Compositio Math. 143 (2007) 47–72
doi:10.1112/S0010437X06002569

The parity conjecture for elliptic curves at supersingular reduction primes

Byoung Du (B. D.) Kim

Abstract

In number theory, the Birch and Swinnerton-Dyer (BSD) conjecture for a Selmer group relates the corank of a Selmer group of an elliptic curve over a number field to the order of zero of the associated L-function $L(E, s)$ at $s = 1$. We study its modulo two version called the parity conjecture. The parity conjecture when a prime number p is a good ordinary reduction prime was proven by Nekovar. We prove it when a prime number $p > 3$ is a good supersingular reduction prime.

1. Introduction

In number theory and arithmetic geometry, we often expect an algebraic aspect and an analytic aspect to be closely related. A classic example is the Birch and Swinnerton-Dyer (BSD) conjecture. The BSD conjecture predicts a precise relation between the Mordell–Weil group and the L-function of an elliptic curve. Its statement is given in the following.

Conjecture 1 (BSD conjecture). Suppose that $E/\mathbb{Q}$ is an elliptic curve defined over $\mathbb{Q}$. Then we expect

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

Another conjecture closely related to the BSD conjecture is the BSD conjecture for a Selmer group. The Selmer group of an elliptic curve is a subgroup of a cohomology group associated to the torsion points of the elliptic curve, and the Shafarevich–Tate conjecture predicts that its corank is equal to the rank of $E(\mathbb{Q})$. The BSD conjecture for a Selmer group is stated as follows.

Conjecture 2 (BSD conjecture for a Selmer group). Let p be a prime number and E an elliptic curve defined over $\mathbb{Q}$. We let $\mathrm{Sel}_p(E/\mathbb{Q})$ denote the p-Selmer group of E over $\mathbb{Q}$, then we expect

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/\mathbb{Q}) = \mathrm{ord}_{s=1}L_{/\mathbb{Q}}(E, s).$$

We consider the modulo two version of the BSD conjecture for a Selmer group, namely the parity conjecture.

Conjecture 3 (Parity conjecture). Let p be a prime number and E an elliptic curve defined over $\mathbb{Q}$. We expect

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/\mathbb{Q}) \equiv \mathrm{ord}_{s=1}L_{/\mathbb{Q}}(E, s) \pmod 2.$$

Note that this conjecture depends on the prime number p (as does Conjecture 2). Although we focus on this conjecture throughout this paper, we can state the BSD conjecture and the parity

Received 1 August 2005, accepted in final form 2 August 2006.
2000 Mathematics Subject Classification 11G05.
Keywords: elliptic curve, BSD conjecture, Iwasawa theory.

conjecture for any number field F in the same way, which we will call the BSD conjecture for F and the parity conjecture for F, respectively. The parity conjecture for a good ordinary reduction prime p was proven by Nekovar (see [Nek01]). He also proved in [Nek06a, ch. 12] that the parity conjecture for a totally real number field F holds if every prime of F lying above p is a good ordinary reduction prime under appropriate conditions. It was difficult to apply his method to prove the conjecture for a good supersingular prime because a p-Selmer group does not behave nicely in that case. In this paper, we overcome this difficulty and prove the parity conjecture when $p > 3$ is a good supersingular reduction prime.

First we generalize norm coherent points of the formal group associated to the elliptic curve. These points were studied first by Kobayashi in [Kob03] and generalized by Iovita and Pollack [IP06]. We generalize the idea further to a totally ramified $\mathbb{Z}_p$-extension of an unramified local field given by torsion points of a relative Lubin–Tate group of height 1. Then we construct a local condition using these points and show that this local condition satisfies self-duality under the Tate local pairing.

Once it is proven, the rest of paper follows standard Iwasawa theory techniques and Nekovar's idea very closely to prove the parity conjecture.

It is natural to try to apply the same idea to the parity conjecture for a totally real field. The result in this direction under some strong conditions will be published in a subsequent paper.

Notation 1.1. Throughout this paper, $\mathrm{Hom}(A, B)$ denotes a set of $\mathbb{Z}_p$-linear continuous homomorphisms from A to B unless stated otherwise.

2. Galois cohomology

Let F be a finite Galois extension of a number field K and $\mathfrak{p}$ be a prime of K. Fix an embedding $\bar{K} \to \mathbb{C}_p$. This embedding induces a prime $\mathfrak{P}$ of F lying above $\mathfrak{p}$. We choose a subset S of $G_K = \mathrm{Gal}(\bar{K}/K)$ such that $\{\mathfrak{P}^g\}_{g\in S}$ is the set of all distinct primes of F lying above $\mathfrak{p}$.

Let C be a G_K-module which is a finite $\mathbb{Z}_p$-module. There is a map between H^0 groups

$$\begin{aligned} C^{G_{K_\mathfrak{p}}} &\to \bigoplus_{g\in S} C^{G_{F_{\mathfrak{P}^g}}} \\ x &\mapsto \bigoplus_{g\in S} (g \cdot x). \end{aligned}$$

Then for a G_K-module B which is a finite $\mathbb{Z}_p$-module, the map above induces the following:

$$\mathrm{Res} : H^i(K_\mathfrak{p}, B) \to \bigoplus_{g\in S} H^i(F_{\mathfrak{P}^g}, B).$$

Similarly, a map between H^0 groups

$$\begin{aligned} \bigoplus_{g\in S} C^{G_{F_{\mathfrak{P}^g}}} &\to C^{G_{K_\mathfrak{p}}} \\ \bigoplus_{g\in S} x_g &\mapsto \sum_{g\in S} N_{F_\mathfrak{P}/K_\mathfrak{p}}(g^{-1} \cdot x_g). \end{aligned}$$

induces

$$\mathrm{Cor} : \bigoplus_{g\in S} H^i(F_{\mathfrak{P}^g}, B) \to H^i(K_\mathfrak{p}, B).$$

Since we can check $\mathrm{Res} \circ \mathrm{Cor} = N_{F/K}$ for H^0 groups, we have the following.

Proposition 2.1. *We have* $\mathrm{Res} \circ \mathrm{Cor} = N_{F/K}$ *on* $\bigoplus_{g\in S} H^i(F_{g\mathfrak{P}}, B)$.

Now we study a Shapiro map of cohomology groups.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

DEFINITION 2.2. We always let G_K act on $\mathrm{Hom}(\cdot,\cdot)$ by $(\gamma\cdot f)(x)=\gamma(f(\gamma^{-1}x))$ for $\gamma\in G_K$. If D_1 and D_2 are $\mathrm{Gal}(F/K)$-modules, we let $\mathrm{Gal}(F/K)$ act on $\mathrm{Hom}(D_1,D_2)$ in the same way. On the other hand, we always let $\mathbb{Z}_p[\mathrm{Gal}(F/K)]$ act on $\mathrm{Hom}(\mathbb{Z}_p[\mathrm{Gal}(F/K)],\cdot)$ by right multiplication on $\mathbb{Z}_p[\mathrm{Gal}(F/K)]$, i.e. for $a\in\mathbb{Z}_p[\mathrm{Gal}(F/K)]$ and $f\in\mathrm{Hom}(\mathbb{Z}_p[\mathrm{Gal}(F/K)],\cdot)$,

$$(a\cdot f)(b)=f(ba).$$

Let C be a finite G_K-module which is a finite $\mathbb{Z}_p$-module. We define the following map between H^0:

$$\begin{aligned}\mathrm{Hom}(\mathbb{Z}_p[\mathrm{Gal}(F/K)],C)^{G_{K_\mathfrak{p}}} &\to \bigoplus_{g\in S} C^{G_{F_{\mathfrak{P}^g}}}\\ \psi &\mapsto \bigoplus_{g\in S}(g\circ\psi)(1).\end{aligned}$$

Then the Shapiro map between H^1 groups follows:

$$Sh : H^1(K_\mathfrak{p},\mathrm{Hom}(\mathbb{Z}_p[\mathrm{Gal}(F/K)],B))\to\bigoplus_{g\in S}H^1(F_{\mathfrak{P}^g},B).$$

From the definition of Galois cohomology we can see that $\mathrm{Gal}(F/K)$ acts on $\bigoplus_{g\in S}H^1(F_{\mathfrak{P}^g},B)$ as well, so we can consider it as a $\mathbb{Z}_p[\mathrm{Gal}(F/K)]$-module. Then we can check that Sh is a $\mathbb{Z}_p[\mathrm{Gal}(F/K)]$-isomorphism.

Remark 2.3. The definition of the Shapiro map differs depending on the source. For example, the definition of [Rub00, Appendix B.4] uses $\mathrm{Ind}_H(\cdot)$ instead of $\mathrm{Hom}(\mathbb{Z}_p[\mathrm{Gal}(F/K)],\cdot)$. We can check that it is equivalent to our definition.

DEFINITION 2.4. The map

$$i:\bigoplus_{g\in S}H^1(F_{\mathfrak{P}^g},\mathrm{Hom}(\mathbb{Z}_p[\mathrm{Gal}(F/K)],B))\to\mathrm{Hom}\left(\mathbb{Z}_p[\mathrm{Gal}(F/K)],\bigoplus_{g\in S}H^1(F_{\mathfrak{P}^g},B)\right)$$

is defined in the natural way.

We define a map

$$\begin{aligned}j:\bigoplus_{g\in S}H^1(F_{\mathfrak{P}^g},B)&\to\mathrm{Hom}\left(\mathbb{Z}_p[\mathrm{Gal}(F/K)],\bigoplus_{g\in S}H^1(F_{\mathfrak{P}^g},B)\right)\\ (x_g)&\mapsto f_x:\sigma\in\mathrm{Gal}(F/K)\mapsto\sigma\cdot(x_g).\end{aligned}$$

We obtain the following.

PROPOSITION 2.5. *The diagram*

$$\begin{array}{ccc} H^1(K_\mathfrak{p},\mathrm{Hom}(\mathbb{Z}_p[\mathrm{Gal}(F/K)],B)) & \xrightarrow{Sh} & \bigoplus_{g\in S}H^1(F_{\mathfrak{P}^g},B)\\ \downarrow\mathrm{Res} & & \downarrow j\\ \bigoplus_{g\in S}H^1(F_{\mathfrak{P}^g},\mathrm{Hom}(\mathbb{Z}_p[\mathrm{Gal}(F/K)],B)) & \xrightarrow{i} & \mathrm{Hom}(\mathbb{Z}_p[\mathrm{Gal}(F/K)],\bigoplus_{g\in S}H^1(F_{\mathfrak{P}^g},B))\end{array}$$

is commutative. The image of j is

$$\mathrm{Hom}\left(\mathbb{Z}_p[\mathrm{Gal}(F/K)],\bigoplus_{g\in S}H^1(F_{\mathfrak{P}^g},B)\right)^{\mathrm{Gal}(F/K)}.$$

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Proof. The commutativity of the diagram follows from the commutativity for a similar diagram for H^0 groups. The image of j is easy to figure out. □

Now we suppose that $\mathfrak{p}$ is unramified over F/K.

Definition 2.6. The same Shapiro map induces

$$Sh : H^1(K_{\mathfrak{p}}^{ur}/K_{\mathfrak{p}}, \mathrm{Hom}(\mathbb{Z}_p[\mathrm{Gal}(F/K)], B^{I_{K_{\mathfrak{p}}}})) \to \prod_S H^1(F_{\mathfrak{P}^g}^{ur}/F_{\mathfrak{P}^g}, B^{I_{F_{\mathfrak{P}^g}}}).$$

We can check that Sh is an isomorphism.

Although our propositions are stated for a finite extension F/K and a finite module B, they are true for any profinite extension F/K (for instance, a $\mathbb{Z}_p$-extension) and any discrete $\mathbb{Z}_p$-module B by passing them to a direct limit.

3. Plus/minus-local conditions

3.1 $\pm$-Coleman maps

We suppose that p is an odd prime number greater than 3. Assume that $E/\mathbb{Q}$ has good supersingular reduction at p, and let $\hat{E}$ be the formal group over $\mathbb{Z}_p$ associated with the minimal model of E over $\mathbb{Q}_p$. In this section we assume the following:

(A) k is an unramified extension of $\mathbb{Q}_p$ of degree d and k_∞ is a totally ramified extension of k with $\mathrm{Gal}(k_\infty/k) \cong \mathbb{Z}_p$.

We let k_n denote the subfield of k_∞ with $\mathrm{Gal}(k_n/k) \cong \mathbb{Z}/p^n\mathbb{Z}$ and write $G_n = \mathrm{Gal}(k_n/k)$. We let m_n denote the maximal ideal of k_n and let $m_{-1} = m_0$.

Proposition 3.1. *For any n, $\hat{E}(m_n)$ is torsion-free.*

Proof. We can prove this in the same way that [Kob03, Proposition 8.7] is proven. □

Suppose that there are given $c_{n,i} \in \hat{E}(m_n)$ for every $i = 0, 1, \ldots, d-1$ and $n \geqslant -1$ such that $Tr_{n/n-1} c_{n,i} = -c_{n-2,i}$ for every $n \geqslant 1$.

Define $c_{0,i}^+ = -c_{0,i}, c_{1,i}^+ = -c_{0,i}, c_{2,i}^+ = c_{2,i}, c_{3,i}^+ = c_{2,i}, \ldots$, and $c_{0,i}^- = c_{-1,i}, c_{1,i}^- = -c_{1,i}, c_{2,i}^- = -c_{1,i}, c_{3,i}^- = c_{3,i}, \ldots$. Then we can note that for every $i = 0, 1, \ldots, d-1$ we have

$$\begin{aligned} Tr_{2n/2n-1} c_{2n,i}^+ &= c_{2n-1,i}^+ \quad \text{for } n \geqslant 1, \\ c_{2n-1,i}^+ &= c_{2n-2,i}^+ \quad \text{for } n \geqslant 1, \\ Tr_{2n+1/2n} c_{2n+1,i}^- &= c_{2n,i}^- \quad \text{for } n \geqslant 0, \\ c_{2n,i}^- &= c_{2n-1,i}^- \quad \text{for } n \geqslant 1. \end{aligned}$$

We let T denote the p-adic Tate module of E and A denote $E[p^\infty]$. The Kummer map $\hat{E}(m_n) \to H^1(k_n, T)$ together with the cup product of the Weil pairing induces

$$(\cdot, \cdot)_n : \hat{E}(m_n) \times H^1(k_n, T) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p.$$

For every $x = (x_i)_{i=0,\ldots,d-1} \in \hat{E}(m_n)^d$ we define a homomorphism $P_{x,n} : H^1(k_n, T) \to (\mathbb{Z}_p[G_n])^d$ by

$$P_{x,n}(z) = \left(\sum_{\sigma \in G_n} (x_i^\sigma, z)_n \sigma \right)_{i=0,\ldots,d-1}$$

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

for $z \in H^1(k_n, T)$. Since $(\cdot,\cdot)_n$ is G_n-equivariant, $P_{x,n}$ is G_n-equivariant as well. As noted in [Kob03] (also in [IP06]), for every $x_n \in \hat{E}(m_n)^d$ and $n \geqslant 1$ the following diagram

$$\begin{array}{ccc} H^1(k_n, T) & \xrightarrow{P_{x_n,n}} & (\mathbb{Z}_p[G_n])^d \\ \downarrow \mathrm{Cor} & & \downarrow \\ H^1(k_{n-1}, T) & \xrightarrow{P_{x_{n-1},n-1}} & (\mathbb{Z}_p[G_{n-1}])^d \end{array}$$

is commutative when $x_{n-1} = Tr_{n/n-1}x_n$ and the right vertical map is the natural projection.

DEFINITION 3.2. (i) Following [Kob03] and [IP06] we define

$$\hat{E}^+(m_n) := \{P \in \hat{E}(m_n) \mid Tr_{n/m+1}P \in \hat{E}(m_m) \text{ for all } 0 \leqslant m < n, m \text{ even}\},$$
$$\hat{E}^-(m_n) := \{P \in \hat{E}(m_n) \mid Tr_{n/m+1}P \in \hat{E}(m_m) \text{ for all } -1 \leqslant m < n, m \text{ odd}\}.$$

(ii) We define a subgroup $C^{\pm}(m_n)$ of $\hat{E}(m_n)$ as a $\mathbb{Z}_p[G_n]$-module generated by $c^{\pm}_{n,0}, c^{\pm}_{n,1}, \ldots, c^{\pm}_{n,d-1}$.

We also define

$$D^{\pm}(m_n) := \{P \in \hat{E}(m_n) \mid p^k P \in C^{\pm}(m_n) \text{ for some integer } k\}.$$

From the definition $\hat{E}(m_n)/D^{\pm}(m_n)$ is torsion-free. Also it is clear that $C^{\pm}(m_n) \subset \hat{E}^{\pm}(m_n)$. Moreover, we have the following.

PROPOSITION 3.3. *We have* $D^{\pm}(m_n) \subset \hat{E}^{\pm}(m_n)$.

Proof. Let Q be any point in $\hat{E}(m_n)$ such that $R = p^b Q \in C^-(m_n)$ for some $b \geqslant 0$. Since $C^-(m_n) \subset \hat{E}^-(m_n)$, we have $p^b Tr_{n/m+1}Q = Tr_{n/m+1}R \in \hat{E}(m_m)$ for every odd m with $-1 \leqslant m < n$. Thus, for any $\sigma \in \mathrm{Gal}(k_{m+1}/k_m), (Tr_{n/m+1}Q)^\sigma - (Tr_{n/m+1}Q)$ is a p^b-torsion point. Since $\hat{E}(m_{m+1})$ is torsion-free by Proposition 3.1, $(Tr_{n/m+1}Q)^\sigma - (Tr_{n/m+1}Q) = 0$, i.e. $Tr_{n/m+1}Q \in \hat{E}(m_m)$. Thus, $Q \in \hat{E}^-(m_n)$. Thus, by the definition of $D^-(m_n)$, we have $D^-(m_n) \subset \hat{E}^-(m_n)$. It is similar for $D^+(m_n)$. For a similar argument, see [Kob03, Lemma 8.17]. □

Remark 3.4. Since $\hat{E}(m_n)/D^{\pm}(m_n)$ is torsion-free, we can check whether $D^{\pm}(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \hat{E}(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is injective and $D^{\pm}(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(k_n, A)$ is injective as well.

Define $P^{\pm}_n : H^1(k_n, T) \to \mathbb{Z}_p[G_n]^d$ as $P^{\pm}_n := P_{c^{\pm}_n,n}$ for $c^{\pm}_n = (c^{\pm}_{n,i})_{i=0,\ldots,d-1} \in \hat{E}(m_n)^d$. On the other hand, define $H^1_{\pm}(k_n, T)$ as the exact annihilator of $D^{\pm}(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ with respect to the Tate local pairing

$$H^1(k_n, A) \times H^1(k_n, T) \to \mathbb{Q}_p/\mathbb{Z}_p,$$

(thus, we have $H^1(k_n, T)/H^1_{\pm}(k_n, T) \cong \mathrm{Hom}(D^{\pm}(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)$).

PROPOSITION 3.5. *We have* $\ker P^{\pm}_n = H^1_{\pm}(k_n, T)$.

Proof. By definition $\ker P^{\pm}_n = \{z \in H^1(k_n, T) \mid (x, z)_n = 0 \text{ for all } x \in C^{\pm}(m_n)\}$. If $x \in \hat{E}(m_n)$ satisfies $p^b x \in C^{\pm}(m_n)$ for some integer b, then, for every $z \in \ker P^{\pm}_n$, we have $p^b(x, z)_n = (p^b x, z)_n = 0$, thus we have $(x, z)_n = 0$. Therefore, we have

$$\ker P^{\pm}_n \subset \{z \in H^1(k_n, T) \mid (x, z)_n = 0 \text{ for all } x \in D^{\pm}(m_n)\}.$$

In fact, this is an equality because the right-hand side is already contained in the left-hand side.

Thus, we have a left exact sequence

$$0 \to \ker P^{\pm}_n \to H^1(k_n, T) \to \mathrm{Hom}(D^{\pm}(m_n), \mathbb{Z}_p) \tag{1}$$

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

where the last arrow is induced by $(\cdot,\cdot)_n$. By taking the Pontryagin dual and using the Tate local duality we have

$$D^{\pm}(m_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p \to H^1(k_n,A) \xrightarrow{(1)} (\ker P_n^{\pm})^{\vee}\to 0$$

where the left arrow is injective by Remark 3.4. We note that the map (1) is induced from the Tate local pairing. Thus, we have $\ker P_n^{\pm} = H^1_{\pm}(k_n,T)$. □

Remark 3.6. From the proof we also obtain the surjectivity of the map (1). In particular, if $D^{\pm}(m_n) = C^{\pm}(m_n)$ (as we will assume for $n=0$), it implies the exactness of

$$0\to \ker P_n^{\pm}\to H^1(k_n,T)\xrightarrow{(2)}\mathrm{Hom}(C^{\pm}(m_n),\mathbb{Z}_p)\to 0$$

where the map (2) is induced from $(\cdot,\cdot)_n$.

Next we study the image of $P_n^{\pm}$. Let $\Phi_n(X) = 1+X^{p^{n-1}}+X^{2p^{n-1}}+\cdots+X^{(p-1)p^{n-1}}$ for $n\geqslant 1$ and $\Phi_0(X)=X-1$. We let $\omega_n(X)=(X+1)^{p^n}-1$ and

$$\omega_n^{+}(X)=\prod_{0\leqslant m\leqslant n,\ m:\text{even}}\Phi_m(X+1), \omega_n^{-}(X)=\Phi_0(X+1)\prod_{1\leqslant m\leqslant n,\ m:\text{odd}}\Phi_m(X+1).$$

We let $\tilde{\omega}_n^{\pm}(X)$ satisfy $\omega_n(X)=\tilde{\omega}_n^{\mp}(X)\omega_n^{\pm}(X)$. Fix a topological generator γ of $\mathrm{Gal}(k_\infty/k)$ and let γ_n be $\gamma|_{k_n}$. We identify $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$ with $\Lambda=\mathbb{Z}_p[[X]]$ by identifying γ with $X+1$. Similarly we identify $\Lambda_n=\mathbb{Z}_p[G_n]$ with $\mathbb{Z}_p[X]/(\omega_n(X))$. Also define $\Lambda_n^{\pm}:=\mathbb{Z}_p[X]/(\omega_n^{\pm}(X))$. We can observe that $\varprojlim \Lambda_n^{-}\cong\Lambda$.

Proposition 3.7. *There exists a unique morphism $Col_n^{\pm}$ which makes the following diagram commutative.*

$$\begin{array}{ccc} H^1(k_n,T) & \xrightarrow{Col_n^{\pm}} & (\Lambda_n^{\pm})^d \\ \downarrow & & \downarrow{\scriptstyle \times\tilde{\omega}_n^{\mp}} \\ \dfrac{H^1(k_n,T)}{H^1_{\pm}(k_n,T)} & \xrightarrow{P_n^{\pm}} & {\Lambda_n}^d \end{array}$$

The right vertical map is injective, thus $\ker Col_n^{\pm}=\ker P_n^{\pm}$.

Proof. See [Kob03, Proposition 8.19 and Corollary 8.20]. □

Proposition 3.8. *The even (odd) Coleman maps are compatible for all $n\geqslant 0$:*

$$\begin{array}{ccc} H^1(k_{n+1},T) & \xrightarrow{Col_{n+1}^{\pm}} & (\Lambda_{n+1}^{\pm})^d \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Proj}} \\ H^1(k_n,T) & \xrightarrow{Col_n^{\pm}} & (\Lambda_n^{\pm})^d \end{array}$$

Proof. See [Kob03, Proposition 8.21]. □

Proposition 3.9. *If $C^{-}(m_0)=\hat{E}(m_0)$, then Col_n^{-} is surjective for every n.*

Proof. First, by the Hochschild–Serre spectral sequence the kernel of $H^1(k_0,A)\to H^1(k_n,A)$ is $H^1(k_n/k_0,A^{G_{k_n}})$, which is trivial by Proposition 3.1. Thus, by the Tate local duality $H^1(k_n,T)\to H^1(k_0,T)$ is surjective.

Second, Remark 3.6 says that the map $H^1(k_0,T)\to\mathrm{Hom}(C^{-}(m_0),\mathbb{Z}_p)$ induced by $(\cdot,\cdot)_0$ is surjective. From the assumption of the proposition we can see that $\{c_{0,0}^{-},c_{0,1}^{-},\ldots,c_{0,d-1}^{-}\}$ is a $\mathbb{Z}_p$-basis of $\hat{E}(m_0)$. Thus, we can choose $x_i\in H^1(k_0,T)$ for each $i=0,\ldots,d-1$ such that $(c_{0,i}^{-},x_i)=1$ and $(c_{0,j}^{-},x_i)=0$ for $j\neq i$.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

We note that $Col_0^- = P_0^-$. We can see that $\{Col_0^-(x_0), Col_0^-(x_1), \dots, Col_0^-(x_{d-1})\}$ generates $(\mathbb{Z}_p)^d$. Thus, $Col_0^- : H^1(k_0, T) \to (\mathbb{Z}_p)^d$ is surjective, thus, by Nakayama's lemma, so is Col_n^- for each n. □

Let $M^\vee$ denote the Pontryagin dual $\mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$.

PROPOSITION 3.10. *If $C^-(m_0) = \hat{E}(m_0)$, then we have $D^-(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p{}^\vee \cong (\Lambda_n^-)^d$. Also $(\bigcup_{n=1}^\infty D^-(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong \Lambda^d$.*

Proof. From the definition

$$\frac{H^1(k_n, T)}{H^1_-(k_n, T)} \cong \mathrm{Hom}(D^-(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

By Proposition 3.5 we have $H^1_-(k_n, T) = \ker P_n^-$ $(= \ker Col_n^-)$ and by Proposition 3.9 we have $\mathrm{Im}\, Col_n^- = (\Lambda_n^-)^d$, thus the first statement follows. The second statement follows by taking an inverse limit. □

PROPOSITION 3.11. *If $C^-(m_0) = \hat{E}(m_0)$, we have $\hat{E}^-(m_n) = D^-(m_n)$.*

Proof. We have $(D^-(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong (\Lambda_n^-)^d$, thus $\mathrm{rank}_{\mathbb{Z}_p} D^-(m_n) = \mathrm{rank}_{\mathbb{Z}_p} \hat{E}^-(m_n)$. By definition $\hat{E}^-(m_n)/D^-(m_n)$ is torsion-free, thus $\hat{E}^-(m_n) = D^-(m_n)$. □

If we assume $C^+(m_0) = \hat{E}(m_0)$, the previous three propositions hold replacing $-$ with $+$.

3.2 Norm subgroups

In addition to the assumption (A) in the previous section, we assume the following:

(B) $k_\infty/\mathbb{Q}_p$ is an abelian extension.

We want to generalize the construction of $\pm$-norm coherent points of [Kob03] and [IP06].

Put $L_0 = k$ and $L_{n+1} = k_n(\mu_p)$ for $n \geqslant 0$. For a local field M we let O_M denote the ring of integers of M and m_M the maximal ideal of O_M. In particular, let O denote $O_k(=O_{L_0})$ and m denote $m_k(=m_{L_0})$. Let ψ be the Frobenius map of $\mathrm{Gal}(k/\mathbb{Q}_p)$ characterized by $x^\psi = x^p \pmod{pO}$.

Then L_∞ is a totally ramified $\mathbb{Z}_p^\times$ extension of k, k is an unramified extension of $\mathbb{Z}_p$, and L_∞ is an abelian extension of $\mathbb{Q}_p$. We fix a valuation $v_p : \bar{\mathbb{Q}}_p^\times \to \mathbb{Q}$ such that $v_p(p) = 1$. Then the group of the universal norms of L_∞ in $\mathbb{Q}_p$ is generated by ξ with $v_p(\xi) = d$.

Let ϖ be any number in k satisfying $N_{k/\mathbb{Q}_p}(\varpi) = \xi$. Let $f(X) \in O[X]$ be any Eisenstein polynomial of degree p such that

$$f(X) \equiv X^p \pmod{p},$$
$$f(X) \equiv \varpi X \pmod{\deg 2},$$
$$\text{coefficient of } X^{p-1} = \zeta p \text{ for a root of unity } \zeta \text{ of } O.$$

Let $f^{(n)}(X)$ denote $f^{\psi^{n-1}} \circ f^{\psi^{n-2}} \circ \cdots \circ f(X)$ for $n \geqslant 1$ and put $f^{(0)}(X) = X$. From the Lubin–Tate group theory we can see that any root π of $f^{(n)}(X)$ that is not a root of $f^{(n-1)}$ is a uniformizer of m_{L_n} and also satisfies $k(\pi) = L_n$ (see [Des87, Proposition 1.8]).

We define

$$\log_F(X) := \sum_{n=0}^{\infty} (-1)^n \frac{f^{(2n)}(X)}{p^n}.$$

We can see that $\log_F'(X) \in O[[X]]$ and $\log_F(X) = a_1 X \pmod{\deg 2}$ for some $a_1 \in O^\times$. We can check

$$\log_F^{\psi^2}(f^\psi \circ f(X)) + p \log_F(X) \equiv 0 \pmod{p}.$$

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

By [Kob03, Lemma 8.1] this implies $\log_F^{\psi^2}(X^{p^2}) + p\log_F(X) \equiv 0 \pmod p$. Similarly, $\log_F^{\psi^{-n}}(X)$ for every integer n satisfies $(\log_F^{\psi^{-n}})^{\psi^2}(X^{p^2}) + p\log_F^{\psi^{-n}}(X) \equiv 0 \pmod p$.

By Honda theory (in particular, [Hon70, Theorems 2 and 4, and Propositions 2.6 and 3.5]) we can see that:

(i) there is a formal group F^n defined over O whose logarithm is given by $\log_F^{\psi^{-n}}$ (we let F denote F^0);

(ii) for any n, an integral power series $s_n = \exp_F \circ \log_F^{\psi^{-n}}(X) \in O[[X]]$ is an isomorphism $F^n \to F$;

(iii) since the Honda type of $\log_{\hat{E}}(X)$ is $t^2 + p$, the Artin–Hasse type power series $\exp_{\hat{E}} \circ \log_F^{\psi^{-n}} \in O[[X]]$ is an isomorphism $F^n \to \hat{E}$.

Let $\pi_0 = 0$. By Propositions 1.5, and 1.7 and the discussion before Proposition 1.7 of [Des87], we can see that $\{\text{roots of } (f^{(n)})^{\psi^{-n}}\} \xrightarrow{f^{\psi^{-n}}} \{\text{roots of } (f^{(n-1)})^{\psi^{-n+1}}\}$ is surjective. Thus, we can inductively choose a uniformizer π_n of m_{L_n} satisfying $f^{\psi^{-n}}(\pi_n) = \pi_{n-1}$ for $n \geqslant 1$.

On the other hand, for each $n \geqslant 0$ put

$$\begin{aligned}\lambda_n :&= \zeta^{\psi^{-(n+2)}}p - \zeta^{\psi^{-(n+4)}}p^2 + \zeta^{\psi^{-(n+6)}}p^3 - \cdots \\ &= \sum_{j=1}^{\infty}(-1)^{j-1}\zeta^{\psi^{-(n+2j)}}p^j \in m.\end{aligned}$$

Since $\log_F^{\psi^{-n}} : F^n(m) \to m$ is an isomorphism, there is $\epsilon_n \in F^n(m)$ such that $\log_F^{\psi^{-n}}(\epsilon_n) = \lambda_n$. Define $b_n \in F(m_{L_n})$ by

$$b_n = s_n(\epsilon_n[+]_{F^n}\pi_n).$$

Then we have

$$\begin{aligned}\log_F(b_n) &= \log_F^{\psi^{-n}}(\epsilon_n[+]_{F^n}\pi_n) \\ &= \lambda_n + \pi_n - \frac{\pi_{n-2}}{p} + \frac{\pi_{n-4}}{p^2} - \cdots.\end{aligned}$$

For $n \geqslant 2$

$$\begin{aligned}Tr_{L_n/L_{n-1}}(\log_F(b_n)) &= p\lambda_n - \zeta^{\psi^{-n}}p - \left[\pi_{n-2} - \frac{\pi_{n-4}}{p} + \cdots\right] \\ &= -\lambda_{n-2} - \left[\pi_{n-2} - \frac{\pi_{n-4}}{p} + \cdots\right] \\ &= -\log_F(b_{n-2}).\end{aligned}$$

We note that $\mathrm{Gal}(L_{n+1}/k) \cong \mathrm{Gal}(L_{n+1}/k_n) \times \mathrm{Gal}(k_n/k)$ and $\mathrm{Gal}(L_{n+1}/k_n) \cong \mathrm{Gal}(L_\infty/k_\infty)$ (we denote this by Δ). For $n \geqslant -1$ let $e_n = Tr_\Delta(b_{n+1}) \in F(m_{k_n})$. Since F and $\hat{E}$ are isomorphic over O, $F(m_{k_n})$ is torsion-free by Proposition 3.1 and $\log_F$ is injective on $F(m_{k_n})$ for every $n \geqslant 0$. Thus, it follows that

$$Tr_{k_n/k_{n-1}}(e_n) = -e_{n-2}$$

for $n \geqslant 1$. In particular, $e_{-1} = [p-1](b_0)$, thus $\log_F(e_{-1}) = (p-1)\lambda_0$.

Let $c_n \in \hat{E}(m_{k_n})$ be the image of e_n under the isomorphism $\exp_{\hat{E}} \circ \log_F(X)$. We obtain the following.

Proposition 3.12. *We assume that assumptions (A) and (B) hold. For any root of unity ζ of k, there is $c_n \in \hat{E}(m_{k_n})$ for each $n \geqslant -1$ (let $k_{-1} = k_0$) satisfying:*

(i) $Tr_{k_n/k_{n-1}}(c_n) = -c_{n-2}$ *for* $n \geqslant 1$;

(ii) $\log_{\hat{E}}(c_{-1}) = (p-1)(\zeta^{\psi^{-2}}p - \zeta^{\psi^{-4}}p^2 + \zeta^{\psi^{-6}}p^3 - \cdots)$.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Fix a generator ζ_0 of the group of roots of unity in k. Since k is unramified over $\mathbb{Q}_p$, we have $O = \mathbb{Z}_p[\zeta_0]$ and $m = p\mathbb{Z}_p[\zeta_0]$. In other words, m is generated over $\mathbb{Z}_p$ by $\{p, p\zeta_0, p\zeta_0^2, \dots, p\zeta_0^{d-1}\}$.

By Proposition 3.12 we can find $c_{n,i} \in \hat{E}(m_{k_n})$ for each $n \geqslant -1$ and $i = 0, 1, \dots, d-1$ such that:

(i) $Tr_{k_n/k_{n-1}}(c_{n,i}) = -c_{n-2,i}$ for $n \geqslant 1$;

(ii) $\log_{\hat{E}}(c_{-1,i}) = (p-1)(\zeta_0^i p - (\zeta_0^i)^{\psi^{-2}} p^2 + (\zeta_0^i)^{\psi^{-4}} p^3 - \cdots)$.

Then using Nakayama's lemma we can see that $\{\log_{\hat{E}}(c_{-1,i})\}_{i=0,\dots,d-1}$ generates m over $\mathbb{Z}_p$. Since $\log_{\hat{E}}$ is an isomorphism from $\hat{E}(m)$ to m, $\{c_{-1,i}\}_{i=0,\dots,d-1}$ generates $\hat{E}(m)$.

Define $c^-_{n,i}$ for $n \geqslant -1, i = 0, \dots, d-1$, as in the previous section. Propositions 3.9, 3.10, and 3.11 hold for these $c^-_{n,i}$, thus we can say the following.

PROPOSITION 3.13. *We have*

$$\left(\bigcup_{n=1}^{\infty} \hat{E}^-(m_{k_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee \cong \Lambda^d.$$

3.3 Self-duality of minus formal groups

We continue to assume that assumptions (A) and (B) hold for k_∞. Let m_n denote the maximal ideal of k_n. We note that the earlier identification of $\mathbb{Z}_p[X]$ with $\mathbb{Z}_p[[\Gamma]]$ gives

$$\Phi_0(X+1) = \gamma - 1,$$
$$\Phi_m(X+1) = 1 + \gamma^{p^{m-1}} + \gamma^{2p^{m-1}} + \cdots + \gamma^{(p-1)p^{m-1}} \quad \text{for } 1 \leqslant m,$$
$$\omega_n^-(X) = (\gamma - 1) \prod_{1 \leqslant m \leqslant n,\ m:\text{odd}} (1 + \gamma^{p^{m-1}} + \gamma^{2p^{m-1}} + \cdots + \gamma^{(p-1)p^{m-1}}).$$

We denote them by Φ_m and ω_n^-. We define $(\Phi_m)^\iota$ and $(\omega_n^-)^\iota$ as the images of Φ_m and ω_n^- each under the involution on $\mathbb{Z}_p[G_n]$ given by $\gamma \mapsto \gamma^{-1}$ and identity on $\mathbb{Z}_p$. First we prove the following.

PROPOSITION 3.14. *We have* $(\omega_n^-)^\iota \hat{E}^-(m_n) = 0$ *and* $\omega_n^- \hat{E}^-(m_n) = 0$.

Proof. First we want to prove that if n is odd, $Tr_{n/n-1}(\hat{E}^-(m_n)) \subset \hat{E}^-(m_{n-2})$, and if n is even, $\hat{E}^-(m_n) = \hat{E}^-(m_{n-1})$.

Suppose that n is odd. Let $y = Tr_{n/n-1}x$ for $x \in \hat{E}^-(m_n)$. By the definition of $\hat{E}^-$, $y \in \hat{E}(m_{n-2})$. For an odd m with $-1 \leqslant m < n-2$ we have

$$p \cdot Tr_{n-2/m+1}y = Tr_{n/m+1}x \in \hat{E}(m_m).$$

Using an argument similar to the proof of Proposition 3.3 we can prove that $\hat{E}(m_{m+1})/\hat{E}(m_m)$ is torsion-free. Thus, we have $Tr_{n-2/m+1}y \in \hat{E}(m_m)$. Thus, $y \in \hat{E}^-(m_{n-2})$.

Now suppose that n is even. From the definition $\hat{E}^-(m_n) \subset \hat{E}(m_{n-1})$. Let $x \in \hat{E}^-(m_n)$. For odd m with $-1 \leqslant m < n-1$, $p \cdot Tr_{n-1/m+1}x = Tr_{n/m+1}x \in \hat{E}(m_m)$. Similarly we can prove $Tr_{n-1/m+1}x \in \hat{E}(m_m)$, thus $x \in \hat{E}^-(m_{n-1})$ follows.

Now we prove our proposition, first for odd n, then for even n.

Suppose that n is odd. Let $x_n \in \hat{E}^-(m_n)$. Since $(\gamma|_{k_n}^{-1})^{p^{n-1}}$ generates $\mathrm{Gal}(k_n/k_{n-1})$, $(\Phi_n)^\iota = 1 + (\gamma^{-1})^{p^{n-1}} + \cdots + (\gamma^{-1})^{(p-1)p^{n-1}}$ acts as $Tr_{n/n-1}$ on $\hat{E}(m_n)$. Thus, we have

$$x_{n-2} := (\Phi_n)^\iota x_n \in \hat{E}^-(m_{n-2}).$$

Similarly

$$x_{n-4} := (\Phi_{n-2})^\iota x_{n-2} \in \hat{E}^-(m_{n-4}), \dots, x_{-1} := (\Phi_1)^\iota x_1 \in E^-(m_{-1}),$$

and, finally, $\Phi_0^\iota x_{-1} = 0$.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

When $n > 0$ is even, $\hat{E}^-(m_n) = \hat{E}^-(m_{n-1})$ and $(\omega_n^-)^\iota = (\omega_{n-1}^-)^\iota$, thus this case is reduced to the case where n is odd, which we have done. When $n = 0$, it is clear. Similarly we can prove $(\omega_n^-)\hat{E}^-(m_n) = 0$ as well. □

Let $\mathbb{H}^- = \bigcup_{n=1}^\infty \hat{E}^-(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and $\mathbb{H}_n^- = (\mathbb{H}^-)^{\mathrm{Gal}(k_\infty/k_n)}$. We note that since $\mathbb{H}^{-\vee} \cong \Lambda^d$, we have $\mathbb{H}_n^{-\vee} \cong \Lambda_n^d$. By the Hochschild–Serre spectral sequence the kernel of $H^1(k_n, A) \to H^1(k_\infty, A)$ is $H^1(k_\infty/k_n, A^{G_{k_\infty}})$, which is trivial by Proposition 3.1. Thus, we consider $\mathbb{H}_n^-$ as a subgroup of $H^1(k_n, A)$. Let a subgroup M_n of $H^1(k_n, T)$ be the exact annihilator of $\mathbb{H}_n^-$ under the Tate local pairing

$$\langle \cdot, \cdot \rangle_n : H^1(k_n, A) \times H^1(k_n, T) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Since $\mathbb{H}_n^-$ is divisible, $H^1(k_n, T)/M_n$ is torsion-free. Thus, we can see that for any integer j, $M_n/p^j M_n$ is the exact annihilator of $\mathbb{H}_n^-[p^j]$ under the Tate local pairing

$$\langle \cdot, \cdot \rangle_n : H^1(k_n, T/p^j T) \times H^1(k_n, T/p^j T) \to \mathbb{Z}/p^j\mathbb{Z}.$$

We want to give hearty thanks to Rubin for suggesting an idea to simplify the proof of the following proposition.

Proposition 3.15. *For every integer j we have $M_n/p^j M_n = \mathbb{H}_n^-[p^j]$.*

Proof. We note that $\mathbb{H}_n^- \cong \mathrm{Hom}(\Lambda_n, \mathbb{Q}_p/\mathbb{Z}_p)^d$. Since $\mathbb{H}_n^-[\omega_n^-] \cong \mathrm{Hom}(\Lambda_n/(\omega_n^-)^\iota, \mathbb{Q}_p/\mathbb{Z}_p)^d$ and $\mathbb{H}_n^-[\tilde{\omega}_n^+] \cong \mathrm{Hom}(\Lambda_n/(\tilde{\omega}_n^+)^\iota, \mathbb{Q}_p/\mathbb{Z}_p)^d$, we know that $\mathrm{corank}_{\mathbb{Z}_p}\mathbb{H}_n^-[\omega_n^-] = d \cdot \deg(\omega_n^-)$ and $\mathrm{corank}_{\mathbb{Z}_p}\mathbb{H}_n^-[\tilde{\omega}_n^+] = d \cdot \deg(\tilde{\omega}_n^+)$. Since $\omega_n^-(X)$ and $\tilde{\omega}_n^+(X)$ are prime to each other, $\mathbb{H}_n^-[\omega_n^-] \cap \mathbb{H}_n^-[\tilde{\omega}_n^+] \cong \mathrm{Hom}(\Lambda_n/((\omega_n^-)^\iota + (\tilde{\omega}_n^+)^\iota), \mathbb{Q}_p/\mathbb{Z}_p)$ is finite. Thus, we obtain $\mathbb{H}_n^- = \mathbb{H}_n^-[\omega_n^-] + \mathbb{H}_n^-[\tilde{\omega}_n^+]$.

By Proposition 3.14 we have $\omega_n^-\hat{E}^-(m_n) = 0$, thus we have $\hat{E}^-(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset \mathbb{H}_n^-[\omega_n^-]$. Also we have $\mathrm{corank}_{\mathbb{Z}_p}\hat{E}^-(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathrm{corank}_{\mathbb{Z}_p}\mathbb{H}_n^-[\omega_n^-]$ by Propositions 3.10 and 3.11 and both are divisible, thus we obtain $\hat{E}^-(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathbb{H}_n^-[\omega_n^-]$. Thus, by the Tate local duality it follows that we have

$$\langle \mathbb{H}_n^-[\omega_n^-], \hat{E}^-(m_n) \rangle_n = \langle \hat{E}^-(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \hat{E}^-(m_n) \rangle_n = 0.$$

On the other hand, we naturally have $\omega_n^-\mathbb{H}_n^- \subset \mathbb{H}_n^-[\tilde{\omega}_n^+]$. Since the kernel of $\mathbb{H}_n^- \xrightarrow{\omega_n^-} \mathbb{H}_n^-$ is $\mathbb{H}_n^-[\omega_n^-]$, we obtain $\mathrm{corank}_{\mathbb{Z}_p}\omega_n^-\mathbb{H}_n^- = d(p^n - \deg(\omega_n^-(X))) = \mathrm{corank}_{\mathbb{Z}_p}\mathbb{H}_n^-[\tilde{\omega}_n^+]$. Since both are divisible, it follows that we have $\omega_n^-\mathbb{H}_n^- = \mathbb{H}_n^-[\tilde{\omega}_n^+]$, thus it follows that we have

$$\begin{aligned}
\langle \mathbb{H}_n^-[\tilde{\omega}_n^+], \hat{E}^-(m_n) \rangle_n &= \langle \omega_n^-\mathbb{H}_n^-, \hat{E}^-(m_n) \rangle_n \\
&= \langle \mathbb{H}_n^-, (\omega_n^-)^\iota \hat{E}^-(m_n) \rangle_n \\
&= \langle \mathbb{H}_n^-, 0 \rangle_n \quad \text{(by Proposition 3.14)} \\
&= 0.
\end{aligned}$$

Thus, $\hat{E}^-(m_n)$ is contained in the annihilator of $\mathbb{H}_n^-$, i.e. $\hat{E}^-(m_n) \subset M_n$ for every n. Thus, we have $\hat{E}^-(m_n)/p^j\hat{E}^-(m_n) \subset M_n/p^j M_n$.

We claim that for every $m \geqslant n$ we have

$$(\hat{E}^-(m_m)/p^j\hat{E}^-(m_m))^{\mathrm{Gal}(k_m/k_n)} \subset M_n/p^j M_n.$$

Let m, n be integers with $m \geqslant n$. First we claim $\mathrm{Cor}_n^m(\mathbb{H}_m^-[p^j]) = \mathbb{H}_n^-[p^j]$.

We identify $\mathbb{H}_m^-[p^j]$ with $\mathrm{Hom}(\Lambda_m, \mathbb{Z}/p^j\mathbb{Z})^d$ and Res_n^m with an injection $\mathrm{Hom}(\Lambda_n, \mathbb{Z}/p^j\mathbb{Z})^d$ to $\mathrm{Hom}(\Lambda_m, \mathbb{Z}/p^j\mathbb{Z})^d$ induced by the natural projection $\mathrm{proj}{:}\Lambda_m \to \Lambda_n$. Since $\mathrm{Res}_n^m \circ \mathrm{Cor}_n^m = Tr_{m/n}$ by Proposition 2.1, we can identify Cor_n^m as follows. First we define $h : \Lambda_n \to \Lambda_m$ as follows. For $x \in \Lambda_n$, we choose a lift x' of x in Λ_m, and take $h(x) = \prod_{n+1 \leqslant n' \leqslant m} \Phi_{n'}(X+1)x'$.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

When x' is any lift of 0, $x' \in (\omega_n)$, thus $\prod_{n+1\leqslant n'\leqslant m}\Phi_{n'}(X+1)x' = 0$ in Λ_m. Thus, h is well defined. Let $h^*: \mathrm{Hom}(\Lambda_m, \mathbb{Z}/p^i\mathbb{Z})^d \to \mathrm{Hom}(\Lambda_n, \mathbb{Z}/p^i\mathbb{Z})^d$ be induced by h.

We can verify that $\mathrm{proj}^* \circ h^* = Tr_{m/n}$ on $\mathrm{Hom}(\Lambda_m, \mathbb{Z}/p^j\mathbb{Z})^d$. Since proj^* is the natural injection and equal to Res^m_n, we can see that $h^* = \mathrm{Cor}^m_n$ on $\mathbb{H}^-_m[p^j]$.

The cokernel of h is $\mathbb{Z}_p[x]/\prod_{n+1\leqslant n'\leqslant m}\Phi_{n'}(X+1)$, and this is a free $\mathbb{Z}_p$-module, thus h^* is surjective. It implies $\mathrm{Cor}^m_n(\mathbb{H}^-_m[p^j]) = \mathbb{H}^-_n[p^j]$.

Now let $y \in (\hat{E}^-(m_m)/p^j\hat{E}^-(m_m))^{\mathrm{Gal}(k_m/k_n)}$. Since $\hat{E}^-(m_m)/p^j\hat{E}^-(m_m) \subset M_m/p^jM_m$, we have $\langle \mathbb{H}^-_m[p^j], y\rangle_m = 0$. Consider y as being in $H^1(k_n, T/p^jT)$ because $H^1(k_n, T/p^jT) \to H^1(k_m, T/p^jT)^{\mathrm{Gal}(k_m/k_n)}$ is an isomorphism. Since $\langle x, \mathrm{Res}^m_n y\rangle_m = \langle \mathrm{Cor}^m_n x, y\rangle_n$ and $\mathrm{Cor}^m_n(\mathbb{H}^-_m[p^j]) = \mathbb{H}^-_n[p^j]$, we have $\langle \mathbb{H}^-_n[p^j], y\rangle_n = 0$, thus $y \in M_n/p^jM_n$.

Since this is true for every $m \geqslant n$, we have

$$\mathbb{H}^-_n[p^j] = \left(\bigcup_{m=n}^{\infty} \hat{E}^-(m_m)/p^j\hat{E}^-(m_m)\right)^{\mathrm{Gal}(k_\infty/k_n)} \subset M_n/p^jM_n.$$

An explicit computation shows that $\mathbb{H}^-_n[p^j] \cong (\mathbb{Z}/p^j\mathbb{Z})^{dp^n}$ and using Tate's Euler characteristic formula, we can check $M_n/p^jM_n \cong (\mathbb{Z}/p^j\mathbb{Z})^{dp^n}$. Thus, $\mathbb{H}^-_n[p^j] = M_n/p^jM_n$. □

3.4 The minus local condition of a ramified $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$

We assume that L_∞ is a $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ and let Λ denote $\mathbb{Z}_p[[\mathrm{Gal}(L_\infty/\mathbb{Q}_p)]]$. Unlike previous sections, we assume that $L_\infty/\mathbb{Q}_p$ is only ramified. In other words, we assume that there is L_N such that $L_N/\mathbb{Q}_p$ is unramified and L_∞/L_N is totally ramified.

We let m_n denote the maximal ideal of L_n. In particular, we let m denote the maximal ideal of $\mathbb{Q}_p$. Let $k_n = L_{n+N}$ for $n \geqslant 0$, then we can see that k_∞ satisfies assumptions (A) and (B). We let $\mathbb{H}^- = \bigcup \hat{E}^-(m_{k_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Since k_∞ satisfies assumptions (A) and (B), by Proposition 3.13 we have

$$\begin{aligned}\mathbb{H}^{-\vee} &\cong \mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k_0)]]^{p^N}\\ &= \mathbb{Z}_p[[\mathrm{Gal}(L_\infty/L_N)]]^{p^N}.\end{aligned}$$

This implies that we have $(\mathbb{H}^-)^{\mathrm{Gal}(L_\infty/L_N)} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{p^N}$. Since $\hat{E}^-(m_N) = \hat{E}(m_N)$, we have $\hat{E}(m_N) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset (\mathbb{H}^-)^{\mathrm{Gal}(L_\infty/L_N)}$. By comparing the coranks and considering they are divisible we can see that $(\mathbb{H}^-)^{\mathrm{Gal}(L_\infty/L_N)} = \hat{E}(m_N) \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

Since $L_N/\mathbb{Q}_p$ is unramified, we have $Tr_{N/0}(\hat{E}(m_N)) = \hat{E}(m)$. By the Tate local duality, it is equivalent to the fact that there is an injection

$$\frac{H^1(\mathbb{Q}_p, A)}{\hat{E}(m) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \to \frac{H^1(L_N, A)}{\hat{E}(m_N) \otimes \mathbb{Q}_p/\mathbb{Z}_p}.$$

Since $H^1(\mathbb{Q}_p, A) = H^1(L_N, A)^{\mathrm{Gal}(L_N/\mathbb{Q}_p)}$ by the Hochschild–Serre spectral sequence, this injection implies that we have

$$\hat{E}(m) \otimes \mathbb{Q}_p/\mathbb{Z}_p = (\hat{E}(m_N) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(L_N/\mathbb{Q}_p)},$$

which, in turn, implies $(\mathbb{H}^-)^{\mathrm{Gal}(L_\infty/\mathbb{Q}_p)} = \hat{E}(m) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Thus, the next proposition follows.

Proposition 3.16. *We have* $(\mathbb{H}^-)^{\mathrm{Gal}(L_\infty/\mathbb{Q}_p)} = \hat{E}(m) \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

Since each $\hat{E}^-(m_n)$ is a $\mathbb{Z}_p[\mathrm{Gal}(L_n/\mathbb{Q}_p)]$-module, $(\mathbb{H}^-)^\vee$ is a Λ-module. When γ is a topological generator of $\mathrm{Gal}(L_\infty/\mathbb{Q}_p)$, Proposition 3.16 implies $(\mathbb{H}^-)^\vee/(\gamma-1)(\mathbb{H}^-)^\vee \cong \mathbb{Z}_p$, which implies that $(\mathbb{H}^-)^\vee$ is generated by one element as a Λ-module by Nakayama's lemma. Since the corank of $(\mathbb{H}^-)^{\mathrm{Gal}(L_\infty/L_n)}$ increases as n increases, we can see that $(\mathbb{H}^-)^\vee$ is a free Λ-module of rank one.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Proposition 3.17. *We have*

$$\mathbb{H}^{-\vee} \cong \Lambda.$$

We also have the following.

Proposition 3.18. *For every integer j, $\mathbb{H}_n^-[p^j]$ is the exact annihilator of itself with respect to the Tate local pairing*

$$H^1(L_n, T/p^jT) \times H^1(L_n, T/p^jT) \to \mathbb{Z}/p^j\mathbb{Z}.$$

Proof. For $n \geqslant N$ our claim follows from Proposition 3.15.

For n where $0 \leqslant n \leqslant N$, using Proposition 3.17 we obtain $(\mathbb{H}^-)^{\mathrm{Gal}(L_\infty/L_n)} = \hat{E}(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ (the proof is similar to how we obtained $(\mathbb{H}^-)^{\mathrm{Gal}(L_\infty/L_N)} = \hat{E}(m_N) \otimes \mathbb{Q}_p/\mathbb{Z}_p$). The rest follows from the Tate local duality. □

4. The parity conjecture

Throughout this section, we fix a prime $p > 3$ and let E be an elliptic curve defined over $\mathbb{Q}$ such that E has good supersingular reduction at p. As before, we let T be the p-adic Tate module of E and A be the set of all p-power torsions of E.

We let K be an imaginary quadratic field extension of $\mathbb{Q}$ such that p splits completely in K. There are two $\mathbb{Z}_p$-extensions K_∞ of K that are Galois extensions over $\mathbb{Q}$. One of them has a property that $K_\infty/\mathbb{Q}_p$ is not an abelian extension. We call such an extension the anti-cyclotomic $\mathbb{Z}_p$-extension of K. Let $\tau \in G_\mathbb{Q}$ be a lift of the nontrivial map of $\mathrm{Gal}(K/\mathbb{Q})$. If K_∞ is the anti-cyclotomic extension of K, we have $\tau\sigma\tau^{-1} = \sigma^{-1}$ for any $\sigma \in \mathrm{Gal}(K_\infty/K)$. Throughout this section we let K_∞ be the anti-cyclotomic $\mathbb{Z}_p$-extension of K.

We let K_n be the subfield of K_∞ with $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$, which we denote by G_n. We let Γ denote $\mathrm{Gal}(K_\infty/K)$, Γ_n denote $\mathrm{Gal}(K_\infty/K_n)$, and Λ denote $\mathbb{Z}_p[[\Gamma]]$. Once and for all, we fix a topological generator γ of Γ.

4.1 Notation and hypotheses

Let P be a prime ideal of Λ generated by an irreducible element not divisible by p. Note that Λ/P is an integral domain and finitely generated $\mathbb{Z}_p$-module. We let O_P denote the integral closure of Λ/P and let S_P denote a Galois module whose underlying group is O_P and on which G_K acts through the canonical map $G_K \to \Gamma$. We let $D_P := \mathrm{Frac}(O_P)/O_P$. Let m_P denote the maximal ideal of O_P and choose a uniformizer π_P of m_P. We observe that G_K acts trivially on S_P/m_PS_P.

We let T_P denote $T \otimes S_P$ and A_P denote $A \otimes S_P$. We fix an embedding $\bar{\mathbb{Q}} \to \mathbb{C}$ and let τ denote the corresponding complex conjugation.

Definition 4.1. Define a pairing $[\cdot,\cdot] : S_P \times S_P \to O_P$ as follows:

$$[s,t] = s \cdot t.$$

With the pairing $[\cdot,\cdot]$ we construct an O_P-bilinear pairing

$$(\cdot,\cdot) : T_P \times A_P \to D_P(1)$$
$$(t \otimes s_1, a \otimes s_2) \to [s_1,s_2] \cdot e(t, a^{\tau^{-1}}).$$

Here $e(\cdot,\cdot)$ is the Weil pairing.

Lemma 4.2. *The first pairing in Definition 4.1 is an O_P-bilinear pairing which satisfies $[s^\sigma, t^{\tau\sigma\tau^{-1}}] = [s,t]$ for every $\sigma \in G_K$.*

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

The pairing $(\cdot,\cdot)$ is a perfect O_P-bilinear pairing and for every $\sigma \in G_K$ it satisfies

$$((t\otimes s_1)^\sigma, (a\otimes s_2)^{\tau\sigma\tau^{-1}}) = (t\otimes s_1, a\otimes s_2)^\sigma. \tag{2}$$

Proof. For $s,t\in S_P$ $[s^\sigma, t^{\tau\sigma\tau^{-1}}] = [s,t]$ because $(\tau\sigma\tau^{-1})|_\Gamma = \sigma|_\Gamma^{-1}$. Then our claim follows from the property of the Weil pairing. □

For any integer $k>0$ we consider the perfect O_P-bilinear pairing

$$T_P/m_P^k T_P \times A_P[m_P^k] \to D_P(1)[m_P^k]. \tag{3}$$

induced by $(\cdot,\cdot)$.

We can identify A_P with $T_P\otimes \mathrm{Frac}(S_P)/S_P$, thus we have

$$A_P[m_P^k] \cong T_P/m_P^k T_P$$

given by multiplication by π_P^k.

LEMMA 4.3. *The pairing in (3) is symmetric when we identify $A_P[m_P^k]$ with $T_P/m_P^kT_P$.*

Proof. Since the Weil pairing is skew-symmetric and Galois-equivariant, this lemma is immediate. □

For convenience let $\mathbb{T}$ denote $T_P/m_P^kT_P$ and $\bar{\mathbb{T}}$ denote the residual representation $\mathbb{T}/m_P\mathbb{T}$. Let $\mathrm{Tw}(\mathbb{T})$ denote the G_K module whose underlying set is $\mathbb{T}$ and on which G_K acts as follows: for $\sigma\in G_K$ and $x\in \mathrm{Tw}\mathbb{T}$, $\sigma\cdot x = (\tau\sigma\tau^{-1})x$ (the action on the right-hand side is that of G_K on $\mathbb{T}$).

Let Σ denote a finite set of places of K including primes lying above p, all infinite places, and all primes at which T is ramified. For $v\in\Sigma$ we consider a certain subgroup $H^1_{\mathcal{F}}(K_v,\mathbb{T}/m_P^i\mathbb{T})$ of $H^1(K_v,\mathbb{T}/m_P^i\mathbb{T})$ for every integer $0\leqslant i\leqslant k$. We call it a local condition at v for $\mathbb{T}/m_P^i\mathbb{T}$, or simply a local condition at v for $\mathbb{T}$ if $i=k$. In this section and the next few sections we define local conditions for $\mathbb{T}$ and show that $\mathbb{T}$ and its local conditions satisfy the following three hypotheses (for similar hypotheses see [MR04, § 3.5] and, in particular, [How04, § 1.3]).

(H1) The residual representation $\bar{\mathbb{T}}$ is an absolutely irreducible representation of G_K, i.e. $\bar{\mathbb{T}}\otimes\overline{O_P/m_P}$ is a G_K-irreducible representation where $\overline{O_P/m_P}$ denotes the algebraic closure of O_P/m_P.

(H2) For every $0\leqslant i\leqslant k$ we have

$$\begin{aligned} H^1_{\mathcal{F}}(K_v,\mathbb{T}/m_P^i\mathbb{T}) &= \mathrm{im}(H^1_{\mathcal{F}}(K_v,\mathbb{T}) \to H^1(K_v,\mathbb{T}/m_P^i\mathbb{T})) \\ &= \ker(H^1(K_v,\mathbb{T}/m_P^i\mathbb{T}) \to H^1(K_v,\mathbb{T})/H^1_{\mathcal{F}}(K_v,\mathbb{T})) \end{aligned}$$

(in this case we say that local conditions are *cartesian*).

(H3) By Lemmas 4.2 and 4.3 we have the following symmetric Galois equivariant O_P-bilinear perfect pairing

$$\mathbb{T}\times \mathrm{Tw}(\mathbb{T}) \to R = O_P/m_P^kO_P.$$

For any non-archimedean v, this pairing combined with the cup product induces a perfect local pairing:

$$H^1(K_v,\mathbb{T})\times H^1(K_v,\mathrm{Tw}(\mathbb{T})) \to H^2(K_v,R(1)) \xrightarrow{\mathrm{inv}} R.$$

Put $\bar v := v^\tau$. Combined with a map

$$\begin{aligned} H^1(K_v,\mathrm{Tw}(\mathbb{T})) &\to H^1(K_{\bar v},\mathbb{T}) \\ \phi &\to \tilde\phi : \sigma \mapsto c(\tau^{-1}\sigma\tau) \end{aligned}$$

the local pairing induces a pairing

$$H^1(K_v,\mathbb{T})\times H^1(K_{\bar v},\mathbb{T}) \to R.$$

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

When we say the local condition at v satisfies hypothesis (H3), we mean that $H^1_{\mathcal{F}}(K_v, \mathbb{T})$ is the exact annihilator of $H^1_{\mathcal{F}}(K_{\bar{v}}, \mathbb{T})$ with respect to this pairing.

In the next proposition we show that hypothesis (H1) holds.

Proposition 4.4. *When $\mathfrak{p}$ is a prime of K lying over p, $\bar{\mathbb{T}}$ is an absolutely irreducible $G_{K_\mathfrak{p}}$-representation, thus an absolutely irreducible G_K-representation.*

Proof. Since our elliptic curve has a supersingular reduction at $p > 3$, by Remark 5.3 or Proposition 8.6 of [Kob03] T/pT is the p-torsion subgroup of the Lubin–Tate group of height 2, thus the action of $G_{\mathbb{Q}_p}$ is completely determined as follows: let L denote the unramified quadratic extension of $\mathbb{Q}_p$, and O_L its ring of integers. We let $\bar{T}$ denote T/pT and for $a \in (O_L/pO_L)^\times$ let $[a]$ denote the Artin map $(a, L(\bar{T})/L)$. By Lubin–Tate group theory we can identify $\bar{T}$ with O_L/pO_L such that $[a]$ acts on $\bar{T}$ as multiplication by a^{-1}. Let $\sigma \in \mathrm{Gal}(L(\bar{T})/\mathbb{Q}_p)$ denote a lift of the nontrivial map of $\mathrm{Gal}(L/\mathbb{Q}_p)$. Then $\sigma[a]\sigma^{-1} = [a^\sigma]$.

We can check that $\bar{\mathbb{T}} \otimes_{O_P/m_P} \overline{O_P/m_P} \cong \bar{T} \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p$, which we denote by $\bar{T} \otimes \bar{\mathbb{F}}_p$. Assume there is a one-dimensional subspace of $\bar{T} \otimes \bar{\mathbb{F}}_p$ invariant under the action of $G_{\mathbb{Q}_p}$. Then there is an action of $\mathrm{Gal}(L(\bar{T})/\mathbb{Q}_p)$ given by a multiplicative character χ whose values are in $\bar{\mathbb{F}}_p^\times$.

Since for any $a \in (O_L/pO_L)^\times$ we have $\sigma[a]\sigma^{-1} = [a^\sigma] = [a^p]$, the value of $\chi([a])$ is in $\mathbb{F}_p^\times$. That is a contradiction because $[a]$ acts on $\bar{T}$ as multiplication by a^{-1}. □

Let K_Σ be the maximal extension of K unramified outside Σ. Then we define

$$H^1_{\mathcal{F}}(K, \mathbb{T}) := \ker\left(H^1(K_\Sigma/K, \mathbb{T}) \to \prod_{v \in \Sigma} \frac{H^1(K_v, \mathbb{T})}{H^1_{\mathcal{F}}(K_v, \mathbb{T})} \right).$$

When the local conditions at all the places in Σ satisfy hypotheses (H1), (H2), and (H3), the following theorem of Howard holds.

Theorem 4.5 [How04, Theorem 1.4.2]. *There is an $O_P/m_P^k O_P$-module M and an integer ε such that we have $H^1_{\mathcal{F}}(K, \mathbb{T}) \cong O_P/m_P^k O_P^\varepsilon \oplus M \oplus M$.*

Remark 4.6. Howard [How04] assumes more hypotheses throughout the paper; however, if we check the proof of Theorem 4.5, we can see that only hypotheses (H1), (H2), and (H3) are necessary.

4.2 Duality of local conditions at the primes lying above p

Let $\mathfrak{p}$ be a prime of K lying above p (thus, the other prime lying above p would be $\bar{\mathfrak{p}} = \mathfrak{p}^\tau$). There are integers N_1, N_2 $(0 \leqslant N_1 \leqslant N_2)$ such that $\mathfrak{p}$ splits completely in K_{N_1}/K, the primes $Q_1, \ldots, Q_{p^{N_1}}$ of K_{N_1} lying above $\mathfrak{p}$ are inert and unramified in K_{N_2}/K_{N_1}, and the primes $Q'_1, \ldots, Q'_{p^{N_1}}$ of K_{N_2} lying above $Q_1, \ldots, Q_{p^{N_1}}$ are totally ramified in K_∞/K_{N_2}.

For $n \geqslant N_1$ let $Q_{n,i}$ be the unique prime of K_n lying above Q_i and, for notational convenience, let K_{n,Q_i} denote $K_{n,Q_{n,i}}$. Put $\overline{Q_i} := Q_i^\tau$, $\overline{Q_{n,i}} := Q_{n,i}^\tau$ and let $K_{n,\overline{Q_i}}$ denote $K_{n,\overline{Q_{n,i}}}$.

Fix Q_i for now and put $L_n := K_{N_1+n,Q_i}$. Then L_∞ is a $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$, $L_\infty/L_{N_2-N_1}$ is totally ramified, and $L_{N_2-N_1}/\mathbb{Q}_p$ is unramified.

Definition 4.7. We put $k_n := K_{N_2+n,Q_i}$. For any $n \geqslant 0$, we define

$$\hat{E}^-(K_{n+N_2,Q_i}) := \hat{E}^-(m_{k_n}),$$

$$\mathbb{H}_{Q_i} := \bigcup_{n=0}^{\infty} \hat{E}^-(K_{n+N_2,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

By Proposition 3.17, we have

$$\mathbb{H}^\vee_{Q_i} \cong \mathbb{Z}_p[[\Gamma_{N_1}]].$$

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

We apply this definition to every Q_i and $\overline{Q_i}$ for $i = 1, \dots, p^{N_1}$.

Definition 4.8. We define a subgroup of $\bigoplus_{i=1}^{p^{N_1}} H^1(K_{\infty,Q_i}, A)$

$$\mathbb{H}_{\mathfrak{p}} := \bigoplus_{i=1}^{p^{N_1}} \mathbb{H}_{Q_i}.$$

Fix a prime ideal $P \subset \Lambda$ generated by an irreducible element not divisible by p. We define a subgroup of $\bigoplus_{i=1}^{p^{N_1}} H^1(K_{\infty,Q_i}, A_P)$

$$\mathbb{H}_{\mathfrak{p},P} := \mathbb{H}_{\mathfrak{p}} \otimes S_P,$$

and, for $n \geqslant 0$, define

$$\mathbb{H}^n_{\mathfrak{p},P} := (\mathbb{H}_{\mathfrak{p},P})^{\Gamma_n}.$$

Assume $n \geqslant N_1$. Since we have $(A \otimes S_P)^{G_{K_\infty}} = A^{G_{K_\infty}} \otimes S_P = 0$, by the Hochschild–Serre spectral sequence $H^1(K_{n,Q_i}, A_P) \to H^1(K_{\infty,Q_i}, A_P)^{\Gamma_n}$ is an isomorphism. Thus, we can consider $\mathbb{H}^n_{\mathfrak{p},P}$ as a subgroup of $\bigoplus_{i=1}^{p^N} H^1(K_{n,Q_i}, A_P)$.

Now we show that, for $0 \leqslant n \leqslant N_1$,

$$\bigoplus_{i=1}^{p^n} H^1(K_{n,p_i}, A_P) \to \left(\bigoplus_{i=1}^{p^{N_1}} H^1(K_{N_1,Q_i}, A_P) \right)^{\mathrm{Gal}(K_{N_1}/K_n)}$$

is an isomorphism so that we can consider $\mathbb{H}^n_{\mathfrak{p},P}$ as a subgroup of $\bigoplus_{i=1}^{p^n} H^1(K_{n,p_i}, A_P)$. First fix $g_i \in \mathrm{Gal}(K_\infty/K)$ for each i such that $g_i Q_{n,1} = Q_{n,i}$ for all n. Without loss of generality we can assume $n = 0$ (other cases can be proven similarly). Fix an embedding $\bar{\mathbb{Q}} \to \mathbb{C}_p$ such that the prime of K_{N_1} induced by this embedding is $Q_{N_1,1}$. This embedding identifies $K_{\mathfrak{p}}$ with K_{N_1,Q_1} and this induces a restriction map $\mathrm{Res}_1 : H^1(K_{\mathfrak{p}}, A_P) \to H^1(K_{N_1,Q_1}, A_P)$ (indeed, this is an isomorphism). Then other restriction maps $\mathrm{Res}_i : H^1(K_{\mathfrak{p}}, A_P) \to H^1(K_{N_1,Q_i}, A_P)$ are equal to $g_i \circ \mathrm{Res}_1$, and we can check

$$\mathrm{Res} : H^1(K_{\mathfrak{p}}, A_P) \to \left(\bigoplus_{i=1}^{p^{N_1}} H^1(K_{N_1,Q_i}, A_P) \right)^{\mathrm{Gal}(K_N/K)}$$

(Res is given by $(\mathrm{Res}_i)_{i=1,\dots,p^{N_1}}$) is an isomorphism.

On the other hand, for any $n \geqslant N_2$, the action $g_i|_{K_n} : H^1(K_{n,Q_1}, A) \to H^1(K_{n,Q_i}, A)$ gives $g_i|_{K_n} \hat{E}^-(K_{n,Q_1}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \hat{E}^-(K_{n,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, thus we have $g_i \mathbb{H}_{Q_1} = \mathbb{H}_{Q_i}$.

Proposition 4.9. *We have*

$$\begin{aligned} \mathbb{H}_{\mathfrak{p}} &\cong \bigoplus_{i=1}^{p^{N_1}} g_i \,\mathrm{Hom}(\mathbb{Z}_p[[\Gamma_{N_1}]], \mathbb{Q}_p/\mathbb{Z}_p) \\ &\cong \mathrm{Hom}(\mathbb{Z}_p[[\Gamma]], \mathbb{Q}_p/\mathbb{Z}_p). \end{aligned}$$

Proof. All we need to show is that

$$\bigoplus_{i=1}^{p^{N_1}} g_i^{-1} \mathbb{Z}_p[[\Gamma_{N_1}]] \to \mathbb{Z}_p[[\Gamma]]$$

is an isomorphism. This is clear. □

Since multiplication by π_P^{-k} gives an isomorphism $H^1(K_{\mathfrak{p}}, T_P/m_P^k T_P) \cong H^1(K_{\mathfrak{p}}, A_P)[m_P^k]$, we can consider $\mathbb{H}^0_{\mathfrak{p},P}[m_P^k]$ as a subgroup of $H^1(K_{\mathfrak{p}}, T_P/m_P^k T_P)$. We want to study this group further. First we check the following.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Lemma 4.10. *For every $n \geqslant N_1$ and integer j, $(\mathbb{H}_{Q_i}[p^j])^{\Gamma_n}$ is the exact annihilator of $(\mathbb{H}_{\overline{Q_i}}[p^j])^{\Gamma_n}$ with respect to the pairing*

$$H^1(K_{n,Q_i}, T/p^jT) \times H^1(K_{n,\overline{Q_i}}, T/p^jT) \to \mathbb{Z}/p^j\mathbb{Z}.$$

Proof. The construction of the pairing illustrated in § 4.1 has the following equivalent construction: for any $m \geqslant N_1$, we have the local Tate pairing induced from the Weil pairing

$$H^1(K_{m,Q_i}, T/p^jT) \times H^1(K_{m,Q_i}, T/p^jT) \to \mathbb{Z}/p^j\mathbb{Z}.$$

This pairing combined with the following map given by the action of τ

$$\begin{aligned} \tau : H^1(K_{m,Q_i}, T/p^jT) &\to H^1(K_{m,\overline{Q_i}}, T/p^jT) \\ \phi &\mapsto \tilde{\phi} : \gamma \mapsto \tau \cdot \phi(\tau^{-1}\gamma\tau) \end{aligned}$$

gives the same pairing given in hypothesis (H3) of § 4.1.

For all m we have $\tau \cdot \hat{E}^-(K_{m,Q_i}) \otimes \mathbb{Z}/p^j\mathbb{Z} = \hat{E}^-(K_{m,\overline{Q_i}}) \otimes \mathbb{Z}/p^j\mathbb{Z}$, thus we have $\tau \cdot \mathbb{H}_{Q_i}[p^j] = \mathbb{H}_{\overline{Q_i}}[p^j]$. Then we can see that $(\mathbb{H}_{Q_i}[p^j])^{\Gamma_n}$ is the exact annihilator of $(\mathbb{H}_{\overline{Q_i}}[p^j])^{\Gamma_n}$ with respect to the pairing in our lemma. □

Proposition 4.11. *For any $k \geqslant 0, \mathbb{H}^0_{\mathfrak{p},P}[m_P^k]$ is the exact annihilator of $\mathbb{H}^0_{\bar{\mathfrak{p}},P}[m_P^k]$ with respect to the pairing*

$$(\cdot,\cdot)_0 : H^1(K_{\mathfrak{p}}, T_P/m_P^kT_P) \times H^1(K_{\bar{\mathfrak{p}}}, T_P/m_P^kT_P) \to O_P/m_P^k.$$

Proof. First fix $n \geqslant 0$ such that $\mathrm{Gal}(K_\infty/K_n)$ acts trivially on $S_P/m_P^kS_P$ and fix $j \geqslant 0$ that $m_P^k \mid p^j$.

For every $i = 1, \ldots, p^{N_1}$, by Lemma 4.10 $(\mathbb{H}_{Q_i}[p^j])^{\Gamma_n}$ is the exact annihilator of $(\mathbb{H}_{\overline{Q_i}}[p^j])^{\Gamma_n}$ with respect to

$$H^1(K_{n,Q_i}, T/p^jT) \times H^1(K_{n,\overline{Q_i}}, T/p^jT) \to \mathbb{Z}/p^j\mathbb{Z}.$$

Since $G_{K_{n,Q_i}}$ and $G_{K_n,\overline{Q_i}}$ act trivially on $S_P/m_P^kS_P$, by taking tensor with $S_P/m_P^kS_P$ we can check that $(\mathbb{H}_{Q_i}[p^j])^{\Gamma_n} \otimes S_P/m_P^kS_P$ is the exact annihilator of $(\mathbb{H}_{\overline{Q_i}}[p^j])^{\Gamma_n} \otimes S_P/m_P^kS_P$ with respect to

$$H^1(K_{n,Q_i}, T_P/m_P^kT_P) \times H^1(K_{n,\overline{Q_i}}, T_P/m_P^kT_P) \to O_P/m_P^kO_P. \tag{4}$$

As the multiplication by π^{-k} identifies $H^1(K_{n,Q_i}, T/p^jT \otimes S_P/m_P^kS_P)$ with $H^1(K_{n,Q_i}, A \otimes S_P)[m_P^k]$, we can check that this multiplication identifies $(\mathbb{H}_{Q_i}[p^j])^{\Gamma_n} \otimes S_P/m_P^kS_P$ (considered to be in the first group) with $(\mathbb{H}_{Q_i} \otimes S_P)^{\Gamma_n}[m_P^k]$ (considered to be in the second group). Thus, $(\mathbb{H}_{Q_i} \otimes S_P)^{\Gamma_n}[m_P^k]$ is the exact annihilator of $(\mathbb{H}_{\overline{Q_i}} \otimes S_P)^{\Gamma_n}[m_P^k]$ under the pairing (4).

Since $\mathbb{H}^n_{\mathfrak{p},P} = \bigoplus_{i=1}^{p^{N_1}} (\mathbb{H}_{Q_i} \otimes S_P)^{\Gamma_n}$, $\mathbb{H}^n_{\mathfrak{p},P}[m_P^k]$ is the exact annihilator of $\mathbb{H}^n_{\bar{\mathfrak{p}},P}[m_P^k]$ with respect to the pairing

$$(\cdot,\cdot)_n : \bigoplus_{i=1}^{p^{N_1}} H^1(K_{n,Q_i}, T_P/m_P^kT_P) \times \bigoplus_{i=1}^{p^{N_1}} H^1(K_{n,\overline{Q_i}}, T_P/m_P^kT_P) \to O_P/m_P^k$$

(this pairing is given by the summation of all pairings for $i = 1, \ldots, p^{N_1}$).

To show that $\mathbb{H}^0_{\mathfrak{p},P}[m_P^k]$ is the exact annihilator of $\mathbb{H}^0_{\bar{\mathfrak{p}},P}[m_P^k]$, we consider the following commutative diagram.

$$\begin{array}{ccccc} \bigoplus_{i=1}^{p^{N_1}} H^1(K_{n,Q_i}, T_P/m_P^kT_P) & \times & \bigoplus_{i=1}^{p^{N_1}} H^1(K_{n,\overline{Q_i}}, T_P/m_P^kT_P) & \longrightarrow & O_P/m_P^k \\ \downarrow \mathrm{Cor}_{\mathfrak{p}} & & \uparrow \mathrm{Res}_{\bar{\mathfrak{p}}} & & \downarrow \\ H^1(K_{\mathfrak{p}}, T_P/m_P^kT_P) & \times & H^1(K_{\bar{\mathfrak{p}}}, T_P/m_P^kT_P) & \longrightarrow & O_P/m_P^k \end{array}$$

The construction of $\mathrm{Cor}_{\mathfrak{p}}$ and $\mathrm{Res}_{\bar{\mathfrak{p}}}$ is given in § 2.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Recall that by definition we have $\mathbb{H}_{\mathfrak{p},P}[m_P^k] \cong \mathrm{Hom}_{O_P}(O_P[[\Gamma]], S_P/m_P^k S_P)$. We want to show $\mathrm{Cor}_{\mathfrak{p}}(\mathbb{H}^n_{\mathfrak{p},P}[m_P^k]) = \mathbb{H}^0_{\mathfrak{p},P}[m_P^k]$ following the argument in the proof of Proposition 3.15. To do so, it might be convenient to have $\mathbb{H}_{\mathfrak{p},P}[m_P^k] \cong \mathrm{Hom}_{O_P}(O_P[[\Gamma]], O_P/m_P^k)$. There is $\alpha \in O_P^\times$ such that a generator γ of Γ acts on S_P as multiplication by α. Then we can give the following homomorphism:

$$\begin{aligned}\phi : \mathrm{Hom}_{O_P}(O_P[[\Gamma]], S_P/m_P^k S_P) &\to \mathrm{Hom}_{O_P}(O_P[[\Gamma]], O_P/m_P^k)\\ f &\mapsto \tilde{f} : \gamma^i \mapsto f(\gamma^i)/\alpha^i.\end{aligned}$$

(i in the last line runs over all integers). We can check that this is a well-defined O_P-isomorphism and also Γ-equivariant.

Thus we can show $\mathrm{Cor}_{\mathfrak{p}}(\mathbb{H}^n_{\mathfrak{p},P}[m_P^k]) = \mathbb{H}^0_{\mathfrak{p},P}[m_P^k]$. Again using an argument in the proof of Proposition 3.15 combined with the commutativity of the diagram above, this implies that $\mathbb{H}^0_{\mathfrak{p},P}[m_P^k]$ is contained in the exact annihilator of $\mathbb{H}^0_{\mathfrak{p},P}[m_P^k]$. We can check

$$|\mathbb{H}^0_{\mathfrak{p},P}[m_P^k]| = |O_P/m_P^k|,$$

and using Tate's Euler characteristic formula, we can check that the size of the exact annihilator of $\mathbb{H}^0_{\mathfrak{p},P}[m_P^k]$ is

$$\frac{|H^1(K_{\mathfrak{p}}, T_P/m_P^k T_P)|}{|\mathbb{H}^0_{\mathfrak{p},P}[m_P^k]|} = \left|\frac{O_P^2/m_P^k O_P^2}{O_P/m_P^k}\right| = |O_P/m_P^k|.$$

Thus, we can conclude that $\mathbb{H}^0_{\mathfrak{p},P}[m_P^k]$ is the exact annihilator of $\mathbb{H}^0_{\mathfrak{p},P}[m_P^k]$. □

4.3 Iwasawa theory techniques

Let $V_P = T_P \otimes_{O_P} \mathrm{Frac}(O_P)$.

DEFINITION 4.12. For a finite place v of K not lying over p, we define the local conditions at v as follows (see [Rub00, Definition 1.3.4]; for the definition of H^1_{ur}, see [Rub00, Definition 1.3.1]):

$$\begin{aligned}H^1_{\mathcal{F}}(K_v, A_P) &:= \mathrm{im}(H^1_{ur}(K_v, V_P) \to H^1(K_v, A_P)),\\ H^1_{\mathcal{F}}(K_v, T_P) &:= \ker\left(H^1(K_v, T_P) \to \frac{H^1(K_v, V_P)}{H^1_{ur}(K_v, V_P)}\right),\\ H^1_{\mathcal{F}}(K_v, T_P/m_P^k T_P) &= \mathrm{im}(H^1_{\mathcal{F}}(K_v, T_P) \to H^1(K_v, T_P/m_P^k T_P)).\end{aligned}$$

As we identify $A_P[m_P^k]$ with $T_P/m_P^k T_P$ by multiplication by π_P^k, we identify $H^1_{\mathcal{F}}(K_v, A_P[m_P^k])$ with $H^1_{\mathcal{F}}(K_v, T_P/m_P^k T_P)$.

Remark 4.13. Note that we have $H^1_{ur}(K_v, V_P) = 0$, hence we have $H^1_{\mathcal{F}}(K_v, A_P) = 0$.

Rubin [Rub00, Lemma 1.3.8(i)] stated that $H^1_{\mathcal{F}}(K_v, A_P[m_P^k])$ is the inverse image of $H^1_{\mathcal{F}}(K_v, A_P)$ under the natural map

$$H^1(K_v, A_P[m_P^k]) \to H^1(K_v, A_P).$$

This implies that for any two integers $0 \leqslant k < k'$, we have

$$H^1_{\mathcal{F}}(K_v, A_P[m_P^k]) = \ker(H^1(K_v, A_P[m_P^k]) \to H^1(K_v, A_P[m_P^{k'}])/H^1_{\mathcal{F}}(K_v, A_P[m_P^{k'}])).$$

On the other hand, Definition 4.12 implies that we naturally have

$$H^1_{\mathcal{F}}(K_v, A_P[m_P^k]) = \mathrm{im}(H^1_{\mathcal{F}}(K_v, A_P[m_P^{k'}]) \to H^1(K_v, A_P[m_P^k])).$$

Thus, the local condition at v for $A_P[m_P^k]$ satisfies hypothesis (H2) for any k. If we define $H^1_{\mathcal{F}}(K_v, Tw(A_P[m_P^k]))$ in the same way, we can check that $H^1_{\mathcal{F}}(K_{\bar{v}}, A_P[m_P^k])$ is the image of $H^1_{\mathcal{F}}(K_v, Tw(A_P[m_P^k]))$ under the map $H^1(K_v, Tw(A_P[m_P^k])) \to H^1(K_{\bar{v}}, A_P[m_P^k])$ defined in

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

hypothesis (H3). Then, by [Rub00, Proposition 1.4.3(ii)], we can see that the local condition at v satisfies hypothesis (H3) as well.

Definition 4.14. For a prime $\mathfrak{p}$ of K lying over p, we define

$$H^1_{\mathcal{F}}(K_{\mathfrak{p}}, A_P) := \mathbb{H}^0_{\mathfrak{p},P},$$
$$H^1_{\mathcal{F}}(K_{\mathfrak{p}}, A_P[m_P^k]) := \mathbb{H}^0_{\mathfrak{p},P}[m_P^k].$$

Since $H^1(K_{\mathfrak{p}}, A_P[m_P^k]) \to H^1(K_{\mathfrak{p}}, A_P[m_P^{k'}])[m_P^k]$ is an isomorphism, we can easily check one part of hypothesis (H2). To check the other part of hypothesis (H2), consider the following map:

$$H^1(K_{\mathfrak{p}}, A_P) \xrightarrow{\pi_P^{k'-k}} H^1(K_{\mathfrak{p}}, A_P).$$

This map induces $\mathbb{H}^0_{\mathfrak{p},P} \xrightarrow{\pi_P^{k'-k}} \mathbb{H}^0_{\mathfrak{p},P}$, which is surjective because $\mathbb{H}^0_{\mathfrak{p},P} \cong \mathrm{Hom}_{O_P}(O_P, D_P)$ is divisible. Thus, we have a surjective map $H^1_{\mathcal{F}}(K_{\mathfrak{p}}, A_P[m_P^{k'}]) \xrightarrow{\pi_P^{k'-k}} H^1_{\mathcal{F}}(K_{\mathfrak{p}}, A_P[m_P^k])$.

In the previous section we checked that this local condition satisfies hypothesis (H3).

Because $K_\infty = \mathbb{C}$, we do not have to discuss local conditions at infinite places. Using Theorem 4.5, we obtain the following proposition.

Proposition 4.15. *We have*

$$H^1_{\mathcal{F}}(K, A_P[m_P^k]) \cong (O_P/m_P^k O_P)^{\epsilon} \oplus M^2$$

for an $O_P/m_P^k O_P$-module M and an integer ϵ.

We define $H^1_{\mathcal{F}}(K, A_P)$ as

$$H^1_{\mathcal{F}}(K, A_P) := \ker\left(H^1(K_\Sigma/K, A_P) \to \prod_{w\in\Sigma} H^1(K_w, A_P)/H^1_{\mathcal{F}}(K_w, A_P)\right).$$

Then we have the following.

Proposition 4.16. *There is an integer r_P and a finite O_P-module $M(P)$ such that we have*

$$H^1_{\mathcal{F}}(K, A_P) \cong (D_P)^{r_P} \oplus M(P)^2.$$

Proof. As mentioned after Definitions 4.12 and 4.14, for any integer k and any finite place v, $H^1_{\mathcal{F}}(K_v, A_P[m_P^k])$ is the inverse image of $H^1_{\mathcal{F}}(K_v, A_P)$ under the natural map

$$H^1(K_v, A_P[m_P^k]) \to H^1(K_v, A_P).$$

Also we have $H^1(K, A_P[m_P^k]) \cong H^1(K, A_P)[m_P^k]$, thus we have

$$H^1_{\mathcal{F}}(K, A_P[m_P^k]) \cong H^1_{\mathcal{F}}(K, A_P)[m_P^k];$$

therefore, by Proposition 4.15 we obtain our claim. □

Proposition 2.5 gives a Λ-isomorphism

$$Sh_{\mathfrak{p}} : H^1(K_{\mathfrak{p}}, \mathrm{Hom}(\Lambda, A)) \xrightarrow{\sim} \prod_{i=1}^{p^{N_1}} H^1(K_{\infty,Q_i}, A).$$

Definition 4.17. For a prime $\mathfrak{p}$ of K lying above p, we define $H^1_{\mathcal{F}}(K_{\mathfrak{p}}, \mathrm{Hom}(\Lambda, A))$ as the inverse image of $\mathbb{H}_{\mathfrak{p}}$ under $Sh_{\mathfrak{p}}$.

For any other finite place v, we define

$$H^1_{\mathcal{F}}(K_v, \mathrm{Hom}(\Lambda, A)) := H^1_{ur}(K_v, \mathrm{Hom}(\Lambda, A)).$$

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

In addition, we define

$$H^1_{\mathcal{F}}(K,\mathrm{Hom}(\Lambda,A))=\ker\left(H^1(K_\Sigma/K,\mathrm{Hom}(\Lambda,A))\to\prod_{v\in\Sigma}\frac{H^1(K_v,\mathrm{Hom}(\Lambda,A))}{H^1_{\mathcal{F}}(K_v,\mathrm{Hom}(\Lambda,A))}\right).$$

Recall that P is a prime ideal generated by an irreducible element not divisible by p. We let x_P denote this element. Note that x_P is (possibly) different from π_P, a uniformizer of the maximal ideal m_P of O_P. For the fixed generator γ of Γ, we let $\iota:\Lambda\to\Lambda$ be the involution map given by $\gamma\to\gamma^{-1}$ and identity on $\mathbb{Z}_p$. Let $P^\iota:=\iota(P)$. We identify S_P with $\mathrm{Hom}_{O_{P^\iota}}(S_{P^\iota},O_{P^\iota})$ as G_K-modules. We construct the following map

$$S_P=\mathrm{Hom}_{O_{P^\iota}}(S_{P^\iota},O_{P^\iota})\xrightarrow{\text{trace}}\mathrm{Hom}_{\mathbb{Z}_p}(S_{P^\iota},\mathbb{Z}_p)\to\mathrm{Hom}_{\mathbb{Z}_p}(\Lambda/P^\iota,\mathbb{Z}_p).$$

This map is injective, and the cokernel is finite. This map tensored by A gives

$$A_P=A\otimes S_P\to\mathrm{Hom}(\Lambda/P^\iota,A)\cong\mathrm{Hom}(\Lambda,A)[P^\iota]$$

(the last group is the kernel of the multiplication by x_P^ι). This map is surjective and its kernel is finite.

For $n\geqslant 1$, let P_n be an ideal of Λ generated by $x_{P_n}=x_P+p^n$, which is irreducible if n is large enough. In § 2 we defined a map

$$j:\bigoplus_{i=1}^{p^{N_1}}H^1(K_{\infty,Q_i},A)\xrightarrow{\sim}\mathrm{Hom}\left(\Lambda,\bigoplus_{i=1}^{p^{N_1}}H^1(K_{\infty,Q_i},A)\right)^\Gamma,$$

and, by Proposition 2.5, $j\circ Sh_{\mathfrak{p}}$ is equal to the following natural map

$$H^1(K_{\mathfrak{p}},\mathrm{Hom}(\Lambda,A))\xrightarrow{\sim}\left(\bigoplus_{i=1}^{p^{N_1}}H^1(K_{\infty,Q_i},\mathrm{Hom}(\Lambda,A))\right)^\Gamma\xrightarrow{\sim}\mathrm{Hom}\left(\Lambda,\bigoplus_{i=1}^{p^{N_1}}H^1(K_{\infty,Q_i},A)\right)^\Gamma.$$

Therefore, the image of $H^1_{\mathcal{F}}(K_{\mathfrak{p}},\mathrm{Hom}(\Lambda,A))$ under this map is $j(\mathbb{H}_{\mathfrak{p}})=\mathrm{Hom}(\Lambda,\mathbb{H}_{\mathfrak{p}})^\Gamma$.

We consider the following commutative diagram whose vertical maps are isomorphisms.

$$\begin{array}{ccccc}
H^1(K_{\mathfrak{p}},A_{P_n}) & \longrightarrow & H^1(K_{\mathfrak{p}},\mathrm{Hom}(\Lambda/P_n^\iota,A)) & \cong & H^1(K_{\mathfrak{p}},\mathrm{Hom}(\Lambda,A))[P_n^\iota] \\
\downarrow & & \downarrow & & \\
\left(S_{P_n}\otimes\bigoplus_{i=1}^{p^{N_1}}H^1(K_{\infty,Q_i},A)\right)^\Gamma & \longrightarrow & \mathrm{Hom}\left(\Lambda/P_n^\iota,\bigoplus_{i=1}^{p^{N_1}}H^1(K_{\infty,Q_i},A)\right)^\Gamma & &
\end{array}$$

By our discussion, the map $H^1_{\mathcal{F}}(K_{\mathfrak{p}},A_{P_n})\to H^1_{\mathcal{F}}(K_{\mathfrak{p}},\mathrm{Hom}(\Lambda,A))[P_n^\iota]$ in the top is equal to a natural map $(S_{P_n}\otimes\mathbb{H}_{\mathfrak{p}})^\Gamma\to\mathrm{Hom}(\Lambda/P_n^\iota,\mathbb{H}_{\mathfrak{p}})^\Gamma$ in the bottom. We can check that as $n\gg 0$ varies this map has finite kernel and cokernel whose orders are bounded. We have the following proposition.

PROPOSITION 4.18. *The kernel and cokernel of*

$$f_{\mathcal{F}}:H^1_{\mathcal{F}}(K,A_{P_n})\to H^1_{\mathcal{F}}(K,\mathrm{Hom}(\Lambda,A))[P_n^\iota]$$

are finite and bounded as n varies.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Proof. We consider the following commutative diagram.

$$\begin{array}{ccccc} 0 \to H^1_{\mathcal{F}}(K, A_{P_n}) & \longrightarrow & H^1(K_\Sigma/K, A_{P_n}) & \longrightarrow & \prod_{v\in\Sigma} \dfrac{H^1(K_v, A_{P_n})}{H^1_{\mathcal{F}}(K_v, A_{P_n})} \\ \downarrow f_{\mathcal{F}} & & \downarrow & & \downarrow \\ 0 \to H^1_{\mathcal{F}}(K, \mathrm{Hom}(\Lambda, A))[P_n^\iota] & \longrightarrow & H^1(K_\Sigma/K, \mathrm{Hom}(\Lambda, A))[P_n^\iota] & \longrightarrow & \prod_{v\in\Sigma} \dfrac{H^1(K_v, \mathrm{Hom}(\Lambda, A))}{H^1_{\mathcal{F}}(K_v, \mathrm{Hom}(\Lambda, A))} \end{array}$$

It is proven in the proof of [MR04, Proposition 5.3.14] that the center vertical arrow has kernel and cokernel whose orders are finite and bounded as $n \gg 0$ varies. Hence, we only need to show that the right vertical arrow has a finite kernel whose order is bounded as $n \gg 0$ varies.

For any place v we consider the following diagram.

$$\begin{array}{ccccc} 0 \to H^1_{\mathcal{F}}(K_v, A_{P_n}) & \longrightarrow & H^1(K_v, A_{P_n}) & \longrightarrow & \dfrac{H^1(K_v, A_{P_n})}{H^1_{\mathcal{F}}(K_v, A_{P_n})} \\ \downarrow & & \downarrow & & \downarrow f_v \\ 0 \to H^1_{\mathcal{F}}(K_v, \mathrm{Hom}(\Lambda, A))[P_n^\iota] & \longrightarrow & H^1(K_v, \mathrm{Hom}(\Lambda, A))[P_n^\iota] & \longrightarrow & \dfrac{H^1(K_v, \mathrm{Hom}(\Lambda, A))}{H^1_{\mathcal{F}}(K_v, \mathrm{Hom}(\Lambda, A))} \end{array}$$

To show that the right vertical map f_v has a finite kernel whose order is bounded as $n \gg 0$ varies, we want to show that the orders of the cokernel of the left vertical map and the kernel of the middle vertical map are finite and bounded as $n \gg 0$ varies.

Let v be a non-archimedean place such that $v \nmid p$. A short exact sequence

$$0 \to \mathrm{Hom}(\Lambda/P_n^\iota, A) \to \mathrm{Hom}(\Lambda, A) \xrightarrow{x^\iota_{P_n}} H^1(\Lambda, A) \to 0$$

induces (from the long exact sequence of $H^\bullet(K_v, \ )$ groups)

$$0 \to \frac{\mathrm{Hom}(\Lambda, A)^{G_{K_v}}}{{P_n}^\iota \mathrm{Hom}(\Lambda, A)^{G_{K_v}}} \to H^1(K_v, \mathrm{Hom}(\Lambda/P_n^\iota, A)) \to H^1(K_v, \mathrm{Hom}(\Lambda, A))[{P_n}^\iota] \to 0. \tag{5}$$

On the other hand, we consider a short exact sequence

$$0 \to \mathrm{Hom}(\Lambda/P_n^\iota, A^{I_{K_v}}) \to \mathrm{Hom}(\Lambda, A^{I_{K_v}}) \xrightarrow{x^\iota_{P_n}} \mathrm{Hom}(\Lambda, A^{I_{K_v}}) \to 0$$

(we have the right exactness because Λ/P_n^ι is a free $\mathbb{Z}_p$-module). This induces (from the long exact sequence of $H^\bullet(K_v^{ur}/K_v, \ )$ groups)

$$\begin{aligned} 0 \to \frac{\mathrm{Hom}(\Lambda, A^{I_{K_v}})^{\mathrm{Gal}(K_v^{ur}/K_v)}}{{P_n}^\iota \mathrm{Hom}(\Lambda, A^{I_{K_v}})^{\mathrm{Gal}(K_v^{ur}/K_v)}} &\to H^1(K_v^{ur}/K_v, \mathrm{Hom}(\Lambda/P_n^\iota, A^{I_{K_v}})) \\ &\to H^1(K_v^{ur}/K_v, \mathrm{Hom}(\Lambda, A^{I_{K_v}}))[{P_n}^\iota] \to 0. \end{aligned} \tag{6}$$

Since v is unramified over K_∞/K, we have $\mathrm{Hom}(\Lambda, A^{I_{K_v}})^{\mathrm{Gal}(K_v^{ur}/K_v)} = \mathrm{Hom}(\Lambda, A)^{G_{K_v}}$.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Thus, as we consider the following diagram:

$$\begin{array}{ccccccc}
 & \mathrm{Ker}_1 & & \mathrm{Ker}_2 & & \mathrm{Ker}_3 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to H^1_{ur}(K_v, \mathrm{Hom}(\Lambda/P_n^\iota, A)) & \longrightarrow & H^1(K_v, \mathrm{Hom}(\Lambda/P_n^\iota, A)) & \longrightarrow & \dfrac{H^1(K_v, \mathrm{Hom}(\Lambda/P_n^\iota, A))}{H^1_{ur}(K_v, \mathrm{Hom}(\Lambda/P_n^\iota, A))} & \to 0 & \\
\downarrow & & \downarrow & & \downarrow & & \\
0 \to H^1_{ur}(K_v, \mathrm{Hom}(\Lambda, A))[P_n^\iota] & \longrightarrow & H^1(K_v, \mathrm{Hom}(\Lambda, A))[P_n^\iota] & \longrightarrow & \dfrac{H^1(K_v, \mathrm{Hom}(\Lambda, A))}{H^1_{ur}(K_v, \mathrm{Hom}(\Lambda, A))} & & \\
\downarrow & & & & & & \\
\mathrm{Cok}_1 & & & & & &
\end{array}$$

we can see that $\mathrm{Ker}_1 = \mathrm{Ker}_2$ from (5) and (6), and $\mathrm{Cok}_1 = 0$ from (6). Therefore, Ker_3 is trivial.

It is not hard to see that the order of the kernel of

$$\frac{H^1(K_v, A_{P_n})}{H^1_{ur}(K_v, A_{P_n})} \to \frac{H^1(K_v, \mathrm{Hom}(\Lambda/P_n^\iota, A))}{H^1_{ur}(K_v, \mathrm{Hom}(\Lambda/P_n^\iota, A))}$$

is finite and bounded as $n \gg 0$ varies. From [Rub00, Lemma 1.3.5] we can see that $H^1_{ur}(K_v, A_{P_n})/H^1_{\mathcal{F}}(K_v, A_{P_n})$ is finite and its order is bounded as $n \gg 0$ varies. Thus, we can see that f_v has a finite kernel whose order is bounded as $n \gg 0$ varies.

As discussed before this proposition, the map $H^1_{\mathcal{F}}(K_{\mathfrak{p}}, A_{P_n}) \to H^1_{\mathcal{F}}(K_{\mathfrak{p}}, \mathrm{Hom}(\Lambda, A))[P_n^\iota]$ has a finite cokernel whose order is finite and bounded as $n \gg 0$ varies. We can easily check that $H^1(K_{\mathfrak{p}}, A_{P_n}) \to H^1(K_{\mathfrak{p}}, \mathrm{Hom}(\Lambda, A))[P_n^\iota]$ has finite kernel and cokernel whose orders are bounded as $n \gg 0$ varies. Thus, $f_{\mathfrak{p}}$ has a finite kernel whose order is bounded as $n \gg 0$ varies.

Thus, $f_{\mathcal{F}}$ has finite kernel and cokernel whose orders are bounded as $n \gg 0$ varies. □

Write X for $H^1_{\mathcal{F}}(K, \mathrm{Hom}(\Lambda, A))^\vee$.

Consider the following:

$$H^1_{\mathcal{F}}(K, A_{P_n}) \to H^1_{\mathcal{F}}(K, \mathrm{Hom}(\Lambda, A))[P_n^\iota] \to H^1_{\mathcal{F}}(K, \mathrm{Hom}(\Lambda, A))[P_n^\iota] \otimes O_{P_n}.$$

(The tensor product in the last term is over Λ/P_n^ι. Also note that O_{P_n} is a Λ/P_n^ι-module through $\Lambda/P_n^\iota \xrightarrow{\iota} \Lambda/P_n \to O_{P_n}$.) Proposition 4.18 states that this map has kernel and cokernel whose orders are finite and bounded as $n \gg 0$ varies.

Then, by taking a Pontryagin dual, we can see that

$$(X/P_n^\iota X)_{\mathrm{tor}} \otimes O_{P_n} \to \mathrm{Hom}(H^1_{\mathcal{F}}(K, A_{P_n}), D_{P_n})_{\mathrm{tor}} \tag{7}$$

has kernel and cokernel whose orders are bounded as n varies. By Proposition 4.16, the last group is isomorphic to $M(P_n)^2$ for a finite O_{P_n}-module $M(P_n)$.

Similar to [How04, Theorem 2.2.10(b)] we can prove the following.

PROPOSITION 4.19. *Suppose that K is an imaginary quadratic field where p splits completely, and let K_∞ is the anti-cyclotomic $\mathbb{Z}_p$-extension of K. Then there are an integer r and a Λ-torsion module Y such that we have*

$$H^1_{\mathcal{F}}(K, \mathrm{Hom}(\Lambda, A))^\vee \sim \Lambda^r \oplus Y^2$$

where $\sim$ is a pseudo-isomorphism.

4.4 The corank of Selmer groups

We let Σ be the set of bad reduction primes for E of K, primes of K lying above p, and infinite places, and containing none else. We borrow the notation $\mathfrak{p}$, $\bar{\mathfrak{p}}$, Q_i, and $\overline{Q_i}$ from § 4.2.

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Definition 4.20. Let $n \geqslant N_2$ and let $\hat{E}^-(K_{n,Q_i})$ denote $\hat{E}^-(m_{K_{n,Q_i}})$.

For $i = 1, \ldots, p^{N_1}$ we define $H^1_f(K_{n,Q_i}, A) := \hat{E}^-(K_{n,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and define $H^1_f(K_{n,\overline{Q_i}}, A)$ similarly. For a place v of K_n not lying above p, we define $H^1_f(K_{n,v}, A) := E(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

We define minus-Selmer groups over K_n $(n \geqslant N_2)$ as

$$\mathrm{Sel}_p^-(E/K_n) = \ker\left(H^1(K_\Sigma/K_n, A) \to \prod_{v|l \text{ for } l\in\Sigma} \frac{H^1(K_{n,v}, A)}{H^1_f(K_{n,v}, A)} \right),$$

and $\mathrm{Sel}_p^-(E/K_\infty)$ as the direct limit of them over n.

We define a Selmer group over K_n as

$$\mathrm{Sel}_p(E/K_n) = \ker\left(H^1(K_\Sigma/K_n, A) \to \prod_{v|l \text{ for } l\in\Sigma} \frac{H^1(K_{n,v}, A)}{E(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right),$$

and define $\mathrm{Sel}_p(E/K_\infty)$ as the direct limit of them over n.

When χ is a character of $\mathrm{Gal}(K_n/K_{N_2})$, we let $\mathbb{Z}_p[\chi] := \mathbb{Z}_p[\chi(\gamma^{p^{N_2}})]$ and for a G_n-module M let $M^\chi := (M \otimes \mathbb{Z}_p[\chi])^\chi$. We say that χ is a primitive character of $\mathrm{Gal}(K_n/K_{N_2})$ if $\chi(\mathrm{Gal}(K_n/K_{n-1}))$ is not 1.

Lemma 4.21. *Assume that n is larger than N_2. If $n - N_2$ is odd and χ is a primitive character of $\mathrm{Gal}(K_n/K_{N_2})$, we have*

$$\mathrm{corank}_{\mathbb{Z}_p[\chi]}(\mathrm{Sel}_p(E/K_n)^\chi) = \mathrm{corank}_{\mathbb{Z}_p[\chi]}(\mathrm{Sel}_p^-(E/K_\infty)^{\Gamma_n})^\chi.$$

Proof. From the definition we can check that the cokernel of $\mathrm{Sel}_p^-(E/K_n)^\chi \to \mathrm{Sel}_p(E/K_n)^\chi$ is contained in

$$\prod_{i=1}^{p^{N_1}} \left(\frac{\hat{E}(K_{n,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{\hat{E}^-(K_{n,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\chi \cdot \prod_{i=1}^{p^{N_1}} \left(\frac{\hat{E}(K_{n,\overline{Q_i}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{\hat{E}^-(K_{n,\overline{Q_i}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\chi.$$

We can easily check

$$\frac{\hat{E}(K_{n,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{\hat{E}^-(K_{n,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \cong \frac{\hat{E}(K_{n,Q_i})}{\hat{E}^-(K_{n,Q_i})} \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

We have

$$\begin{aligned} \mathrm{corank}_{\mathbb{Z}_p[\chi]} \left(\frac{\hat{E}(K_{n,Q_i})}{\hat{E}^-(K_{n,Q_i})} \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^\chi &= \mathrm{rank}_{\mathbb{Z}_p[\chi]} \left(\frac{\hat{E}(K_{n,Q_i})}{\hat{E}^-(K_{n,Q_i})} \right)^\chi \\ &= \mathrm{rank}_{\mathbb{Q}_p[\chi]}(\hat{E}(K_{n,Q_i}) \otimes \mathbb{Q}_p)^\chi - \mathrm{rank}_{\mathbb{Q}_p[\chi]}(\hat{E}^-(K_{n,Q_i}) \otimes \mathbb{Q}_p)^\chi \\ &= p^{N_2-N_1} - p^{N_2-N_1} = 0. \end{aligned}$$

Thus, we can conclude that $\mathrm{corank}_{\mathbb{Z}_p[\chi]}\mathrm{Sel}_p^-(E/K_n)^\chi = \mathrm{corank}_{\mathbb{Z}_p[\chi]}\mathrm{Sel}_p(E/K_n)^\chi$.

On the other hand, consider the following diagram.

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}_p^-(E/K_n) & \longrightarrow & H^1(K_\Sigma/K_n, A) & \longrightarrow & \displaystyle\prod_{v|l, l\in\Sigma} H^1(K_{n,v}, A)/H^1_f(K_{n,v}, A) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Sel}_p^-(E/K_\infty)^{\Gamma_n} & \longrightarrow & H^1(K_\Sigma/K_\infty, A)^{\Gamma_n} & \longrightarrow & \displaystyle\prod_{w|l, l\in\Sigma} H^1(K_{\infty,w}, A)/H^1_f(K_{\infty,w}, A) \end{array}$$

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

The middle vertical map has trivial kernel and cokernel. For a place $v \nmid p$ of K_n, the kernel of

$$\frac{H^1(K_{n,v}, A)}{E(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \to \prod_{w|v} \frac{H^1(K_{\infty,w}, A)}{E(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

is finite by [Gre99, Lemma 3.3].

The kernel of

$$\left(\frac{H^1(K_{n,Q_i}, A)}{\hat{E}^-(K_{n,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^\chi \to \left(\frac{H^1(K_{\infty,Q_i}, A)}{\hat{E}^-(K_{\infty,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^\chi$$

is

$$\left(\frac{(\hat{E}^-(K_{\infty,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n}}{E^-(K_{n,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^\chi.$$

Because we have $\hat{E}^-(K_{\infty,Q_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p{}^\vee \cong \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K_{N_2})]]$, the χ-parts of the numerator and the denominator of this group have the same corank. Thus, this group is finite.

Therefore, the cokernel of $\mathrm{Sel}_p^-(E/K_n)^\chi \to (\mathrm{Sel}_p^-(E/K_\infty)^{\Gamma_n})^\chi$ is finite as well. □

We let N denote the conductor of E. For the rest of this section we assume that K is an imaginary quadratic field such that every prime l dividing N splits completely in K (the so-called 'Heegner hypothesis'). In addition, we assume that p splits completely in K. We define Heegner points of E over the ring class field extensions of K of conductor p^n as follows (see [Gro84]).

Definition 4.22 (Heegner points). Let $\mathcal{O}_K$ be the ring of integers of K. We may choose an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. For an integer $c \geqslant 1$, we let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ denote the unique order of O_K of conductor c. It is known that $H_c = K(j(O_c))$ is the ring class field of conductor c over K. If $(c, N) = 1$, then $\mathcal{N}_c = \mathcal{O}_c \cap \mathcal{N}$ is an invertible ideal in $\mathcal{O}_c$ satisfying $\mathcal{O}_c/\mathcal{N}_c \cong \mathbb{Z}/N\mathbb{Z}$. The cyclic N-isogeny

$$[\mathbb{C}/\mathcal{O}_c \to \mathbb{C}/\mathcal{N}_c^{-1}]$$

defines a non-cuspidal point on the modular curve $X_0(N)$, which is defined over H_c. The image of this point under the modular parametrization

$$\pi : X_0(N) \to E$$

is denoted by $\bar{x}_c \in E(H_c)$ and called a Heegner point of conductor c on E.

The union of the ring class fields of conductor p^n for $n \geqslant 0$ $H_{p^\infty} = \bigcup H_{p^n}$ contains the anti-cyclotomic $\mathbb{Z}_p$-extension K_∞ of K, and its Galois group has decomposition

$$\mathrm{Gal}(H_{p^\infty}/K) \cong G_0 \times \mathrm{Gal}(K_\infty/K)$$

where G_0 is the finite torsion subgroup of $\mathrm{Gal}(H_{p^\infty}/K)$. For $n \geqslant 0$ we have

$$\mathrm{Gal}(H_{p^{n+1}}/K) \cong G_0 \times \mathrm{Gal}(K_{n+n_0}/K),$$

for some fixed number n_0. We define a Heegner point for K_{n+n_0} by

$$x_{n+n_0} = Tr_{H_{p^{n+1}}/K_{n+n_0}}(\bar{x}_{p^{n+1}}) \in E(K_{n+n_0}).$$

The Heegner points x_n satisfy the following distribution property

$$Tr_{K_{n+1}/K_n}(x_{n+1}) = a_p x_n - x_{n-1}$$

for $n \geqslant n_0 + 1$ where the local Euler factor of E at p is $1 - a_p X + pX^2$. Since p is a supersingular reduction prime and $p > 3$, we have $a_p = 0$.

Theorem 4.23 [Vat03, Theorem 1.4]. *The χ-component of x_n is non-torsion for all but finitely many primitive characters χ of $\mathrm{Gal}(K_n/K)$ as $n > n_0$ varies.*

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Proof. We recall that we have the decomposition

$$\mathrm{Gal}(H_{p^\infty}/K) \cong G_0 \times \mathrm{Gal}(K_\infty/K).$$

Let χ' be a character of $\mathrm{Gal}(H_{p^{n+1}}/K)$. When p is a good supersingular reduction prime, Vatsal [Vat03] proved that the χ'-component of $\bar{x}_{p^{n+1}}$ is non-torsion if the order of the character χ' on the tame part ($= G_0$) is prime to p and n is large enough (the condition on G_0 is not stated in [Vat03, Theorem 1.4], but it is used in the proof). In our case the character χ on the tame part is trivial, therefore our claim follows. Cornut and Vatsal have produced a much more general result on CM-points of Shimura varieties [CV05, CV07]. □

Because we assume the Heegner hypothesis, the discriminant of K is prime to the conductor of E, hence E does not have CM by K. Then we have the following.

Theorem 4.24 (see [Nek06b]). *Let χ' be a character of $\mathrm{Gal}(H_{p^{n+1}}/K)$. If χ'-component of $\bar{x}_{p^{n+1}}$ is non-torsion, then the corank of χ'-part of $\mathrm{Sel}_p(E/H_{p^{n+1}})$ is 1.*

Combining all of the discussed results, we obtain the following.

Proposition 4.25. *We have*

$$\mathrm{corank}_\Lambda Sel_p^-(E/K_\infty) = 1.$$

Proof. For an integer $n > N_2$, let χ be a primitive character of $\mathrm{Gal}(K_n/K_{N_2})$. The χ-part of $\mathrm{Sel}_p(E/K_n)$ is the sum of χ'-parts of $\mathrm{Sel}_p(E/K_n)$ when χ' runs over all characters of $\mathrm{Gal}(K_n/K)$ whose restriction on $\mathrm{Gal}(K_n/K_{N_2})$ are equal to χ (and these characters are certainly primitive for $\mathrm{Gal}(K_n/K)$). Thus, if n is large enough, by Theorems 4.23 and 4.24 we obtain $\mathrm{corank}_{\mathbb{Z}_p[\chi]}\mathrm{Sel}_p(E/K_n)^\chi = p^{N_2}$. Combined with Lemma 4.21, this implies that the Λ-corank of $\mathrm{Sel}_p^-(E/K_\infty)$ is equal to 1. □

Now we want to relate $\mathrm{Sel}_p^-(E/K_\infty)$ with $H^1_{\mathcal{F}}(K, \mathrm{Hom}(\Lambda, A))$.

Proposition 4.26. *We have*

$$H^1_{\mathcal{F}}(K, \mathrm{Hom}(\Lambda, A)) \cong \mathrm{Sel}_p^-(E/K_\infty).$$

Proof. Since a prime in $\Sigma - \{p\}$ splits completely in K by assumption and $H_{p^{n+1}}$ is the ring class field for $\mathbb{Z}+p^{n+1}O_K$, that prime does not split completely over K_∞/K (without this property we will get a homomorphism with a cokernel whose exponent is finite, although its order might be infinite; this is not a huge problem for proving the parity conjecture, but it certainly is a technicality we want to avoid). Thus, when a prime w of K_∞ lies above such a prime v, $K_{\infty,w}/K_v$ is a $\mathbb{Z}_p$-extension.

The maps in § 2 give isomorphisms

$$\begin{aligned} Sh &: H^1(K_\Sigma/K, \mathrm{Hom}(\Lambda, A)) \to H^1(K_\Sigma/K_\infty, A), \\ Sh_{\mathfrak{p}} &: H^1(K_{\mathfrak{p}}, \mathrm{Hom}(\Lambda, A)) \to \prod_{i=1}^{p^{N_1}} H^1(K_{\infty,Q_i}, A) \\ Sh_v &: H^1(K_v, \mathrm{Hom}(\Lambda, A)) \to \prod_{w|v} H^1(K_{\infty,w}, A). \end{aligned}$$

By definition $Sh_{\mathfrak{p}}(H^1_{\mathcal{F}}(K_{\mathfrak{p}}, \mathrm{Hom}(\Lambda, A))) = \mathbb{H}^-_{\mathfrak{p},\infty}$ and, discussed in § 2, $Sh_v(H^1_{ur}(K_v, \mathrm{Hom}(\Lambda, A))) = \prod_{w|v} H^1_{ur}(K_{\infty,w}, A)$.

By [Rub87, Lemma B.3.3], $H^1_{ur}(K_{\infty,w}, A) = 0$. Since $v \nmid p$, $E(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. Our claim follows. □

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Combining Propositions 4.19, 4.25, and 4.26, we obtain the following.

COROLLARY 4.27. *We have*

$$\mathrm{Sel}_p^-(E/K_\infty)^\vee \sim \Lambda \oplus Y^2,$$

for a Λ-torsion module Y.

4.5 Main result

The proof of this section follows [Nek01] very closely. We assume the underlying hypothesis on K stated before Definition 4.22.

PROPOSITION 4.28. *We have that* $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/K)$ *is odd.*

Proof. First we examine the kernel and cokernel of $\mathrm{Sel}_p(E/K) \to \mathrm{Sel}_p^-(E/K_\infty)^\Gamma$. For a place $v \nmid p$ and a place $w|v$ of K_∞ we check that $\ker(H^1(K_v, A) \to H^1(K_{\infty,w}, A)) = H^1_{ur}(K_v, A)$ is finite.

The kernel of $H^1(K_\mathfrak{p}, A)/E(K_\mathfrak{p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \prod_{i=1}^{p^{N_2}} H^1(K_{\infty,Q_i}, A)/\mathbb{H}_\mathfrak{p}$ is $(\mathbb{H}_\mathfrak{p})^\Gamma/E(K_\mathfrak{p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. It is 0, since $(\mathbb{H}_\mathfrak{p})^\Gamma \cong \mathbb{Q}_p/\mathbb{Z}_p$ and $E(K_\mathfrak{p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is divisible and of corank 1. Since $H^1(K, A) \to H^1(K_\infty, A)^\Gamma$ is an isomorphism, $\mathrm{Sel}_p(E/K) \to \mathrm{Sel}_p^-(E/K_\infty)^\Gamma$ has finite kernel and cokernel.

From Corollary 4.27 it follows that the $\mathbb{Z}_p$-corank of $(\mathrm{Sel}_p^-(E/K_\infty))^\Gamma$ is odd, thus we obtain our claim. □

THEOREM 4.29. *We have*

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/K) \equiv \mathrm{ord}_{s=1}L_{/K}(E,s) \equiv 1 \pmod 2.$$

Proof. On the algebraic side we have

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/K) \equiv 1 \pmod 2$$

by Proposition 4.28. On the analytic side, K satisfies the Heegner hypothesis, which implies that the root number of the functional equation is -1. Therefore, we have

$$\mathrm{ord}_{s=1}L_{/K}(E,s) \equiv 1 \pmod 2.$$ □

When D is a negative square-free integer, let E_D be the quadratic twist of E by the nontrivial character of $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$. Then we have

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/\mathbb{Q}(\sqrt{D})) = \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/\mathbb{Q}) + \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E_D/\mathbb{Q}), \tag{8}$$

$$\mathrm{ord}_{s=1}L_{/\mathbb{Q}(\sqrt{D})}(E,s) = \mathrm{ord}_{s=1}L_{/\mathbb{Q}}(E,s) + \mathrm{ord}_{s=1}L_{/\mathbb{Q}}(E_D,s). \tag{9}$$

We can finally obtain our main result.

THEOREM 4.30. *Let E be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at $p > 3$. Then we have*

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/\mathbb{Q}) \equiv \mathrm{ord}_{s=1}L_{/\mathbb{Q}}(E,s) \pmod 2.$$

Proof. When $\mathrm{ord}_{s=1}L_{/\mathbb{Q}}(E,s)$ is odd, by [Wal84] there are infinitely many negative square-free integers D such that the Heegner hypothesis holds for $\mathbb{Q}(\sqrt{D})$, p splits completely in $\mathbb{Q}(\sqrt{D})$, and $\mathrm{ord}_{s=1}L_{/\mathbb{Q}}(E_D,s) = 0$. By the results of Kolyvagin [Kol90], we have

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E_D/\mathbb{Q}) = 0;$$

thus, from Theorem 4.29 and (8), it follows that $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/\mathbb{Q})$ is odd.

When $\mathrm{ord}_{s=1}L_{/\mathbb{Q}}(E,s)$ is even, choose a negative square-free integer D such that the Heegner hypothesis holds for $\mathbb{Q}(\sqrt{D})$, p splits completely in $\mathbb{Q}(\sqrt{D})$, and $p \nmid D$. Then E_D has obviously good supersingular reduction at p, and from (9) it follows that $\mathrm{ord}_{s=1}L_{/\mathbb{Q}}(E_D,s)$ is odd. Previously we showed that if $\mathrm{ord}_{s=1}L_{\mathbb{Q}}(E_D,s)$ is odd, then $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E_D/\mathbb{Q})$ is odd. From Theorem 4.29 and (8) it follows that $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/\mathbb{Q})$ is even. □

https://doi.org/10.1112/S0010437X06002569 Published online by Cambridge University Press

Acknowledgements

Much of the study in this paper was done during the author's PhD program. The author is very grateful to Karl Rubin for sharing his deep wisdom in mathematics and for his guidance throughout and even after the author's graduate study. The author also extends his thanks to the Mathematics Department of Stanford University. The author wishes to give thanks to Ralph Greenberg for his heartfelt help and advice. Finally, the author gives due thanks to the referee for pointing out a gap which led to a significant change in the final version.

References

CV05 C. Cornut and V. Vatsal, *CM points and quaternion algebras*, Doc. Math. **10** (2005), 263–309.

CV07 C. Cornut and V. Vatsal, *Nontriviality of Rankin–Selberg L-functions and CM points*, in *L-functions and Galois representations*, Proc. LMS Durham Symposium, 2004, to appear.

Des87 E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Perspectives in Mathematics, vol. 3 (Academic Press, New York, 1987).

Gre99 R. Greenberg, *Iwasawa theory for elliptic curves*, in *Arithmetic theory of elliptic curves. Lectures from the 3rd CIME session held in Cetraro, 12–19 July 1997*, ed. C. Viola, Lecture Notes in Mathematics, vol. 1716 (Springer, Berlin; Centro Internazionale Matematico Estivo (CIME), Florence, 1999), 51–144.

Gro84 B. Gross, *Heegner points on $X_0(N)$*, in *Modular forms*, Durham, 1983, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res. (Horwood, Chichester, 1984), 87–105.

Hon70 T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), 213-246.

How04 B. Howard, *The Heegner point Kolyvagin system*, Compositio. Math. **140** (2004), 1439–1472.

IP06 A. Iovita and R. Pollack, *Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields*, J. reine angew. Math. **598** (2006), 71–103.

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

Kol90 V. Kolyvagin, *Euler systems*, in *The Grothendieck Festschrift, Vol. II*, Progress in Mathematics, vol. 87 (Birkhäuser, Boston, MA, 1990), 435–483.

MR04 B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799.

Nek01 J. Nekovář, *On the parity of ranks of Selmer groups. II*, C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), 99–104.

Nek06a J. Nekovář, *Selmer complexes*, Astérisque, to appear.

Nek06b J. Nekovář, *The Euler system method for CM points on Shimura curves*, in *L-functions and Galois representations*, Proc. LMS Durham Symposium, 2004, to appear.

Rub87 K. Rubin, *Local units, elliptic units, Heegner points and elliptic curves*, Invent. Math. **88** (1987), 405–422.

Rub00 K. Rubin, *Euler systems*, in *Hermann Weyl Lectures*, Annals of Mathematics Studies, vol. 147 (The Institute for Advanced Study and Princeton University Press, Princeton, NJ, 2000).

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

Wal84 J.-L. Waldspurger, *Correspondences de Shimura*, in *Proceedings of the International Congress of Mathematicians*, Warsaw, 1983, vols 1, 2 (PWN, Warsaw, 1984), 525–531.

Byoung Du (B. D.) Kim bdkim@math.mcmaster.ca
Department of Mathematics and Statistics, McMaster University, 1280 Main Street West, Hamilton, Ontario L8S 4K1, Canada