Math. Ann. 291, 253–259 (1991)

Mathematische Annalen

On the structure of Selmer groups *

V. A. Kolyvagin

Steklov Mathematical Institute, Vavilova 42, SU-117966 Moscow, GSP-1, USSR

Received June 29, 1990; in revised form April 15, 1991

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 $l \in B(E)$ (see below for notations), formulations of corresponding results for $l \notin B(E)$, 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 $E_M = E(\bar{\mathbb{Q}})_M$. If R is some extension of $\mathbb{Q}$, then the exact sequence $0 \to E_M \to E(\bar{R}) \to E(\bar{R}) \to 0$ induces the exact sequence

$$0 \to E(R)/M \to H^1(R, E_M) \to H^1(R, E)_M \to 0. \tag{1}$$

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

---

* This paper was partly prepared during my stay at the Max-Planck-Institut für Mathematik in Bonn. I want to express my gratitude for the support and the hospitality provided by this institute

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 $\ker(H^1(R, E) \to \prod_v H^1(R(v), E))$, so (1) induces the exact sequence:

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

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, $0 \leqq \operatorname{rank} E(R) \in \mathbb{Z}$.

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, $\gamma: X_0(N) \to E$ 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 $\mathbb{C}/O_\lambda \to \mathbb{C}/i_\lambda^{-1}$ (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 $\operatorname{End}(E)$, $Q = \mathcal{O} \otimes \mathbb{Q}$. Let l be a rational prime, $T = \varprojlim E_{l^n}$ be the Tate-module and $\hat{\mathcal{O}} = \mathcal{O} \otimes \mathbb{Z}_l$. 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 $\varrho: G(\bar{Q}/Q) \to \operatorname{Aut}_{\hat{\mathcal{O}}} T$ 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 $l \geqq 11$ belongs to $B(E)$ according to a theorem of Mazur.

In my paper "Euler systems" I proved that $\operatorname{rank} E(K) = 1$ 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 $Ш(K, E)_{l^\infty}$ for $l \in B(E)$, under the same condition. Moreover, our explicit cohomology classes give information on the structure of $S(K, E_{l^n})$ 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 $l \in B(E)$. 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 $n(p) := \operatorname{ord}_l(p+1, a_p) > 1$, 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 $\Lambda = \bigcup_{r \geqq 0} \Lambda^r$. 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, $1 \leqq n \leqq n(\lambda)$, $M = l^n$. To define these note that the condition $l \in B(E)$

implies the triviality of $E(K_\lambda)_{l^\infty}$. So, by a spectral sequence, the restriction homomorphism $\mathrm{res}: H^1(K, E_M) \to H^1(K_\lambda, E_M)^{G(K_\lambda/K)}$ 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 $G(K_\lambda/K_1) \to \prod_{p|\lambda} G(K_p/K_1)$ is an isomorphism and we also have $G(K_\lambda/K_{\lambda/p}) \to G(K_p/K_1) \xrightarrow{\sim} \mathbb{Z}/(p+1)$.

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 $I_p = -\sum_{j=1}^{p} j t_p^j$, $I_\lambda = \prod_{p|\lambda} I_p \in \mathbb{Z}[G(K_\lambda/K_1)]$. 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

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

Now we formulate some of our results on the invariants of $S(K, E_M)$, see Theorems 2 and 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 $i \geqq 1$, $n_i \geqq n_{i+1}$, $n_i = 0$ for all sufficiently large i. Concretely, $\{n_i\} \leftrightarrow$ class of $\sum_i \mathbb{Z}/l^{n_i}$. For a group A we let $\mathrm{Inv}(A)$ 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 $\mathbb{Q}$, $g = \mathrm{ord}_{s=1} L(E,s)$, $\varepsilon = (-1)^{g-1}$.

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

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

Let $m'(\lambda)$ be the maximal nonnegative integer such that $P_\lambda \in l^{m'(\lambda)} E(K_\lambda)$. 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 $m = \min_{r \geqq 0} m_r$.

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.

Conjecture A. $T \neq \{0\}$.

Assume for the following that Conjecture A is true (for the field K and the prime l). 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 1. *Suppose Conjecture A is true. Then the inequality $m_r \geqq m_{r+1}$ holds for $r \geqq 0$. Let $n > m_f$, $c = f + v$, where $v \in \{0,1\}$ as usual. Then*

$$\mathrm{Inv}(S_M^{(c)}) = \underbrace{\ldots\ldots}_{c \text{ values}}, m_c - m_{c+1}, m_c - m_{c+1}, \ldots, m_{c+2k} - m_{c+2k+1}, m_{c+2k} - m_{c+2k+1}, \ldots,$$

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

Theorem 1 is a special case of Theorems 2 and 3, see Sect. 2. For further results on the ordinary Selmer groups see the Sect. 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, Sects. 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 $u \geqq 0$, 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 $p_0 p_1 \dots p_r$ with distinct primes $p_1, \dots, p_r$ that do not divide p_0. We let A^v denote $(1-(-1)^{v+u}\varepsilon\sigma)A$, where $v=0$ or 1, as usual. Then consider $X=S_{p_0,p_0,n(p_0)-m(p_0)}/(\mathbb{Z}_l \tau_{p_0,n(p_0)})$ (see Sect. 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 $M=l^n$.

The notations n, n', n'' are used only for natural numbers $\leqq n(p_0)$. 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 $(E(K)/M)^v$ 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^v 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 $r \geqq 0$. 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 $\mathbb{Z}_l$-module, then, for $j \geqq 1$, $\{\mathrm{inv}_j(A)\}$ denotes the sequence of invariants of A (see Sect. 1 above). Finally, (i) denotes the representative of $i \pmod 2$ in the set $\{0,1\}$.

The following is a generalization of Theorem 1 in [1].

Theorem 2. *Suppose Conjecture A is true. 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 $1 \leqq j \leqq r$, $\#\varphi_{p_j,n}(\tau_{\omega(j-1),n}) = \#\tau_{\omega(j-1),n}$ and if $v \in \{0,1\}$ is such that $r>f+v$, then, for $1+v+f \leqq j \leqq r$, $c=f+v$, 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 $\forall k \geqq f\, \exists \lambda \in \Lambda^k$ such that $m(\lambda)=m_k$ and $\#T^v_{\lambda,n}=\mathrm{inv}_{k+1}(S^v_{p_0,p_0,n})$ for $v=0$ and $v=1$. 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

Theorem 3. *Suppose Conjecture A is true. Then $\exists p_0 p_1 \dots p_{2f+1} \in \Lambda^{2f+1}_{n'}$ such that for $1 \leqq i \leqq f+1$ $\mathrm{ord}_l \psi_{p_{f+1},n'}(\eta_i)=m_f$, 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 *$1 \leqq j \leqq f+1$ we have that $\mathrm{inv}_j(S^{(f+1)}_{p_0,p_0,n})=n$.*

Proof. 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 [1, 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 $(-1)^r\varepsilon$ if $\lambda \in \Lambda^r_{n'}$). We set $R_{ij} = \varphi_{p_{f+j},n'}(\eta_i)$ for $1 \leqq i, j \leqq f+1$. Then $R_{ij} = 0$ for $j<i$ because (see [1, Sect. 1]) $\psi_p(\tau_{\lambda,n'}) = 0$ when $p \mid \lambda$. We have $R_{ii} \in l^{m_f}(\mathbb{Z}/M)^*$. 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 $S^\nu = \varinjlim S^\nu_{l^n}$ is isomorphic to a direct sum of $(\mathbb{Q}_l/\mathbb{Z}_l)^{r^\nu}$ and a finite group $\mathscr{X}^\nu$. The group $S^\nu_{l^n}$ 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 $(-1)^{\nu+1}\varepsilon = 1$, and E^ν is the form of E over K otherwise. A priori, $\operatorname{rank} E^\nu(\mathbb{Q}) \leqq r^\nu$, and equality is equivalent to the statement that $\text{Ш}(\mathbb{Q}, E^\nu)_{l^\infty}$ is a finite group, which will then be isomorphic to $\mathscr{X}^\nu$. We have

Theorem 4. *Suppose Conjecture A is true. Then* $r^{(f+1)} = f+1$, $r^{(f)} \leqq f$, *and* $f - r^{(f)}$ *is even. For* $j \geqq 1 + \nu + f$ $\operatorname{inv}_{j-r^{(c)}}(\mathscr{X}^{(c)}) = m_{(j,(c))-1} - m_{(j,(c))}$.

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

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

Theorem 5. *Suppose Conjecture A is true. Then* $r^\nu - g^\nu$ *is even for* $\nu = 0$ *and* $\nu = 1$. □

If f and m are known, then we have an algorithm (see the beginning of this section, and Sect. 4 of [1]) for computing some n' and $q = p_{f+1} \dots p_{2f+1} \in \Lambda^{f+1}_{n'}$ such that $n' > 3m(q)$, $\min_r m_r(q) = m$, with a parametrization of $\mathscr{Y} = S^{(f+1)}_{q,q,n}$, 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 $p_0 \dots p_f$ ($p_0 = 1$) such that $p_0 \dots p_{2f+1} \in \Lambda^{2f+1}_{n'}$ and $\operatorname{ord}_l R_{ii} = \operatorname{ord}_l(m(\eta_i)) = n' - n$ for $1 \leqq i \leqq f+1$. Then (see the proof of Theorem 3) the group $\mathscr{Z} \subset S^{(f+1)}_M$ generated by η_i is isomorphic to the group $\sum_{i=1}^{f+1} \mathbb{Z}/M$ and its pairing with $\sum_{i=1}^{f+1} \mathbb{Z}/M \varphi^{(f+1)}_{p_{i+f},n}$ is non-degenerate. Hence $S^{(f+1)}_M$ is the direct sum of $\mathscr{Z}$ and $\mathscr{W} = S^{(f+1)}_M \cap \mathscr{Y} \simeq \mathscr{X}^{(f+1)}$. 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 $\mathscr{X}^{(f+1)}$.

By using Proposition 9 of [1] (with the condition $n > m_0$ replaced by $n > m_{r-1}$) we have that for $p_1 \dots p_j \in \Lambda^j_n$ with $m(p_1 \dots p_j) = m < n$, the characters $\varphi^{(j)}_{p_1,n}, \dots, \varphi^{(j)}_{p_j,n}$ generate $\operatorname{Hom}(S^{(j)}_M, \mathbb{Z}/M)$. 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 $l \in B(E)$ [see Sect. 1 for the definition of $B(E)$]. For $l \notin B(E)$ 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], where $l^{k_0/2}E(\mathbb{K})_{l^\infty}=0$, $\mathbb{K}$ the composite of K_λ for all $\lambda \in \Lambda$ [$k_0=0$ for $l \in B(E)$].

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

$$\forall k \geqq k_0 \ \exists n \mid V^r_{n,k} \neq 0 . \tag{2}$$

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

Conjecture B. *For all l, $\{\tau_{\lambda,n}\}$ is a strong nonzero system.*

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

Conjecture C. *$m \neq 0$ for only a finite set of primes in $B(E)$.*

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

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

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

Conjecture$_l$ D. *There exist $v \in \{0,1\}$ and a subgroup $V \subset (E(K)/E(K)_{\mathrm{tor}})^v$ such that $1 \leqq \operatorname{rank} V \equiv v (\operatorname{mod} 2)$ and for all sufficiently large k and all n, one has $V^a_{n,k} = V(\operatorname{mod} M(E(K)/E(K)_{\mathrm{tor}}))$, where $a = \operatorname{rank} V - 1$.*

Conjecture D, by definition, is the union $\forall l$ of Conjectures$_l$ D 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) of it exists.

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

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

First, Conjecture$_l$ D implies that $\{\tau_{\lambda,n}\}$ is a strong nonzero system with $f=a$ (for the last statement we use the Propositions 1, 2, and 5 of [1]), $\operatorname{rank} E^v(\mathbb{Q}) = \operatorname{rank} V$, $r^{1-v} < \operatorname{rank} V$, $Ш(\mathbb{Q}, E^v)_{l^\infty}$ is finite. Moreover, if $l \in B(E)$, then $V \otimes \mathbb{Z}_l = l^{m_f}(E^v(\mathbb{Q}) \otimes \mathbb{Z}_l)$, $[Ш(\mathbb{Q}, E^v)_{l^\infty}] \mid l^{2m_f}$, $l^{m_f} Ш(\mathbb{Q}, E^v)_{l^\infty}=0$, $\operatorname{rank} E^v(\mathbb{Q}) \equiv g^v \equiv v (\operatorname{mod} 2)$, $r^{1-v} \equiv g^{1-v} \equiv 1 - v (\operatorname{mod} 2)$.

---

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

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

We note that $\exists k_3$, which is zero for $l \in B(E)$, such that if the condition from Conjecture$_l$ D holds with some $k' \geqq k_3$ then it holds for all $k \geqq k'$.

From Conjecture D we have, with the union of consequences from Conjectures$_l$ D, that Conjecture C holds and Ш$(\mathbb{Q}, E^{\nu})$ is finite. Conjecture D is equivalent to the statement: Conjectures B and C hold, $f+1$ is independent of l, Ш$(\mathbb{Q}, E^{(f+1)})$ is finite; for only a finite set of $l \in B(E)$ $\mathrm{inv}_{f+1-r^{1-\nu}}\mathscr{X}^{1-\nu} \neq 0$. In particular, Conjecture D holds when Conjectures B and C hold and Ш(K, E) is finite.

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

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

References

1. Kolyvagin, V.A.: On the structure of Shafarevich-Tate groups. Proceedings of USA-USSR Symposium on Algebraic Geometry, Chicago, 1989 (Lect. Notes Math. vol. 1479) Berlin Heidelberg New York: Springer 1991
2. Kolyvagin, V.A.: Euler systems, Birkhäuser volume in honor of Grothendieck. Progr. Math. **87**, 435–483 (1990)
3. Kolyvagin, V.A.: On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves. Proceedings of ICM-90 in Kyoto (to appear)