On the structure of Selmer groups

by

V.A. Kolyvagin

Max–Planck–Institut
für Mathematik
Gottfried–Claren–Straße 26
D–5300 Bonn 3

Federal Republic of Germany

Steklov Mathematical
Institute
Vavilova 42
117966 Moscow, GSP–1

USSR

MPI/90-70

On the structure of Selmer groups

by

V.A. Kolyvagin

The paper contains some applications of explicit cohomology classes (which the author has constructed earlier using Heegner points) to the theory of Selmer groups of a modular elliptic curve. Moreover some generalizations of Selmer groups are considered.

The case when the Heegner point over the imaginary–quadratic field has infinite order was studied in the work [1]. In fact, the theory of [1] is valid under a more general assumption which is, hypothetically, always true and discussed below.

For the convenience of the reader, we recall in part 1 the definitions of the Selmer groups and of our explicit cohomology classes, and formulate some of our results. The second part is essentially based on the work [1] and requires some familiarity with it. The second part contains proofs of results for $\ell \in B(E)$ (see below for notations), formulations of corresponding results for $\ell \notin B(E)$, and some global consequences of these results.

1. Selmer groups and explicit cohomology classes.

Let E be an elliptic curve over the field of rational numbers $\mathbb{Q}$. For an arbitrary abelian group A and a natural number M we let A_M denote the maximal M–torsion subgroup of A. We use the abbreviation $A/M = A/MA$. Let $E_M = E(\overline{\mathbb{Q}})_M$. If R is some extension of $\mathbb{Q}$, then the exact sequence $0 \longrightarrow E_M \longrightarrow E(\overline{R}) \longrightarrow E(\overline{R}) \longrightarrow 0$ induces the exact sequence

$$0 \longrightarrow E(R)/M \longrightarrow H^1(R,E_M) \longrightarrow H^1(R,E)_M \longrightarrow 0 . \qquad (1)$$

If L/R is a Galois extension, then $G(L/R)$ denotes its Galois group, $H^1(R,A) := H^1(G(\overline{R}/R),A)$ for a $G(\overline{R}/R)$–module A, $H^1(R,E) := H^1(R,E(\overline{R}))$.

Now let R be a finite extension of $\mathbb{Q}$. For a place v of R, we let $R(v)$ denote the corresponding completion of R, for $x \in H^1(R,E_M)$, $x(v)$ denotes its natural image in $H^1(R(v),E_M)$. The Selmer group $S(R,E_M) \subset H^1(R,E_M)$, by definition, consists of all elements x such that for all places v of R, $x(v) \in E(R(v))/M$. We recall that the Shafarevich–Tate group $Ш(R,E)$ is $\ker(H^1(R,E) \longrightarrow \prod_{\nu} H^1(R(\nu),E))$, so (1) induces the exact sequence:

$$0 \longrightarrow E(R)/M \longrightarrow S(R,E_M) \longrightarrow Ш(R,E)_M \longrightarrow 0 .$$

By the weak Mordell–Weil theorem, the Selmer group $S(K,E_M)$ is finite, by the Mordell–Weil theorem, $E(R) \simeq F \times \mathbb{Z}^{\operatorname{rank} E(R)}$, where $F \simeq E(R)_{\mathrm{tor}}$ is finite, $0 \leq \operatorname{rank} E(R) \in \mathbb{Z}$.

It is conjectured that $Ш(R,E)$ is finite. Only recently Rubin and the author proved this conjecture in some cases. I shall give some examples below.

We suppose further that E is modular. Let N be the conductor of E, $\gamma : X_0(N) \longrightarrow E$ be a modular parametrization. Here $X_0(N)$ is the modular curve over $\mathbb{Q}$ which parametrizes isomorphism classes of isogenies of elliptic curves with cyclic kernel of order N. We note that, according to the Taniyama–Shimura–Weil conjecture, every elliptic curve over $\mathbb{Q}$ is modular.

We now define explicit cohomology classes, we start from the definition of Heegner points. Let $K = \mathbb{Q}(\sqrt{D})$ be a field of discriminant D such that $0 > D \equiv \square \pmod{4N}$, $D \neq -3,-4$. We fix an ideal i_1 of the ring of integers O_1 of K such that $O_1/i_1 \simeq \mathbb{Z}/N\mathbb{Z}$ (such an ideal exists because of the conditions on D). If $\lambda \in \mathbb{N}$, let K_λ be the ring class field of K of conductor λ. It is a finite abelian extension of K. In particular, K_1 is the maximal abelian unramified extension of K. If $(\lambda,N) = 1$, we let $O_\lambda = \mathbb{Z} + \lambda O_1$, $i_\lambda = i_1 \cap O_\lambda$, z_λ will be the point of $X_0(N)$ rational over K_λ corresponding to the class of the isogeny $\mathbb{C}/O_\lambda \longrightarrow \mathbb{C}/i_\lambda^{-1}$ (here $i_\lambda^{-1} \supset O_\lambda$ is the inverse of i_λ in the group of proper O_λ–ideals). We set $y_\lambda = \gamma(z_\lambda) \in E(K_\lambda)$, $P_1 \in E(K)$ is the norm of y_1 from K_1 to K. The points y_λ, P_1 are called Heegner points.

Let $\mathcal{O}$ be $\mathrm{End}(E)$, $Q = \mathcal{O} \otimes \mathbb{Q}$. Let ℓ be a rational prime, $T = \varprojlim E_{\ell^n}$ be the Tate–module and $\hat{\mathcal{O}} = \mathcal{O} \otimes \mathbb{Z}_\ell$. We let $B(E)$ denote the set of odd rational primes which do not divide the discriminant of $\mathcal{O}$ and for which the natural representation $\rho : G(\overline{Q}/Q) \longrightarrow \mathrm{Aut}_{\hat{\mathcal{O}}} T$ is surjective. It is known (from the theory of complex multiplication and Serre's theory, resp.) that almost all (all but a finite number of) primes belong to $B(E)$. For example, if $\mathcal{O} = \mathbb{Z}$ and N is squarefree, then $\ell \geq 11$ belongs to $B(E)$ according to a theorem of Mazur.

In my paper "Euler systems" I proved that rank $E(K) = 1$ and $Ш(K,E)$ is finite when P_1 has infinite order. Then, in the paper "On the structure of Shafarevich–Tate groups" I determined the structure of $Ш(K,E)_{\ell^\infty}$ for $\ell \in B(E)$, under the same condition. Moreover, our explicit cohomology classes give information on the structure of $S(K,E_{\ell^n})$ under some more general condition (which, hypothetically, always holds). It will be discussed later, now we continue with the definition of the cohomology classes.

We fix a prime $\ell \in B(E)$. Further in the paper we use the notation p or p_k, where $k \in \mathbb{N}$, only for rational primes which do not divide N, remain prime in K and satisfy $n(p) := \mathrm{ord}_\ell(p+1,a_p) > 1$, where $a_p = p+1-[\tilde{E}(\mathbb{Z}/p)]$, $\tilde{E}$ is the reduction of E

modulo p. For natural r we let $\Lambda^r = \{p_1 \dots p_r\}$ denote the set of all products of r distinct such primes. The set Λ^0, by definition, consists only of $p_0 := 1$. We let $\Lambda = \bigcup_{r \geq 0} \Lambda^r$. If $r > 0$, $\lambda \in \Lambda^r$, we let $n(\lambda) = \min_{p \mid \lambda} n(p)$, $n(p_0) := \infty$.

The set T of explicit cohomology classes consists of $\tau_{\lambda,n} \in H^1(K,E_M)$, where λ runs through Λ, $1 \leq n \leq n(\lambda)$, $M = \ell^n$. To define these note that the condition $\ell \in B(E)$ implies the triviality of $E(K_\lambda)_{p^\infty}$. So, by a spectral sequence, the restriction homomorphism $\mathrm{res} : H^1(K,E_M) \longrightarrow H^1(K_\lambda,E_M)^{G(K_\lambda/K)}$ is an isomorphism and $\tau_{\lambda,n}$ is uniquely defined by the value $\mathrm{res}(\tau_{\lambda,n})$ which we will now exhibit.

We need more notations. We use standard facts on ring class fields. If $1 < \lambda \in \mathbb{N}$, then the natural homomorphism $G(K_\lambda/K_1) \longrightarrow \prod_{p \mid \lambda} G(K_p/K_1)$ is an isomorphism and we also have $G(K_\lambda/K_{\lambda/p}) \longrightarrow G(K_p/K_1) \xrightarrow{\sim} \mathbb{Z}/(p+1)$.

For each p, fix a generator $t_p \in G(K_p/K_1)$ and let t_p also denote the corresponding generator of $G(K_\lambda/K_{\lambda/p})$. Let $I_p = -\sum_{j=1}^{p} j t_p^j$, $I_\lambda = \prod_{p \mid \lambda} I_p \in \mathbb{Z}[G(K_\lambda/K_1)]$. Let $\mathbb{K}$ be the composite of $K_{\lambda'}$ when λ' runs through the set Λ. We let $J_\lambda = \Sigma \bar{g}$, where g runs through a fixed set of representatives of $G(\mathbb{K}/K)$ modulo $G(\mathbb{K}/K_1)$, $\bar{g}$ is the restriction of g to K_λ, so $\{\bar{g}\}$ is a set of representatives of $G(K_\lambda/K)$ modulo $G(K_\lambda/K_1)$. Let $P_\lambda = J_\lambda I_\lambda y_\lambda \in E(K_\lambda)$. Then

$$\mathrm{res}(\tau_{\lambda,n}) = P_\lambda (\mathrm{mod}\ ME(K_\lambda)) .$$

Now we formulate some of our results on the invariants of $S(K,E_M)$, see theorems 2, 3 of the second part for more general statements.

There is a bijective correspondence between the set of isomorphism classes of finite abelian ℓ–groups and the set of sequences of nonnegative integers $\{n_i\}$ such that $i \geq 1$,

$n_i \geq n_{i+1}$, $n_i = 0$ for all sufficiently large i . Concretely, $\{n_i\} \longleftrightarrow$ class of $\sum_i \mathbb{Z}/\ell^{n_i}$.

For a group A we let Inv(A) denote the sequence of invariants of class A , we call it the sequence of invariants of A .

Let $L(E,s)$ be the canonical L–function of E over $\mathbb{Q}$, $g = \mathrm{ord}_{s=1} L(E,s)$, $\epsilon = (-1)^{g-1}$.

If G is a group of order 2 with generator σ and A is a $\mathbb{Z}_\ell[G]$–module, then for $\nu \in \{0,1\}$ we let A^ν denote the submodule $(1-(-1)^\nu \epsilon\sigma)A$. Then A is the direct sum of A^0 and A^1 and σ acts on A^ν via multiplication by $(-1)^{\nu-1}\epsilon$.

Let $S_M = S(K,E_M)$, $G = G(K/\mathbb{Q})$. We are interested in the sequence $\mathrm{Inv}(S_M^\nu)$. For the formulation of the results we need some more notations.

Let $m'(\lambda)$ be the maximal positive integers such that $P_\lambda \in p^{m'(\lambda)} E(K_\lambda)$. We let $m(\lambda) = m'(\lambda)$ if $m'(\lambda) < n(\lambda)$, $m(\lambda) = \infty$ otherwise. Let $m_r = \min m(\lambda)$ when λ runs through Λ^r . In particular, ℓ^{m_0} is the maximal power of ℓ which divides P_1 , so $m_0 < \infty \Leftrightarrow P_1$ has infinite order. Let $m = \min_{r \geq 0} m_r$.

The condition $m < \infty$ is equivalent to the condition $T \neq \{0\}$. It is the generalization of the condition that P_1 has infinite order.

<u>Conjecture A</u>. $T \neq \{0\}$

Assume for the following that conjecture A is true for K . Let f be the minimal r such that $m_r < \infty$. In particular, $f = 0 \Leftrightarrow P_1$ has infinite order.

We let $(r) = 1$ if r is odd, $(r) = 0$ if r is even. We have

Theorem B. The inequality $m_r \geq m_{r+1}$ holds for $r \geq 0$. Let $n > m_f$, $c = f+\nu$, where $\nu \in \{0,1\}$ as usual. Then

$$\mathrm{Inv}(S_M^{(c)}) =$$

$$\underbrace{\cdots\cdots\cdots}_{\text{c values}} m_c-m_{c+1}, m_c-m_{c+1}, \ldots, m_{c+2k}-m_{c+2k+1}, m_{c+2k}-m_{c+2k+1}, \ldots$$

where $k = 0,1,\ldots$ Moreover, $\underbrace{\cdots\cdots\cdots}_{\text{c values}} = n,\ldots,n$ if $\nu = 1$.

For further results on the ordinary Selmer groups see the section 2 after the proof of theorem 3.

2. An application of the theory [1].

We use the notations and definitions from [1] with those already defined here.

First we note that all wordings and proofs in the basic text of [1] (§ 1–4) remain valid in the following situation provided one changes notations as is to be explained. We can use instead of the condition $m(1) < \infty$ (or, equivalently, that the Heegner point P_1 has infinite order) the weaker condition that there exists $\lambda_0 \in \Lambda^u$, where $u \geq 0$, such that $2m(\lambda_0) < n(\lambda_0)$. Then we let p_0 be some such λ_0, to be fixed throughout, and redefine Λ^r to be set of products of the form $p_0 p_1 \ldots p_r$ with distinct primes $p_1,\ldots,p_r$ that do not divide p_0. We let A^ν denote $(1-(-1)^{\nu+u}\epsilon\sigma)A$, where $\nu = 0$ or 1, as usual. Then consider $X = S_{p_0,p_0,n(p_0)-m(p_0)}/(\Pi_\ell \, \tau_{p_0,n(p_0)})$ (see § 2 of [1] for the definition of $S_{\lambda,\delta,n}$). In the case $p_0 = 1$, $S_{1,1,\infty} = \varinjlim S_{1,1,n}$ and $S_{1,1,n} =$

$S_{1,n} = S_M$ is the ordinary Selmer group of E over K of level $M = \ell^n$.

The notations n, n', n'' are used only for natural numbers $\leq n(p_0)$. Of course, the definitions in [1] must now be adapted to these new notations; for example, $m_r = m_r(p_0)$. Instead of the group $S_{1,n}$ the group $S_{p_0,p_0,n}$ must be used.

In the sequence (24) the group $(E(K)/M)^\nu$ must be replaced by the group $\mathbb{Z}/M'\ \tau_{p_0,n'}$, where $n' = n+m_0$. To use (38) with the isomorphism β_3^ν it is necessary to require that $3m(p_0) < n(p_0)$. When $p_0 = 1$ we return to the original setup.

Now generalize this further: We fix p_0 for which we require only that the sequence $\{m_r\}$ becomes eventually finite, $m_r < \infty$ for some $r \geq 0$. Or, equivalently, we require that $\{\tau_{\lambda,n}\} \neq \{0\}$ (λ runs through the set Λ). Then we let f denote the minimal r such that $m_r < \infty$ and if $p_0 > 1$ we require moreover that $\theta m_f < m(p_0)$, where $\theta = 2$ or 3 (as may be needed).

If A is a finite $\mathbb{Z}_\ell$–module, then, for $j \geq 1$, $\{\mathrm{inv}_j(A)\}$ denotes the sequence of invariants of A (see section 1 above). Finally (i) denotes the representative of $i(\mathrm{mod}\ 2)$ in the set $\{0,1\}$.

The following is a generalization of theorem 1:

Theorem 2. Let $r > f$, $n > m_f$, $n' = n+m_f$. Then the set $\Omega^r_{n'}$ is nonempty. Moreover, for all $\omega \in \Omega^{r-1}_{n'}$, there exists p_r such that the sequence $(\omega, p_r) \in \Omega^r_{n'}$. Let $\omega \in \Omega^r_{n'}$. Then, for $1 \leq j \leq r$, $\#\ \varphi_{p_j,n}(\tau_{\omega(j-1),n}) = \#\ \tau_{\omega(j-1),n}$ and if $\nu \in \{0,1\}$ is such that $r > f+\nu$, then, for $1+\nu+f \leq j \leq r$, $c = f+\nu$, we have

$$\#\ \varphi^{(c)}_{p_j,n}(\mathrm{mod}\ \Phi^{(c)}_{\omega(j-1),n}) = m_{(j,(c))-1} - m_{(j(c))} = \mathrm{inv}_j(S^{(c)}_{p_0,p_0,n}) .$$

The proof duplicates the proof of theorem 1 of [1] (the case $f = 0$) if we note that $\forall\, k \geq f\ \exists\ \lambda \in \Lambda^k$ such that $m(\lambda) = m_k$ and $\#\, T^{\nu}_{\lambda,n} = \mathrm{inv}_{k+1}(S^{\nu}_{p_0,p_0,n})$ for $\nu = 0$ and $\nu = 1$. This is a consequence of the analog of [1] proposition 8 (proved analogously) where condition 3) is replaced by the condition $\#\, \varphi^{\alpha}_{q,n'}(\mathrm{mod}\ \Phi^{\alpha}_{\delta,n'}) = \#\, T^{\alpha}_{\delta,n}$. ■

Furthermore we get

<u>Theorem 3</u>. $\exists\ p_0 p_1 \dots p_{2f+1} \in \Lambda^{2f+1}_{n'}$ such that for $1 \leq i \leq f+1$ $\mathrm{ord}_{\ell}\, \psi_{p_{f+1},n'}(\eta_i) = m_f$, where $\eta_i = \tau_{p_0 p_i \dots p_{i+f-1},n'}$. Then the subgroup of $S^{(f+1)}_{p_0\,,\,p_0,n}$ generated by η_i is isomorphic to the group $\sum_{i=1}^{f+1} \mathbb{Z}/M$. In particular, for $1 \leq j \leq f+1$ we have that $\mathrm{inv}_j(S^{(f+1)}_{p_0\,,\,p_0,n}) = n$.

<u>Proof</u>. Let $\eta_1' = p_0 p_1' \dots p_f' \in \Lambda^{f}_{m_f+1}$ is such that $m(\eta_1') = m_f$. By means of [1], proposition 8 we can, by induction, replace $p_1', \dots, p_f'$ by $p_1, \dots, p_f$ such that $\eta_1 = p_0 \dots p_f \in \Lambda^{f}_{n'}$ and $m(\eta_1) = m_f$ (this step is trivial when $f = 0$). Then we again use [1], proposition 8 (which is true for $r = k$ as well, see the proof) and by induction find a suitable η_i. Because of the proposition 1 and (for $f > 0$) the condition $\tau_{\lambda,n'} = 0\ \ \forall\, \lambda \in \Lambda^{f-1}_{n'}$ it then follows that $\eta_i \in S^{(f+1)}_{p_0\,,\,p_0,n}$ (we recall that complex conjugation acts on $\tau_{\lambda,n'}$ as multiplication by $(-1)^r \epsilon$ if $\lambda \in \Lambda^{r}_{n'}$). We set $R_{ij} = \varphi_{p_{f+j},n'}(\eta_i)$ for $1 \leq i, j \leq f+1$. Then $R_{ij} = 0$ for $j < i$ because (see § 1) $\psi_p(\tau_{\lambda,n'}) = 0$ when $p \mid \lambda$. We have $R_{ii} \in \ell^{m_f}(\mathbb{Z}/M)^*$. If $\sum \alpha_i \eta_i = 0$, then by applying to this identity the characters $\varphi_{p_{f+j}}$ for $j = 1, \dots, f+1$ we obtain that $\alpha_i \equiv 0 (\mathrm{mod}\ M)$. ■

Hence theorems 2 and 3 fully determine the sequence of invariants for $S^{(f+1)}_{p_0, p_0, n}$.

Further we suppose that $p_0 = 1$ and $\{\tau_{\lambda,n}\} \neq \{0\}$. The group $S^\nu = \varinjlim S^\nu_{\ell^n}$ is isomorphic to a direct sum of $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{r^\nu}$ and a finite group $\mathcal{S}^\nu$. The group $S^\nu_{\ell^n}$ coincides with the maximal ℓ^n–torsion subgroup of S^ν and with the Selmer group of level ℓ^n for E^ν over $\mathbb{Q}$. Here E^ν is E if $(-1)^{\nu+1}\epsilon = 1$, and E^ν is the form of E over K otherwise. Apriori, rank $E^\nu(\mathbb{Q}) \leq r^\nu$, and equality is equivalent to the statement that $Ш(\mathbb{Q},E^\nu)_{\ell^\infty}$ is a finite group, which will then be isomorphic to $\mathcal{S}^\nu$. We have

Theorem 4. $r^{(f+1)} = f+1$, $r^{(f)} \leq f$ and $f-r^{(f)}$ is even. For $j \geq 1+\nu+f$ $\mathrm{inv}_{j-r^{(c)}}(\mathcal{S}^{(c)}) = m_{(j,(c))-1} - m_{(j,(c))}$.

Proof. Because of theorems 2, 3 it is enough to explain why $f-r^{(f)}$ is even. From theorem 2 we have that the (parity of nonzero invariants of $\mathcal{S}^{(f)}$ with index $\geq f+1-r^{(f)}$) is even, but the common parity of nonzero invariants of $\mathcal{S}^{(f)}$ is even because of the existence of a non–degenerate alternating Cassels form on $\mathcal{S}^{(f)}$. Hence $f-r^{(f)}$ is even.

Let $g^\nu = \mathrm{ord}_{s=1} L(E^\nu,s)$. We recall that according to the conjecture of Birch and Swinnerton–Dyer, $g^\nu = \mathrm{rank}\, E^\nu(\mathbb{Q})$. Since $(-1)^{g^\nu} = -\epsilon$ or ϵ according as $E^\nu = E$ or E^ν = form of E over K , we have from theorem 4:

Theorem 5. $r^\nu - g^\nu$ is even for $\nu = 0$ and $\nu = 1$. ∎

If f and m are known, then we have an algorithm (see the beginning of the paper, and § 4 of [1]) for computing some n' and $q = p_{f+1} \cdots p_{2f+1} \in \Lambda_{n'}^{f+1}$ such that $n' > 3m(q)$, $\min_r m_r(q) = m$, with a parametrization of $\mathscr{Y} = S_{q,q,n}^{(f+1)}$, where $n = n' - m(q)$, by finite linear combinations of elements of $\{\tau_{\lambda,n'}\}$. Moreover such a procedure can be combined with the selection of $p_0 \cdots p_f$ $(p_0 = 1)$ such that $p_0 \cdots p_{2f+1} \in \Lambda_{n'}^{2f+1}$ and $\mathrm{ord}_\ell R_{ii} = \mathrm{ord}_\ell(m(\eta_i)) = n' - n$ for $1 \leq i \leq f+1$. Then (see the proof of theorem 3) the group $\mathscr{Z} \subset S_M^{(f+1)}$ generated by η_i is isomorphic to the group $\sum_{i=1}^{f+1} \mathbb{Z}/M$ and its pairing with $\sum_{i=1}^{f+1} \mathbb{Z}/M\, \varphi_{p_{i+f},n}^{(f+1)}$ is non–degenerate. Hence $S_M^{(f+1)}$ is the direct sum of $\mathscr{Z}$ and $\mathscr{W} = S_M^{(f+1)} \cap \mathscr{Y} \simeq \mathscr{S}^{(f+1)}$. The parametrization for $\mathscr{Y}$ induces a parametrization for $\mathscr{W}$ and, as a consequence, we obtain its complete structure. In particular, we have an algorithm for computing the sequence of invariants for $\mathscr{S}^{(f+1)}$.

By using proposition 9 of [1] (with the condition $n > m_0$ replaced by $n > m_{r-1}$) we have that for $p_1 \cdots p_j \in \Lambda_n^j$ with $m(p_1 \cdots p_j) = m < n$, the characters $\varphi_{p_1,n}^{(j)}, \ldots, \varphi_{p_j,n}^{(j)}$ generate $\mathrm{Hom}(S_M^{(j)}, \mathbb{Z}/M)$. So we can apply this to the effective solution of the problem when a principal homogeneous space over E has a rational point, in the same vein as at the end of [1] for the case $f = 0$.

We recall that we considered $\ell \in B(E)$ (see section 1 for the definition of $B(E)$). For $\ell \notin B(E)$ the theory in [1] and above holds with modifications in the manner of [2]. Let ℓ now be an arbitrary rational prime. In particular, $\tau_{\lambda,n} \in H^1(K, E_M)$ is defined for all $\lambda \in \Lambda_{n+k_0}$ [1)],

---

[1)] In [3] $\tau_{\lambda,n}$ is defined for all $\lambda \in \Lambda_n$ as in the case $\ell \in B(E)$.

---

where $\ell^{k_0/2} E(\mathbb{K})_{\ell^\infty} = 0$, $\mathbb{K}$ the composite of K_λ for all $\lambda \in \Lambda$ ($k_0 = 0$ for

$\ell \in B(E)$).

We let $U_M \subset E(K)/M$, H, $S \subset H$ denote respectively the groups $E(K)_{tor}/M$, $\varinjlim H^1(K,E_M)$, $\varinjlim S(K,E_M)$. We have the exact sequence $0 \longrightarrow U_M \longrightarrow H^1(K,E_M) \longrightarrow H_M \longrightarrow E(K)_M \longrightarrow 0$ and we identify the group $H^1(K,E_M)/U_M$ with its image in H_M. We recall that, for $\ell \in B(E)$, $E(K)_{\ell^\infty} = 0$ and we identified $H^1(K,E_M)$, $S(K,E_M)$ with H_M, S_M respectively. We let $\tau'_{\lambda,n}$ be the image of $\tau_{\lambda,n}$ in H_M, and for $n \geq 1$, $k \geq k_0$, $r \geq 0$, $V^r_{n,k}$ is the subgroup of H_M generated by $\tau'_{\lambda,n}$ when λ runs through $\Lambda^r_{n,k}$. We say that $\{\tau_{\lambda,n}\}$ is a strong nonzero system if $\exists\, r \geq 0$ such that

$$\forall\, k \geq k_0 \; \exists\, n \,|\, V^r_{n,k} \neq 0 . \tag{2}$$

There exists $k(r) \geq k_0$ such that the condition (2) is equivalent to the condition that $\exists\, n \,|\, V^r_{n,k(r)} \neq 0$. We know that, for $\ell \in B(E)$, $k(r) = 0$ satisfies this property. We now formulate

<u>Conjecture 1</u>. For all ℓ, $\{\tau_{\lambda,n}\}$ is a strong nonzero system.

For $\ell \in B(E)$, this is equivalent to the statement that $\{\tau_{\lambda,n}\} \neq 0$.

<u>Conjecture 2</u>. $m \neq 0$ for only a finite set of primes in $B(E)$.

Apparently, theorem 4 is closely connected with the Birch and Swinnerton–Dyer conjecture (see [1] for the case $f = 0$). For example, it would be natural to find that $f+1$ is equal to the order of zero at $s = 1$ of an ℓ–adic L–function for $E^{(f+1)}$ (when such a function exists), and (more difficult ?) to find that $f+1 = g^{(f+1)}$.

If A is a $\mathbb{Z}[1,\sigma]$–module and $\nu \in \{0,1\}$, then $A^\nu := \{b \in A \mid \sigma b = (-1)^{\nu+1}\epsilon b\}$.

Let $SD = \ell^n S$, so $SD^\nu \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{r^\nu}$. Let $\ell \in B(E)$. Because of the relation $\ell^k \tau'_{\lambda,n+k} = \tau'_{\lambda,n}$ (which is true for an arbitrary ℓ) and the relation $\ell^{m_{f+1}} \mathscr{S}^{(f+1)} = 0$, it then follows that $V^f_{n,m_{f+1}} \subset SD^{(f+1)}_M$. From theorem 3 we have that $\forall k \geq m_f$ $V^f_{n,k} = \ell^{m_f} SD^{(f+1)}$. For arbitrary ℓ $\exists k_1, k_2$ such that for $k \geq k_1$ $\ell^{k_2} SD^{(f+1)}_M \subset V^f_{n,k} \subset SD^{(f+1)}_M$.

Interpolating the situation of the case $f = 0$ we formulate

<u>Conjecture$_\ell$3</u>. There exist $\nu \in \{0,1\}$ and a subgroup $V \subset (E(K)/E(K)_{tor})^\nu$ such that $1 \leq \text{rank } V \equiv \nu (\text{mod } 2)$ and for all sufficiently large k and all n, one has $V^a_{n,k} = V(\text{mod } M(E(K)/E(K)_{tor}))$, where $a = \text{rank } V-1$.

Conjecture 3, by definition, is the union $\forall \ell$ of conjectures$_\ell$3 with a universal V (independent of ℓ). We note that such V is uniquely determined (by the usual description of a lattice over $\mathbb{Z}$ by its completions) if it exists.

It is clear that $2V \subset E^\nu(\mathbb{Q})/E^\nu(\mathbb{Q})_{tor}$.

For the following implications we use the arguments above with the theorems 2–5 (with a natural modification for $\ell \notin B(E)$).

First, conjecture$_\ell$3 implies that $\{\tau_{\lambda,n}\}$ is a strong nonzero system with $f = a$ (for the last statement we use the propositions 1, 2, 5 of [1]), $\text{rank } E^\nu(\mathbb{Q}) = \text{rank } V$, $r^{1-\nu} < \text{rank } V$, $Ш(\mathbb{Q},E^\nu)_{\ell^\infty}$ is finite. Moreover, if $\ell \in B(E)$, then $V \otimes \mathbb{Z}_\ell =$

$\ell^{m_f}(E^\nu(\mathbb{Q}) \otimes \mathbb{Z}_\ell)$, $[\text{Ш}(\mathbb{Q},E^\nu)_{\ell^\infty}] \mid \ell^{2m_f}$, $\ell^{m_f}\text{Ш}(\mathbb{Q},E^\nu)_{\ell^\infty} = 0$, $\operatorname{rank} E^\nu(\mathbb{Q}) \equiv g^\nu \equiv \nu(\mathrm{mod}\ 2)$, $r^{1-\nu} \equiv g^{1-\nu} \equiv 1-\nu(\mathrm{mod}\ 2)$.

Conjecture$_\ell$3 is equivalent to the statement: $\{\tau_{\lambda,n}\}$ is a strong nonzero system and $\text{Ш}(\mathbb{Q},E^{(f+1)})_{\ell^\infty}$ is finite.

We note that $\exists\, k_3$, which is zero for $\ell \in B(E)$, such that if the condition from conjecture$_\ell$3 holds with some $k' \geq k_3$ then it holds for all $k \geq k'$.

From conjecture 3 we have, with the union of consequences from conjectures$_\ell$3, that conjecture 2 holds and $\text{Ш}(\mathbb{Q},E^\nu)$ is finite. Conjecture 3 is equivalent to the statement: conjectures 1, 2 hold, f+1 is independent of ℓ, $\text{Ш}(\mathbb{Q},E^{(f+1)})$ is finite; for only a finite set of $\ell \in B(E)$ $\operatorname{inv}_{f+1-r^{1-\nu}}\mathcal{S}^{1-\nu} \neq 0$. In particular, conjecture 3 holds when conjectures 1, 2 hold and $\text{Ш}(K,E)$ is finite.

Of course, for the case that the Heegner point P_1 has infinite order (f=0) conjecture 3 holds with $\nu = 1$, $V = \mathbb{Z}P_1(\mathrm{mod}\ E(K)_{tor})$.

Recall that $g = \operatorname{ord}_{s=1}L(E,s)$. It is known that there exists an imaginary quadratic field K such that $g^0+g^1-g = 0$ or 1 according as g is even or odd. For $g \leq 1$ it is known that $\operatorname{rank} E(\mathbb{Q}) = g$ and $\text{Ш}(\mathbb{Q},E)$ is finite. Let $g > 1$ and for K as above $g = g^{\nu'}$. Then $\operatorname{ord}_{s=1}L(E,K,s) = g^{\nu'}+g^{1-\nu'} > 1$, so P_1 has finite order by the formula of Gross and Zagier. Suppose that for K conjecture$_\ell$3 holds for some ℓ. Then $\nu = \nu'$ because otherwise $g^{1-\nu'} = f+1 > 1$ but $g^{1-\nu'} \leq 1$. So we have for $E = E^\nu$ all consequences of the conjecture$_\ell$3 (see above), in particular, that $\operatorname{rank} E(\mathbb{Q}) = \operatorname{rank} V$ and $\text{Ш}(\mathbb{Q},E)_{\ell^\infty}$ is finite. If conjecture 3 holds for K, we also have that $\text{Ш}(\mathbb{Q},E)$ is finite and $\operatorname{rank} E(\mathbb{Q}) \equiv g(\mathrm{mod}\ 2)$. Of course, $\operatorname{rank} E(\mathbb{Q}) = g$ if the equality $g = \operatorname{rank} V$ holds.

References.

[1] V.A. Kolyvagin, On the structure of Shafarevich–Tate groups. Proceedings of USA—USSR Symposium on Algebraic Geometry, Chicago, 1989. Springer Lecture Notes (to appear)

[2] V.A. Kolyvagin, Euler systems, Birkhäuser volume in honor of Grothendieck.

[3] V.A. Kolyvagin, On the Mordell–Weil group and the Shafarevich–Tate group of modular elliptic curves, Proceedings of ICM–90 in Kyoto (to appear).