Studying the Growth of Mordell-Weil

To Kazuya Kato, with admiration

Barry Mazur and Karl Rubin

Received: December 1, 2002
Revised: February 16, 2003

Abstract. We study the growth of the Mordell-Weil groups $E(K_n)$ of an elliptic curve E as K_n runs through the intermediate fields of a $\mathbf{Z}_p$-extension. We describe those $\mathbf{Z}_p$-extensions K_∞/K where we expect the ranks to grow to infinity. In the cases where we know or expect the rank to grow, we discuss where we expect to find the submodule of universal norms.

2000 Mathematics Subject Classification: Primary 11G05, 11G40; Secondary 11R23, 14G05

1 Introduction

Fix an elliptic curve E over $\mathbf{Q}$ of conductor N, and an odd prime number p. Let K be a number field and K_∞/K a $\mathbf{Z}_p$-extension. For $n \geq 0$ denote by K_n/K the intermediate extension in K_∞/K of degree p^n. What is the rate of growth of the Mordell-Weil groups $E(K_n)$ as n tends to ∞? The shape of these asymptotics for general number fields K and prime numbers p of good ordinary reduction is given by the following result, conditional on the Shafarevich-Tate conjecture (more specifically, on the finiteness of p-primary components of Shafarevich-Tate groups).

Proposition 1.1. *If the Shafarevich-Tate conjecture is true, and E has good, ordinary reduction at p, then there is a non-negative integer $r = r(E, K_\infty/K)$ such that*

$$\mathrm{rank}_{\mathbf{Z}}(E(K_n)) = rp^n + O(1)$$

where the bound $O(1)$ depends on E and K_∞/K, but not on n.

We will review the proof of this proposition in §3 below, Proposition 3.2. For convenience, if the above asymptotics hold, we will say that $(E, K_\infty/K)$ has *growth number* $r = r(E, K_\infty/K)$. In particular, if E does not have complex multiplication by a subfield of K, then $(E, K_\infty/K)$ has growth number zero if and only if $E(K_\infty)$ is finitely generated. When $r(E, K_\infty/K) > 0$ let us say that the Mordell-Weil rank of E has *positive growth* relative to K_∞/K. Recent work has significantly increased our knowledge of questions related to growth number, and has allowed us to compute these growth numbers in two specific instances.

Example 1.2. When K is a real abelian field there is only one $\mathbf{Z}_p$-extension K_∞/K (the cyclotomic $\mathbf{Z}_p$-extension) and Kato's celebrated work (cf. [K, Sc, Ru]) shows that $E(K_n)$ stabilizes for large n. Therefore $E(K_\infty)$ is a finitely generated group and the growth number vanishes. This had been conjectured in [M1], at least for good, ordinary, primes p.

Example 1.3. Suppose $K/\mathbf{Q}$ is a quadratic imaginary field and let K_∞/K denote the anti-cyclotomic $\mathbf{Z}_p$-extension. This is the unique $\mathbf{Z}_p$-extension of K such that $K_\infty/\mathbf{Q}$ is Galois with nonabelian Galois group. It was conjectured in [M2] (for the case of primes p of good, ordinary, reduction for E; but see, e.g., [V] for arbitrary p) that the growth number $r(E, K_\infty/K)$ is at most 2. Moreover, the conjectures in [M2] assert that

- the growth number $r = 2$ can only occur in the "exceptional case" where E has complex multiplication by K,
- if we are not in this "exceptional case" then the distinction between growth number 0 and 1 is determined by the root number in the functional equation satisfied by the relevant L-functions.

A good deal of this conjecture, as well as other information about the p-anti-cyclotomic arithmetic of elliptic curves over $\mathbf{Q}$, is now established, thanks to work of Gross & Zagier, Kolyvagin, Perrin-Riou, Bertolini & Darmon, Vatsal, Cornut, Nekovář, and Zhang.

The object of this note is to indicate a slightly wider context where "signs of functional equations" would lead one to conjecture positive growth of Mordell-Weil ranks, and to formulate some open problems suggested by the recent work regarding anti-cyclotomic extensions of quadratic imaginary fields.
Specifically, we will do two things. Let E be an elliptic curve over $\mathbf{Q}$. For a number field K, call a $\mathbf{Z}_p$-extension K_∞/K *new* over K if it is not the base extension of a $\mathbf{Z}_p$-extension of a proper subfield of K.

(i) Assuming standard conjectures, we will consider *new* $\mathbf{Z}_p$-extensions K_∞/K of number fields K that have the property that (in a sense to be made precise) the root number in the functional equation predicts positive growth for E relative to K_∞/K. These $\mathbf{Z}_p$-extensions have a very tight structure. As we shall see, in such a situation K has an automorphism of order 2, and if $K^+ \subset K$ is the fixed field of this automorphism then K_∞/K^+ is an infinite dihedral extension. To be sure, the "classical case" where K is a quadratic imaginary field is of this form, but–again as we shall see–there are quite a number of other "nonclassical" instances (in general K need not even be a CM field). An open problem is to prove positive growth in all (or even just *one*) of these "nonclassical" instances.

(ii) When K is a quadratic imaginary field we shall discuss a certain intriguing p-adic "line" in the $\mathbf{Q}_p$-vector space $E(K)\otimes\mathbf{Q}_p$ that can be constructed, under certain hypotheses, via universal norms from the anti-cyclotomic $\mathbf{Z}_p$-extension of K. This line is stable under the action of complex conjugation and we offer a conjecture, and some beginning numerical evidence, about its "sign." In the "nonclassical" instances alluded to above, where at present we cannot prove positive growth, if the growth number is 1 we can define a similar "sign" (see Remark 4.12).

We only consider here the growth of Mordell-Weil groups in $\mathbf{Z}_p$-power extensions of number fields, i.e., infinite extensions F/K where $\mathrm{Gal}(F/K)$ is an abelian p-adic Lie group. There are recent studies (see for example [CH]) by Coates, Howson, and others concerning the growth of Mordell-Weil groups in infinite extensions F/K where $\mathrm{Gal}(F/K)$ is a *nonabelian* p-adic Lie group.
We conclude this introduction with an example in which Proposition 1.1, along with the rest of this paper, does not apply.

Example 1.4. Suppose E has complex multiplication by the quadratic imaginary field K, p is a prime of good, supersingular reduction, and K_∞/K is the anticyclotomic $\mathbf{Z}_p$-extension of K. Then standard conjectures imply (see the remark near the end of §1 of [G1])

$$\mathrm{rank}_{\mathbf{Z}}(E(K_n)) = \begin{cases} \frac{p^{2[n+1/2]}-1}{p+1} + O(1) & \text{if } W(E/\mathbf{Q}) = +1 \\[2ex] \frac{p^{2[n/2]+1}+1}{p+1} + O(1) & \text{if } W(E/\mathbf{Q}) = -1 \end{cases}$$

where $W(E/\mathbf{Q})$ is the root number in the functional equation of the L-function $L(E/\mathbf{Q}, s)$ (see §2.2) and [ ] is the greatest integer function.

2 Where can we find Mordell-Weil contribution in bulk?

Fix an odd prime p. Let E be an elliptic curve over $\mathbf{Q}$, $K/\mathbf{Q}$ a finite Galois extension of degree prime to p, and L the pro-p-abelian extension of K that is the compositum of all $\mathbf{Z}_p$-extensions of K in $\bar{\mathbf{Q}}$. Put $\Delta := \mathrm{Gal}(K/\mathbf{Q})$ and $\Gamma := \mathrm{Gal}(L/K) \cong \mathbf{Z}_p^d$, so we have $d \geq r_2(K) + 1$ with equality if Leopoldt's conjecture holds, where $r_2(K)$ is the number of complex archimedean places of K. The extension $L/\mathbf{Q}$ is Galois, and "conjugation" in $\mathcal{G} := \mathrm{Gal}(L/\mathbf{Q})$ induces a natural action of the group Δ on Γ. By the classical Schur-Zassenhaus

Theorem, $\mathcal{G}$ is noncanonically isomorphic to the semi-direct product of Δ and Γ, the semi-direct product being formed via this conjugation action.

Example 2.1 (Mordell-Weil growth when K is totally real). Assume that Leopoldt's conjecture holds. If K is (totally) real, it follows that $d = 1$ and the unique $\mathbf{Z}_p$-extension of K is the base change of the p-cyclotomic $\mathbf{Z}_p$-extension over $\mathbf{Q}$. The action of Δ on Γ is therefore trivial. In this case it has been conjectured that $E(L)$ is finitely generated (cf. [M1] when p is of good ordinary reduction for E) and this conjecture has been proved by Kato [K] in the case where $K/\mathbf{Q}$ is real abelian.

Example 2.2 (Mordell-Weil growth when K is totally complex). Assume that Leopoldt's conjecture holds, and that $K/\mathbf{Q}$ is (totally) complex. Consider the *$\mathbf{Q}_p$-vector space of $\mathbf{Z}_p$-extensions of K*. That is, form the vector space

$$V(K) := \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mathbf{Q}_p),$$

whose one-dimensional $\mathbf{Q}_p$-subspaces are in one-to-one correspondence with $\mathbf{Z}_p$-extensions of K. The vector space $V(K)$ inherits a natural $\mathbf{Q}_p$-linear representation of Δ. An exercise using class field theory gives us that the character of this Δ-representation is

$$\mathrm{Ind}_{\langle\sigma\rangle}^{\Delta}\chi \oplus \mathbf{1},$$

where $\mathbf{1}$ is the trivial character on Δ, $\sigma \in \Delta$ is a complex conjugation involution,

$$\chi : \langle\sigma\rangle \to \{\pm 1\} \subset \mathbf{C}^{\times}$$

is the nontrivial character on $\langle\sigma\rangle = \{1, \sigma\} \subset \Delta$, and $\mathrm{Ind}_{\langle\sigma\rangle}^{\Delta}$ refers to induction of characters from the subgroup $\langle\sigma\rangle$ to Δ. Here the "$\mathbf{1}$" corresponds to the cyclotomic $\mathbf{Z}_p$-extension and the "$\mathrm{Ind}_{\langle\sigma\rangle}^{\Delta}\chi$" cuts out a hyperplane in $V(K)$ that we call the *anti-cyclotomic hyperplane*

$$V(K)^{\mathrm{anti-cyc}} \subset V(K).$$

2.1 Representations in Mordell-Weil.

The "big" Mordell-Weil group $E(L)$ of all L-rational points of E is a union of finite-rank $\mathcal{G} = \mathrm{Gal}(L/\mathbf{Q})$-stable subgroups, so one way of trying to understanding the growth of Mordell-Weil is to ask, for finite dimensional irreducible complex characters τ of $\mathcal{G}$, whether or not the $\mathcal{G}$-representation space V of τ occurs in $E(F) \otimes \mathbf{C}$ for some intermediate Galois extension $F/\mathbf{Q}$. Mackey's criterion (cf. [Se] §8.2, Prop. 25) gives a description of all the irreducible characters on $\mathcal{G}$ in terms of induced characters. Here, in any event, is how to get quite a few irreducible characters of $\mathcal{G}$.

Define an action of Δ on the group of (continuous, hence finite order) characters of Γ as follows. For $\psi \in \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mathbf{C}^{\times})$ and $\delta \in \Delta$, define ψ^{δ} by the formula

$$\psi^{\delta}(\gamma) := \psi(\delta^{-1}(\gamma)) \quad \text{for } \gamma \in \Gamma.$$

For such a ψ let $H_\psi \subset \Delta$ be the stabilizer of ψ, let $K_\psi \subset K$ be the fixed field of H_ψ, and put $\mathcal{G}_\psi := \mathrm{Gal}(L/K_\psi) \subset \mathcal{G}$.

Lemma 2.3. *With notation as above, every $\psi : \Gamma \to \mathbf{C}^\times$ extends uniquely to a character $\psi_0 : \mathcal{G}_\psi \to \mathbf{C}^\times$ of p-power order (that is, the restriction of ψ_0 to Γ is ψ).*

Proof. Fix ψ. Since $|\Delta|$ is prime to p, $\mathcal{G}_\psi$ is (noncanonically) a semidirect product of H_ψ and Γ. More precisely, there is a subgroup $\tilde{H}_\psi \subset \mathcal{G}_\psi$ that projects isomorphically to H_ψ, and such that $\mathcal{G}_\psi = \Gamma \cdot \tilde{H}_\psi$. We define ψ_0 by $\psi_0(\gamma h) = \psi(\gamma)$ for $h \in \tilde{H}_\psi$ and $\gamma \in \Gamma$. Then ψ_0 is a homomorphism because $\psi^h = \psi$ for $h \in H_\psi$, ψ_0 clearly has p-power order, and the restriction of ψ_0 to Γ is ψ.

If ψ_0' is another such extension of ψ, then $\psi_0'\psi_0^{-1}$ is trivial on Γ, and hence is the inflation of a character of H_ψ of p-power order, which must be trivial. $\square$

Definition 2.4. Suppose $\psi : \Gamma \to \mathbf{C}^\times$. Lemma 2.3 shows that ψ is the restriction to K of a character of a $\mathbf{Z}_p$-extension of K_ψ, and clearly K_ψ is minimal with this property. We will call K_ψ the *level* of ψ, and we say that ψ is *new of level* K_ψ. We will say that ψ is *generic* if ψ is new of level K, i.e., if H_ψ is trivial.

Let $\psi_0 : \mathcal{G}_\psi \to \mathbf{C}^\times$ be the extension of ψ given by Lemma 2.3, and define

$$\phi_\psi := \mathrm{Ind}_{\mathcal{G}_\psi}^{\mathcal{G}} \psi_0,$$

the induced character from $\mathcal{G}_\psi$ to $\mathcal{G}$. By [Se] §8.2, Proposition 25, ϕ_ψ is an irreducible character of $\mathcal{G}$. We will also say that ϕ_ψ has level K_ψ, and that ϕ_ψ is generic if ψ is generic.

Proposition 2.5. *Suppose $\psi : \Gamma \to \mathbf{C}^\times$, and let $\phi_\psi = \mathrm{Ind}_{\mathcal{G}_\psi}^{\mathcal{G}} \psi_0$ be the induced character given by Definition 2.4.*

Then ϕ_ψ is real-valued if and only if there is an element $\sigma \in \Delta$ such that $\psi^\sigma = \psi^{-1}$. Such a σ lies in the normalizer $N(H_\psi)$ of H_ψ in Δ, and if $\psi \neq \mathbf{1}$ then σ has order 2 in $N(H_\psi)/H_\psi$.

Proof. Let $\langle\ ,\ \rangle_G$ denote the usual pairing on characters of a profinite group G. Then using Frobenius reciprocity ([Se] Theorem 13, §7.2) for the second equivalence, and [Se] Proposition 22, §7.3, for the third and fourth,

$$\begin{aligned}
\phi_\psi \text{ is real-valued} &\iff \langle \phi_\psi, \bar{\phi}_\psi \rangle_{\mathcal{G}} > 0 \\
&\iff \langle \mathrm{Res}_{\mathcal{G}_\psi}^{\mathcal{G}} \phi_\psi, \bar{\psi}_0 \rangle_{\mathcal{G}_\psi} > 0 \\
&\iff \langle \mathrm{Ind}_{H_\sigma}^{\mathcal{G}_\psi} (\psi^\sigma)_0, \bar{\psi}_0 \rangle_{\mathcal{G}_\psi} > 0 \text{ for some } \sigma \in \Delta
\end{aligned}$$

where $H_\sigma = H_\psi \cap H_{\psi^\sigma}$ and $(\psi^\sigma)_0$ is the extension of ψ^σ to H_σ of Lemma 2.3

$$\iff \psi^\sigma = \bar{\psi} = \psi^{-1} \text{ for some } \sigma \in \Delta.$$

If $\psi^\sigma = \bar\psi$ then we have $\sigma H_\psi \sigma^{-1} = H_{\psi^\sigma} = H_\psi$, so $\sigma \in N(H_\psi)$, and $\psi^{\sigma^2} = \psi$ so $\sigma^2 \in H_\psi$. If further $\psi \neq \mathbf{1}$ then (since p is odd) $\psi^\sigma \neq \psi$, so $\sigma \notin H_\psi$. This completes the proof. □

Corollary 2.6. *Suppose $\psi \neq \mathbf{1}$. Then ϕ_ψ is real-valued if and only if there is a subfield $K_\psi^+ \subset K_\psi$ such that $[K_\psi : K_\psi^+] = 2$ and $L^{\ker(\psi_0)}$ is Galois over K_ψ^+ with dihedral Galois group. In particular, if ϕ_ψ is real-valued then $[\Delta : H_\psi]$ is even.*

Proof. This follows directly from Proposition 2.5. If ϕ_ψ is real-valued we take K_ψ^+ to be be the subfield of K_ψ fixed by the element σ of Proposition 2.5. Conversely, if there is such a field K_ψ^+, let σ be a lift to Δ of the nontrivial automorphism of K_ψ/K_ψ^+ and apply Proposition 2.5. □

2.2 Mordell-Weil and root numbers

Let τ be the character of an irreducible finite dimensional complex $\mathcal{G}$-representation V. Appealing to a suitably general version of the conjecture of Birch and Swinnerton-Dyer, and assuming that the relevant L-function $L(E, \tau, s)$ has analytic continuation to the entire complex plane, we expect that the representation V occurs in $E(F) \otimes \mathbf{C}$ (for F the fixed field of the $\mathcal{G}$-representation V) if and only if the L-function $L(E, \tau, s)$ vanishes at $s = 1$. We also expect (but do not yet have, in general) a functional equation of the form

$$L(E, \tau, s) = W(E, \tau, s) L(E, \bar\tau, 2 - s),$$

where $W(E, \tau, s)$ is an explicit function involving the exponential function and the Γ-function. Even though the functional equation remains conjectural, there is an explicit definition of $W(E, \tau, s)$ (see for example [D, Ro]). If τ is real-valued, then the *root number* $W(E, \tau) := W(E, \tau, 1) = \pm 1$. Moreover, if $W(E, \tau, 1) = -1$ it would follow that $L(E, \tau, s)$ vanishes at $s = 1$ (to odd order). Then, by the Birch and Swinnerton-Dyer conjecture we would expect that the representation space V occurs in $E(L) \otimes \mathbf{C}$.

It is natural to ask if the really huge contribution to Mordell-Weil (if there is any) will come from this "expected" occurrence of representations in $E(L)$. This leads us to seek out real irreducible characters τ with root number $W(E, \tau) = -1$. Proposition 2.5 provides us with a substantial collection of real characters, and it remains to determine their root numbers.

Example 2.7. Suppose first that K is quadratic imaginary. We also suppose, for simplicity, that the discriminant of the field K, the conductor N of the elliptic curve E, and the prime number p are pairwise relatively prime. The unique nontrivial element $\sigma \in \Delta$ is complex conjugation, and the nontrivial character $\chi : \langle\sigma\rangle = \Delta \to \mathbf{C}^\times$ corresponds in the usual way to the quadratic Dirichlet character χ_K attached to the field K.

Choose $\psi \in \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mathbf{C}^\times)^-$ (the subgroup of homomorphisms on which σ acts as -1), and put $\phi_\psi = \mathrm{Ind}_\Gamma^{\mathcal{G}} \psi$ as in Definition 2.4. Then ϕ_ψ is real and generic by Proposition 2.5. Viewing $\det\phi_\psi : \mathcal{G} \to \mathbf{C}^\times$ as a Dirichlet character in the usual way we have

$$W(E,\phi_\psi) = (\det\phi_\psi)(-N)\cdot W(E)^{\dim\phi_\psi}$$

where $W(E) = W(E,\mathbf{1})$ is the root number of E (see for example Proposition 10 of [Ro]). But $(\det\phi_\psi)$ is simply the inflation of χ, and $\dim\phi_\psi = 2$, so this identity simplifies to

$$W(E,\phi_\psi) = \chi_K(-N). \tag{1}$$

The surprising consequence of this formula, which we will see repeated even more generally, is that the root number does not depend upon much: it is independent of the choice of generic (real) character ψ. and the elliptic curve E only enters into the formula for the root number via its conductor.
This is the case that has seen extraordinary progress recently via the detailed study of the tower of Heegner points. We will return to this in §4 of this article.

We now return to the general case, where $K/\mathbf{Q}$ is Galois with group Δ, L is the maximal $\mathbf{Z}_p^d$-extension of K, and $\mathcal{G} = \mathrm{Gal}(L/\mathbf{Q})$. From now on we suppose that the discriminant $\mathrm{disc}(K)$ of the field K, the conductor N of the elliptic curve E, and the prime p are pairwise relatively prime.
If $H \subset \Delta$ let $\chi_{\Delta/H} : G_\mathbf{Q} \to \pm 1$ be the determinant of $\mathrm{Ind}_H^\Delta \mathbf{1}$, the permutation representation of Δ on the set of left cosets Δ/H. (If $H = \{1\}$ we will write simply χ_Δ.) We will view $\chi_{\Delta/H}$ (and every other one-dimensional character of $G_\mathbf{Q}$) as a Dirichlet character in the usual way.

Theorem 2.8. *If $\psi \neq \mathbf{1}$ and ϕ_ψ is real-valued, then $W(E,\phi_\psi) = \chi_{\Delta/H_\psi}(-N)$. In particular characters of the same level have the same root number.*

Proof. We have $\phi_\psi = \mathrm{Ind}_{\mathcal{G}_\psi}^{\mathcal{G}} \psi_0$ from Definition 2.4. By Corollary 2.6, $\dim(\phi_\psi) = [\mathcal{G} : \mathcal{G}_\psi] = [\Delta : H]$ is even. Hence Proposition 10 of [Ro] ("a special case of a well-known formula") shows that

$$W(E,\phi_\psi) = (\det\phi_\psi)(-N)W(E)^{\dim(\phi_\psi)} = (\det\phi_\psi)(-N).$$

It remains to show that $\det\phi_\psi = \chi_{\Delta/H_\psi}$. We thank the referee for pointing out the following simple argument.
Let $\mathfrak{p}$ be a prime of $\bar{\mathbf{Q}}$ above p. Since ψ_0 has p-power order, $\psi_0 \equiv \mathbf{1} \pmod{\mathfrak{p}}$ and so

$$\det\phi_\psi = \det(\mathrm{Ind}_{\mathcal{G}_\psi}^{\mathcal{G}} \psi_0) \equiv \det(\mathrm{Ind}_{\mathcal{G}_\psi}^{\mathcal{G}} \mathbf{1}) = \det(\mathrm{Ind}_{H_\psi}^{\Delta} \mathbf{1}) = \chi_{\Delta/H_\psi} \pmod{\mathfrak{p}}.$$

Since p is odd and both $\det\phi_\psi$ and χ_{Δ/H_ψ} take only the values ± 1, it follows that $\det\phi_\psi = \chi_{\Delta/H_\psi}$. □

Proposition 2.9. *The following are equivalent:*

(i) $\chi_\Delta \neq \mathbf{1}$,

(ii) Δ *has a nontrivial cyclic* 2*-Sylow subgroup,*

(iii) Δ *is the semi-direct product of a (normal) subgroup of odd order with a nontrivial cyclic* 2*-group.*

If these (equivalent) conditions hold then Δ *is solvable,* K *contains a unique quadratic subfield* $k/\mathbf{Q}$*, and* $\chi_\Delta = \chi_k$*, the quadratic character of* k*.*

Proof. We have

$$\chi_\Delta(\sigma) = \mathrm{sign}(\pi_\sigma)$$

where π_σ is the permutation of Δ given by left multiplication by σ. If $\sigma \in \Delta$ has order d, then the permutation π_σ is a product of $|\Delta|/d$ d-cycles, so

$$\chi_\Delta(\sigma) = \mathrm{sign}(\pi_\sigma) = (-1)^{(d-1)|\Delta|/d} = \begin{cases} -1 & \text{if } d \text{ is even and } |\Delta|/d \text{ is odd,} \\ 1 & \text{otherwise.} \end{cases}$$

Thus $\chi_\Delta(\sigma) = -1$ if and only if the cyclic subgroup generated by σ contains a nontrivial 2-Sylow subgroup of Δ, and so (i) is equivalent to (ii).
If (i) and (ii) hold, then $\ker(\chi)$ is a (normal) subgroup of index 2 in Δ, which also has a cyclic 2-Sylow subgroup. Proceeding by induction we get a filtration

$$\Delta = \Delta_0 \supset \Delta_1 \supset \cdots \supset \Delta_k$$

where $[\Delta_i : \Delta_{i+1}] = 2$ and $|\Delta_k|$ is odd.
We claim that Δ_k is normal in Δ. For if H is a conjugate of Δ_k, then $|H|$ is odd so we see by induction that for every $i \geq 1$ the map $H \to \Delta_{i-1}/\Delta_i$ is injective, i.e., $H \subset \Delta_i$. Thus $H \subset \Delta_k$, so Δ_k is normal. Therefore the Schur-Zassenhaus Theorem shows that Δ is the semidirect product of Δ_k with a 2-Sylow subgroup. This shows that (ii) implies (iii)[1], and it is immediate that (iii) implies (ii).
Suppose now that conditions (i)-(iii) hold. It follows from (iii) and the Feit-Thompson theorem that Δ is solvable. By (i), $\chi_\Delta = \chi_k$ for some quadratic field $k \subset K$, and by (ii), K contains at most one quadratic field. This completes the proof. □

Corollary 2.10. *Suppose that* ϕ_ψ *is real and generic. Then* $W(E,\phi) = -1$ *if and only if the equivalent conditions of Proposition 2.9 hold and* $\chi_k(-N) = -1$.

Proof. This is immediate from Theorem 2.8 and Proposition 2.9. □

Definition 2.11. Following Theorem 2.8, if $F \subset K$ we define $W(E/F)$ to be the common root number of all real characters ϕ_ψ of level F. (The proof of Theorem 2.8 shows that this common root number is also the root number in the functional equation of $L(E/F,s)$.)

[1] The fact that (ii) implies (iii) was proved by Frobenius in §6, p. 1039 of [F], by the same method we give here. Another proof was given by Burnside in [Bu], Corollary II of §244, p. 327. We thank Persi Diaconis for pointing us toward these references.

In particular if $F = K$, then $W(E/K) = \chi_k(-N)$ if Δ has nontrivial cyclic 2-Sylow subgroup (where k is the quadratic field inside K), and $W(E/K) = 1$ otherwise.

Suppose now that we are in such a situation where $W(E/K) = -1$. From the discussion above we expect significant growth of Mordell-Weil rank as we ascend the tower of intermediate finite extensions contained in $\mathbf{Z}_p^d$-extensions that correspond to the -1-eigenspace in $V(K)$ of some element of order 2 in Δ. We next work out the elementary features of two examples that are more general than the case of $K/\mathbf{Q}$ quadratic imaginary, and for which we do not, as yet, have any satisfactory theory of Mordell-Weil growth.

EXAMPLE 2.12 ($K/\mathbf{Q}$ IS A COMPLEX ABELIAN GALOIS EXTENSION). In this case Leopoldt's conjecture is known to be true, there is a unique complex conjugation involution, and its -1-eigenspace is the entire anti-cyclotomic hyperplane.

QUESTION 2.13. *Can one use towers of Heegner points in Shimura curves over totally real fields to account for (at least some of) the* expected *Mordell-Weil growth as one ascends the finite intermediate extensions of the anti-cyclotomic hyperplane?*

EXAMPLE 2.14 ($K/\mathbf{Q}$ IS A COMPLEX S_3-EXTENSION). To guard against complacency, we wish to mention this relatively simple case, where no analogue of the detailed results known in the quadratic imaginary case is currently available. Suppose $\Delta \cong S_3$, the symmetric group on three letters, and suppose that $W(E/K) = -1$. Let k be the quadratic field contained in K. Leopoldt's conjecture holds for K (for "easy" reasons: if Leopoldt's conjecture failed the natural homomorphism from global units to local units would be trivial, which it is not). We may decompose the four-dimensional Δ-representation space $V(K)$ into the sum of two Δ-stable planes

$$V(K) = V(K)_{\mathrm{new}} \oplus V(k)$$

where the *new* plane $V(K)_{\mathrm{new}} \subset V(K)^{\mathrm{anti-cyc}}$ is of codimension one in the anti-cyclotomic hyperplane. There are three involutions $\sigma, \sigma', \sigma''$ in Δ, none of which act as scalars either on $V(K)_{\mathrm{new}}$ or on $V(k)$. Let L_σ/K denote the unique $\mathbf{Z}_p^2$-extension of K on whose Galois group σ acts as -1, and similarly for σ' and σ''. We have, then, three $\mathbf{Z}_p^2$-extensions, L_σ/K, $L_{\sigma'}/K$ and $L_{\sigma''}/K$, sub-extensions of the anti-cyclotomic $\mathbf{Z}_p^3$-extension of K. Each of these $\mathbf{Z}_p^2$-extensions is the compositum of the "old" anti-cyclotomic $\mathbf{Z}_p$-extension of the quadratic subfield $k \subset K$ and the unique $\mathbf{Z}_p$-extension of K that corresponds to a line in $V(K)_{\mathrm{new}}$ that is a -1-eigenspace for one of the three involutions in Δ.

CHALLENGE 2.15. *As one ascends the intermediate fields of finite degree in each of these $\mathbf{Z}_p^2$-extensions we* expect *significant growth in the ranks of the corresponding Mordell-Weil groups. Find this Mordell-Weil contribution.*

Remark 2.16. Theorem 2.10 fails in the situation of Example 1.4 because in that case E has complex multiplication by K, so the conductor of E is not relatively prime to the discriminant of K.

3 Where is the support of the Selmer module?

Keep the notation of the previous section. In particular we continue to assume that the conductor of E, the discriminant of K, and the prime p are pairwise relatively prime.

3.1 Selmer modules

If F is an abelian extension of K we put $\Lambda_F = \mathbf{Z}_p[[\mathrm{Gal}(F/K)]]$; if $[F : K]$ is finite this is just the group ring $\mathbf{Z}_p[\mathrm{Gal}(F/K)]$, and if $\mathrm{Gal}(F/K) \cong \mathbf{Z}_p^d$ then Λ_F is noncanonically isomorphic to a power series ring $\mathbf{Z}_p[[T_1, \ldots, T_d]]$. If $F' \subset F$ then $\Lambda_{F'}$ is naturally a quotient of Λ_F.
For every number field F let $S_p(E/F) \subset H^1(F, E[p^\infty])$ be the classical Selmer group, which sits in the center of the exact sequence

$$0 \longrightarrow E(F) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow S_p(E/F) \longrightarrow Ш(E/F)[p^\infty] \longrightarrow 0 \tag{2}$$

where $Ш(E/F)[p^\infty]$ is the p-part of the Shafarevich-Tate group of E over F. We extend this definition to possibly infinite algebraic extensions of $\mathbf{Q}$ by passing to a direct limit

$$S_p(E/F) := \underset{0}{\varinjlim} F' \subset F S_p(E/F')$$

where F' ranges through the finite extensions of $\mathbf{Q}$ in F. If F/K is Galois then $S_p(E/F)$ has a natural $\mathbf{Z}_p[[\mathrm{Gal}(F/K)]]$-module structure. Specifically, $S_p(E/L)$ is a Λ_L-module. We will refer to $S_p(E/L)$ as the *discrete Selmer module* attached to L/K. If $K_\infty \subset L$ is a $\mathbf{Z}_p$-extension of K we will write $K_n \subset K_\infty$ for the subfield of degree p^n over K, and we have the Λ_{K_∞}-module

$$S_p(E/K_\infty) = \underset{0}{\varinjlim} n S_p(E/K_n).$$

The following Control Theorem is a strengthening by Greenberg ([G2] Proposition 3.1) of a theorem of the first author [M1].

Theorem 3.1 (Control Theorem). *Suppose that K_∞ is a $\mathbf{Z}_p$-extension of K, and E has good ordinary reduction at p. Then the restriction maps $H^1(K_n, E[p^\infty]) \to H^1(K_\infty, E[p^\infty])$ induce maps*

$$S_p(E/K_n) \longrightarrow S_p(E/K_\infty)^{\mathrm{Gal}(K_\infty/K_n)}$$

whose kernels and cokernels are finite and bounded independently of n.

For every F we form the corresponding compact Selmer group

$$X(E/F) := \mathrm{Hom}(S_p(E/F), \mathbf{Q}_p/\mathbf{Z}_p).$$

Then $X(E/L)$ is a finitely generated Λ_L-module, and if K_∞ is a $\mathbf{Z}_p$-extension of K then $X(E/K_\infty)$ is finitely generated over Λ_{K_∞}.

Proposition 3.2. *Suppose K_∞ is a $\mathbf{Z}_p$-extension of K. If E has good ordinary reduction at p, and $\text{Ш}(E/K_n)[p^\infty]$ is finite for every n, then the growth number $r(E, K_\infty/K)$ defined in Proposition 1.1 is equal to the rank of the compact Selmer Λ_{K_∞}-module $X(E/K_\infty)$.*

Proof. Write $\Lambda_\infty = \Lambda_{K_\infty}$ and $\Lambda_n = \Lambda_{K_n} = \mathbf{Z}_p[\mathrm{Gal}(K_n/K)]$. The Control Theorem (Theorem 3.1) shows that there is a map with finite kernel and cokernel

$$X(E/K_\infty) \otimes_{\Lambda_\infty} \Lambda_n \to X(E/K_n).$$

If $\text{Ш}(E/K_n)[p^\infty]$ is finite then (2) shows that

$$\mathrm{rank}_{\mathbf{Z}}(E(K_n)) = \mathrm{rank}_{\mathbf{Z}_p}(X(E/K_n)) = \mathrm{rank}_{\mathbf{Z}_p}(X(E/K_\infty) \otimes_{\Lambda_\infty} \Lambda_n),$$

and the structure theory of Λ_{K_∞}-modules shows that

$$\mathrm{rank}_{\mathbf{Z}_p}(X(E/K_\infty) \otimes_{\Lambda_\infty} \Lambda_n) = p^n \mathrm{rank}_{\Lambda_\infty}(X(E/K_\infty)) + O(1). \qquad \square$$

3.2 The support of the Selmer module

Definition 3.3. Recall that $\Gamma = \mathrm{Gal}(L/K) \cong \mathbf{Z}_p^d$, so $\Lambda_L = \mathbf{Z}_p[[\Gamma]]$. The group Δ acts naturally and $\mathbf{Z}_p$-linearly on Γ.
If $F \subset K$ let L_F denote the compositum of all $\mathbf{Z}_p$-extensions of F. The group $\mathrm{Aut}(F)$ of automorphisms of F acts on $\Gamma_F := \mathrm{Gal}(L_F/F)$. If $\sigma \in \mathrm{Aut}(F)$ has order 2, we let $\Gamma^{\sigma,-}$ denote the maximal quotient of Γ on which σ acts as -1, and $L_F^{\sigma,-} \subset L_F$ the extension of F.
The *minus locus* in $\mathrm{Spec}\,\Lambda_L$ is the closed subscheme of $\mathrm{Spec}\,\Lambda_L$

$$\bigcup_{\substack{F \subset K \\ W(E/F) = -1}} \bigcup_{\substack{\sigma \in \mathrm{Aut}(F) \\ \sigma^2 = 1, \sigma \neq 1}} \mathrm{Spec}\,\Lambda_{KL_F^{\sigma,-}},$$

where we view $\mathrm{Spec}\,\Lambda_{KL_F^{\sigma,-}} \subset \mathrm{Spec}\,\Lambda_L$ via the projection map $\Lambda_L \twoheadrightarrow \Lambda_{KL_F^{\sigma,-}}$.

Using the root number considerations above, the following conjecture follows from a suitably general version of the Birch and Swinnerton-Dyer conjecture.

Conjecture 3.4. *The support of the compact Selmer module $X(E/L)$ in $\mathrm{Spec}\,\Lambda_L$ contains the minus locus.*

Example 3.5. For each quadratic imaginary field $F \subset K$ such that $\chi_F(-N) = -1$, the minus locus contains a $\mathbf{Z}_p$-line corresponding to the anticyclotomic $\mathbf{Z}_p$-extension of F, and Heegner points should provide the corresponding part of the Selmer group.
On the other hand, if $\chi_F(-N) = +1$ for every quadratic field F contained in K, then Theorem 2.8 shows that $W(E/F) = +1$ for *every* subfield F of K, and the minus locus is empty.
In Example 2.14, the minus locus consists of the union of the 3 $\mathbf{Z}_p$-planes $\operatorname{Spec}\Lambda_{L^\sigma}$, $\operatorname{Spec}\Lambda_{L^{\sigma'}}$, and $\operatorname{Spec}\Lambda_{L^{\sigma''}}$.

Let

$$\mathrm{MW}_p(E/L) := \operatorname{Hom}(E(L), \mathbf{Z}_p) = \operatorname{Hom}(E(L) \otimes \mathbf{Q}_p/\mathbf{Z}_p, \mathbf{Q}_p/\mathbf{Z}_p),$$

a quotient of $X(E/L)$. We will say that L/K has *unexpected large Mordell-Weil* if there exists a subscheme of Krull dimension greater than 1 in $\operatorname{Spec}\Lambda_L$ that is in the support of $\mathrm{MW}_p(E/L)$, but in the complement of the minus locus.

Question 3.6. *Are there Galois extensions $K/\mathbf{Q}$ such that L/K has unexpected large Mordell-Weil?*

We will call an abelian extension F/K a $\mathbf{Z}_p$-power extension of K if $\operatorname{Gal}(F/K) = \mathbf{Z}_p^k$ for some $k \geq 0$.

Question 3.7. *Are there $\mathbf{Z}_p$-power extensions $L_1, \ldots, L_k$ of K, and a finite subset $\Psi \subset \operatorname{Hom}(\Gamma, \mathbf{C}^\times)$, such that*

$$\{\psi : \Gamma \to \mathbf{C}^\times : \psi \textit{ occurs in } E(L) \otimes \mathbf{C}\} \;=\; \cup_i \operatorname{Hom}(\operatorname{Gal}(L_i/K), \mathbf{C}^\times) \;\cup\; \Psi?$$

Remark 3.8. Question 3.7 is motivated by work of Monsky, who was the first to study what the support of a Selmer module (in his case, an ideal class group module) over a $\mathbf{Z}_p^d$-extension should look like when $d \geq 2$. Iwasawa theory suggests that there should be an ideal $\mathcal{A} \subset \Lambda$ such that ψ occurs in $E(L) \otimes \mathbf{C}$ if and only if $\psi(\mathcal{A}) = 0$ (where we fix an embedding $\bar{\mathbf{Q}}_p \hookrightarrow \mathbf{C}$ so that we can view ψ as a character into $\bar{\mathbf{Q}}_p$). Monsky (Theorem 2.6 of [Mo]) showed that there is a set $\{L_1, \ldots, L_k\}$ of $\mathbf{Z}_p$-power extensions of K, and $\psi_i, \ldots, \psi_k \in \operatorname{Hom}(\Gamma, \mathbf{C}^\times)$ such that

$$\{\psi : \psi(\mathcal{A}) = 0\} \;=\; \cup_{i=1}^k \psi_i \cdot \operatorname{Hom}(\operatorname{Gal}(L_i/K), \mathbf{C}^\times).$$

Combining this with the root number calculation of Theorem 2.8 leads to Question 3.7. One can also ask the following variant of Question 3.7.

Question 3.9. *Is there a collection $L_1, \ldots, L_k$ of $\mathbf{Z}_p$-power extensions of K (not necessarily distinct) such that for every finite extension F of K in L we have*

$$\operatorname{rank}_{\mathbf{Z}}(E(F)) = \sum_{i=1}^k [F \cap L_i : K] + O(1)?$$

Here the bound $O(1)$ should depend only on E and K, not on F.

4 Where are the universal norms in Mordell-Weil?

Fix for this section a $\mathbf{Z}_p$-extension K_∞/K, and let $\Gamma := \mathrm{Gal}(K_\infty/K)$ and $\Lambda := \Lambda_{K_\infty} = \mathbf{Z}_p[[\Gamma]]$. As before, K_n will denote the extension of K of degree p^n in K_∞, and $\Lambda_n = \Lambda_{K_n} = \mathbf{Z}_p[\mathrm{Gal}(K_n/K)]$.

4.1 Universal norms

Definition 4.1. For $m \geq n$ consider the ($\mathbf{Z}_p$-linear) norm maps (or, perhaps, "trace maps" since one usually writes Mordell-Weil groups additively)

$$N_{m,n} : E(K_m) \otimes \mathbf{Z}_p \longrightarrow E(K_n) \otimes \mathbf{Z}_p.$$

Define

$$\mathcal{U}(E, K_\infty/K_n) := \bigcap_{m \geq n} N_{m,n}(E(K_m) \otimes \mathbf{Z}_p) \ \subset E(K_n) \otimes \mathbf{Z}_p.$$

Passing to the projective limits we define a $\mathrm{Gal}(K/\mathbf{Q})$-semi-linear Λ-module

$$\mathcal{U}(E/K_\infty) := \underset{0}{\varprojlim}\, n\, E(K_n) \otimes \mathbf{Z}_p = \underset{0}{\varprojlim}\, n\, \mathcal{U}(E, K_\infty/K_n),$$

and $\mathcal{U}(E, K_\infty/K_n)$ is the image of the projection $\mathcal{U}(E/K_\infty) \to E(K_n) \otimes \mathbf{Z}_p$.

Theorem 4.2. *Suppose E has good ordinary reduction at p, and $\text{Ш}(E/K_n)[p^\infty]$ is finite for every n. Let $r = \mathrm{rank}_\Lambda(X(E/K_\infty))$. Then*

(i) *$\mathcal{U}(E/K_\infty)$ has finite index in a free Λ-module of rank r,*

(ii) *$\mathcal{U}(E, K_\infty/K_n) \otimes \mathbf{Q}_p$ is a free $\Lambda_n \otimes \mathbf{Q}_p$-submodule of $E(K_n) \otimes \mathbf{Q}_p$ of rank r.*

Proof. Write simply X for the finitely generated Λ-module $X(E/K_\infty)$, and $X_n = X \otimes \Lambda_n$.
It follows from the Control Theorem (Theorem 3.1) that there is an injection with finite cokernel bounded independently of n

$$\mathrm{Hom}(X(E/K_n), \mathbf{Z}_p) \longrightarrow \mathrm{Hom}(X_n, \mathbf{Z}_p).$$

Further, it follows from (2) that if $\text{Ш}(E/K_n)[p^\infty]$ is finite then

$$\mathrm{Hom}(X(E/K_n), \mathbf{Z}_p) \cong E(K_n) \otimes \mathbf{Z}_p.$$

Taking inverse limits we get an injective map

$$\mathcal{U}(E/K_\infty) = \varprojlim(E(K_n) \otimes \mathbf{Z}_p) \longrightarrow \varprojlim(\mathrm{Hom}(X_n, \mathbf{Z}_p)) =: \mathcal{U}(X)$$

with finite cokernel, where $\mathcal{U}(X)$ is the abstract universal norm Λ-module studied in Appendix A.2. Since $\mathcal{U}(X)$ is free of rank r (Proposition A.20), this proves (i).

Consider the diagram

$$\begin{tikzcd}
\mathcal{U}(E/K_\infty)\otimes\mathbf{Q}_p \arrow[r] \arrow[d, "\cong"] & \mathcal{U}(E/K_\infty)\otimes\Lambda_n\otimes\mathbf{Q}_p \arrow[r] \arrow[d, "\cong"] & E(K_n)\otimes\mathbf{Q}_p \arrow[d] \\
\mathcal{U}(X)\otimes\mathbf{Q}_p \arrow[r, two heads] & \mathcal{U}(X)\otimes\Lambda_n\otimes\mathbf{Q}_p \arrow[r, hook] & \mathrm{Hom}(X_n,\mathbf{Q}_p)
\end{tikzcd}$$

where the horizontal maps are the natural projections. The lower right-hand map is injective by Proposition A.21, so the upper right-hand map is injective, which proves (ii). □

4.2 Anticyclotomic $\mathbf{Z}_p$-extensions of quadratic imaginary fields

From now on we assume that K is quadratic imaginary, and K_∞ is the anticyclotomic $\mathbf{Z}_p$-extension of K (the unique $\mathbf{Z}_p$-extension, Galois over $\mathbf{Q}$, on which the nontrivial element of $\mathrm{Gal}(K/\mathbf{Q})$ acts as -1). Let $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$. We assume in addition that E has good ordinary reduction at p, that $Ш(E/K_n)[p^\infty]$ is finite for every n, and that every prime dividing the conductor N of E splits in K. The last assumption guarantees that $W(E/K) = \chi_K(-N) = -1$.

Theorem 4.3 (Vatsal [V], Cornut [Co]). *With assumptions as above,* $\mathrm{rank}_\Lambda(X(E/K_\infty)) = 1$.

Let $E(K)^\pm \subset E(K)$ denote the $+1$ and -1 eigenspaces for the action of $\Delta = \mathrm{Gal}(K/\mathbf{Q})$ on $E(K)$. Thus $E(K)^+ = E(\mathbf{Q})$, and $E(K)^- \cong E^{(K)}(\mathbf{Q})$ where $E^{(K)}$ is the quadratic twist of E by $K/\mathbf{Q}$. Also write $r_\pm = \mathrm{rank}_{\mathbf{Z}}(E(K)^\pm)$, and let $W(E/\mathbf{Q}) = \pm 1$ denote the root number in the functional equation of $L(E/\mathbf{Q}, s)$.

Corollary 4.4. *The universal norm subgroup $\mathcal{U}(E, K_\infty/K)\otimes\mathbf{Q}_p$ is a one-dimensional $\mathbf{Q}_p$-subspace of $E(K)\otimes\mathbf{Q}_p$, contained either in $E(K)^+\otimes\mathbf{Q}_p$ or $E(K)^-\otimes\mathbf{Q}_p$.*

Proof. By Theorems 4.2(ii) and 4.3, $\dim_{\mathbf{Q}_p}(\mathcal{U}(E, K_\infty/K)\otimes\mathbf{Q}_p) = 1$. It is clear from the definition that $\mathcal{U}(E, K_\infty/K)\otimes\mathbf{Q}_p$ is stable under Δ, so it must lie in $E(K)^\pm\otimes\mathbf{Q}_p$. □

Definition 4.5. Following Corollary 4.4, if $\mathcal{U}(E, K_\infty/K)\otimes\mathbf{Q}_p \subset E(K)^+\otimes\mathbf{Q}_p$ (resp., $E(K)^-\otimes\mathbf{Q}_p$) we say that the *sign of the p-anti-cyclotomic norms* in $E(K)$ is $+1$ (resp., -1).
In the language of Appendix A.1, the sign of the p-anti-cyclotomic norms is $\mathrm{sign}(\mathcal{U}(E/K_\infty))$, the sign of the Δ-semi-linear Λ-module $\mathcal{U}(E/K_\infty)$.

Theorem 4.6 (Nekovář [N]). *Under the hypotheses above,*

$$(-1)^{r_\pm} = \pm W(E/\mathbf{Q}) \text{ and } \mathrm{rank}_{\mathbf{Z}}(E(K)) \text{ is odd.}$$

Proof. Using (1), the root numbers in the functional equations of $L(E/\mathbf{Q},s)$, $L(E^{(K)}/\mathbf{Q},s)$, and $L(E/K,s)$ are, respectively, $W(E/\mathbf{Q})$, $\chi_K(-N)W(E/\mathbf{Q})$, and $\chi_K(-N)$. By Theorem 2.10 and our assumption that all primes dividing N split in K (the "Heegner hypothesis"), $\chi_K(-N)=\chi_K(-1)=-1$. Thus the conclusions of the theorem follow from the Parity Conjecture (which predicts, for every number field F, that $\mathrm{rank}_{\mathbf{Z}}(E(F)\equiv \mathrm{ord}_{s=1}L(E,s) \pmod 2)$), which under our hypotheses was proved by Nekovář. $\square$

Definition 4.7. By Theorem 4.6, $\mathrm{rank}_{\mathbf{Z}}(E(K)^+)\neq \mathrm{rank}_{\mathbf{Z}}(E(K)^-)$. We define

$$\epsilon(E/K)=\begin{cases}+1 & \text{if } \mathrm{rank}_{\mathbf{Z}}(E(K)^+)>\mathrm{rank}_{\mathbf{Z}}(E(K)^-),\\ -1 & \text{if } \mathrm{rank}_{\mathbf{Z}}(E(K)^-)>\mathrm{rank}_{\mathbf{Z}}(E(K)^+).\end{cases}$$

Conjecture 4.8 (Sign Conjecture). *We have*

$$\mathrm{sign}(\mathcal{U}(E/K_\infty))=\epsilon(E/K).$$

In other words $\mathcal{U}(E,K_\infty/K)\otimes\mathbf{Q}_p$ *lies in the* larger *of* $E(K)^+\otimes\mathbf{Q}_p$ *and* $E(K)^-\otimes\mathbf{Q}_p$*, and in particular* $\mathrm{sign}(\mathcal{U}(E/K_\infty))$ *is independent of* p*.*

Remark 4.9. Here is a brief heuristic argument that supports the Sign Conjecture. It is straightforward to prove that $\mathcal{U}(E,K_\infty/K)$ is contained in the nullspace of the (symmetric, bilinear) p-anti-cyclotomic height pairing (cf. [MT])

$$\langle\ ,\ \rangle_{\mathrm{anti-cycl}}: E(K)\otimes\mathbf{Z}_p\times E(K)\otimes\mathbf{Z}_p\longrightarrow \mathrm{Gal}(K_\infty/K)\otimes_{\mathbf{Z}_p}\mathbf{Q}_p.$$

Moreover, this height pairing is compatible with the action of $\mathrm{Gal}(K/\mathbf{Q})$ in the sense that if τ is the nontrivial automorphism of K, then

$$\langle\tau(v),\tau(w)\rangle_{\mathrm{anti-cycl}}=-\langle v,w\rangle_{\mathrm{anti-cycl}}.$$

It follows that $E(K)^+\otimes\mathbf{Z}_p$ and $E(K)^-\otimes\mathbf{Z}_p$ are each isotropic under the anti-cyclotomic height pairing, and the null-space of $\langle\ ,\ \rangle_{\mathrm{anti-cycl}}$ is the sum of the left and right nullspaces of the restriction of $\langle\ ,\ \rangle_{\mathrm{anti-cycl}}$ to

$$E(K)^+\otimes\mathbf{Z}_p\times E(K)^-\otimes\mathbf{Z}_p\longrightarrow \mathrm{Gal}(K_\infty/K)\otimes_{\mathbf{Z}_p}\mathbf{Q}_p. \tag{3}$$

It seems natural to conjecture that the pairing (3) is *as nondegenerate as possible.* (For a precise statement of this conjecture, and further discussion, see §3 of [BD1]). This "maximal nondegeneracy" would imply that (3) is either left or right nondegenerate, depending upon which of the two spaces $E(K)^-$ or $E(K)^+$ is larger, and this in turn would imply the Sign Conjecture.

4.3 Heegner points and the Sign Conjecture

We are grateful to Christophe Cornut who communicated to us Proposition 4.10 below and its proof.

Keep the assumptions of the previous section, and fix a modular parametrization $X_0(N) \twoheadrightarrow E$ and an embedding $K_\infty \hookrightarrow \mathbf{C}$. Let $\mathcal{H}_n \subset E(K_n)$ be the module of Heegner points as defined, for example, in [BD2] §2.5 or [M2] §19, and

$$\mathcal{H}_\infty = \varprojlim(\mathcal{H}_n \otimes \mathbf{Z}_p) \subset \mathcal{U}(E/K_\infty).$$

Then $\mathcal{H}_\infty$ is free of rank one over Λ, and stable under the action of $\Delta = \mathrm{Gal}(K/\mathbf{Q})$. In particular it is a Δ-semi-linear Λ-module in the sense of Appendix A.1, and $\mathrm{sign}(\mathcal{H}) \in \{1,-1\}$ describes the action of Δ on $\mathcal{H} \otimes_\Lambda \mathbf{Z}_p$ (Definition A.16).

Since $\mathcal{U}(E/K_\infty)$ is a torsion-free, rank-one Λ-modules (Theorem 4.2(i)), we can fix $\mathcal{L} \in \Lambda$ so that $\mathcal{L}\mathcal{U}(E/K_\infty) \subset \mathcal{H}_\infty$ and $[\mathcal{H}_\infty : \mathcal{L}\mathcal{U}(E/K_\infty)]$ is finite (take $\mathcal{L}$ to be a generator of the characteristic ideal of $\mathcal{U}(E/K_\infty)/\mathcal{H}_\infty$). Let I denote the augmentation ideal of Λ, the kernel of the natural map $\Lambda \twoheadrightarrow \mathbf{Z}_p$, and let $\mathrm{ord}_I(\mathcal{L})$ denote the largest power of I that contains $\mathcal{L}$. If we fix an isomorphism $\Lambda \cong \mathbf{Z}_p[[T]]$, then $\mathrm{ord}_I(\mathcal{L}) = \mathrm{ord}_{T=0}(\mathcal{L})$.

Proposition 4.10. (i) $\mathrm{sign}(\mathcal{H}_\infty) = -W(E/\mathbf{Q})$.

(ii) $\mathrm{sign}(\mathcal{U}(E/K_\infty)) = -W(E/\mathbf{Q})(-1)^{\mathrm{ord}_I(\mathcal{L})}$.

Proof. The Heegner module $\mathcal{H}_\infty$ has a generator h_∞ with the property that

$$\tau h_\infty = -W(E/\mathbf{Q})\sigma h_\infty$$

for some $\sigma \in \mathrm{Gal}(K_\infty/K)$, where τ is complex conjugation (see [Gr] §§1.4-1.5). Thus $\tau h_\infty \equiv -W(E/\mathbf{Q})h_\infty$ in $\mathcal{H}_\infty/I\mathcal{H}_\infty$, which proves (i). The second assertion then follows by Proposition A.17(ii). □

Conjecture 3.10 of Bertolini and Darmon in [BD1] asserts (in our notation) that

$$\mathrm{ord}_I(\mathcal{L}) = \max\{r_+, r_-\} - 1. \tag{4}$$

Corollary 4.11. *Conjecture 3.10 of Bertolini and Darmon [BD1] implies the Sign Conjecture.*

Proof. Let $\epsilon = \epsilon(E/K)$ as given by Definition 4.7, so $r_\epsilon = \max\{r_+, r_-\}$. Combining Proposition 4.10(ii), the conjecture (4), and Theorem 4.6 gives

$$\mathrm{sign}(\mathcal{U}(E/K_\infty)) = (-1)^{r_\epsilon} W(E/\mathbf{Q}) = \epsilon,$$

which is the Sign Conjecture. □

Remark 4.12. Suppose now that K is arbitrary (possibly even non-Galois), and K_∞/K is a $\mathbf{Z}_p$-extension that is "new", in the sense that it is not the base-change of a $\mathbf{Z}_p$-extension of a proper subfield of K. Suppose further that the compact Selmer module $X(E/K_\infty)$ has rank 1 over $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$. Then by Proposition 3.2 (assuming the Shafarevich-Tate conjecture) the growth number of $(E, K_\infty/K)$ is 1.

In the spirit of the questions from §3, we expect this can only happen if the characters ϕ_ψ are real-valued for every $\psi \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(K_\infty/K), \mathbf{C}^\times)$, and have root number $W(E, \phi_\psi) = W(E/K) = -1$. In this case Corollary 2.6 shows that K has an automorphism of order 2, with fixed field K^+, such that K_∞/K^+ is Galois with dihedral Galois group.

Thus in this setting, exactly as when K is quadratic imaginary, the universal norm module $\mathcal{U}(E, K_\infty)$ is a $\mathrm{Gal}(K/K^+)$-semi-linear Λ-module that is torsion-free of rank one over Λ, and we get a one-dimensional universal norm subspace $\mathcal{U}(E, K_\infty/K) \subset E(K) \otimes \mathbf{Q}_p$. Again $\mathcal{U}(E, K_\infty/K) \otimes \mathbf{Q}_p \subset E(K)^\pm \otimes \mathbf{Q}_p$, where $E(K)^\pm$ means the plus and minus spaces for the action of $\mathrm{Gal}(K/K^+)$, $\mathrm{rank}_{\mathbf{Z}}(E(K)^+)$ and $\mathrm{rank}_{\mathbf{Z}}(E(K)^-)$ (conjecturally) have opposite parity, and we can conjecture that $\mathcal{U}(E, K_\infty/K) \otimes \mathbf{Q}_p$ lies in the larger of $E(K)^+ \otimes \mathbf{Q}_p$ and $E(K)^- \otimes \mathbf{Q}_p$. As in Remark 4.9, such a conjecture would follow from the "maximal nondegeneracy" of the p-adic height attached to $(E, K_\infty/K)$.

4.4 Computational examples

The Sign Conjecture is trivially true if either $E(K)^+$ or $E(K)^-$ is finite. In the first nontrivial case, i.e., if $\min\{\mathrm{rank}(E(K)^\pm)\} = 1$, the Sign Conjecture would follow (using Remark 4.9) if the anti-cyclotomic height pairing is not identically zero.

Let us focus on this "first nontrivial case". Fix an elliptic curve E with $\mathrm{rank}_{\mathbf{Z}} E(\mathbf{Q}) = 2$, and let $R, S \in E(\mathbf{Q})$ generate a subgroup of finite index. If K is a quadratic field, let $E^{(K)}$ be the twist of E by the quadratic character attached to K. Fix a prime number p where E has good ordinary reduction. Let K run through the set $\mathcal{K}_E$ of all quadratic imaginary fields such that E and K satisfy our running hypotheses, and such that the rank of the Mordell-Weil group $E^{(K)}(\mathbf{Q})$ is 1; for each of these fields, choose a rational point $P_K \in E^{(K)}(\mathbf{Q}) \subset E(K)$ of infinite order. If the anti-cyclotomic height pairing is not identically zero, then the Sign Conjecture is true, so the p-anti-cyclotomic norm line for $K \in \mathcal{K}_E$ (call it ℓ_K) will lie in the $\mathbf{Q}_p$ vector space $E(\mathbf{Q}) \otimes \mathbf{Q}_p$. The *slope* of $\ell_K \subset E(\mathbf{Q}) \otimes \mathbf{Q}_p$ with respect to the basis $\{R, S\}$ is given by

$$\mathrm{slope}(\ell_K) = -\frac{h(S + P_K)}{h(R + P_K)}$$

where $h = h_{K_\infty/K}$ is the quadratic function $h(P) = \langle P, P \rangle_{\mathrm{anti-cycl}}$ on $E(K)$.

Some numerical experiments. We are grateful to William Stein for providing us with the following data. Stein works with the prime $p = 3$ and performs two types of numerical experiment. The first experiment is to test whether or not the 3-anti-cyclotomic height pairing is not identically zero (and hence whether or not the Sign Conjecture is true) for optimal curves E of Mordell-Weil rank 2 of small conductor, and for the quadratic imaginary field K of smallest discriminant in $\mathcal{K}_E$. This Stein did for the elliptic curves labelled

389A, 433A,446D, 571B, 643A, 655A, 664A, 707A, 718B, 794A, 817A

in [Cr]. In all these instances, the height pairing is indeed not identically zero. We also expect that the lines ℓ_K (for $K \in \mathcal{K}_E$) generate the $\mathbf{Q}_p$-vector space $E(\mathbf{Q}) \otimes \mathbf{Q}_p$, and further that it is never the case that $\ell_K = \ell_{K'}$ for different fields K, K'. To test this, Stein computed the slopes of $\ell_K \pmod 9$ (and mod 27, when necessary) for certain selected curves E and various $K \in \mathcal{K}_E$. In particular

- for $E = 389\mathrm{A}$ the first 6 $K \in \mathcal{K}_E$ have the property that the ℓ_K are distinct, with slopes (mod 9) equal to $4, 4, 4, 0, 7, 4$,
- for $E = 433\mathrm{A}$ the first 4 $K \in \mathcal{K}_E$ have the property that the ℓ_K are distinct, with slopes (mod 9) equal to $2, 1, 6, \infty$,
- for $E = 571\mathrm{B}$ the first 4 $K \in \mathcal{K}_E$ have the property that the ℓ_K are distinct, with slopes (mod 9) all equal to 6.

Remark 4.13. If the anti-cyclotomic height pairing is *not* identically zero, then computing it modulo some sufficiently high power of p will detect its nontriviality. Unfortunately, at present, we know of no recipe for an a priori upper bound on how high a power of p one must check, before being able to conclude with certainty that the height pairing is trivial. In other words, if the Sign Conjecture were to fail in some example, it seems difficult to formulate a numerical experiment that would prove this failure.

Appendix

A.1 Semi-linear Λ-modules

Suppose $\mathcal{G}$ is a profinite group with a normal subgroup of finite index $\Gamma \cong \mathbf{Z}_p^d$ for some natural number d. This is the situation discussed earlier in the paper, with $\mathcal{G} = \mathrm{Gal}(L/\mathbf{Q})$ and $\Gamma = \mathrm{Gal}(L/K)$. We let $\Delta = \mathcal{G}/\Gamma$ and we assume further that the order of Δ is prime to p.
Let $\Lambda = \mathbf{Z}_p[[\Gamma]]$. Then Δ acts on both Γ and Λ, and $\mathcal{G}$ is noncanonically isomorphic to the the semidirect product of Δ and Γ. We fix such a semidirect product decomposition.

Definition A.14. A $\mathbf{Z}_p[[\mathcal{G}]]$-module M is a Λ module with a *semi-linear* action of Δ in the following sense:

$$\delta(\lambda \cdot m) = \lambda^\delta \cdot \delta(m)$$

for all $\delta \in \Delta, \lambda \in \Lambda, m \in M$. We will call such a module a Δ-*semi-linear* Λ-*module*, or simply a semi-linear Λ-module if the group Δ and its action on Λ are understood.

Given a semi-linear Λ-module M define $M_\Gamma := M \otimes_\Lambda \mathbf{Z}_p$, and note that the semi-linear Δ-action on M induces a $\mathbf{Z}_p$-linear action of Δ on M_Γ. We can also produce semi-linear Λ-modules by "inverting" this procedure. Namely, if N is a $\mathbf{Z}_p[\Delta]$-module, then $M = N \otimes_{\mathbf{Z}_p} \Lambda$ (with the natural "diagonal" action of Δ) is a semi-linear Λ-module and $M_\Gamma = N$. We say that a semi-linear Λ-module M is *split* if $M \cong N \otimes_{\mathbf{Z}_p} \Lambda$ for some $\mathbf{Z}_p[\Delta]$-module N. Clearly a split semi-linear Λ-module M is determined, up to isomorphism, by the $\mathbf{Z}_p[\Delta]$-module M_Γ.

LEMMA A.15. *If M is a semi-linear Λ-module that is free of finite rank over Λ, then M is split.*

Proof. For every subgroup H of finite index in Γ that is stable under Δ, the projection $M \otimes_\Lambda \mathbf{Z}_p[\Gamma/H] \twoheadrightarrow M_\Gamma$ of finite-type $\mathbf{Z}_p[\Delta]$-modules admits a section because $\mathbf{Z}_p[\Delta]$ is semisimple. It follows by a compactness argument that $M \twoheadrightarrow M_\Gamma$ admits a $\mathbf{Z}_p[\Delta]$-section $\iota : M_\Gamma \hookrightarrow M$, and it is straightforward to verify that $M = \iota(M_\Gamma) \otimes \Lambda$. □

DEFINITION A.16. Suppose that M is a semi-linear Λ-module. If $M \otimes \mathbf{Q}_p$ is free of rank one over $\Lambda \otimes \mathbf{Q}_p$, we define the *sign* $\mathrm{sign}(M)$ to be the character

$$\chi_M : \Delta \to \mathrm{Aut}(M_\Gamma \otimes \mathbf{Q}_p) \cong \mathbf{Q}_p^\times.$$

By Lemma A.15, if M is free of rank one over Λ then $\mathrm{sign}(M)$ determines M up to isomorphism.

If Δ has order two (which is the case of most interest in this paper), and τ is the nontrivial element of Δ, we will also call $\chi_M(\tau) = \pm 1$ the sign of M.

Let I denote the augmentation ideal of Λ, the kernel of the natural map $\Lambda \twoheadrightarrow \mathbf{Z}_p$.

PROPOSITION A.17. *Suppose that $\Gamma \cong \mathbf{Z}_p$, and let $\psi : \Delta \to \mathrm{Aut}(\Gamma) \cong \mathbf{Z}_p^\times$ be the character giving the action of Δ on Γ. Suppose $N \subset M$ are semi-linear Λ-modules, and $N \otimes \mathbf{Q}_p$, $M \otimes \mathbf{Q}_p$ are free of rank one over $\Lambda \otimes \mathbf{Q}_p$. Then there is an $\mathcal{L} \in \Lambda$ such that $N \otimes \mathbf{Q}_p = \mathcal{L} M \otimes \mathbf{Q}_p$, and for every such $\mathcal{L}$*

(i) $\mathrm{sign}(N) = \psi^{\lambda(\mathcal{L})}\mathrm{sign}(M)$, *where* $\lambda(\mathcal{L}) = \dim_{\mathbf{Q}_p}(M/N \otimes \mathbf{Q}_p)$ *is the λ-invariant of $\mathcal{L}$,*

(ii) $\mathrm{sign}(N) = \psi^r \mathrm{sign}(M)$, *where $r = \mathrm{ord}_I(\mathcal{L})$ is maximal such that $\mathcal{L} \in I^r$.*

Proof. The existence of such an $\mathcal{L} \in \Lambda$ is clear. Further, replacing M and N by their double duals $\mathrm{Hom}(\mathrm{Hom}(M, \Lambda), \Lambda)$ and $\mathrm{Hom}(\mathrm{Hom}(N, \Lambda), \Lambda)$, we may assume that M and N are both free of rank one over Λ and that $N = \mathcal{L} M$.

The natural isomorphism $\Gamma \xrightarrow{\sim} I/I^2$ by $\gamma \mapsto \gamma - 1$ is Δ-equivariant, so Δ acts on I/I^2 via ψ. Hence $\mathrm{sign}(IM)$, the character giving the action of Δ on $(IM)_\Gamma = (IM) \otimes_\Lambda \mathbf{Z}_p = M_\Gamma \otimes I/I^2$, is $\psi \cdot \mathrm{sign}(M)$ and by induction

$$\mathrm{sign}(I^r M) = \psi^r \mathrm{sign}(M) \tag{5}$$

for every $r \geq 0$.
Identify Λ with a power series ring $\mathbf{Z}_p[[T]]$, so that $I = T\mathbf{Z}_p[[T]]$. The Weierstrass Preparation Theorem shows that $\mathcal{L} = p^\mu T^r g(T)$, where g is a distinguished polynomial of degree $\lambda(\mathcal{L}) - r$ and $g(0) \neq 0$. Since $\mathrm{sign}(M) = \mathrm{sign}(pM)$, we may suppose that $\mu = 0$.
Write $\bar{M} = M/pM$ and $\bar{N} = N/pN$. Then we have $\bar{N} = I^{\lambda(\mathcal{L})}\bar{M}$. Using (5) we see that $\mathrm{sign}(N) \equiv \psi^{\lambda(\mathcal{L})}\mathrm{sign}(M) \pmod{p}$. Since $\mathrm{sign}(N)$ is a character of order prime to p, this proves (i).
To prove (ii), thanks to (5) it is enough to consider the case $r = 0$, i.e., $N = g(T)M$ with $g(0) \neq 0$. In that case

$$N_\Gamma = N \otimes_\Lambda \mathbf{Z}_p = g(0)(M \otimes_\Lambda \mathbf{Z}_p) = g(0)M_\Gamma$$

so $\mathrm{sign}(N) = \mathrm{sign}(M)$ as desired. $\square$

A.2 Universal norms and growth of ranks in Iwasawa modules.

In this appendix Γ will denote a topological pro-p-group written multiplicatively and isomorphic to $\mathbf{Z}_p$, and Γ_n is the unique open subgroup in Γ of index p^n. If $\gamma \in \Gamma$ is a topological generator, then γ^{p^n} is a topological generator of Γ_n. Put $\Lambda := \mathbf{Z}_p[[\Gamma]]$ and for each $n \geq 0$, $\Lambda_n := \mathbf{Z}_p[\Gamma/\Gamma_n] = \mathbf{Z}_p[\gamma]/(\gamma^{p^n} - 1)$. We have $\Lambda_n = \Lambda/(\gamma^{p^n} - 1)\Lambda$, and $\Lambda = \varprojlim \Lambda_n$. IF $n \geq M$ there are natural Λ-module homomorphisms

- the canonical surjection $\pi_{n,m} : \Lambda_n \to \Lambda_m$,
- an injection $\nu_{n,m} : \Lambda_m \to \Lambda_n$, given by multiplication by

$$\frac{\gamma^{p^n} - 1}{\gamma^{p^m} - 1} = \sum_{i=0}^{p^{n-m}-1} \gamma^{ip^m} \in \Lambda$$

  which takes cosets of $(\gamma^{p^m} - 1)\Lambda$ to cosets of $(\gamma^{p^n} - 1)\Lambda$,

and $\pi_{n,m} \circ \nu_{n,m} = p^{n-m}$.
Suppose M is a module of finite type over Λ. Put

$$M_n := M \otimes_\Lambda \Lambda_n = M/(\gamma^{p^n} - 1)M,$$

and let $\mathrm{rank}_{\mathbf{Z}_p}(M_n) = \dim_{\mathbf{Q}_p}(M_n \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)$, the the $\mathbf{Z}_p$-rank of M_n. Then the structure theory of Λ-modules shows that

$$\mathrm{rank}_{\mathbf{Z}_p}(M_n) = rp^n + \epsilon_n$$

where the error term ϵ_n is non-negative, monotone non-decreasing with n, and bounded (i.e., there is an $n_0 \in \mathbf{Z}^+$ such that if $n \geq n_0$ then $\epsilon_n = \epsilon_{n_0}$).

Definition A.18. Put

$$M_n^* := \mathrm{Hom}_{\mathbf{Z}_p}(M_n, \mathbf{Z}_p).$$

If $n \geq m$ the map $1 \otimes \nu_{m,n} : M_m \to M_n$ induces a map $\nu_{m,n}^* : M_n^* \to M_m^*$. The *universal norm Λ-module attached to M* is the projective limit

$$\mathcal{U}(M) := \varprojlim_{0} n M_n^*$$

with respect to the maps $\nu_{n,m}^*$, with its natural Λ-module structure.

Lemma A.19. *There are canonical horizontal isomorphisms making the following diagram commute*

$$\begin{array}{ccc} M_n^* & \xrightarrow{\sim} & \mathrm{Hom}_{\Lambda_n}(M_n, \Lambda_n) \\ {\scriptstyle \nu_{m,n}^*}\downarrow & & \downarrow \\ M_m^* & \xrightarrow{\sim} & \mathrm{Hom}_{\Lambda_m}(M_m, \Lambda_m) \end{array}$$

where the right-hand map is induced by the isomorphism $M_m = M_n \otimes_\Lambda \Lambda_m$.

Proof. Define $p_1 : \Lambda_n \to \mathbf{Z}_p$ by $p_1(\sum_{i=0}^{p^n-1} a_i \gamma^i) = a_0$. It is straightforward to check that composition with p_1 induces a Λ_n-module isomorphism $\mathrm{Hom}_{\Lambda_n}(M_n, \Lambda_n) \xrightarrow{\sim} \mathrm{Hom}(M_n, \mathbf{Z}_p)$ (see for example [Br] Proposition VI.3.4), and that with these isomorphisms the diagram of the lemma commutes. □

The Λ-*dual* of M is $M^\bullet := \mathrm{Hom}_\Lambda(M, \Lambda)$, which is a free Λ-module (of finite rank). The Λ-rank of M is

$$\mathrm{rank}_\Lambda(M) := \dim_{\mathcal{K}}(M \otimes \mathcal{K})$$

where $\mathcal{K}$ is the field of fractions of Λ. Equivalently, the Λ-rank of M is the rank of the free module $M^\bullet$.

Proposition A.20. *Suppose M is a finitely generated Λ-module. Then $\mathcal{U}(M) \cong M^\bullet$, so in particular $\mathcal{U}(M)$ is free over Λ of rank $\mathrm{rank}_\Lambda(M)$.*

Proof. Clearly $M^\bullet \cong \varprojlim \mathrm{Hom}_{\Lambda_n}(M_n, \Lambda_n)$. Thus by Lemma A.19 we have an isomorphism

$$\mathcal{U}(M) \xrightarrow{\sim} M^\bullet$$

and the proposition follows. □

Proposition A.21. *Suppose M is a finitely generated Λ-module. Then the projection map $\mathcal{U}(M) \to M_n^*$ factors through an injective map $\mathcal{U}(M) \otimes \Lambda_n \hookrightarrow M_n^*$. In particular $\cap_{m>n} \nu_{m,n}^*(M_m^*)$ is a free Λ_n-submodule of M_n^* of rank equal to* $\mathrm{rank}_\Lambda(M)$.

Proof. Using the identification $\mathcal{U}(M) \cong M^\bullet$ of Proposition A.20, and the identification $M_n^* \cong \mathrm{Hom}_\Lambda(M_n, \Lambda_n) = \mathrm{Hom}_\Lambda(M, \Lambda_n)$ of Lemma A.19, the projection map $\mathcal{U}(M) \to M_n^*$ is identified with the natural composition

$$\mathrm{Hom}_\Lambda(M, \Lambda) \longrightarrow \mathrm{Hom}_\Lambda(M, \Lambda) \otimes \Lambda_n \xrightarrow{\beta_n} \mathrm{Hom}_\Lambda(M, \Lambda_n). \tag{6}$$

We need to show that the map β_n is injective.

Let $r = \mathrm{rank}_\Lambda(M)$. By Proposition A.20, $\mathrm{Hom}_\Lambda(M, \Lambda) \otimes \Lambda_n$ is a free $\mathbf{Z}_p$-module of rank rp^n, so to prove the injectivity of β_n it will suffice to show that the image of the composition (6) contains a $\mathbf{Z}_p$-module of rank rp^n.

Fix a free Λ-module N of rank r and a map $M \to N$ with finite cokernel (for example, we can take N to be the double dual $M^{\bullet\bullet}$, with the canonical map). We have a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_\Lambda(M, \Lambda) \arrow[r] & \mathrm{Hom}_\Lambda(M, \Lambda_n) \\
\mathrm{Hom}_\Lambda(N, \Lambda) \arrow[r, two heads] \arrow[u, hook] & \mathrm{Hom}_\Lambda(N, \Lambda_n) \arrow[u, hook]
\end{tikzcd}$$

The vertical maps are injective because Λ and Λ_n have no p-torsion, and the bottom map is surjective because N is free. Since $\mathrm{Hom}_\Lambda(N, \Lambda_n)$ is free of rank rp^n over $\mathbf{Z}_p$, this proves that β_n is injective.

By definition the image of $\mathcal{U}(M) \otimes \Lambda_n \hookrightarrow M_n^*$ is $\cap_{m>n} \nu_{m,n}^*(M_m^*)$, and since $\mathcal{U}(M)$ is free of rank r over Λ, this module is free of rank r over Λ_n $\square$

References

[BD1] M. Bertolini, H. Darmon, Derived p-adic heights, *Duke Math. J.* 117 (1995) 1517–1554.

[BD2] ———, Heegner points on Mumford-Tate curves, *Invent. math.* 126 (1996) 413–456.

[Br] K. Brown, Cohomology of groups, *Grad. Texts in Math.* 87, Springer, New York (1982).

[Bu] W. Burnside, Theory of groups of finite order (second edition), Cambridge University Press, Cambridge (1911).

[CH] J. Coates, S. Howson, Euler Characteristics and Elliptic Curves II, J. Math. Soc. Japan, 53 (2001) 175–235.

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

[Cr] J. Cremona, Algorithms for modular elliptic curves, Second edition. Cambridge: Cambridge University Press (1997).

[D] P. Deligne, Les constantes des équations fonctionelles des fonctions L. In: Modular Functions of One Variable II, *Lect. Notes in Math.* 349, Springer, New York (1973) 501–595.

[F] F. G. Frobenius, Über auflösbare Gruppen II, *Sitzungsbericht der Königlich Preußischen Akademie der Wissenshaften zu Berlin* (1895) 1027–1044.

[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. To appear.

[Gr] B. Gross, Heegner points on $X_0(N)$. In: Modular forms (Durham, 1983), Horwood, Chichester (1984) 87–105.

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

[M1] B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* 18 (1972) 183–266.

[M2] ———, Modular curves and arithmetic, in: *Proceedings of the International Congress of Mathematicians (Warsaw, 1983)*, PWN, Warsaw (1984) 185–211.

[MT] B. Mazur, J. Tate, Canonical height pairings via biextensions. In: *Arithmetic and Geometry*, Progr. Math. 35, Birkhaüser, Boston (1983) 195–237.

[Mo] P. Monsky, On p-adic power series, *Math. Ann.* 255 (1981) 217–227.

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

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

[Ru] K. Rubin, Euler systems and modular elliptic curves, in: Galois representations in arithmetic algebraic geometry, A. J. Scholl and R. L. Taylor, eds., *London Math. Soc. Lect. Notes* 254 Cambridge Univ. Press, Cambridge (1998) 351–367.

[Sc] A. Scholl, An introduction to Kato's Euler systems, in: Galois representations in arithmetic algebraic geometry, A. J. Scholl and R. L. Taylor, eds., *London Math. Soc. Lect. Notes* 254 Cambridge Univ. Press, Cambridge (1998) 379–460.

[Se] J-P. Serre, Représentations linéaires des groupes finis. Hermann, Paris (1971).

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

Barry Mazur
Department of Mathematics
Harvard University
Cambridge MA 02138 USA
mazur@math.harvard.edu

Karl Rubin
Department of Mathematics
Stanford University
Stanford CA 94305 USA
rubin@math.stanford.edu