FINDING LARGE SELMER GROUPS

BARRY MAZUR AND KARL RUBIN

1. Introduction

Raoul Bott has inspired many of us by the magnificence of his ideas, by the way he approaches and explains mathematics, and by his warmth, friendship, and humor. In celebration of Raoul's eightieth birthday we offer this brief article in which we will explain how the recent cohomological ideas of Jan Nekovář [N2] imply (under mild hypotheses plus the Shafarevich-Tate conjecture) systematic growth of the ranks of the group of rational points in certain elliptic curves as one ascends the finite layers of appropriate towers of number fields.

Let K/k be a quadratic extension of number fields, and denote by σ the nontrivial automorphism of K/k. Let p be an odd prime number.

By a $\mathbf{Z}_p$-power extension of K we mean an abelian extension L/K with Galois group $\mathbf{Z}_p^d$ for some d. If L/K is a $\mathbf{Z}_p$-power extension and L/k is Galois, then σ acts on $\mathrm{Gal}(L/K)$ and we will say that L/K is *k-positive* (resp. *k-negative*) if σ acts trivially (resp. by the scalar -1) on $\mathrm{Gal}(L/K)$. Thus L/k is abelian if L/K is k-positive, and $\mathrm{Gal}(L/k)$ is a generalized dihedral group if L/K is k-negative.

For any such K/k there is a *maximal* k-positive $\mathbf{Z}_p$-power extension $\mathcal{K}^+$, and a *maximal* k-negative one $\mathcal{K}^-$. The extension $\mathcal{K}^+/K$ is always nontrivial because $\mathcal{K}^+$ contains the cyclotomic $\mathbf{Z}_p$-extension of K. The extension $\mathcal{K}^-/K$ is nontrivial if K is not totally real (see Lemma 3.2).

If E is an elliptic curve defined over K and L is a (possibly infinite) extension of K, say that E has *Mordell-Weil growth relative to L/K* if for every finite extension F of K in L, the rank of the Mordell-Weil group $E(F)$ is at least $[F : K]$. In particular, if $[L : K]$ is infinite this property will imply that the Mordell-Weil rank of E over L is infinite. Say that E has *p-Selmer growth relative to L/K* if the pro-p-Selmer rank of E over F is at least $[F : K]$ for all finite extensions F of K in L.

Recent work of Nekovář ([N2], especially §10.7) shows that under extremely mild hypotheses, if E is an elliptic curve over k that has odd pro-p-Selmer rank over K and that is of good ordinary reduction at the primes above p, then E has p-Selmer growth relative to $\mathcal{K}^-/K$. Assuming the Shafarevich-Tate conjecture, this is equivalent to the statement that (under the same hypotheses) if E has odd Mordell-Weil rank over K, then it has Mordell-Weil growth relative to either $\mathcal{K}^-/K$.

In this paper we do two things. First, we give a somewhat different exposition of Nekovář's theorem, in the hope of making this important result more accessible and widely known. Namely, we will show how to derive a weaker version of Nekovář's theorem (Theorem 3.1 below) from the main result of [MR2] (which in turn relies

version of March 15 2005

The authors are supported by NSF grants DMS-0403374 and DMS-0140378, respectively.

crucially on [N2]) using a pair of functional equations satisfied by an "algebraic" p-adic L-function attached to E over K.

Second, we describe some conditions under which we can prove that the pro-p-Selmer rank and/or the Mordell-Weil rank of E over K are necessarily odd (Corollaries 3.6 and 3.7). This enables us to give families of examples (see §5) of $\mathbf{Z}_p^d$-extensions with p-Selmer growth.

An important instance of the above setup is when K is a quadratic imaginary field, $k = \mathbf{Q}$, and σ is complex conjugation. In this case $\mathcal{K}^+$ is the cyclotomic $\mathbf{Z}_p$-extension of K and $\mathcal{K}^-$ is the anti-cyclotomic $\mathbf{Z}_p$-extension of K. The results of Cornut, Vatsal, and Nekovář [C, V, N1] show that if E is defined over $\mathbf{Q}$, E has good ordinary reduction at p, and $\operatorname{rank}(E(K))$ is odd, then E has Mordell-Weil growth relative to $\mathcal{K}^-/K$. (See also the recent preprint [CV] of Cornut and Vatsal generalizing their work to CM-fields.)

There are other prior results that unconditionally imply only p-Selmer growth (as ours do) rather than Mordell-Weil growth, relative to the anticyclotomic $\mathbf{Z}_p$-extension $\mathcal{K}^-/K$ of an imaginary quadratic field. Greenberg proved in [G1] that if E is an elliptic curve over $\mathbf{Q}$ with complex multiplication by K, $p > 3$ is a prime of good ordinary reduction for E, and $\operatorname{ord}_{s=1} L(E/\mathbf{Q}, s)$ is odd, then E has p-Selmer growth relative to $\mathcal{K}^-/K$. Skinner and Urban prove in a recent preprint [SU] that given a p-ordinary classical newform of arbitrary weight at least 2 and of odd analytic rank over a quadratic imaginary field K, and satisfying some mild conditions, its pro-p-Selmer group has p-Selmer growth relative to $\mathcal{K}^-/K$.

Most of the work in this article is on the "algebraic," rather than the "analytic," aspect of the arithmetic. However, the motivation for our work is analytic, in the sense that our main result would follow fairly directly from a generalized version of the Parity conjecture. Namely, if F is a finite extension of K in $\mathcal{K}^-$ and ψ is a character of $\operatorname{Gal}(F/K)$, the Parity conjecture gives the first and last congruences

$$\begin{aligned}\operatorname{rank}(E(K)) \equiv \operatorname{ord}_{s=1} L(E/K, s) &\equiv \operatorname{ord}_{s=1} L(E/K, \psi, s) \\ &\equiv \text{multiplicity of } \psi \text{ in } E(F) \otimes \mathbf{C} \pmod 2\end{aligned}$$

and the middle one is a root number calculation. Our result (if we assume the Shafarevich-Tate conjecture) is the weaker implication that for every such ψ

$$\operatorname{rank}(E(K)) \text{ is odd} \Rightarrow \text{the multiplicity of } \psi \text{ in } E(F) \otimes \mathbf{C} \text{ is positive.}$$

See Corollaries 3.6 and 3.7 for special cases in which we can replace our "odd rank" assumption by a root number assumption (i.e., a congruence condition on the conductor of $E/\mathbf{Q}$).

We conclude this introduction with two potential generalizations of the results of this paper.

First, in general $L(E/K, s)$ will factor into a product of L-functions. It is possible that $\operatorname{ord}_{s=1} L(E/K, s)$ is even because an even number of the factors have odd-order vanishing. In this case we expect that $\operatorname{rank}(E(K))$ is even, so the results of this paper would not apply. However, we expect that the individual factors of $L(E/K, s)$ that vanish will contribute $\mathbf{Z}_p$-power extensions of L/K where E has p-Selmer growth. This should lead to examples in which the pro-p-Selmer rank of E over F is at least $r[F : K]$ for every finite extension F of K in L, with $r > 1$.

Second, the results of this paper for Selmer groups of elliptic curves should also apply to Selmer groups of (classical) p-ordinary newforms of arbitrary even weight $k \geq 2$.

We hope to deal with these generalizations in a future paper, by refining the results of [MR2] and combining those refined results with the methods of this paper.

We would like to thank Jay Pottharst for reading a preliminary version of this paper and for providing us with a simpler version of Lemmas 6.3 and 6.4.

2. The setting

Fix an elliptic curve E defined over a number field k, and a rational prime $p > 2$. For every finite extension F of k we have the p-power Selmer group

$$\mathrm{Sel}_p(E,F) := \ker\biggl(H^1(F, E[p^\infty]) \longrightarrow \prod_v H^1(F_v, E)\biggr),$$

where $E[p^\infty]$ is the Galois module of p-power torsion on E, and the product is over all places v of F. This Selmer group sits in an exact sequence

$$0 \longrightarrow E(F) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}_p(E,F) \longrightarrow Ш(E,F)[p^\infty] \longrightarrow 0$$

where $Ш(E,F)[p^\infty]$ is the p-primary part of the Shafarevich-Tate group of E over F. If F is an arbitrary algebraic extension of $\mathbf{Q}$, we define

$$\mathrm{Sel}_p(E,F) := \varinjlim \mathrm{Sel}_p(E,F'),$$

direct limit (with respect to restriction maps on Galois cohomology) over finite extensions F' of k in F, and the Pontrjagin dual

$$\mathcal{S}_p(E,F) := \mathrm{Hom}(\mathrm{Sel}_p(E,F), \mathbf{Q}_p/\mathbf{Z}_p).$$

Throughout this paper, if M is a module over an integral domain R, the R-rank of M will be defined by $\mathrm{rank}_R(M) := \dim_{\mathrm{Frac}(R)} M \otimes_R \mathrm{Frac}(R)$, where $\mathrm{Frac}(R)$ is the field of fractions of R.

Fix a quadratic extension K of k and let σ denote the nontrivial automorphism of K/k. Let $\mathcal{K}$ denote the maximal $\mathbf{Z}_p$-power extension of K (the compositum of all $\mathbf{Z}_p$-extensions of K) and $\Gamma := \mathrm{Gal}(\mathcal{K}/K)$. Then $\mathcal{K}$ is Galois over k, and so σ acts on Γ. We let $\Gamma^\pm$ denote the subgroup of Γ on which σ acts by ± 1, and let $\mathcal{K}^\pm$ be the fixed field of $\Gamma^\mp$, so that $\mathrm{Gal}(\mathcal{K}^\pm/K) \cong \Gamma^\pm$. Then $\mathcal{K}^+$ is the maximal k-positive $\mathbf{Z}_p$-power extension of K, and $\mathcal{K}^-$ is the maximal k-negative one, as discussed in the introduction. Putting $d_\pm = \mathrm{rank}_{\mathbf{Z}_p}(\Gamma^\pm)$, Leopoldt's conjecture for K implies that $d_+ = r_2(k) + 1$ and $d_- = r_2(K) - r_2(k)$, where r_2 denotes the number of conjugate pairs of complex embeddings of a number field.

For example, if K is an imaginary quadratic field, then $k = \mathbf{Q}$, $d_+ = d_- = 1$ and $\mathcal{K}^+$ and $\mathcal{K}^-$ are the usual cyclotomic and anticyclotomic $\mathbf{Z}_p$-extensions of K.

If K_v is the completion of K at a prime v, we denote by $E_0(K_v)$ the subgroup of points of $E(K_v)$ with nonsingular reduction, so $[E(K_v) : E_0(K_v)]$ is the Tamagawa number at v in the Birch and Swinnerton-Dyer conjecture for E/K.

We will assume the following throughout this paper:

$$p > 2 \text{ and } E \text{ has good ordinary reduction at all primes of } K \text{ above } p, \tag{2.1}$$

$$E(K) \text{ has no } p\text{-torsion}, \tag{2.2}$$

$$\text{for every prime } v \text{ of } K \text{ of bad reduction, } [E(K_v) : E_0(K_v)] \text{ is prime to } p. \tag{2.3}$$

3. Results

Assume for this section that (2.1), (2.2), and (2.3) hold. The following theorem is a weakened version of Nekovář's Theorem 10.7.17 [N2] (Nekovář shows that in fact the conclusion holds with $\epsilon =$ "$-$").

Theorem 3.1. *Suppose that* (2.1), (2.2), *and* (2.3) *hold. If* $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ *is odd, then for at least one sign* $\epsilon =$ "$+$" *or* "$-$" *we have*

(i) $\mathcal{S}_p(E,\mathcal{K}^\epsilon)$ *is not a torsion* $\mathbf{Z}_p[[\Gamma^\epsilon]]$*-module,*
(ii) *for every finite extension* F *of* K *in* $\mathcal{K}^\epsilon$ *the Selmer module* $\mathcal{S}_p(E,F)$ *has a submodule isomorphic to* $\mathbf{Z}_p[\mathrm{Gal}(F/K)]$*, and in particular*

$$\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,F)) \geq [F:K].$$

We will give a proof of Theorem 3.1 in §10. Our method is to show that there is an "algebraic p-adic L-function" satisfying two different functional equations (see Corollary 9.2), and taken together these functional equations imply the theorem. In addition, assuming a standard conjecture we will show (as Nekovář does) that Theorem 3.1 holds with $\epsilon =$ "$-$" (see Corollary 3.5 below).

See Proposition 4.1 below for an explanation of why one would expect a result like Theorem 3.1 to hold.

Theorem 3.1(ii) says that E has p-Selmer growth relative to $\mathcal{K}^\epsilon/K$, using the terminology of the introduction. The following lemma shows that this statement is often nontrivial.

Lemma 3.2. *If* K *is not totally real then both* $[\mathcal{K}^+ : K]$ *and* $[\mathcal{K}^- : K]$ *are infinite.*

Proof. We need to show that both d_+ and d_- are positive. We have $d_+ \geq 1$ since $K\mathbf{Q}_\infty \subset \mathcal{K}^+$. Class field theory shows that $d_- \geq r_2(K) - r_2(k)$ (with equality if Leopoldt's conjecture holds), and we have $r_2(K) \geq 2r_2(k)$ since each complex place of k splits in K. Therefore if K is not totally real then $r_2(K) > r_2(k)$ and $d_- > 0$. □

Before giving some corollaries of Theorem 3.1 we recall two well-known conjectures. Let $\mathbf{Q}_\infty$ denote the (cyclotomic) $\mathbf{Z}_p$-extension of $\mathbf{Q}$.

p-primary Shafarevich-Tate Conjecture. *For every finite extension* F *of* K *in* $\mathcal{K}$*, the* p*-part* $Ш(E,F)[p^\infty]$ *of the Shafarevich-Tate group of* E *over* F *is finite.*

Torsion Conjecture ([M])**.** *The Selmer module* $\mathcal{S}_p(E,K\mathbf{Q}_\infty)$ *is a torsion* $\mathbf{Z}_p[[\mathrm{Gal}(K\mathbf{Q}_\infty/K)]]$*-module.*

Remark 3.3. If $Ш(E,F)[p^\infty]$ is finite, then $\mathcal{S}_p(E,F) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p = E(F) \otimes_{\mathbf{Z}} \mathbf{Q}_p$. Thus if the p-primary Shafarevich-Tate conjecture holds, then in Theorem 3.1 and the corollaries below we can replace the Selmer groups $\mathcal{S}_p(E,K)$ and $\mathcal{S}_p(E,F)$ by the Mordell-Weil groups $E(K)$ and $E(F)$ (and replace $\operatorname{rank}_{\mathbf{Z}_p}$ by $\operatorname{rank}_{\mathbf{Z}}$).

Corollary 3.4. *Suppose that* $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ *is odd.*

(i) *If* K *is not totally real then* $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,F))$ *is unbounded as* F *runs through finite extensions of* K *in* $\mathcal{K}$*.*
(ii) *More generally, if* L *is a* $\mathbf{Z}_p^d$*-extension of* K *that is Galois over* k*, and the nontrivial automorphism* σ *of* K/k *acts on* $\mathrm{Gal}(L/K)$ *with both eigenvalues* $+1$ *and* -1*, then* $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,F))$ *is unbounded as* F *runs through finite extensions of* K *in* L*.*

Proof. First consider (ii). Since σ acts on $\mathrm{Gal}(L/K)$ with both eigenvalues $+1$ and -1, we have that both $L \cap \mathcal{K}^+$ and $L \cap \mathcal{K}^-$ have infinite degree over K. Thus assertion (ii) follows directly from Theorem 3.1(ii).

Assertion (i) now follows from (ii) and Lemma 3.2. □

The following result was proved by Nekovář ([N2] Theorem 10.7.17) even without assuming the Torsion conjecture.

Corollary 3.5. *Suppose that* $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ *is odd and that the Torsion conjecture holds. Then Theorem 3.1 holds with the sign* $\epsilon =$ "$-$", *i.e.,*

(i) $\mathcal{S}_p(E,\mathcal{K}^-)$ *is not a torsion* $\mathbf{Z}_p[[\Gamma^-]]$*-module,*
(ii) *for every finite extension* F *of* K *in* $\mathcal{K}^-$ *the Selmer module* $\mathcal{S}_p(E,F)$ *has a submodule isomorphic to* $\mathbf{Z}_p[\mathrm{Gal}(F/K)]$*, and in particular*

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,F)) \geq [F:K].$$

Proof. If the Torsion conjecture holds then by Corollary 6.6 below $\mathcal{S}_p(E,\mathcal{K}^+)$ is a torsion $\mathbf{Z}_p[[\Gamma^+]]$-module, and so the corollary follows from Theorem 3.1. □

The following two corollaries apply when the elliptic curves E is defined over $\mathbf{Q}$, and the field K is Galois over $\mathbf{Q}$. They replace the condition "$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ is odd" by group-theoretic conditions on $\mathrm{Gal}(K/\mathbf{Q})$ and congruence conditions on the conductor of E. We will deduce both of them from Corollary 3.5 in §11, by showing that their hypotheses imply that $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ is odd. Corollary 3.6 assumes the p-primary Shafarevich-Tate conjecture, while Corollary 3.7 does not, and the two corollaries make different assumptions about $\mathrm{Gal}(K/\mathbf{Q})$.

Corollary 3.6. *Suppose that the* p*-primary Shafarevich-Tate conjecture and the Torsion conjecture hold, and that*

(a) E *is defined over* $\mathbf{Q}$ *and* K *is a Galois extension of* $\mathbf{Q}$ *whose discriminant is relatively prime to the conductor* N_E *of* E*,*
(b) $\Delta := \mathrm{Gal}(K/\mathbf{Q})$ *is the semidirect product of a (normal) subgroup of odd order with a nontrivial cyclic* 2*-group,*
(c) *the Dirichlet character* χ *corresponding to the (unique) quadratic field contained in* K *satisfies* $\chi(-N_E) = -1$*.*

Then for every subfield k *of* K *with* $[K:k] = 2$*, if* $\mathcal{K}^-$ *is the maximal* k*-negative* $\mathbf{Z}_p$*-power extension of* K*,*

(i) $\mathcal{S}_p(E,\mathcal{K}^-)$ *is not a torsion* $\mathbf{Z}_p[[\Gamma^-]]$*-module,*
(ii) *for every finite extension* F *of* K *in* $\mathcal{K}^-$*,* $E(F)$ *has a submodule isomorphic to* $\mathbf{Z}[\mathrm{Gal}(F/K)]$*, and in particular* $\mathrm{rank}_{\mathbf{Z}}(E(F)) \geq [F:K]$*.*

Corollary 3.7. *Suppose that the Torsion conjecture holds, and that*

(a) E *is defined over* $\mathbf{Q}$ *and* K *is a Galois extension of* $\mathbf{Q}$ *whose discriminant is relatively prime to the conductor* N_E *of* E*,*
(b) $\Delta := \mathrm{Gal}(K/\mathbf{Q})$ *has a unique quotient of order* 2*, and every irreducible* $\mathbf{Q}_p$*-representation of* Δ *not factoring through that quotient has even dimension,*
(c) *the Dirichlet character* χ *corresponding to the (unique) quadratic field contained in* K *satisfies* $\chi(-N_E) = -1$*.*

Then for every subfield k *of* K *with* $[K:k] = 2$*, if* $\mathcal{K}^-$ *is the maximal* k*-negative* $\mathbf{Z}_p$*-power extension of* K*,*

(i) $\mathcal{S}_p(E, \mathcal{K}^-)$ *is not a torsion* $\mathbf{Z}_p[[\Gamma^-]]$*-module,*
(ii) *for every finite extension* F *of* K *in* $\mathcal{K}^-$*,* $\mathcal{S}_p(E, F)$ *has a submodule isomorphic to* $\mathbf{Z}_p[\mathrm{Gal}(F/K)]$*, and in particular* $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, F)) \geq [F : K]$.

4. Aside on root numbers

Although we will not need it, the following proposition on root numbers explains why Theorem 3.1 and Corollary 3.6 are consistent with standard conjectures.

Proposition 4.1. (i) *Suppose that the hypotheses of Theorem 3.1 are satisfied. Then for every character* $\psi \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\mathcal{K}^-/K), \mathbf{C}^\times)$*, the induced representation* $\mathrm{Ind}_k^K \psi$ *is real valued and the root number of the L-function* $L(E/K, \psi, s)$ *is independent of* ψ.
(ii) *Suppose that the hypotheses of Corollary 3.6(a)-(c) are satisfied. Then for every character* $\psi \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\mathcal{K}^-/K), \mathbf{C}^\times)$*, the induced representation* $\mathrm{Ind}_{\mathbf{Q}}^K \psi$ *is real valued and the root number of the L-function* $L(E/K, \psi, s)$ *is* -1.

Proposition 4.1 is essentially proved in [MR1] §2.2. We will recall the proof in §12.

Remark 4.2. If F is a finite Galois extension of K and ψ is a complex character of $\mathrm{Gal}(F/K)$, then a suitably general version of the Birch and Swinnerton-Dyer conjecture would predict that the multiplicity of ψ in the representation $E(F) \otimes \mathbf{C}$ is the order of vanishing of $L(E/K, \psi, s)$ at $s = 1$. When $\mathrm{Ind}_k^K \psi$ is real valued, there is a conjectured functional equation that implies that this order of vanishing is even if the root number is $+1$, and odd if the root number is -1. Thus (using Proposition 4.1) under the hypotheses of Theorem 3.1 and Corollary 3.6 one expects that for every finite extension F of K in $\mathcal{K}^-$ and every character ψ of $\mathrm{Gal}(F/K)$, ψ occurs in $E(F) \otimes \mathbf{C}$. Theorem 3.1 and Corollary 3.6 show that this expectation is correct, at least if we replace $E(F)$ by $\mathcal{S}_p(E, F)$ (or assume that $Ш(E, F)[p^\infty]$ is finite for all such F).

Remark 4.3. There is a partial converse to Proposition 4.1. Namely, suppose that ψ is a character of finite order of $\Gamma := \mathrm{Gal}(\mathcal{K}/K)$. Suppose further that ψ is generic, in the sense that ψ is not the restriction to K of a character of a $\mathbf{Z}_p$-extension of a proper subfield of K. Then the induced representation $\mathrm{Ind}_{\mathbf{Q}}^K \psi$ is real-valued if and only if there is an involution σ of K such that $\psi^\sigma = \psi^{-1}$ (see Proposition 2.5 of [MR1]).

Now suppose in addition that E is defined over $\mathbf{Q}$, the discriminant of K is relatively prime to the conductor E, and K is Galois over $\mathbf{Q}$. Then the root number of $L(\mathrm{Ind}_{\mathbf{Q}}^K \psi, s)$ is -1 if and only if hypotheses (b) and (c) of Corollary 3.6 are satisfied (this is Theorem 2.8 and Proposition 2.9 of [MR1]).

When K is not Galois over $\mathbf{Q}$ the situation is more complicated. We plan to discuss this, and the further implication for p-Selmer growth related to odd parity functional equations, in a future paper.

5. Examples

Example 5.1. Let K be an abelian extension of $\mathbf{Q}$ containing a unique quadratic field (i.e., $\Delta := \mathrm{Gal}(K/\mathbf{Q})$ is an abelian group with cyclic 2-part). Then Δ satisfies the hypothesis of Corollary 3.6(b). Let σ be the unique element of order 2 in Δ,

and k the fixed field of σ. We will assume that K is imaginary, for if K is real then the cyclotomic $\mathbf{Z}_p$-extension is the only $\mathbf{Z}_p$-extension of K. Thus σ is complex conjugation and k is the real subfield of K. Let χ be the quadratic character of Δ.

Since Leopoldt's conjecture holds for K, we have $\mathcal{K}^+ = K\mathbf{Q}_\infty$, so $d_+ = 1$, and $\mathcal{K}^-/K$ is a $\mathbf{Z}_p^{d_-}$-extension with $d_- = r_2(K) = [K : \mathbf{Q}]/2$.

Let E be an elliptic curve over $\mathbf{Q}$ with good ordinary reduction at p, satisfying (2.2) and (2.3), with conductor N_E prime to the discriminant of K, and such that $\chi(-N_E) = -1$. By work of Kato [K], the Torsion conjecture holds for E/K.

By Corollary 3.6, if the p-primary Shafarevich-Tate conjecture holds, then the Selmer module $\mathcal{S}_p(E, \mathcal{K}^-)$ is a non-torsion $\mathbf{Z}_p[[\Gamma^-]]$-module and $\mathrm{rank}_{\mathbf{Z}}(E(F)) \geq [F : K]$ for all finite extensions F of K in $\mathcal{K}^-$.

If K is an imaginary quadratic field, then $\mathcal{K}^-$ is the anticyclotomic $\mathbf{Z}_p$-extension of K and the conclusions of Corollary 3.6 were already known by work of Vatsal [V] and Cornut [C].

If p has even order in $(\mathbf{Z}/\ell\mathbf{Z})^\times$ for every odd prime ℓ dividing $[K : \mathbf{Q}]$, and either $p \equiv 3 \pmod 4$ or 4 does not divide $[K : \mathbf{Q}]$, then we can apply Corollary 3.7 instead of Corollary 3.6 and hence remove the assumption that the p-primary Shafarevich-Tate conjecture holds.

Example 5.2. Suppose K is a complex Galois extension of $\mathbf{Q}$ with

$$\Delta := \mathrm{Gal}(K/\mathbf{Q}) \cong S_3.$$

Note that Δ satisfies the hypothesis of Corollary 3.7(b). Let M denote the (imaginary) quadratic extension of $\mathbf{Q}$ in K, and χ the Dirichlet character corresponding to $M/\mathbf{Q}$. Leopoldt's conjecture holds for K (for group-theoretic reasons), so $\Gamma := \mathrm{Gal}(\mathcal{K}/K) \cong \mathbf{Z}_p^4$.

Let $\sigma \in \Delta$ be one of the elements of order 2 and k_σ its fixed field. The (non-Galois) cubic field k_σ has one pair of complex embeddings, so $d_- = r_2(K) - r_2(k_\sigma) = 2$. Hence for each such σ there is a (unique) $\mathbf{Z}_p^2$-extension $\mathcal{K}_\sigma^-$ of K, each containing the anticyclotomic $\mathbf{Z}_p$-extension of M.

Let E be an elliptic curve over $\mathbf{Q}$ with good ordinary reduction at p, satisfying (2.2) and (2.3), with conductor N_E prime to the discriminant of K, and such that $\chi(-N_E) = -1$. Suppose further that the Torsion conjecture holds for E/K (which in practice would be very difficult to verify).

We conclude by Corollary 3.7 that for each of the three elements $\sigma \in \Delta$ of order 2, the Selmer module $\mathcal{S}_p(E, \mathcal{K}_\sigma^-)$ is not $\mathbf{Z}_p[[\mathrm{Gal}(\mathcal{K}_\sigma^-/K)]]$-torsion, and for every finite extension F of K in $\mathcal{K}_\sigma^-$ we have $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, F)) \geq [F : K]$. (Note that the three $\mathbf{Z}_p^2$-extensions $\mathcal{K}_\sigma^-$ are isomorphic over K, and hence the three Selmer modules $\mathcal{S}_p(E, \mathcal{K}_\sigma^-)$ are isomorphic as well.)

Example 5.3. Suppose K' is a complex Galois extension of $\mathbf{Q}$ with

$$\Delta := \mathrm{Gal}(K'/\mathbf{Q}) \cong S_4.$$

Note that Δ does *not* satisfy Corollary 3.6(b). Let H be a subgroup of order 2 in Δ, generated by a 2-cycle (so $H \not\subset A_4$) and let K be the fixed field of H in K'. Let $\sigma \in \Delta - H$ be an element in the normalizer of H, so σ is an automorphism of K of order 2, and let k be the fixed field of σ. One can check that K has 5 pairs of complex embeddings if the complex conjugations in Δ are 2-cycles, and 6 otherwise; k has 2 pairs of complex embeddings in either case.

Assume that Leopoldt's conjecture holds for K. The discussion above shows that $\Gamma := \mathrm{Gal}(\mathcal{K}/K) \cong \mathbf{Z}_p^n$ where n is 6 or 7, and $\Gamma^- := \mathrm{Gal}(\mathcal{K}^-/K)$ has $\mathbf{Z}_p$-rank 3 or 4.

Let E be an elliptic curve over $\mathbf{Q}$, with good ordinary reduction at p, satisfying (2.2) and (2.3), with conductor N_E prime to the discriminant of K, and suppose that the Torsion conjecture holds as well. It follows from Theorem 2.8 of [MR1] (or see the proof of Proposition 4.1) that the root number of $L(E/K, s)$ is $\chi(-N_E)$, where χ is the quadratic Dirichlet character corresponding to the fixed field of A_4 in K.

Assume now that $\chi(-N_E) = -1$. Then conjecturally $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, K))$ is odd, and if so we can use Theorem 3.1 to conclude that the Selmer module $\mathcal{S}_p(E, \mathcal{K}^-)$ is not $\mathbf{Z}_p[[\Gamma^-]]$-torsion, and that for every finite extension F of K in $\mathcal{K}^-$ we have $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, F)) \geq [F : K]$.

Unfortunately, unlike the situation of Corollary 3.6, we have no general way to show that $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, K))$ is odd. We do know (using Nekovář's parity theorem [N1]) that $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, M))$ is odd, where M is the (quadratic) fixed field of A_4 in K, but $M \not\subset K$ so there is no apparent way to relate the parity of $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, K))$ to that of $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, M))$.

6. The control theorem

Define the Iwasawa algebra

$$\Lambda := \mathbf{Z}_p[[\Gamma]].$$

If $K \subset F \subset \mathcal{K}$ we let $\Gamma_F := \mathrm{Gal}(F/K)$ and $\Lambda_F := \mathbf{Z}_p[[\Gamma_F]]$ denote the corresponding quotients of Γ and Λ, and $I_F \subset \Lambda$ the corresponding augmentation ideal:

$$0 \longrightarrow I_F \longrightarrow \Lambda \longrightarrow \Lambda_F \longrightarrow 0.$$

Thus I_F is generated by $\{\gamma - 1 : \gamma \in \mathrm{Gal}(\mathcal{K}/F)\}$.

Suppose that either

(i) F is a $\mathbf{Z}_p^d$-extension of K in $\mathcal{K}$ and $R = \Lambda_F$, or
(ii) F is an arbitrary extension of K in $\mathcal{K}$ and $R = \Lambda_F \otimes \mathbf{Q}_p$.

In case (i) R is an integrally closed noetherian domain, and in case (ii) R is a direct sum of integrally closed noetherian domains. If M is a finitely generated torsion R-module we let $\mathrm{char}_R(M)$ denote the characteristic ideal of M, called the divisor of M in [B] Chapter VII, §4.5. (In case (ii) we make this definition component-by-component.) If (some component of) M is not torsion, we set (that component of) $\mathrm{char}_R(M)$ equal to zero. Then M has a submodule isomorphic to R if and only if $\mathrm{char}_R(M) = 0$.

The following "control theorem" is due to Greenberg ([G2] Theorem 2).

Theorem 6.1. *Suppose that $K \subset F \subset L \subset \mathcal{K}$, and F/K is finite. Then the natural map*

$$\mathcal{S}_p(E, L) \otimes_{\Lambda_L} \Lambda_F \longrightarrow \mathcal{S}_p(E, F)$$

(induced by the restriction map $\mathrm{Sel}_p(E, F) \to \mathrm{Sel}_p(E, L)^{\mathrm{Gal}(L/F)}$) has finite kernel and cokernel. In particular

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, F)) = \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, \mathcal{K}) \otimes_\Lambda \Lambda_F).$$

Corollary 6.2. *The Λ-module $\mathcal{S}_p(E, \mathcal{K})$ is finitely generated.*

Proof. This is immediate from Theorem 6.1 and Nakayama's Lemma. □

Lemma 6.3. *Suppose that $K \subset F \subset L \subset \mathcal{K}$, and M is a finitely generated Λ_L-module. Let $M_F = M \otimes_{\Lambda_L} \Lambda_F$. Then*

(i) *M_F is a finitely generated Λ_F-module,*
(ii) $\mathrm{char}_{\Lambda_F \otimes \mathbf{Q}_p}(M_F \otimes \mathbf{Q}_p) \subset \mathrm{char}_{\Lambda_L}(M)(\Lambda_F \otimes \mathbf{Q}_p)$,

Proof. The first assertion is clear.

For (ii), since $\mathrm{char}_{\Lambda_L \otimes \mathbf{Q}_p}(M \otimes \mathbf{Q}_p) = \mathrm{char}_{\Lambda_L}(M) \otimes \mathbf{Q}_p$, we can reduce by induction to the case that L/F is either finite or a $\mathbf{Z}_p$-extension. If $[L : F]$ is finite then $\Lambda_F \otimes \mathbf{Q}_p$ is a direct summand of $\Lambda_L \otimes \mathbf{Q}_p$ and we have equality in (ii). If L/F is a $\mathbf{Z}_p$-extension then (ii) follows from Lemmas 2 and 4 of §I.1 of [PR1]. □

Lemma 6.4. *Suppose that $K \subset F \subset L \subset \mathcal{K}$, L/K is a $\mathbf{Z}_p$-power extension, and M is a finitely generated Λ_L-module. If $\mathrm{char}_{\Lambda_L}(M) \subset I_F\Lambda_L$ then $M \otimes_{\Lambda_L} \Lambda_F$ has a submodule isomorphic to Λ_F.*

Proof. Let $M_F = M \otimes_{\Lambda_L} \Lambda_F$. If $\mathrm{char}_{\Lambda_L}(M) \subset I_F\Lambda_L$ then by Lemma 6.3(ii), $\mathrm{char}_{\Lambda_F \otimes \mathbf{Q}_p}(M_F \otimes \mathbf{Q}_p) = 0$. Hence $M_F \otimes \mathbf{Q}_p$ has a submodule isomorphic to $\Lambda_F \otimes \mathbf{Q}_p$, and the lemma follows. □

Proposition 6.5. *Suppose that $K \subset F \subset L \subset \mathcal{K}$, L/K is a $\mathbf{Z}_p$-power extension, and $\mathrm{char}_{\Lambda_L}(\mathcal{S}_p(E, L)) \subset I_F\Lambda_L$.*

(i) *If F/K is finite then $\mathcal{S}_p(E, F)$ has a submodule isomorphic to Λ_F.*
(ii) *If F/K is a $\mathbf{Z}_p$-power extension, then $\mathcal{S}_p(E, F)$ is not a torsion Λ_F-module.*

Proof. Suppose first that F/K is finite. By Lemma 6.4 applied with $M = \mathcal{S}_p(E, L)$, the Λ_F-module $\mathcal{S}_p(E, L) \otimes_{\Lambda_L} \Lambda_F$ has a submodule isomorphic to Λ_F. Now (i) follows from Theorem 6.1.

Now suppose F is a $\mathbf{Z}_p$-power extension of K and $\mathrm{char}_\Lambda(\mathcal{S}_p(E, L)) \subset I_F\Lambda_L$. If F' is a finite extension of K in F, then $I_F \subset I_{F'}$ so assertion (i) shows that $\mathcal{S}_p(E, F')$ has a submodule isomorphic to $\Lambda_{F'}$. Thus by Theorem 6.1, $\mathcal{S}_p(E, F) \otimes \Lambda_{F'}$ has a submodule isomorphic to $\Lambda_{F'}$. Since this holds for every finite extension F' of K in F, it follows that $\mathcal{S}_p(E, F)$ cannot be a torsion Λ_F-module. □

Corollary 6.6. *If the Torsion conjecture holds, then $\mathcal{S}_p(E, \mathcal{K})$ is a torsion Λ-module and $\mathcal{S}_p(E, \mathcal{K}^+)$ is a torsion $\Lambda_{\mathcal{K}^+}$-module.*

Proof. If $\mathcal{S}_p(E, \mathcal{K})$ is not a torsion Λ-module, then $\mathrm{char}_\Lambda(\mathcal{S}_p(E, \mathcal{K})) = 0$, and so Proposition 6.5(ii) (with $L = \mathcal{K}$ and $F = K\mathbf{Q}_\infty$) would contradict the Torsion conjecture.

The proof for $\mathcal{K}^+$ is the same. □

7. Involutions and functional equations

Suppose that τ is a $\mathbf{Z}_p$-linear involution of Γ. Then τ induces an involution of Λ (which we will also denote simply by τ, or by $\lambda \mapsto \lambda^\tau$). If M is a Λ-module we let M^τ be the Λ-module with the same underlying abelian group as M, but with Λ-module structure obtained from that of M by composition with τ.

For example, an automorphism σ of order 2 of K with fixed field k as in §2 gives an involution of Γ (which we will also denote simply by σ), and we always have the involutions ± 1.

Lemma 7.1. *Suppose that T is a (commutative) group of involutions of Γ. Then the natural inclusion $\{\pm 1\} \hookrightarrow \Lambda^\times$ induces an isomorphism*

$$\mathrm{Hom}(T, \{\pm 1\}) \xrightarrow{\sim} H^1(T, \Lambda^\times).$$

Proof. We have a direct sum decomposition $\Lambda^\times \cong \mathbf{F}_p^\times \oplus \Lambda'$ where Λ' is the kernel of the reduction map $\Lambda^\times \to \mathbf{F}_p^\times$. Since Λ' is a pro-p group and $p > 2$, $H^1(T, \Lambda') = 0$ and so

$$H^1(T, \Lambda^\times) = H^1(T, \mathbf{F}_p^\times) = \mathrm{Hom}(T, \mathbf{F}_p^\times) = \mathrm{Hom}(T, \{\pm 1\}). \qquad \square$$

Proposition 7.2. *Suppose that T is a (commutative) group of involutions of Γ, and $\mathcal{A} \subset \Lambda$ is a principal ideal that is stable under every involution in T. Then there is a homomorphism $\epsilon : T \to \{\pm 1\}$ and a generator $\mathcal{L}$ of $\mathcal{A}$ such that*

$$\mathcal{L}^\tau = \epsilon(\tau)\mathcal{L} \quad \text{for every } \tau \in T.$$

Further, for each $\tau \in T$, $\epsilon(\tau)$ is uniquely determined by τ and $\mathcal{A}$, and does not depend on T or $\mathcal{L}$.

Proof. Let α be a generator of $\mathcal{A}$. Since $\mathcal{A}$ is stable under involutions in T, the map $c(\tau) = \alpha^\tau/\alpha$ is a 1-cocycle from T to $\Lambda^\times$. By Lemma 7.1 there is a homomorphism $\epsilon : T \to \{\pm 1\}$ that is equivalent in $H^1(T, \Lambda^\times)$ to c. In other words, there is a $u \in \Lambda^\times$ such that $(u^\tau/u)c(\tau) = \epsilon(\tau)$ for every $\tau \in T$. Put $\mathcal{L} = u\alpha$. Then $\mathcal{L}$ is a generator of $\mathcal{A}$ and $\mathcal{L}^\tau = \epsilon(\tau)\mathcal{L}$ for every $\tau \in T$.

Now fix τ, and suppose that there is another generator $\mathcal{L}_0$ of $\mathcal{A}$ such that $\mathcal{L}_0^\tau = w\mathcal{L}_0$ with $w = \pm 1$. Then if $v = \mathcal{L}_0/\mathcal{L}$ we have $v \in \Lambda^\times$ and $v^\tau/v = w\epsilon(\tau)$. But τ induces the identity map on $\Lambda_K \cong \mathbf{Z}_p$, and the image of v in Λ_K is nonzero, so we cannot have $v^\tau = -v$. Hence $\epsilon(\tau) = w$ is uniquely determined by $\mathcal{A}$ and τ. $\square$

If τ is an involution of Γ, we let $\Gamma_\tau^\pm$ be the submodule of Γ on which τ acts via ± 1, and $\mathcal{K}_\tau^\pm$ the fixed field of $\Gamma_\tau^\mp$. (If τ is the nontrivial automorphism of a quadratic extension K/k, then $\mathcal{K}_\tau^\pm$ is what we previously called simply $\mathcal{K}^\pm$.)

Proposition 7.3. *Suppose that τ is an involution of Γ, and $\mathcal{L} \in \Lambda$ satisfies $\mathcal{L}^\tau = -\mathcal{L}$. Then $\mathcal{L}$ lies in the augmentation ideal $I_{\mathcal{K}_\tau^+}$.*

Proof. In the exact sequence

$$0 \longrightarrow I_{\mathcal{K}_\tau^+} \longrightarrow \Lambda \longrightarrow \Lambda_{\mathcal{K}_\tau^+} \longrightarrow 0,$$

$I_{\mathcal{K}_\tau^+}$ is stable under τ, and τ induces the identity map on $\Lambda_{\mathcal{K}_\tau^+}$. Since $\mathcal{L}^\tau = -\mathcal{L}$, the image of $\mathcal{L}$ in $\Lambda_{\mathcal{K}_\tau^+}$ must be zero, and the proposition follows. $\square$

8. The inversion involution

Let ι be the inversion involution on Γ, i.e., $\iota(\gamma) = \gamma^{-1}$. Under our hypotheses (2.1)-(2.3) we have the following result from [MR2] (Theorem 7.5).

Theorem 8.1. *Suppose that $\mathcal{S}_p(E, \mathcal{K})$ is a torsion Λ-module. Then there is a free Λ-module Φ of finite rank with a nondegenerate skew-Hermitian pairing*

$$\Phi \otimes \Phi^\iota \longrightarrow \Lambda$$

such that $\mathcal{S}_p(E, \mathcal{K})$ is the cokernel of the induced injection

$$\Phi \hookrightarrow \mathrm{Hom}(\Phi^\iota, \Lambda).$$

Here a skew-Hermitian pairing means a Λ-homomorphism $h : \Phi \otimes \Phi^\iota \to \Lambda$ such that $h(a \otimes b) = -h(b \otimes a)^\iota$.

Proposition 8.2. *With Φ as in Theorem 8.1, we have*

$$\mathrm{rank}_\Lambda(\Phi) \equiv \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, K)) \pmod 2.$$

Proof. Let $I := I_K$ denote the augmentation ideal of Λ, so $\Lambda/I = \Lambda_K \cong \mathbf{Z}_p$. Theorem 8.1 gives an exact sequence

$$0 \longrightarrow \Phi \longrightarrow \mathrm{Hom}(\Phi^\iota, \Lambda) \longrightarrow \mathcal{S}_p(E, \mathcal{K}) \longrightarrow 0,$$

and tensoring with Λ/I gives

$$\Phi/I\Phi \xrightarrow{\bar{h}} \mathrm{Hom}(\Phi^\iota/I\Phi^\iota, \mathbf{Z}_p) \longrightarrow \mathcal{S}_p(E, \mathcal{K}) \otimes_\Lambda \mathbf{Z}_p \longrightarrow 0.$$

Since ι acts trivially on Λ/I, the map $\bar{h}$ is represented by a skew symmetric matrix with entries in $\mathbf{Z}_p$. Such a matrix has even rank (that is, the nondegeneracy rank of the matrix, which is the $\mathbf{Z}_p$-rank of the image), and it follows that

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, \mathcal{K}) \otimes_\Lambda \mathbf{Z}_p) \equiv \mathrm{rank}_{\mathbf{Z}_p}(\Phi/I\Phi) = \mathrm{rank}_\Lambda(\Phi) \pmod 2.$$

On the other hand, Theorem 6.1 shows that

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, K)) = \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, \mathcal{K}) \otimes_\Lambda \mathbf{Z}_p),$$

and the proposition follows. □

Corollary 8.3. *Suppose that $\mathcal{S}_p(E, \mathcal{K})$ is a torsion Λ-module. Let H be the matrix giving the skew-Hermitian pairing of Theorem 8.1 with respect to some Λ-basis of Φ, and $\mathcal{L} := \det(H) \in \Lambda$. Then $\mathcal{L}$ is a generator of $\mathrm{char}(\mathcal{S}_p(E, \mathcal{K}))$ and $\mathcal{L}^\iota = (-1)^r \mathcal{L}$, where $r := \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, K))$.*

Proof. By Theorem 8.1, $\det(H)$ is a generator of $\mathrm{char}(\mathcal{S}_p(E, \mathcal{K}))$. On the other hand, H is a skew-Hermitian matrix (i.e., the transpose of H is $-H^\iota$) so

$$\det(H)^\iota = \det(H^\iota) = \det(-H) = (-1)^{\mathrm{rank}_\Lambda(\Phi)} \det(H) = (-1)^r \det(H)$$

the final equality by Proposition 8.2. □

9. The involution σ

Let σ be the nontrivial automorphism of K/k as in §2, and let σ also denote the corresponding involutions of Γ and Λ.

Lemma 9.1. *Every lifting of σ to $\mathrm{Gal}(\mathcal{K}/k)$ induces an isomorphism $\mathcal{S}_p(E,\mathcal{K})^\sigma \cong \mathcal{S}_p(E,\mathcal{K})$.*

Proof. This is clear. □

Corollary 9.2. *Suppose that $\mathcal{S}_p(E,\mathcal{K})$ is a torsion Λ-module. Then there is a generator $\mathcal{L}$ of $\mathrm{char}(\mathcal{S}_p(E,\mathcal{K}))$ such that*

$$\mathcal{L}^\iota = (-1)^r\mathcal{L}, \quad \mathcal{L}^\sigma = \pm\mathcal{L}$$

where $r := \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$.

Proof. Let T be the group generated by the (commuting) involutions ι and σ of Γ. By Corollary 8.3 and Lemma 9.1, the ideal $\mathrm{char}(\mathcal{S}_p(E,\mathcal{K}))$ is stable under every element of T. Now the corollary follows from Proposition 7.2 and Corollary 8.3. □

10. Proof of Theorem 3.1

Proof of Theorem 3.1. If $\mathcal{S}_p(E,\mathcal{K})$ is not a torsion Λ-module, then Theorem 3.1 holds with both $\epsilon =$ "+" and "−" by Proposition 6.5 (with $L = \mathcal{K}$ and $F \subset \mathcal{K}^+$ or $F \subset \mathcal{K}^-$). So we may assume that $\mathcal{S}_p(E,\mathcal{K})$ is a torsion Λ-module.

Let $\mathcal{L}$ be a generator of $\mathrm{char}_\Lambda(\mathcal{S}_p(E,\mathcal{K}))$ satisfying Corollary 9.2. We consider two cases.

Case 1: $\mathcal{L}^\sigma = -\mathcal{L}$. By Proposition 7.3 we have $\mathcal{L} \in I_{\mathcal{K}^+}$, so by Proposition 6.5 (with $L = \mathcal{K}$ and $F \subset \mathcal{K}^+$) Theorem 3.1 holds with $\epsilon =$ "+".

Case 2: $\mathcal{L}^\sigma = \mathcal{L}$. In this case we use the involution $\iota\sigma$ instead of σ. Note that $\Gamma^\pm_{\iota\sigma} = \Gamma^\mp$ and $\mathcal{K}^\pm_{\iota\sigma} = \mathcal{K}^\mp$. Since we assume that $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ is odd, we have $\mathcal{L}^{\iota\sigma} = -\mathcal{L}$ by Corollary 9.2. Proposition 7.3 now shows that $\mathcal{L} \in I_{\mathcal{K}^+_{\iota\sigma}} = I_{\mathcal{K}^-}$, so by Proposition 6.5 (with $L = \mathcal{K}$ and $F \subset \mathcal{K}^-$) Theorem 3.1 holds with $\epsilon =$ "−". □

11. Proof of Corollaries 3.6 and 3.7

Corollaries 3.6 and 3.7 will follow immediately from Corollary 3.5 once we show that (under the hypotheses of Corollary 3.6 or 3.7) $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ is odd. We will deduce this from Nekovář's parity theorem [N1] for Selmer groups over $\mathbf{Q}$.

Lemma 11.1. *Suppose G is a finite group of odd order. If V is a nontrivial irreducible representation of $\mathbf{R}[G]$, then $\dim_{\mathbf{R}}(V)$ is even.*

Proof. We will prove this by induction on the order of G. If G is cyclic, then the lemma is clear. If not, then by the Feit-Thompson theorem G has a proper normal subgroup H. If H acts trivially on V then we are done by induction (applied to G/H), so we may assume that H acts nontrivially on V.

Decompose $V = \oplus_i V_i$ where each V_i is an irreducible representation of $\mathbf{R}[H]$. If some V_j is the trivial representation then (since H is normal) H acts trivially on the G-span of V_j. But the G-span of V_j is nonzero and G-stable, hence equal to V. This contradicts our assumption that H acts nontrivially on V.

Thus by induction each $\dim_{\mathbf{R}}(V_i)$ is even, and so $\dim_{\mathbf{R}}(V)$ is even. □

Lemma 11.2. *Suppose Δ satisfies Corollary 3.6(b). If ρ is an irreducible representation of $\mathbf{R}[\Delta]$, not equal to either the trivial representation or the unique quadratic one-dimensional character, then* $\dim(\rho)$ *is even.*

Proof. Let H denote the (normal) odd-order subgroup of Δ with cyclic 2-power quotient. If ρ is trivial on H then the proposition is clear.

Decompose $\rho|_H = \oplus_i \rho_i$ into irreducible representations of $\mathbf{R}[H]$. Arguing exactly as in the proof of Lemma 11.1 we conclude that each ρ_i is nontrivial, and then by Lemma 11.1 each $\dim(\rho_i)$ is even. □

Proposition 11.3. (i) *If K satisfies Corollary 3.6(b), and M is the quadratic field contained in K, then* $\mathrm{rank}_{\mathbf{Z}}(E(K)) \equiv \mathrm{rank}_{\mathbf{Z}}(E(M)) \pmod 2$.

(ii) *If K satisfies Corollary 3.7(b), and M is the quadratic field contained in K, then* $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K)) \equiv \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,M)) \pmod 2$.

Proof. Let $V := (E(K)\otimes\mathbf{R})/(E(M)\otimes\mathbf{R})$. Then

$$\mathrm{rank}_{\mathbf{Z}}(E(K)) - \mathrm{rank}_{\mathbf{Z}}(E(M)) = \dim_{\mathbf{R}}(V).$$

The $\mathbf{R}[\Delta]$-module V contains no copies of either of the two one-dimensional real representations of Δ, so in case (i) Lemma 11.2 shows that $\dim_{\mathbf{R}}(V)$ is even.

Similarly in case (ii), the hypothesis of Corollary 3.7(b) shows that the $\mathbf{Q}_p$-dimension of $(\mathcal{S}_p(E,K)\otimes\mathbf{Q}_p)/(\mathcal{S}_p(E,M)\otimes\mathbf{Q}_p)$ is even. □

Theorem 11.4. *Suppose that either*

(i) *the hypotheses of Corollary 3.6(a)-(c) are satisfied and* $Ш(E,K)[p^\infty]$ *is finite, or*

(ii) *the hypotheses of Corollary 3.7(a)-(c) are satisfied.*

Then $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ *is odd.*

Proof. Let M denote the quadratic extension of $\mathbf{Q}$ inside K, and let E' denote the quadratic twist of E by M. Then $L(E/M,s) = L(E/\mathbf{Q},s)L(E'/\mathbf{Q},s)$ and $\mathcal{S}_p(E,M) \cong \mathcal{S}_p(E,\mathbf{Q}) \oplus \mathcal{S}_p(E',\mathbf{Q})$. Nekovář [N1] proved that $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,\mathbf{Q})) \equiv \mathrm{ord}_{s=1}L(E/\mathbf{Q},s) \pmod 2$ and similarly for E'. We deduce that

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,M)) \equiv \mathrm{ord}_{s=1}L(E/M,s) \pmod 2.$$

By (for example) Proposition 4.1(ii) applied with K replaced by M, the root number of $L(E/M,s)$ is -1, so $\mathrm{ord}_{s=1}L(E/M,s)$ is odd and we conclude that $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,M))$ is odd.

In case (ii), it follows from Proposition 11.3(ii) that $\mathrm{rank}_{\mathbf{Z}_p}\mathcal{S}_p(E,K)$ is odd. In case (i), since $Ш(E,K)[p^\infty]$ is finite we have that $Ш(E,M)[p^\infty]$ is finite as well, so $\mathrm{rank}_{\mathbf{Z}}(E(M)) = \mathrm{rank}_{\mathbf{Z}_p}\mathcal{S}_p(E,M)$ and $\mathrm{rank}_{\mathbf{Z}}(E(K)) = \mathrm{rank}_{\mathbf{Z}_p}\mathcal{S}_p(E,K)$. Then $\mathrm{rank}_{\mathbf{Z}}(E(M))$ is odd, so by Proposition 11.3(i) $\mathrm{rank}_{\mathbf{Z}}(E(K))$ is odd, and finally $\mathrm{rank}_{\mathbf{Z}_p}\mathcal{S}_p(E,K)$ is odd. □

Proof of Corollaries 3.6 and 3.7. Corollaries 3.6 and 3.7 follow immediately from Corollary 3.5, using Theorem 11.4. □

12. Proof of Proposition 4.1

Proposition 4.1 is essentially proved in [MR1] §2.2. For completeness we sketch the proof here.

Proof of Proposition 4.1. Suppose $\psi \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\mathcal{K}^-/K), \mathbf{C}^\times)$. Since σ acts as -1 on $\mathrm{Gal}(\mathcal{K}^-/K)$, we have $\psi^\sigma = \psi^{-1} = \bar{\psi}$. Therefore $\mathrm{Ind}_k^K \psi = \mathrm{Ind}_k^K \bar{\psi}$ so $\mathrm{Ind}_k^K \psi$ is real valued in part (i), and similarly for $\mathrm{Ind}_{\mathbf{Q}}^K \psi$ in part (ii).

In Proposition 10 of [Ro], Rohrlich gives a formula for the root number of $L(E/K, \psi, s) = L(E/k, \mathrm{Ind}_k^K \psi, s)$ that depends only on E and $\det(\mathrm{Ind}_k^K \psi)$, and does not otherwise depend on ψ. To complete the proof of (i) we need only show that $\det(\mathrm{Ind}_k^K \psi)$ does not depend on ψ.

Let $\mathfrak{p}$ be a prime of $\bar{\mathbf{Q}}$ above p. Since ψ has p-power order, $\psi \equiv \mathbf{1} \pmod{\mathfrak{p}}$ where $\mathbf{1}$ is the trivial character, and so

$$\det(\mathrm{Ind}_k^K \psi) \equiv \det(\mathrm{Ind}_k^K \mathbf{1}) \pmod{\mathfrak{p}}.$$

Since p is odd and both sides of this congruence are characters taking only the values ± 1, it follows that the congruence must be an equality. This proves (i).

For (ii), we use Rohrlich's Proposition 10 [Ro] again to conclude that the root number of $L(E/K, \psi, s) = L(E/\mathbf{Q}, \mathrm{Ind}_{\mathbf{Q}}^K \psi, s)$ is $\chi(-N_E)$ where $\chi = \det(\mathrm{Ind}_{\mathbf{Q}}^K \psi)$. Exactly as above we see that $\det(\mathrm{Ind}_{\mathbf{Q}}^K \psi) = \det(\mathrm{Ind}_{\mathbf{Q}}^K \mathbf{1})$, and by Proposition 2.9 of [MR1], the condition of Corollary 3.6(b) ensures that $\det(\mathrm{Ind}_{\mathbf{Q}}^K \mathbf{1})$ is the unique quadratic character of $\mathrm{Gal}(K/\mathbf{Q})$. Now the condition of Corollary 3.6(c) completes the proof of (ii). □

References

[B] N. Bourbaki, Éléments de mathmatique. Fasc. XXXI. Algèbre commutative. Chapitre 7: Diviseurs. *Actualités Scientifiques et Industrielles* **1314** Paris: Hermann (1965).

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

[CV] C. Cornut and V. Vatsal, CM points and quaternion algebras, preprint (2004).

[G1] R. Greenberg, On the Birch and Swinnerton-Dyer conjecture. *Invent. Math.* **72** (1983) 241–265.

[G2] ———, Galois theory for the Selmer group of an abelian variety. *Compositio Math.* **136** (2003) 255–297.

[K] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms. To appear.

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

[MR1] B. Mazur, K. Rubin, Studying the growth of Mordell-Weil. *Documenta Math.* extra volume (2003) 585–607.

[MR2] ———, Organizing the arithmetic of elliptic curves. To appear.

[N1] J. Nekovář, On the parity of ranks of Selmer groups. II, *C. R. Acad. Sci. Paris Sér. I Math.* **332** (2001) 99–104.

[N2] ———, Selmer complexes. Preprint available at `http://www.math.jussieu.fr/~nekovar/pu/`.

[PR1] B. Perrin-Riou, Arithmétique des courbes elliptiques et théorie d'Iwasawa. *Bull. Soc. Math. Suppl.*, Mémoire **17** (1984).

[PR2] ———, Groupes de Selmer et accouplements: cas particulier des courbes elliptiques. *Documenta Math.* extra volume (2003) 725–760.

[Ro] D. Rohrlich, Galois theory, elliptic curves, and root numbers, *Compositio Math.* **100** (1996) 311–349.

[SU] C. Skinner, E. Urban, Sur les déformations p-adiques de certaines représentations automorphes. To appear in *Journal de l'Institut de Mathématiques de Jussieu.*

[V] V. Vatsal, Uniform distribution of Heegner points, *Invent. Math.* **148** (2002) 1–46.

Department of Mathematics, Harvard University, Cambridge, MA 02138 USA
E-mail address: mazur@math.harvard.edu

Department of Mathematics, University of California Irvine, Irvine, CA 92697 USA
E-mail address: krubin@math.uci.edu