2:

Theorem 4.4. *Suppose that Nekovář's p-adic height pairing associated to the canonical splitting of the Hodge-filtration on the semi-stable Dieudonné module $D_{\mathrm{st}}(V)$ is non-vanishing. Then,*

$$\log_V(\mathrm{res}_p(\mathbf{BK}_1)) \cdot \log_V(\mathrm{res}_p(P))^{-2} \in \overline{\mathbb{Q}}^\times .$$

Remark 4.5. Our methods so far easily adapt to prove that analogous conclusions hold true for a *potentially self-dual* elliptic modular form f which verifies the hypotheses of Remark 1.6 and for which the natural map

$$\mathrm{res}_p : H^1_f(\mathbb{Q}, V_f) \to H^1_f(\mathbb{Q}_p, V_f)$$

is non-zero. Here, V_f is the self-dual twist of Deligne's representation, as in Remark 1.6.

Acknowledgements. I would to express my gratitude to Masataka Chida for carefully reading an earlier version of this manuscript and for his comments which helped me improve parts of the text, and to Daniel Disegni and Karl Rubin for very helpful correspondence. Special thanks are due to Henri Darmon for generously sharing his insights with me, for his suggestions and his constant encouragement. I also would like to thank Denis Benois, whose question on the Tate-Shafarevich groups of higher weight modular forms started the train of thoughts which lead me to the main results of this article.

Appendix A. Proof of Theorem 2.10

Until the end of this article, we shall assume that $p > 5$ is an anomalous prime for E, namely that $E(\mathbb{Q}_p)[p] \neq 0$. In view of Remark 2.12, this in particular means that E has either good ordinary reduction at p or split multiplicative reduction and $p = 1$ (since we never allow additive reduction). In either case, note that $a_p(E) = 1$.

Lemma A.1. *Let $\mathbb{Q}_{n,p}$ denote the completion of $\mathbb{Q}_n$ at its unique prime above p. Then,*

$$E(\mathbb{Q}_{n,p})[p] \cong \mathbb{Z}/p\mathbb{Z}.$$

[3] We remark that this conclusion does not formally follow directly from Kato's explicit reciprocity laws. For its proof, see [LZ13, Han15].

Proof. If $E(\mathbb{Q}_{n,p})[p]$ were not cyclic, it would mean that $E(\overline{\mathbb{Q}}_p)[p] \subset E(\mathbb{Q}_{n,p})$. This in turn would imply that $\mu_p \subset \mathbb{Q}_{n,p}$. □

Lemma A.2. *Suppose $p > 7$ if E has split multiplicative reduction at p. Then*

$$E(\mathbb{Q}_p)[p^\infty] \cong \mathbb{Z}/p\mathbb{Z}.$$

Proof. Since $p \geq 3$, the formal group of $\widehat{E}(p\mathbb{Z}_p)$ is torsion-free. This means that the natural map $E(\mathbb{Q}_p)[p^\infty] \to E(\mathbb{F}_p)$ is injective. In particular, p divides the order of $E(\mathbb{F}_p)$. The Riemann hypothesis for elliptic curves show that $E(\mathbb{F}_p)$ has exactly p elements. □

1.1. An analysis of local cohomology groups.

Lemma A.3. *The Λ-module $H^1(\mathbb{Q}, \mathbb{T})$ is free of rank 2.*

Proof. According to Perrin-Riou (c.f., [PR94]), the Λ-torsion submodule $H^1(\mathbb{Q}, \mathbb{T})_{\Lambda-\mathrm{tor}}$ of $H^1(\mathbb{Q}, \mathbb{T})$ is isomorphic to $H^0(\mathbb{Q}_{\infty,p}, T)$. It follows from the work of Cherbonnier and Colmez [CC99] that the quotient $H^1(\mathbb{Q}, \mathbb{T})/H^1(\mathbb{Q}, \mathbb{T})_{\Lambda-\mathrm{tor}}$ is a free Λ-module of rank 2 (see for example [Col05, Corollary 6.3.3]). It therefore suffices to check the vanishing of $H^0(\mathbb{Q}_{\infty,p}, T)$.

Since $a_p(E) = 1$, it follows from the Serre-Tate theory that

$$T\big|_{G_{\mathbb{Q}_p}} \cong \begin{pmatrix} \chi_{\mathrm{cyc}} & \star \\ 0 & 1 \end{pmatrix}.$$

If we had $H^0(G_{\mathbb{Q}_{p,\infty}}, T) \neq 0$, then the sequence

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow T \longrightarrow \mathbb{Z}_p \longrightarrow 0 \tag{A1}$$

of $G_{\mathbb{Q}_{p,\infty}}$-modules splits. This in turn implies that Serre-Tate class of the extension determined by $\star$ belongs to

$$\ker\left(H^1(\mathbb{Q}_p, \mathbb{Z}_p(1)) \to H^1(\mathbb{Q}_{\infty,p}, \mathbb{Z}_p(1))\right) = H^1\left(\Gamma, H^0(\mathbb{Q}_{p,\infty}, \mathbb{Z}_p(1))\right) = 0$$

where the first equality is due to the inflation-restriction sequence. This in turn shows that (A1) splits as $G_{\mathbb{Q}_p}$-modules and by Serre-Tate theory, E is a quasi-canonical lift of the reduced curve $\widetilde{E}_{/\mathbb{F}_p}$ and in particular, it has CM. This contradicts our assumption on the image of $\overline{\rho}_E$. □

Lemma A.4. *The Λ-module $H^2(\mathbb{Q}_p, \mathbb{T})$ is pseudo-null.*

Proof. The fact that $H^2(\mathbb{Q}_p, \mathbb{T})$ is a torsion Λ-module is well-known. Let $f \cdot \Lambda \subset \Lambda$ denote the characteristic ideal of this module and let

$$\begin{aligned} \mathcal{Z}^1(T) &\subset H^1(\mathbb{Q}_p, T) \\ &\cong H^1(\mathbb{Q}_p, \mathbb{T})/(\gamma - 1)H^1(\mathbb{Q}_p, \mathbb{T}) \end{aligned}$$

denote the image of $H^1(\mathbb{Q}_p, \mathbb{T})$ under the map induced from pr_0. By Lemma A.3, it follows that

$$H^0(\mathbb{Q}_p, E[p^\infty]) = H^1(\mathbb{Q}_p, T)_{\mathrm{tor}} \hookrightarrow H^1(\mathbb{Q}_p, T)/\mathcal{Z}_1(T)$$

where the first identification follows on applying the functor $H^0(\mathbb{Q}_p, -)$ on the short exact sequence

$$0 \longrightarrow T \longrightarrow T \otimes \mathbb{Q}_p \longrightarrow E[p^\infty] \longrightarrow 0\,.$$

It therefore follows that $|H^0(\mathbb{Q}_p,E[p^\infty])|\leq [H^1(\mathbb{Q}_p,T):\mathcal{Z}^1(T)]$ and therefore also that

$$\begin{aligned} \left|H^2(\mathbb{Q}_p,\mathbb{T})/(\gamma-1)H^2(\mathbb{Q}_p,\mathbb{T})\right| &= \left|H^2(\mathbb{Q}_p,T)\right| = \left|H^0(\mathbb{Q}_p,E[p^\infty])\right| \\ &\leq \left|\mathrm{coker}\left(H^1(\mathbb{Q}_p,\mathbb{T})\to H^1(\mathbb{Q}_p,T)\right)\right| \\ &= \left|H^2(\mathbb{Q}_p,\mathbb{T})[\gamma-1]\right| \end{aligned} \tag{A2}$$

Here, the first equality on the first line and the equality on the second line follow from the long exact sequence of the $G_{\mathbb{Q}_p}$-cohomology of the sequence

$$0\longrightarrow \mathbb{T}\overset{\gamma-1}{\longrightarrow}\mathbb{T}\longrightarrow T\longrightarrow 0\,,$$

as well as the fact that the cohomological dimension of $G_{\mathbb{Q}_p}$ equals to 2; whereas the second equality on the first line from local Tate duality. Thence,

$$1\leq \frac{\left|H^2(\mathbb{Q}_p,\mathbb{T})[\gamma-1]\right|}{\left|H^2(\mathbb{Q}_p,\mathbb{T})/(\gamma-1)H^2(\mathbb{Q}_p,\mathbb{T})\right|}=|f(0)|_p$$

where $|a|_p=p^{-v_p(a)}$ is the normalized norm on $\mathbb{Q}_p$, and the inequality is due to (A2). This shows that $f(0)\in\mathbb{Z}_p^\times$ and the proof of the Lemma follows. □

Definition A.5. Let π_α denote the natural projection map $H^1(\mathbb{Q}_p,\mathbb{T})\to H^1(\mathbb{Q}_p,T_\alpha)$ (so that we have $\pi_1=\mathrm{pr}_0$). We let $\mathcal{Z}^1(T_\alpha):=\mathrm{im}\,(\pi_\alpha)$.

Corollary A.6. *For every positive integer α, the natural inclusions*

$$\mathcal{Z}^1(T_\alpha)\hookrightarrow H^1(\mathbb{Q}_p,T_\alpha)\quad \textit{and}$$
$$H^1(\mathbb{Q}_p,T_\alpha)_{p-\mathrm{tor}}\hookrightarrow H^1(\mathbb{Q}_p,T_\alpha)$$

induce a splitting

$$H^1(\mathbb{Q}_p,T_\alpha)=H^1(\mathbb{Q}_p,T_\alpha)_{p-\mathrm{tor}}\oplus\mathcal{Z}^1(T_\alpha)\,.$$

Furthermore, $|H^1(\mathbb{Q}_p,T_\alpha)_{p-\mathrm{tor}}|$ is bounded independendly of α.

Proof. Let $\iota:\Lambda\to\Lambda$ denote the involution given by $\gamma\mapsto\gamma^{-1}$ on the group-like elements of Λ. Set $W_\alpha=V/T\otimes R_\alpha$ and $T_\alpha^\iota:=T\otimes R_\alpha^\iota=\mathbb{T}^\iota/(\gamma-1)^\alpha\mathbb{T}^\iota$. As in the proof of Lemma A.4 we have

$$\left|H^1(\mathbb{Q}_p,T_\alpha)_{p-\mathrm{tor}}\right|=\left|H^0(\mathbb{Q}_p,T_\alpha^*)\right|=\left|H^2(\mathbb{Q}_p,T_\alpha^\iota)\right|=\left|M^\iota/(\gamma-1)^\alpha M^\iota\right|,$$

and

$$\left[H^1(\mathbb{Q}_p,T_\alpha):\mathcal{Z}^1(T_\alpha)\right]=\left|M\left[(\gamma-1)^\alpha\right]\right| \tag{A3}$$

where $M=H^2(\mathbb{Q}_p,\mathbb{T})$. The exact sequence

$$0\longrightarrow M[(\gamma-1)^\alpha]\longrightarrow M\overset{(\gamma-1)^\alpha}{\longrightarrow}M\longrightarrow M/(\gamma-1)^\alpha M\longrightarrow 0$$

and Lemma A.4 shows that

$$\left|H^1(\mathbb{Q}_p,T_\alpha)_{p-\mathrm{tor}}\right|=\left[H^1(\mathbb{Q}_p,T_\alpha):\mathcal{Z}^1(T_\alpha)\right]\,. \tag{A4}$$

Thence, the injection $H^1(\mathbb{Q}_p,T_\alpha)_{p-\mathrm{tor}}\hookrightarrow H^1(\mathbb{Q}_p,T_\alpha)/\mathcal{Z}^1(T_\alpha)$ of R_α-modules is indeed an isomorphism and the first assertion of the corollary follows. The second assertion follows from (A4), (A3) and Lemma A.4. □

Fix once and for all a power h of p that is divisible by $\left|H^1(\mathbb{Q}_p,T_\alpha)_{p-\mathrm{tor}}\right|$ for every α. Set $r=h^2$ and $\nu=2v_p(h)$.

Corollary A.7. *Let α be a any positive integer and let d be any integer divisible by h.*
i) $d \cdot \mathcal{Z}^1(T_\alpha) = d \cdot H^1(\mathbb{Q}_p, T_\alpha)$.
ii) *For all positive integers $\alpha \geq \alpha'$, the natural map*

$$\gamma_{\alpha',\alpha} : T_{\alpha'} \xrightarrow{(\gamma-1)^{\alpha-\alpha'}} T_\alpha\, [(\gamma-1)^{\alpha'}]$$

induces isomorphisms

$$\text{(A5)}\qquad \begin{tikzcd} d \cdot \mathcal{Z}^1(T_{\alpha'}) \arrow[r, "\gamma_{\alpha',\alpha}", "\sim"'] \arrow[d, "\sim"'] & d \cdot \mathcal{Z}^1(T_\alpha)[(\gamma-1)^{\alpha'}] \arrow[d, "\sim"'] \\ d \cdot H^1(\mathbb{Q}_p, T_{\alpha'}) \arrow[r, dotted, "\sim", "\gamma_{\alpha',\alpha}"'] & d \cdot H^1(\mathbb{Q}_p, T_\alpha)[(\gamma-1)^{\alpha'}] \end{tikzcd}$$

where the vertical isomorphisms are the identifications from i).

Proof. This follows from Corollary A.6 and the fact that each $\mathcal{Z}^1(T_\alpha)$ is free over R_α. Note that the isomorphism on the second row of (A5) is deduced by completing the cartesian square. □

Definition A.8. For positive integers β and k, let $\mathcal{Z}^1(T_{k,\beta})$ denote the isomorphic image of $\mathcal{Z}^1(T_\beta)/p^k\mathcal{Z}^1(T_\beta)$ inside $H^1(\mathbb{Q}_p, T_{k,\beta})$. This is a free $R_{k,\beta}$-module of rank 2.

Lemma A.9. *Recall the positive integer $r = h^2$ we have fixed above. For every positive integer β and $k > \nu$, the image of $r \cdot \mathcal{Z}^1(T_\beta)$ inside $H^1(\mathbb{Q}_p, T_{k,\beta})$ (under the compositum of the arrows*

$$r \cdot \mathcal{Z}^1(T_\beta) \hookrightarrow H^1(\mathbb{Q}_p, T_\beta) \longrightarrow H^1(\mathbb{Q}_p, T_{k,\beta}))$$

equals $r \cdot \mathcal{Z}^1(T_{k,\beta})$.

Proof. Note that the size of the cokernel of the map

$$\operatorname{coker}\left(H^1(\mathbb{Q}_p, T_\beta)_{p-\mathrm{tor}} \oplus \mathcal{Z}^1(T_\beta) = H^1(\mathbb{Q}_p, T_\beta) \longrightarrow H^1(\mathbb{Q}_p, T_{k,\beta})\right) = H^2(\mathbb{Q}_p, T_\beta)[p^k]$$

is bounded by h. This means that the order of $H^1(\mathbb{Q}_p, T_{k,\beta})$ is at most $p^{2k\beta} \cdot h^2$. Since $H^1(\mathbb{Q}_p, T_{k,\beta})$ contains $\mathcal{Z}^1(T_{k,\beta}) \cong \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\beta$ and $k > \nu$, elementary divisors of the abelian p-group $H^1(\mathbb{Q}_p, T_{k,\beta})$ are of the form $(a_i, \cdots, a_s, p^k, \cdots, p^k)$ with $a_i \mid r$ $(i = 1, \cdots, s)$. This shows that

$$\left|r \cdot H^1(\mathbb{Q}_p, T_{k,\beta})\right| = \left|r \cdot \mathcal{Z}^1(T_{k,\beta})\right|$$

and the proof follows. □

Proposition A.10. *For r as above, positive integers k and $\alpha \geq \alpha'$, the map $\gamma_{\alpha',\alpha}$ induces an isomorphism*

$$r \cdot H^1_{\mathcal{F}_{\alpha'}}(\mathbb{Q}_p, T_{k,\alpha'}) \xrightarrow{\sim} r \cdot H^1_{\mathcal{F}_\alpha}(\mathbb{Q}_p, T_{k,\alpha})[(\gamma-1)^{\alpha'}]\,.$$

Proof. We have

$$\begin{aligned} r \cdot H^1_{\mathcal{F}_\beta}(\mathbb{Q}_p, T_\beta) &= \operatorname{im}\left(r \cdot H^1(\mathbb{Q}_p, T_\beta) \to H^1(\mathbb{Q}_p, T_{k,\beta})\right) \\ &= \operatorname{im}\left(r \cdot \mathcal{Z}^1(T_\beta) \to H^1(\mathbb{Q}_p, T_{k,\beta}\right) \\ &= r \cdot \mathcal{Z}^1(T_{k,\beta}) \end{aligned}$$

for $\beta = \alpha, \alpha'$, where the first equality follows from definitions, the second from Corollary A.7 and the last from Lemma A.9. The proof follows, since $\mathcal{Z}^1(T_{k,\beta})$ is free as an $R_{k,\beta}$-module (and $r \cdot \mathcal{Z}^1(T_{k,\beta})$ is free as an $R_{k-\nu,\beta}$-module). □

1.2. **Patching Kolyvagin systems.** In the final portion of this article, we explain how the proof of Theorem 2.10 follows as a consequence of our detailed analysis in Section A.1.1.

Theorem A.11. *Let $r \in \mathbb{Z}^+$ as above. For $\alpha \geq \alpha'$ and $k \geq k'$ the map*

$$r \cdot \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \longrightarrow r \cdot \mathbf{KS}(\mathcal{F}_{\alpha'}, T_{k',\alpha'}, \mathcal{P}_j)$$

is a surjection. Furthermore, the module $r \cdot \mathbf{KS}(\mathbb{T})$ is contained in a free Λ-module of rank one.

Proof. We will follow the Steps 1 to 3 in Section 2.2 (which leads to the proof of Theorem 2.11) and will appropriately modify Step 4 to conclude with the proof.

We fix $\alpha \in \mathbb{Z}^+$ and let $n \in \mathcal{N}_{k,m}$ be a core vertex for the Selmer structure on $\mathcal{F}_{\text{can}} = \mathcal{F}_1$ on $\overline{T}$. We claim that

$$\text{length}\, H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, T_{k,\alpha}) - \text{length}\, H^1_{\mathcal{F}_\alpha(n)^*}(\mathbb{Q}, T_{k,\alpha}) = k \cdot \alpha\,. \tag{A6}$$

To ease notation we set $S_k = R_{k,1}$ ($\cong \mathbb{Z}/p^k\mathbb{Z}$). By [MR04, Corollary 2.3.6], it suffices to prove this claim only for $n = 1$, namely for $\mathcal{F}_\alpha(n) = \mathcal{F}_\alpha$. Using [MR04, Theorem 4.1.5], we infer that there exists integers a_k, b_k (one of which may be taken to be zero) such that, there is an isomorphism

$$H^1_{\mathcal{F}_\alpha}(\mathbb{Q}, T_{k,\alpha}) \oplus S_k^{a_k} \cong H^1_{\mathcal{F}^*_\alpha}(\mathbb{Q}, T^*_{k,\alpha}) \oplus S_k^{b_k}.$$

Here we regard $T_{k,\alpha}$ as an S_k-representation. We note that proof of [MR04, Theorem 4.1.5] still carries over (by Lemma 3.7.1 of loc. cit.) to our case of interest. The proof of the same theorem in fact shows that a_k, b_k do not depend on k, we denote this common value by $\chi(T^*_\alpha)$, $\chi(T_\alpha)$, respectively. We therefore have an isomorphism

$$H^1_{\mathcal{F}_\alpha}(\mathbb{Q}, T_{k,\alpha}) \oplus S_k^{\chi(T^*_\alpha)} \cong H^1_{\mathcal{F}^*_\alpha}(\mathbb{Q}, T^*_{k,\alpha}) \oplus S_k^{\chi(T_\alpha)} \tag{A7}$$

and hence

$$\begin{aligned} \text{length}_{\mathbb{Z}_p} H^1_{\mathcal{F}_\alpha}(\mathbb{Q}, T_{k,\alpha}) \quad &- \quad \text{length}_{\mathbb{Z}_p} H^1_{\mathcal{F}^*_\alpha}(\mathbb{Q}, T^*_{k,\alpha}) = k \cdot (\chi(T_\alpha) - \chi(T^*_\alpha)) \\ &= \quad k \cdot \left(\text{rank}_{\mathbb{Z}_p} H^1_{\mathcal{F}_\alpha}(\mathbb{Q}, T_\alpha) - \text{corank}_{\mathbb{Z}_p} H^1_{\mathcal{F}^*_\alpha}(\mathbb{Q}, T^*_\alpha)\right) \\ &= \quad k\alpha \cdot \text{rank}_{\mathbb{Z}_p} T^- = k\alpha \end{aligned} \tag{A8}$$

where the second equality follows passing to limit in (A7), the third using [MR04, Lemma 5.2.15] together with the proof of Lemma A.3 (here, T^- stands as usual for the (-1)-eigenspace for a complex conjugation) and the very last equality by the skew-symmetric isomorphism $\text{Hom}(T, \mathbb{Z}_p(1)) \xrightarrow{\sim} T$ (induced from the Weil-pairing). The proof of our claim (A6) follows.

Furthermore, since $n \in \mathcal{N}_{k,\alpha}$ is a core vertex for $\mathcal{F}_{\text{can}}$ on $\overline{T}$, it follows that the $\mathbb{Z}/p^k\mathbb{Z}$-module $H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, E[p^k])$ is free of rank one. Thence, the submodule $H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, E[p^k])$ of $H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, E[p^k])$ is cyclic as well. It therefore follows from the natural inclusion $H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, T_{k,\alpha})/(\gamma - 1) \hookrightarrow H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, E[p^k])$ and Nakayama's lemma that $H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, T_{k,\alpha})$ is a cyclic $R_{k,\alpha}$-module. This combined with (A6) shows that the module $H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, T_{k,\alpha})$

is in fact a cyclic $R_{k,\alpha}$-module of rank one, and also that $H^1_{\mathcal{F}_\alpha(n)^*}(\mathbb{Q},T^*_{k,\alpha}) = 0$. This completes Step **1**.

Step 1 at hand, one may formally verify the Steps 2 and 3 (following Sections 3.1.2 and 3.1.3 of [Büy11]) to deduce that the natural map

$$\mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \longrightarrow H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q},T_{k,\alpha}) \tag{A9}$$

is an isomorphism for every $j \geq k+\alpha$. In view of (A9), the first assertion of the theorem is equivalent to the statements that the natural maps

$$\begin{aligned} r\cdot H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q},T_{k,\alpha}) &\longrightarrow r\cdot H^1_{\mathcal{F}_{\alpha'}(n)}(\mathbb{Q},T_{k,\alpha'}), \quad \text{and} \\ r\cdot H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q},T_{k,\alpha}) &\longrightarrow r\cdot H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q},T_{k',\alpha}) \end{aligned} \tag{A10}$$

are both surjective for $\alpha \geq \alpha'$, $k \geq k'$. The surjectivity of the second map follows from [Büy11, Lemma 3.22], since the Selmer structure $\mathcal{F}_\alpha$ is cartesian (in the sense of Definition 2.5 of loc. cit.) on the collection $\{T_{k,\alpha}\}_{k\in\mathbb{Z}^+}$ (for fixed α). To verify the surjectivity of the first map, consider the diagram

(A11)
$$\begin{tikzcd} r\cdot H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q},T_{k,\alpha}) \arrow[r] \arrow[dr, "\pi_{\alpha,\alpha'}"'] & r\cdot H^1_{\mathcal{F}_{\alpha'}(n)}(\mathbb{Q},T_{k,\alpha'}) \arrow[d, "\gamma_{\alpha',\alpha}"] \\ & r\cdot H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q},T_{k,\alpha})[(\gamma-1)^\alpha] \end{tikzcd}$$

where the map $\pi_{\alpha,\alpha'}$ is multiplication by $(\gamma-1)^{\alpha-\alpha'} \in R_{k,\alpha}$, and the map $\gamma_{\alpha',\alpha}$ is also induced from the natural injection $T_{k,\alpha'} \hookrightarrow T_{k,\alpha}$ which is also given multiplication by $(\gamma-1)^{\alpha-\alpha'}$. The map $\pi_{\alpha,\alpha'}$ is surjective since we have checked that the $R_{k-\nu,\alpha}$-module $r\cdot H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q},T_{k,\alpha})$ is free of rank one. We now analyze the vertical map $\gamma_{\alpha',\alpha}$ in (A11) and prove that it is in fact an isomorphism. Considering the $G_{\mathbb{Q},S}$-cohomology of the exact sequence

$$0 \longrightarrow T_{k,\alpha'} \stackrel{\gamma_{\alpha',\alpha}}{\longrightarrow} T_{k,\alpha} \longrightarrow T_{k,\alpha-\alpha'} \longrightarrow 0$$

we obtain an exact sequence

$$0 \longrightarrow H^1(\mathbb{Q}_S/\mathbb{Q},T_{k,\alpha'}) \stackrel{\gamma_{\alpha',\alpha}}{\longrightarrow} H^1(\mathbb{Q}_S/\mathbb{Q},T_{k,\alpha}) \stackrel{\mathfrak{P}}{\longrightarrow} H^1(\mathbb{Q}_S/\mathbb{Q},T_{k,\alpha-\alpha'})\,. \tag{A12}$$

where the injection on the left is due to our running hypothesis on the image of $\overline{\rho}_E$. Likewise, starting with the exact sequence

$$0 \longrightarrow T_{k,\alpha-\alpha'} \stackrel{\gamma_{\alpha-\alpha',\alpha}}{\longrightarrow} T_{k,\alpha} \longrightarrow T_{k,\alpha'} \longrightarrow 0\,,$$

we obtain an injection $H^1(\mathbb{Q}_S/\mathbb{Q},T_{k,\alpha-\alpha'}) \overset{\gamma_{\alpha-\alpha',\alpha}}{\hookrightarrow} H^1(\mathbb{Q}_S/\mathbb{Q},T_{k,\alpha})$. This together with (A12) yields the identifications

$$\begin{aligned} \mathrm{im}(\gamma_{\alpha',\alpha} :\ & H^1(\mathbb{Q}_S/\mathbb{Q},T_{k,\alpha'}) \to H^1(\mathbb{Q}_S/\mathbb{Q},T_{k,\alpha})) \\ &= \ker(\gamma_{\alpha-\alpha',\alpha}\circ\mathfrak{P} :\ H^1(\mathbb{Q}_S/\mathbb{Q},T_{k,\alpha}) \to H^1(\mathbb{Q}_S/\mathbb{Q},T_{k,\alpha})) \\ &= H^1(\mathbb{Q}_S/\mathbb{Q},T_{k,\alpha})[(\gamma-1)^{\alpha'}]\,. \end{aligned}$$

It follows from Proposition A.10 (the local conditions away from p are handled in Sections 2.3.1 and 2.6 of [Büy11]) that the module $r\cdot H^1_{\mathcal{F}_{\alpha'}(n)}(\mathbb{Q},T_{k,\alpha'})$ is the exact inverse image of $r\cdot H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q},T_{k,\alpha})[(\gamma-1)^{\alpha'}]$ under this identification. This completes the proof that the vertical map in (A11) is an isomorphism. We conclude that the horizontal map is a surjection and the first assertion in the theorem is verified.

We now prove the second claim. First note that we have a tautological inclusion

$$\mathbf{KS}(\mathcal{F}_\Lambda, T_{k,\alpha}, \mathcal{P}_j) \hookrightarrow \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \tag{A13}$$

for every $j \geq k+\alpha$, and since the direct limit functor is exact, it follows on passing to limit in (A13) that

$$\varinjlim_j r \cdot \mathbf{KS}(\mathcal{F}_\Lambda, T_{k,\alpha}, \mathcal{P}_j) \hookrightarrow \varinjlim_j r \cdot \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \tag{A14}$$

Since the map (A9) is an isomorphism for every $j \geq k+\alpha$, we see that

$$\varinjlim_j r \cdot \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \xrightarrow{\sim} r \cdot H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, T_{k,\alpha}) \tag{A15}$$

for any core vertex $n \in \mathcal{N}_s$ with $s \geq k+\alpha$. This shows that both modules that appear in (A14) are compact and since the inverse limit functor is left exact on sequences of compact modules, it follows that

$$r \cdot \mathbf{KS}(\mathbb{T}) = \varprojlim_{k,\alpha} \varinjlim_j r \cdot \mathbf{KS}(\mathcal{F}_\Lambda, T_{k,\alpha}, \mathcal{P}_j) \hookrightarrow \varprojlim_{k,\alpha} \varinjlim_j r \cdot \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \tag{A16}$$

Furthermore, for every $k \geq k'$ and $\alpha \geq \alpha'$, we have the following commutative diagram

$$\begin{tikzcd}
r \cdot \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \arrow[r, "\sim"] \arrow[d] & r \cdot H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, T_{k,\alpha}) \arrow[d] \\
r \cdot \mathbf{KS}(\mathcal{F}_{\alpha'}, T_{k',\alpha'}, \mathcal{P}_j) \arrow[r, "\sim"] & r \cdot H^1_{\mathcal{F}_{\alpha'}(n)}(\mathbb{Q}, T_{k',\alpha'})
\end{tikzcd}$$

for any core vertex $n \in \mathcal{N}_{k+\alpha} \subset \mathcal{N}_{k',\alpha'}$, where the vertical surjections are deduced above, as well as the fact that the $R_{k-\nu,\alpha}$-module $r \cdot H^1_{\mathcal{F}_\alpha(n)}(\mathbb{Q}, T_{k,\alpha})$ (and likewise, the $R_{k'-\nu,\alpha'}$-module $r \cdot H^1_{\mathcal{F}_{\alpha'}(n)}(\mathbb{Q}, T_{k',\alpha'})$) is free of rank one. Passing to projective limit (with respect to vertical arrows) in the diagram above, it follows that the Λ-module $\varprojlim_{k,\alpha} \varinjlim_j r \cdot \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j)$ is free of rank one, and the proof of the second claim in the theorem is now complete thanks to the inclusion of (A16). □

Proof of Theorem 2.10. Using the inclusions

$$r \cdot \mathbf{KS}(\mathbb{T}) \hookrightarrow \varprojlim_{k,\alpha} \varinjlim_j r \cdot \mathbf{KS}(\mathcal{F}_\alpha, T_{k,\alpha}, \mathcal{P}_j) \hookrightarrow \mathbf{KS}(\mathbb{T}) \tag{A17}$$

(where the first inclusion is (A14) and the second follows from Corollary A.7), together with the fact that the module in the middle is free of rank one (as we have checked as part of the proof of Theorem A.11), we conclude with the proof of (i). Mazur and Rubin in [MR04, Theorem 5.2.10] have proved that the module $\mathbf{KS}(T)$ is free of rank one. The proof of (ii) now follows using this fact along with with the first assertion in Theorem A.11 and the inclusions in (A17). □

References

[BB15] Denis Benois and Kâzim Büyükboduk. On the exceptional zeros of p-non-ordinary p-adic L-functions and a conjecture of Perrin-Riou, 2015. Preprint, 47 pages, http://arxiv.org/abs/1510.01915.

[BD07] Massimo Bertolini and Henri Darmon. Hida families and rational points on elliptic curves. *Invent. Math.*, 168(2):371–431, 2007.

[BD15] Massimo Bertolini and Henri Darmon. Kato's Euler system and rational points on elliptic curves III: The conjecture of Perrin-Riou, $\geq$ 2015.

[BDP13] Massimo Bertolini, Henri Darmon, and Kartik Prasanna. Generalized Heegner cycles and p-adic Rankin L-series. *Duke Math. J.*, 162(6):1033–1148, 2013. With an appendix by Brian Conrad.

[Büy11] Kâzım Büyükboduk. Λ-adic Kolyvagin systems. *IMRN*, 2011(14):3141–3206, 2011.

[Büy14] Kâzım Büyükboduk. On Nekovar's heights, exceptional zeros and a conjecture of Mazur-Tate-Teitelbaum, 2014. *IMRN*, to appear. DOI:10.1093/imrn/rnv205.

[CC99] Frédéric Cherbonnier and Pierre Colmez. Théorie d'Iwasawa des représentations p-adiques d'un corps local. *J. Amer. Math. Soc.*, 12(1):241–268, 1999.

[Col05] Pierre Colmez. Fontaine's rings and p-adic L-functions, 2005. Lecture Notes, available at: http://webusers.imj-prg.fr/ pierre.colmez/tsinghua.pdf.

[Dis15] Daniel Disegni. The p-adic Gross-Zagier formula on Shimura curves, 2015. Preprint, 81 pages, http://arxiv.org/abs/1510.02114.

[DW08] Chantal David and Tom Weston. Local torsion on elliptic curves and the deformation theory of Galois representations. *Math. Res. Lett.*, 15(2-3):599–611, 2008.

[Han15] David Hansen. Iwasawa theory of overconvergent modular forms, I: Critical p-adic L-functions, 2015. Preprint, 30 pages, http://arxiv.org/abs/1508.03982.

[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, (295):ix, 117–290, 2004. Cohomologies p-adiques et applications arithmétiques. III.

[Kob03] Shinichi Kobayashi. Iwasawa theory for elliptic curves at supersingular primes. *Invent. Math.*, 152(1):1–36, 2003.

[Kob13] Shinichi Kobayashi. The p-adic Gross-Zagier formula for elliptic curves at supersingular primes. *Invent. Math.*, 191(3):527–629, 2013.

[Kol90] V.A. Kolyvagin. Euler systems. In *Jacobiennes généralisées globale relatives. (Relative global generalized Jacobians)*, pages 435–483. 1990.

[LZ13] David Loeffler and Sarah Livia Zerbes. Wach modules and critical slope p-adic L-functions. *J. Reine Angew. Math.*, 679:181–206, 2013.

[Maz72] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.

[MR04] Barry Mazur and Karl Rubin. Kolyvagin systems. *Mem. Amer. Math. Soc.*, 168(799):viii+96, 2004.

[PR87] Bernadette Perrin-Riou. Points de Heegner et dérivées de fonctions L p-adiques. *Invent. Math.*, 89(3):455–510, 1987.

[PR93] Bernadette Perrin-Riou. Fonctions L p-adiques d'une courbe elliptique et points rationnels. *Ann. Inst. Fourier (Grenoble)*, 43(4):945–995, 1993.

[PR94] Bernadette Perrin-Riou. Théorie d'Iwasawa des représentations p-adiques sur un corps local. *Invent. Math.*, 115(1):81–161, 1994. With an appendix by Jean-Marc Fontaine.

[PR95] Bernadette Perrin-Riou. Fonctions L p-adiques des représentations p-adiques. *Astérisque*, (229):198, 1995.

[Roh84] David E. Rohrlich. On L-functions of elliptic curves and cyclotomic towers. *Invent. Math.*, 75(3):409–423, 1984.

[Rub98] Karl Rubin. Euler systems and modular elliptic curves. In *Galois representations in arithmetic algebraic geometry. Proceedings of the symposium, Durham, UK, July 9–18, 1996*, pages 351–367. Cambridge: Cambridge University Press, 1998.

[Rub00] Karl Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.

[Ski14a] Christopher Skinner. A converse to a theorem of Gross, Zagier, and Kolyvagin, 2014. http://arxiv.org/abs/1405.7294.

[Ski14b] Christopher Skinner. Multiplicative reduction and the cyclotomic main conjecture for GL_2, 2014. http://arxiv.org/abs/1407.1093.

[SU14] Christopher Skinner and Eric Urban. The Iwasawa Main Conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[SZ14] Christopher Skinner and Wei Zhang. Indivisibility of Heegner points in the multiplicative case, 2014. http://arxiv.org/abs/1407.1099.

[Ven15] Rodolfo Venerucci. Exceptional zero formulae and a conjecture of Perrin-Riou, 2015. *Invent. Math.*, to appear.

[Wan14] Xin Wan. Iwasawa Main Conjecture for Supersingular Elliptic Curves, 2014. http://arxiv.org/abs/1411.6352.

[Wan15] Xin Wan. Iwasawa Main Conjecture for Hilbert Modular Forms. *Forum Math., Sigma*, 3(e18), 2015.

[Zha14] Wei Zhang. Selmer groups and the indivisibility of Heegner points. *Camb. J. Math.*, 2(2):191–253, 2014.

Kâzim Büyükboduk
Koç University, Mathematics
Rumeli Feneri Yolu, 34450 Sariyer
Istanbul, Turkey

E-mail address: kbuyukboduk@ku.edu.tr