On the Mordell–Weil group and the Shafarevich–Tate group of modular elliptic curves

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/90-69

On the Mordell–Weil group and the Shafarevich–Tate group of modular elliptic curves

Victor Alecsandrovich Kolyvagin

The main purpose of this paper is to describe some recent results pertaining to the diophantine analysis of elliptic curves. A new element is an extension of the set of explicit cohomology classes see section 2.

1. The Conjecture of Birch and Swinnerton–Dyer and the Hypothesis of Finiteness of the Shafarevich–Tate group.

Let E be an elliptic curve defined over the field of rational numbers $\mathbb{Q}$, for example, by its Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$. Let R be a finite extension of $\mathbb{Q}$. We are interested in the group $E(R)$ called the Mordell–Weil group of E over R and the Shafarevich-Tate group $Ш(R,E)$. The group $Ш(R,E)$ is, by definition, $\ker(H^1(R,E) \longrightarrow \prod_v H^1(R(v),E))$, where v runs through the set of all places (equivalence classes of valuations) of R, $R(v)$ is the v–adic completion of R. For an arbitrary extension L of $\mathbb{Q}$, we let $\bar{L}$ denote an algebraic closure of L. If V/L is a Galois extension, then $G(V/L)$ denotes its Galois group, and $H^1(L,E) = H^1(G(\bar{L}/L),E(\bar{L}))$.

Let Y be some set of algebraic curves over R. By definition, the Hasse principle holds for Y, if for all $X \in Y$ one has: $X(R)$ is nonempty $\Leftrightarrow$ $X(R(v))$ is nonempty for each v. The group $Ш(R,E)$ is the obstacle to the Hasse principle for the set $Y(R,E)$

of main principal homogeneous spaces over E defined over R . In particular, the Hasse principle holds for Y(R,E) if and only if the group Ш(R,E) is trivial.

According to the Mordell–Weil theorem, $E(R) \simeq F \times \mathbb{Z}^{r(R,E)}$, where $F \simeq E(R)_{tor}$ is a finite group, and r(R,E) is a nonnegative integer called the rank of E over R . Concerning the group Ш(R,E) , it is conjectured that it is finite. In general, it is known that Ш(R,E) is a torsion group (being a subgroup of the torsion group $H^1(R,E)$) and for a natural M its subgroup $Ш(R,E)_M$ is finite. If A is an abelian group, we let A_M denote its subgroup of all elements of exponents M . Only recently in works of Rubin and the author, the finiteness of Ш(R,E) was proved for some E and R . We shall discuss these results later.

The elements of $E(R)_{tor}$ can be effectively calculated. For example, let R be $\mathbb{Q}$ and let E be defined by an equation $u^2 = w^3 + \alpha w + \beta$, where $\alpha,\beta \in \mathbb{Z}$, $\delta = 4\alpha^3 + 27\beta^2 \neq 0$ (this is always possible). According to the Nagell–Lutz theorem, if $P \in E(\mathbb{Q})_{tor}$ is nonzero, then $u(P) = 0$ or $u(P)^2 \mid \delta$. Mazur determined all possible types of $E(\mathbb{Q})_{tor}$, in particular, $[E(\mathbb{Q})_{tor}] \leq 16$.

We are interested here in the case $R = \mathbb{Q}$. No algorithm is known in general for calculating $r(\mathbb{Q},E)$ and generators of $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$. But recently here and in the study of Ш(R,E) essential progress was made.

More specifically, it is connected to advances towards proving the Birch-Swinnerton-Dyer conjecture (BSD) which predicts a connection between the arithmetic of E and its L–function.

We let L(E,s) denote the L–function of E over $\mathbb{Q}$, defined for $Re(s) > 3/2$ as

$$\prod_q L_q(E,s) = \sum_{n=1}^{\infty} a_n n^{-s} , \ a_n \in \mathbb{Z} .$$

Here q runs through the set of rational primes. Let $N \in \mathbb{N}$ be the conductor of E. If $(q,N) = 1$, then $L_q(E,s) = (1-a_q q^{-s}+q^{1-2s})^{-1}$, where $a_q = q+1-[\tilde{E}(\mathbb{Z}/q\mathbb{Z})]$, $\tilde{E}$ being the reduction of E modulo q (E has the good reduction at q). If $q|N$, then $L_q(E,s) = 1,(1\pm q^{-s})^{-1}$ depending on the type of bad reduction of E at q.

Assume that E is modular, that is there exists a weak Weil parametrization $\gamma : X_0(N) \longrightarrow E$ [12]. Here $X_0(N)$ is the modular algebraic curve over $\mathbb{Q}$ parametrizing classes of isogenies of elliptic curves with cyclic kernel of order N. According to the Taniyama–Shimura–Weil conjecture, every elliptic curve over $\mathbb{Q}$ is modular. Then $L(E,s)$ has an analytic continuation to an entire function on the complex plane which satisfies a functional equation

$$Z(E,2-s) = \epsilon Z(E,s) \tag{1}$$

where $Z(E,s) = (2\pi)^{-s}N^{s/2}\Gamma(s)L(E,s)$ and $\epsilon = \pm 1$ depends on E.

An analogeous L–function $L(R,E,s)$ of E over R can be defined (its definition is essential for us only up to a finite product of Euler factors), having analogous properties. We let $ar(R,E)$ denote the order of vanishing $L(R,E,s)$ at $s = 1$. According to BSD, one conjectures the identity:

$$r(R,E) = ar(R,E)\,. \tag{2}$$

Moreover BSD connects the first nonzero coefficient of the expansion of $L(R,E,s)$ around $s=1$ with the order of Ш(R,E) (using the hypothesis that Ш(R,E) is finite) and other parameters of E, but we do not go into this here.

In the sequel we will omit the letter $\mathbb{Q}$ in the notations Ш$(\mathbb{Q},E)$, $r(\mathbb{Q},E)$, $ar(\mathbb{Q},E)$. It follows from (1) that $ar(E)$ is even when $\epsilon = 1$, $ar(E)$ is odd when $\epsilon = -1$. E is called even or odd, respectively.

For $R = \mathbb{Q}$ the current state of conjecture (2) and of the hypothesis of finiteness of $Ш(E)$ is expressed by the result:

Theorem 1. The equality $r(E) = ar(E)$ holds and $Ш(E)$ is finite if $ar(E) \leq 1$.

We remark that empirical material shows that curves with $ar(E) > 1$ compose a relatively small part in the set of all curves. Apparently (taking into account the Taniyama—Shimura–Weil conjecture), Theorem 1 covers a substantial part of all elliptic curves over $\mathbb{Q}$.

Further we discuss a scheme of the proof of Theorem 1, formulate earlier results and give some examples.

Let D be a fundamental discriminant of the imaginary–quadratic field $K = \mathbb{Q}(\sqrt{D})$ such that $D \equiv \square (\mathrm{mod}\ 4N)$, $D \neq -3,-4$. As E is modular, there exists the Heegner point $P_D \in E(K)$ (which will be defined later), it satisfies the condition:

$$\sigma\, \epsilon\, P_D = -\epsilon\, e\, P_D \qquad (3)$$

where $e =$ exponent of $E(\mathbb{Q})_{tor}$, σ is the generator of $G(K/\mathbb{Q})$. The author proved [6]–[8]:

Theorem 2. The equality $r(E) = ar(E)$ holds and $Ш(E)$ is finite if 1) $ar(E) \leq 1$, 2) $\exists\, D \mid P_D$ has infinite order.

From the Gross and Zagier results [5] it follows

Theorem 3. If $(D,2N) = 1$, then $ar(K,E) \geq 1$, $ar(K,E) = 1 \Leftrightarrow P_D$ has infinite order.

Waldspurger [21] for $ar(E) = 1$ and, independently, Bump, Friedberg, Hoffstein [2] and M. Murty, B. Murty [14] for $ar(E) = 0$ proved

Theorem 4. If $ar(E) \leq 1$, then $(D,2N) = 1$ and $ar(K,E) = 1$ for an infinite set of values of D.

So from Theorems 3, 4 it then follows that condition 2) in Theorem 2 follows from condition 1), that is Theorem 2 is equivalent to Theorem 1.

From (1) we have that $ar(E) = 0 \Rightarrow \epsilon = 1$, $ar(E) = 1 \Rightarrow \epsilon = -1$. Using (3), we deduce from the conditions: P_D has infinite order, $r(K,E) = 1$, and $ar(E) \leq 1$, that $r(E) = ar(E)$. The kernel of the natural homomorphism $Ш(E) \longrightarrow Ш(K,E)$ is $Ш(E) \cap H^1(G(K/\mathbb{Q}),E(K)) \subset Ш(E)_2$ which is a finite group.

Thus Theorem 2 is a consequence of the author's result [8]:

Theorem 5. The equality $r(K,E) = 1$ holds, and $Ш(K,E)$ is finite, if P_D has infinite order.

We note that Theorems 5, 3 give (1) for $R = K$ when $ar(K,E) = 1$. The inequality $r(E) \geq 1$ when $ar(E) = 1$ follows already from Theorem 3 and Waldspurger's result.

A subclass in the class of modular elliptic curves is formed by elliptic curves with complex multiplication: $End(E) \neq \mathbb{Z}$ and then $End(E)$ is an order with class number one of an imaginary–quadratic extension k of $\mathbb{Q}$. We let W' denote this subclass. The modular invariant $j = g_2^3/(g_2^3 - 27g_3^2)$, which runs through all rational numbers on the set of elliptic curves over $\mathbb{Q}$, takes on 13 values on the set W'.

The specific property of a curve from W' is the possibility to use, in studying it, the theory of abelian extensions of k because $E(\mathbb{Q})_{tor} \subset E(k^{ab})$ for $E \in W'$. In particular, by using so called elliptic units, Coates and Wiles [3] proved (2) for $E \in W'$, $ar(E) \neq 0$. Recently Rubin [17], also using elliptic units (we will come back to this later), proved under the same condition that Ш(E) is finite. This gave the first examples of finite groups Ш(E). Moreover he proved that, for $E \in W'$, $ar(E) = 1 \Rightarrow r(E) \leq 1$.

2. Explicit Cohomology Classes.

Now we discuss briefly the method of proof of Theorem 5.

For an arbitrary extension L of $\mathbb{Q}$ the exact sequence $0 \longrightarrow E_M \longrightarrow E(\bar{L}) \longrightarrow E(\bar{L}) \longrightarrow 0$ $(E_M = E(\bar{\mathbb{Q}})_M)$ induces the exact sequence

$$0 \longrightarrow E(L)/ME(L) \longrightarrow H^1(L,E_M) \longrightarrow H^1(L,E)_M \longrightarrow 0 . \qquad (4)$$

The Selmer group $S_M(R,E)$, by definition, is the subgroup of $H^1(R,E_M)$ consisting of elements whose image in $H^1(R(v),E_M)$ lies in $E(R(v))/ME(R(v))$ for all places v of R. In particular, (4) induces the exact sequence

$$0 \longrightarrow E(R)/ME(R) \longrightarrow S_M(R,E) \longrightarrow Ш(R,E)_M \longrightarrow 0 . \qquad (5)$$

It is known (the weak Mordell–Weil theorem) that $S_M(R,E)$ is a finite M–torsion group. In particular, $Ш(R,E)_M$ is a finite group as we remarked before.

Let $R = K$. If $P = P_D$ has infinite order, then we define $C = C_D$ to be the maximal natural number dividing the image of P in $E(K)/E(K)_{tor} \simeq \mathbb{Z}^{r(K,E)}$. We let $C = 0$ if $P \in E(K)_{tor}$. Thus P has infinite order $\Leftrightarrow$ $C \neq 0$. We let S'_M denote the factor group of $S_M(K,M)$ modulo the subgroup generated by P. Taking into account (5) and the Mordell–Weil theorem: $E(K) \simeq F \times \mathbb{Z}^{r(K,E)}$, with F finite, Theorem 5 will follow from the existence of $C' \in \mathbb{N}$ such that $C' S'_M = 0 \ \forall M \in \mathbb{N}$.

The non-degenerate alternating Weil pairing $[\ ,\ ]_M : E_M \times E_M \longrightarrow \mu_M = \mathbb{Q}^*_M$ induces a pairing

$$\langle\ ,\ \rangle_{M,v} : H^1(K(v),E_M) \times H^1(K(v),E_M) \longrightarrow H^2(K(v),\mu_M)$$

For $v = \infty$ the field $K(\infty) \simeq \mathbb{C}$ and the corresponding cohomology groups are trivial. For $v \neq \infty$ the group $H^2(K(v),\mu_M)$ is identified canonically with $\mathbb{Z}/M\mathbb{Z}$ by local class field theory. If $a,b \in H^1(K,E_M)$, then $\langle a,b \rangle_{M,v} \overset{\text{def}}{=} \langle a(v),b(v) \rangle_{M,v}$, where $a(v)$, $b(v)$ are the localizations of a, b. According to global class field theory (the reciprocity law) $\langle a,b \rangle_{M,v} \neq 0$ only for a finite set of places v and the following relation holds:

$$\sum_{v \neq \infty} \langle a,b \rangle_{M,v} = 0 \,. \tag{6}$$

Relation (6) can be considered as a condition on a if an element b is fixed. To use (6) for the study of $S_M(K,E)$ it is necessary to find explicit elements b. This was my strategy. Thus I constructed a set T of explicit elements of $H^1(K,E_M)$ by using Heegner points over ring class fields of K. The special properties of these elements allowed to deduce from (6) with $a \in S_M(K,E)$ and $b \in T$ the relation $C' S'_M = 0$ for some $C' \in \mathbb{N}$, the divisor and main component of which is C.

Now we describe the construction of an element from T. First we define the Heegner points. Fix an ideal i in the ring of integers O of K such that $O/i \simeq \mathbb{Z}/N\mathbb{Z}$ (i exists in view of the assumptions on D). If $\lambda \in \mathbb{N}$, then K_λ denotes the ring class field of K of conductor λ. It is a finite abelian extension of K. Let O_λ be $\mathbb{Z} + \lambda O$, $i_\lambda = i \cap O_\lambda$. If $(\lambda,N) = 1$, we define the point $z_\lambda \in X_N(K_\lambda)$ as corresponding to the class of the isogeny

$\mathbb{C}/O_\lambda \longrightarrow \mathbb{C}/i_\lambda^{-1}$, where i_λ^{-1} is the inverse of i_λ in the group of proper O_λ–ideals. We let $y_\lambda = \gamma(z_\lambda) \in E(K_\lambda)$, $P = P_D$ = the norm of y_1 from K_1 to K . The points y_λ , P are called Heegner points (corresponding to the parametrization $\gamma : X_0(N) \longrightarrow E$, $K = \mathbb{Q}(\sqrt{D})$ and i).

We use the notation p (or p with (a subscript) for rational primes which do not divide N and remain prime in K . We let Λ^r denote the set of all products $p_1 \ldots p_r$ with distinct p_m , $\Lambda = \bigcup_{n=1}^{\infty} \Lambda^r$.

Let $\lambda \in \Lambda$, $G_\lambda = G(K_\lambda/K_1)$. The group G_λ is the direct product of the subgroups $G_{\lambda,p} = G(K_\lambda/K_{\lambda/p})$ for $p \mid \lambda$. The natural homomorphism $G_{\lambda,p} \longrightarrow G_p$ is an isomorphism. The group G_p is isomorphic to the group $\mathbb{Z}/(p+1)\mathbb{Z}$. For each p , we fix a generator $t_p \in G_p$; $t_p \in G_{\lambda,p}$ denotes the corresponding generator of $G_{\lambda,p}$. We let $Tr_p = \sum_{j=0}^{p} t_p^j$. Recall that $\sum_{n=1}^{\infty} a_n n^{-s} = L(E,s)$ for $Re(s) > 3/2$. For $p \mid \lambda$ one finds the relation:

$$Tr_p y_\lambda = a_p y_{\lambda/p} \,. \tag{7}$$

These relations (7) are the basis for the definition of explicit cohomology classes.

Let Δ_λ denote the ring $\mathbb{Z}[G_\lambda]$. We define a Δ_λ–module B_λ in the following way. Let F_λ be the direct sum $\sum_{\eta \mid \lambda} \Delta_q$, where G_λ acts on Δ_η by the natural homomorphism $\Delta_\lambda \longrightarrow \Delta_\eta$. Let 1_η denote the unit of Δ_η , H_λ be the Δ_λ–submodule of F_λ generated by the elements $Tr_p 1_\eta - a_p 1_{\eta|p}$ for all $p \mid \eta \mid \lambda$. Then $B_\lambda = F_\lambda/H_\lambda$.

It is not difficult to prove that $(B_\lambda)_{tor} = 0$. Let $1'_\eta$ be the image of 1_η in B_λ , then $\{1'_\eta, \eta \mid \lambda\}$ is a system of generators of B_λ over Δ_λ . By (7) $\exists!$ homomoprhism

$\varphi : B_\lambda \longrightarrow E(K_\lambda)$ such that $1'_\eta \longrightarrow y_\eta$. We let $I_p = -\sum_{j=1}^{p} jt_p^j \in \Delta_\lambda$, $I_\lambda = \prod_{p|\lambda} I_p$. Let Q_λ be the element $I_\lambda 1'_\lambda$.

For $M \in \mathbb{N}$ we define $\Lambda(M)$ as the subset of Λ consisting of elements λ such that $M|(p+1)$, $M|a_p \; \forall p|\lambda$. Further, $\Lambda^r(M) = \Lambda^r \cap \Lambda(M)$. We claim that $(1-g)Q_\lambda \in MB_\lambda$ for $\lambda \in \Lambda(M)$ and $g \in G_\lambda$. It is enough to verify this for $g = t_p$, where $p|\lambda$. It is clear that

$$(1-t_p)I_p = Tr_p-(p+1)\,. \tag{8}$$

Thus, we have $(1-t_p)Q_\lambda = I_{\lambda/p}(1-t_p)I_p 1'_\lambda = I_{\lambda/p}(Tr_p-(p+1))1'_\lambda = = I_{\lambda/p}(a_p 1'_{\lambda/p} - (p+1)1'_\lambda) \in MB_\lambda$.

As $(B_\lambda)_{tor} = 0$, there exists a unique element $((1-g)Q_\lambda)/M \in B_\lambda$. We define the element $\tau'_\lambda(M) \in H^1(K_1,E_M)$ to be the class of the cocycle:

$$\psi : g \longmapsto (g-1)(\varphi(Q_\lambda)/M) + \varphi(((1-g)Q_\lambda)/M)\;,$$

where $g \in G(\overline{K}_1/K_1)$. The element $\tau_\lambda(M) \in H^1(K,E_M)$ we define as the corestriction of $\tau'_\lambda(M)$. We call T the set $\{\tau_\lambda(M), M \in \mathbb{N}, \lambda \in \Lambda(M)\}$.

Let (b) denote the image of $b \in H^1(K,E_M)$ in $H^1(K,E)_M$, $c_\lambda(M) = (\tau_\lambda(M))$. That is, $c_\lambda(M)$ is the corestriction of the element of $H^1(K_1,E)_M$ defined by the cocycle, $g \longmapsto \varphi((1-g)Q_\lambda)/M)$. If $\lambda \in \Lambda^r(M)$, then the automorphism $\sigma \in G(K/\mathbb{Q})$ acts on $c_\lambda(M)$ by multiplication by $(-1)^{r+1}\epsilon$. The symbol $\langle a,b\rangle_{M,v}$ depends only on (b), if $a \in S_M(K,E)$.

The elements $c_p(M)$ were defined first see [6]. This allowed to prove the relation $C'(\sigma+\epsilon)S_M(K,E) = 0$, which is equivalent to the finiteness of $E(\mathbb{Q})$ and Ш(E) when $\epsilon = 1$, and to the finiteness of $E_{(D)}(\mathbb{Q})$ and Ш$(E_{(D)})$ when $\epsilon = -1$. Here $E_{(D)}$ is the elliptic curve (the form of E over K) defined by the equation $Dy^2 = 4x^3 - g_2x - g_3$.

In [8] there were defined elements $\tau_\lambda(M)$ for some subset of the set $\{M \in \mathbb{N}, \lambda \in \Lambda(M)\}$ containing the set $\{M \mid (M,d) = 1, \lambda \in \Lambda(M)\}$, where d = exponent of $E(\mathbb{K})_{tor}$, $\mathbb{K}$ is the composite of the $K_{\lambda'}$ for $\lambda' \in \Lambda$. By using here the modules B_λ and the property $(B_\lambda)_{tor} = 0$ we shake off the additional restrictions on (M,λ) when $(M,d) > 1$. The relation (6) with $(b) = c_\lambda(M)$ when $\lambda \in \Lambda^r(M)$, $r \leq 2$, allowed to prove the relation $C' S'_M = 0$.

We note that an application of the elements $\tau_\lambda(M)$ when $\lambda \in \Lambda^r$ with arbitrary $r \geq 0$ allowed in [8] to pass from a relation of the type $C\,Ш(K,E) = 0$ to a relation of the type $[\,Ш(K,E)] \mid C^2$. Because of the existence on $Ш(K,E)$ of a non–degenerate (as $Ш(K,E)$ is finite) alternate Cassels pairing with values in $\mathbb{Q}/\mathbb{Z}$, it then follows that the second relation implies the first relation.

In [20] Thaine used the cyclotomic units for a new proof of annihilating relations in the ideal class groups of real abelian extensions of $\mathbb{Q}$. Rubin [16] adapted Thaine's approach, using elliptic units instead of cyclotomic units, for proving annihilating relations in the ideal class groups of abelian extensions of the imaginary–quadratic field $k = End(E) \otimes \mathbb{Q}$ when $E \in W'$. By using the natural connection between ideal class groups and the Selmer group $S_M(\mathbb{Q},E)$ Rubin proved an universal annihilating relation for $S_M(\mathbb{Q},E)$ by the condition that $ar(E) = 0$.

A comparison of the approaches of Thaine [20] and of the author [6] for proving annihilating relations in the ideal class groups and in the Selmer groups, respectively, suggested the possibility in [7] of combining them into a single general framework. A further step was a construction and use in [8] of sets of cohomology classes of the type T , both in the theory of modular elliptic curves and in the theory of ideal class groups of abelian extensions of $\mathbb{Q}$ or an imaginary–quadratic extension of $\mathbb{Q}$. For information on this theory and some further applications we refer to the papers [8], [1], [4], [9], [10], [11], [13], [15], [18], [19].

3. Examples.

Example 1, Rubin [17]. For the curves with complex multiplication $(k = \mathbb{Q}(\sqrt{-1}))$ $y^2 = x^3 - x$, $y^2 = x^3 + 17x$ we have: $r(E) = ar(E) = 0$, Ш$(E) = 0$, $\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$, respectively.

Example 2, Kolyvagin [7]. Let $E : y^2 = 4x^3 - 4x + 1$. It is an odd modular curve without complex multiplication, of conductor $N = 37$. Let $(D,2N) = 1$. The curves $E_{(D)}$:

$$Dy^2 = 4x^3 - 4x + 1 \tag{9}$$

are even and have no complex multiplication. For computation of $L(E_{(D)},1)$ and C_D the following identity can be used:

$$L(E_{(D)},1) = 2 \sum_{n=1}^{\infty} \frac{a_n}{n} \left[\frac{D}{n}\right] \exp(-2\pi n/(|D|\sqrt{37})) = (2\Omega_{-}/\sqrt{D})C_D^2 \tag{10}$$

where Ω_{-} – the imaginary period of E, $\left[\frac{D}{n}\right]$ – the Legendre symbol. See [22] for (10); the connection between $L(E_{(D)},1)$ and C_D is a consequence of the results of Gross and Zagier [5].

Let $L(E_{(D)},1) \neq 0$ or, equivalently, $C_D \neq 0$. Then $E_{(D)}(\mathbb{Q})$ is finite and, moreover, is trivial because always $E_{(D)}(\mathbb{Q})_{tor} = 0$. That is equation (9) has no solutions in rational numbers. Further, $Ш(E_{(D)})$ is finite and $C_D Ш(E_{(D)}) = 0$. For example, if $D = -7, -11$ then $C_D = 1$, so $Ш(E_{(D)}) = 0$. See [7] for further information on this example.

We recall that $C_D \neq 0$ for an infinite set of values of D according to a result of Waldspurger.

It is a classical fact that $E(\mathbb{Q}) \simeq \mathbb{Z}$ is generated by the point $(y=1, x=0)$. Of course, $ar(E) = 1$, see [22], for example. The author proved [8] that $Ш(E) = 0$.

References

1. Bertolini, M., Darmon, H.: Kolyvagin's descent and Mordell–Weil groups over ring class fields. Preprint (1989)

2. Bump, D., Friedberg, S., Hoffstein, J.: A non vanishing theorem for derivatives of automorphic L–functions with applications to elliptic curves. Bull. AMS. Math. Soc. 21, 89–93 (1989)

3. Coates, J., Wiles, A.: On the conjecture of Birch and Swinnerton–Dyer. Invent. Math. 39, 223–251 (1977)

4. Gross, B.H.: Kolyvagin's work on modular elliptic curves. Proceedings of Durham Conference on L–functions and Arithmetic, 1989. Cambridge University Press (to appear)

5. Gross, B.H., Zagier, D.B.: Heegner points and derivatives of L–series. Invent. Math. 84, 225–320 (1986)

6. Kolyvagin, V.A.: Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a subclass of Weil curves, Izvestia AN SSSR, Ser. Mat., 52, 522–540 (1988) English transl.: Math. of the USSR Izvestia 32, 523–542 (1989)

7. Kolyvagin, V.A.: On the Mordell–Weil and Shafarevich–Tate groups for Weil elliptic curves, Izvestia AN, SSSR, Ser. Mat., 52, 1154–1180 (1988) English transl.: Math. of the USSR Izvestia 33, 474–499 (1989)

8. Kolyvagin, V.A.: Euler systems (1988). Birkhäuser volume in honor of Grothendieck (to appear)

9. Kolyvagin, V.A., Logachev, D.Y.: Finiteness of the Shafarevich–Tate group and the group of rational points for some modular abelian varieties, Algebra and Analysis 1, $N^{\circ}5$ (1989)

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

11. Kolyvagin, V.A.: On the structure of Selmer groups. Preprint (1990)

12. Mazur, B., Swinnerton–Dyer, H.P.F.: Arithmetic of Weil curves. Invent. Math. 25, 1–61 (1974)

13. McCallum, W.G.: Kolyvagin's work on Shafarevich–Tate groups, Proceedings of Durham Conference on L–functions and Arithmatic, 1989. Cambridge University Press (to appear)

14. Murty, M.R., Murty, V.K.: Mean values of derivatives of modular L–series. Preprint (1989)

15. Perrin–Riou, B.: Travaux de Kolyvagin et Rubin. Séminaire Bourbaki 717 (1989/1990)

16. Rubin, K.: Global units and ideal class groups. Invent. Math. 89, 511–526 (1987)

17. Rubin, K.: Tate–Shafarevich group and L–functions of elliptic curves with complex multiplications. Invent. Math. 89, 527–560 (1987)

18. Rubin, K.: The Main Conjecture. Appendix to: Cyclotomic fields I–II (second ed.) by S. Lang. Grad. Texts in Math. 121. Springer, New York, Berlin, Heidelberg, 1990. pp. 397–419.

19. Rubin, K.: The "main conjectures" of Iwasawa theory for imaginary quadratic fields. Preprint (1990)

20. Thaine, F.: On the ideal class groups of real abelian extensions of $\mathbb{Q}$. Ann. Math. 128, 1–18 (1988)

21. Waldspurger, J.–L.: Sur les valeurs de certaines fonctions L automorphes en leur centre de symmetrie. Comp. Math. 54, 173–242 (1985)

22. Zagier, D.B.: Modular points, modular curves, modular surfaces and modular forms. (Lecture Notes in Mathematic, vol. 1111). Springer, New York, Berlin, Heidelberg, 1985, pp. 225–246.