J. reine angew. Math. **412** (1990), 63—74

Journal für die reine und
angewandte Mathematik
© Walter de Gruyter
Berlin · New York 1990

Kolyvagin's descent and Mordell-Weil groups over ring class fields[1]

By *Massimo Bertolini*[2] at New York and *Henri Darmon*[3] at Cambridge

1. Introduction

Let $E/\mathbb{Q}$ be a modular elliptic curve with the modular parametrization:

$$\phi : X_0(N) \to E,$$

where $X_0(N)$ is the complete curve over $\mathbb{Q}$ which classifies pairs of elliptic curves related by a cyclic N-isogeny. The curve E is equipped with the collection of Heegner points defined over ring class fields of suitable imaginary quadratic fields.

More precisely, let K be an imaginary quadratic field in which all rational primes dividing N are split and let $\mathcal{O}$ be the order of K of conductor c prime to N. There exists a proper $\mathcal{O}$-ideal $\mathcal{N}$ such that the natural projection of complex tori

$$\mathbb{C}/\mathcal{O} \to \mathbb{C}/\mathcal{N}^{-1} \tag{1}$$

is a cyclic N-isogeny. The moduli interpretation of $X_0(N)$ identifies the diagram (1) with a point of $X_0(N)$. By the theory of complex multiplication, this point is defined over H, the ring class field of K of conductor c. Let $\alpha \in E(H)$ be its image under ϕ.

The group $G = \mathrm{Gal}(H/K)$ acts naturally on the $\mathbb{Z}$-module $E(H)$, and $E(H) \otimes \mathbb{C}$ can be decomposed as a direct sum of eigenspaces under this action:

$$E(H) \otimes \mathbb{C} = \bigoplus_{\chi \in \hat{G}} E(H)^{\chi},$$

where $\hat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$ is the group of complex characters of G. Let

[1] The authors wish to thank B. H. Gross and K. C. Rubin for having proposed this problem and provided helpful suggestions in the write-up.

[2] Partially supported by a grant from the Consiglio Nazionale delle Ricerche of Italy.

[3] Partially supported by a Doctoral Fellowship from the Natural Sciences and Engineering Research Council of Canada (NSERC).

$$e_\chi = \frac{1}{\# G} \sum_{\sigma \in G} \chi^{-1}(\sigma)\,\sigma$$

be the idempotent in the group ring giving the projection onto the χ-eigenspace.

Gross and Zagier [3] proved the following limit formula when $c=1$ (so that H is the Hilbert class field of K):

$$L'(E/K, \chi, 1) = a\hat{h}(e_\chi \alpha),$$

where $L(E/K, \chi, s)$ is the L-series of E/K twisted by the character χ, a is a non-zero invariant depending on E and K, and $\hat{h}$ is the canonical height extended by linearity to $E(H)\otimes \mathbb{C}$. In view of the conjecture of Birch and Swinnerton-Dyer, Gross formulated the following:

Conjecture 1. 1. *If* $e_\chi \alpha \neq 0$, *then* $\dim_{\mathbb{C}} E(H)^\chi = 1$.

In his paper on Euler systems [4], Kolyvagin proves the above conjecture when χ is the trivial character. We will apply Kolyvagin's descent techniques to prove the general case when E has no complex multiplications.

2. Preliminaries

Our strategy will be to do a p-descent for a suitable prime p. We choose p so that

1. $p \nmid 6cN\,\mathrm{Disk}(K)$,

2. $\mathbb{Q}(E_p)/\mathbb{Q}$ is a $\mathrm{GL}_2(\mathbb{F}_p)$-extension,

3. $p \equiv 1 \pmod{\# G}$.

These conditions can be imposed simultaneously, provided that E has no complex multiplications, by combining the "open image" theorem of Serre [8] with the result of Dirichlet on primes in arithmetic progressions. The following lemma is a simple consequence of conditions 1 and 2:

Lemma 2. 1. *If L is an extension of $\mathbb{Q}$ which is unramified at all primes dividing Np, then* $\mathrm{Gal}(L(E_p)/L) \cong \mathrm{GL}_2(\mathbb{F}_p)$.

Proof. The extension $\mathbb{Q}(E_p)/\mathbb{Q}$ is ramified only at places dividing Np, and hence $\mathbb{Q}(E_p)$ and L are linearly disjoint over $\mathbb{Q}$ (the intersection of these two fields is an unramified extension of $\mathbb{Q}$, which is $\mathbb{Q}$ by Minkowski's theorem). Hence $\mathrm{Gal}(L(E_p)/L) = \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_p)$.

By condition 3, any $\mathbb{F}_p[G]$-module M splits as a direct sum of primary representations:

$$M = \bigoplus_{\chi \in \hat{G}} M^\chi,$$

where χ ranges over the $\mathbb{F}_p$-valued characters of G. (By choosing a reduction map

$$\mathbb{Z}[\mu_{\# G}] \to \mathbb{F}_p,$$

we identify complex and $\mathbb{F}_p$-valued characters of G.) Notice that if $e_\chi \alpha$ is non-zero in $E(H) \otimes \mathbb{C}$, then it is also non-zero in $E(H) \otimes \mathbb{F}_p$ for almost all primes p. Furthermore, lemma 2. 1 implies that $E_p(H)=0$ and hence

$$\dim_{\mathbb{C}} E(H)^\chi = \dim_{\mathbb{F}_p} (E(H) \otimes \mathbb{F}_p)^\chi .$$

Conjecture 1. 1 is thus reduced to the following "mod p" analogue:

Theorem 2. 2. *If $e_\chi \alpha \neq 0$ in $E(H) \otimes \mathbb{F}_p = E(H)/pE(H)$, then*

$$\dim_{\mathbb{F}_p} (E(H)/pE(H))^\chi = 1 .$$

Let us introduce some conventions and results that will be used throughout. We fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ which contains all of the field extensions which will be introduced later on. Let $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be a fixed complex conjugation corresponding to a choice of an embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$, and denote by $[\tau]$ its conjugacy class. It will be convenient to identify τ with its images in finite quotients of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. If M is a module on which τ acts, the superscripts $+$ and $-$ are used to designate projection onto the eigenspaces for the action of τ (we assume that 2 is invertible in $\mathrm{End}_{\mathbb{Z}}(M)$, so that M decomposes as a direct sum of such eigenspaces):

$$M^\pm = \{ m \in M \mid \tau m = \pm m \} .$$

Also, if $x \in M$ and $X \subset M$, we let

$$x^\pm = \frac{1}{2}(x \pm \tau x),$$

$$X^\pm = \{ x^\pm \mid x \in X \} .$$

For conciseness, we shall occasionally use the notation M/p to denote the $\mathbb{F}_p$-vector space $M \otimes \mathbb{F}_p = M/pM$.

Let $H[n] \subset \bar{\mathbb{Q}}$ denote the ring class field of K associated to the order $\mathcal{O}_n$ of conductor cn, where $(n, pN)=1$, let $G_n = \mathrm{Gal}(H[n]/H)$, and let $\alpha(n)$ be the Heegner point corresponding to the N-isogeny

$$\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/(\mathcal{O}_n \cap \mathcal{N})^{-1} .$$

By class field theory, G_n is canonically isomorphic to $(\mathcal{O}/n\mathcal{O})^*/(\mathbb{Z}/n\mathbb{Z})^*$, and complex conjugation acts on the group $\mathrm{Gal}(H[n]/K)$ by

$$\tau x \tau^{-1} = x^{-1} . \tag{2}$$

Let $\varepsilon = \pm 1$ denote the negative of the sign in the functional equation for $L(E/\mathbb{Q}, s)$. The following describes the action of τ on the Heegner points in $E(H[n])/p$:

Lemma 2.3. *There exists $\sigma_0 \in \mathrm{Gal}(H[n]/K)$ such that $\tau\alpha(n) = \varepsilon\sigma_0\alpha(n)$ in $E(H[n])/p$. Hence, $\tau e_\chi \alpha(n) = \varepsilon\bar{\chi}(\sigma_0)\, e_{\bar{\chi}}\alpha(n)$.*

Proof. In [2], it is observed that

$$\tau\alpha(n) = \varepsilon\sigma_0\,\alpha(n) + \text{torsion},$$

for some $\sigma_0 \in \mathrm{Gal}(H[n]/K)$. By lemma 2.1, the group $E(H[n])$ has no p-torsion, and the first statement follows. The second is a consequence of the identity:

$$\tau e_\chi = e_{\bar{\chi}}\tau,$$

which results from equation (2).

Kolyvagin's idea is to construct elements in the dual of the Selmer group,

$$\mathrm{Sel}_p^{\mathrm{dual}}(E/H) = \mathrm{Hom}(\mathrm{Sel}_p(E/H), \mathbb{F}_p),$$

via local Tate duality, and to control the size of this module by certain global cohomology classes related to Heegner points. Section 3 is devoted to the construction and study of these "Heegner cohomology classes".

3. The Heegner cohomology classes

Definition 3.1. A rational prime l is said to be *special* if $l \nmid Npc$ and

$$\mathrm{Frob}_l(K(E_p)/\mathbb{Q}) = [\tau].$$

Observe that, if l is special, then

$$a_l \equiv l + 1 \equiv 0 \pmod{p}, \tag{3}$$

where a_l denotes the trace of Frobenius acting on the Tate module $T_p(E)$. This follows from comparing the minimal polynomials of Frob_l and τ acting on E_p.

Let n denote a squarefree product of special primes, and let l be a special prime not dividing n. The prime l is inert in K by definition; let $\lambda = (l)$ be the unique prime of K above it. The prime λ splits completely in $H[n]/K$ (its image in $G_n = (\mathcal{O}/n\mathcal{O})^*/(\mathbb{Z}/n\mathbb{Z})^*$ by the Artin map is trivial), and any prime λ' of $H[n]$ above λ is totally ramified in $H[nl]$. Fix a choice of λ', and denote by λ'' the unique prime of $H[nl]$ above it. The following proposition summarizes the properties of Heegner points that will be needed in the constructions:

Proposition 3. 2. *The system of Heegner points* $\alpha(n) \in H[n]$ *satisfies*:

1. $\mathrm{Tr}_{H[nl]/H[n]}\,\alpha(nl) = a_l\,\alpha(n)$;

2. $\alpha(nl) \equiv \mathrm{Frob}_{\lambda'}\,\alpha(n) \pmod{\lambda''}$.

These two properties are axiomatized by Kolyvagin in his definition of "Euler systems" with congruence [4], § 1. For a proof, see for example [2], prop. 3. 7.

Since $H[n]$ is the compositum of the extensions $H[l]$ which are linearly disjoint over H, we have a canonical isomorphism $G_n = \prod_{l|n} G_l$, allowing us to view G_l as a subgroup of G_n. By class field theory, each G_l is isomorphic to $(\mathcal{O}_k/\lambda)^*/(\mathbb{Z}/l)^*$. Choose for each l a generator σ_l of G_l, and let

$$\mathrm{Tr}_l = \sum_{i=0}^{l} \sigma_l^i \in \mathbb{F}_p[G_l],$$

$$\mathrm{D}_l = \sum_{i=1}^{l} i\sigma_l^i \in \mathbb{F}_p[G_l],$$

$$\mathrm{D}_n = \prod_{l|n} \mathrm{D}_l \in \mathbb{F}_p[G_n].$$

Lemma 3. 3. $\mathrm{D}_n\alpha(n) \in (E(H[n])/p)^{G_n}$.

Proof. For all primes l dividing n,

$$(\sigma_l - 1)\,\mathrm{D}_l = 1 + l - \mathrm{Tr}_l = -\mathrm{Tr}_l,$$

where the last equality follows from eq. (3). Combining prop. 3. 2 with eq. (3), one has:

$$-\mathrm{Tr}_l\,\alpha(n) = -a_l\,\alpha(n/l) = 0.$$

Hence $\sigma_l \mathrm{D}_n \alpha(n) = \mathrm{D}_n \alpha(n)$; since the σ_l generate G_n, the lemma follows.

By lemma 2. 1, $E_p(H[n]) = 0$, and the following sequence is exact:

$$0 \longrightarrow E(H[n]) \xrightarrow{p} E(H[n]) \longrightarrow E(H[n])/p \longrightarrow 0.$$

Taking G_n-invariants yields the exact sequence of $\mathbb{F}_p[G]$-modules:

$$0 \to E(H)/pE(H) \to (E(H[n])/p)^{G_n} \to H^1(G_n, E(H[n]))_p \to 0.$$

Let $v(n)$ be the image of $\mathrm{D}_n\alpha(n)$ in $H^1(G_n, E(H[n]))_p$. By abuse of notation, we identify $v(n)$ with its image in $H^1(H, E)_p$ under inflation.

Let w be a prime of K lying above the rational prime v. There is a natural localization map

$$\mathrm{res}_w : H \to \bigoplus_{w'|w} H_{w'}.$$

By abuse of notation, we identify the map res_w with its image by any functor (from the category of étale algebras to the category of $\mathbb{F}_p$-vector spaces). The context will make it clear what the source and target of res_w are. Denote by $\mathbb{F}_{w'}$ the residue field of $H_{w'}$.

Lemma 3. 4. *The behaviour of the class $v(n)$ under the localization maps is given by*:

1. *If v does not divide n, then* $\mathrm{res}_w v(n) = 0$.
2. *For l special, there is a canonical G-equivariant isomorphism*

$$T\colon \bigoplus_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p \cong \bigoplus_{\lambda'|\lambda} \mathrm{Hom}(\mu_p(\mathbb{F}_{\lambda'}), E_p(\mathbb{F}_{\lambda'}))$$

such that, when l divides n, the homomorphism $T(\mathrm{res}_\lambda v(n))$ maps each $\mu_p(\mathbb{F}_{\lambda'})$ onto the subgroup of $E_p(\mathbb{F}_{\lambda'})$ generated by

$$\left(\frac{(l+1)\,\mathrm{Frob}_l - a_l}{p}\right) \mathrm{D}_{n/l}\,\alpha(n/l),$$

where we identify the point $\mathrm{D}_{n/l}\,\alpha(n/l)$ with its reduction mod λ'.

When v is a place of good reduction for E, part 1 follows from standard cohomological arguments, using the fact that $v(n)$ is inflated from a class in $H^1(H[n]/H, E)$ and that the w' are unramified in $H[n]/H$. The general case is proved in [2], prop. 6. 2. The isomorphism in part 2 is explicitly constructed in [2], prop. 6. 2, using local class field theory.

Part 2 of lemma 3. 4 will be applied via the following corollary:

Corollary 3. 5. *There is a G-equivariant isomorphism*

$$\bigoplus_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p \longrightarrow \bigoplus_{\lambda'|\lambda} E(\mathbb{F}_{\lambda'})/p$$

which sends $\mathrm{res}_\lambda v(n)$ *to* $\mathrm{res}_\lambda \mathrm{D}_{n/l}\,\alpha(n/l)$.

(Observe that $\mathrm{res}_\lambda \mathrm{D}_{n/l}\,\alpha(n/l)$ is well-defined in $\bigoplus_{\lambda'|\lambda} E(\mathbb{F}_{\lambda'})/p$.) Using the map T of lemma 3. 4, a choice of generators for $\mu_p(\mathbb{F}_{\lambda'})$ defines a (non-canonical) isomorphism

$$i\colon \bigoplus_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p \xrightarrow{\sim} \bigoplus_{\lambda'|\lambda} E_p(\mathbb{F}_{\lambda'}).$$

By choosing the generators appropriately, we may ensure that i sends $\mathrm{res}_\lambda v(n)$ to

$$\left(\frac{(l+1)\,\mathrm{Frob}_l - \mathrm{a}_l}{p}\right) \mathrm{res}_\lambda \mathrm{D}_{n/l}\,\alpha(n/l).$$

The operator $W = \left(\frac{(l+1)\,\mathrm{Frob}_l - \mathrm{a}_l}{p}\right)$ induces an isomorphism $E(\mathbb{F}_{\lambda'})/p \longrightarrow E_p(\mathbb{F}_{\lambda'})$. (This can be shown by decomposing $E(\mathbb{F}_{\lambda'})$ into eigencomponents for the action of the involution Frob_l. The trivial and non-trivial components are of order $l+1-a_l$ and $l+1+a_l$ respectively, and hence W is an isomorphism on the eigencomponents.) The composition $W^{-1}i$ gives the desired map.

4. Local Tate duality: generating $\mathrm{Sel}_p^{\mathrm{dual}}(E/H)$

Local Tate duality [6] gives a perfect pairing

$$\langle\ \rangle_{\lambda'} : E(H_{\lambda'})/p \times H^1(H_{\lambda'}, E)_p \to \mathbb{Z}/p\mathbb{Z}$$

which identifies $\bigoplus_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p$ with $(\bigoplus_{\lambda'|\lambda} E(H_{\lambda'})/p)^{\mathrm{dual}}$. The p-Selmer group $\mathrm{Sel}_p(E/H)$ consists of the cohomology classes $s \in H^1(H, E_p)$ whose restrictions $\mathrm{res}_v(s) \in H^1(H_v, E_p)$ belong to $E(H_v)/p$ for all places v of H, where we view $E(H_v)/p$ as a subspace of $H^1(H_v, E_p)$ by using the local p-descent exact sequence

$$0 \to E(H_v)/p \to H^1(H_v, E_p) \to H^1(H_v, E)_p \to 0.$$

Transposing the map:

$$\mathrm{res}_\lambda : \mathrm{Sel}_p(E/H) \to (\bigoplus_{\lambda'|\lambda} E(H_{\lambda'})/p),$$

and using the identification given by the local Tate pairing, we get a homomorphism

$$\Psi_l : \bigoplus_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p \to \mathrm{Sel}_p^{\mathrm{dual}}(E/H).$$

Let X_l denote the image of Ψ_l in $\mathrm{Sel}_p^{\mathrm{dual}}(E/H)$. We choose an auxiliary special prime l_1 and define the following Galois extensions of $\mathbb{Q}$:

$$\begin{aligned} F &= H[l_1]\,(E_p), \\ M_0 &= F(\alpha/p)^{\mathrm{Gal}}, \\ M_1 &= F(\mathrm{D}_{l_1}\alpha(l_1)/p)^{\mathrm{Gal}}, \\ M &= M_0 M_1, \end{aligned}$$

where the superscript "Gal" indicates taking normal closure over $\mathbb{Q}$. (The reasons for these definitions will become clear in the next section.) By lemma 2. 1,

$$\mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(H[l_1]/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) = \mathrm{Gal}(H[l_1]/\mathbb{Q}) \times \mathrm{GL}_2(\mathbb{F}_p).$$

The Galois groups V_0, V_1, and V of M_0, M_1, and M over F are $\mathbb{F}_p$-vector spaces equipped with a natural action of $\mathrm{Gal}(F/\mathbb{Q})$.

$$\begin{tikzcd}[arrows=dash]
 & M \arrow[dl] \arrow[dr] \arrow[dd, "V"] & \\
M_0 \arrow[dr, "V_0"'] & & M_1 \arrow[dl, "V_1"] \\
 & F \arrow[d] & \\
 & K &
\end{tikzcd}$$

Given a subset U of V, define

$$\mathscr{L}(U)=\{l \text{ rational prime } | \operatorname{Frob}_l(M/\mathbb{Q})=[\tau u], \text{ for } u\in U\}.$$

Note that every $l\in\mathscr{L}(U)$ is special.

Proposition 4. 1. *If U^+ generates V^+, then the X_l, with l ranging over $\mathscr{L}(U)$, generate* $\mathrm{Sel}_p^{\mathrm{dual}}(E/H)$.

Proof. Let s be in $\mathrm{Sel}_p(E/H)$. To prove the proposition, it suffices (by the non-degeneracy of the local Tate pairing) to show that $\mathrm{res}_\lambda(s)=0$ for all $l\in\mathscr{L}(U)$ implies $s=0$. Assume without loss of generality that s is in an eigenspace for the action of τ. Let us identify s with its image by restriction in:

$$H^1(F, E_p)^{\mathrm{Gal}(F/H)}\subset \mathrm{Hom}_{\mathrm{Gal}(H(E_p)/H)}(\mathrm{Gal}(\bar{M}/F), E_p),$$

where $\bar{M}$ denotes the maximal abelian extension of F whose Galois group is of exponent p. The restriction is injective because it can be written as a composition

$$H^1(H, E_p)\longrightarrow H^1(H(E_p), E_p)^{\mathrm{Gal}(H(E_p)/H)}\longrightarrow H^1(F, E_p)^{\mathrm{Gal}(H(E_p)/H)}.$$

Both arrows are injections: the kernel of the first is

$$H^1(H(E_p)/H, E_p)=H^1(\mathrm{GL}_2(\mathbb{F}_p), \mathbb{F}_p^2)=0,$$

and the kernel of the second is

$$\mathrm{Hom}_{\mathrm{Gal}(H(E_p)/H)}(\mathrm{Gal}(F/H(E_p)), E_p)=0.$$

Choose a minimal Galois extension $\tilde{M}$ of $\mathbb{Q}$ containing M with the property that s factors throught $\mathrm{Gal}(\tilde{M}/F)$. Let $x\in\mathrm{Gal}(\tilde{M}/F)$ be such that $x|_M\in U$. By the Chebotarev density theorem, we may find $l\in\mathscr{L}(U)$ such that $\operatorname{Frob}_l(\tilde{M}/Q)=[\tau x]$. The hypothesis $\mathrm{res}_\lambda(s)=0$ means that:

$$s(\operatorname{Frob}_{\lambda'}(\tilde{M}/F))=0,$$

for all primes λ' of $\tilde{M}$ above l. On the other hand, for some λ' above l,

$$\operatorname{Frob}_{\lambda'}(\tilde{M}/F)=(\tau x)^2=x^\tau x=(x^+)^2,$$

and hence $s(x^+)=0$. Since U^+ generates V^+, the homomorphism s vanishes on $\mathrm{Gal}(\tilde{M}/F)^+$. Hence the image of s is contained in an eigenspace of E_p for the action of τ. In particular, it is a proper $\mathrm{Gal}(H[l_1](E_p)/H[l_1])$-submodule of E_p. Hence it is trivial, since

$$\mathrm{Gal}(H[l_1](E_p)/H[l_1])=\mathrm{GL}_2(\mathbb{F}_p)$$

by lemma 2. 1. Therefore $s=0$.

5. Global Tate duality: relations in $\mathrm{Sel}_p^{\mathrm{dual}}(E/H)$

The tool for finding relations in $\mathrm{Sel}_p^{\mathrm{dual}}(E/H)$ is:

Proposition 5. 1. *If $s \in \mathrm{Sel}_p(E/H)$ and $\gamma \in H^1(H, E)_p$, then*

$$\sum_w \langle \mathrm{res}_w s, \mathrm{res}_w \gamma \rangle_w = 0,$$

where the sum is taken over all places of H.

This proposition is an immediate consequence of the global reciprocity law for elements in the Brauer group of H, taking into account the definition of the local Tate duality [6].

We suppose that the auxiliary special prime l_1 of the previous section satisfies the following property:

$$\mathrm{res}_{\lambda_1} e_{\bar\chi} \alpha \neq 0 \tag{4}$$

(and hence $\mathrm{res}_{\lambda_1} e_\chi \alpha \neq 0$, by lemma 2. 3.) Such an l_1 exists by the Chebotarev density theorem applied to the extension $H(E_p)(e_{\bar\chi}\alpha/p)/\mathbb{Q}$, using the hypothesis that $e_{\bar\chi}\alpha \neq 0$ in $E(H)/p$. By corollary 3. 5, condition (4) implies that

$$\mathrm{res}_{\lambda_1} e_{\bar\chi} v(l_1) \neq 0. \tag{5}$$

We need to examine the extensions M of F defined in the previous section. Let $M_0^{\bar\chi}$ (resp. $M_1^{\bar\chi}$, $M^{\bar\chi}$) denote the extensions

$$F(e_{\bar\chi}\alpha/p) \quad (\text{resp. } F(e_{\bar\chi}\mathrm{D}_{l_1}\alpha(l_1)/p),\ F(e_{\bar\chi}\alpha/p, e_{\bar\chi}\mathrm{D}_{l_1}\alpha(l_1)/p)).$$

Lemma 5. 2. *The extensions $M_0^{\bar\chi}$ and $M_1^{\bar\chi}$ are linearly disjoint over F.*

Proof. Indeed, linearly independent points in $E(H[l_1])/p$ give rise to linearly disjoint extensions over F. This is because the map

$$E(H[l_1])/p \to \mathrm{Hom}_{\mathrm{Gal}(F/H[l_1])}(V, E_p)$$

is injective, and linearly independent elements of $\mathrm{Hom}_{\mathrm{Gal}(F/H[l_1])}(V, E_p)$ cut out linearly disjoint extensions over F (use the fact $\mathrm{Gal}(F/H[l_1]) \cong \mathrm{GL}_2(\mathbb{F}_p)$, by lemma 2. 1). Hence, if $M_0^{\bar\chi}$ and $M_1^{\bar\chi}$ were not linearly disjoint over $\mathbb{F}$, we would have:

$$e_{\bar\chi}\mathrm{D}_{l_1}\alpha(l_1) = u e_{\bar\chi}\alpha \text{ in } E(H[l_1])/p,\ u \in \mathbb{F}_p^*.$$

The exact sequence

$$0 \to (E(H)/p)^{\bar{\chi}} \to (E(H[l_1])/p)^{G_{l_1},\bar{\chi}} \to H^1(G_{l_1}, E)_p^{\bar{\chi}} \to 0,$$

$$e_{\bar{\chi}} \mathrm{D}_{l_1} \alpha(l_1) \mapsto e_{\bar{\chi}} v(l_1)$$

and equation (5) show that this cannot happen.

We now describe the action of complex conjugation on $V^{\bar{\chi}}$, by using 2. 3 and the relation $\tau \mathrm{D}_l = -\mathrm{D}_l \tau$. There are two cases:

Case 1. $\chi = \bar{\chi}$. Complex conjugation τ acts on $V^\chi = V_0^\chi \times V_1^\chi = E_p \times E_p$ by

$$\tau(x, y)\tau = (\varepsilon\chi(\sigma_0)\,\tau x, \ -\varepsilon\chi(\sigma_0)\,\tau y).$$

Case 2. $\chi \neq \bar{\chi}$. Then τ does not stabilize V^χ or $V^{\bar{\chi}}$, but interchanges these two components. The action of τ on

$$V_0^\chi \times V_0^{\bar{\chi}} \times V_1^\chi \times V_1^{\bar{\chi}} \cong E_p^4$$

is given by:

$$\tau(x, y, z, w)\tau = (\varepsilon\bar{\chi}(\sigma_0)\,\tau y, \ \varepsilon\chi(\sigma_0)\tau x, \ -\varepsilon\bar{\chi}(\sigma_0)\tau w, \ -\varepsilon\chi(\sigma_0)\tau z).$$

We define a subset U of V as follows:

(6) Case 1: $U^\chi = \{(x, y) \mid \varepsilon\bar{\chi}(\sigma_0)\tau x + x$ and $-\varepsilon\bar{\chi}(\sigma_0)\tau y + y$ generate $E_p\}$,

(7) Case 2: $U^\chi \oplus U^\chi = \{(x, y, z, w) \mid \varepsilon\chi(\sigma_0)\tau x + y$ and $-\varepsilon\bar{\chi}(\sigma_0)\tau z + w$ generate $E_p\}$.

Note that, in both cases, U satisfies the property of prop. 4. 1. Let l be a prime in $\mathscr{L}(U)$:

Lemma 5. 3. *The local cohomology classes* $\mathrm{res}_\lambda e_{\bar{\chi}} v(l)$ *and* $\mathrm{res}_\lambda e_{\bar{\chi}} v(l l_1)$ *generate* $(\bigoplus_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p)^{\bar{\chi}}$.

Proof. Since $\bigoplus_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p \cong (\bigoplus_{\lambda'|\lambda} E(H_{\lambda'})/p)^{\mathrm{dual}}$ is isomorphic to two copies of the regular representation as an $\mathbb{F}_p[G]$-module, we have

$$\dim_{\mathbb{F}_p} (\bigoplus_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p)^{\bar{\chi}} = 2.$$

The isomorphism of corollary 3. 5 sends $\mathrm{res}_\lambda e_{\bar\chi} v(l)$ and $\mathrm{res}_\lambda e_{\bar\chi} v(ll_1)$ to $e_{\bar\chi}\alpha$ and $e_{\bar\chi} \mathrm{D}_{l_1}\alpha(l_1)$. The frobenius condition on l in the definitions (6), (7) of U show that these two points are linearly independent in $\bigoplus\limits_{\lambda'|\lambda} E(\mathbb{F}_{\lambda'})/p$. Hence $\mathrm{res}_\lambda e_{\bar\chi} v(l)$ and $\mathrm{res}_\lambda e_{\bar\chi} v(ll_1)$ are linearly independent, and span $(\bigoplus\limits_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p)^{\bar\chi}$. We recall that X_l is the image of $(\bigoplus\limits_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p)^{\mathrm{dual}}$ in $\mathrm{Sel}_p(E/H)^{\mathrm{dual}}$.

Proposition 5. 4. *The module $X_l^{\bar\chi}$ is of dimension* 1 *over $\mathbb{F}_p$.*

Proof. By prop. 5. 1 and part 1 of lemma 3. 4, the kernel of the map

$$(\bigoplus_{\lambda'|\lambda} H^1(H_{\lambda'}, E)_p)^{\bar\chi} \to X_l^{\bar\chi}$$

contains the non-trivial element $\mathrm{res}_\lambda e_{\bar\chi} v(l)$. On the other hand, $X_l^{\bar\chi} \neq 0$: it does not vanish identically on $e_{\bar\chi}\alpha$, since $\mathrm{res}_\lambda e_{\bar\chi}\alpha \neq 0$, and the local Tate pairing is non-degenerate. Hence $X_l^{\bar\chi}$ is one-dimensional.

Proposition 5. 5. *All of the $X_l^{\bar\chi}$ are equal, for $l \in \mathcal{L}(U)$.*

Proof. We show that $X_l^{\bar\chi} = X_{l_1}^{\bar\chi}$ for all $l \in \mathcal{L}(U)$. By prop. 5. 1 applied to the Heegner class $e_{\bar\chi} v(ll_1)$, we have:

$$\Psi_l(\mathrm{res}_\lambda e_{\bar\chi} v(ll_1)) + \Psi_{l_1}(\mathrm{res}_{\lambda_1} e_{\bar\chi} v(ll_1)) = 0 \text{ in } \mathrm{Sel}_p^{\mathrm{dual}}(E/H)^{\bar\chi}.$$

By lemma 5. 3, $\Psi_l(\mathrm{res}_\lambda e_{\bar\chi} v(ll_1))$ generates $X_l^{\bar\chi}$. Hence $\Psi_{l_1}(\mathrm{res}_{\lambda_1} e_{\bar\chi} v(ll_1))$ is non-zero and generates $X_{l_1}^{\bar\chi}$, and $X_l^{\bar\chi} = X_{l_1}^{\bar\chi}$.

6. Conclusion of the proof

Let δ denote the coboundary map $E(H)/p \to H^1(H, E_p)$. We can now show:

Theorem 6. 1. *The following are true*:

1. $\mathrm{Sel}_p(E/H)^\chi = \mathbb{F}_p \delta(e_\chi \alpha)$;
2. $E(H)/pE(H)^\chi = \mathbb{F}_p e_\chi \alpha$.

Proof. By prop. 4. 1, the $X_l^{\bar\chi}$ generate $\mathrm{Sel}_p^{\mathrm{dual}}(E/H)^{\bar\chi}$ when l ranges over $\mathcal{L}(U)$. On the other hand, each $X_l^{\bar\chi}$ is one-dimensional, and all the $X_l^{\bar\chi}$ are equal. Hence

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p^{\mathrm{dual}}(E/H)^{\bar\chi} = \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/H)^\chi = 1,$$

and $\mathrm{Sel}_p(E/H)^\chi$ is generated by the non-zero element $\delta(e_\chi\alpha)$. It follows that $(E(H)/p)^\chi$ is one-dimensional, generated by the Heegner point $e_\chi\alpha$.

Remarks. 1. In [1], Gross formulates his conjecture for abelian varieties which are quotients of the jacobian of the modular curve $X_0(N)$. The argument given above extends to this more general situation. For more details, see [5].

2. For applications of the formalism of Euler systems to different arithmetic situations, see [7].

References

[1] *B. H. Gross*, Heegner points on $X_0(N)$, Modular Forms, Chichester (1984), 87—106.

[2] *B. H. Gross*, Kolyvagin's work on modular elliptic curves, Proc. Durham symposium on L-functions and arithmetic, 1989, to appear.

[3] *B. H. Gross* and *D. B. Zagier*, Heegner points and derivatives of L-series, Invent. Math. **84** (1986), 225—320.

[4] *V. A. Kolyvagin*, Euler Systems, 1988, to appear in a Birkhäuser volume in honor of Grothendieck.

[5] *V. A. Kolyvagin* and *D. Y. Logachev*, Finiteness of the Shafarevich-Tate group and group of rational points for some modular abelian varieties, Algebra and analysis (USSR) **5** (1989).

[6] *J. S. Milne*, Arithmetic duality theorems, Perspectives in mathematics, London-New York 1986.

[7] *K. Rubin*, Appendix to S. Lang, Cyclotomic Fields I and II, combined second edition, Grad. Texts Math., Berlin-Heidelberg-New York 1990.

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

Columbia University, Department of Mathematics, New York, NY 10027, USA
Harvard University, Department of Mathematics, 1 Oxford St., Cambridge MA 02138, USA

Eingegangen 20. September 1989, in revidierter Fassung 7. Februar 1990