ON THE LOCAL DIVISIBILITY OF HEEGNER POINTS

BENEDICT H. GROSS
JAMES A. PARSON

1. Introduction

Heegner points on the modular curve $X_0(N)$, and their images on elliptic curve factors E of the Jacobian, enjoy many remarkable properties. These points are the moduli of level structures with endomorphisms by the ring of integers of an imaginary quadratic field K. Their traces to $E(K)$ have height given by the first derivative at $s = 1$ of the L-function of E over K (cf. [GZ86]), and their ℓ-divisibility in the Mordell-Weil group controls the first ℓ-descent on E over K (cf. [Gro]).

In this note, we show how their ℓ-divisibility in the local group $E(K_p)$, where p is a prime that is inert in K, often determines a first descent over K on a related abelian variety A over $\mathbb{Q}$. The abelian variety A is associated to a modular form of weight 2 and level Np that is obtained by Ribet's level-raising theorem from the modular form of level N associated to E. This descent result is Theorem 2 below. To prove the descent theorem, we compare the local conditions defining a certain Selmer group for A with those defining the ℓ-Selmer group for E. The conditions agree at places of K prime to p, and at p the condition changes from the unramified local condition to a transverse condition. The parity lemma proved in §5.3 then compares the ranks of the corresponding Selmer groups in terms of the ℓ-divisibility of P in $E(K_p)$ and allows us to understand a first descent on A/K based on Kolyvagin's determination of the first ℓ-descent on E/K.

Some related work on the Selmer group can be found in [BD99, Prop 1.5] and [BD05]; a comparison with the value of the L-function at $s = 1$ is given in [BD99, Thm 1.3].

2. The main theorem

2.1. **Heegner points and Kolyvagin's descent.** Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. It is now known that E is modular (cf. [BCDT01]): the L-function $L(s, E) = \sum_{n\geq 1} a_n n^{-s}$ of E over $\mathbb{Q}$ is the Mellin transform of a modular form $f(\tau) = \sum_{n\geq 1} a_n e^{2\pi i n\tau}$ of weight 2 on $\Gamma_0(N)$. Together with the isogeny theorem of [Fal83], this implies that there is a dominant morphism

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

over $\mathbb{Q}$, where $X_0(N)$ is the modular curve classifying elliptic curves with a cyclic N-isogeny (cf. [BSD75]). We will assume π has minimal degree, and that it maps the cusp ∞ to the origin of E. Then π is determined up to sign.

Let K be an imaginary quadratic field where all primes dividing N are split, and choose a factorization $(N) = \mathfrak{n} \cdot \overline{\mathfrak{n}}$ with $\gcd(\mathfrak{n}, \overline{\mathfrak{n}}) = 1$ in the ideals of the ring of integers $\mathcal{O}_K$ of K. The isogeny of complex elliptic curves $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathfrak{n}^{-1}$ defines a point $x \in X_0(N)(\mathbb{C})$. By the theory of complex multiplication, x is defined over the Hilbert class field H of K. We define

$$P = \mathrm{Tr}_{H/K}\, \pi(x) \qquad \text{in } E(K).$$

Then P is defined up to sign by E and K. For these facts and a general introduction to Heegner points, see [Gro84].

We will assume, in the rest of this paper, that P has infinite order in $E(K)$. By the main result in [GZ86], this condition holds precisely when $L'(1, E/K) \neq 0$. Since $E(K)$ is finitely generated, P can be divisible only by a finite number of primes ℓ in $E(K)$. Kolyvagin showed that the group $E(K)$ has rank 1, and he completed the first ℓ-descent at the primes that do not divide P. More precisely, assume that

a: ℓ is an odd prime that does not divide P in $E(K)$,
b: the Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[\ell](\overline{\mathbb{Q}}))$$

is surjective.

Recall that the ℓ-Selmer group $\mathrm{Sel}(E/K, \ell)$ is the subgroup of classes in $\mathrm{H}^1(K, E[\ell])$ consisting of classes c whose local restrictions $c_v \in \mathrm{H}^1(K_v, E[\ell])$ lie in the images of the local Kummer maps $E(K_v) \to \mathrm{H}^1(K_v, E[\ell])$. Kolyvagin showed the following:

Theorem 1. *Assume that P has infinite order in $E(K)$ and that conditions a) and b) hold. Then the ℓ-Selmer group $\mathrm{Sel}(E/K, \ell)$ has dimension 1 over $\mathbb{Z}/\ell\mathbb{Z}$, and it is generated by the image of $P \in E(K)$ under the global Kummer map $E(K) \to \mathrm{H}^1(K, E[\ell])$.*

A proof is given in [Gro].

2.2. **Level-raising and local divisibility of P.** Now let $p \neq \ell$ be a prime that is inert in K. Then p does not divide N. Under the conditions of Theorem 1, we will consider the local divisibility of P by ℓ in $E(K_p)$. The following observation motivates the analysis below:

Lemma 1. *If the Heegner point P is not divisible by ℓ in $E(K_p)$, then*

c: $a_p \equiv \pm(p+1) \pmod{\ell}$.

More precisely, the sign in c) can be taken to be $-\epsilon$, where ϵ is the sign of the functional equation of $L(s, f)$.

Proof. Since P is not divisible by ℓ in $E(K_p)$, it has non-zero image in $E(K_p)/\ell E(K_p)$. As p does not divide $N\ell$, the latter group is isomorphic to $\mathcal{E}(\mathbb{F}_{p^2})/\ell\mathcal{E}(\mathbb{F}_{p^2})$, where $\mathcal{O}_p$ is the ring of integers of K_p and $\mathcal{E}/\mathcal{O}_p$ is the Néron model. Since $\mathcal{E}(\mathbb{F}_{p^2})$ is a finite group, the elliptic curve $\mathcal{E}/\mathbb{F}_{p^2}$ has a rational ℓ-torsion point. Therefore, Frob_p^2 acts on $E[\ell](\overline{\mathbb{Q}})$ with eigenvalues $(1, p^2)$. Since the determinant of Frob_p on $E[\ell](\overline{\mathbb{Q}})$ is p, its eigenvalues on $E[\ell](\overline{\mathbb{Q}})$ are $(\pm 1, \pm p)$. As the trace of Frob_p on $E[\ell](\overline{\mathbb{Q}})$ is equal to a_p modulo ℓ, this completes the proof of c).

The more precise statement about the sign follows from the formula

$$\overline{P} = -\epsilon P + t,$$

where $t \in E(\mathbb{Q})$ is a torsion point (cf. [Gro84]): by assumption b), the order of t is prime to ℓ, and so the image of P in $E(K_p)/\ell E(K_p)$ satisfies $\mathrm{Frod}_p(P) = -\epsilon P$. Consequently, $\mathcal{E}/\mathbb{F}_{p^2}$ has a rational ℓ-torsion point in the $-\epsilon$ eigenspace for Frob_p, and the eigenvalues of Frob_p are $-\epsilon$ and $-\epsilon p$. □

From now on, we assume that condition c) holds, which is automatic when P is not divisible by ℓ in $E(K_p)$ by the lemma. Conditions b) and c) are the hypotheses of the level-raising Theorem 1 of [Rib90]. This theorem produces a normalized newform g of level dividing Np that is p-new and that has trivial Nebentypus character. The theorem also constructs a place λ of $\overline{\mathbb{Q}}$ over ℓ, and g and λ have the property that for all rational primes $q \neq p$, one has

$$a_q(f) \equiv a_q(g) \pmod{\lambda}. \tag{2.1}$$

2.3. **The Eichler-Shimura construction.** Let $h \in S_2(\Gamma_0(M), \mathbb{C})$ be a normalized newform, and let $F = \mathbb{Q}(h)$ be the subfield of $\mathbb{C}$ generated by its Hecke eigenvalues. The Eichler-Shimura construction associates to h a pair (A, i), where A is an abelian variety up to isogeny over $\mathbb{Q}$ of dimension $[F : \mathbb{Q}]$, and where $i : F \to \mathrm{End}^0(A)$ is an isogeny action of F on A that is defined over $\mathbb{Q}$.

Recall the construction: corresponding to the newform h, one has an algebra homomorphism $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T} \to F$, where $\mathbb{T}$ is the Hecke algebra at level M. The object (A, i) is $\mathrm{Hom}_{\mathbb{Q}\otimes\mathbb{T}}(F, J_0(M))$, suitably interpreted, where $J_0(M)$ is considered as an abelian variety over $\mathbb{Q}$ up to isogeny with action of $\mathbb{Q} \otimes \mathbb{T}$ as endomorphisms. Since $J_0(M)$ has good reduction at finite places of $\mathbb{Q}$ not dividing M, so does A. Let ω be a finite place of F over the place w of $\mathbb{Q}$. The ω-adic Tate module $V_\omega(A, i) = F_\omega \otimes_{\mathbb{Q}_w} V_w(A)$ is a 2-dimensional vector space over F_ω, which admits an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that is unramified away from M and w. The Eichler-Shimura relation implies that for any finite place v of $\mathbb{Q}$ prime to M and w, the characteristic polynomial of (arithmetic) Frobenius at v acting on $V_\omega(A, i)$ is $T^2 - a_v(h)T + q_v$, where the Hecke eigenvalue $a_v(h)$ is considered as an element of $\mathbb{Q}(h) = F \subset F_\omega$.

2.4. **The theorem.** Let (A, i) be the object associated by the Eichler-Shimura construction to the newform g provided by Ribet's level-raising theorem. There is an abelian variety over $\mathbb{Q}$ in the isogeny class A such that the maximal order $R \subset F = \mathbb{Q}(g)$ acts on A compatibly with i (cf. [Shi98], §7.1, Proposition 7). We fix one such abelian variety in the isogeny class, and we write (A, i) for it as well. Many constructions below depend on the action $i : R \to \mathrm{End}(A)$, but since it is fixed throughout, we will generally omit it from the notation.

Let I be the maximal ideal of R induced by the finite place λ of $\overline{\mathbb{Q}}$ provided by Ribet's theorem. The main result below compares the first I-descent on A/K with the first ℓ-descent on E/K. The I-descent structures on A are very similar to the ℓ-descent structures on an elliptic curve. Since I need not be principal, however, one must often tensor with powers of the R-modules I and I^{-1} to define maps whose ℓ-descent analogues would involve multiplying by powers of the generator ℓ of $(\ell) \subset \mathbb{Z}$. For example, for an R-module M, the R-linear analogue of the multiplication-by-ℓ endomorphism is the homomorphism $I \otimes_R M \to M$: if I is principal, then the choice of a generator x, which can also be viewed as an isomorphism $x : R \to I$, converts $I \otimes_R M \to M$ into the endomorphism of multiplication by x on M.

To complete the first I-descent, we define an I-Selmer group of A/K as follows: let $I^{-1} \otimes_R A$ be the K-scheme that represents the functor $T \mapsto I^{-1} \otimes_R A(T) = \mathrm{Hom}_R(I, A(T))$. We show that this functor is representable, and we give more details on the abstract formalism of I-descent, in the appendix below. Then $I^{-1} \otimes_R A$ is an abelian variety of the same dimension as A/K, on which R acts as endomorphisms. For example, if $A(\mathbb{C}) = \mathbb{C}^{[F:\mathbb{Q}]}/\Lambda$, then the lattice Λ has a natural R-module structure, and $I^{-1} \otimes_R A(\mathbb{C}) = \mathbb{C}^{[F:\mathbb{Q}]}/I^{-1} \otimes_R \Lambda$. (The embedding of

$I^{-1} \otimes_R \Lambda$ as a lattice in $\mathbb{C}^{[F:\mathbb{Q}]}$ is the unique extension of the embedding of its finite-index subgroup Λ.)

The inclusion $R \to I^{-1}$ induces an isogeny $A \to I^{-1} \otimes_R A$ defined over K with kernel $A[I]$, the group scheme of I-torsion sections of A. We thus have the exact sequence

$$0 \longrightarrow A[I] \longrightarrow A \longrightarrow I^{-1} \otimes_R A \longrightarrow 0$$

of group schemes over $\operatorname{Spec}(K)$. Passing to Galois cohomology, we find a global Kummer (boundary) map

$$I^{-1} \otimes_R A(K) \to \mathrm{H}^1(K, A[I]).$$

In the familiar situation of ℓ-descent, the boundary map $E(K) \to \mathrm{H}^1(K, E[\ell])$ maps a point $x \in E(K)$ to the $E[\ell]$-torsor composed of the points $\{\ell^{-1}x\} \subset E(\overline{K})$. In the I-descent formalism, we would replace $x \in E(K)$ with $(\ell^{-1}) \otimes x \in (\ell)^{-1} \otimes E(K)$. The image of $(\ell^{-1}) \otimes x$ under the Kummer map is the fiber over this point of the isogeny $E \to (\ell)^{-1} \otimes E$.

For each place v of K, there are analogous local Kummer maps

$$I^{-1} \otimes_R A(K_v) \to \mathrm{H}^1(K_v, A[I]).$$

The *I-Selmer group of* (A, i), denoted $\operatorname{Sel}(A/K, I)$, is the group of classes $c \in \mathrm{H}^1(K, A[I])$ such that the restriction $c_v \in \mathrm{H}^1(K_v, A[I])$ is in the image of $I^{-1} \otimes_R A(K_v)$ for all places v of K. Evidently the global Kummer map factors through $\operatorname{Sel}(A/K, I) \subset \mathrm{H}^1(K, A[I])$.

Just as in for standard ℓ-descent, one can show that $\operatorname{Sel}(A/K, I)$ is a finite group and hence a finite-dimensional R/I-vector space. The kernel of the global Kummer map $I^{-1} \otimes_R A(K) \to \operatorname{Sel}(A/K, I)$ is the image of the natural map

$$R \otimes_R A(K) \to I^{-1} \otimes_R A(K),$$

and so the image of the Kummer map is $I^{-1}/R \otimes_R A(K)$ or, equivalently,

$$I^{-1} \otimes_R (R/I \otimes_R A(K)).$$

The R/I-dimension of $\operatorname{Sel}(A/K, I)$ is thus an upper bound on the rank of $A(K)$ as R-module, just as the $\mathbb{Z}/\ell\mathbb{Z}$-dimension of $\operatorname{Sel}(E/K, \ell)$ is an upper bound on the rank of $E(K)$ as $\mathbb{Z}$-module.

Let us impose the following additional assumptions on p, N, and E:

d: ℓ is prime to N,

e: For each prime q dividing N, the dimension of the q-inertia invariants of the modulo-ℓ Galois representation

$$\rho : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut}(E[\ell](\overline{\mathbb{Q}}))$$

is 1, if E has multiplicative reduction at q, and is 0, if E has additive reduction at q,

f: $p^2 \not\equiv 1 \pmod{\ell}$.

Since ℓ is prime to N, condition e) is equivalent to the statement that the conductor of ρ in the sense of [Ser87] is equal to the conductor N of $E/\mathbb{Q}$. By level-lowering theorems (cf. [Dia95]), condition e) means that f is a form of minimal level among those giving rise to the modulo-ℓ representation ρ. It also implies that the form g constructed by level raising has level Np.

We will deduce the following result about the I-descent on A/K from Kolyvagin's result stated in Theorem 1:

Theorem 2. *Assume that $P \in E(K)$ has infinite order and that conditions a)–f) hold. Then*

$\dim_{R/I} \mathrm{Sel}(A/K, I) = 0,$ *if P is not divisible by ℓ in $E(K_p)$, and*

$\dim_{R/I} \mathrm{Sel}(A/K, I) = 2,$ *if P is divisible by ℓ in $E(K_p)$.*

The I-adic Tate module

$$T_I(A, i) = \varprojlim (I^{\otimes n} \otimes_R A[I^n](\overline{\mathbb{Q}}))$$

is a lattice in $V_\lambda(A, i)$ and is thus free of rank 2 over the I-adic completion of R. Therefore, $R/I \otimes_R T_I(A, i) = I \otimes_R A[I](\overline{\mathbb{Q}})$ and hence $A[I](\overline{\mathbb{Q}})$ is 2-dimensional over R/I. By the Eichler-Shimura relation and (2.1), the characteristic polynomials of prime-to-$Np\ell$ Frobenius elements on $R/I \otimes E[\ell](\overline{\mathbb{Q}})$ and $A[I](\overline{\mathbb{Q}})$ agree. Thus, by the Brauer-Nesbitt principle, these Galois modules have isomorphic semi-simplifications. By assumption b), the Galois module $R/I \otimes E[\ell](\overline{\mathbb{Q}})$ is irreducible, and so the two $(R/I)[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-modules are isomorphic. We choose and fix such an isomorphism for the rest of the paper.

The plan for proving Theorem 2 is to compare the local conditions defining $\mathrm{Sel}(A/K, I) \subset \mathrm{H}^1(K, A[I])$ and

$$R/I \otimes \mathrm{Sel}(E/K, \ell) \subset R/I \otimes \mathrm{H}^1(K, E[\ell]) = \mathrm{H}^1(K, R/I \otimes E[\ell]),$$

by means of the fixed isomorphism $R/I \otimes E[\ell]/\mathbb{Q} = A[I]/\mathbb{Q}$. Using assumptions a)–f), we describe these local conditions entirely in terms of the Galois module

$$A[I](\overline{\mathbb{Q}}) = R/I \otimes E[\ell](\overline{\mathbb{Q}}).$$

The local conditions agree at all places v of K except at $v = p$, where the two conditions are transverse. By combining this local analysis with a global parity lemma, proved in §5.3, we deduce Theorem 2 from Theorem 1. In §4 we study the local conditions defining the Selmer groups at places $v \neq p$ of K, and in §5 we study the conditions at

$v = p$ and use the parity lemma to prove the theorem. In §6 below, we make explicit the compatibility with the parity predictions of the conjecture of Birch and Swinnerton-Dyer.

3. Néron models of abelian varieties with real multiplication

This section contains preliminary remarks that will be applied in §§4 and 5 to Néron models of E and A in order to describe the images of the local Kummer maps entirely in terms of the Galois modules underlying $E[\ell]/\mathbb{Q}$ and $A[I]/\mathbb{Q}$.

3.1. **Semi-stable case.** Let L be the quotient field of a Henselian discrete valuation ring $\mathcal{O}_L$ with residue field k_L, and let B/L be an abelian variety. Let F_0 be a number field with maximal order R_0. Assume that the dimension of B/L is $[F_0 : \mathbb{Q}]$. Let $j : R_0 \to \mathrm{End}(B/L)$ be a faithful action of R_0. In what follows, we will use $F_0 = \mathbb{Q}$ and $F_0 = F$.

Let $\mathcal{B}/\mathcal{O}_L$ be the Néron model of B/L. We consider first the case when B/L has semi-stable reduction. This condition means that the identity component $\mathcal{B}^0/k_L$ of the special fiber of the Néron model is an extension of an abelian variety by a torus T/k_L. Let $\overline{k_L}$ be a separable closure of k_L. The torus T/k_L is determined by its geometric character lattice $X^*(T/\overline{k_L})$, which is a free $\mathbb{Z}$-module of rank $\dim(T)$, with the induced action of $\mathrm{Gal}(\overline{k_L}/k_L)$ on this lattice. The semi-stable abelian variety B/L has *good reduction*, if the torus component of the special fiber is trivial. In this case, the special fiber is connected and is an abelian variety, and so $\mathcal{B}/\mathcal{O}_L$ is an abelian scheme. If the abelian-variety component of $\mathcal{B}^0/k_L$ is trivial, then B/L has *purely toric reduction.*

Lemma 2. *If B/L has semi-stable reduction, then B/L has either good reduction or purely toric reduction. In the purely toric-reduction case, the functorial action of R_0 on $X^*(T/\overline{k_L})$ makes this lattice an invertible R_0-module.*

Proof. By functoriality of the Néron model, the action j induces a (unital) ring homomorphism $R_0 \to \mathrm{End}(T/\overline{k_L}) = \mathrm{End}(X^*(T/\overline{k_L}))$. Tensoring with $\mathbb{Q}$, we find an F_0-vector-space structure on $\mathbb{Q} \otimes X^*(T/\overline{k_L})$. Therefore, the dimension of T/k_L is a multiple of $[F_0 : \mathbb{Q}] = \dim(B)$. Since $\dim(T) \leq \dim(B/L) = \dim(\mathcal{B}^0/k_L)$, we see that either $T = 0$ or $T = \mathcal{B}^0/k_L$. In the first case, B/L has good reduction. In the second case, B/L has purely toric reduction, and $X^*(T/\overline{k_L})$ is an R_0-lattice in the 1-dimensional F_0-vector space $\mathbb{Q} \otimes X^*(T/\overline{k_L})$. Thus the character lattice is an invertible R_0-module, since R_0 is the maximal order of F_0. $\square$

Consider the purely-toric reduction case of the lemma. Since T is split over $\overline{k_L}$, we have the natural isomorphism

$$T/\overline{k_L} = \underline{\mathrm{Hom}}(X^*(T/\overline{k_L}), \mathbb{G}_m),$$

which is a functorial expression of the fact that $T/\overline{k_L}$ is isomorphic to a product of copies of the multiplicative group $\mathbb{G}_m$ indexed by any basis of $X^*(T/\overline{k_L})$. Thus for any ideal I_0 of R_0, we have

$$T[I_0]/\overline{k_L} = \underline{\mathrm{Hom}}(X^*(T/\overline{k_L}), \mathbb{G}_m)[I_0] = \underline{\mathrm{Hom}}(R_0/I_0 \otimes_{R_0} X^*(T/\overline{k_L}), \mathbb{G}_m).$$

Therefore, we have

$$T[I_0](\overline{k_L}) = \mathrm{Hom}_{\mathbb{Z}}(R_0/I_0 \otimes_{R_0} X^*(T/\overline{k_L}), \overline{k_L}^{\times}).$$

As an abstract group, $\overline{k_L}^{\times}$ is isomorphic to $\prod_{q \neq q_0} \mathbb{Q}_q/\mathbb{Z}_q$, where q runs over primes not equal to the characteristic q_0 of k_L. Consequently, if I_0 is a maximal ideal such that the order of R_0/I_0 is invertible in k_L, then $T[I_0](\overline{k_L})$ is 1-dimensional over R_0/I_0. We state this fact as a lemma for later reference.

Lemma 3. *Assume that B/L has purely toric reduction. Let I_0 be a maximal ideal of R_0 such that the order of R_0/I_0 is invertible in k_L. Then $\mathcal{B}^0[I_0](\overline{k_L})$ is 1-dimensional over R_0/I_0.*

3.2. **Component groups in the general case.** We now consider abelian varieties B/L with endomorphisms $j : R_0 \to \mathrm{End}(B)$ as above, but we allow arbitrary (not necessarily semi-stable) reduction. Let $\mathcal{B}/\mathcal{O}_L$ be the Néron model of B/L, and let $\mathcal{B}^0/k_L$ be the connected component of the identity of $\mathcal{B}/k_L$. In the general case $\mathcal{B}^0/k_L$ is a successive extension of an abelian variety, a torus, and a connected unipotent group. In this section, we are concerned with the component group scheme $\Phi = \mathcal{B}/\mathcal{B}^0$ of the special fiber. It is a finite, étale R_0-module scheme over k_L. Let $\mathcal{B}^0/\mathcal{O}_L$ be the smooth group scheme whose generic fiber is B/L and whose special fiber is $\mathcal{B}^0/k_L$, i.e. $\mathcal{B}^0/\mathcal{O}_L$ is the complement in $\mathcal{B}/\mathcal{O}_L$ of the non-identity components of $\mathcal{B}/k_L$.

Let $I_0 \subset R_0$ be a maximal ideal such that the order of R_0/I_0 is invertible in $\mathcal{O}_L$ and thus in L and k_L. Let us see how the group $\Phi[I_0](\overline{k_L})$ appears in the Galois module $B[I_0]/L$. Consider the R_0-module extension of $\Phi[I_0](\overline{k_L})$ by $\mathcal{B}^0(\overline{k_L})$ obtained by restricting

$$0 \to \mathcal{B}^0(\overline{k_L}) \to \mathcal{B}(\overline{k_L}) \to \Phi(\overline{k_L}) \to 0$$

to $\Phi[I_0](\overline{k_L})$. We claim that this extension of R_0-modules splits. Since the group $\Phi[I_0](\overline{k_L})$ is a direct sum of copies of R_0/I_0 as R_0-module, it suffices to show that

$$\mathrm{Ext}^1_{R_0}(R_0/I_0, \mathcal{B}^0(\overline{k_L})) = 0. \tag{3.1}$$

To see this vanishing, we consider the homomorphism $\mathcal{B} \to I_0^{-1} \otimes_{R_0} \mathcal{B}$ of smooth group schemes over $\mathcal{O}_L$, as in the formalism of I_0-descent discussed in the appendix. On the relative Lie algebras, this morphism is the natural homomorphism of free $\mathcal{O}_L$-modules

$$\mathrm{Lie}(\mathcal{B}/\mathcal{O}_L) \to \mathrm{Lie}(I_0^{-1} \otimes_{R_0} \mathcal{B}/\mathcal{O}_L) = I_0^{-1} \otimes_{R_0} \mathrm{Lie}(\mathcal{B}/\mathcal{O}_L).$$

The kernel and cokernel are annihilated by I_0; since I_0 contains the order of R_0/I_0, which is a unit in $\mathcal{O}_L$, the map is an isomorphism. Consequently, the homomorphism of smooth group schemes $\mathcal{B} \to I_0^{-1} \otimes_{R_0} \mathcal{B}$ over $\mathcal{O}_L$ is étale. Since the geometric fibers of $\mathcal{B}^0$ and $I_0^{-1} \otimes_{R_0} \mathcal{B}^0$ over $\mathcal{O}_L$ are connected, the homomorphism $\mathcal{B}^0 \to I_0^{-1} \otimes_{R_0} \mathcal{B}^0$ is thus étale and surjective. In particular, $\mathcal{B}^0(\overline{k_L}) \to I_0^{-1} \otimes_{R_0} \mathcal{B}^0(\overline{k_L})$ is surjective.

Consider the projective resolution

$$0 \longrightarrow I_0 \longrightarrow R_0 \longrightarrow R_0/I_0 \longrightarrow 0$$

of the R_0-module R_0/I_0. From the long exact Ext_{R_0}-sequence with coefficients $\mathcal{B}^0(\overline{k_L})$, we find that $\mathrm{Ext}^1_{R_0}(R_0/I_0, \mathcal{B}^0(\overline{k_L}))$ is the cokernel of

$$\mathrm{Hom}_{R_0}(R_0, \mathcal{B}^0(\overline{k_L})) \longrightarrow \mathrm{Hom}_{R_0}(I_0, \mathcal{B}^0(\overline{k_L})).$$

Since the map

$$\mathcal{B}^0(\overline{k_L}) = \mathrm{Hom}_{R_0}(R_0, \mathcal{B}^0(\overline{k_L})) \to \mathrm{Hom}_{R_0}(I_0, \mathcal{B}^0(\overline{k_L})) = I_0^{-1} \otimes_{R_0} \mathcal{B}^0(\overline{k_L})$$

is surjective, we obtain the desired vanishing (3.1).

If we choose a splitting, then we find an R_0/I_0-module isomorphism

$$\mathcal{B}[I_0](\overline{k_L}) = \mathcal{B}^0[I_0](\overline{k_L}) \oplus \Phi[I_0](\overline{k_L}). \tag{3.2}$$

Let $\widetilde{L}$ be a maximal unramified extension of L with residue field $\overline{k}_L$, and let $\mathcal{O}_{\widetilde{L}}$ be the valuation ring of $\widetilde{L}$. By the Néron property, we have $B[I_0](\widetilde{L}) = \mathcal{B}[I_0](\mathcal{O}_{\widetilde{L}})$. Since $\mathcal{B}[I_0]/\mathcal{O}_L$ is étale (as the kernel of an étale homomorphism $\mathcal{B} \to I_0^{-1} \otimes_{R_0} \mathcal{B}$ over $\mathcal{O}_L$) and $\mathcal{O}_L$ is Henselian, the reduction map $\mathcal{B}[I_0](\mathcal{O}_{\widetilde{L}}) \to \mathcal{B}[I_0](\overline{k_L})$ is an isomorphism. Therefore $B[I_0](\widetilde{L}) = \mathcal{B}[I_0](\overline{k_L})$. The R_0/I_0-module $\mathcal{B}[I_0](\widetilde{L})$ is the space of inertia invariants in $\mathcal{B}[I_0](\overline{L})$, where $\overline{L}$ is a separable closure of L containing $\widetilde{L}$. In summary, we have

Lemma 4. *If the order of R_0/I_0 is invertible in $\mathcal{O}_L$, then as R_0/I_0-module, the space of inertia invariants in $B[I_0](\overline{L})$ is $\mathcal{B}^0[I_0](\overline{k_L}) \oplus \Phi[I_0](\overline{k_L})$.*

3.3. **Reduction of E and A at finite places of K.** We now describe some aspects of the reduction of E and A at primes q of $\mathbb{Q}$ and at finite places v of K using the results of this section and hypotheses a)-f). Since N is the conductor of $E/\mathbb{Q}$, if q and v are prime to N, then $E/\mathbb{Q}$ has good reduction at q, and E/K has good reduction at v. Let v be a place of K dividing N and let q be the prime of $\mathbb{Q}$ lying under v. The elliptic curve $E/\mathbb{Q}$ then has either multiplicative or additive reduction at q. Since, by assumption, q is unramified and splits in K, we have $\mathbb{Q}_q = K_v$, and the elliptic curve E/K has the same reduction at v as $E/\mathbb{Q}$ at q. If $E/\mathbb{Q}$ has additive reduction, then by condition e), there are no non-zero inertia invariants in $E[\ell](\overline{\mathbb{Q}_q})$. Thus by Lemma 4, since ℓ is prime to N, the component group of the reduction at q has no ℓ-torsion. If $E/\mathbb{Q}$ has multiplicative reduction at q, then the inertia invariants in $E[\ell](\overline{\mathbb{Q}_q})$ are 1-dimensional over $\mathbb{Z}/\ell\mathbb{Z}$ by assumption e). By Lemma 3 and 4, all of these inertia invariants come from the torus part of the reduction, and the component group of the reduction at q again has no non-zero ℓ-torsion.

If q and v are prime to Np, then the abelian variety $A/\mathbb{Q}$ has good reduction at q, and A/K has good reduction at v, since $A/\mathbb{Q}$ is an isogeny factor of $J_0(Np)/\mathbb{Q}$, which has good reduction away from Np. It follows from the construction of the semi-stable model of $J_0(Np)/\mathbb{Q}_p$ over $\mathbb{Z}_p$ (cf. [DR73]) that the new quotient of $J_0(Np)/\mathbb{Q}$ has purely toric reduction at p. Since the eigenform g used to construct $A/\mathbb{Q}$ is new at p, the abelian variety $A/\mathbb{Q}$ thus has purely toric reduction at p. Therefore, A/K has purely toric reduction at places v of K dividing p.

By condition e), the Galois module $E[\ell](\overline{\mathbb{Q}})$ is ramified at primes q dividing N. Since $R/I \otimes E[\ell](\overline{\mathbb{Q}}) = A[I](\overline{\mathbb{Q}})$ as Galois modules, the Galois module $A[I](\overline{\mathbb{Q}})$ is also ramified at primes q dividing N. Therefore, $A/\mathbb{Q}_q$ has bad reduction at all primes q dividing N. As above, if v is a place of K dividing N and lying over the rational prime q, then q is unramified and split in K. Therefore $K_v = \mathbb{Q}_q$, and so the reduction of A/K at v is the same as the reduction of $A/\mathbb{Q}$ at q. If q divides N but q^2 does not divide N, then $A/\mathbb{Q}$ has semi-stable reduction at q (and hence v), since it is an isogeny factor of $J_0(Np)/\mathbb{Q}$, which has semi-stable reduction at q. Since $A/\mathbb{Q}$ has bad reduction at q, it has purely toric reduction by Lemma 2. The inertia invariants in $A[I](\overline{\mathbb{Q}_q})$ are 1-dimensional over R/I by assumption e) and the isomorphism $R/I \otimes E[\ell](\overline{\mathbb{Q}}) = A[I](\overline{\mathbb{Q}})$. Therefore, by Lemmas 3 and 4, the component group of the reduction of $A/\mathbb{Q}$ at q has no I-torsion. On the other hand, if q^2 divides N, then $E/\mathbb{Q}$ has additive reduction at q, the inertia invariants in $A[I](\overline{\mathbb{Q}_q})$ are 0-dimensional over R/I by assumption e) and the isomorphism $R/I \otimes E[\ell](\overline{\mathbb{Q}}) = A[I](\overline{\mathbb{Q}})$. Therefore, by Lemma 4, the component group of the reduction of $A/\mathbb{Q}$ at q has no I-torsion.

4. Proof of Theorem 2: local conditions at $v \neq p$

To prove Theorem 2, we will compare

$$R/I \otimes \mathrm{Sel}(E/K, \ell) \subset R/I \otimes \mathrm{H}^1(K, E[\ell]) = \mathrm{H}^1(K, R/I \otimes E[\ell])$$

with $\mathrm{Sel}(A/K, I) \subset \mathrm{H}^1(K, A[I])$. Here we identify $\mathrm{H}^1(K, R/I \otimes E[\ell])$ with $\mathrm{H}^1(K, A[I])$ using the fixed isomorphism $R/I \otimes E[\ell] = A[I]$ over $\mathbb{Q}$ from §2.4. We compare these two Selmer groups by comparing the local conditions in $\mathrm{H}^1(K_v, A[I])$ that define them. Let $L_v \subset \mathrm{H}^1(K_v, A[I])$ be the R/I-span of the image of

$$E(K_v) \to \mathrm{H}^1(K_v, E[\ell]) \subset \mathrm{H}^1(K_v, A[I]).$$

Then $R/I \otimes \mathrm{Sel}(E/K, \ell)$ consists of the classes $c \in \mathrm{H}^1(K, A[I])$ such that each restriction $c_v \in \mathrm{H}^1(K_v, A[I])$ belongs to L_v. Let $L'_v \subset \mathrm{H}^1(K_v, A[I])$ be the image of the local Kummer map $I^{-1} \otimes_R A(K_v) \to \mathrm{H}^1(K_v, A[I])$, so that $\mathrm{Sel}(A/K, I)$ is the set of classes $c \in \mathrm{H}^1(K, A[I])$ such that $c_v \in L'_v$ for all places v of K.

The remainder of the present section is devoted to proving

Lemma 5. *For $v \neq p$, we have $L_v = L'_v$.*

We prove the lemma by deducing from assumptions a)–f) descriptions of L_v and L'_v entirely in terms of the Galois modules $E[\ell]/\mathbb{Q}$ and $A[I]/\mathbb{Q}$. The fixed isomorphism $R/I \otimes E[\ell] = A[I]$ over $\mathbb{Q}$ then allows us to identify the local conditions as in the lemma. In §5 below, we complete the local comparison by analyzing L_p and L'_p, which is the only place at which the defining local conditions for the two Selmer groups differ. With the local comparison in hand, we use a parity lemma based on local and global duality theory in Galois cohomology to deduce Theorem 2 from Theorem 1.

4.1. **Types of local conditions.**

Let $\mathcal{O}_L$ be a discrete valuation ring with quotient field L and residue field k_L. Let V be a locally constant constructible sheaf of abelian groups on the small étale site of $\mathrm{Spec}(L)$. The data of V is carried equivalently by the finite-order $\mathbb{Z}[\mathrm{Gal}(\overline{L}/L)]$-module $V(\overline{L})$, where $\overline{L}/L$ is a separable closure.

The subspace of $\mathrm{H}^1(L,V)$ composed of classes that split over an unramified extension of L is denoted $\mathrm{H}^1_{\mathrm{unr}}(L,V)$. Alternatively, if $j : \mathrm{Spec}(L) \to \mathrm{Spec}(\mathcal{O}_L)$ denotes the inclusion, the unramified classes are

$$\mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_L), j_*V) \subset \mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(L), V) = \mathrm{H}^1(L,V).$$

From either description, it is clear that formation of unramified classes is functorial in V.

Suppose that there is a finite, free group scheme $G/\mathrm{Spec}(\mathcal{O}_L)$ whose restriction to $\mathrm{Spec}(L)$ represents V. One then has the subspace of flat classes valued in $G/\mathcal{O}_L$

$$\mathrm{H}^1_{\text{fl}}(\mathrm{Spec}(\mathcal{O}_L), G) \subset \mathrm{H}^1_{\text{fl}}(\mathrm{Spec}(L), G) = \mathrm{H}^1(L,V).$$

The formation of such a subspace is functorial in the flat model G over $\mathrm{Spec}(\mathcal{O}_L)$.

4.2. **Identifying local conditions for I_0-descent on abelian varieties.** We return briefly to the general notation of §3: $\mathcal{O}_L$ is a Henselian discrete valuation ring with quotient field L and residue field k_L; one has an abelian variety B/L, equipped with an action of the ring of integers R_0 of a number field F_0 such that $[F_0 : \mathbb{Q}] = \dim(B/L)$. Let $\mathcal{B}/\mathcal{O}_L$ be the Néron model, and let Φ/k_L be the component group scheme of $\mathcal{B}/k_L$. Let $I_0 \subset R_0$ be a maximal ideal such that the order of R_0/I_0 is invertible in L. Then the homomorphism $B \to I_0^{-1} \otimes_{R_0} B$ is an étale isogeny with kernel $B[I_0]$, and we have the Kummer map $I_0^{-1} \otimes_{R_0} B(L) \to \mathrm{H}^1(L, B[I_0])$. The following two lemmas identify the image of the Kummer map under certain restrictions on the reduction of B/L. The cases with $R_0 = \mathbb{Z}$ are entirely standard facts (cf. [Maz72], for instance).

Lemma 6. *If the order of R_0/I_0 is invertible in $\mathcal{O}_L$ and $\Phi[I_0] = 0$, then the image of the Kummer map in $\mathrm{H}^1(L, B[I_0])$ is $\mathrm{H}^1_{\mathrm{unr}}(L, B[I_0])$.*

Proof. Since the order of R_0/I_0 is invertible in $\mathcal{O}_L$, as in §3.2, we find that the homomorphism $\mathcal{B} \to I_0^{-1} \otimes_{R_0} \mathcal{B}$ is étale and that $\mathcal{B}^0 \to I_0^{-1} \otimes_{R_0} \mathcal{B}^0$ is surjective and étale. Since $\Phi[I_0] = 0$ and Φ/k_L is finite étale, the natural map $\Phi \to I_0^{-1} \otimes_{R_0} \Phi$ is an isomorphism, and so $\mathcal{B} \to I_0^{-1} \otimes \mathcal{B}$ is surjective and étale. One thus has the Kummer maps for B/L and $\mathcal{B}/\mathcal{O}_L$, as discussed in the appendix, which are connected by restriction maps in étale cohomology:

$$\begin{array}{ccc} I_0^{-1} \otimes_{R_0} \mathcal{B}(\mathcal{O}_L) & \longrightarrow & \mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_L), \mathcal{B}[I_0]) \\ \downarrow & & \downarrow \\ I_0^{-1} \otimes_{R_0} B(L) & \longrightarrow & \mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(L), B[I_0]). \end{array} \tag{4.1}$$

By the Néron mapping property we have $\mathcal{B}(\mathcal{O}_L) = \mathcal{B}(L)$, and so the left vertical arrow in an isomorphism. Furthermore, the top arrow is surjective, which one sees as follows:

The cokernel of the top arrow is the kernel of

$$\mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_L), \mathcal{B}) \longrightarrow \mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_L), I_0^{-1} \otimes_R \mathcal{B}),$$

and so to see surjectivity, it suffices to check that $\mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_L), \mathcal{B}^0) = 0$ and that $\Phi \to I_0^{-1} \otimes_{R_0} \Phi$ is an isomorphism. The second fact follows from $\Phi[I_0] = 0$, as noted above. To see the first fact, recall that a class in $\mathrm{H}^1(\mathrm{Spec}(\mathcal{O}_L), \mathcal{B}^0)$ can be represented by a right torsor under the étale sheaf represented by $\mathcal{B}^0$. Since the base $\mathcal{O}_L$ is a discrete valuation ring and $\mathcal{B}^0$ is smooth over $\mathcal{O}_L$, this torsor is representable by a scheme over $\mathrm{Spec}(\mathcal{O}_L)$ by a theorem of Raynaud (cf. [Mil80], Chapter III, Theorem 4.3). It suffices therefore to show that any scheme $\mathcal{P}$ over $\mathrm{Spec}(\mathcal{O}_L)$ that is a right $\mathcal{B}^0$-torsor has a section. Since $\mathcal{B}^0/k_L$ is connected, Lang's theorem (cf. [Lan56], Theorem 2) implies that $\mathcal{P}(k_L)$ is non-empty. As $\mathcal{B}^0/\mathrm{Spec}(\mathcal{O}_L)$ and hence $\mathcal{P}/\mathrm{Spec}(\mathcal{O}_L)$ are smooth and $\mathcal{O}_L$ is Henselian, the map $\mathcal{P}(\mathcal{O}_L) \to \mathcal{P}(k_L)$ is surjective. Consequently, the element of $\mathcal{P}(k_L)$ provided by Lang's theorem lifts to a section over $\mathcal{O}_L$.

Since the left vertical arrow in (4.1) is an isomorphism and the top arrow is a surjection, the image of the Kummer map in $\mathrm{H}^1(L, B[I_0])$ is $\mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_L), \mathcal{B}[I_0])$. The Néron mapping property identifies $j_*B = \mathcal{B}$ as sheaves on the small étale site of $\mathrm{Spec}(\mathcal{O}_L)$. Thus

$$\mathcal{B}[I_0] = (j_*B)[I_0] = j_*(B[I_0]),$$

and $\mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_L), \mathcal{B}[I_0]) = \mathrm{H}^1_{\text{unr}}(L, B[I_0])$. □

Alternatively, assume that the order of R_0/I_0 is invertible only in L, but consider only B/L with good reduction. The Néron model $\mathcal{B}/\mathcal{O}_L$ is then an abelian scheme.

Lemma 7. *If B/L has good reduction, then $\mathcal{B}[I_0]/\mathcal{O}_L$ is finite and locally free. Furthermore, the image of the Kummer map $I_0^{-1} \otimes_{R_0} B(L) \to \mathrm{H}^1(L, B[I_0])$ is $\mathrm{H}^1_{\text{fl}}(\mathrm{Spec}(\mathcal{O}_L), \mathcal{B}[I_0])$.*

Proof. As explained in the appendix, since $\mathcal{B}/\mathcal{O}_L$ is an abelian scheme, the homomorphism $\mathcal{B} \to I_0^{-1} \otimes_{R_0} \mathcal{B}$ is flat and surjective. Furthermore, the kernel $\mathcal{B}[I_0]/\mathcal{O}_L$ is finite and locally free. To complete the proof othe lemma, one can apply the same argument as in Lemma 6, replacing étale cohomology with flat cohomology. □

4.3. **Proof of Lemma 5.** For v the infinite place of K, we have $K_v = \mathbb{C}$, and so $\mathrm{H}^1(K_v, A[I]) = 0$ and $L_v = L'_v = 0$.

Next consider a finite place v of K prime to $p\ell$. Let $\mathcal{E}/\mathcal{O}_v$ and $\mathcal{A}/\mathcal{O}_v$ be the Néron models of E/K_v and A/K_v, respectively. Let Φ_E and Φ_A be the component group schemes of the special fibers of $\mathcal{E}/\mathcal{O}_v$ and $\mathcal{A}/\mathcal{O}_v$, respectively. By the discussion in §3.3, we have $\Phi_E[\ell] = 0$ and $\Phi_A[I] = 0$. Therefore, Lemma 6 implies that

$$L_v = R/I \otimes \mathrm{H}^1_{\mathrm{unr}}(K_v, E[\ell]) \quad \text{and} \quad L'_v = \mathrm{H}^1_{\mathrm{unr}}(K_v, A[I]).$$

Consequently, $L_v = L'_v$.

Finally, let v be a place of K dividing ℓ. Let $\mathcal{E}/\mathbb{Z}_\ell$ and $\mathcal{A}/\mathbb{Z}_\ell$ be the Néron models of $E/\mathbb{Q}_\ell$ and $A/\mathbb{Q}_\ell$, respectively. Since ℓ is prime to Np, these models are abelian schemes. Furthermore, the base changes $\mathcal{E}/\mathcal{O}_v$ and $\mathcal{A}/\mathcal{O}_v$ are the Néron models of E/K_v and A/K_v, respectively. The R/I-vector schemes $R/I \otimes_{\mathbb{Z}} \mathcal{E}[\ell]/\mathbb{Z}_\ell$ and $\mathcal{A}[I]/\mathbb{Z}_\ell$ are finite, free models of $A[I]/\mathbb{Q}_\ell$. Since $\ell > 2$, by Theorem 3.3.3 of [Ray74], the identification of their generic-fiber Galois modules extends uniquely to an isomorphism $R/I \otimes \mathcal{E}[\ell] = \mathcal{A}[I]$ over $\mathbb{Z}_\ell$. By Lemma 7, we have

$$L_v = R/I \otimes \mathrm{H}^1_{\mathrm{fl}}(\mathrm{Spec}(\mathcal{O}_v), \mathcal{E}[\ell]) \quad \text{and} \quad L'_v = \mathrm{H}^1_{\mathrm{fl}}(\mathrm{Spec}(\mathcal{O}_v), \mathcal{A}[I]).$$

Therefore, $L_v = L'_v$.

5. Proof of Theorem 2: local condition at $v = p$ and the parity lemma

5.1. **The conditions at $v = p$.** The $\mathrm{Gal}(\overline{K_p}/K_p)$-module $E[\ell](\overline{K_p})$ is unramified at p, since p is prime to the conductor N of $E/\mathbb{Q}$. By assumption c), the eigenvalues of Frob_{p^2} on $E[\ell](\overline{K_p})$ are 1 and p^2. By assumption f), we have $p^2 \not\equiv 1 \pmod{\ell}$, and so $E[\ell](\overline{K_p})$ splits as a sum of the Frob_{p^2}-eigenspaces for the eigenvalues 1 and p^2. Therefore, we have an isomorphism of R/I-vector schemes (or $(R/I)[\mathrm{Gal}(\overline{K_p}/K_p)]$-modules):

$$A[I]/K_p = R/I \oplus R/I(1),$$

where $R/I(1)$ is the R/I-vector scheme $R/I \otimes \mu_\ell$.

Lemma 8. *The spaces* $\mathrm{H}^1(K_p, R/I)$ *and* $\mathrm{H}^1(K_p, R/I(1))$ *are each* 1-*dimensional over* R/I. *Furthermore,*

$$L_p = \mathrm{H}^1(K_p, R/I) \quad \text{and} \quad L'_p = \mathrm{H}^1(K_p, R/I(1)).$$

Proof. We have $\mathrm{H}^1(K_p, R/I) = \mathrm{Hom}(\mathrm{Gal}(\overline{K_p}/K_p), R/I)$. Since R/I is abstractly a sum of copies of $\mathbb{Z}/\ell\mathbb{Z}$ and $\ell \neq p$, any such homomorphism is tamely ramified. Furthermore, by assumption f), any tamely ramified homomorphism is unramified. Therefore all classes in $\mathrm{H}^1(K_p, R/I)$ are unramified, and $\mathrm{H}^1(K_p, R/I) \to R/I$, sending a cohomology class to the image of Frob_{p^2} in R/I, is an isomorphism.

By Kummer theory, we have $\mathrm{H}^1(K_p, \mu_\ell) = K_p^\times/(K_p^\times)^\ell$, and the unramified classes are $\mathcal{O}_p^\times/(\mathcal{O}_p^\times)^\ell$. Thus by assumption f), we have $\mathrm{H}^1_{\mathrm{unr}}(K_p, \mu_\ell) = 0$, and $\mathrm{H}^1(K_p, \mu_\ell)$ is 1-dimensional over $\mathbb{Z}/\ell\mathbb{Z}$, generated by the class of a uniformizer in $K_p^\times/(K_p^\times)^\ell$. Since E/K_p has good reduction we have, by Lemma 6,

$$L_p = R/I \otimes \mathrm{H}^1_{\mathrm{unr}}(K_p, E[\ell]),$$

and so we find that L_p is the summand $\mathrm{H}^1(K_p, R/I)$ of $\mathrm{H}^1(K_p, A[I])$.

To see that $L'_p = \mathrm{H}^1(K_p, R/I(1))$, we will use the rigid-analytic uniformization of A/K_p. Since it is an isogeny factor of the new quotient of $J_0(Np)/\mathbb{Q}$, the abelian variety $A/\mathbb{Q}_p$ has purely toric reduction. Let $\mathcal{A}/\mathbb{Z}_p$ be its Néron model. By Lemma 2, the F-vector space $\mathbb{Q} \otimes_{\mathbb{Z}} X^*(\mathcal{A}^0/\overline{\mathbb{F}_p})$ is 1-dimensional, and so the group $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ acts on it via a continuous $F^\times$-valued character. Since F is totally real, this character must be quadratic. The group scheme $\mathcal{A}^0/\mathbb{F}_{p^2}$ is thus a split torus.

Since $A/\mathbb{Q}_p$ has semi-stable reduction, the (split) torus $\mathcal{A}^0/\mathbb{F}_{p^2}$ is identity component of the special fiber of the Néron model of A/K_p. Let T/K_p be the split torus whose character group is $X^*(\mathcal{A}^0/\mathbb{F}_{p^2})$. Let R act as endomorphisms of T/K_p dual to the action of R on $X^*(\mathcal{A}^0/\mathbb{F}_{p^2})$. One then has the rigid-analytic uniformization $T^{\mathrm{an}} \to A^{\mathrm{an}}$ over K_p (cf. [BL91]), which yields a surjection of $R[\mathrm{Gal}(\overline{K_p}/K_p)]$-modules $T(\overline{K_p}) \to A(\overline{K_p})$. The kernel Λ of $T(\overline{K_p}) \to A(\overline{K_p})$ is a free $\mathbb{Z}$-module of rank $\dim(A)$, on which $\mathrm{Gal}(\overline{K_p}/K_p)$ acts trivially.

Consider the following diagram comparing the Kummer maps for T/K_p and A/K_p, where the vertical maps come from the analytic uniformization $T(\overline{K_p}) \to A(\overline{K_p})$:

$$\begin{array}{ccc} I^{-1} \otimes_R T(K_p) & \longrightarrow & \mathrm{H}^1(K_p, T[I]) \\ \downarrow & & \downarrow \\ I^{-1} \otimes_R A(K_p) & \longrightarrow & \mathrm{H}^1(K_p, A[I]). \end{array} \tag{5.1}$$

Since $\Lambda[I] = 0$, the uniformization induces an injection $T[I] \to A[I]$ over K_p. As $X^*(\mathcal{A}^0/\mathbb{F}_{p^2})$ is locally free of rank 1 over R, the R/I-module scheme $T[I]$ is abstractly $R/I(1)$. Thus the image of $T[I]$ in $A[I]$ is the $R/I(1)$ summand of $A[I] = R/I \oplus R/I(1)$. Consequently, the image of the right vertical arrow in (5.1) is the summand $\mathrm{H}^1(K_p, R/I(1))$ of $\mathrm{H}^1(K_p, A[I])$. The cokernel of the top arrow is contained in $\mathrm{H}^1(K_p, T)$, which vanishes by Hilbert Theorem 90, since T/K_p is a split torus. Finally, the left vertical arrow is surjective, since

$\mathrm{H}^1(K_p, \Lambda) = 0$. These three observations imply that the image L'_p of the Kummer map in $\mathrm{H}^1(K_p, A[I])$ is the summand $\mathrm{H}^1(K_p, R/I(1))$. $\square$

5.2. **Comparing the Selmer groups.** To prove Theorem 2, we compare the subspaces $R/I \otimes \mathrm{Sel}(E/K, \ell)$ and $\mathrm{Sel}(A/K, I)$ of $\mathrm{H}^1(K, A[I])$. Let $\mathrm{Sel}_s(A/K, I) \subset \mathrm{Sel}(A/K, I)$ (with s for "strict") be the intersection of these two Selmer groups. By Lemmas 5 and 8, the Selmer group $\mathrm{Sel}_s(A/K, I)$ is the space of classes $c \in \mathrm{H}^1(K, A[I])$ such that for $v \neq p$ the local restriction c_v belongs to $L_v = L'_v$ and such that the local restriction x_p is 0. Since the spaces L_p and L'_p are both 1-dimensional over R/I, the codimension of $\mathrm{Sel}_s(A/K, I)$ in each of $R/I \otimes \mathrm{Sel}(E/K, \ell)$ and $\mathrm{Sel}(A/K, I)$ is at most 1. More precisely, by Theorem 1, the Selmer group $\mathrm{Sel}_s(A/K, I)$ is 1-dimensional, if the Heegner point P is divisible by ℓ in $E(K_p)$: in this case the restriction to p of the image of P in $\mathrm{Sel}(E/K, \ell)$ vanishes, and so $R/I \otimes \mathrm{Sel}(E/K, \ell) = \mathrm{Sel}_s(A/K, I)$. Therefore, if P is divisible by ℓ in $E(K_p)$, the R/I-dimension of $\mathrm{Sel}(A/K, I)$ is either 1 or 2. Similarly, if P is not divisible by ℓ in $E(K_p)$, then $\mathrm{Sel}_s(A/K, I)$ is 0-dimensional; in this case, the R/I-dimension of $\mathrm{Sel}(A/K, I)$ is either 0 or 1.

As is explained in §6 below, the conjecture of Birch and Swinnerton-Dyer suggests that the R/I-dimension of $\mathrm{Sel}(A/K, I)$ should be even. In order to finish the proof of Theorem 2, we must exclude the possibility that $\mathrm{Sel}(A/K, I)$ is 1-dimensional over R/I, in harmony with the conjecture. In order rule out the 1-dimensional case, we present in §5.3 a variant of an argument which was shown to us by Benjamin Howard.

5.3. **The parity lemma.** Let k be a finite field of characteristic ℓ and let M be a totally imaginary number field. In what follows, we will take $k = R/I$ and $M = K$. Let V be locally constant constructible étale sheaf of k-vector spaces over $\mathrm{Spec}(M)$, equipped with a perfect, alternating, k-bilinear pairing $V \times V \to k(1)$. In the application to Theorem 2, we will take $V = A[I]$ and use the pairing coming from the Weil pairing on $E[\ell]$. For each finite place v of M one then has the perfect, symmetric, k-bilinear Tate-local-duality pairing $\mathrm{H}^1(M_v, V) \times \mathrm{H}^1(M_v, V) \to k$ mapping $x \times y \mapsto \langle x, y \rangle_v$. The duality pairing is the composition of the product $\mathrm{H}^1(M_v, V) \times \mathrm{H}^1(M_v, V) \to \mathrm{H}^2(M_v, k(1))$ with the reciprocity isomorphism $\mathrm{H}^1(M_v, k(1)) \to k$. For each finite place v of M, let $\Lambda_v \subset \mathrm{H}^1(M_v, V)$ be a k-subspace. Assume that for almost all v, one has $\Lambda_v = \mathrm{H}^1_{\mathrm{unr}}(M_v, V)$. Assume furthermore that each Λ_v is its own annihilator under the Tate pairing. This assumption implies that each $\mathrm{H}^1(M_v, V)$ has even dimension over k and that each Λ_v is a totally isotropic subspace of half the dimension of $\mathrm{H}^1(M_v, V)$.

Thus the Tate pairing on $\mathrm{H}^1(M_v, V)$ is a split symmetric bilinear form, and Λ_v is a maximal totally isotropic subspace.

We distinguish one fixed finite place w of M, which will be the place p of K in the proof of Theorem 2. Assume that $\mathrm{H}^1(M_w, V)$ is 2-dimensional over k, so that $\mathrm{H}^1(M_w, V)$ equipped with the Tate pairing is a hyperbolic plane. There are then exactly two maximal totally isotropic subspaces (lines), namely, the given Λ_w and another subspace Λ'_w. (Recall that k has characteristic $\ell \neq 2$.)

We consider four Selmer groups contained in $\mathrm{H}^1(M, V)$, defined by the local conditions Λ_v for $v \neq w$ and differing only in their defining local conditions at w. Let $\mathrm{Sel}_u(V)$ ("unramified") be defined by the local conditions Λ_v at all places v, i.e. $\mathrm{Sel}_u(V) \subset \mathrm{H}^1(M, V)$ is the space of classes x such that the restriction x_v belongs to Λ_v for all finite places v of M. Let $\mathrm{Sel}_t(V)$ ("transverse") be defined by the local conditions Λ_v at $v \neq w$ and by Λ'_w at w. Let $\mathrm{Sel}_r(V)$ ("relaxed") be defined by the local conditions Λ_v at $v \neq w$ and no condition at w. Let $\mathrm{Sel}_s(V)$ ("strict") be defined by the local conditions L_v at $v \neq w$ and local vanishing at w.

Lemma 9. *The k-dimensions of* $\mathrm{Sel}_u(V)$ *and* $\mathrm{Sel}_t(V)$ *differ by exactly* 1*; moreover, either*

$$\mathrm{Sel}_u(V) = \mathrm{Sel}_r(V) \quad \textit{and} \quad \mathrm{Sel}_t(V) = \mathrm{Sel}_s(V), \ \textit{or}$$
$$\mathrm{Sel}_u(V) = \mathrm{Sel}_s(V) \quad \textit{and} \quad \mathrm{Sel}_t(V) = \mathrm{Sel}_r(V).$$

Proof. Let $x, y \in \mathrm{Sel}_r(V)$. By global class field theory, one has

$$\sum_v \langle x_v, y_v \rangle_v = 0,$$

where $x_v, y_v \in \mathrm{H}^1(M_v, V)$ are the restrictions of x and y. Since x, y restrict to elements of the totally isotropic spaces Λ_v for $v \neq w$, one has

$$\langle x_w, y_w \rangle_w = \sum_v \langle x_v, y_v \rangle_v = 0.$$

Therefore, the image of $\mathrm{Sel}_r(V)$ in $\mathrm{H}^1(M_w, V)$ under the restriction map is a totally isotropic subspace. Consequently this image is contained in Λ_w or Λ'_w, and

$$\mathrm{Sel}_r(V) = \mathrm{Sel}_u(V) \quad \text{or} \quad \mathrm{Sel}_r(V) = \mathrm{Sel}_t(V).$$

On the other hand, it follows from the global Euler characteristic formula and global duality (cf. [DDT94], Theorem 2.19) that the k-codimension of $\mathrm{Sel}_s(V)$ in $\mathrm{Sel}_r(V)$ is 1: the local conditions for $\mathrm{Sel}_s(V)$ are obtained by relaxing the local condition at w from the self-dual, 1-dimensional Λ_w to the 2-dimensional $\mathrm{H}^1(M_w, V)$, and the dual of the relaxed condition at w is the strict condition at w defining $\mathrm{Sel}_s(V)$. As $\mathrm{Sel}_s(V) = \mathrm{Sel}_u(V) \cap \mathrm{Sel}_t(V)$ in $\mathrm{Sel}_r(V)$, one cannot have $\mathrm{Sel}_r(V) = \mathrm{Sel}_t(V) = \mathrm{Sel}_r(V)$. Therefore, one has either $\mathrm{Sel}_r(V) = \mathrm{Sel}_u(V)$ and $\mathrm{Sel}_s(V) = \mathrm{Sel}_t(V)$ or $\mathrm{Sel}_r(V) = \mathrm{Sel}_t(V)$ and $\mathrm{Sel}_s(V) = \mathrm{Sel}_u(V)$. These relations and the fact that the k-codimension of $\mathrm{Sel}_s(V)$ in $\mathrm{Sel}_r(V)$ is 1 prove the lemma. □

5.4. **Completion of the proof of Theorem 2.** To finish the proof the theorem, we apply the parity lemma to $A[I]/K$ to compare the subspaces $R/I \otimes \mathrm{Sel}(E/K, \ell)$ and $\mathrm{Sel}(A/K, I)$ of $\mathrm{H}^1(K, A[I])$. The transfer of the Weil pairing on $R/I \otimes E[\ell]$ via the isomorphism $R/I \otimes E[\ell] = A[I]$ to $A[I]$ provides a perfect, alternating pairing $A[I] \times A[I] \to R/I(1)$. The fact that the spaces $L_v \subset \mathrm{H}^1(K_v, A[I])$ are their own annihilators under the Tate pairing follows from Tate local duality for the elliptic curve E/K. Alternatively, one can deduce it directly from the description $L_v = \mathrm{H}^1_{\mathrm{unr}}(K_v, A[I])$ for v prime to ℓ and $L_v = \mathrm{H}^1_{\mathrm{fl}}(\mathrm{Spec}(\mathcal{O}_v, \mathcal{A}[I])$ for v dividing ℓ (cf. [Mil86], Theorem I.2.6, Corollary II.1.10(b), and Theorem III.1.8(b)). As we observed above in Lemma 8, conditions c) and f) imply that $A[I]/K_p = R/I \oplus R/I(1)$ and that $\mathrm{H}^1(K_p, A[I])$ is 2-dimensional over R/I. Each 1-dimensional summand R/I and $R/I(1)$ is isotropic for the (alternating) Weil pairing, and so the 1-dimensional summands $\mathrm{H}^1(K_p, R/I)$ and $\mathrm{H}^1(K_p, R/I(1))$ of $\mathrm{H}^1(K_p, A[I])$ are isotropic for the Tate pairing.

We now apply the parity lemma with $M = K$, the étale sheaf $V = A[I]$, equipped with the Weil pairing, and the local conditions $\Lambda_v = L_v$. These structures satisfy the hypotheses of §5.3. We take the distinguished place w to be the place p of K. By the discussion in §5.1, we have $\Lambda'_p = L'_p$. Since for $v \neq p$, we have $L_v = L'_v$, the parity lemma compares the Selmer groups $\mathrm{Sel}_u(A[I]) = R/I \otimes \mathrm{Sel}(E/K, \ell)$ and $\mathrm{Sel}_t(A[I]) = \mathrm{Sel}(A/K, I)$ in $\mathrm{H}^1(K, A[I])$. By Kolyvagin's result stated in Theorem 1, we know that $\mathrm{Sel}(E/K, \ell)$ is 1-dimensional over $\mathbb{Z}/\ell\mathbb{Z}$, generated by the image of the Heegner point P under the Kummer map. Therefore, the parity lemma implies Theorem 2. □

6. Compatibility with the functional equation

In this section we study the signs of the functional equations for L-functions related to f and g. Let $\epsilon = \pm 1$ be the sign of the complete L-function of f, i.e. if $\Lambda(s, f) = (2\pi)^{-s}\Gamma(s)L(s, f)$ is the complete L-function of f, then $\Lambda(s, f) = \epsilon N^{1-s}\Lambda(2 - s, f)$. If W is the Fricke involution of level N, then $Wf = -\epsilon f$ by Theorem 3.66 of [Shi94]. Let χ be the quadratic Dirichlet character corresponding to $K/\mathbb{Q}$. By [Shi94], Theorem 3.66 and Lemma 3.63 (2), the sign of the complete twisted L-function $\Lambda(s,f,\chi)=(2\pi)^{-s}\Gamma(s)L(s,f,\chi)$ is $\chi(-N)\times\epsilon$. That is,

$$\Lambda(s,f,\chi)=(\chi(-N)\times\epsilon)(r^2N)^{1-s}\Lambda(2-s,f,\chi),$$

where r is the conductor of χ. Since the primes dividing N split in K and K is imaginary quadratic, one has $\chi(-N)=\chi(-1)=-1$, and so the sign of $\Lambda(f,s,\chi)$ is $-\epsilon$. Therefore, the sign of $\Lambda(s,f)\times\Lambda(s,f,\chi)$, which is the complete L-function of the base change of f to K, is -1. By the compatibility of the Eichler-Shimura construction with the local Langlands correspondence (cf. [Car86]), the complete L-function $\Lambda(s,E/K)=\Lambda(s,E/\mathbb{Q})\times\Lambda(s,E/\mathbb{Q},\chi)$ is $\Lambda(s,f)\times\Lambda(s,f,\chi)$. Thus the functional equation for $\Lambda(s,E/K)$ has sign -1, which is what one would expect from the Birch and Swinnerton-Dyer conjecture and Theorem 1, since $E[\ell](K)=0$ by condition b).

Recall that the new level of the newform g is Np by condition e). Let ϵ' be the sign of the functional equation of $\Lambda(s,g)$. Then, as in the case of f, the sign of the functional equation of $\Lambda(s,g,\chi)$ is $\chi(-Np)\times\epsilon'=\epsilon'$, since the primes dividing N split in K, the field K is imaginary quadratic, and p is inert in $K/\mathbb{Q}$. Consequently, the sign of $\Lambda(s,g)\times\Lambda(s,g,\chi)$, which is the complete L-function of the base change of g to K, is $+1$.

The conjecture of Birch and Swinnerton-Dyer conjecture for A/K, when combined with the conjecture of Deligne and Gross [D79, Conj 2.7], predicts that the dimension of of the F-vector space $F\otimes_R A(K)$ is equal to the order of vanishing of $L(s,g)\times L(s,g,\chi)$ at $s=1$. From the sign of the functional equation, one thus expects $F\otimes_R A(K)$ to have even dimension. Theorem 2 implies that the dimension is 0, if ℓ does not divide P in $E(K_p)$, since $I^{-1}/R\otimes_R A(K)$ injects into $\mathrm{Sel}((A,i)/K,I)=0$. If ℓ does divide P in $E(K_p)$, then by Theorem 2, the group $\mathrm{Sel}((A,i)/K,I)$ is 2-dimensional over R/I. If $Ш(A/K)$ is finite, then one can check using the Cassels-Tate pairing that the dimensions of $\mathrm{Sel}(A/K,I)$ and of $I^{-1}/R\otimes_R A(K)$ have the same parity; thus $F\otimes_R A(K)$ has dimension 2 or 0, according to whether $Ш(A/K)[I]=0$ or not.

Note that if ℓ does not divide P in $E(K_p)$, then, since the dimension of $F\otimes_R A(K)$ is 0, one finds that the rank of $A/\mathbb{Q}$ is 0. The following lemma shows that this conclusion is compatible with the parity prediction of the Birch and Swinnerton-Dyer conjecture over $\mathbb{Q}$.

Lemma 10. *Suppose that ℓ does not divide P in $E(K_p)$. Then the sign ϵ' of the functional equation of $\Lambda(s,g)$ is $+1$.*

Proof. Owing to the congruence between f and g, we have

$$a_p(f) \equiv a_p(g)(p+1) \pmod{\lambda}, \tag{6.1}$$

as one sees by comparing the local Galois representations at p associated to f and g. According to Lemma 1, the congruence in (6.1) holds with $a_p(g)$ replaced by $-\epsilon$. Since $p+1$ is invertible modulo ℓ by assumption f), we have, therefore, $a_p(g) \equiv -\epsilon \pmod{\lambda}$. As $a_p(g) = \pm 1$ and $\ell \neq 2$, we conclude that $a_p(g) = -\epsilon$.

Let α be the root in $\overline{\mathbb{Q}_\ell}$ of the Hecke polynomial $T^2 - a_p(f)T + p$ that is congruent to $-\epsilon$ modulo λ, and let β be the other root. Consider the oldform with coefficients in $\overline{\mathbb{Z}_\ell}$

$$h(z) = f(z) - \beta f(pz)$$

in the old space for f at level Np. The form $h(z)$ is an eigenfunction of the Hecke operators T_q for q prime to Np and of U_q for q dividing Np; the eigenvalues at q prime to p agree with those of f, and at p, we have $U_p h = \alpha h$. Since $\alpha \equiv -\epsilon \pmod{\lambda}$, the reductions $\overline{g}, \overline{h} \in S_2(\Gamma_0(Np), \overline{\mathbb{F}}_\ell)$ are eigenfunctions for the Hecke operators T_q for q prime to Np and U_q for q dividing Np with the same eigenvalues. Since both of these cuspidal eigenforms have $a_1 = 1$, we have $\overline{g} = \overline{h}$ by the q-expansion principle.

For a prime q dividing N, let W_q be the Atkin-Lehner involution at q for level N. Since f is a newform with new level N, it is an eigenfunction of all of the W_q. Let $W_q f = \epsilon_q f$. Then the sign ϵ is $-\prod_{q|N} \epsilon_q$.

For each q dividing Np, let W'_q be the Atkin-Lehner involution at q at level Np. Since g is a newform at level Np, it is an eigenfunction for all of the W'_q. One has $W'_p = -U_p$, and so $W'_p g = \epsilon g$. For q dividing N, we have $W'_q h = \epsilon_q h$, and so $\overline{W'_q g} = \overline{W'_q h} = \epsilon_q \overline{g}$. Therefore, $W'_q g = \epsilon_q g$ for q dividing N. The sign ϵ' of the functional equation for $\Lambda(s,g)$ is thus

$$-\epsilon \times \prod_{q|N} \epsilon_q = \epsilon^2 = +1.$$

□

7. Examples

We now give two examples. The data consist of a 4-tuple (E, K, p, ℓ) satisfying hypothesis a)–f). The examples are chosen so that the lifted form g has rational Fourier coefficients. In this case, we have $\mathbb{Q}(g) = \mathbb{Q}$

and $R = \mathbb{Z}$; the abelian variety (A, i) is an elliptic curve, and the I-descent on (A, i) is simply the ℓ-descent A. We wish to thank Noam Elkies and William Stein for help with the computations.

The first example is:

$$
\begin{array}{ll}
E = X_0(57)/\langle W_3, W_{19}\rangle & N = 57 \\
K = \mathbb{Q}(\sqrt{-59}) & h = 3 \\
p = 2 & a_2 = -2 \\
\ell = 5 &
\end{array}
$$

The minimal equation of E is (cf. [BK75]):

$$y^2 + y = x^3 - x^2 - 2x + 2 \qquad \Delta = -3^2.19,$$

and the modular form f associated to E has q-expansion

$$f = q - 2q^2 - q^3 + 2q^4 - 3q^5 + 2q^6 - 5q^7 + \dots$$

The sign in the functional equation of $L(s, E) = L(s, f)$ is $\epsilon = -1$, and $E(\mathbb{Q})$ is free of rank 1, with generator $e = (2, 1)$. The Heegner point P associated to K is equal to $\pm 2e$. This is *not* divisible by $\ell = 5$ in $E(K_p) = E(K_2)$.

Their is a unique newform g of weight 2 and level $114 = Np$ where $W_3' = W_{19}' = +1$ and $W_2' = \epsilon = -1$. It has q-expansion

$$g = q + q^2 - q^3 + q^4 + 2q^5 - q^6 + 0q^7 + \dots$$

congruent (mod 5) to the old form $f(\tau) - 2f(2\tau)$. The elliptic curve A has minimal equation

$$y^2 + xy + y = x^3 + x^2 - 352x - 2431 \qquad \Delta = 2^{20}.3^3.19.$$

The Selmer group $\mathrm{Sel}(A/K, 5) = 0$, and $A(K)$ has rank 0.

The second example is

$$
\begin{array}{ll}
E = X_0(26)/\langle W_2\rangle & N = 26 \\
K = \mathbb{Q}(\sqrt{-79}) & h = 5 \\
p = 3 & a_3 = 1 \\
\ell = 5 &
\end{array}
$$

The minimal equation of E is (cf. [BK75]):

$$y^2 + xy + y = x^3 - 5x - 8 \qquad \Delta = -2^3.13^3$$

and the modular form f associated to E has q-expansion beginning

$$f = q - q^2 + q^3 + q^4 - 3q^5 - q^6 - q^7 + \dots$$

The sign in the functional equation of $L(s,E) = L(s,f)$ is $\epsilon = +1$, and $E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$.

The Heegner point P associated to K has x-coordinate $x(P) = 1700/711$, and generates the free group $E(K)/\text{torsion}$. On the other hand, since the denominator of $x(P)$ is divisible by $p = 3$, the point P reduces to the identity (mod 3) and *is* divisible by $\ell = 5$ in $E(K_3)$. We note that E has three points over the field with $p = 3$ elements, and fifteen points over the field with $p^2 = 9$ elements.

In this case, g is the unique newform of weight 2 and level $78 = Np$. It has Fourier expansion beginning

$$g = q - q^2 - q^3 + q^4 + 2q^5 + q^6 + 4q^7 + \dots$$

and is congruent to the old form $f(\tau) + 3f(3\tau)$ (mod 5). The elliptic curve A has minimal equation

$$y^2 + xy = x^3 + x^2 - 19x + 685 \qquad \Delta = -2^{16}.3^5.13$$

and rank 0 over $\mathbb{Q}$. Since P is locally divisible by 5 in $E(K_3)$, the Selmer group $\mathrm{Sel}(A/K, 5)$ has dimension 2 over $\mathbb{Z}/5\mathbb{Z}$. In fact, $A(K)$ has rank 2. In the twisted model over $\mathbb{Q}$:

$$y^2 + xy + y = x^3 - 121830x - 341716424$$
$$\Delta = -2^{16}.3^5.13.79^6$$

the points
$(x,y) = (2732, 139056)$
$(x,y) = (410357, -263076219)$
generate the Mordell-Weil group modulo torsion.

Appendix A. Descent with endomorphisms

In this appendix, we give an expanded discussion of the I-descent used on the abelian variety A/K and its Néron model above. In order to have results general enough to apply easily to group schemes such as the Néron model, we begin very generally with some abstract constructions on sheaves. We then specialize to the sheaves represented by smooth group schemes, explaining how to apply the abstract results to such cases.

A.1. **First descent with endomorphisms.** Let R be a commutative, unital ring, and let $I \subset R$ be an ideal. Let A be a sheaf of R-modules on some site S, and assume that A is I-injective in the sense that the map of sheaves

$$A = \underline{\mathrm{Hom}}_R(R, A) \to \underline{\mathrm{Hom}}_R(I, A)$$

is surjective. (Note that for any R-module M, the presheaf $T \mapsto \mathrm{Hom}_R(M, A(T))$ is a sheaf.) The kernel of this map is $\underline{\mathrm{Hom}}_R(R/I, A)$. Associating to a sheaf homomorphism $R/I \to A$ the image of the section 1 identifies $\underline{\mathrm{Hom}}_R(R/I, A)$ with $A[I]$, the sheaf of sections of A killed by elements of I. We thus have an exact sequence of sheaves

$$0 \longrightarrow A[I] \longrightarrow A \longrightarrow \underline{\mathrm{Hom}}_R(I, A) \longrightarrow 0.$$

The boundary map

$$\mathrm{Hom}_R(I, A(S)) \to \mathrm{H}^1(S, A[I])$$

in the associated long exact sequence in cohomology is the *Kummer map*. From the long exact sequence, we see that the kernel of the Kummer map is the image of $\mathrm{Hom}_R(R, A(S)) = A(S)$ in $\mathrm{Hom}_R(I, A(S))$. Similarly, the cokernel of the Kummer map is the kernel of

$$\mathrm{H}^1(S, A) \to \mathrm{H}^1(S, \underline{\mathrm{Hom}}_R(I, A)).$$

If I is invertible as an R-module, then we have

$$\underline{\mathrm{Hom}}_R(I, A) = I^{-1} \otimes_R A,$$

where $I^{-1} = \mathrm{Hom}_R(I, R)$. Here $I^{-1} \otimes_R A$ denotes the presheaf

$$T \mapsto I^{-1} \otimes_R A(T),$$

which is a sheaf since I^{-1} is a flat R-module. Thus we have the exact sequence of sheaves

$$0 \longrightarrow A[I] \longrightarrow A \longrightarrow I^{-1} \otimes_R A \longrightarrow 0.$$

The kernel of the Kummer map

$$I^{-1} \otimes_R A(S) \to \mathrm{H}^1(S, A[I])$$

is the image of $R \otimes_R A(S) = A(S)$, and so the Kummer image is $(I^{-1}/R) \otimes_R A(S)$, or, equivalently, it is $I^{-1} \otimes_R (R/I \otimes_R A(S))$. In this case, we also have

$$\mathrm{H}^1(S, I^{-1} \otimes_R A) = I^{-1} \otimes_R \mathrm{H}^1(S, A),$$

The cokernel of the Kummer map is then the kernel of

$$\mathrm{H}^1(S, A) \to I^{-1} \otimes_R \mathrm{H}^1(S, A),$$

which is $\mathrm{H}^1(S, A)[I]$, the I-torsion of the R-module $\mathrm{H}^1(S, A)$.

If S is the small étale site of $\mathrm{Spec}(K)$ for a number field K, we define $\mathrm{Sel}(A/K, I)$, the I-Selmer group of A, to be the subspace of classes $x \in \mathrm{H}^1(K, A[I])$ whose local restrictions $x_v \in \mathrm{H}^1(K_v, A[I])$ lie in the image of $\mathrm{Hom}_R(I, A(K_v))$ under the local Kummer map for all places v of K. As in the standard case with $R = \mathbb{Z}$ and $I = (\ell)$, the global Kummer map

$$\mathrm{Hom}_R(I, A(K)) \to \mathrm{H}^1(K, A[I])$$

factors through $\mathrm{Sel}(A/K, I)$.

In topology the most familiar analogue of the above formalism is the following: let M be an R-module that has no I-torsion, so that $M \to \mathrm{Hom}_R(I, M)$ is injective. Let N be the cokernel, so that we have the exact sequence of constant sheaves of R-modules on any topological space X

$$0 \longrightarrow M \longrightarrow \underline{\mathrm{Hom}}_R(I, M) \longrightarrow N \longrightarrow 0.$$

Passing to cohomology, we find

$$\begin{array}{ccccc} \ldots & \longrightarrow & \mathrm{H}^i(X, M) & \longrightarrow & \mathrm{H}^i(X, \underline{\mathrm{Hom}}_R(I, M)) \longrightarrow \\ \mathrm{H}^i(X, N) & \longrightarrow & \mathrm{H}^{i+1}(X, M) & \longrightarrow & \ldots, \end{array}$$

which is a Bockstein-type sequence in the case $R = \mathbb{Z}$ and $I = (\ell)$.

To recast the above discussion in this style, we replace the sheaves A and $\underline{\mathrm{Hom}}_R(I, A)$ with the complexes

$$M = A[-1] \quad \text{and} \quad M' = \underline{\mathrm{Hom}}_R(I, A)[-1],$$

concentrated in degree 1. The I-injectivity of A translates into something like I-torsion freeness of M: the exact sequence of sheaves

$$0 \longrightarrow A[I] \longrightarrow A \longrightarrow \underline{\mathrm{Hom}}_R(I, A) \longrightarrow 0$$

gives rise to a distinguished triangle

$$M \to M' \to A[I] \to M[1].$$

The sheaf $A[I]$ thus plays the same role as the cokernel N in the picture over a topological space X, and the Kummer map is

$$\mathrm{Hom}(I, A(S)) = \mathrm{H}^1(S, M') \to \mathrm{H}^1(S, A[I]).$$

For a concrete example, let S be the fppf site of a field K, and let A is the sheaf represented by an abelian variety over K on which R acts as endomorphisms. Assume that I is invertible as an R-module. Then, as explained in the next section, $\underline{\mathrm{Hom}}_R(I, A) = I^{-1} \otimes_R A$ is also represented by an abelian variety, on which R acts as endomorphisms. Furthermore, the natural map $A \to I^{-1} \otimes_R A$ of sheaves is surjective. The complexes M and M' are the 1-motives associated to these abelian varieties, and the surjection of sheaves $A \to \underline{\mathrm{Hom}}_R(I, A)$ becomes an injection of motives $M \to M'$. The sheaf $A[I]$ (in degree 0) stands in for the (hypothetical) torsion motive $\mathrm{coker}(M \to M')$.

A.2. **Smooth R-module schemes.** Let R and I be as in §A.1. Assume moreover that I is finitely presented as an R-module. Let X be a scheme and let G/X be an R-module scheme. The choice of a presentation of I produces a scheme representing the fppf sheaf $\underline{\mathrm{Hom}}_R(I, G)$: let $R^{\oplus r} \to R^{\oplus s} \to I \to 0$ be an R-module presentation. Then the kernel of $G^{\oplus r} \to G^{\oplus s}$ represents $\underline{\mathrm{Hom}}_R(I, G)$. We fix a presentation of I and write $\underline{\mathrm{Hom}}_R(I, G)$ for the representing scheme as well as the sheaf. Many scheme-theoretic properties of G/X carry over to $\underline{\mathrm{Hom}}_R(I, G)$. For instance, if G/X is separated (resp. quasi-compact, quasi-separated, locally of finite type, locally of finite presentation, proper, ...), then so is $\underline{\mathrm{Hom}}_R(I, G)/X$. Note finally that if I is invertible as an R-module and G/X has connected geometric fibers, then so does $\underline{\mathrm{Hom}}_R(I, G)$: the surjection $R^{\oplus s} \to I$ splits, and so $\underline{\mathrm{Hom}}_R(I, G)/X$ is a factor of $G^{\oplus r}/X$, which has connected geometric fibers.

Assume from now on that G/X is smooth and that I is invertible as an R-module. It follows from the functorial criterion for smoothness that $\underline{\mathrm{Hom}}_R(I, G)/X$ is smooth. Furthermore, there is a natural isomorphism $\underline{\mathrm{Hom}}_R(I, \mathrm{Lie}(G/X)) = \mathrm{Lie}(\underline{\mathrm{Hom}}_R(I, G)/X)$, and so the relative dimensions of G/X and $\underline{\mathrm{Hom}}_R(I, G)/X$ agree.

The kernel and cokernel of the map on Lie algebras

$$\mathrm{Lie}(G/X) \to \mathrm{Lie}(I^{-1} \otimes_R G/X) = I^{-1} \otimes_R \mathrm{Lie}(G/X)$$

are coherent sheaves on X on which R acts and that are annihilated by I. Thus if I contains the image of $\ell \in \mathbb{Z}$ such that ℓ is invertible on X, this map is an isomorphism, and $G \to I^{-1} \otimes_R G$ is étale. By [SGA70], Exposé VIB, Proposition 3.11, if G/X has connected geometric fibers, the map $G \to \underline{\mathrm{Hom}}_R(I, G)$ is étale and surjective, and so the sheaf on the small étale (or fppf or fpqf) site of X represented by G/X is I-injective.

Alternatively, assume that G/X has connected and semi-abelian geometric fibers, and that I contains the image of any non-zero $\ell \in \mathbb{Z}$. The multiplication-by-ℓ endomorphism of G is then surjective. Since $G \to I^{-1} \otimes_R G$ factors through multiplication by ℓ, the geometric fibers of $I^{-1} \otimes_R G/X$ are connected, and the relative dimensions of G/X and $I^{-1} \otimes_R G/X$ agree, the homomorphism $G \to I^{-1} \otimes_R G$ is also surjective. By [SGA70], Exposé VIB, Proposition 3.11, the homomorphism $G \to I^{-1} \otimes_R G$ is then flat and surjective. Consequently, the sheaf on the fppf (or fpqf) site of X represented by G/X is I-injective.

In either of these cases, since $G \to I^{-1} \otimes_R G$ is flat, the kernel $G[I]/X$ is flat and quasi-finite for dimensional reasons. If G/X is proper, then $G[I]/X$ is moreover finite and locally free.

References

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[BD99] M. Bertolini and H. Darmon, *Euler systems and Jochnowitz congruences*, Amer. J. Math. **121** (1999), no. 2, 259–281.

[BD05] M. Bertolini and H. Darmon, *Iwasawa's main conjecture for elliptic curves over anticyclotomic Z_p-extensions*, Annals of Mathematics **162** (2005), 1–64.

[BK75] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Springer-Verlag, Berlin, 1975, Lecture Notes in Mathematics, Vol. 476.

[BL91] Siegfried Bosch and Werner Lütkebohmert, *Degenerating abelian varieties*, Topology **30** (1991), no. 4, 653–698.

[BSD75] B. J. Birch and H. P. F. Swinnerton-Dyer, *Elliptic curves and modular functions*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 2–32. Lecture Notes in Math., Vol. 476.

[Car86] Henri Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 3, 409–468.

[DDT94] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Internat. Press, Cambridge, MA, 1994, pp. 1–154.

[Dia95] Fred Diamond, *The refined conjecture of Serre*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995, pp. 22–37.

[D79] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Automorphic forms, representations, and L-functions, Proceedings of Symposia in Pure Mathematics, volume 33, part 2 (1979) 313–346.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[Gro] Benedict H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, pp. 235–256.

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

[GZ86] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[Lan56] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

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

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.

[Mil86] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press Inc., Boston, MA, 1986.

[Ray74] Michel Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.

[Rib90] Kenneth A. Ribet, *Raising the levels of modular representations*, Séminaire de Théorie des Nombres, Paris 1987–88, Progr. Math., vol. 81, Birkhäuser Boston, Boston, MA, 1990, pp. 259–271.

[Ser87] Jean-Pierre Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[SGA70] *Schémas en groupes. I: Propriétés générales des schémas en groupes*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 151, Springer-Verlag, Berlin, 1970.

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Shi98] ———, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, Princeton, NJ, 1998.