ON THE STRUCTURE OF SHAFAREVICH-TATE GROUPS

V. A. Kolyvagin
Steklov Mathematical Institute, 117966, Moscow, GSP-1,
Vavilova St. 42, USSR.

Let E be a Weil elliptic curve over the field of rational numbers $\mathbb{Q}$. Note that, according to the Weil-Taniyama conjecture, every elliptic curve over $\mathbb{Q}$ is a Weil curve. Let R be a finite extension of $\mathbb{Q}$ and E(R) the group of points of E over $\mathbb{Q}$. According to the Mordell-Weil theorem, E(R) is a finitely generated (abelian) group, that is, $E(R)_{tor}$ is finite and $E(R) \simeq E(R)_{tor} \times \mathbb{Z}^{g(R,E)}$, where $0 \leq g(R, E) \in \mathbb{Z}$ is the rank of E over R. Let L(E, R, s) denote the L-function of E over R (which is defined modulo the product of a finite number of Euler factors). According to the Birch-Swinnerton-Dyer conjecture (which we abbreviate as BS), g(R, E) is the order of the zero of L(E, R, s) at s = 1.

Another important arithmetic invariant of E is the Shafarevich-Tate group of E over R:

$$Ш(R, E) = \ker (H^1(R, E) \longrightarrow \prod_v H^1(R(v), E))$$

(v runs through the set of all places of R; see the section on notation at the end of the introduction). It is known (the weak Mordell-Weil theorem) that Ш(R, E) is a periodic group and for all natural M its subgroup $Ш(R, E)_M$ of M-periodic elements is finite.

It is conjectured that Ш(R, E) is finite. In that case, BS suggests an expression for the order of Ш(R, E) as a product of $L^{(g(R, E))}(E, R, 1)$ and some other nonzero values connected with E (for examples, see (1) in [1] for the case R = $\mathbb{Q}$, and see Theorem B below). Let $[Ш(R, E)]^?$ denote the hypothetical order of Ш(R, E); then, according to BS, we have the equality $[Ш(R, E)] = [Ш(R, E)]^?$.

For a long time, no examples of E and R were known where Ш(R, E) is finite. Only recently, Rubin [2] proved that Ш(R, E) is finite if E has complex multiplication, R is the field of complex multiplication, and $L(E, \mathbb{Q}, 1) \neq 0$; the author [1], [3], [4] proved finiteness of Ш for some family (see below) of Weil curves and imaginary quadratic extensions of $\mathbb{Q}$. For a more detailed exposition of these methods, results, and examples, see the introductions to [1] and [4].

We now state some results [4] from which we begin the study of Ш in this article.

Let N be the conductor of E and $\gamma: X_N \longrightarrow E$ a Weil parameterization. Here X_N is the modular curve over $\mathbb{Q}$ which parameterizes isomorphism classes

of isogenies $E' \longrightarrow E''$ of elliptic curves with cyclic kernel of order N. The field $K = \mathbb{Q}(\sqrt{D})$ has discriminant D satisfying $0 > D \equiv$ square (mod 4N), where $D \neq -3$ or -4. Fix an ideal i_1 of the ring of integers O_1 of K for which $O_1/i_1 \simeq \mathbb{Z}/N$. If $\lambda \in \mathbb{N}$, let K_λ be the ring class field of K with conductor λ. In particular, K_1 is the maximal abelian unramified extension of K. If $(\lambda, N) = 1$, $O_\lambda = \mathbb{Z} + \lambda O_1$, and $i_\lambda = i_1 \cap O_\lambda$, let z_λ denote the point of X_N over K_λ corresponding to 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). Set $y_\lambda = \gamma(z_\lambda) \in E(K_\lambda)$; the point P_1 is the norm of y_1 from K_1 to K. The points y_λ and P_1 are called Heegner points.

Let $O = \mathrm{End}(E)$ and $Q = O \otimes \mathbb{Q}$. Let l be a rational prime, $T = \varprojlim E_{l^n}$ the Tate module, and $\hat{O} = O \otimes \mathbb{Z}_l$. Let B(E) denote the set of odd rational primes which do not divide the discriminant of O and for which the natural representation ρ: $G(\bar{Q}/Q) \longrightarrow \mathrm{Aut}_{\hat{O}} T$ is surjective. It is known (from the theory of complex multiplication and Serre theory) that the set of primes not belonging to B(E) is finite. Moreover, according to the Mazur theorem, if $O = \mathbb{Z}$ and N is square-free, then all $l \geq 11$ belong to B(E).

If the point P_1 has infinite order, (that is, $P_1 \notin E(K)_{tor}$) and $g(K, E) = 1$, let C_K denote the integer $[E(K)/\mathbb{Z}P_1]$. The author proved the following theorem in [4].

THEOREM A. *Suppose that* P_1 *has infinite order. Then* $g(K, E) = 1$, *the group* $Ш(K, E)$ *is finite, and* $[Ш(K, E)]$ *divides* dC_K^2, *where for all* $l \in B(E)$ *we have* $\mathrm{ord}_l d = 0$.

In Theorem A, d is an integer which depends upon E but not upon K. The application of Theorem A to BS is clear from the following result of Gross and Zagier [5] for $(D, 2N) = 1$.

THEOREM B. *The function* $L(E, K, s)$ *vanishes at* $s = 1$. *The point* P_1 *has infinite order* $\Leftrightarrow L'(E, K, 1) \neq 0$. *If* P_1 *has infinite order, then the conjecture that the group* $Ш(K, E)$ *is finite and* BS *for* E *over* K, *together, are equivalent to the following statement:* $g(K, E) = 1$, $Ш(K, E)$ *is finite, and* $[Ш(K, E)] = (C_K/(c \prod_{q|N} b\langle q\rangle))^2$.

In theorem B, the integer c is defined in terms of the parameterization γ (cf. [5]), and the integer $b\langle q\rangle$, where $q|N$ is prime, is the index in $E(\mathbb{Q}_q)$ of the subgroup of points which have nonsingular reduction modulo q.

Let $\sum_{n=1}^{\infty} a_n n^{-s}$, where $a_n \in \mathbb{Z}$, be the canonical L-series of E. It converges absolutely for Re(s) > 3/2 and has an analytical continuation to an entire function of the complex argument. Let L(E, s) denote this function; it is the canonical L-function over $\mathbb{Q}$ of the elliptic curve E. The function

$$\Xi(E, s) = (2\pi)^{-s} N^{s/2} \Gamma(s) L(E, s)$$

satisfies the following functional equation:

$$\Xi(E, 2 - s) = (-\varepsilon)\Xi(E, s),$$

where $\varepsilon = \varepsilon(E)$ is equal to 1 or -1.

Fix a prime $l \in B(E)$. Let $n(p) = \mathrm{ord}_l(p + 1, a_p)$, where p is a rational prime. Hereafter in this article 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 for which $n(p) > 0$. If $r \in \mathbb{N}$, let Λ^r denote the set of all products of r distinct such primes. The set Λ^0 contains only $p_0 \stackrel{df}{=} 1$, and $\Lambda = \bigcup_{r \geq 0} \Lambda^r$. If $r > 0$ and $\lambda \in \Lambda^r$, let $n(\lambda)$ denote $\min n(p)$; then $M_\lambda = l^{n(\lambda)}$ and $n(1) = \infty$. Let $\lambda \in \Lambda$, $1 \leq n \leq n(\lambda)$, and $M = \prod_{p|\lambda} l^n$. In [4], we constructed some cohomology classes $\tau_{\lambda,n} \in H^1(K, E_M)$ which played a central role in the proof of Theorem A.

If R is an extension of $\mathbb{Q}$, then the exact sequence

$$0 \longrightarrow E_M \longrightarrow E(\bar{R}) \xrightarrow{\times M} E(\bar{R}) \longrightarrow 0$$

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 R/L is a Galois extension, then

$$\mathrm{res}_{R/L}: H^1(L, E_M) \longrightarrow H^1(R, E_M)^{G(R/L)}$$

is the restriction homomorphism, which is an isomorphism when the l-component of the torsion part of E(R) is trivial (because of the spectral sequence). It is easily seen that the condition $l \in B(E)$ leads to the triviality of the l-component of the torsion subgroup of $E(K_\lambda)$ (cf. [6] for the case $\mathcal{O} = \mathbb{Z}$; the case $\mathcal{O} \neq \mathbb{Z}$ can be considered analogously). In particular, the value $\mathrm{res}_{K_\lambda/K}$ completely determines the element $\tau_{\lambda,n}$. We now give an expression for this value. We use the standard facts about ring class fields (which follow from Galois theory and class field theory, cf. §1 in [3]). If $1 < \lambda \in \Lambda$, then the natural homomorphism

$G(K_\lambda/K_1) \longrightarrow \prod_{p|\lambda} G(K_p/K_1)$ is an isomorphism, and we also have the isomorphisms $G(K_\lambda/K_{\lambda/p}) \xrightarrow{\sim} G(K_p/K_1) \xrightarrow{\sim} \mathbb{Z}/(p+1)$. For all p, fix a generator $t_p \in G(K_p/K_1)$ and let t_p also denote the generator of $G(K_\lambda/K_{\lambda/p})$ corresponding to this t_p. Let $I_p = -\sum_{j=1}^{p} j t_p^j$ and $I_\lambda = \prod_{p|\lambda} I_p \in \mathbb{Z}[G(K_\lambda/K_1)]$. Let $\mathbb{K}$ be the composite of the $K_{\lambda'}$, where λ' runs through the set Λ. Let J_λ denote $\sum \bar{g}$, where g runs through a set of fixed representatives of $G(\mathbb{K}/K)$ with respect to $G(\mathbb{K}/K_1)$ and $\bar{g}$ is the restriction of g to K_λ; thus $\{\bar{g}\}$ is the set of representatives of $G(K_\lambda/K)$ with respect to $G(K_\lambda/K_1)$. Let $P_\lambda = J_\lambda I_\lambda y_\lambda \in E(K_\lambda)$. Then

$$\mathrm{res}_{K_\lambda/K}(\tau_{\lambda,n}) = P_\lambda \pmod{ME(K_\lambda)}. \tag{2}$$

Suppose, further, that P_1 has infinite order. Let X denote the 1-component of $Ш(K, E)$. Let $m_0 = \mathrm{ord}_1 C_K$. As a consequence of Theorem A, we have the relation $[X]|1^{2m_0}$. A natural development of the technique of using the classes $\tau_{1,n}$ is a complete description of the structure of X in terms of the Heegner points. I announced this result in [4] (as an analogue of a similar theorem in [4] for ideal class groups). In particular, the proof is given in this article. Now we shall formulate the theorem.

We have a bijective correspondence between the set of isomorphism classes of finite abelian 1-groups and the set of sequences of nonnegative integers $\{n_i\}$ such that $i \geq 1$, $n_i \geq n_{i+1}$, and $\lim_{i\to\infty} n_i = 0$. Concretely, the sequence $\{n_i\}$ corresponds to the group $\sum_i \mathbb{Z}/1^{n_i}$. The sequence corresponding to a group A is called the sequence of invariants of A. If Σ is a group of order 2 with generator σ and A is a $\mathbb{Z}_1[\Sigma]$-module, then for $\nu = 0$ or $\nu = 1$ let A^ν denote the submodule $(1 - (-1)^\nu \varepsilon\sigma)A$. Then A is the direct sum of A^0 and A^1 and σ acts on A^ν as multiplication by $(-1)^{\nu-1}\varepsilon$. Let $\{x_i^\nu\}$ be the sequence of invariants of X^ν. If $r \in \mathbb{N}$, let $\nu(r)$ denote the element from the set $\{0, 1\}$ such that $r - \nu(r) - 1$ is an even integer. Let $(r, \nu) = r - |\nu - \nu(r)|$. Let $m'(\lambda)$ be the exponent of the highest power of 1 which divides P_λ in $E(K_\lambda)$. Define $m(\lambda)$ as $m'(\lambda)$ if $m'(\lambda) < n(\lambda)$, and as ∞ otherwise. Let $m_r = \min m(\lambda)$, where λ runs through

Λ^r. In particular, m_0 is as previously defined, since $E(K)_{1^\infty} = 0$. We have the following theorem.

THEOREM C. *The sequence* $\{m_r\}$ *is a sequence of nonnegative integers such that* $m_r \geq m_{r+1}$. *If* $\nu = 0$ *or* $\nu = 1$ *and* $r \geq 1 + \nu$, *then we have the equality* $x^{\nu}_{r-\nu} = m_{(r,\nu)-1} - m_{(r,\nu)}$.

Let m denote min $m(\lambda)$, where λ runs through Λ, that is, $m = \min_{r\geq 0} m_r = \lim_{r\to\infty} m_r$. Obviously, the next theorem follows from Theorem C.

THEOREM D. $[X] = 1^{2m_0-2m}$.

By combining Theorem D with Theorems A and B, we obtain Theorem E.

THEOREM E. *The equality* $\operatorname{ord}_1[X] = \operatorname{ord}_1[\text{Ш}(K, E)]^?$ *(the 1-component of BS) holds* $\Leftrightarrow m = m^? \overset{df}{=} \operatorname{ord}_1(c \prod_{q|N} b<q>)$. *In particular, if* $m^? = 0$, $\Leftrightarrow$ *there exists* $\lambda \in \Lambda$ *such that* $P_\lambda \notin 1E(K_\lambda)$.

Theorem C is a corollary of the more detailed Theorem 1 in §3. As I noted in [4], the classes $\tau_{\lambda,n}$ can generate elements in X; see the introduction to [4] for the simplest examples. Thus, we have the material from which to construct elements in X. On the other hand, the orthogonality relation (from class field theory) between the elements of $H^1(K, E_M)$ and $\tau_{\lambda,n}$ (cf. (15) in §2) restricts the size of X. The Chebotarev density theorem plays an important role as well.

In §3 we also obtain a description of the structure of X and its dual group in terms of a special system of primes p, and connected with it a system of p-adic characters and the elements $\tau_{\lambda,n}$; cf. (33) and (38). On this basis we obtain, under the assumptions that $m = m^?$ and that it is possible to effectively calculate the coordinates of P_λ (mod p) (this possibility can, it seems, be easily demonstrated), a description of the structure of X, a parameterization of X by $\tau_{\lambda,n}$, and a parameterization of its dual group by p-adic characters. If the inequality $m \geq m^?$ holds (in particular, if $m^? = 0$), the corresponding scheme of calculations can be used simultaneously for the proof of the equality $m = m^?$, which holds $\Leftrightarrow$ such a program is effective. See the end of §3 for some applications to an effective solution of the problem when a curve of genus 1 has a rational point.

In the case of ideal class groups, we have an analogue of the equality $m = m^?$ (from the analytical formula for the ideal class number), and the

localization of an analogue of $\tau_{\lambda,n}$ can be effectively calculated. Thus, we have an effective description of some ideal class groups by means of the analogues of $\tau_{\lambda,n}$ (the effective version of Theorem 7 in [4]). We shall discuss these questions in detail in the next article.

We now list some general notation used in this article. If A is an abelian group and M is a natural number, then A_M and A/M denote the kernel and cokernel, respectively, of multiplication by M. If L is a field, then $\bar{L}$ denotes its algebraic closure. If R/L is a Galois extention, then G(R/L) denotes the Galois group of R over L. We shall abbreviate $H^1(G(\bar{L}/L), A)$ as $H^1(L, A)$, where A is a $G(\bar{L}/L)$-module. If O is a commutative ring with 1, then O^* denotes its subgroup of invertible elements.

If R is a finite extension of $\mathbb{Q}$ and v is a place (a class of equivalent valuations) of R, then R(v) denotes the corresponding completion of R. If $\tau \in H^1(R, A)$, then $\tau(v) \in H^1(R(v), A)$ denotes the v-localization of τ.

For all $p \in \Lambda^1$, fix a place $\mathfrak{p}$ of $\bar{K}$ which divides p. Let $\bar{K}(p) \simeq \bar{\mathbb{Q}}_p$ denote the union of the R(v), where R runs through the set of finite extensions of K and v is a place of R such that $\mathfrak{p}|v$ (we use the more common notation $\mathbb{Q}_p$ for $\mathbb{Q}(p)$). We assume that $\bar{K}$ is a subfield of the field of complex numbers $\mathbb{C}$. We use the notation n, n', n" for natural numbers and M, M', M", respectively, for the numbers l^n, $l^{n'}$, $l^{n"}$.

1. Properties of the Classes $\tau_{\lambda,n}$.

In the sequel, we shall assume that λ belongs to Λ. Here we list the properties of the points y_λ ([4], cf. also [6]), which play an important role in the theory of the classes $\tau_{\lambda,n}$. Let $Tr_p = \sum_{j=0}^{p} t_p^j$ and suppose that p divides λ; then

$$Tr_p\, y_\lambda = a_p\, y_{\lambda/p}. \tag{3}$$

Let $\tilde{E}$ be the reduction of E modulo p and $\mathfrak{F}$ the residue field of K(p); if $\alpha \in E(\bar{K}(\mathfrak{p})$, then let $\tilde{\alpha} \in E(\mathfrak{F})$ be the reduction of α. Let Fr_p denote the Frobenius automorphism (raising to the p^{th} power) of the field $\mathfrak{F}$. If p divides λ, then for all $g \in G(K_\lambda/\mathbb{Q})$ we have the relation

$$gy_\lambda = Fr_p\, gy_{\lambda/p}. \tag{4}$$

Let $\theta_\lambda(i_\lambda)$ denote the value on the class of the ideal i_λ of the reciprocity hommorphism θ_λ between the group of classes of proper O_λ-ideals and the group $G(K_\lambda/K)$. Let σ be the automorphism of complex conjugation.

We have the relation

$$\sigma y_\lambda = \varepsilon\theta_\lambda(i_\lambda)y_\lambda \pmod{E(\mathbb{Q})_{tor}}. \tag{5}$$

Obviously, we have $(t_p - 1)I_p = Tr_p - (p + 1)$, and since (3) holds, it follows that if $M|(p + 1)$ and $M|a_p$, then for all $g \in G(K_\lambda/\mathbb{Q})$, we have $gP_\lambda = P_\lambda \pmod{ME(K_\lambda)}$. Thus, the relation (2) may be used as a definition of $\tau_{\lambda,n}$.

Since $\sigma g = g^{-1}\sigma$ for all $g \in G(K_\lambda/K)$, it then follows that $\sigma I_p = -I_p\sigma \pmod{M}$. From this relation and (5) we obtain that $\sigma P_\lambda = \varepsilon(-1)^r P_\lambda \pmod{ME(K_\lambda)}$, where $\lambda \in \Lambda^r$. The corresponding property of the class $\tau_{\lambda,n}$ is as follows:

$$\sigma\tau_{\lambda,n} = (-1)^r\varepsilon\tau_{\lambda,n}. \tag{6}$$

We shall now discuss the properties of the localizations of $\tau_{\lambda,n}$. We first present some facts concerning local cohomology and list some notation. Recall that p does not divide N. Therefore the curve E has good reduction at p and we can use the standard properties of good reduction (cf. [7]).

Let $\mathbb{Q}_p^{un}$ be the maximal unramified extension of $\mathbb{Q}_p$; then $\mathcal{F}$ is its residue field and reduction induces an isomorphism between $G = G(\mathbb{Q}_p^{un}/\mathbb{Q}_p)$ and $G(\mathcal{F}/\mathbb{Z}/p)$.

We shall also use Fr_p to denote the element of G corresponding to Fr_p.

By the properties of good reduction, for all $M' = l^{n'}$ we have $E_{M'} \subset E(\mathbb{Q}_p^{un})$, and reduction induces a G-isomorphism between $E_{M'}$ and $E(\mathcal{F})_{M'}$. Then $E_{M'} = \mathbb{Z}/M' + \mathbb{Z}/M'$ and $Y^2 - a_pY + p$ is the characteristic polynomial of Fr_p on $E_{M'}$, so that $Fr_p^2 - a_pFr_p + p = 0$ on $E_{M'}$ and on $E(\mathcal{F})_{M'}$. Since $a_p \equiv p + 1 \equiv 0 \pmod{M}$, it then follows that $Fr_p - 1 = 0$ on $E_{M'}$, therefore $E_M \subset E(\mathcal{K})$. Here $\mathcal{K}$ is an unramified quadratic extension of $\mathbb{Q}_p$, that is, the fixed field for Fr_p^2. Since p is prime in K, it follows that $\mathcal{K} = K(p)$. Let F be the residue field of $\mathcal{K}$. Let $f_{p,n} = \dfrac{Fr_p^2 - 1}{M}$ and $\tilde{f}_{p,n} = \dfrac{a_p}{M}Fr_p - \dfrac{p + 1}{M}$. We have the following comutative diagram of isomorphisms with the vertical isomorphisms induced by reduction:

$$\begin{array}{ccc} f_{p,n}\colon E(\mathcal{K})/M & \longrightarrow & E_M \\ \downarrow & & \downarrow \\ \tilde{f}_{p,n}\colon E(F)/M & \longrightarrow & E(F)_M \end{array}$$

Indeed, the vertical homomorphisms are isomorphisms by the propertiesof good reduction. Then $\tilde{f}_{p,n}$ coincides with the reduction of $f_{p,n}$, since $Fr_p^2 - 1 = a_p Fr_p - (p+1)$ on $E(\mathcal{F})_{l^\infty}$. Thus, we must only prove that $f_{p,n}$ is an isomorphism. This is true, since $f_{p,n}$ is an injection and $[E(\mathcal{K})/M] = [E(F)/M] = M^2$ (since $E(F)_M \simeq \mathbb{Z}/M + \mathbb{Z}/M$).

Let $[\ ,\ ]_{M'}\colon E_{M'} \times E_{M'} \longrightarrow \mu_{M'}$ denote the nondegenerate alternating Weil pairing, where $\mu_{M'}$ is the group of M'^{th} roots of unity. We have the following equality (cf. §4.3 in [8]):

$$[ge_1, ge_2]_{M'} = g[e_1, e_2]_{M'}. \tag{7}$$

Let $E_M = E_M^0 + E_M^1$ be the decomposition relative to the action of Fr_p (see the introduction). We shall show that $E_M^\nu = \mathbb{Z}/M$ for $\nu \in \{0, 1\}$. Otherwise, $Fr_p = \pm 1$ on E_1 and we have $[e_1, e_2]_1 = [Fr_p e_1, Fr_p e_2]_1 = Fr_p[e_1, e_2]_1 = [e_1, e_2]_1^p = [e_1, e_2]_1^{-1} \Rightarrow [e_1, e_2]_1 = 1$ (since l is odd), which is impossible, since $[\ ,\ ]_1$ is a nondegenerate pairing.

Let $H_{p,n}$ denote $H^1(\mathcal{K}, E_M) = \mathrm{Hom}\,(G^{ab}/(G^{ab})^M, E_M)$, where G^{ab} is the Galois group of the maximal abelian extension of $\mathcal{K}$. Using the isomorphism $\theta_p\colon \mathcal{K}^*/\mathcal{K}^{*M} \longrightarrow G^{ab}/(G^{ab})^M$ from local class field theory, identify $H_{p,n}$ with $\mathrm{Hom}(\mathcal{K}^*/\mathcal{K}^{*M}, E_M)$. The group $\mathcal{K}^*/\mathcal{K}^{*M}$ is the direct sum of its cyclic subgroups of order M, $\mathcal{A}_n = p^{\mathbb{Z}/M}$ and $\mathcal{B}_n = U/U^M$, where U is the group of units of $\mathcal{K}$. Let $A_{p,n}$ and $B_{p,n}$ be the subgroups of $H_{p,n}$ of all homomorphisms which are trivial on $\mathcal{B}_n$ and $\mathcal{A}_n$, respectively. Then the group $H_{p,n}$ is the direct sum of $A_{p,n}$ and $B_{p,n}$, and $A_{p,n} = E(\mathcal{K})/M$, since $E(\mathcal{K})/M \subset A_{p,n} = H_{p,n}^{un}$ and $[E(\mathcal{K})/M] = [A_{p,n}] = M^2$.

If $\mathcal{L}_{p,n}$ is the class field of $\mathcal{K}$ which corresponds to the subgroup $\mathcal{K}^{*M}p^{\mathbb{Z}}$ of $\mathcal{K}^*$, then $B_{p,n} = H^1(G_{p,n}, E_M)$, where $G_{p,n} = G(\mathcal{L}_{p,n}/\mathcal{K})$.

The decomposition $H_{p,n} = A_{p,n} + B_{p,n}$ implies that $H^{\nu}_{p,n}$ decomposes into a direct sum of the cyclic subgroups of order M, $A^{\nu}_{p,n}$ and $B^{\nu}_{p,n}$.

Let $\mathcal{K}_p$ be the class field of $\mathcal{K}$ corresponding to the subgroup $p^{\mathbb{Z}}(\mathbb{Z}_p^* + pO(p))$, where $O(p)$ is the ring of integers of $\mathcal{K}$. The field $\mathcal{K}_p$ is a cyclic totally ramified extension of $\mathcal{K}$ of degree $p + 1$ and $\mathcal{L}_{p,n}$ is a subextension of $\mathcal{K}_p$ of degree M over $\mathcal{K}$. Suppose that p divides λ. By the properties of ring class fields (cf. §1 in [3]), the completion of $K_{\lambda/p}$ in $\bar{K}(p)$ is the field $\mathcal{K}$, the completion of K_{λ} is the field $\mathcal{K}_p$, and the embedding of $G(\bar{K}(p)/\mathcal{K})$ into $G(\bar{K}/K_{\lambda/p})$ induces an isomorphism between $G(\mathcal{K}_p/\mathcal{K})$ and $G(K_{\lambda}/K_{\lambda/p})$. Thus, the generator t_p of $G(K_{\lambda}/K_{\lambda/p})$ can also be considered as a generator of $G(\mathcal{K}_p/\mathcal{K})$. Let $t_{p,n}$ denote the generator of $G_{p,n}$ which is the image of t_p.

If $e \in E_{M'}$, then define $b_{p,n}(e)$ to be the element of $G_{p,n}$ which maps $t_{p,n}$ to e. We define a nondegenerate alternating pairing $<\ ,\ >'_{p,n}\colon H_{p,n} \times H_{p,n} \longrightarrow \mathbb{Z}/M$ by the following conditions: the group $H^0_{p,n}$ is orthogonal to the group $H^1_{p,n}$, and for $s \in A_{p,n}$ we have the relation

$$\zeta_{p,n}^{<s,\ b_{p,n}(e)>'_{p,n}} = [f_{p,n}(s),\ e]_M,$$

where

$$\zeta_{p,n} \equiv (\theta_p^{-1}(t_{p,n}))^{(p^2-1)/M} \pmod{p}.$$

Let $<\ ,\ >_{p,n}\colon H_{p,n} \times H_{p,n} \longrightarrow \mathbb{Z}/M$ be the alternating pairing induced by the pairing $[\ ,\ ]_M$ and the canonical isomorphism $H^2(\mathcal{K},\ \mu_M) \longrightarrow \mathbb{Z}/M$ from local class field theory. This is a pairing of $G(\mathcal{K}/\mathbb{Z}_p)$-modules, hence, the group $H^0_{p,n}$ is orthogonal to the group $H^1_{p,n}$. Since, according to formula (5) of [3], $<s,\ b_{p,n}(e)>_{p,n} = <s,\ b_{p,n}(e)>'_{p,n}$, it then follows that $<\ ,\ >_{p,n} = <\ ,\ >'_{p,n}$.

Fix generators e^{ν}_p of the groups $E^{\nu}_{M_p}$, where $M_p = l^{n(p)}$, such that

$[e_p^0, e_p^1]_M = \zeta_{p,n(p)}$. Let $e_{p,n}^\nu$ be equal to $(M_p/M)e_p^\nu$. Then $[e_{p,n}^0, e_{p,n}^1] = \zeta_{p,n}$, since $[M_\beta, M_\alpha]_M = [\alpha, \beta]_{M_p}^M$ for all $\alpha, \beta \in E_{M_p}$ and $M = M_p/M$.

Define the homomorphism $\psi_{p,n}^\nu: H_{p,n}^\nu \longrightarrow \mathbb{Z}/M$ as $< , b_{p,n}^\nu >_{p,n}$, where $b_{p,n}^\nu = b_{p,n}(e_{p,n}^{\nu'})$ and $\nu' \stackrel{df}{=} 1 - \nu$. Note that $\psi_{p,n}^\nu$ is trivial on $B_{p,n}^\nu = \mathbb{Z}/Mb_{p,n}^\nu$ and induces an isomorphism between $A_{p,n}^\nu$ and $\mathbb{Z}/M$ such that for all $s \in A_{p,n}^\nu$ we have

$$\psi_{p,n}^\nu(s)\, e_{p,n}^\nu = (-1)^\nu f_{p,n}(s). \tag{8}$$

The homomorphism $\psi_{p,n}: H_{p,n} \longrightarrow \mathbb{Z}/M$ is, by definition, $\psi_{p,n}^0 + \psi_{p,n}^1$ and the homomorphism $\psi_{p,n}: H^1(K, E_M) \longrightarrow \mathbb{Z}/M$ is the composition of $\psi_{p,n}$ and the localization homomorphism $H^1(K, E_M) \longrightarrow H_{p,n}$.

Let $S_{\lambda,n}$ denote the subgroup of $H^1(K, E_M)$ of all elements α such that $\alpha(v) \in E(K(v))/M$ for all places v of the field K which do not divide λ. We have the following proposition.

PROPOSITION 1. *Let* $\lambda \in \Lambda^r$. *Then* $\tau_{\lambda,n} \in S_{\lambda,n}^{\nu(r)}$ *(see the definition of* $\nu(r)$ *in the introduction). If* $(p, \lambda) = 1$, *then* $\tau_{p,n}(p) = P_\lambda \pmod{ME(K(p))}$. *Suppose that* p *divides* λ. *Then we have the relations*

$$\tau_{\lambda,n}(p) = \varepsilon\, \psi_{p,n}(\tau_{\lambda/p,n})\, b_{p,n}^\beta, \text{ where } \beta = \nu(r) \tag{9}$$

and

$$\varepsilon\, \psi_{p,n}(\tau_{\lambda/p,n})\, e_{p,n}^{\beta'} = \left(\frac{p+1}{M}(-1)^\beta \varepsilon - \frac{a_p}{M}\right) \tilde{P}_{\lambda/p}. \tag{10}$$

Remark. *In the main, the statements of Proposition* 1 *were proved in* [4] (*Theorem* 4). *Here we remove some of the restrictions imposed in* [4] *on* λ *in the relation* (9).

Proof. Note that $\tau_{\lambda,n}$ corresponds to the cocycle

$$k_{\lambda,n}(g) = \left(g\frac{P_\lambda}{M} - \frac{P_\lambda}{M}\right) + \frac{(1-g)P_\lambda}{M}, \tag{11}$$

where $\dfrac{(1-g)P_\lambda}{M} \in E(K_\lambda)$ is the unique (since $E(K_\lambda)_{1^\infty}$ is trivial) solution of the equation $Mx = (1-g)P_\lambda \in ME(K_\lambda)$. If $(p, \lambda) = 1$, then $K_\lambda \subset \mathcal{K}$ and $G(\bar{K}(p)/\mathcal{K}) \subset G(\bar{K}/K_\lambda)$, hence, in view of (11), we see that $\tau_{\lambda,n}(p) = P_\lambda \pmod{ME(\mathcal{K})}$. Let (α), where $\alpha \in H^1(R, E_M)$, denote the image of α in

$H^1(R, E)_M$ (cf. (1)). Again, in view of (11), we see that $(\tau_{\lambda,n})$ corresponds to the cocycle $k'_{\lambda,n}(g) = \frac{(1-g)P_\lambda}{M}$; in particular, $(\tau_{\lambda,n}) \in H^1(G(K_\lambda/K), E(K_\lambda))$. Let v be a place of K which does not divide λ. Since K_λ/K is unramified outside λ, it then follows that $(\tau_{\lambda,n})(v) \in H^1(K(v), E)^{un}$, the unramified cohomology group of E over K(v). This group is always finite and is trivial if (v, N) = 1. Gross observed that in the case $v|\lambda$, $(\tau_{\lambda,n})(v) = 0$ as well.
Hence, taking into account (1) and (6), we have $\tau_{\lambda,n} \in S^{\beta}_{\lambda,n}$.

Suppose that p divides λ. Since reduction induces an isomorphism between E_M and $E(F)_M$, then $k_{\lambda,n}(g)$ may be defined by its reduction. We shall show that if $g \in G(\bar{K}(p)/\mathcal{K}) \subset G(\bar{K}/K_{\lambda/p})$, then the reduction of the first term in (11) is trivial. Indeed, it is equal to $\frac{\tilde{g}\tilde{P}_\lambda}{M} - \frac{\tilde{P}_\lambda}{M} =$ 0, since, by virtue of (4) and the definition of P_λ, we have $\tilde{P}_\lambda = -(1 + 2 + \ldots + p)Fr_p\tilde{P}_{\lambda/p} \in ME(F)$. Hence, $\tau_{\lambda,n}(p) \in H^1(G(\mathcal{K}_p/\mathcal{K}), E_M) = B_{p,n}$. It remains to calculate the value of $\tau_{\lambda,n}(p)$ at t_p. We have

$$\frac{(1-t_p)P_\lambda}{M} = \frac{(1-t_p)I_pI_{\lambda/p}J_\lambda y_\lambda}{M} = \frac{(p+1-Tr_p)I_{\lambda/p}J_\lambda y_\lambda}{M}$$

$$= \frac{p+1}{M} I_{\lambda/p}J_\lambda y_\lambda - \frac{a_p}{M} P_{\lambda/p},$$

and for its reduction, in view of (4), (6), and (8), we have the expression:

$$\left(\frac{p+1}{M} Fr_p - \frac{a_p}{M}\right) \tilde{P}_{\lambda/p} = \tilde{f}_{p,n}(-Fr_p \tilde{P}_{\lambda/p}) = \tilde{f}_{p,n}((-1)^{\beta'}\varepsilon \tilde{P}_{\lambda/p})$$

$$= \varepsilon \psi_{p,n}(\tau_{\lambda/p}) e^{\beta'}_{p,n} . \quad \blacksquare$$

2. The Orthogonality Relation and the Characters $\psi_{p,n}$.

Let R be an extension of $\mathbb{Q}$, $n \le n'$, and $n'' = n' - n$. The exact sequence

$$0 \longrightarrow E_M \longrightarrow E_{M'} \xrightarrow{M} E_{M''} \longrightarrow 0$$

induces the exact sequence

$$0 \longrightarrow E(R)_{M''}/ME(R)_{M'} \longrightarrow H^1(R, E_M) \xrightarrow{\alpha_{n,n'}} H^1(R, E_{M'}) \xrightarrow{\alpha_{n',n''}} H^1(R, E_{M''})$$

Suppose that for all $n \le n'$ we have $E(R)_{M''} = ME(R)_{M'}$. Then $\alpha_{n,n'}$ is an injection and its image is $H^1(R, E_{M'})_M$, since $\alpha_{n'',n'}$ is also an injection and $\alpha_{n'',n'} \circ \alpha_{n',n''}$ is multiplication by M. In this situation, it is useful to identify $H^1(R, E_M)$ with $H^1(R, E_{M'})_M$. Specifically, we have the following two cases. First, suppose that R = K. In this case, since $E(K)_{l^\infty} = 0$, we identify $H^1(R, E_M)$ with H_M, where $H = \varinjlim H^1(K, E_{M'})$. Note that $S_{\lambda,n}$ coincides with $(S_{\lambda,n'})_M$ under this identification. The second case is when R = K(p) and $n' \le n(p)$. Then $E(R)_{M'} = E_{M'}$, hence, $ME(R)_{M'} = E_{M''} = E(R)_{M''}$.

Let $n \le n' \le n(\lambda)$. Then it follows from (2) that $\tau_{\lambda,n} = \alpha_{n',n}\tau_{\lambda,n'}$, or $\tau_{\lambda,n} = M''\tau_{\lambda,n'}$, in view of the identification. From (8) and Proposition 1, for $(p, \lambda) = 1$ and $s \in S_{\lambda,n}$, we obtain the relations

$$\psi_{p,n'}(\tau_{\lambda,n'}) = \psi_{p,n}(\tau_{\lambda,n}) \pmod{M} \tag{12}$$

and

$$\psi_{p,n'}(s) = M''\,\psi_{p,n}(s) \pmod{M'}. \tag{13}$$

If A is a periodic $\mathbb{Z}_l$-module, then #A denotes the minimum nonnegative integer k such that $l^k A = 0$. If $a \in A$, then $\#a = \#(a, A) = \#\mathbb{Z}_l a$.

By the definition of $m(\lambda)$, $\tau_{\lambda,n'} \ne 0$ if and only if $n' > m(\lambda)$, and in that case we have

$$\#\tau_{\lambda,n'} = n' - m(\lambda). \tag{14}$$

Let $n' - m(\lambda) \le n \le n' \le n(\lambda)$, and let $p|\lambda \in \Lambda^r$. Then $\tau_{\lambda,n'} \in S_{\lambda,n}^{\nu(r)}$. From (9), in view of the equalities $M\tau_{\lambda,n'} = 0$ and $b_{p,n}^{\nu(r)} = M''b_{p,n}^{\nu(r)}$, it follows that $M''|\psi_{p,n'}(\tau_{\lambda/p,n'})$ and $\tau_{\lambda,n'}(p) = \varepsilon(\psi_{p,n'}(\tau_{\lambda/p,n'})/M'')b_{p,n}^{\nu(r)}$. If $s \in S_{\lambda,n}^{\nu(r)}$, then, in consequence of the reciprocity law, we have the orthogonality relation $\sum_{p|\lambda} \langle \tau_{\lambda,n'}(p), s(p) \rangle_{p,n} = 0$. This relation, taking into account the previous equality and the definition of the homomorphism $\psi_{p,n}$, gives us the relation

$$\sum_{p|\lambda} (\psi_{p,n'}(\tau_{\lambda/p,n'})/M'')\,\psi_{p,n}(s) = 0 \pmod{M}. \tag{15}$$

The universality of the characters $\psi_{p,n}$ (where $n \le n(p)$) is evident from the following proposition. We use the decomposition $H = H^0 + H^1$ relative to the action of $G(K/\mathbb{Q})$.

PROPOSITION 2. *Let* A^0 *and* A^1 *be finite subgroups of* H_M^0 *and* H_M^1, *respectively,* $\psi^{0,1} \in \mathrm{Hom}(A^{0,1}, \mathbb{Z}/M)$, *and* $n' \geq n$. *Then there exist infinitely many primes* p *such that* $M' | M_p$, (i.e., $n' \leq n(p)$) *and* $\mathbb{Z}/M$(*restriction of* $\psi_{p,n}^{0,1}$ *to* $A^{0,1}$) $= (\mathbb{Z}/M)\psi^{0,1}$.

Proof. We consider in detail the case where E has no complex multiplication. The other case is handled analogously.

Let $E_M = E_M^0 + E_M^1$ be the decomposition of E_M relative to the action of $\Sigma = \{1, \sigma\}$, where σ is the automorphism of complex conjugation. Since $\sigma\zeta = \zeta^{-1}$ for all $\zeta \in \mu_M$, it then follows that $E_M^{0,1} \simeq \mathbb{Z}/M$ (cf. (7) and below). Let $e^{0,1}$ be the respective generator of $E_M^{0,1}$. Let $V = K(E_{M'})$. Note that from (7), since the pairing $[\ ,\ ]_{M'}$ is nondegenerate, it follows that $\mu_{M'} \subset V$.

Define the homomorphism $f: H_M \longrightarrow H^1(V; \mu_M) = \mathrm{Hom}(G_V^{ab}, \mu_M)$ (where $G_V^{ab} = G(V^{ab}/V)$ and V^{ab} is the maximal abelian extension of V) as follows: for all $z \in G_V^{ab}$ and $h = h^0 + h^1 \in H_{M'}$ we have

$$f(h): z \longmapsto [h^0(z), e^1]_M^2 [h^1(z), e^0]_M^2. \tag{16}$$

Suppose that f is an injection. Let W be the abelian extension of V corresponding to f(A), where $A = A^0 + A^1$, that is, W is the fixed field for $\ker f(A) \subset G_V^{ab}$.

By Kummer theory, the natural homomorphism $G(W/V) \longrightarrow \mathrm{Hom}(f(A), \mu_M)$ is an isomorphism, hence, in view of the isomorphism $f: A \longrightarrow f(A)$, we have the isomorphism $G(W/V) \longrightarrow \mathrm{Hom}(A, \mu_M)$. Suppose that $\eta \in G(W/V)$ corresponds to the element $\chi \in \mathrm{Hom}(A, \mu_M)$ such that $\chi = \zeta^{\psi^\nu}$ on A^ν, where $\zeta = [e^0, e^1]_M$. Let $\beta = \eta\sigma_1 \in G(W/\mathbb{Q})$, where σ_1 is the restriction of σ to W. According to the Chebotarev density theorem, there exist infinitely many rational primes q which do not divide Nl, are unramified in W, and such that $\beta = \mathrm{Fr} \overset{\mathrm{df}}{=\!=} \mathrm{Fr}_{W(w)/\mathbb{Q}_q}$ for some place w of W dividing q. We shall show that such primes q satisfy the conditions of the proposition.

Since β is nontrivial on K, it follows that q is a prime of K. Furthermore, $M' | (q + 1)$, since for $\xi \in \mu_{M'} \subset V$, we have $\xi^{-1} = \xi^\sigma = \xi^\beta = \xi^{\mathrm{Fr}} = \xi^q$. We see that $\mathrm{Fr}^2 = \sigma_1^2 = 1$ on $E_{M'}$, and, on the other hand, $\mathrm{Fr}^2 - a_q\mathrm{Fr} + q = 0$ on $E_{M'}$. Hence, $a_q\mathrm{Fr} = q + 1 = 0$ on $E_{M'}$, or, equivalently, $M' | a_q$. Therefore $M' | M_q$.

Let $g \in G(V/\mathbb{Q})$ and let $\alpha(g) = 1$ if $g \in G(V/K)$, and $\alpha(g) = -1$, otherwise. If $(-1)^{\nu-1}\varepsilon = 1$, then, by definition, σ acts trivially on H_M^ν, hence, $h^\nu(z^g) = gh^\nu(z)$. If $(-1)^{\nu-1}\varepsilon = -1$, then σ acts on H_M^ν by multiplication by -1, hence, $h^\nu(z^g) = \alpha(g)gh^\nu(z)$. Using (7) as well, for $h^\nu \in A^\nu$, we have $[h^\nu(Fr^2),\ e^{\nu'}]_M = [h^\nu(\eta),\ e^{\nu'}]_M^2 = \chi^\nu(h^\nu) = [e^0,\ e^1]_M^b$, where $b = \psi^\nu(h^\nu)$. Hence, considering (8), we see that $\psi^\nu_{q,n}$ is proportional to ψ^ν by a factor from $(\mathbb{Z}/M)^*$.

Now we shall prove that f is an injection. Let $h \in \ker f$. Then it follows from (16) that for all $z \in G_V^{ab}$ we have

$$[h^0(z),\ e^1]_M = [h^1(z),\ e^0]_M^{-1}. \tag{17}$$

The substitution $z \longmapsto z^{g^{-1}}$ gives us the equality

$$[h^0(z),\ ge^1]_M = [h^1(z),\ ge^0]_M^{-\alpha(g)}. \tag{18}$$

Let $e^{0,1}$ be the respective generator of $E^{0,1}$ such that $(M'/M)e_1^{0,1} = e^{0,1}$. Define the homomorphism ρ: $G(V/K) \longrightarrow GL_2(\mathbb{Z}/M')$ so that $g\begin{pmatrix} e_1^0 \\ e_1^1 \end{pmatrix} = \rho(g)\begin{pmatrix} e_1^0 \\ e_1^1 \end{pmatrix}$. Since $1 \in B(E)$, it then folows that $\operatorname{Im}\rho = GL_2(\mathbb{Z}/M')$. Furthermore, the homomorphism ρ: $G(V/K) \longrightarrow GL_2(\mathbb{Z}/M')$ is an injection, and is an isomorphism when $K \subset \mathbb{Q}(E_{M'})$. The field K is a subfield of $\mathbb{Q}(E_{M'})$ if and only if $l \equiv 3 \pmod 4$ and $K = \mathbb{Q}(\sqrt{-1})$, in which case $\rho(G(V/K)) = \ker \delta'$, where the homomorphism δ': $GL_2(\mathbb{Z}/M') \longrightarrow \{\pm 1\}$ is induced by det: $GL_2(\mathbb{Z}/M') \longrightarrow (\mathbb{Z}/M')^*$ and the unique nontrivial homomorphism δ: $(\mathbb{Z}/M')^* \longrightarrow \{\pm 1\}$ (cf. §4 in [1]).

Let $g_0 \in G(V/K)$ be such that $\rho(g_0) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Substituting gg_0 for g in (18), we obtain the equality

$$[h^0(z),\ ge^0]_M = [h^1(z),\ ge^1]_M^{\alpha(g)}. \tag{19}$$

Let $K \subset \mathbb{Q}(E_{M'})$. Then there exists an element $g_1 \in G(V/\mathbb{Q}/E_{M'}))$ such that $\alpha(g_1) = -1$. Obviously, the relations (18) and (19) for $g = 1$ and $g = g_1$, respectively, together imply that $[h^0(z),\ e^{0,1}]_M = 1$ and $[h^1(z),\ e^{0,1}]_M = 1$, hence, $h^0(z) = h^1(z) = 0$.

Suppose that $K \subset \mathbb{Q}(E_{M'})$. Then $K = \mathbb{Q}(\sqrt{-1})$, hence $l > 3$, since we are assuming that $K \neq \mathbb{Q}(\sqrt{-3})$. Since $l > 3$, then there exists an element $a \in \mathbb{Z}/M'$ such that $\delta(a) = 1$ but $a \not\equiv 1 \pmod{l}$. Let $g_2 \in G(V/K)$ be such that $\rho(g_2) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$. Comparing (18) and (19) for $g = 1$ and $g = g_2$, respectively, we obtain $h^0(z) = h^1(z) = 0$.

Thus, $\mathrm{res}_{V/K}(h) = 0$. It remains to show that $\mathrm{res}_{V/K}\colon H_M \longrightarrow H^1(V, E_M)$ is an injection. Let $g_3 \in G(V/K)$ be such that $\rho(g_3) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and $G_3 = \{1, g_3\}$. Then G_3 is a subgroup of order 2 in the center of $G(V/K)$. Obviously, we have $E_M = 0$ and $H^1(G_3, E_M) = 0$. In view of the spectral sequence applied to the group $G(V/K)$ and its normal subgroup G_3, we see that $\ker(\mathrm{res}_{V/K}) = H^1(G(V/K), E_M)$ is the trivial group. ∎

We need the following corollary to Proposition 2.

PROPOSITION 3. *Let* A^0 *and* A^1 *be finite subgroups of* H_M^0 *and* H_M^1, *respectively, let* $f_{1,2}^{0,1}\colon \mathrm{Hom}(A^{0,1}, \mathbb{Z}/M) \longrightarrow C_{1,2}^{0,1}$ *be surjective homomorphisms, and suppose that* $n' \geq n$. *Then there exist infinitely many primes* p *such that* $M' \mid M_p$ *and* $\#f_{1,2}^{0,1}$(*restriction of* $\psi_{p,n}^{0,1}$ *to* $A^{0,1}$) $= \#C_{1,2}^{0,1}$.

Proof. By virtue of Proposition 2, it is enough to prove the existence of characters $\psi^{0,1} \in \mathrm{Hom}(A^{0,1}, \mathbb{Z}/M)$ such that $\#f_{1,2}^{0,1}(\psi^{0,1}) = \#C_{1,2}^{0,1}$. There exists a character ψ^{ν}, since otherwise $\mathrm{Hom}(A^{\nu}, \mathbb{Z}/M)$ is the union of two proper subgroups, which is impossible. ∎

Let $\lambda \in \Lambda^r$, $\delta \in \Lambda^k$, and $\delta \mid \lambda$. Let $S_{\lambda,\delta,n}$ denote the group $S_{\lambda,n}$ when $\delta = 1$, the intersection of $S_{\lambda,n}$ with the kernels of the characters $\psi_{p,n}$ for all $p \mid \delta > 1$. We have the following proposition.

PROPOSITION 4. *Let* $\nu \in \{0, 1\}$ *and* $r - k > 0$. *Then* $\#S_{\lambda,\delta,n}^{\nu} = n$.

Proof. Since $S_{\lambda,\delta,n-1}^{\nu}$ is the subgroup of $S_{\lambda,\delta,n}^{\nu}$ of all elements of period l^{n-1}, it is sufficient to prove the equality

$$[S_{\lambda,\delta,n}^{\nu}/S_{\lambda,\delta,n-1}^{\nu}] \geq l^{r-k}. \tag{20}$$

Note that (20) implies that the multiplicity of n in the sequence of invariants of $S_{\lambda,\delta,n}^{\nu}$ is not less than $(r - k)/n$.

If v is a place of K, then $H_{v,n}$ denotes $H^1(K(v), E_M)$ and $A_{v,n}$ denotes $E(K(v))/M$. If β is a set of places of K, then $H_{\beta,n}$ denotes the locally

compact group $\prod_{v|\beta} H_{v,n}$. The pairing $\langle\ ,\ \rangle_{\beta,n} = \sum_{v|\beta} \langle\ ,\ \rangle_{v,n}$ identifies the group $H_{\beta,n}$ with its dual group. We use multiplicative notation: $v|\beta$ signifies that $v \in \beta$ and $\beta_1\beta_2$ denotes $\beta_1 \cup \beta_2$. An element of Λ is identified with its set of prime divisors. Let $\beta = \lambda/\delta$ and let Z_n be the image of $S_{\lambda,\delta,n}$ in $H_{\beta,n}$. It is sufficient to prove that Z_n is an isotropic subgroup of $H_{\beta,n}$, because then Z_n^ν is an isotropic subgroup of $H_{\beta,n}^\nu$, hence $[Z_n] = [H_{\beta,n}]^{1/2} = M^{r-k}$ and $[Z_{n-1}^\nu] = (M/1)^{r-k}$ (the latter equaltiy holds since, in the previous equality, n is any natural number $\leq n(\lambda)$). Thus, $[Z_n^\nu/Z_{n-1}^\nu] = 1^{r-k}$, whence follows (20).

Let α be the set of all places of K. By the Tate-Poitou theorem (cf. [9]), the image Y_1 of the group H_M in $H_{\alpha,n}$ is an isotropic subgroup of $H_{\alpha,n}$. Let Y_3 denote the group $\prod_{p|\delta} B_{p,n} \prod_{(v,\lambda)=1} A_{v,n}$. Since $A_{v,n}$ is an isotropic subgroup of $H_{v,n}$, by local Tate theory, and $B_{p,n}$ is an isotropic subgroup of $H_{p,n}$ (cf. §1), it follows that Y_3 is an isotropic subgroup of $H_{\alpha/\beta,n}$.

Let $Y_2 = H_{\beta,n} \times Y_3$. We have $Z_n = Pr_\beta(Y_1 \cap Y_2)$. Obviously, the equality $\langle Z_n, Z_n\rangle_{\beta,n} = 0$ holds. Let $z \in H_{\beta,n}$ and $\langle Z_n, z\rangle_{\beta,n} = 0$. Let z' denote an element of $H_{\alpha,n}$ such that $Pr_\beta(z') = z$ and $Pr_{\alpha/\beta}(z') = 0$. Since z' is orthogonal to $Y_1 \cap Y_2$, then by Pontryagin theory, $z' = z_1 + z_2$, where $z_1 \in Y_1^\perp = Y_1$ and $z_2 \in Y_2^\perp$. We have $Pr_\beta(z_2) \in H_{\beta,n}^\perp = 0$ and $Pr_{\alpha/\beta}(z_2) \in Y_3^\perp = Y_3$. Hence, $z' - z_2 = z_1 \in Y_1 \cap Y_2$ and $Pr_\beta(z' - z_2) = z$, that is, $z \in Z_n$. ∎

We now have all that is necessary for the study of the group $X = Ш(K, E)_{1^\infty}$.

3. A Structural Theorem for X.

Let Λ_n^r denote the subset of Λ^r consisting of all elements λ such that $n(\lambda) \geq n$; then Λ_n denotes $\cup\Lambda_n^r$. Let $\varphi_{p,n}^\nu$ be the restriction of $\psi_{p,n}^\nu$ to the Selmer group $S_M^\nu = S_{1,n}^\nu$ and $\Phi_{\lambda,n}^\nu$ the subgroup of $\mathrm{Hom}(S_M^\nu, \mathbb{Z}/M)$ generated by $\varphi_{p,n}^\nu$ for all $p|\lambda$.

In the sequel, we shall assume that $n'' \geq n' \geq n$. We have the following proposition.

PROPOSITION 5. *Let* $\delta \in \Lambda_{n''}^k$, $n > m(\delta)$, $\delta q \in \Lambda_{n''}^{k+1}$, *and* $\#\psi_{q,n}(\tau_{\delta,n}) = \#\tau_{\delta,n}$. *Then* $m(\delta q) \leq m(\delta)$. *If, moreover,* $n'' - n \geq m(\delta q)$ *and* $\iota = 1 - \nu(k)$,

then $\#\varphi^{\iota}_{q,n} \pmod{\Phi^{\iota}_{\delta,n}} \le m(\delta) - m(\delta q)$.

Proof. By Proposition 1, $\tau_{\delta q,n}(q) = \varepsilon\psi_{q,n}(\tau_{\delta,n})b^{\iota}_{q,n}$. Then, in view of (14) and our assumptions, we have $n - m(\delta q) = \#\tau_{\delta q,n} \ge \#\psi_{q,n}(\tau_{\delta,n}) = \#\tau_{\delta,n} = n - m(\delta)$. Hence, $m(\delta q) \le m(\delta)$.

It is a consequence of (15) that $a\varphi^{\iota}_{q,n} \in \Phi^{\iota}_{\delta,n}$, where $\mathbb{Z}/M \ni a = \psi_{q,n'}(\tau_{\delta,n'})/l^{m(\delta q)}$ and $n' = n + m(\delta q)$. Since $\operatorname{ord}_l(\psi_{q,n}(\tau_{\delta,n})) = n - \#\tau_{\delta,n} = m(\delta)$ and (12) holds, it then follows that $\operatorname{ord}_l(a) = m(\delta) - m(\delta q)$. ∎

If $\delta \in \Lambda^k$, where $r \ge k$, then $m_r(\delta)$ denotes $\min m(\lambda)$, where λ runs through the set of elements of Λ^r for which δ is a divisor. We have the following proposition.

PROPOSITION 6. *If* $\delta \in \Lambda^k$ *is such that* $m(\delta) < \infty$, *then* $m_{k+1}(\delta) \le m(\delta)$.

Proof. Let $n = n(\delta)$; then $n > m(\delta)$, since $m(\delta) < \infty$. According to Proposition 3, there exists q such that $\delta q \in \Lambda^{k+1}_n$ and $\#\psi_{q,n}(\tau_{\delta,n}) = \#\tau_{\delta,n}$. Then, by Proposition 5, we have the equality $m(\delta q) \le m(\delta)$. ∎

Recall that, for $r \ge 0$, m_r denotes $m_r(1)$. The following proposition holds.

PROPOSITION 7. *The sequence* $\{m_r\}$ *is such that* $m_r \ge m_{r+1}$.

Proof. By assumption, the point P_1 has infinite order. Hence $m_0 < \infty$ (m_0 is the exponent of the highest power of l dividing P_1 in $E(K)$). Now apply Proposition 6 and use induction on r. ∎

Let $T^{\nu}_{\delta,n}$ denote the quotient group of $\operatorname{Hom}(S^{\nu}_M, \mathbb{Z}/M)$ with respect to $\Phi^{\nu}_{\delta,n}$. Recall that ν' denotes $1 - \nu$, where $\nu \in \{0, 1\}$. We have the following proposition.

PROPOSITION 8. *Let* $k \ge 0$, $r \ge k$, $\alpha = \nu(k)$, $\beta = \nu(r)$, *and* $n'' \ge n' \ge n$. *Let* $\delta \in \Lambda^k_{n''}$ *be such that* $x \overset{\text{df}}{=\!=} m_r(\delta) < n$ *and* $\lambda \in \Lambda^r_n$ *such that* $m(\lambda) = x$. *Then there exists* $q \in \Lambda^1$ *satisfying the following conditions*:

0) $(q, \lambda) = 1$ *and* $M''|M_q$;

1) $\#\psi^{\beta}_{q,n'}(\tau_{\lambda,n'}) = \#\tau_{\lambda,n'}$;

2) *at our discretion, one of the following two conditions is fulfilled*:

21) $\#\psi^{\alpha'}_{q,n'} \pmod{\Phi^{\alpha'}_{\delta,n'}} = \#T^{\alpha'}_{\delta,n'}$;

22) *if* $k \ge 1$, *then for a preassigned* $p_1|\delta$, $\#\varphi^{\alpha'}_{q,n'}(\tau_{\delta/p_1,n'}) = \#\tau_{\delta/p_1,n'}$;

3) $\#\psi^{\alpha}_{q,n'}(\tau_{\delta,n'}) = \#\tau_{\delta,n'}$;

4) *there exists* $p|(\lambda/\delta)$ *such that* $m(\lambda q/p) = x$.

Moreover, if $\alpha = \beta'$ *and* $n'' - n \geq y \overset{df}{=\!=} m(\delta)$, *then we may choose a* p *satisfying* 4) *so that the following condition is fulfilled*:

5) $\#\psi^{\alpha}_{p,n}(\tau_{\delta,n}) = \#\tau_{\delta,n}$.

Proof. By Proposition 4, there exists $s \in S^{\beta'}_{\lambda,\delta,n}$ such that $\#s = n$. According to Proposition 3, there exists $q \in \Lambda^1$ satisfying conditions 0) - 3) and the following condition:

6) $\#\psi^{\beta'}_{q,n'}(s) = \#s = n$.

Since $\tau_{\lambda q,n}$ and s are orthogonal (cf. (15)), we have the relation

$$\sum_{p|(\lambda/\delta)} \psi^{\beta'}_{p,n}(s)\psi^{\beta}_{p,n}(\tau_{\lambda q/p,n}) = -\psi^{\beta'}_{q,n}(s)\psi^{\beta}_{q,n}(\tau_{\lambda,n}) \overset{df}{=\!=} z \in \mathbb{Z}/M.$$

It follows from (12) and (13) that conditions 1) and 6) are satsified as well after the substitution $n' \mapsto n$. Hence, $\#z = n - x > 0$. By the definition of x, we have $\#\psi^{\beta}_{p,n}(\tau_{\lambda q/p,n}) \leq \#\tau_{\lambda q/p,n} \leq n - x$. Thus, there exists $p|(\lambda/\delta)$ such that the following conditions are fulfilled:

7) $\#\psi^{\beta}_{p,n}(\tau_{\lambda q/p,n}) = n - x$ and, hence, $m(\lambda q/p) = x$;

8) $\#\psi^{\beta'}_{p,n}(s) = n$.

If $\alpha = \beta'$ and $n'' - n \geq y$, then we may take the element $\tau_{\delta,n+y}$ to be s. If $\tau_{\delta,n} = 0$, then 5) obviously holds. Otherwise, $\#\tau_{\delta,n} = n - y > 0$, and then 5) follows from 8), since $\tau_{\delta,n} = l^{y}\tau_{\delta,n+y}$. ∎

Moreover, we have the following proposition.

PROPOSITION 9. *Let* $n > m_0$ *and* $n' = m + m_0$. *Suppose that* $r = k + 1 \geq 1$, $\delta \in \Lambda^{k}_{n'}$, *and* $m(\delta) = m_{r-1}$. *Then there exists* p_r *such that* $\delta p_r \in \Lambda^{r}$ *and* $m(\delta p_r) = m_r(\delta)$. *For every such* p_r, *if* $\beta = \nu(r)$, *we have*

$$\#\varphi^{\beta}_{p_r,n} \pmod{\Phi^{\beta}_{\delta,n}} = \#T^{\beta}_{\delta,n} = m_{r-1} - m_r(\delta) \tag{21}$$

$$\#\psi_{p_r,n}(\tau_{\delta,n}) = \#\tau_{\delta,n} \tag{22}$$

$$\#\varphi^{\beta'}_{p_r,n} \pmod{\Phi^{\beta'}_{\delta,n}} \geq m_{r-2} - m_{r-1}, \text{ where } r \geq 2. \tag{23}$$

Proof. Let $\lambda \in \Lambda_{x+1}^{r}$, where $x = m(\delta)$, be such that $m(\lambda) = x$. The existence of p_r follows from Proposition 8 applied to δ and λ (and $n'' = n'$, $n' = n$, $n = x + 1$).

Now apply Proposition 8 to δ and $\lambda = \delta p_r$ (where $n'' = n'$ and $n' = n$). Select a q corresponding to condition 21). From conditions 1) and 21), and Proposition 5, it follows that $\#T_{\delta,n}^{\beta} \le y - x$, where $y = m(\delta) = m_{r-1}$. The element $a = \tau_{\delta q, y}$ belongs to $S_{1,y}^{\beta} \subset S_{1,n}^{\beta}$, by virtue of Proposition 1 and the relation $\tau_{\delta', y} = 0$ for all $\delta' \in \Lambda_{y}^{r-1}$ (by the definition of $m_{r-1} = y$). Since $a = l^{n-y}\tau_{\delta,n}$, it then follows from 7) that $\#\varphi_{p_r,n}^{\beta}(a) = \#\varphi_{p_r,n}^{\beta}(\tau_{\delta q,n})$ $- (n - y) = y - x$. Since $a \perp \Phi_{\delta,n}$, then we have that $\#\varphi_{p_r,n}^{\beta} \pmod{\Phi_{\delta,n}^{\beta}} \ge$ $y - x$ and, hence, (21) is true.

Analogously, the element $b = \tau_{\delta, m_{r-2}} \in S_{1,n}^{\beta'}$ and $b \perp \Phi_{\delta,n}^{\beta'}$. According to 5), (22) is true, hence, $\#\varphi_{p_r,n}^{\beta'}(b) = m_{r-2} - y$, and (23) holds. ∎

If ω is the sequence $p_0, \ldots, p_r$, then for $0 \le i \le r$, $\omega(i)$ denotes the product $p_0 \ldots p_r$. Define Ω_n^r to be the set of sequences $\omega = (p_0, \ldots, p_r)$ such that $\omega(r) \in \Lambda_n^r$ and $m(\omega(i)) = m_i$ for $0 \le i \le r$. In particular, Ω_n^0 contains only $p_0 \stackrel{df}{=} 1$.

A priori, by the Mordell-Weil theorem, and because $E(K)_{l^\infty}$ is trivial, the group $(E(K)/M)^{\nu}$ is isomorphic to $(\mathbb{Z}/M)^{g^\nu}$, where $g^0 + g^1$ is equal to the rank of E over K. The sequence (1) induces the exact sequence

$$0 \longrightarrow (E(K)/M)^{\nu} \longrightarrow S_{1,n}^{\nu} \longrightarrow X_{1,n}^{\nu} \longrightarrow 0. \qquad (24)$$

Here $X_{1,n}^{\nu} = X_M^{\nu}$. By the weak Mordell-Weil theorem, the group $S_{1,n}^{\nu}$ is finite.

Recall that the Heegner point P_1 has a unique representation $P_1 = l^{m_0}æ$, where $æ \in E(K) \setminus lE(K)$.

Let $n > m_0$, $r = 1$, $\omega = p_0 = 1$, and choose p_1 as in Proposition 9. Then $T_{\delta,n}^{0} = \mathrm{Hom}(S_{1,n}^{0}, \mathbb{Z}/M)$ and $m_1(\delta) = m_1$. According to (21), we have $\#S_{1,n}^{0} = \#T_{\delta,n}^{0} = m_0 - m_1 < n$. Hence, in view of (24), it follows that $g^0 =$

0, $S^0_{1,n} = S^0_{1,m_0-m_1}$, and $X^0 = X^0_{1,n} = X^0_{1,m_0-m_1}$ is a finite group. In particular, the invariants x^0_i of X^0 coincide with the invariants of $T^0_{1,n}$.

Moreover, it follows from (22) that $\#\varphi^1_{p_1,n}$ (æ(mod ME(K))) = n, hence, $S^1_{1,n}$ is the direct sum of $\mathbb{Z}/M$æ (mod ME(K)) $\propto \mathbb{Z}/M$ and $Y = \ker \varphi^1_{p_1,n}$.

Let r = 2, $\omega = (1, p_1)$, and $\delta = p_1$. Then $T^1_{\delta,n}$ is the dual group for Y. Hence, it follows from (21) that $\#Y = \#T^1_{\delta,n} = m_1 - m_2(\delta)$ and, in view of (24), , we have $g^1 = 1$ and $X^1 = X^1_{1,n} = X^1_{1,m_1-m_2(\delta)}$ is finite and isomorphic to Y. In particular, the invariants x^1_i of the group X^1 coincide with the invariants of the group $T^1_{p_1,n}$.

In [1] it was proved that $g^0 = 0$, and in [4] that $g^1 = 1$ and $[X]|1^{2m_0}$.

Recall that, for $\nu \in \{0, 1\}$ and $j \in \mathbb{N}$, $\nu(j)$ denotes the element of $\{0, 1\}$ such that $j - \nu(j) - 1$ is even, and (j, ν) denotes $j - |\nu - \nu(j)|$. We have the following theorem.

THEOREM 1. *Let* $r > 0$, $n > m_0$, *and* $n' = n + m_0$. *Then the set* $\Omega^r_{n'}$ *is nonempty. Moreover, for all* $\omega \in \Omega^{r-1}_{n'}$, *there exists* $p_r|(\omega, p_r) \in \Omega^r_{n'}$. *Let* $\omega \in \Omega^r_{n'}$. *Then for* $1 \le j \le r$ *we have the equality* $\#\varphi_{p,n}(\tau_{\omega(j-1),n}) = \#\tau_{\omega(j-1),n}$, *and if* $\nu \in \{0, 1\}$ *is such that* $r - \nu > 0$, *then for* $1 + \nu \le j \le r$ *we have*

$$\#\varphi^\nu_{p_j,n} (\mathrm{mod}\ \Phi^\nu_{\omega(j-1),n}) = m_{(j,\nu)-1} - m_{(j,\nu)} = x^\nu_{j-\nu}. \tag{25}$$

Proof. For r = 1, the theorem was proved above. Therefore, by induction, it is sufficient to prove the theorem for $r \ge 2$, assuming it to be true for all $r' > r$. Let $\omega \in \Omega^{r-1}_{n'}$, $\delta = \omega(r - 1)$, and choose p_r as in Proposition 9 so that, in particular, the relations (21) - (23) hold. Since the theorem is true for r - 1, it then follows that $\#T^\nu_{\delta,n} = x^\nu_{r-\nu}$, and for $\beta = \nu(r)$, $x^{\beta'}_{r-1-\beta'} = m_{r-2} - m_{r-1}$. Hence the equality $x^{\beta'}_{r-\beta'} = m_{r-2} - m_{r-1}$ holds, by (23) and the inequality $x^{\beta'}_{r-\beta'} \le x^{\beta'}_{r-1-\beta'}$. In view of (21), (22), and the induction hypothesis, it remains only to prove that $m_r(\delta) = m_r$. This will be done if we prove that the set $\Omega^r_{n'}$ is nonempty. Indeed, using the fact that $(\omega', p') \in \Omega^r_{n'}$, as above, we then have $m_{r-1} - m_r = x^\beta_{r-\beta}$ $= m_{r-1} - m_r(\delta)$. If $u = m_r + 1$ for $0 \le k \le r$, then U^k denotes the set of

pairs $\omega \in \Omega_{n'}^{k}$, $\lambda \in \Lambda_u^r$ such that $\omega(k)|\lambda$ and $m(\lambda) = m_r$. It follows from Proposition 9 that $\Omega_{n'}^{r}$ is nonempty if U^{r-1} is nonempty. Then, since U^0 is nonempty, it is sufficient to prove that U^{k+1} is nonempty if $k < r - 1$ and U^k is nonempty. Then, by induction, U^{r-1} is nonempty. Let $(\omega, \lambda) \in U^k$. Apply Proposition 8 to $\delta = \omega(k)$, λ (and $n'' = n'$, $n = u$), and choose a q corresponding to condition 21). We need to show that $m(\delta q) = m_{k+1}$; then the pair $((\omega, q), \lambda q/p)$ will belong to U^{k+1}. By Theorem 1 for $k + 1 \le r - 1$, we have that $m_k - m_{k+1} = x_{k+1-\alpha'}^{\alpha'} = \#T_{\delta,n}^{\alpha'}$, where $\alpha = \nu(k)$. On the other hand, in view of Propsition 5 and condition 21), we see that $\#T_{\delta,n}^{\alpha'} \le m_k - m(\delta q)$. Hence, $m(\delta q) \le m_{k+1}$, but, by the definition of m_{k+1}, we have $m_{m+1} \le m(\delta q)$. Thus, $m(\delta q) = m_{k+1}$. ∎

The purpose of the remainder of §3 is the parameterization of X and its dual group by a sequence of prime numbers more arbitrary than Ω. This is essential for an effective description of the structure of X and its dual group, and for the parameterization of X by the classes $\tau_{\lambda,n}$ and of its dual group by the characters $\varphi_{p,n}$.

For $r \ge 0$ define $\Pi_{n'}^{r}$ to be the set of sequences $\pi = (p_0, \ldots, p_r)$ such that $\pi(r) \in \Lambda_{n'}^{r}$; if $r > 0$ and $1 \le j \le r$, then

$$\#\psi_{p_j,n'}(\tau_{\pi(j-1),n'}) = \#\tau_{\pi(j-1),n'} \tag{26}$$

and, if $r \ge 2$ and $2 \le j \le r$, moreover,

$$\#\psi_{p_j,n'}(\tau_{\pi(j-1)/p_1,n'}) = \#\tau_{\pi(j-1)/p_1,n'}. \tag{27}$$

Recall that $m = \min_{r\ge 0} m_r = \lim_{r\to\infty} m_r$. Let $\lambda \in \Lambda^r$ be such that $m(\lambda) = m$. As in the above proof of the nonemptiness of U^{r-1}, using Proposition 8, condition 22), and induction, we shall prove that for all n' there exists $\pi \in \Pi_{n'}^{r}$ such that $m(\pi(r)) = m$. We shall say that $\pi \in \Pi_{n'}^{r}$ is minimal if $m(\pi(r)) = m$. From Propositions 5 and 8 it follows that if $\pi' \in \Pi_{n'}^{r-1}$ is minimal, then there exists p_r such that $(\pi', p_r) \in \Pi_{n'}^{r}$ is minimal.

Let $n > m_0$ and $n' \ge n + m_0$. Assume that $r \ge 2$, that $\pi \in \Pi_{n'}^{r}$ is minimal, and $\pi - p_r$ is minimal as well. If $\nu \in \{0, 1\}$, then $u(\nu)$ denotes $r - \nu$ if $r - \nu$ is even (i.e., $\nu = \nu(r + 1)$), otherwise (i.e., when $\nu = \nu(r)$), $u(\nu)$ denotes $r - \nu - 1$. Let $\lambda^\nu = \pi(u(\nu) + \nu)$. By Proposition 9,

$T^{\nu}_{\lambda^{\nu},n} = 0$, that is, $\varphi^{\nu}_{p_j,n}$, where $1 \le j \le u(\nu) + \nu$, generate $\mathrm{Hom}(S^{\nu}_{M}, \mathbb{Z}/M)$. In particular, the homomorphism α^{ν}_{2} in (33) is an isomorphism. For $1 - \nu \le i \le u(\nu)$, set

$$\lambda^{\nu}_{i} = \pi(i + \nu)/p_{\nu(i)} \tag{28}$$

and

$$z^{\nu}_{i} = \tau_{\lambda^{\nu}_{i},n+m(\lambda^{\nu}_{i})} \in S_{\lambda^{\nu}_{i},n} \tag{29}$$

For $1 \le i \le u(\nu)$ and $1 - \nu \le j \le u(\nu)$, define the elements $a^{\nu}_{ij} \in \mathbb{Z}/M$ as follows: if $j > i$, or if $j + \nu = 1$ and i is even, then

$$a^{\nu}_{ij} = 0, \tag{30}$$

and for the remaining pairs ij:

$$a^{\nu}_{ij} = \psi_{p_{j+\nu},n+m(\lambda^{\nu}_{i})}\left(\tau_{\lambda^{\nu}_{i}/p_{j+\nu},n+m(\lambda^{\nu}_{i})}\right)/l^{m(\lambda^{\nu}_{i})}. \tag{31}$$

From the orthogonality relation (15), with $n' = n + m(\lambda^{\nu}_{i})$ and $\lambda = \lambda^{\nu}_{i}$, it follows that for $1 \le i \le u(\nu)$ we have

$$\sum_{j=1-\nu}^{u(\nu)} a_{ij}\varphi_{p_{j+\nu},n} = 0. \tag{32}$$

Let $a = \{a_{ij}\}$ be a square matrix of dimension u with coefficients n $\mathbb{Z}/M$. Let $A(a)$ denote the abelian M-periodic group given by generators 1_j, where $1 \le j \le n$, and relations $\sum_{j=1}^{u} a_{ij}1_j = 0$. By identifying 1_j with the element of $(\mathbb{Z}/M)^u$ having the j^{th} component equal to 1 and the others equal to zero, we can identify $A(a)$ with the quotient group of $(\mathbb{Z}/M)^u$ with respect to the subgroup generated by the rows of a.

Let $r \ge 2 + \nu$, $a^{\nu} = \{a^{\nu}_{ij}\}$ for $1 \le i,j \le u(\nu)$, and $A^{\nu} = A(a^{\nu})$. Sending 1_j to $\varphi^{\nu}_{p_{j+\nu},n} \pmod{\varphi^{\nu}_{p_{\nu},n}}$ and taking (32) into account, we define the surjective homomorphism α^{ν}_{1} in (33). We have the isomorphisms

$$\begin{array}{ccccc} A^\nu & \xrightarrow[\sim]{\alpha_1^\nu} & \Phi^\nu_{\lambda^\nu,n}/(\varphi^\nu_{p_\nu,n}) & \xrightarrow[\sim]{\alpha_2^\nu} & \mathrm{Hom}(S_M^\nu,\ \mathbb{Z}/M)/(\varphi^\nu_{p_\nu,n}) \\ & & & & \uparrow \alpha_3^\nu \\ & & X^\nu & \xrightarrow[\sim]{\alpha_4^\nu} & \mathrm{Hom}(X^\nu,\ \mathbb{Z}/M). \end{array} \tag{33}$$

Here $\varphi^0_{p_0,n} \overset{\mathrm{df}}{=\!=} 1$ and $(\varphi^\nu_{p_\nu,n})$ is the subgroup generated by $\varphi^\nu_{p_\nu,n}$. It was proved above that the natural injection α_2^ν is an isomorphism. The isomorphism α_3^ν is induced by the exact sequence (24), and α_4^ν is any isomorphism between X^ν and its dual group. We shall prove below that α_1^ν is an isomorphism as well.

If $b \in \mathbb{Z}/M$, then $\mathrm{ord}_1(b) \overset{\mathrm{df}}{=\!=} n - \#b$. Using Proposition 5, (26), and (27), we obtain the relation

$$\mathrm{ord}_1(a^\nu_{ii}) = m(\lambda^\nu_i/p_{i+\nu}) - m(\lambda^\nu_i) \le m_0 < n. \tag{34}$$

Since $a_{ij} = 0$ if $j > i$, it then follows that $\mathrm{ord}_1[A^\nu] \le z^\nu \overset{\mathrm{df}}{=\!=} \sum_{i=1}^{u(\nu)} \mathrm{ord}_1(a^\nu_{ii})$. Equation (34) implies that $z^0 + z^1 = 2m_0 - m(\pi(r-1)) - m(\pi(r)/p_1)$. We shall show that $m(\pi(r)/p_1) = m$. Since $m(\pi(r-1)) = m$, by the conditions on π, it follows that

$$\mathrm{ord}_1([A^0][A^1]) \le z^0 + z^1 = 2m_0 - 2m. \tag{35}$$

Let $\lambda = \pi(r)$. Since $\tau_{\lambda,n+m}$ and $s = \tau_{\lambda/(p_1p_r),n+m}$ are orthogonal, considered as elements of $S_{\lambda,n}$ (cf. (15)), then if $\theta_1 = \psi_{p_1,n+m}(\tau_{\lambda/p_1,n+m})/l^m$, it follows that

$$\theta_1\psi_{p_1,n}(s) = \theta_2 \overset{\mathrm{df}}{=\!=} -(\varphi_{p_r,n+m}(\tau_{\lambda/p_r,n+m})/l^m)\psi_{p_r,n}(s).$$

From conditions (26) and (27) and the equality $m(\lambda/p_r) = m$, we obtain that $\#\theta_2 = \#s > 0$. Thus, $\theta_1 \in (\mathbb{Z}/M)^*$ and $m(\lambda/p_1) = m$, since otherwise $m(\lambda/p_1) > m$, which implies that $\theta_1 \in l(\mathbb{Z}/M)$.

Since $\mathrm{ord}_1([X^0][X^1]) = 2m_0 - 2m$ (cf. Theorem D of the introduction) and (35) holds, it follows that the surjective homomorphisms α_1^0 and α_1^1 are isomorphisms.

Note that $\psi_{p_{j+\nu},n}(z_i^\nu) = 0$ for $1 \le j \le i$, because then, by Proposition

1, $z_i^\nu(p_{j+\nu}) \in B^\nu_{p_{j+\nu},n}$ and $\psi_{p,n}(B_{p,n}) = 0$ (cf. §1). We see from (26) and (27) that, if $u(\nu) \geq 2$ and $i < u(\nu)$, then $\varphi_{p_{i+1+\nu}}(z_i^\nu) \in (\mathbb{Z}/M)^*$. According to (14), $\#z_i^\nu = n + m(\lambda_i^\nu) - m(\lambda_i^\nu) = n$. We shall show that if $(c_1,\ldots,c_{u(\nu)}) \in (\mathbb{Z}/M)^{u(\nu)}$ is such that

$$\sum_{i=1}^{u(\nu)} c_i z_i^\nu = 0, \tag{36}$$

then $c_i = 0$ for $1 \leq i \leq u(\nu)$. It is sufficient to consider the case $u(\nu) \geq 2$. Then for $2 \leq j \leq u(\nu) + \nu$, we apply the characters $\psi_{p_{j+\nu},n}$ to (36). By the properties of z^ν noted above, we obtain $c_1 = \ldots = c_{u(\nu)-1} = 0$ and, hence, $c_{u(\nu)} = 0$ as well.

Then, from the definition of z_i^ν and Proposition 1, it follows that $z_i^\nu(p_{j+\nu}) = a_{ij}^\nu b^\nu_{p_{j+\nu},n} \pmod{E(K(p_{j+\nu}))/M}$. Thus, $w = \sum_{i=1}^{u(\nu)} c_i z_i^\nu \in S^\nu_{p_\nu,n}$ and the following relation holds for $1 \leq j \leq u(\nu)$:

$$\sum_{i=1}^{u(\nu)} c_i a_{ij}^\nu = 0. \tag{37}$$

Note that the orthogonality between elements of $S^1_{p_1,n}$ and $æ \pmod{ME(K)}$, in view of the fact that $\varphi_{p_1,n}(æ \pmod{ME(K)}) \in (\mathbb{Z}/M)^*$ and (26), implies that $S^1_{p_1,n} = S^1_M$. Therefore, (37) is the condition that w belong to the group S^ν_M. Let $B^\nu = \{c_1,\ldots,c_{u(\nu)}\}$ be the subgroup of $(\mathbb{Z}/M)^{u(\nu)}$ defined by (37). If a is a matrix, then a^{tr} denotes the transpose of the matrix a.

The pairing $(\mathbb{Z}/M)^{u(\nu)} \times (\mathbb{Z}/M)^{u(\nu)} \longrightarrow \mathbb{Z}/M$, under which $(1_i, 1_j) = \delta_{ij}$ (the Kronecker symbol), induces the isomorphism β_2^ν in (38). The isomorphism β_1^ν is any isomorphism of the dual groups. Then β_3^ν is an injection under which $(c_1,\ldots,c_{u(\nu)}) \mapsto w$. The isomorphism β_4^ν is induced by the homomorphism $S^\nu_M \longrightarrow X^\nu$ in (24). We have

$$A(a^{\nu\ tr}) \xrightarrow[\sim]{\beta_1^\nu} \mathrm{Hom}(A(a^{\nu\ tr}), \mathbb{Z}/M) \xrightarrow[\sim]{\beta_2^\nu} B^\nu \xrightarrow[\sim]{\beta_3^\nu} \ker \varphi^\nu_{p_{2\nu}} \xrightarrow[\sim]{\beta_4^\nu} X^\nu. \tag{38}$$

We shall show that, for $n > 2m_0$, β_3^ν is also an isomorphism. Let a be a square matrix of dimension u over $\mathbb{Z}/M$ such that $a_{ij} = 0$ for $j > i$ and $\xi = \sum_{i=1}^{u} \mathrm{ord}_l(a_{ii}) \le n$. Using induction on u and our assumptions, we see that $\mathrm{ord}_l[A(a)] = \xi$.

In particular, if $n > 2m$ and $a = a^{\nu\ \mathrm{tr}}$, then $\xi \le n$, by virtue of (35), and hence, $\mathrm{ord}_l[B^\nu] = \xi = z^\nu$. Thus, since $\mathrm{ord}_l([X^0][X^1]) = z^0 + z^1 = 2m_0 - 2m$, and β_3^0 and β_3^1 are injections, it follows that β_3^0 and β_3^1 are isomorphisms.

Note that since $l^{m_0}X^\nu = 0$, then for $n = m_0$ and $n' > 2m_0$, we have the isomorphisms α_k^ν, and for $n' > 3m_0$, the isomorphisms β_k^ν for $1 \le k \le 4$ (obtained by reduction modulo l^{m_0} of the corresponding homomorphisms for $n = m_0 + 1$).

Fix $\theta = 2$ or $\theta = 3$. Assume that the value of m is known, for example, $m = m^?$; that is, the l-component of BS for $\hat{E}$ over K is true. Assume as well that we can effectively calculate the values of $\psi_{p,n''}$ on $\tau_{\lambda',n''}$ for $\lambda' \in \Lambda$ and $(p, \lambda') = 1$, i.e., in view of (10), we can calculate the coordinates of $\tilde{P}_{\lambda'} \in \tilde{E}(F)$, where F is the residue field of K(p).

Then the above exposition gives us an algorithm for calculating m_0 for some $r \ge 1$, $n' \ge \theta m_0 + 1$, and $\pi = (p_0, \ldots, p_r) \in \Pi_{n'}^r$, such that $m(\lambda) = m(\lambda/p_1) = m$, where $\lambda = \pi(r)$, and for calculating the coefficients $a_{ij}^\nu \in \mathbb{Z}/M_0$, where $M_0 = l^{m_0}$. Then for $n = m_0$, we will obtain the isomorphism (33), in particular, the isomorphism $A^\nu \xrightarrow{\sim} X^\nu$ and the parameterization of the dual group of X^ν by the characters ψ_{p,m_0}^ν for $p|(\lambda^\nu/p)$. If $\theta = 3$, then we also obtain the isomorphisms in (38), in particular, the parameterization of X^ν by means of $\{z_i^\nu\}$. We can, of course, use the explicit matrix $a^\nu = \{a_{ij}\}$ to calculate the invariants of X^ν.

Now we shall demonstrate the algorithm. Sort out (in any order) a triple $n' > m$, $r \ge 1$, π such that $\lambda \in \Lambda_{n'}^r$, until one is obtained which satisfies the following conditions.

First, we verify the condition

$$\psi_{p_r,m+1}(\tau_{\lambda/p,m+1}) = 0. \tag{39}$$

It follows from (39) that $m(\lambda/p) = m$ and, in view of Proposition 5,

that $m(\lambda) = m$. If $r = 1$, then (39) implies that $m_0 = m$, hence $X = 0$, since $[X] = l^{2m-2m_0}$, and we complete the calculations. If $r > 1$, then we verify the conditions

$$\frac{n' - 1}{\theta} \geq m_0' \stackrel{df}{=\!=} \min_{1 \leq j \leq u(1)+1} \operatorname{ord}_l(\psi_{p_j, n'}(\tau_{1,n'})) \tag{40}$$

and

$$\psi_{p_2, m_0'+1}(\tau_{1, m_0+1}) \neq 0. \tag{41}$$

It follows from (40) that $m_0 = m_0'$. If $r > 2$, then we verify the condition

$$\psi_{p_1, m_0+1}(\tau_{1, m_0+1}) \neq 0. \tag{42}$$

Furthermore, for $1 \leq i \leq u(\nu)$, we can calculate the values $m(\lambda_i^\nu)$ according to the formula

$$m(\lambda_i^\nu) = \min_{j=\nu(i)-\nu, i<j\leq u(\nu)} \operatorname{ord}_l \psi_{p_{j+\nu}, m_0+1}\left(\tau_{\lambda_i^\nu, m_0+1}\right). \tag{43}$$

Recall that $(r, \nu) = r$ if $r - \nu$ is odd and $(r, \nu) = r - 1$, otherwise. Then for $\nu = 0$, and for $\nu = 1$ and $1 \leq i \leq (r, \nu) - \nu - 1$ (if such i exist), we verify the condition

$$\psi_{p_{i+\nu+1}, m(\lambda_i^\nu)+1}\left(\tau_{\lambda_i^\nu, m(\lambda_i^\nu)+1}\right) \neq 0. \tag{44}$$

The conditions (39), (41), and (40) if $r = 2$, or (42) and (44) if $r > 2$, are equivalent to the conditions (26) and (27); thus, we require a triple n', r, π for which (39) and (40) hold and, if $r \geq 2$, (42) and (44) hold as well (for the case $r = 1$, see above).

The coefficients of a^ν for $r - \nu \geq 2$ are calculated using (30) and (31).

If $r = 2$ or 3, then $m_2 = m(p_1, p_2) = m$, hence, $m_r = m$ for $r \geq 2$. Furthermore, $u(0) = 2$ and the matrix a^0 is a square diagonal matrix such that $\operatorname{ord}_l(a_{11}^0) = m_0 - m(p_1)$. In view of Theorem C (see the introduction) and (33), we obtain that $m_1 = m(p_1)$ and $\operatorname{ord}_l(a_{22}^0) = m_0 - m(p_1)$. Then (38), as well as (33), holds already (if $n = m_0$) for $\theta = 2$. In particular, $X^0 \simeq S_{M_0}^0 \simeq (\mathbb{Z}/l^{m_0-m_1})^2$; moreover, τ_{p_1, m_0} and τ_{p_2, m_0} form a basis for $S_{M_0}^0$, and φ_{p_1, m_0}^0 and φ_{p_2, m_0}^0 form a basis for $\operatorname{Hom}(S_{M_0}^0, \mathbb{Z}/M_0)$. If $r = 2$, then $m_1 =$

$m(p_1) = m$; if $r = 3$, then $p_1 = \lambda_1^0$ and, according to (43), $m_1 = \operatorname{ord}_{l^{\psi}p_2,m_0+1}(\tau_{p_1,m_0+1})$.

If $r = 2$, then $\#X^1 = m_1 - m_2 = m - m = 0$, so $X^1 = 0$. Suppose that $r = 3$. Then $Y = \ker \varphi_{p_1,m_0} \simeq X^1 \simeq (\mathbb{Z}/l^{m(p_1)-m})^2$, and $\varphi^1_{p_2,m_0}$ and $\varphi^1_{p_3,m_0}$, restricted to Y, form a basis of $\operatorname{Hom}(Y, \mathbb{Z}/M_0)$.

For $r > 3$, the group $\Lambda^{\nu} \simeq X^{\nu}$ splits into the direct sum of two isomorphic subgroups (according to Theorem C). Such a decomposition is obtained as a result of the orthogonality between τ_{λ',m_0} and τ_{λ'',m_0} for $\lambda' | \lambda$ and $\lambda'' | \lambda$. This permits more rapid calculation of the invariants of X^{ν}.

Recall (cf. Theorem E of the Introduction) that the l-component of BS is the equality $m = m^?$. If it is known that $m \geq m^?$, which is automatically true when $m^? = 0$, then we can use the algorithm, as above, with $m^?$ in place of m. A calculation using this process ends if and only if $m = m^?$, hence it allows us to obtain the information above simultaneously with the proof of the equality $m = m^?$.

Let C be a curve of genus 1 over K having a point over K(v) for all places v of K. Suppose that C is a principal homogeneous space over E, $(z) \in H^1(K, E)$ is the cohomology class corresponding to C, M is the period of (z), every rational prime dividing M belongs to B(E), $z \in S_M$ is the element of the Selmer group which lies over (z), and that for all $l|M$ and $p \in \Lambda^1$ we can calculate the value $z(p) \in E(K(p))/M$. Adding to z, if necessary, the element $T\left(\sum_{l|M} l^{-m_0}\right)P_1 \pmod{ME(K)}$, with the corresponding $T \subset \mathbb{N}$, we may assume that for all $l|M$ we have $z(p_1)^1 \equiv 0 \pmod{l^{m_0-m}}$. Then we have the following effective criterion (necessary and sufficient condition) for the curve C to have a point over K (with m, m_0, and λ, of course, corresponding to l):

$$\forall\, l|M,\ \forall p|\lambda \quad z(p) \equiv 0 \pmod{l^{m_0-m} E(K(p))}. \tag{45}$$

If the curve C is defined over $\mathbb{Q}$ and has a point over $\mathbb{Q}(v)$ forall places of $\mathbb{Q}$, then the effective criterion for C to have a point over $\mathbb{Q}$ is the criterion (45) with $z(p)^{\nu}$ in place of z(p), where $(1)^{\nu-1}\varepsilon = 1$.

References

1. Kolyvagin, V. A., "On the Mordell-Weil group and the Shafarevich-Tate group of Weil elliptic curves," Izv. Akad. Nauk SSSR, Ser. Mat., 52, No. 6, 1154-1180 (1988).
2. Rubin, K., "The Tate-Shafarevich group and L-functions of elliptic curves with complex multiplication," Invent. Math., 89, 527-560 (1987).
3. Kolyvagin, V. A., "Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves," Izv. Akad. Nauk SSSR, Ser. Mat, 52, No. 3, 522-540 (1988)
4. Kolyvagin, V. A., "Euler systems." To appear in the Grothendieck Festschrift, Birkhäuser.
5. Gross, B. H., Zagier, D., "Heegner points and derivatives of L-series," Invent. Math., 84, 225-320 (1986).
6. Gross, B. H., "Kolyvagin's work on modular elliptic curves." To appear in Procedings of the Durham Symmposium on L-functions and Arithmetic (1989).
7. Tate, J., "The arithmetic of elliptic curves," Invent. Math., 23, 179-206 (1974).
8. Shimura, G., Introduction to the Arithmetic Theory of Automorphic Functions, Princeton University Press, Princeton, New Jersey (1971).
9. Serre, J. -P., Cohomologie Galoisienne, Springer-Verlag, Berlin-New York (1973).
10. 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 (USSR), No. 5 (1989).