COMPOSITIO MATHEMATICA

# Tate–Shafarevich groups in anticyclotomic $\mathbb{Z}_p$-extensions at supersingular primes

Mirela Çiperiani

Compositio Math. **145** (2009), 293–308.

doi:10.1112/S0010437X08003874

FOUNDATION COMPOSITIO MATHEMATICA

The London Mathematical Society

https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

Compositio Math. 145 (2009) 293–308
doi:10.1112/S0010437X08003874

# Tate–Shafarevich groups in anticyclotomic $\mathbb{Z}_p$-extensions at supersingular primes

Mirela Çiperiani

Abstract

Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve and $p$ a prime of supersingular reduction for E. Denote by $\mathrm{K}_\infty$ the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field K which satisfies the Heegner hypothesis. Assuming that $p$ splits in $\mathrm{K}/\mathbb{Q}$, we prove that $Ш(\mathrm{K}_\infty, \mathrm{E})_{p^\infty}$ has trivial $\Lambda$-corank and, in the process, also show that $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})$ and $\mathrm{E}(\mathrm{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ both have $\Lambda$-corank two.

## Introduction

Let E be an elliptic curve of conductor N defined over $\mathbb{Q}$, and let $p$ be a rational prime such that E has supersingular reduction at $p$. We denote by $\mathrm{E}_p$ the $p$-torsion of E and assume throughout the paper that $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}_p)/\mathbb{Q})$ is not solvable. Let $\mathrm{K}/\mathbb{Q}$ be any imaginary quadratic extension such that the primes dividing $p\mathrm{N}$ split. Denote by $\mathrm{K}_\infty$ the anticyclotomic $\mathbb{Z}_p$-extension of K which is the unique Galois extension of K such that $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K}) \simeq \mathbb{Z}_p$ and $\mathrm{Gal}(\mathrm{K}_\infty/\mathbb{Q})$ is a pro-dihedral group. We now consider the Tate–Shafarevich group of $\mathrm{E}/\mathrm{K}_\infty$, namely the group of genus-one curves defined over $\mathrm{K}_\infty$ with E as their Jacobian possessing a point over every completion of $\mathrm{K}_\infty$; this is a torsion group. The $p$-primary part of the Tate–Shafarevich group of $\mathrm{E}/\mathrm{K}_\infty$, denoted by $Ш(\mathrm{K}_\infty, \mathrm{E})_{p^\infty}$, can be viewed as a module over $\Lambda := \mathbb{Z}_p[[\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})]]$, and its Pontryagin dual

$$\widehat{Ш(\mathrm{K}_\infty, \mathrm{E})}_{p^\infty} := \mathrm{Hom}(Ш(\mathrm{K}_\infty, \mathrm{E})_{p^\infty}, \mathbb{Q}_p/\mathbb{Z}_p)$$

is finitely generated over $\Lambda$. The $\Lambda$-corank of $Ш(\mathrm{K}_\infty, \mathrm{E})_{p^\infty}$ is defined to be the rank of its Pontryagin dual. We will prove the following theorem.

Theorem 0.1. *The $\Lambda$-module $Ш(\mathrm{K}_\infty, \mathrm{E})_{p^\infty}$ has trivial corank.*

This result is a manifestation of the break in the behavior of the Tate–Shafarevich group at supersingular primes in comparison to ordinary primes. When $p$ is a prime of ordinary reduction, Rubin [Rub88] (in the CM case) and Kato [Kat04] (in the non-CM case) have analyzed the behavior of the Tate–Shafarevich group over the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$, showing that $Ш(\mathbb{Q}_\infty, \mathrm{E})_{p^\infty}$ has trivial corank. In this same case, assuming that the primes dividing N split in $\mathrm{K}/\mathbb{Q}$, Bertolini [Ber95] has shown that $Ш(\mathrm{K}_\infty, \mathrm{E})_{p^\infty}$ has trivial $\Lambda$-corank also.

When $p$ is a prime of supersingular reduction, by using the work of Schneider [Sch85], Rohrlich [Roh84] and Kato [Kat04] one can see that the $\Lambda$-corank of $Ш(\mathbb{Q}_\infty, \mathrm{E})_{p^\infty}$ is greater than or equal to one. Furthermore, under certain conditions which, in particular, imply that $\mathrm{E}/\mathbb{Q}$ has trivial analytic rank, Kurihara [Kur02] has proven that $Ш(\mathbb{Q}_\infty, \mathrm{E})_{p^\infty}$ has $\Lambda$-corank one.

Received 5 September 2007, accepted in final form 15 August 2008, published online 19 February 2009.
*2000 Mathematics Subject Classification* 11G05.
*Keywords:* elliptic curve, supersingular reduction, Selmer group, Tate–Shafarevich group.
The author was partially supported by an NSF fellowship during the preparation of this paper.

An algebraic proof of this result has been given by Pollack [Pol05]. In this paper, we shall see that the $\Lambda$-corank of $\text{Ш}(\mathrm{K}_\infty, \mathrm{E})_{p^\infty}$ is trivial, and in the process we will analyze the $\Lambda$-corank of the Selmer group $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})$ (defined in § 1) and of $\mathrm{E}(\mathrm{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

## 1. Structure results

For every number field F and $m \in \mathbb{N}$, we can define the $p^m$-torsion of the Selmer group of E/F to be

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{F}, \mathrm{E}_{p^m}) := \ker\Big[\mathrm{H}^1(\mathrm{F}, \mathrm{E}_{p^m}) \to \prod_{\lambda \subseteq \mathrm{F}} \mathrm{H}^1(\mathrm{F}_\lambda, \mathrm{E})\Big],$$

where $\lambda$ denotes primes in F and $\mathrm{F}_\lambda$ is the completion of F at $\lambda$. Then, the $p^m$-torsion of the Tate–Shafarevich group of E/F fits in the exact sequence

$$0 \to \mathrm{E}(\mathrm{F})/p^m\mathrm{E}(\mathrm{F}) \to \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{F}, \mathrm{E}_{p^m}) \to \text{Ш}(\mathrm{F}, \mathrm{E})_{p^m} \to 0. \tag{1}$$

Let $\mathrm{K}_n \subseteq \mathrm{K}_\infty$ be the unique extension of K such that $\mathrm{Gal}(\mathrm{K}_n/\mathrm{K}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. One can consider

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^\infty}) := \varinjlim_{m} \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^m}),$$

where the transition maps are induced by the inclusions $\mathrm{E}_{p^m} \hookrightarrow \mathrm{E}_{p^{m+1}}$. We now define

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty}) := \varinjlim_{n} \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^\infty}),$$

where the transition maps are simply restrictions. Observe that since we are assuming $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}_p)/\mathbb{Q})$ is not solvable, the transition maps in both of the above direct limits are injective. Since

$$\text{Ш}(\mathrm{K}_n, \mathrm{E})_{p^\infty} = \varinjlim_{m} \text{Ш}(\mathrm{K}_n, \mathrm{E})_{p^m} \quad \text{and} \quad \text{Ш}(\mathrm{K}_\infty, \mathrm{E})_{p^\infty} = \varinjlim_{n} \text{Ш}(\mathrm{K}_n, \mathrm{E})_{p^\infty},$$

the exactness of the sequence (1) implies that the sequence

$$0 \to \mathrm{E}(\mathrm{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty}) \to \text{Ш}(\mathrm{K}_\infty, \mathrm{E})_{p^\infty} \to 0$$

is also exact.

Let us now choose a strictly increasing sequence of natural numbers $\{m_n\}$ such that $m_n \geq n$ and $\mathrm{E}(\mathrm{K}_{\lambda_n})_{p^\infty} \subseteq \mathrm{E}_{p^{m_n}}$ for all primes $\lambda_n \subset \mathrm{K}_n$ which divide N, where $\mathrm{K}_{\lambda_n}$ denotes the completion of $\mathrm{K}_n$ at $\lambda_n$. One can verify that

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty}) = \varinjlim_{n} \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}).$$

For any finite set of rational primes Q, we can consider the group

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) := \ker\Big[\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \to \prod_{\lambda_n \nmid \ell \in p\cup\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_{\lambda_n}, \mathrm{E})\Big],$$

where $\lambda_n$ denotes primes of $\mathrm{K}_n$ and $\mathrm{K}_{\lambda_n}$ is the completion of $\mathrm{K}_n$ at $\lambda_n$. Notice that $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \subseteq \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$. Set

$$\mathrm{R}_n := \mathbb{Z}/p^{m_n}\mathbb{Z}[\mathrm{Gal}(\mathrm{K}_n/\mathrm{K})]$$

and observe that $\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ can be viewed as an $\mathrm{R}_n$-module.



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

Let $n' \geq n$. The assumption that $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}_p)/\mathbb{Q})$ is not solvable implies that the restriction map

$$\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \to \mathrm{H}^1(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_n}}),$$

as well as the map

$$\mathrm{H}^1(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_n}}) \to \mathrm{H}^1(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})$$

induced by the inclusion $\mathrm{E}_{p^{m_n}} \hookrightarrow \mathrm{E}_{p^{m_{n'}}}$, are both injective. By composing the above maps, we obtain the injection

$$\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \hookrightarrow \mathrm{H}^1(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}}). \tag{2}$$

Lemma 1.1. *The map* (2) *induces an isomorphism between the following* $\mathrm{R}_n$*-modules:*

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \simeq \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n} - 1, p^{m_n}],$$

*where* $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K}_n) = \langle g^{p^n} \rangle$ *and* $n' \geq n$.

*Proof.* The restriction map induces the isomorphism

$$\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_{n'}}}) \simeq \mathrm{H}^1(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})^{\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K}_n)} = \mathrm{H}^1(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n} - 1].$$

Since $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \simeq \mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_{n'}}})[p^{m_n}]$, it follows that

$$\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \simeq \mathrm{H}^1(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n} - 1, p^{m_n}]$$

under the map (2). It is clear that

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \hookrightarrow \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n} - 1, p^{m_n}].$$

We will now show that the above map is surjective. Let $\lambda_n$ be a prime of $\mathrm{K}_n$ and $\lambda_{n'}$ a prime of $\mathrm{K}_{n'}$ that divides $\lambda_n$. We will assume that $\lambda_n$ does not divide any of the primes in $\{p\} \cup \mathrm{Q}_{k_{n'}}$.

If $\lambda_{n'}$ is a prime of good reduction, then the image of

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n} - 1, p^{m_n}] \to \mathrm{H}^1(\mathrm{K}_{\lambda_{n'}}, \mathrm{E}_{p^{m_{n'}}})$$

lies in $\mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_{\lambda_{n'}}/\mathrm{K}_{\lambda_{n'}}, \mathrm{E}_{p^{m_{n'}}})[g^{p^r} - 1, p^{m_n}]$; here $\mathrm{K}_{\lambda_{n'}}$ denotes the completion of $\mathrm{K}_{n'}$ at $\lambda_{n'}$, $\mathrm{K}^{\mathrm{unr}}_{\lambda_{n'}}$ denotes its maximal unramified extension, and $g^{p^r}$ generates $\mathrm{Gal}(\mathrm{K}_{\lambda_{n'}}/\mathrm{K}_{\lambda_n})$. Since $\mathrm{K}_{\lambda_{n'}}/\mathrm{K}_{\lambda_n}$ is unramified, the preimage of $\mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_{\lambda_{n'}}/\mathrm{K}_{\lambda_{n'}}, \mathrm{E}_{p^{m_{n'}}})[g^{p^r} - 1]$ under the restriction map

$$\mathrm{H}^1(\mathrm{K}_{\lambda_n}, \mathrm{E}_{p^{m_{n'}}}) \to \mathrm{H}^1(\mathrm{K}_{\lambda_{n'}}, \mathrm{E}_{p^{m_{n'}}})$$

lies in $\mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_{\lambda_n}/\mathrm{K}_{\lambda_n}, \mathrm{E}_{p^{m_{n'}}})$. Finally, since

$$\mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_{\lambda_n}/\mathrm{K}_{\lambda_n}, \mathrm{E}_{p^{m_{n'}}})[p^{m_n}] = \mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_{\lambda_n}/\mathrm{K}_{\lambda_n}, \mathrm{E}_{p^{m_n}}),$$

we see that the image of

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_{n'}}}}(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n} - 1, p^{m_n}] \to \mathrm{H}^1(\mathrm{K}_{\lambda_n}, \mathrm{E}_{p^{m_{n'}}})$$

lies in $\mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_{\lambda_n}/\mathrm{K}_{\lambda_n}, \mathrm{E}_{p^{m_n}})$.

If $\lambda_{n'}$ is a prime of bad reduction, then the image of

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n} - 1, p^{m_n}] \to \mathrm{H}^1(\mathrm{K}_{\lambda_{n'}}, \mathrm{E}_{p^{m_{n'}}})$$

lies in the image of

$$(\mathrm{E}(\mathrm{K}_{\lambda_{n'}})/p^{m_{n'}})[g^{p^n} - 1, p^{m_n}] \to \mathrm{H}^1(\mathrm{K}_{\lambda_{n'}}, \mathrm{E}_{p^{m_{n'}}}).$$



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

By our choice of the sequence $m_n$ and [ÇW08, Lemma 2.1.3], we know that

$$\mathrm{E}(\mathrm{K}_{\lambda_{n'}})/p^{m_{n'}} \simeq \mathrm{E}(\mathrm{K}_{\lambda_{n'}})_{p^{m_{n'}}} \quad \text{and} \quad \mathrm{E}(\mathrm{K}_{\lambda_n})/p^{m_n} \simeq \mathrm{E}(\mathrm{K}_{\lambda_n})_{p^{m_n}}.$$

It then follows that

$$(\mathrm{E}(\mathrm{K}_{\lambda_{n'}})/p^{m_{n'}})[g^{p^n}-1, p^{m_n}] \simeq \mathrm{E}(\mathrm{K}_{\lambda_{n'}})_{p^{m_{n'}}}[g^{p^n}-1, p^{m_n}] = \mathrm{E}(\mathrm{K}_{\lambda_n})_{p^{m_n}} \simeq \mathrm{E}(\mathrm{K}_{\lambda_n})/p^{m_n}.$$

This concludes the proof that the preimage of $\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n}-1, p^{m_n}]$ under the map (2) is $\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$. $\square$

Let $\{\mathrm{Q}_n \mid n \in \mathbb{N}\}$ be a sequence of sets of rational primes such that:

(i) $q \in \mathrm{Q}_n$ is inert in $\mathrm{K}/\mathbb{Q}$;

(ii) $q \in \mathrm{Q}_n$ is prime to $p\mathrm{N}$;

(iii) $\mathrm{E}(\mathrm{K}_q)_{p^\infty} = \mathrm{E}(\overline{\mathrm{K}_q})_{p^{m_n}}$, where $\mathrm{K}_q$ denotes the completion of K at the prime of K above $q$;

(iv) $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{m_n}}) \hookrightarrow \prod_{q\in\mathrm{Q}_n} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{m_n}})$;

(v) the set $\mathrm{Q}_n$ is finite and its size does not depend on $n$.

By [ÇW08, Proposition 2.6.3], all the $\mathrm{R}_n$-modules in the set

$$\{\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_k}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \mid k \geq n\}$$

have the same size. This implies that we can find a strictly increasing sequence $\{k_n \in \mathbb{N} \mid n \in \mathbb{N}\}$ such that

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_n}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \simeq \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_{n'}}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$$

as $\mathrm{R}_n$-modules for all $n' \geq n$. Moreover, from Lemma 1.1 we know that

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_{n'}}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \simeq \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_{n'}}}}(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n}-1, p^{m_n}].$$

Consequently, even if the $\mathrm{R}_n$-modules $\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_n}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ are not naturally related as $n$ grows, we have that

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_n}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \simeq \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_{n+1}}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \simeq \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_{n+1}}}}(\mathrm{K}_{n+1}, \mathrm{E}_{p^{m_{n+1}}})[g^{p^n}-1, p^{m_n}],$$

where the first isomorphism is formal while the second is induced by the map (2). It follows that we can now fix maps

$$i_n : \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_n}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \to \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_{n+1}}}}(\mathrm{K}_{n+1}, \mathrm{E}_{p^{m_{n+1}}})$$

for every $n \in \mathbb{N}$, and we observe that all these maps are injective. Using $i_n$ as transition maps, we construct the direct limit

$$\mathcal{M}_s := \varinjlim_{n} \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_n}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}).$$

The following theorem describes the structure of $\mathcal{M}_s$ as a $\Lambda$-module.

THEOREM 1.2 (Theorem 2.6.4 in [ÇW08]). *The $\Lambda$-module $\widehat{\mathcal{M}_s}$ is isomorphic to $\Lambda^{2t+2}$, where $t = \#\mathrm{Q}_{k_n}$.*

Observe that for every $n \in \mathbb{N}$ and any $n' \geq n$ there is a noncanonical isomorphism

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_{n'}}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \simeq \mathrm{H}^1_{\mathrm{Sel}_{p\cup\mathrm{Q}_{k_n}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$$



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

and that the map

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup \mathrm{Q}_{k_n}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \to \mathcal{M}_s$$

is injective with image contained in $\mathcal{M}_s[g^{p^n} - 1, p^{m_n}]$. The composition therefore determines an injection

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup \mathrm{Q}_{k_{n'}}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \to \mathcal{M}_s[g^{p^n} - 1, p^{m_n}].$$

In addition, by [ÇW08, Proposition 2.6.3], we know that

$$\#\mathrm{H}^1_{\mathrm{Sel}_{p\cup \mathrm{Q}_{k_{n'}}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) = \#({\mathrm{R}_n}^{2t+2}) \quad \text{for all } n' \geq n.$$

This implies that

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup \mathrm{Q}_{k_{n'}}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \simeq \mathcal{M}_s[g^{p^n} - 1, p^{m_n}]$$

and, consequently, that

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup \mathrm{Q}_{k_{n'}}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \simeq {\mathrm{R}_n}^{2t+2} \quad \text{for every } n' \geq n.$$

Let us now consider the maps

$$\mathrm{H}^1_{\mathrm{Sel}_{p\cup \mathrm{Q}_{k_{n'}}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \to \prod_{q\in \mathrm{Q}_{k_{n'}}} \mathrm{H}^1(\mathrm{K}_n(q), \mathrm{E})_{p^{m_n}}, \tag{3}$$

where $n' \geq n$ and $\mathrm{H}^1(\mathrm{K}_n(q), \mathrm{E})_{p^{m_n}} := \prod_{q_n|q} \mathrm{H}^1(\mathrm{K}_{q_n}, \mathrm{E})_{p^{m_n}}$, with $q_n$ denoting primes of $\mathrm{K}_n$ above $q$ and $\mathrm{K}_{q_n}$ denoting the completion of $\mathrm{K}_n$ at $q_n$. Notice that the kernel of the map (3) is $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ and, as in Lemma 1.1, one can see that

$$\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n} - 1, p^{m_n}] \simeq \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \quad \text{for all } n' \geq n.$$

The first three properties of primes $q \in \mathrm{Q}_n$ imply that (see [Ber95, Corollary 6])

$$\mathrm{H}^1(\mathrm{K}_n(q), \mathrm{E})_{p^{m_n}} \simeq {\mathrm{R}_n}^2.$$

Thus, the maps (3) can be viewed as maps between formal $\mathrm{R}_n$-modules

$$\theta_{n,n'} : {\mathrm{R}_n}^{2t+2} \to {\mathrm{R}_n}^{2t}.$$

Since for every $n$ we have infinitely many maps ${\mathrm{R}_n}^{2t+2} \to {\mathrm{R}_n}^{2t}$, it follows that infinitely many of them are identical. This allows us to assume (by switching to a subsequence of the sequence $k_n$ if necessary) that

$$\theta_{n,n'} = \theta_{n,n} \quad \text{for all } n' \geq n.$$

We now view $\mathrm{R}_n$ as the $\Lambda$-module $\hat{\Lambda}[g^{p^n} - 1, p^{m_n}]$. It is then easy to see that $\mathrm{R}_n \subseteq \mathrm{R}_{n+1}$. By using Lemma 1.1, the fact that

$$\mathrm{H}^1(\mathrm{K}_{n+1}(q), \mathrm{E})_{p^{m_{n+1}}}[g^{p^n} - 1, p^{m_n}] = \mathrm{H}^1(\mathrm{K}_n(q), \mathrm{E})_{p^{m_n}}$$

and the commutative diagram

$$\begin{tikzcd}
\mathrm{H}^1_{\mathrm{Sel}_{p\cup \mathrm{Q}_{k_{n+1}}}}(\mathrm{K}_{n+1}, \mathrm{E}_{p^{m_{n+1}}}) \arrow[r] & \prod_{q\in \mathrm{Q}_{k_{n+1}}} \mathrm{H}^1(\mathrm{K}_{n+1}(q), \mathrm{E})_{p^{m_{n+1}}} \\
\mathrm{H}^1_{\mathrm{Sel}_{p\cup \mathrm{Q}_{k_{n+1}}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \arrow[r] \arrow[u, hook] & \prod_{q\in \mathrm{Q}_{k_{n+1}}} \mathrm{H}^1(\mathrm{K}_n(q), \mathrm{E})_{p^{m_n}} \arrow[u, hook]
\end{tikzcd}$$



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

we see that the diagram

$$\begin{tikzcd} {\mathrm{R}_{n+1}}^{2t+2} \arrow[r, "\theta_{n+1,n+1}"] & {\mathrm{R}_{n+1}}^{2t} \\ {\mathrm{R}_n}^{2t+2} \arrow[u, hook] \arrow[r, "\theta_{n,n+1}"] & {\mathrm{R}_n}^{2t} \arrow[u, hook] \end{tikzcd}$$

commutes. Since $\theta_{n,n+1} = \theta_{n,n}$, we can now consider the $\Lambda$-module map

$$\theta : \hat{\Lambda}^{2t+2} \to \hat{\Lambda}^{2t}, \tag{4}$$

where the restriction of $\theta$ to ${\mathrm{R}_n}^{2t+2}$ equals $\theta_{n,n}$.

Notice that the kernel of the map (3) is $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$, which is equivalent to saying that

$$\ker \theta_{n,n} \simeq \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}).$$

Consequently, the kernel of the map $\theta$ is a direct limit of $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$, where the transition maps are injective but not necessarily the natural ones.

PROPOSITION 1.3. *The $\Lambda$-corank of $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})$ is equal to the $\Lambda$-corank of the kernel of $\theta$.*

*Proof.* As in Lemma 1.1, we can show that

$$\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})[g^{p^n} - 1, p^{m_n}] \simeq \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \quad \text{for all } n' \geq n. \tag{5}$$

On the one hand, since $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty}) = \varinjlim_{n'} \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_{n'}, \mathrm{E}_{p^{m_{n'}}})$, we have

$$\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})[g^{p^n} - 1, p^{m_n}] \simeq \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}).$$

On the other hand, (5) and the fact that the transition maps used in viewing $\ker \theta$ as a direct limit of $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ are injective together imply that

$$\ker \theta \, [g^{p^n} - 1, p^{m_n}] \simeq \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}).$$

So we have that

$$\ker \theta \, [g^{p^n} - 1, p^{m_n}] \simeq \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})[g^{p^n} - 1, p^{m_n}],$$

which implies that the $\Lambda$-corank of $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})$ equals that of the kernel of $\theta$. □

## 2. Heegner points and Kolyvagin classes

**2.1** We fix a parametrization $\pi : \mathrm{X}_0(\mathrm{N}) \to \mathrm{E}$ which maps the cusp at $\infty$ to the origin of E (see [BCDT01] and [Wil95]). Let $\mathcal{O}_\mathrm{K}$ be the ring of integers of K. Since we have assumed that the primes dividing N (the conductor of E) split in K/$\mathbb{Q}$, we can choose an ideal $\mathcal{N}$ such that $\mathcal{O}_\mathrm{K}/\mathcal{N} \simeq \mathbb{Z}/\mathrm{N}\mathbb{Z}$. For any positive integer $\mathfrak{f}$ prime to N, we can consider $x_\mathfrak{f} = (\mathbb{C}/\mathcal{O}_\mathfrak{f}, \mathbb{C}/\mathcal{N}_\mathfrak{f}) \in \mathrm{X}_0(\mathrm{N})$, where $\mathcal{O}_\mathfrak{f}$ denotes the order of K of conductor $\mathfrak{f}$ and $\mathcal{N}_\mathfrak{f} = \mathcal{N} \cap \mathcal{O}_\mathfrak{f}$. We define the Heegner point by $y_\mathfrak{f} = \pi(x_\mathfrak{f})$. The Heegner point $y_\mathfrak{f}$ is defined over K[$\mathfrak{f}$], the ring class field of K of conductor $\mathfrak{f}$.

Let $\widetilde{\mathrm{K}}_\infty = \bigcup_{n \geq 1} \mathrm{K}[p^n]$. Then $\mathrm{Gal}(\widetilde{\mathrm{K}}_\infty/\mathrm{K})$ is isomorphic to $\mathbb{Z}_p \times \Delta$, where $\Delta$ is a finite abelian group. The unique $\mathbb{Z}_p$-extension contained in $\widetilde{\mathrm{K}}_\infty$ is the anticyclotomic $\mathbb{Z}_p$-extension $\mathrm{K}_\infty$. Denote by $\mathrm{K}[p^{k(n)}]$ the minimal ring class field of $p$-power conductor that contains $\mathrm{K}_n$, the subextension



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

of $K_\infty$ of degree $p^n$ over K. We then define $\alpha_n \in E(K_n)$ to be the trace of $y_{p^{k(n)}}$ from $K[p^{k(n)}]$ to $K_n$. Perrin-Riou [Per87, § 3.3, Lemma 2] has shown that

$$a_p y_{p^{n+1}} = y_{p^n} + \mathrm{tr}_{K[p^{n+2}]/K[p^{n+1}]} y_{p^{n+2}} \quad \text{for } n \geq 0.$$

Since we are assuming that $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q})$ is not solvable, it follows that $p \geq 5$; in conjunction with the fact that E has supersingular reduction at $p$, this implies that $a_p = 0$. We can therefore deduce that

$$\mathrm{tr}_{K_{n+2}/K_n} \alpha_{n+2} = -\alpha_n \tag{6}$$

for all $n \geq k_0 := \max\{n \in \mathbb{N} \mid K_n \subseteq K[1]\}$.

For any $n' \geq n$, let $R_{n'}\alpha_n$ denote the $R_{n'}$-submodule of $H^1(K_{n'}, E_{p^{m_{n'}}})$ generated by the image of $\alpha_n$ under the map

$$E(K_{n'}) \to H^1(K_{n'}, E_{p^{m_{n'}}}).$$

Since the group $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q})$ is not solvable, the map

$$H^1(K_n, E_{p^{m_n}}) \to H^1(K_{n'}, E_{p^{m_{n'}}}) \tag{7}$$

is injective and induces the isomorphism

$$R_n\alpha_n \simeq R_{n'}(p^{m_{n'}-m_n}\alpha_n).$$

By using

$$R_{n'}(p^{m_{n'}-m_n}\alpha_n) \subseteq R_{n'}\alpha_n \subseteq H^1(K_{n'}, E_{p^{m_{n'}}}),$$

we see that the map (7) induces the injective homomorphism

$$R_n\alpha_n \hookrightarrow R_{n'}\alpha_n.$$

Moreover, the relations (6) imply that

$$R_{n+2k}\alpha_n \subseteq R_{n+2k}\alpha_{n+2k} \subseteq H^1_{\mathrm{Sel}}(K_{n+2k}, E_{p^{m_{n+2k}}}) \subseteq H^1_{\mathrm{Sel}}(K_\infty, E_{p^\infty}),$$

where $k$ is any positive integer. Hence, we have the following maps:

$$R_{2n+1}\alpha_{2n} \hookrightarrow R_{2n'+1}\alpha_{2n'} \quad \text{and} \quad R_{2n+1}\alpha_{2n+1} \hookrightarrow R_{2n'+1}\alpha_{2n'+1},$$

which can be used as transition maps in defining the direct limits

$$\varinjlim_n R_{2n+1}\alpha_{2n} \quad \text{and} \quad \varinjlim_n R_{2n+1}\alpha_{2n+1}.$$

Since the transition maps of the above direct limits are simply restrictions of the maps (7), these direct limits are submodules of $H^1_{\mathrm{Sel}}(K_\infty, E_{p^\infty})$.

PROPOSITION 2.1. *The $\Lambda$-modules $\varinjlim_n R_{2n+1}\alpha_{2n}$ and $\varinjlim_n R_{2n+1}\alpha_{2n+1}$ have nontrivial coranks, and together they give rise to a submodule of $H^1_{\mathrm{Sel}_p}(K_\infty, E_{p^\infty})$ of corank greater than or equal to two.*

*Remark* 2.2. Observe that, while the statement of this proposition is the same as that of [ÇW08, Lemma 2.6.5], in this case we do not assume that $K_\infty/K$ is totally ramified at the primes above $p$.

*Proof.* Cornut [Cor02] and Vatsal [Vat03] have shown that all but finitely many of the Heegner points are nontorsion. Using this result, one can show (see [ÇW08, Proposition 2.5.1]) that the $\Lambda$-modules $\varinjlim_n R_{2n+1}\alpha_{2n}$ and $\varinjlim_n R_{2n+1}\alpha_{2n+1}$ have nontrivial coranks. It then follows that we can restrict our attention to the case where each of these submodules of $H^1_{\mathrm{Sel}_p}(K_\infty, E_{p^\infty})$ has



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

$\Lambda$-corank one. In this case, we will consider the restrictions of the submodules at primes above $p$ and analyze their image in the local cohomology group.

Let $\wp$ be a prime of $\mathrm{K}$ above $p$, $\wp_n$ a prime of $\mathrm{K}_n$ dividing $\wp$, $\mathrm{K}_\wp$ the completion of $\mathrm{K}$ at $\wp$, and $\mathrm{K}_{\wp_n}$ the completion of $\mathrm{K}_n$ at $\wp_n$. Following Kobayashi [Kob03], we define the following subgroups of $\mathrm{E}(\mathrm{K}_{\wp_n})$:

$$\mathrm{E}^+(\mathrm{K}_{\wp_n}) := \{x \in \mathrm{E}(\mathrm{K}_{\wp_n}) \mid \mathrm{tr}_{\mathrm{K}_{\wp_n}/\mathrm{K}_{\wp_{m+1}}}(x) \in \mathrm{E}(\mathrm{K}_{\wp_m}) \text{ for all } k_0 \leq m < n, m \text{ even}\},$$
$$\mathrm{E}^-(\mathrm{K}_{\wp_n}) := \{x \in \mathrm{E}(\mathrm{K}_{\wp_n}) \mid \mathrm{tr}_{\mathrm{K}_{\wp_n}/\mathrm{K}_{\wp_{m+1}}}(x) \in \mathrm{E}(\mathrm{K}_{\wp_m}) \text{ for all } k_0 \leq m < n,\ m \text{ odd}\}.$$

Observe that $\mathrm{res}_{\wp_{2n}}\alpha_{2n} \in \mathrm{E}^+(\mathrm{K}_{\wp_{2n}})$ and $\mathrm{res}_{\wp_{2n+1}}\alpha_{2n+1} \in \mathrm{E}^-(\mathrm{K}_{\wp_{2n+1}})$, where

$$\mathrm{res}_{\wp_n} : \mathrm{E}(\mathrm{K}_n) \to \mathrm{E}(\mathrm{K}_{\wp_n}).$$

Since the subgroups $\mathrm{E}^\pm(\mathrm{K}_{\wp_n})$ are closed under the action of $\mathrm{Gal}(\mathrm{K}_{\wp_n}/\mathrm{K}_\wp)$, they can be viewed as $\mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_n}/\mathrm{K}_\wp)]$-modules. Our aim now is to show that $\varinjlim_n \mathrm{E}^\pm(\mathrm{K}_{\wp_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, viewed as modules over $\Lambda = \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_\infty}/\mathrm{K}_\wp)]$, have corank one.

We know that the $\mathbb{Z}_p$-rank of $\mathrm{E}(\mathrm{K}_{\wp_n})$ equals that of $\mathcal{O}_{\wp_n}$, the ring of integers of $\mathrm{K}_{\wp_n}$. Since $\mathrm{E}(\mathrm{K}_{\wp_n})/(\mathrm{E}^+(\mathrm{K}_{\wp_n}) + \mathrm{E}^-(\mathrm{K}_{\wp_n}))$ is annihilated simultaneously by

$$\prod_{k_0 < 2m \leq n} \mathrm{tr}_{\mathrm{K}_{\wp_{2m}}/\mathrm{K}_{\wp_{2m-1}}} \quad \text{and} \quad \prod_{k_0 < 2m+1 \leq n} \mathrm{tr}_{\mathrm{K}_{\wp_{2m+1}}/\mathrm{K}_{\wp_{2m}}},$$

it follows that

$$p^n \mathrm{E}(\mathrm{K}_{\wp_n}) \subseteq \mathrm{E}^-(\mathrm{K}_{\wp_n}) + \mathrm{E}^+(\mathrm{K}_{\wp_n}).$$

Moreover, $\mathrm{E}^+(\mathrm{K}_{\wp_{2m+1}}) \subseteq \mathrm{E}(\mathrm{K}_{\wp_{2m}})$ and $\mathrm{E}^-(\mathrm{K}_{\wp_{2m}}) \subseteq \mathrm{E}(\mathrm{K}_{\wp_{2m-1}})$ for all $m \geq k_0$. Consequently, we can deduce the following facts about the $\mathbb{Z}_p$-ranks of $\mathrm{E}^\pm(\mathrm{K}_{\wp_n})$:

$$\mathrm{rank}_{\mathbb{Z}_p}\mathrm{E}^+(\mathrm{K}_{\wp_n}) = \mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{\wp_{k_0}} + \sum_{k_0 < 2m \leq n} (\mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{\wp_{2m}} - \mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{\wp_{2m-1}}),$$
$$\mathrm{rank}_{\mathbb{Z}_p}\mathrm{E}^-(\mathrm{K}_{\wp_n}) = \mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{\wp_{k_0}} + \sum_{k_0 < 2m+1 \leq n} (\mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{\wp_{2m+1}} - \mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{\wp_{2m}}).$$

Let $r_0 = \min\{n \in \mathbb{N} \mid \alpha_{2n} \notin \mathrm{E}(\mathrm{K}_{\wp_{2n}})_{\mathrm{tors}},\ 2n \geq k_0\}$. Then, for some $f_0(g)$ dividing $g^{k_0} - 1$, we have that

$$f_0(g) \prod_{r_0 < r \leq m} \mathrm{tr}_{\mathrm{K}_{\wp_{2r}}/\mathrm{K}_{\wp_{2r-1}}}$$

is a minimal annihilator $\mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2m}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2m}}\alpha_{2m} \subseteq \mathrm{E}^+(\mathrm{K}_{\wp_{2m}})$ and $r_0$ is by definition independent of $m$. This implies that the difference between the $\mathbb{Z}_p$-rank of $\mathrm{E}^+(\mathrm{K}_{\wp_{2m}})$ and the $\mathbb{Z}_p$-rank of its submodule $\mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2m}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2m}}\alpha_{2m}$ is bounded independently of $m$. One can draw the same conclusion about the difference between the $\mathbb{Z}_p$-ranks of $\mathrm{E}^-(\mathrm{K}_{\wp_{2m+1}})$ and $\mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2m+1}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2m+1}}\alpha_{2m+1}$. It then follows that

$$\mathrm{corank}_\Lambda \varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2n}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2n}}\alpha_{2n} \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^+(\mathrm{K}_{\wp_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \tag{8}$$
$$\mathrm{corank}_\Lambda \varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2n+1}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2n+1}}\alpha_{2n+1} \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^-(\mathrm{K}_{\wp_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p. \tag{9}$$

Since $\alpha_n$ is nontorsion for almost all $n$, the same holds for $\mathrm{res}_{\wp_n}\alpha_n$. Consequently, as in [ÇW08, Proposition 2.5.1], one can show that the modules $\varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2n}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2n}}\alpha_{2n} \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and $\varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2n+1}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2n+1}}\alpha_{2n+1} \otimes \mathbb{Q}_p/\mathbb{Z}_p$ have nontrivial $\Lambda$-coranks.

Moreover, using the fact that the maps

$$\varinjlim_n \mathrm{R}_{2n+1}\alpha_{2n} \to \varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2n}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2n}}\alpha_{2n} \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

and

$$\varinjlim_n \mathrm{R}_{2n+1}\alpha_{2n+1} \to \varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2n+1}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2n+1}}\alpha_{2n+1} \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

are surjective, together with our assumption that $\varinjlim_n \mathrm{R}_{2n+1}\alpha_{2n}$ and $\varinjlim_n \mathrm{R}_{2n+1}\alpha_{2n+1}$ have $\Lambda$-corank one, we deduce that

$$\mathrm{corank}_\Lambda \varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2n}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2n}}\alpha_{2n} \otimes \mathbb{Q}_p/\mathbb{Z}_p = 1,$$
$$\mathrm{corank}_\Lambda \varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2n+1}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2n+1}}\alpha_{2n+1} \otimes \mathbb{Q}_p/\mathbb{Z}_p = 1.$$

Hence, in view of (8) and (9), we have that

$$\mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^+(\mathrm{K}_{\wp_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^-(\mathrm{K}_{\wp_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 1.$$

Consider the exact sequence

$$0 \to \mathrm{E}^+(\mathrm{K}_{\wp_n}) + \mathrm{E}^-(\mathrm{K}_{\wp_n}) \to \mathrm{E}(\mathrm{K}_{\wp_n}) \to \mathrm{E}(\mathrm{K}_{\wp_n})/(\mathrm{E}^+(\mathrm{K}_{\wp_n}) + \mathrm{E}^-(\mathrm{K}_{\wp_n})) \to 0.$$

The last term is annihilated by $p^n$. Moreover, since $p$ is a prime of supersingular reduction and $\mathrm{K}_{\wp_n}/\mathbb{Q}_p$ is a cyclic Galois extension, we know that $\mathrm{E}(\mathrm{K}_{\wp_n})_p = 0$. Hence, by applying the snake lemma, we get

$$\begin{aligned} 0 &\to \mathrm{E}(\mathrm{K}_{\wp_n})/(\mathrm{E}^+(\mathrm{K}_{\wp_n}) + \mathrm{E}^-(\mathrm{K}_{\wp_n})) \\ &\to (\mathrm{E}^+(\mathrm{K}_{\wp_n}) + \mathrm{E}^-(\mathrm{K}_{\wp_n})) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{E}(\mathrm{K}_{\wp_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0. \end{aligned}$$

The fact that $p$ is a supersingular prime also implies that

$$\varinjlim_n \mathrm{E}(\mathrm{K}_{\wp_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq \varinjlim_n \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty})$$

under the natural inclusion maps. In addition, we know that (see [Gre01, ch. 2])

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty}) = 2[\mathrm{K}_{\wp_n} : \mathrm{K}_\wp],$$

which implies that $\varinjlim_n \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty})$ has $\Lambda$-corank two. By the above we have that

$$\varinjlim_n \mathrm{E}^+(\mathrm{K}_{\wp_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p + \varinjlim_n \mathrm{E}^-(\mathrm{K}_{\wp_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \twoheadrightarrow \varinjlim_n \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty});$$

therefore the cokernel of

$$\begin{aligned} &\varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2n}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2n}}\alpha_{2n} \otimes \mathbb{Q}_p/\mathbb{Z}_p \\ &\quad + \varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}_{\wp_{2n+1}}/\mathrm{K}_\wp)]\mathrm{res}_{\wp_{2n+1}}\alpha_{2n+1} \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \varinjlim_n \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty}) \end{aligned}$$



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

is torsion over $\Lambda$ and, consequently, the image of

$$\varinjlim_n \mathrm{R}_{2n+1}\alpha_{2n} + \varinjlim_n \mathrm{R}_{2n+1}\alpha_{2n+1} \quad \text{in} \quad \varinjlim_n \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty})$$

has $\Lambda$-corank two. Thus we can now conclude that the Heegner points give rise to a submodule of $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})$ of $\Lambda$-corank greater than or equal to two. □

**2.2** Kolyvagin used Heegner points to construct cohomology classes whose ramification can be controlled. We will now describe a natural generalization of Kolyvagin's cohomology classes to ring class fields (following [BD90]). Let $r$ be a squarefree product of primes $\ell | r$ satisfying the following conditions:

(i) $\ell$ is relatively prime to $p\mathrm{ND}_\mathrm{K}$;

(ii) $\tau \in \mathrm{Frob}_\ell(\mathrm{K}(\mathrm{E}_{p^{m_{n'}}})/\mathbb{Q})$, where $\tau$ denotes complex conjugation.

Let $k_0 \leq n \leq n'$, and denote by $\mathrm{K}_n[r]$ the maximal subextension of $\mathrm{K}_n\mathrm{K}[r]$ which is a $p$-primary extension of $\mathrm{K}_n$. We now define $\alpha_n(r)$ to be the trace of $y_{rp^{k(n)}}$ over $\mathrm{K}[rp^{k(n)}]/\mathrm{K}_n[r]$.

Let $\mathsf{G}_{n,r} = \mathrm{Gal}(\mathrm{K}_n[r]/\mathrm{K}_n[r] \cap \mathrm{K}_n\mathrm{K}[1])$ and $\mathsf{G}_{n,\ell} = \mathrm{Gal}(\mathrm{K}_n[\ell]/\mathrm{K}_n[\ell] \cap \mathrm{K}_n\mathrm{K}[1])$. By class field theory, $\mathsf{G}_{n,r} = \prod_{\ell | r} \mathsf{G}_{n,\ell}$ and $\mathsf{G}_{n,\ell} \simeq \mathbb{Z}/p^{n_\ell}\mathbb{Z}$ for $n_\ell = p^{\mathrm{ord}_p(\ell+1)}$. Consider $D_\ell := \sum_{i=1}^{n_\ell} i\sigma_\ell^i \in \mathbb{Z}/p^{m_n}\mathbb{Z}[\mathsf{G}_{n,\ell}]$ and $D_r := \prod_{\ell|r} D_\ell \in \mathbb{Z}/p^{m_n}\mathbb{Z}[\mathsf{G}_{n,r}]$ (with $D_1 := 1$). One can then show that $D_r\alpha_n(r)$ belongs to $(\mathrm{E}(\mathrm{K}_n[r])/p^{m_n})^{\mathsf{G}_{n,r}}$ (see [BD90, Lemma 3.3]). It follows that

$$\mathrm{tr}_{(\mathrm{K}_n[r] \cap \mathrm{K}_n\mathrm{K}[1])/\mathrm{K}_n} D_r\alpha_n(r) \in (\mathrm{E}(\mathrm{K}_n[r])/p^{m_n})^{\mathcal{G}_{n,r}},$$

where $\mathcal{G}_{n,r} = \mathrm{Gal}(\mathrm{K}_n[r]/\mathrm{K}_n)$. We now consider the following commutative diagram.

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & & & \mathrm{H}^1(\mathrm{K}_n[r]/\mathrm{K}_n, \mathrm{E})_{p^{m_n}} \arrow[d, "\mathrm{Inf}"] & \\
0 \arrow[r] & \mathrm{E}(\mathrm{K}_n)/p^{m_n}\mathrm{E}(\mathrm{K}_n) \arrow[r, "\phi"] \arrow[d] & \mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \arrow[r] \arrow[d, "\mathrm{res}"', "\wr"] & \mathrm{H}^1(\mathrm{K}_n, \mathrm{E})_{p^{m_n}} \arrow[r] \arrow[d, "\mathrm{res}"] & 0 \\
0 \arrow[r] & (\mathrm{E}(\mathrm{K}_n[r])/p^{m_n})^{\mathcal{G}_{n,r}} \arrow[r, "\phi_r"] & \mathrm{H}^1(\mathrm{K}_n[r], \mathrm{E}_{p^{m_n}})^{\mathcal{G}_{n,r}} \arrow[r] & \mathrm{H}^1(\mathrm{K}_n[r], \mathrm{E})_{p^{m_n}}^{\mathcal{G}_{n,r}} &
\end{tikzcd} \tag{10}$$

Let $c_n(r) \in \mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ be such that

$$\phi_r(\mathrm{tr}_{(\mathrm{K}_n[r] \cap \mathrm{K}_n\mathrm{K}[1])/\mathrm{K}_n} D_r\alpha_n(r)) = \mathrm{res}(c_n(r)),$$

and let $d_n(r)$ be the image of $c_n(r)$ in $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E})_{p^{m_n}}$. In particular, $\mathrm{res}(c_n(1)) = \phi_1(\alpha_n)$. These generalized Kolyvagin cohomology classes have the following properties.

(1) Let $-\epsilon$ denote the sign of the functional equation of the L-function of $\mathrm{E}/\mathbb{Q}$, and let $f_r$ be the number of prime divisors of $r$. After extending $\tau$ to a complex conjugation in $\mathrm{Gal}(\mathrm{K}_\infty/\mathbb{Q})$, we see that $\tau$ acts on $\alpha_n$ with $\tau\alpha_n = \epsilon g^{i_{n,1}}\alpha_n + \beta_n$, where $\beta_n \in \mathrm{E}(\mathrm{K}_n)_{\mathrm{tors}}$, $g$ is a generator of $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})$ and $i_{n,1} \in \{0, \dots, p^n - 1\}$. Moreover, the complex conjugation $\tau$ acts on $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$, and we can deduce that $\tau c_n(r) = \epsilon_r g^{i_{n,r}} c_n(r)$ where $\epsilon_r = (-1)^{f_r}\epsilon$ and $i_{n,r} \in \{0, \dots, p^n - 1\}$.



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

(2) If $v$ is a rational prime which does not divide $r$, then $d_n(r)_{v_n} = 0$ in $\mathrm{H}^1(\mathrm{K}_{v_n}, \mathrm{E})_{p^{m_n}}$ for all primes $v_n$ of $\mathrm{K}_n$ such that $v_n|v$.

(3) Let $\mathrm{H}^1(\mathrm{K}_n(\ell), \mathrm{E}_{p^{m_n}}) := \prod_{\lambda_n|\ell} \mathrm{H}^1(\mathrm{K}_{\lambda_n}, \mathrm{E}_{p^{m_n}})$ and $\mathrm{H}^1(\mathrm{K}_n(\ell), \mathrm{E})_{p^{m_n}} := \prod_{\lambda_n|\ell} \mathrm{H}^1(\mathrm{K}_{\lambda_n}, \mathrm{E})_{p^{m_n}}$. Define $\mathrm{res}_\ell$ and $\mathtt{res}_\ell$ to be the following localization maps:

$$\mathrm{res}_\ell : \mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \to \mathrm{H}^1(\mathrm{K}_n(\ell), \mathrm{E}_{p^{m_n}}),$$
$$\mathtt{res}_\ell : \mathrm{H}^1(\mathrm{K}_n, \mathrm{E})_{p^{m_n}} \to \mathrm{H}^1(\mathrm{K}_n(\ell), \mathrm{E})_{p^{m_n}}.$$

We set $\mathrm{E}(\mathrm{K}_n(\ell))/p^{m_n} := \prod_{\lambda_n|\ell} \mathrm{E}(\mathrm{K}_{\lambda_n})/p^{m_n}$. Then if $\ell|r$, there exists a $G_n$-equivariant and $\tau$-antiequivariant isomorphism

$$\psi_\ell : \mathrm{H}^1(\mathrm{K}_n(\ell), \mathrm{E})_{p^{m_n}} \to \mathrm{E}(\mathrm{K}_n(\ell))/p^{m_n}$$

such that $\psi_\ell(\mathtt{res}_\ell(d_n(r))) = \mathrm{res}_\ell(c_n(r/\ell))$.

(4) As in the case where $r = 1$ (see § 2.1), Perrin-Riou [Per87, § 3.3, Lemma 2]) has shown that

$$a_p y_{rp^{n+1}} = y_{rp^n} + \mathrm{tr}_{\mathrm{K}[rp^{n+2}]/\mathrm{K}[rp^{n+1}]} y_{rp^{n+2}}$$

for any $n \geq 0$ and any $r \in \mathbb{N}$ prime to $p$. Since $a_p = 0$, it follows that

$$y_{rp^n} = -\mathrm{tr}_{\mathrm{K}[rp^{n+2}]/\mathrm{K}[rp^{n+1}]} y_{rp^{n+2}}. \tag{11}$$

Let $\mathrm{R}_n c_n(r)$ be the $\mathrm{R}_n$-submodule of $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ generated by $c_n(r)$. Under the injective map

$$\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \to \mathrm{H}^1(\mathrm{K}_{n+2}, \mathrm{E}_{p^{m_{n+2}}}),$$

$\mathrm{R}_n c_n(r)$ can be viewed as a submodule of $\mathrm{H}^1(\mathrm{K}_{n+2}, \mathrm{E}_{p^{m_{n+2}}})$. Moreover, by (11) we can then see that $\mathrm{R}_n c_n(r) \subseteq \mathrm{R}_{n+2} c_{n+2}(r)$ and, consequently, that $\mathrm{R}_n d_n(r) \subseteq \mathrm{R}_{n+2} d_{n+2}(r)$.

By identifying $\mathrm{R}_{2n}\alpha_{2n}$ with its image under the injective map

$$\mathrm{H}^1(\mathrm{K}_{2n}, \mathrm{E}_{p^{m_{2n}}}) \to \mathrm{H}^1(\mathrm{K}_{2n+1}, \mathrm{E}_{p^{m_{2n+1}}}),$$

we now view $\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}$ as an $\mathrm{R}_{2n+1}$-submodule of $\mathrm{H}^1(\mathrm{K}_{2n+1}, \mathrm{E}_{p^{m_{2n+1}}})$.

PROPOSITION 2.3. *For almost all $n \in \mathbb{N}$, there exists a set of rational primes*

$$\mathrm{Q}_n = \{\ell_n(1), \ldots, \ell_n(t)\}$$

*satisfying the following properties:*

(i) *$\ell_n(i)$ is inert in $\mathrm{K}/\mathbb{Q}$;*

(ii) *$\ell_n(i)$ is prime to $p\mathrm{N}$;*

(iii) *$\mathrm{E}(\mathrm{K}_\lambda)_{p^\infty} = \mathrm{E}(\overline{\mathrm{K}_\lambda})_{p^{m_n}}$ for all $\lambda \mid \ell_n(i)$, where $\mathrm{K}_\lambda$ denotes the completion of $\mathrm{K}$ at $\lambda$;*

(iv) *$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{m_n}}) \hookrightarrow \prod_{i=1}^t \mathrm{H}^1(\mathrm{K}_{\lambda_n(i)}, \mathrm{E}_{p^{m_n}})$;*

(v) *the images of $\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}$ under*

$$\mathrm{res}_{\ell_m(i)} : \mathrm{H}^1(\mathrm{K}_{2n+1}, \mathrm{E}_{p^{m_{2n+1}}}) \to \mathrm{H}^1(\mathrm{K}_{2n+1}(\ell_m(i)), \mathrm{E}_{p^{m_{2n+1}}})$$

*are isomorphic as $\mathrm{R}_{2n+1}$-modules for all $m \geq 2n+1$;*

(vi) *the direct limits*

$$\varinjlim_n \mathrm{res}_{\ell_{2n+1}(i)}(\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}),$$

*which will be defined using injective transition maps, have $\Lambda$-corank two for each $i \in \{1, \ldots, t\}$.*



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

*Proof.* Let $L_n = K(E_{p^{m_n}})$ and $\mathscr{G}_n = \mathrm{Gal}(L_n/K)$. Consider the exact sequence

$$0 \to H^1(\mathscr{G}_n, E_{p^{m_n}}) \to H^1(K, E_{p^{m_n}}) \xrightarrow{\mathrm{res}} H^1(L_n, E_{p^{m_n}})^{\mathscr{G}_n}. \tag{12}$$

Since $H^1(\mathscr{G}_n, E_{p^{m_n}}) = 0$ for all $n$ [ÇW08, Proposition 1.3.1], the above diagram implies that

$$H^1(K, E_{p^{m_n}}) \hookrightarrow H^1(L_n, E_{p^{m_n}})^{\mathscr{G}_n} = \mathrm{Hom}_{\mathscr{G}_n}(\mathrm{Gal}(\overline{L}_n/L_n), E_{p^{m_n}}).$$

Let $M_n$ be the splitting field over $L_n$ of the finite subgroup $H^1_{\mathrm{Sel}}(K, E_{p^{m_n}})$ of $H^1(L_n, E_{p^{m_n}})^{\mathscr{G}_n}$. The complex conjugation $\tau$ acts on $\mathrm{Gal}(M_n/L_n)$ and the $+1$ eigenspace

$$\mathrm{Gal}(M_n/L_n)^+ = \{(\tau h)^2 \mid h \in \mathrm{Gal}(M_n/L_n)\}.$$

Fix $\{h_n(1), \ldots, h_n(t)\}$ to be a minimal set of generators of $\mathrm{Gal}(M_n/L_n)^+$. One can easily see that $t$ does not depend on $n$. We then choose primes $\ell_n(i) \in \mathbb{Q}$ such that $\tau h'_n(i) \in \mathrm{Frob}_{\ell_n}(M_n/\mathbb{Q})$, where $h_n(i) = (\tau h'_n(i))^2$. This choice ensures that the prime $\ell_n(i)$ satisfies the first two required properties.

In [ÇW08, § 1.3.2] we showed that $M_n$ and $L_{n+1}$ are disjoint over $L_n$. We also know that the index of $\mathrm{Gal}(L_n/K)$ in $\mathrm{GL}(2, \mathbb{Z}/p^{m_n}\mathbb{Z})$ is finite and depends only on E and K (see [Ser72]). This implies that, for almost all $n$, we can extend each $\tau h'_n(i)$ to an element of $\mathrm{Gal}(M_n K(E_{p^{m_{n+1}}})/\mathbb{Q})$ in such a way that the restriction of $(\tau h'_n(i))^2$ to $\mathrm{Gal}(K(E_{p^{m_{n+1}}})/L_n)$ has no fixed points in $E_{p^{m_{n+1}}}/E_{p^{m_n}}$. Hence we have

$$E(K_\lambda)_{p^\infty} = E(\overline{K_\lambda})_{p^{m_n}} \quad \text{where } \lambda \mid \ell_n(i) \text{ and } i \in \{1, \ldots, t\}.$$

Observe that if $s \in H^1_{\mathrm{Sel}}(K, E_{p^{m_n}})$ is an eigenvector of the complex conjugation $\tau$ and if, viewed as an element of $\mathrm{Hom}_{\mathscr{G}_n}(\mathrm{Gal}(\overline{L}_n/L_n), E_{p^{m_n}})$, it is trivial on $\mathrm{Gal}(M_n/L_n)^+$, then $s(\mathrm{Gal}(M_n/L_n))$ is a $\mathscr{G}_n$-invariant submodule of one of the eigenspaces of $E_{p^{m_n}}$. Since we have assumed that $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q})$ is not solvable, it follows that $s(\mathrm{Gal}(M_n/L_n)) = 0$. Hence, by the choice of $\{h_n(1), \ldots, h_n(t)\}$, we know that if $s \in H^1_{\mathrm{Sel}}(K, E_{p^{m_n}})^\pm$ and $s(h_n(i)) = 0$ for all $i \in \{1, \ldots, t\}$, then $s = 0$. By [Gro91, Proposition 9.6] and [ÇW08, Proposition 2.4.2], we have that for any $s \in H^1_{\mathrm{Sel}}(K, E_{p^{m_n}})$,

$$\mathrm{res}_{\lambda_n(i)} s = 0 \quad \text{if and only if } s(h_n(i)) = 0.$$

Since $H^1_{\mathrm{Sel}}(K, E_{p^{m_n}})$ is the direct sum of its eigenspaces under the action of $\tau$, we can conclude that the map

$$H^1_{\mathrm{Sel}}(K, E_{p^{m_n}}) \to \prod_{i=1}^{t} H^1(K_{\lambda_n(i)}, E_{p^{m_n}})$$

is injective. We have now shown that the set $Q_n = \{\ell_n(1), \ldots, \ell_n(t)\}$ satisfies the first four properties.

We shall now refine the choice of primes in $Q_n$ to ensure that the last two properties are satisfied. Let $h_n \in \mathrm{Gal}(\overline{L_n}/K_n L_n)$. In [ÇW08, § 2.5.2] we defined the $R_n$-module $[R_n\alpha_n](h_n)$ as follows:

$$[R_n\alpha_n](h_n) = \left\{ \sum_{i=1}^{p^{2n}} [(g^{-i}c)(h_n)] \cdot g^i \text{ such that } c \in R_n\alpha_n \right\} \subseteq \mathrm{Hom}_{\mathrm{sets}}(G_n, E_{p^{m_n}}),$$

where $G_n = \langle g \rangle$ and $[(g^{-i}c)(h_n)] \in E_{p^{m_n}}$ is simply the evaluation of the class $g^{-i}c$ at $h_n \in \mathrm{Gal}(\overline{K_n(E_{p^{m_n}})}/K_n(E_{p^{m_n}}))$. The action of $G_n$ on this module is the one induced by the standard action on $\mathrm{Hom}_{\mathrm{sets}}(G_n, E_{p^{m_n}})$, namely by multiplication on $G_n$, $(gf)(g_1) = f(gg_1)$. The map

$R_n\alpha_n \to [R_n\alpha_n](h_n)$ is seen to be an $R_n$-module homomorphism. By picking a basis for $E_{p^{m_n}}$, we view the right-hand side as ${R_n}^2$ and hence view $[R_n\alpha_n](h_n)$ as a submodule of ${R_n}^2$.

By [ÇW08, Lemma 2.5.3], we know that $K_\infty$ and $L_n$ are disjoint over K. Since we are assuming that $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q})$ is not solvable, it follows that $M_n$ and $K_n$ are disjoint over K. Hence we can assume that $h_n(i) \in \mathrm{Gal}(\overline{L_n}/K_nL_n)$. Then, by [ÇW08, Proposition 2.5.7], we know that

$$\mathrm{res}_{\ell_n(i)}(R_n\alpha_n) \simeq [R_n\alpha_n](h_n(i)) \text{ as } R_n\text{-modules.}$$

Let $(h_n(i))_{n\in\mathbb{N}} \in \mathrm{Gal}(\overline{L_\infty}/L_\infty)$, where $h_n(i) \in \mathrm{Gal}(\overline{L_n}/K_nL_n)$ and $i \in \{1, \ldots, t\}$. As above, we have that

$$\mathrm{res}_{\ell_m(i)}(R_n\alpha_n) \simeq [R_n\alpha_n](h_m(i)) \quad \text{for all } m \geq n$$

and, moreover, the compatibility of $h_n(i) \in \mathrm{Gal}(\overline{L_n}/K_nL_n)$ implies that

$$[R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1}](h_{2n+1}(i)) = [R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1}](h_m(i)) \quad \text{for all } m \geq 2n+1.$$

Hence we have

$$\begin{aligned}\mathrm{res}_{\ell_{2n+1}(i)}(R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1}) &\simeq [R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1}](h_{2n+1}(i))\\ &= [R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1}](h_m(i))\\ &\simeq \mathrm{res}_{\ell_m(i)}(R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1})\end{aligned}$$

for all $m \geq 2n+1$. This concludes the proof of part (v) of this proposition.

By the compatibility of $h_n(i) \in \mathrm{Gal}(\overline{L_n}/K_nL_n)$ and the fact that $R_n\alpha_n \hookrightarrow R_{n+2}\alpha_{n+2}$ under the map

$$H^1(K_n, E_{p^{m_n}}) \to H^1(K_{n+2}, E_{p^{m_{n+2}}}),$$

we have that

$$[R_n\alpha_n](h_n(i))) = [R_n\alpha_n](h_{n+2}(i)) \hookrightarrow [R_{n+2}\alpha_{n+2}](h_{n+2}(i)) \quad \text{for every } n \in \mathbb{N}.$$

By choosing the basis of $E_{p^{m_n}}$ compatibly as $n$ grows, we can consider the direct limit $\varinjlim_n [R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1}](h_{2n+1}(i))$ and view it as a $\Lambda$-submodule of $\hat{\Lambda}^2$.

By observing that the diagram

$$\begin{tikzcd} R_n\alpha_n \arrow[r] \arrow[d] & {[R_n\alpha_n](h_n(i))} \arrow[d] \\ R_{n+2}\alpha_{n+2} \arrow[r] & {[R_{n+2}\alpha_{n+2}](h_{n+2}(i))} \end{tikzcd}$$

is commutative, we deduce that there is the following surjective map of $\Lambda$-modules:

$$\psi : \varinjlim_n (R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1}) \to \varinjlim_n [R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1}](h_{2n+1}(i)).$$

In [ÇW08, § 2.6.4], we used the first property of Kolyvagin's classes and the fact that the module $\varinjlim_n (R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1})$ has $\Lambda$-corank at least two (Proposition 2.1) to show that we can choose $(h_n(i))_{n\in\mathbb{N}} \in \mathrm{Gal}(\overline{L_\infty}/L_\infty)$ such that:

(i) $h_n(i) \in \mathrm{Gal}(\overline{L_n}/K_nL_n)$ and the restriction of $h_n(i)$ to $M_n$ lies in $\mathrm{Gal}(M_n/L_n)^+$;

(ii) $\langle h_n(1), \ldots, h_n(t)\rangle = \mathrm{Gal}(M_n/L_n)^+$;



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

(iii) the invariants of $f \varinjlim_n [\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}](h_{2n+1}(i))$ contain a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^2$ for all $f \in \Lambda$, which implies that $\varinjlim_n [\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}](h_{2n+1}(i))$ has $\Lambda$-corank two.

By part (v), we have the following diagram.

$$\begin{tikzcd}
\mathrm{res}_{\ell_{2n+1}(i)}(\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}) \arrow[r, "\simeq"] & {[\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}](h_{2n+1}(i))} \arrow[d, hook] \\
\mathrm{res}_{\ell_{2n+3}(i)}(\mathrm{R}_{2n+2}\alpha_{2n+2} + \mathrm{R}_{2n+3}\alpha_{2n+3}) \arrow[r, "\simeq"] & {[\mathrm{R}_{2n+2}\alpha_{2n+2} + \mathrm{R}_{2n+3}\alpha_{2n+3}](h_{2n+3}(i))}
\end{tikzcd} \tag{13}$$

This allows us to see that we can define injective maps

$$\mathrm{res}_{\ell_{2n+1}(i)}(\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}) \hookrightarrow \mathrm{res}_{\ell_{2n+3}(i)}(\mathrm{R}_{2n+2}\alpha_{2n+2} + \mathrm{R}_{2n+3}\alpha_{2n+3}) \tag{14}$$

which transform (13) into a commutative diagram. We use the above maps to construct the direct limit $\varinjlim_n \mathrm{res}_{\ell_{2n+1}(i)}(\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1})$, and then we have that

$$\varinjlim_n \mathrm{res}_{\ell_{2n+1}(i)}(\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}) \simeq \varinjlim_n [\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}](h_{2n+1}(i)).$$

It follows that the formal direct limit $\varinjlim_n \mathrm{res}_{\ell_{2n+1}(i)}(\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1})$ has $\Lambda$-corank two for each $i \in \{1, \dots, t\}$. Hence the set $\mathrm{Q}_n$ satisfies all the required properties. $\square$

## 3. The $\Lambda$-corank of the Tate–Shafarevich group

We will now use Kolyvagin's classes to analyze the image of the map

$$\mathrm{H}^1{}_{\mathrm{Sel}_{p\cup \mathrm{Q}_{k_{2n+1}}}}(\mathrm{K}_{2n+1}, \mathrm{E}_{p^{m_{2n+1}}}) \to \prod_{q \in \mathrm{Q}_{k_{2n+1}}} \mathrm{H}^1(\mathrm{K}_{2n+1}(q), \mathrm{E})_{p^{m_{2n+1}}}, \tag{15}$$

where $\mathrm{Q}_n$ is the set of primes chosen in Proposition 2.3. Using properties (2) and (3) of Kolyvagin's classes, we can see that the image of

$$\begin{aligned} &\mathrm{R}_{2n}c_{2n}(\ell_{k_{2n+1}}(1)) + \mathrm{R}_{2n+1}c_{2n+1}(\ell_{k_{2n+1}}(1)) + \cdots + \mathrm{R}_{2n}c_{2n}(\ell_{k_{2n+1}}(t)) \\ &\quad + \mathrm{R}_{2n+1}c_{2n+1}(\ell_{k_{2n+1}}(t)) \subseteq \mathrm{H}^1{}_{\mathrm{Sel}_{p\cup \mathrm{Q}_{k_{2n+1}}}}(\mathrm{K}_{2n+1}, \mathrm{E}_{p^{m_{2n+1}}}) \end{aligned}$$

under the map (15) is

$$\prod_{i=1}^{t} \mathtt{res}_{\ell_{k_{2n+1}}(i)}[\mathrm{R}_{2n}d_{2n}(\ell_{k_{2n+1}}(i)) + \mathrm{R}_{2n+1}d_{2n+1}(\ell_{k_{2n+1}}(i))].$$

We know that the maps $\psi_{\ell_{k_{2n+1}}(i)}$, from property (3) of Kolyvagin's classes, induce the isomorphisms

$$\mathtt{res}_{\ell_{k_{2n+1}}(i)}[\mathrm{R}_{2n}d_{2n}(\ell_{k_{2n+1}}(i)) + \mathrm{R}_{2n+1}d_{2n+1}(\ell_{k_{2n+1}}(i))] \simeq \mathrm{res}_{\ell_{k_{2n+1}}(i)}[\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}]$$



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press

for each $i = 1, \ldots, t$. We now use the maps (14) to define the injective maps

$$\begin{aligned}&\mathtt{res}_{\ell_{k_{2n+1}}(i)}[\mathrm{R}_{2n}d_{2n}(\ell_{k_{2n+1}}(i)) + \mathrm{R}_{2n+1}d_{2n+1}(\ell_{k_{2n+1}}(i))]\\ &\quad\hookrightarrow \mathtt{res}_{\ell_{k_{2n+3}}(i)}[\mathrm{R}_{2n+2}d_{2n+2}(\ell_{k_{2n+3}}(i)) + \mathrm{R}_{2n+3}d_{2n+3}(\ell_{k_{2n+3}}(i))],\end{aligned}$$

which can be used as transition maps in defining the direct limit

$$\varinjlim_{n} \mathtt{res}_{\ell_{k_{2n+1}}(i)}[\mathrm{R}_{2n}d_{2n}(\ell_{k_{2n+1}}(i)) + \mathrm{R}_{2n+1}d_{2n+1}(\ell_{k_{2n+1}}(i))].$$

We can immediately see that

$$\begin{aligned}&\varinjlim_{n} \mathtt{res}_{\ell_{k_{2n+1}}(i)}[\mathrm{R}_{2n}d_{2n}(\ell_{k_{2n+1}}(i)) + \mathrm{R}_{2n+1}d_{2n+1}(\ell_{k_{2n+1}}(i))]\\ &\quad\simeq \varinjlim_{n} \mathrm{res}_{\ell_{2n+1}(i)}(\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1}).\end{aligned}$$

Since, by Proposition 2.3(v), the $\Lambda$-modules $\varinjlim_{n} \mathrm{res}_{\ell_{2n+1}(i)}(\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1})$ have corank two, it follows that the formal direct limit

$$\varinjlim_{n} \mathtt{res}_{\ell_{k_{2n+1}}(i)}[\mathrm{R}_{2n}d_{2n}(\ell_{k_{2n+1}}(i)) + \mathrm{R}_{2n+1}d_{2n+1}(\ell_{k_{2n+1}}(i))]$$

has $\Lambda$-corank two for each $i \in \{1, \ldots, t\}$. The fact that all the transition maps that we are using are injective implies that the image of the formal map $\theta$ (see § 1) has corank $2t$, even if the modules $\varinjlim_{n} \mathrm{res}_{\ell_{k_{2n+1}}(i)}(\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1})$ cannot be viewed as submodules of the image of $\theta$. It then follows that the kernel of $\theta$ has $\Lambda$-corank two. Proposition 1.3 implies that we have now proven the following theorem.

THEOREM 3.1. *The $\Lambda$-module $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})$ has corank two.*

By Proposition 2.1, we know that the image of $\mathrm{E}(\mathrm{K}_\infty)$ in $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})$ has $\Lambda$-corank at least two. Hence Theorem 3.1 implies this corollary.

COROLLARY 3.2. *The $\Lambda$-module $\mathrm{E}(\mathrm{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ has corank two.*

Then, the exactness of the sequence

$$0 \to \mathrm{E}(\mathrm{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty}) \to Ш(\mathrm{K}_\infty, \mathrm{E})_{p^\infty} \to 0$$

implies that the $\Lambda$-corank of $Ш(\mathrm{K}_\infty, \mathrm{E})_{p^\infty}$ is trivial. This concludes the proof of Theorem 0.1.

## ACKNOWLEDGEMENTS

The author would like to thank her thesis advisor, Andrew Wiles, for introducing her to ideas and methods used in this paper. She would also like to thank Christophe Cornut and Byoung Du Kim for several useful conversations.

## REFERENCES

Ber95 M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions*, Compositio Math. **99** (1995), 153–182.

BD90 M. Bertolini and H. Darmon, *Kolyvagin's descent and Mordell–Weil groups over ring class fields*, J. Reine Angew. Math. **412** (1990), 63–74.

BCDT01 C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939 electronic.

ÇW08 M. Çiperiani and A. Wiles, *Solvable points on genus one curves*, Duke Math. J. **142** (2008), 381–464.

Cor02 C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), 495–523.

Gre01 R. Greenberg, *Introduction to Iwasawa theory for elliptic curves*, in *Arithmetic algebraic geometry (Park City, Utah, 1999)*, IAS/Park City Mathematical Series, vol. 9 (American Mathematical Society, Providence, RI, 2001), 407–464.

Gro91 B. H. Gross, *Kolyvagin's work on modular elliptic curves*, in *L-functions and arithmetic (Durham, 1989)*, London Math. Soc. Lecture Note Series, vol. 153 (Cambridge University Press, Cambridge, 1991), 235–256 11G10 (11G40).

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

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

Kur02 M. Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I*, Invent. Math. **149** (2002), 195–224.

Per87 B. Perrin-Riou, *Fonctions Lp-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), 399–456.

Pol05 R. Pollack, *An algebraic version of a theorem of Kurihara*, J. Number Theory **110** (2005), 164–177.

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

Rub88 K. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **93** (1988), 701–713.

Sch85 P. Schneider, *p-adic height pairings. II*, Invent. Math. **79** (1985), 329–374.

Ser72 J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

Vat03 V. Vatsal, *Special values of anticyclotomic L-functions*, Duke Math. J. **116** (2003), 219–261.

Wil95 A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443–551.

Mirela Çiperiani mirela@math.columbia.edu
Mathematics Department, Columbia University, 2990 Broadway, New York, NY 10027, USA



https://doi.org/10.1112/S0010437X08003874 Published online by Cambridge University Press