Bill Stein

Изв. Акад. Наук СССР
Сер. Матем. Том 52(1988), № 3

Math. USSR Izvestiya
Vol. 32(1989), No. 3

FINITENESS OF $E(\mathbf{Q})$ AND Ш$(E, \mathbf{Q})$ FOR A SUBCLASS OF WEIL CURVES

UDC 519.4

V. A. KOLYVAGIN

ABSTRACT. Let E be an elliptic curve over $\mathbf{Q}$, admitting a Weil parametrization $\gamma: X_N \to E$, $L(E, \mathbf{Q}, 1) \neq 0$. Let K be an imaginary quadratic extension of $\mathbf{Q}$ with discriminant $\Delta \equiv$ square (mod $4N$), and let $y_K \in E(K)$ be a Heegner point. We show that if y_K has infinite order (K must not belong to a finite set of fields that can be described in terms of γ), then the Mordell-Weil group $E(\mathbf{Q})$ and the Tate-Shafarevich group Ш$(E, \mathbf{Q})$ of the curve E (over $\mathbf{Q}$) are finite. For example, Ш$(X_{17}, \mathbf{Q})$ is finite. In particular, $E(\mathbf{Q})$ and Ш$(E, \mathbf{Q})$ are finite if $(\Delta, 2N) = 1$ and $L'_f(E, K, 1) \neq 0$, where $f = \infty$ or f is a rational prime such that $(\frac{f}{K}) = 1$ and $(f, Na_f) = 1$, where a_f is the coefficient of f^{-s} in the L-series of E over $\mathbf{Q}$. We indicate in terms of E, K, and y_K a number annihilating $E(\mathbf{Q})$ and Ш$(E, \mathbf{Q})$.

Bibliography: 11 titles.

Introduction

Let E be an elliptic curve defined over the field of rational numbers $\mathbf{Q}$, and let $L(E, \mathbf{Q}, s) = \sum_{n=1}^{\infty} a_n n^{-s}$, $a_n \in \mathbf{Z}$, be the canonical L-function of E over $\mathbf{Q}$. The Birch–Swinnerton-Dyer conjecture asserts that the rank of E over $\mathbf{Q}$ is equal to the order of the zero at $s = 1$ of the function $L(E, \mathbf{Q}, s)$. In particular, $E(\mathbf{Q})$ is finite $\Leftrightarrow L(E, \mathbf{Q}, 1) \neq 0$. If E has complex multiplication, Coates and Wiles [1] showed that $E(\mathbf{Q})$ is finite if $L(E, \mathbf{Q}, 1) \neq 0$. If E is a Weil curve (by Weil's conjecture, every elliptic curve defined over $\mathbf{Q}$ is such a curve) and $E(\mathbf{Q})$ is finite, then according to a result of Gross and Zagier [2] either $L(E, \mathbf{Q}, 1) \neq 0$ or $L'(E, \mathbf{Q}, 1) = 0$.

There also exists a conjecture on the finiteness of the Tate-Shafarevich group of E: Ш$(E, \mathbf{Q}) = \ker(H^1(\mathbf{Q}, E) \to \prod_v H^1(\mathbf{Q}_v, E))$, where v runs over all rational prime numbers and ∞.

Let N be a natural number, and X_N a modular curve over $\mathbf{Q}$ parametrizing isogenies of elliptic curves $E' \to E''$ with a cyclic kernel of order N. We assume that E is a Weil curve, i.e., for some N there exists a (weak) Weil parametrization $\gamma: X_N \to E$ (see [2] or [3]). Let K be an imaginary quadratic extension of $\mathbf{Q}$ with discriminant Δ ($\Delta < 0$) such that $\Delta \equiv$ square (mod $4N$); $O = O_K$ denotes the ring of integers of K, and i is an ideal of O such that $O/i \simeq \mathbf{Z}/N$; i exists as a consequence of a condition on Δ (see [2]) and is assumed to be fixed. Let H denote the Hilbert class field of K; $z_1 = z_{1,K,i} \in X_N(H)$ is a point corresponding in complex notation to the

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G40, 11G05, 11F67; Secondary 14K07, 11D25, 14G10, 11R23.

©1989 American Mathematical Society
0025-5726/89 $1.00 + $.25 per page

isogeny $C/O \to C/i^{-1}$, where $i^{-1} \supset O$ is invertible in the group of proper O-ideals. By $y_1 \in E(H)$ we denote a Heegner point $\gamma(z_1)$, and we set $y_K = N_{H/K}(y_1)$.

In this paper we shall prove that if $L(E, Q, 1) \neq 0$ and y_K has infinite order, then $E(Q)$ and Ш(E, Q) are finite. A priori, (K, i) in this criterion should not belong to a finite set Z of pairs (K', i') described in terms of the Weil parametrization of E. For example, Ш(X_{17}, Q) is finite. In terms of K, E, and y_K we indicate the number annihilating $E(Q)$ and Ш(E, Q). Actually, the picture that arises is reminiscent of the Stickelberger relations in cyclotomic theory.

Let $(\Delta, 2N) = 1$. We denote by χ_K the quadratic character associated with K, and we set

$$L(E, Q, \chi_K, s) = \sum_{n=1}^{\infty} \chi_K(n) a_n n^{-s}, \qquad L(E, K, s) = L(E, Q, s) L(E, Q, \chi_K, s).$$

Then $L(E, K, 1) = 0$. It follows from [2] that y_K is a point of infinite order $\Leftrightarrow$ $L'(E, K, 1) \neq 0$. Hence, for a Weil curve E with $L(E, Q, 1) \neq 0$, $E(Q)$ and Ш(E, Q) are finite if $\exists (K, i) \notin Z$ such that $(\Delta, 2N) = 1$ and $L'(E, Q, \chi_K, 1) \neq 0$. Let f be a rational prime splitting in K and such that $(f, N) = 1$ and $(f, a_f) = 1$; [4] allows us to replace the Archimedean L-function in the last criterion by an f-adic one.

We introduce some common notation: $N = \{1, 2, 3, \dots\}$ is the set of natural numbers, and Z_+ is the set of nonnegative numbers. If A is an abelian group and $D \in Z_+$, then A_D and A/D denote the kernel and cokernel of the endomorphism of multiplication by D. If M is a field, then $\overline{M}$ is an algebraic closure of M. If L/M is a Galois extension, then $G(L/M)$ denotes the Galois group of L over M. We shall use the abbreviations $H^1(M, A) = H^1(G(\overline{M}/M), A)$, where A is a $G(\overline{M}/M)$-module, and $H^1(M, E) = H^1(M, E(\overline{M}))$. "For almost all" means "for all, except a finite number". If O is a commutative ring with identity, then O^* denotes the group of invertible elements of O. The field $\overline{Q}$ is assumed to be imbedded in the field of complex numbers C, σ denotes the automorphism of complex conjugation, and ■ denotes the end of a proof.

§1. Norm relations for Heegner points

Throughout this paper p denotes a rational prime number relatively prime to N. We set $O_p = Z + pO$ and $i_p = i \cap O_p$; K_p denotes the ray class field of K with conductor p; $z_p \in X_N(K_p)$ is a point corresponding in complex notation to the isogeny $C/O_p \to C/i_p^{-1}$, where $i_p^{-1} \supset O_p$ is invertible in the group of proper O_p-ideals; $y_p \in E(K_p)$ denotes $\gamma(z_p)$; Cl_K denotes the ideal class group of K; and $\theta: Cl_K \xrightarrow{\sim} G(H/K)$ is the Artin isomorphism. We set u_p equal to the order of the image of O^* in $(O/p)^*/(Z/p)^*$; $u_p = 1$ if $K \neq Q(\sqrt{-1})$ and $K \neq Q(\sqrt{-3})$. If δ is an ideal of O, then $\theta(\delta)$ denotes the value of θ on the image of δ in Cl_K.

PROPOSITION 1. *The following norm relations hold:*

$$u_p N_{K_p/H}(y_p) = a_p y_1, \qquad (a_p - \theta^{-1}(\delta) - \theta^{-1}(\overline{\delta})) y_1, \qquad (a_p - \theta^{-1}(\delta)) y_1,$$

if respectively $(p/K) = -1$, i.e., p remains prime in K; $(p/K) = 1$, i.e., p splits in $K: (p) = \delta\overline{\delta}$; or $(p/K) = 0$, i.e., p is ramified in $K: (p) = \delta^2$.

PROOF. Let

$$\Gamma = \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(Z) \mid c \equiv 0 \ (\mathrm{mod}\ N) \right\},$$

$$T = \{\tau \in C,\ \mathrm{Im}(\tau) > 0\}, \qquad \tau \mapsto (C/[\tau, 1] \to C/[\tau, 1/N]),$$

where $[\tau_1, \tau_2] = Z\tau_1 + Z\tau_2$ is the standard mapping of $\Gamma\backslash T$ into $X_N(C)$. Let ω be a nonzero invariant differential form on E, and let $q = \exp(2\pi\sqrt{-1}\tau)$. By the definition of γ, $f(\tau) = \sum_{n=1}^{\infty} a_n q^n$ is a cusp form of weight 2 relative to Γ that is an eigenform for the Hecke operator T_p, $\gamma^*(\omega) = c f(\tau)(dq/q)$, $c \neq 0$. In complex notation the parametrization γ' can be represented as a mapping $\tau \mapsto \int_{\sqrt{-1}\infty}^{\tau} \gamma^*(\omega)$ (mod(the lattice of periods of $\gamma^*(\omega)$)). Using the fact that $f(\tau)$ is an eigenform for T_p:

$$p f(p\tau) + \sum_{k=0}^{p-1} \frac{1}{p} f\left(\frac{\tau + k}{p}\right) = a_p f(\tau),$$

we obtain the relation

$$\gamma(p\tau) + \sum_{k=0}^{p-1} \gamma\left(\frac{\tau + k}{p}\right) = a_p \gamma(\tau). \tag{1}$$

Here $\gamma': X_N \to E'$ is a Weil parametrization (see [3]) and $\gamma = \eta \circ \gamma'$, where $\eta: E' \to E$ is an isogeny. Applying (1) to the τ corresponding to z_1, we will obtain the desired norm relations, since in this case the terms in the left-hand side with residue 2 or 1 in the cases $(p/K) = 1$ and $(p/K) = 0$ will form the orbit of y_p relative to $G(K_p/H)$ with multiplicity u_p.

Let $x = (E' \xrightarrow{\varphi} E'') \in X_N$. The expression (1) can be written in the following equivalent way: $\sum \gamma(x_s) = a_p \gamma(x)$, where the summation is over the subgroups $S \subset E'$ of order p, $x_s = (E'/S \to E''/(\varphi(S)))$. If $E' = C/T$, then S has the form $(\frac{1}{p}L)/T$, where $L \subset T$ is a sublattice of index p. In our case $x = z_1$ and we have

$$\sum \gamma\left(\left(C\Big/\left(\frac{1}{p}L\right) \to C\Big/\left(\frac{1}{p}L + i^{-1}\right)\right)\right) = a_p y_1, \tag{2}$$

where the sum is over the sublattices $L \subset O$ of index p. We shall show that $\frac{1}{p}L + i^{-1} = i_p^{-1}\left(\frac{1}{p}L\right)$. It suffices to show that $i_p L + p i_p i^{-1} = L$, i.e., $i_p L + pO = L$ ($i_p i^{-1} = i_p(Oi^{-1}) = (i_p O) i^{-1} = i i^{-1} = O$). This is so if the index of $i_p L$ in L is relatively prime to p. Since $(N, p) = 1$, then $\exists A, B \in Z$ such that $pA + NB = 1$. We shall show that $L/(i_p L) \to O/i \simeq Z/N$ is an imbedding, i.e. $L \cap i = i_p L$. Let $a \in L \cap i$. Then $a = Apa + BNa$. Since $N \in i_p$ and $a \in L$, then $Na \in i_p L$. Hence it suffices to show that $pa \in i_p L$. For this in turn it suffices to show that $p^2 a \in i_p L$. But this is so because $pa \in i_p$ and $p \in L$. ■

Let $O = [\tau, 1]$. It is well known that every sublattice L of O of finite index admits a representation in the form $[a\tau + b, d]$, where $a, b, d \in Z$ and $a, d > 0$. The index of L in O is equal to ad. We shall prove some simple general facts about sublattices of O and their conductors. The *conductor of a lattice* L is the conductor of its ring of multipliers, i.e., the minimal $c \in N$ such that $\{x \in K \mid xL \subset L\} = Z + cO$.

PROPOSITION 2. *Let L be a sublattice of O of index n. Suppose $L = [a\tau + b, d]$. The conductor of L is the minimal $c \in N$ such that cd is divisible by a, cb is divisible by a, and $cN_{K/Q}(a\tau + b)$ is divisible by ad.*

PROOF. It suffices to prove that $c\tau L \subset L \Leftrightarrow c$ satisfies the given hypotheses; $c\tau d \in L \Leftrightarrow \exists e, s \in Z$ such that $cd\tau = e(a\tau + b) + sd \Leftrightarrow cd$ is divisible by a and $\exists s \in Z$ such that $(cd/a)b + sd = 0 \Leftrightarrow a$ divides cd and a divides cb. Further, let $r = N_{K/Q}(a\tau + b)$; then $c\tau(a\tau + b) \in L \Leftrightarrow \exists e, s \in Z$ such that $c\tau(a\tau + b) = e(a\tau + b) + sd \Leftrightarrow \exists e, s \in Z$ such that $(c\tau - e)r = sd(-a\tau + aR + b)$, where $R = \mathrm{Tr}_{K/Q}(\tau)$, $\Leftrightarrow ad$ divides cr and $\exists e \in Z$ such that $-er = cr(-R - b/a) \Leftrightarrow ad$ divides cr and a divides cb. ■

PROPOSITION 3. *Let $L = [a\tau + b, d]$, $ad = n$. Then the set of sublattices of index n equivalent to L ...*

Proposition 3. *Let $L = [a\tau + b, d]$, $ad = n$. Then the set of sublattices of O of index n equivalent to L consists of lattices of the form $(v/d)L$, where v is an arbitrary integer of K such that $N_{K/\mathbf{Q}}(v) = d^2$ and v is divisible by $d/((a\tau + b), d)$.*

Proof. Obviously, the desired set consists of lattices of the form $(v/d)L$, where $v \in K$ such that $(v/d)L \subset O$ and the index of $(v/d)L$ in O is equal to n. Obviously, $(v/d)L \subset O \Leftrightarrow v \in O$ and v is divisible by $d/((a\tau+b), d)$. We shall show that in this case the index of $(v/d)L$ in O is equal to $n \Leftrightarrow N_{K/\mathbf{Q}}(v) = d^2$. We have the inclusions $vL \subset dO \subset O$ and $vL \subset vO \subset O$. Hence

$$|O/(v/d)L| = |dO/vL| = |O/vL|/|O/dO| = |vO/vL|/|O/vO|/d^2 = nN_{K/\mathbf{Q}}(v)/d^2. \blacksquare$$

Proposition 4. *Let L be the same as in Proposition 3. Then L has conductor $n \Leftrightarrow (d, r) = 1$, where $r = N_{K/\mathbf{Q}}(a\tau + b)$. Multiplication by units belonging to $O^\cdot$ represents such lattices, and $L_1 \sim L_2 \Leftrightarrow L_1 = \varepsilon L_2$ for some $\varepsilon \in O^\cdot$. Further, if the conductor of L is equal to n, then $LO = O$.*

Proof. Let c be the conductor of L. From Proposition 2 it follows that $c \mid (a(d/(d,r))) \mid n$. Hence $(d, r) = 1$ if $c = n$. Conversely, if $(d, r) = 1$, then it follows from Proposition 2 that $n \mid c$. Since c always divides n, $c = n$. Further, if $(d, r) = 1$, then $(d, (a\tau + b)) = 1$. Therefore the second assertion of Proposition 4 follows from Proposition 3. We shall show that $LO = O$ if $(d, a\tau + b) = 1$. In fact, $LO \subseteq O$ is an O-ideal and contains the relatively prime numbers d and $a\tau + b$. Hence $LO = O$. $\blacksquare$

In particular, the sublattices $L \subset O$ of index p have the form $[p\tau, 1] = O_p$ and $[\tau + k, p]$, where $k = 0, 1, \dots, p-1$. It follows from Proposition 2 that the conductor of $[\tau + k, p]$ is equal to p $\forall k$ if $(\frac{p}{K}) = -1$, or is equal to p if $(\frac{p}{K}) = 1$ and $k \neq k_1, k_2$ such that $\tau + k_1 \equiv 0 \pmod{\delta}$ and $\tau + k_2 \equiv 0 \pmod{\overline{\delta}}$. In these last two cases, we obviously have that $[\tau + k, p] = \delta$ and $\overline{\delta}$ respectively. Analogously, for $(\frac{p}{K}) = 0$ the conductor of L is equal to p if $\tau + k \not\equiv 0 \pmod{\delta}$, and $[\tau + k, p] = \delta$ for the unique k for which $\tau + k \equiv 0 \pmod{\delta}$. It follows from Proposition 4 that the image of the set of lattices $L \subset O$ of index p and conductor p under mapping into the group $Cl_{K,p}$ of proper O_p-ideal classes consists of $(p - (\frac{p}{K}))/u_p$ elements and in each element of the image there are u_p lattices.

If E' is an elliptic curve, then $J(E')$ is the value of the modular invariant of E' (see [5], p. 107). For $E' = \mathbf{C}/L$ we set $J(L) = J(E')$. There is the classical fact that $J(O_p)$ generates K_p over K and $G(K_p/K)$ is isomorphic to $Cl_{K,p}$ relative to the correspondence $g \mapsto$ the class of b, under which $J(O_p)^g = J(b^{-1})$. There is a natural homomorphism of the idele group $K_A^\cdot$ of the field K into the group of proper O_p-ideals: $a \mapsto aO_p$ (for the definition of the action of an idele on a lattice see [5], p. 116), whose factorization through $Cl_{K,p}$ under the identification of $Cl_{K,p}$ with $G(K_p/K)$ given above coincides with the global reciprocity map $\theta\colon K_A^\cdot \to G(K_p/K)$ (see [5], pp. 122, 123). Moreover, there is a natural exact sequence $1 \to \Psi_p \to Cl_{K,p} \to Cl_K \to 1$, where Ψ_p denotes the factor-group of $(O/p)^\cdot/(\mathbf{Z}/p)^\cdot$ by the image of $O^\cdot$ corresponding to the exact sequence

$$1 \to G(K_p/H) \to G(K_p/K) \to G(H/K) \to 1.$$

Both to finish the proof of Proposition 1 and for later use we need the following

Proposition 5. *$G(K_p/H)$ is a cyclic group of order $(p - (\frac{p}{K}))/u_p$. The extension K_p/H is totally ramified at prime divisors of p in H.*

Proof. If $(\frac{p}{K}) = -1$, then $(O/p)^\cdot$ is a cyclic group of order $p^2 - 1$, $(\mathbf{Z}/p)^\cdot$ is a subgroup of order $p - 1$, and u_p is by definition the order of the image of $O^\cdot$ in $(O/p)^\cdot/(\mathbf{Z}/p)^\cdot$. Hence, $G(K_p/H) \simeq \Psi_p$ is a cyclic group of order $(p+1)/u_p$. If $(\frac{p}{K}) = 1$, then $(O/p)^\cdot \simeq (\mathbf{Z}/p)^\cdot \times (\mathbf{Z}/p)^\cdot$ is the subgroup of diagonal elements (a, a). Hence, $G(K_p/H)$ is a cyclic group of order $(p-1)/u_p$. Finally, in the case $(\frac{p}{K}) = 0$, $(O/p)^\cdot/(\mathbf{Z}/p)^\cdot \simeq (1 + \rho)^{\mathbf{Z}/p} \simeq \mathbf{Z}/p$, where $\rho \in O$, $\delta \mid \rho$, and $\delta^2 \nmid \rho$ ($(p) = \delta^2$). Again $G(K_p/H)$ is a cyclic group of order equal to p/u_p. Let $\mathscr{K}$ be a completion of K with respect to the prime divisor δ dividing p. The assertion about the ramification follows from the explicit form of the reciprocity map: the group of units of $\mathscr{K}$ is mapped epimorphically onto $G(K_p/H)$. $\blacksquare$

We finish the proof of Proposition 1. The field of functions on X_N over $\mathbf{Q}$ is generated by functions J_1 and J_2 such that $J_1((E' \to E'')) = J(E')$ and $J_2((E' \to E'')) = J(E'')$. A point $x \in X_N$ can be identified with $(J_1(x), J_2(x))$. When we take the above into account, formula (2) has the form $u_p \sum (\gamma(z_p))^g = (a_p - \varepsilon)y_1$, where $\varepsilon = 0$, $\theta^{-1}(\delta) + \theta^{-1}(\overline{\delta})$, $\theta^{-1}(\delta)$ respectively when $(\frac{p}{K}) = -1, 1, 0$, and g runs through the set of elements of $Cl_{K,p}$ that consists of the elements invertible to elements of the image in $Cl_{K,p}$ of the set of lattices $L \subset O$ of index and conductor p. As was shown above, there will be $(p - (\frac{p}{K}))/u_p$ such elements. Since $LO = O$ by Proposition 4, the class of L in $Cl_{K,p}$ is contained in Ψ_p. From Proposition 5 it then follows that g runs through exactly all the elements of $G(K_p/H)$. $\blacksquare$

§2. Canonical homogeneous spaces

A key for what follows is the fact that the norm relations of Proposition 1 allow us to construct a lot of homogeneous spaces over E whose orthogonality relative to a sum of local Tate symbols to elements of the Selmer groups for E (reciprocity law) leads eventually to the desired results.

Let D be a natural number. Let p be a rational prime number such that $(\frac{p}{K}) = -1$, $D \mid ((p+1)/u_p)$, and $D \mid a_p$. By L_p we denote the subextension of K_p of degree D over H. We set

$$R_p \in E(L_p), \qquad R_p = u_p N_{K_p/L_p}(y_p) - (a_p/D)y_1.$$

From Proposition 1 it follows that $N_{L_p/H}(R_p) = 0$. Let t be the generator of $G(L_p/H)$. We define the element $r_p \in H^1(G(L_p/H), E(L_p))$ as the class of the cocycle $t^j \mapsto (t^{j-1} + \dots + 1)R_p$. The corestriction gives us an element

$$c_p \in H^1(G(L_p/\mathbf{Q}), E(L_p))_D \subset H^1(\mathbf{Q}, E)_D.$$

If $(\frac{p}{K}) = 1$, $(p) = \delta\overline{\delta}$, δ is a principal ideal of O, $D \mid ((p-1)/u_p)$, and $D \mid (a_p - 2)$, then one analogously defines an element r_p corresponding to $R_p = u_p N_{K_p/L_p}(y_p) - ((a_p - 2)/D)y_1$, and an element $c_p \in H^1(\mathbf{Q}, E)_D$. In an analogous way we introduce homogeneous spaces for the other cases ($D = p$, $p \mid (a_p - 1)$, $(p) = \delta^2$, δ is principal, $u_p = 1$, $R_p = y_p - ((a_p - 1)/D)y_1$, etc.), but for our purposes even the homogeneous spaces for $(\frac{p}{K}) = -1$ suffice.

We denote the Tate pairing $E(\mathbf{Q}_q)/D \times H^1(\mathbf{Q}_q, E)_D \to \mathbf{Z}/D$ (see §3) by $\langle\ ,\ \rangle_{D,q}$; $S_D = S_D(\mathbf{Q})$ is the Dth Selmer group for E over $\mathbf{Q}$, i.e.,

$$S_D = \ker\left(H^1(\mathbf{Q}, E_D) \to \prod_v H^1(\mathbf{Q}_v, E)_D\right),$$

where $E_D = E(\overline{\mathbf{Q}})_D$ is the group of points of period D on E. In the product v runs over all rational prime numbers q and ∞; S_D is finite, and D is a periodic group (see

[6]). There are the standard exact sequences

$$0 \to E(\mathbf{Q})/D \to S_D \to Ш(E,\mathbf{Q})_D \to 0,$$
$$0 \to E(\mathbf{Q}_q)/D \to H^1(\mathbf{Q}_q, E_D) \to H^1(\mathbf{Q}_q, E)_D \to 0.$$

By definition, the localization of $s \in S_D$ in $H^1(\mathbf{Q}_q, E_D)$ lies in $E(\mathbf{Q}_q)/D$, so that the symbol $\langle s, c_p\rangle_{D,q}$ is defined, and $\sum_q \langle s, c_p\rangle_{D,q} = 0$ as a consequence of global class field theory. The summation is taken over all rational prime numbers (the Archimedean component $\langle s, c_p\rangle_{D,\infty} = 0$, since c_p is the corestriction from $H^1(K,E)$), for almost all q, $\langle s, c_p\rangle_{D,q} = 0$.

Let $y_2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$, $a_k' \in \mathbf{Z}$, be a Weierstrass equation for E, and let Δ_1 be the discriminant of this equation. Suppose

$$y \circ \gamma = P_1(J_1, J_2)/Q_1(J_1, J_2), \qquad x \circ \gamma = P_2(J_1, J_2)/Q_2(J_1, J_2),$$

where P_k and Q_k are integer polynomials and the coefficients of P_1 and Q_1 are all relatively prime to each other; analogously for P_2 and Q_2. We denote by Z the finite set of those (K, i) for which $Q_1(J_1, J_2)Q_2(J_1, J_2)$ is equal to zero on $z_{1,K,i}$.

The following congruence for y_p plays an important role in what follows. If w is a prime divisor of K_p lying over a prime divisor v of H, $v|p$, then we denote by F_v the residue field of the v-completion of H, and by $\mathrm{red}_w\colon E(K_p) \to E(F_v)$ the reduction homomorphism (see [6]). By Fr we denote the Frobenius automorphism of $\overline{\mathbf{Z}/p}$ over $\mathbf{Z}/p$. We have

PROPOSITION 6. *Assume that p is relatively prime to Δ_1, $Q_1(J_1(z_1), J_2(z_1))$, $Q_2(J_1(z_1), J_2(z_1))$, $(\frac{p}{K}) \neq 0$, and the prime divisor δ dividing p in K is principal. Then we have the congruence*

$$\mathrm{red}_w(y_p) = \mathrm{Fr}(\mathrm{red}_v(y_1)). \tag{3}$$

PROOF. We have the equality

$$J(p\tau) + \sum_{k=0}^{p-1} J\left(\frac{\tau+k}{p}\right) = a_1'' J^n(\tau) + \cdots + a_{n+1}'',$$

where $a_1'', \ldots, a_{n+1}'' \in \mathbf{Z}$ (see [5], p. 109). Further, there is the $q = \exp(2\pi\sqrt{-1}\tau)$-expansion (see [5], p. 108) for $J(\tau)$: $J(\tau) = q^{-1}\left(1 + \sum_{m=1}^{\infty} b_m q^m\right)$, $b_m \in \mathbf{Z}$. Comparing q-expansions, we will obtain that $n = p$, $a_1 = 1$, and $a_m \equiv 0 \pmod p$ for $m > 1$. Hence,

$$J(p\tau) + \sum_{k=0}^{p-1} J\left(\frac{\tau+k}{p}\right) \equiv J^p(\tau) \pmod{p\mathbf{Z}[J(\tau)]}.$$

In equivalent notation,

$$\sum_{L \subset T} J(L) \equiv J^p(T) \pmod{p\mathbf{Z}[J(T)]},$$

where the summation is over all sublattices of T of index p. We denote by λ the product of all prime divisors of K_p that divide p. As we know, $J(O)$ and $J(O_p)$ are algebraic integers (see [5], p. 108). Let $T = O$. If $(p/K) = -1$ then (see §1) $J(L)$ is conjugate to $J(O_p)$ relative to $G(K_p/H)$. Since by Proposition 5 K_p/H is totally

ramified at the prime divisors of H that divide p, then $\sum_{L \subset O} J(L) \equiv (p+1)J(O_p) \equiv J(O_p) \pmod\lambda$. Hence, $J(O_p) \equiv J(O)^p \pmod\lambda$. If $(\frac{p}{K}) = 1$, then, considering that by hypothesis the prime divisor $\delta|p$ in K is principal, we have

$$\sum_{L \subset O} J(L) \equiv (p-1)J(O_p) + 2J(O) \pmod\lambda.$$

Since p splits in H, then $J(O) \equiv J(O)^p \pmod\lambda$, and hence we also have $J(O_p) \equiv J(O)^p \pmod\lambda$. Further, $J(O_p)^g \equiv (J(O)^g)^p \pmod\lambda$, where $g \in G(K_p/K)$ corresponds to the class of the ideal i_p. Hence $J_1(z_p) = J(O_p) \equiv J_1(z_1)^p \pmod\lambda$ and $J_2(z_p) = J(i_p^{-1}) = J(O_p)^g \equiv J_2(z_1)^p \pmod\lambda$. Therefore

$$x(z_p) = \frac{P_2(J_1(z_p), J_2(z_p))}{Q_2(J_1(z_p), J_2(z_p))} \equiv \frac{P_2(J_1(z_1)^p, J_2(z_1)^p)}{Q_2(J_1(z_1)^p, J_2(z_1)^p)}$$
$$\equiv \left(\frac{P_2(J_1(z_1), J_2(z_1))}{Q_2(J_1(z_1), J_2(z_1))}\right)^p = x(z_1)^p \pmod\lambda.$$

Analogously,

$$y(z_p) \equiv y(z_1)^p \pmod\lambda$$

(by hypothesis $Q_1(J_1(z_1), J_2(z_1))$, $Q_2(J_1(z_1), J_2(z_1))$, and hence also $Q_1(J_1(z_p), J_2(z_p))$, $Q_2(J_1(z_p), J_2(z_p))$ are algebraic integers relatively prime to p). ■

§3. Computation of $\langle s, c_p\rangle_{D,p}$

In what follows we assume that $w_N(\gamma^*(w)) = -\gamma^*(w)$, where $w_N\colon X_N \to X_N$ is the principal involution: $w_N(\tau) = -\frac{1}{N\tau}$. This is equivalent to the fact that the function $L(E, \mathbf{Q}, s)$ has a zero of even order at $s = 1$. It is easy to see that then $\gamma(w_N(x)) = -\gamma(x) + \gamma(0)$, where $\gamma(0)$ is the image under γ of a cusp on X_N corresponding to $\tau = 0$. It is known that $\gamma(0) \in E(\mathbf{Q})$ is a point of finite order. As will be shown, it follows from this condition that $y_K^\sigma = -y_K + h\gamma(0)$, where h is the class number of K.

The congruence (3) is used in order to express $\langle s, c_p\rangle_{D,p}$ by means of invariants of s and y_K. If $W \in \mathbf{N}$, then by μ_W we denote the group of Wth roots of 1 in $\overline{\mathbf{Q}}$; $[\ ,\ ]_D\colon E_D \times E_D \to \mu_D$ is the Weil pairing (see [5], pp. 100–101). We fix an imbedding $\kappa\colon \overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_p$; κ determines the prime divisor δ of K dividing p. We assume that δ is a principal ideal. In what follows we assume that $(\frac{p}{K}) \neq 0$. Let $D \in \mathbf{N}$ be such that $D|((p+1)/u_p)$, $D|a_p$ if $(\frac{p}{K}) = -1$, and $D|((p-1)/u_p)$ and $D|(a_p - 2)$ if $(\frac{p}{K}) = 1$. Recall that t denotes the generator of $G(L_p/H)$. From t we define a generator $\zeta_{D,p} \in \mu_D$ in the following way. Let $\mathscr{K}$ denote the completion of K in $\overline{\mathbf{Q}}_p$; $\mathscr{K}$ coincides with the completion of H, since δ splits in H; $\theta\colon \mathscr{K}^* \to G(L_p/H)$ is the local reciprocity map; F denotes the residue field of $\mathscr{K}$; and ξ is a generator of $\mu_{(|F|-1)}$ such that $\theta(\xi) = t$. Then we set $\zeta_{D,p} = \xi^a$, where $a = (|F| - 1)/D$. For $s \in S_D$ we define an element $e_p(s) \in E_D$ as follows. Let $P \in E(\mathbf{Q}_p)$ be such that P represents s in $E(\mathbf{Q}_p)/D$. Let $\overline{Q} \in E(\overline{\mathbf{Z}/p})$ and $D\overline{Q} = \mathrm{red}(P)$. Then $e_p'(s) \in E_D$ is determined by the condition $\mathrm{red}(e_p'(s)) = \mathrm{Fr}(\overline{Q}) - \overline{Q}$. We set $e_p(s) = (\mathrm{Fr}+1)e_p'(s)$ if $(\frac{p}{K}) = -1$ and $e_p(s) = e_p'(s)$ if $(\frac{p}{K}) = 1$. Furthermore, we define an element $e_p(y_K) \in E_D$ as

$$\mathrm{red}(e_p(y_K)) = -((p+1+a_p)/D)\mathrm{red}(y_K) + ((p+1)/D)h(\mathrm{red}(\gamma(0)))$$

if $(\frac{p}{K}) = -1$, and as

$$\mathrm{red}(e_p(y_K)) = 2((p+1-a_p)/D)\mathrm{red}(y_K) - ((p+1 \ldots$$

where $E(\mathscr{K})/D$ …

product of all prime divisors of ... algebraic integers (see [5], p. 108). Let $T = O$. If $(p/K) = \ldots$ Since by Proposition 5 K_p/H is totally ... is conjugate to $J(O_p)$ relative to $G(K_p/H)$.

if $(\frac{p}{K}) = -1$, and as

$$\operatorname{red}(e_p(y_K)) = 2((p+1-a_p)/D)\operatorname{red}(y_K) - ((p+1-a_p)/D)h(\operatorname{red}(\gamma(0)))$$

if $(\frac{p}{K}) = 1$. The right-hand sides of the expressions for $\operatorname{red}(e_p(y_K))$ actually belong to $(E(F))_D$ since, for $(\frac{p}{K}) = -1$,

$$\begin{aligned} -((p+1+a_p)/D)\operatorname{red}(y_K) &+ ((p+1)/D)h(\operatorname{red}(\gamma(0))) \\ &= ((p+1)/D)\operatorname{red}(y_K^\sigma) - (a_p/D)\operatorname{red}(y_K) \\ &= ((p+1)/D)\operatorname{Fr}(\operatorname{red}(y_K)) - (a_p/D)\operatorname{red}(y_K), \end{aligned}$$

and $(p+1)\operatorname{Fr}(\operatorname{red}(y_K)) = a_p\operatorname{red}(y_K)$, which follows from Proposition 1, (2), and the fact that K_p/H is totally ramified at prime divisors of p. And if $(\frac{p}{K}) = 1$, then $\operatorname{red}(y_K), \operatorname{red}(\gamma(0)) \in E(\mathbf{Z}/p)$, and the order of $E(\mathbf{Z}/p)$ is equal to $p + 1 - a_p$ (see §4). We have

PROPOSITION 7. *Let p be the same as in Proposition 6, and suppose that $D|((p+1)/u_p)$, $D|A_p$ if $(\frac{p}{K}) = -1$, and $D|((p-1)/u_p)$, $D|(a_p - 2)$ if $(\frac{p}{K}) = 1$. Then*

$$\zeta_{D,p}^{(s,c_p)_{D,p}} = [e_p(s), e(y_K)]_D. \tag{4}$$

PROOF. Let $\mathscr{L}$ denote the completion of L_p in $\overline{\mathbf{Q}_p}$; $T = G(L_p/H)$ is identified with $G(\mathscr{L}/\mathscr{K})$. First we compute the value of the Tate symbol for arbitrary $s \in E(\mathscr{K})/D$ and $r \in H^1(T, E(\mathscr{L}))$, where here $\mathscr{K}$ is permitted to be an arbitrary finite extension of $\mathbf{Q}_p$ with residue field F and $\mathscr{L}$ is a cyclic totally ramified extension of $\mathscr{K}$ with Galois group $T = t^{\mathbf{Z}/D}$ of order D, where $(D, p) = 1$ and $D \mid (|F| - 1)$. Let $R \in E(\mathscr{L})$ be such that $N_{\mathscr{L}/\mathscr{K}}(R) = 0$. We denote by $r_R = r_{R,t}$ an element of $H^1(T, E(\mathscr{L}))$ corresponding to the cocycle $\varphi = \varphi_{R,t}: t^k \mapsto (t^{k-1} + \cdots + 1)R$ (every element of $H^1(T, E(\mathscr{L}))$ is obtained in this way). Let $\mathscr{M}$ be a finite extension of $\mathscr{K}$ with residue field F_1. Since $p \nmid \Delta_1$, E has good reduction at p and the reduction homomorphism $\operatorname{red}: E(\mathscr{M}) \to E(F_1)$ is defined. Here red is surjective, multiplication by D is an isomorphism onto its kernel $E_0(\mathscr{M})$, and $\operatorname{red}: E_D \to E(\overline{F})_D$ is an isomorphism. In particular, E_D is unramified as a $G(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-module. All these are standard properties of good reduction (see [6],§6). Since $\mathscr{L}$ is totally ramified over $\mathscr{K}$, the residue field of $\mathscr{L}$ coincides with F. Since $N_{\mathscr{L}/\mathscr{K}}(R) = 0$, we have $D\operatorname{red}(R) = 0$. We denote by e_R an element of $E(\mathscr{K})_D$ such that $\operatorname{red}(e_R) = \operatorname{red}(R)$. Let $P \in E(\mathscr{K})$ and let s be the class of P in $E(\mathscr{K})/D$. We denote by $\operatorname{Fr}_{\mathscr{K}}$ the Frobenius automorphism of $\overline{F}$ over F. We define $e(s) \in E_D$ by the condition $\operatorname{red}(e(s)) = \operatorname{Fr}_{\mathscr{K}}(\overline{Q}) - \overline{Q}$, where $\overline{Q} \in E(\overline{F})$, $D\overline{Q} = \operatorname{red}(P)$; $a = (|F| - 1)/D$, and $\zeta_D = \xi^a$, where ξ is a generator of $\mu_{(|F|-1)}$ such that $\theta(\xi) = t$, where $\theta: \mathscr{K}^* \to T$ is the reciprocity map.

PROPOSITION 8.

$$\zeta_D^{(s,r_R)_D} = [e(s), e_R]_D. \tag{5}$$

PROOF. The Weil pairing $[\ ,\ ]_D: E_D \times E_D \to \mu_D$ induces a nondegenerate pairing $H^1(\mathscr{K}, E_D) \times H^1(\mathscr{K}, E_D) \to H^2(\mathscr{K}, \mu_D) \xrightarrow{\sim} \mathbf{Z}/D$. The canonical isomorphism $\iota: H^2(\mathscr{K}, \mu_D) \xrightarrow{\sim} \mathbf{Z}/D$ is obtained as a composition of the isomorphism

$$H^2(\mathscr{K}, \mu_D) \xrightarrow{\sim} H^2(\mathscr{K}, \overline{\mathscr{K}}^*)_D \xrightarrow[\sim]{\text{inv}} \frac{1}{D}\mathbf{Z}/\mathbf{Z} \xrightarrow[\sim]{\times D} \mathbf{Z}/D,$$

where inv is the mapping defined in local class field theory (see [7], p. 131). Further, we have the exact sequence

$$0 \to E(\mathscr{K})/D \to H^1(\mathscr{K}, E_D) \to H^1(\mathscr{K}, E)_D \to 0,$$

where $E(\mathscr{K})/D$ is an isotropic subgroup of $H^1(\mathscr{K}, E_D)$ relative to the pairing

$$H^1(\mathscr{K}, E_D) \times H^1(\mathscr{K}, E_D) \to \mathbf{Z}/D$$

and the induced nondegenerate pairing $E(\mathscr{K})/D \times H^1(\mathscr{K}, E)_D \to \mathbf{Z}/D$ is the Tate symbol (see [8]).

We set

$$\begin{aligned} C &= ((D-1) + (D-2)t + \cdots + t^{D-2})R; \\ (t-1)C &= (D-1)t + (D-2)t^2 + \cdots + t^{D-1} - (D-1) - (D-2)t - \cdots - t^{D-2} \\ &= (1 + t + \cdots + t^{D-1} - D)R = -DR. \end{aligned}$$

If $g \in G(\overline{\mathscr{K}}/\mathscr{K})$, then by $\overline{g}$ we denote the image of g in $G(\mathscr{L}/\mathscr{K})$. Let $\check{C} \in E(\overline{\mathscr{K}})$ be such that $D\check{C} = C$. The mapping $\psi: g \mapsto \varphi(\overline{g}) + (g-1)\check{C}$ is a cocycle in E_D. In fact, it is obvious that ψ is a cocycle in $E(\overline{\mathscr{K}})$, and if $\overline{g} = t^k$, then

$$\begin{aligned} D\psi(g) &= D(t^{k-1} + \cdots + 1)R + (t^k - 1)C \\ &= D(t^{k-1} + \cdots + 1)R + (t^{k-1} + \cdots + 1)(t-1)C \\ &= (t^{k-1} + \cdots + 1)DR - (t^{k-1} + \cdots + 1)DR = 0. \end{aligned}$$

The class b of the cocycle ψ in $H^1(\mathscr{K}, E_D)$ is mapped onto r_R in $H^1(\mathscr{K}, E)_D$. Hence, we can use it in the computation of the Tate symbol. We have $R = e_R + R_0$, where $R_0 \in E_0(\mathscr{L})$, where $E_0(\mathscr{L})$ is the kernel of red. Since $E_0(\mathscr{L})$ is D-divisible, there is an $\check{R}_0 \in E_0(\mathscr{L})$ such that $D\check{R}_0 = R_0$ and

$$C = ((D-1) + (D-2)t + \cdots + t^{D-2})e_R + D((D-1) + (D-2)t + \cdots + t^{D-2})\check{R}_0.$$

We set

$$\check{C} = \check{e}_R + ((D-1) + (D-2)t + \cdots + t^{D-2})\check{R}_0,$$

where $D\check{e}_R = ((D-1) + (D-2)t + \cdots + t^{D-2})e_R$. Since we are interested in the value of the pairing of the cohomology class in $H^1(\mathscr{K}, E_D)$ corresponding to $s \in E(\mathscr{K})/D$ with the class b, then because $E(\mathscr{K})/D$ is isotropic, we can simply replace $\check{C}$ by $((D-1) + (D-2)t + \cdots + t^{D-2})\check{R}_0$. Thus,

$$\check{C} = ((D-1) + (D-2)t + \cdots + t^{D-2})\check{R}_0.$$

Suppose $\overline{g} = t^k$. Then

$$\begin{aligned} \psi(g) &= (t^{k-1} + \cdots + 1)R + (t^{k-1} + \cdots + 1)(t-1)((D-1) + \cdots + t^{D-2})\check{R}_0 \\ &= (t^{k-1} + \cdots + 1)R - (t^{k-1} + \cdots + 1)D\check{R}_0 = (t^{k-1} + \cdots + 1)e_R = ke_R. \end{aligned}$$

That is, the corresponding cohomology class $b \in H^1(\mathscr{K}, E_D)$ is simply the homomorphism $G(\overline{\mathscr{K}}/\mathscr{K}) \to E_D$ induced by the homomorphism of $G(\mathscr{L}/\mathscr{K})$ into E_D under which $t^k \mapsto ke_R$. Let η be the uniformizing parameter of $\mathscr{K}$ which is a norm from $\mathscr{L}$; we have $\mathscr{K}^*/\mathscr{K}^{*D} = \eta^{\mathbf{Z}/D}\xi^{\mathbf{Z}/D}$. We denote by G_D the Galois group of the maximal abelian D-periodic extension of $\mathscr{K}$; $\theta: \mathscr{K}^*/\mathscr{K}^{*D} \to G_D$ is an isomorphism, and we identify G_D with $\mathscr{K}^*/\mathscr{K}^{*D}$. The cocycle $\varphi_1: G_D \to E_D$ corresponding to $s \in E(\mathscr{K})/D$ is determined by the values $\varphi_1(\xi) = 0$ and $\varphi_1(\eta) = e(s)$, since $\mathscr{K}(Q)$ is an unramified extension of $\mathscr{K}$, where $DQ = P$ and s is the class of P in $E(\mathscr{K})/D$. The cocycle φ_2 corresponding to r_R is determined by the values $\varphi_2(\xi) = e_R$, $\varphi_2(\eta) = 0$. The cohomology class $\varphi_1 \smile \varphi_2 \in H^2(G_D, \mu_D)$ is defined by a bilinear mapping $B_1: G_D \times G_D \to \mu_D$ such that $B_1(\eta, \eta) = 1$, $B_1(\eta, \xi) = [e(s), e_R]_D$, $B_1(\xi, \eta) = 1$, and $B_1(\xi, \xi) = 1$. Since $\mu_D \subset \mathscr{K}^*$, the Hilbert symbol $(\ ,\ )_D: \mathscr{K}^*/\mathscr{K}^{*D} \times \mathscr{K}^*/\mathscr{K}^{*D} \to \mu_D$ is defined. If

$\beta \in \mathscr{K}^*$, then β is associated to a $\varphi_\beta \in H^1(G_D, \mu_D)$ such that $\varphi_\beta(g) = g(\tilde\beta)/\tilde\beta$, where $(\tilde\beta)^D = \beta$; $(\alpha,\beta)_D \overset{\text{def}}{=} \varphi_\beta(\theta(\alpha))$. An equivalent definition (see [9], §8.11) is the following. We define homomorphisms $\overline{\varphi}_\alpha: G_D \to \mathbf{Z}/D$ and $\overline{\varphi}_\beta: G_D \to \mathbf{Z}/D$ by the conditions $\zeta_D^{\overline{\varphi}_\alpha(g)} = \varphi_\alpha(g)$ and $\zeta_D^{\overline{\varphi}_\beta(g)} = \varphi_\beta(g)$. We define an element of $H^2(G_D, \mu_D)$ by the bilinear form $B_{\alpha,\beta}(g_1, g_2) = \zeta_D^{\overline{\varphi}_\alpha(g_1)\overline{\varphi}_\beta(g_2)}$. Then $(\alpha,\beta)_D = \zeta_D^{(D \operatorname{inv} B_{\alpha,\beta})}$. ($D\operatorname{inv} B_{\alpha,\beta}$ is defined as an element of $\mathbf{Z}/D$.) In particular, we have

$$\varphi_\xi(\xi) = (\xi,\xi)_D = 1, \qquad \varphi_\xi(\eta) = (\eta,\xi)_D = \zeta_D,$$
$$\varphi_{-\eta}(\xi) = (\xi,-\eta)_D = (-\eta,\xi)_D^{-1} = (\eta,\xi)_D^{-1} = \zeta_D^{-1}, \qquad \varphi_{-\eta}(\eta) = (\eta,-\eta)_D = 1.$$

Therefore $B_{\xi,-\eta}(\eta,\eta) = 1$, $B_{\xi,-\eta}(\eta,\xi) = \zeta_D^{-1}$, $B_{\xi,-\eta}(\xi,\eta) = 1$, and $B_{\xi,-\eta}(\xi,\xi) = 1$. Let $[e(s), e_R]_D = \zeta_D^x$, $x \in \mathbf{Z}/D$. Then $B_1 = B_{\xi,-\eta}^{-x}$. Hence, $D \operatorname{inv} B_1 = (-x) D \operatorname{inv} B_{\xi,-\eta}$. But $\zeta_D^{(D \operatorname{inv} B_{\xi,-\eta})} = (\xi,\eta)_D = \zeta_D^{-1}$. Hence $D \operatorname{inv} B_1 = x$, which proves Proposition 8. ■

If G is a finite group, B is a subgroup of G, and A is a G-module, then the mapping $\operatorname{cor}: H^1(B,A) \to H^1(G,A)$ is defined in the following way. Let $\overline{\varphi} \in H^1(B,A)$ be the class of a cocycle $\varphi: B \to A$. Let $\{\alpha_k\}$ be a system of representatives for G/B: $G = \bigcup \alpha_k B$. We define a mapping $\varphi': G \to A$ by setting $\varphi'(\alpha_k b) = \alpha_k \varphi(b)$. In addition, we define a mapping $\psi: G \to A$ such that $\psi(g) = \sum_j \varphi'(g\alpha_j)$. Then ψ is a cocycle of G in A, and $\overline{\psi} = \operatorname{cor}(\overline{\varphi})$.

Let $G = G(L_p/\mathbf{Q})$ and $B = T = t^{\mathbf{Z}/D}$. We recall that we have assumed that $\overline{\mathbf{Q}}$ is embedded in $\mathbf{C}$ and that σ denotes the automorphism of complex conjugation. We choose a system of representatives $\{\beta_j\}$ of $G(L_p/K)/T$ in $G(L_p/K)$. Then $\{\beta_j, \sigma\beta_j\}$ will be a system of representatives of G/T. We recall that the cohomology class $r_p \in H^1(T, E(L_p))$ is defined by the cocycle $\varphi: t^k \mapsto (t^{k-1} + \cdots + 1)R_p$, where $R_p = u_p N_{K_p/L_p}(y_p) - (a_p/D)y_1$ if $\left(\frac{p}{K}\right) = -1$ and $R_p = u_p N_{K_p/L_p}(y_p) - ((a_p-2)/D)y_1$ if $\left(\frac{p}{K}\right) = 1$; $c_p \in H^1(G, E(L_p))$, $c_p = \operatorname{cor}(r_p)$; and c_p is given by a cocycle $\psi: G \to E(L_p)$, constructed as above from φ and $\{\beta_j, \sigma\beta_j\}$. In particular,

$$\psi(t) = \sum_j \varphi'(t\beta_j) + \sum \varphi'(t\sigma\beta_j) = \left(\sum \beta_j\right)\varphi(t) + \sigma\left(\sum\beta_j\right)\varphi(t^{-1})$$
$$= \left(\sum \beta_j\right)\varphi(t) - \sigma\left(\sum\beta_j\right)t^{-1}\varphi(t) = \left(\sum \beta_j\right)\varphi(t) - t\sigma\left(\sum\beta_j\right)\varphi(t)$$

(σ acts by inversion on $G(L_p/K)$). Further,

$$\psi(\sigma) = \sum_j \varphi'(\sigma\beta_j) + \sum_j \varphi'(\beta_j) = 0 \qquad (\varphi(1) = 0).$$

First we consider the case $\left(\frac{p}{K}\right) = 1$. Taking (5) into account, in order to prove (4) it suffices to show that

$$\operatorname{red}\left(\left(\sum_j \beta_j\right) R_p - t\sigma\left(\sum_j \beta_j\right) R_p\right)$$
$$= 2((p+1-a_p)/D)\operatorname{red}(y_K) - ((p+1-a_p)/D)h(\operatorname{red}(\gamma(0))).$$

We first show that $y_K^\sigma = -y_K + h\gamma(0)$. Let a be a proper O_p-ideal, α the image of a in $Cl_{K,p}$. Let n be an ideal of O such that $O/n \simeq \mathbf{Z}/N$. We set $n_p = n \cap O_p$. Let (α, n_p) denote a point of X_N defined over K_p, corresponding to the isogeny $(\mathbf{C}/a \to \mathbf{C}/(n_p^{-1}a))$; $\lambda \in Cl_{K,p}$ acts on (α, n_p) in the following way: $(\alpha, n_p)^{\theta(\lambda)} = (\alpha\lambda^{-1}, n_p)$, and $(\alpha, n_p)^\sigma = (\alpha^\sigma, n_p^\sigma)$. The principal involution $w_N: X_N \to X_N$ maps (α, n_p) into $(\alpha[n_p], n_p^\sigma)$. Here $[n_p]$ is the image of n_p in $Cl_{K,p}$ (see [2]). Further, $\gamma \circ w_N = -\gamma + \gamma(0)$. We have

$$\gamma((\alpha,n_p))^\sigma = \gamma((\alpha,n_p)^\sigma) = \gamma((\alpha^\sigma, n_p^\sigma)) = \gamma((\alpha^\sigma[n_p^{-1}][n_p], n_p^\sigma))$$
$$= \gamma(w_N((\alpha^\sigma[n_p^{-1}], n_p))) = -\gamma((a^\sigma, n_p))^{\theta(n_p)} + \gamma(0).$$

In particular, $y_p^\sigma = -y_p^{\theta(i_p)} + \gamma(0)$. Analogously, $y_1^\sigma = -y_1^{\theta(i)} + \gamma(0)$. Passing to the norm from H to K in the last equality, we will obtain $y_K^\sigma = -y_K + h\gamma(0)$ (h is the class number of K); (3) is equivalent to the congruence $\operatorname{red}(g(y_p)) = \operatorname{Fr}(\operatorname{red}(g(y_1)))$ $\forall g \in G(K_p/\mathbf{Q})$. Hence

$$\operatorname{red}\left(\left(\sum\beta_j\right)R_p\right) = ((p-1)/D - (a_p-2)/D)\operatorname{red}(y_K)$$
$$= ((p+1-a_p)/D)\operatorname{red}(y_K),$$
$$\operatorname{red}\left(\sigma\left(\sum\beta_j\right)R_p\right) = ((p+1-a_p)/D)\operatorname{red}(y_K^\sigma)$$
$$= -((p+1-a_p)/D)(\operatorname{red}(y_K)((p+1-a_p)/D)h(\operatorname{red}(\gamma(0)))).$$

Therefore,

$$\operatorname{red}\left(\left(\left(\sum\beta_j\right) - t\sigma\left(\sum\beta_j\right)\right)R_p\right)$$
$$= 2((p+1-a_p)/D)\operatorname{red}(y_K) - ((p+1-a_p)/D)h(\operatorname{red}(\gamma(0))),$$

which proves (4) for the case $\left(\frac{p}{K}\right) = 1$. Now we consider the case $\left(\frac{p}{K}\right) = -1$. The decomposition group of p, i.e., $G(\mathscr{L}/\mathbf{Q}_p)$, where $\mathscr{L}$ is the completion of L_p in $\overline{\mathbf{Q}}_p$, is a subgroup of G, generated by T and σ. Let c_{1p} denote the image of r_p under $\operatorname{cor}: H^1(T, E(L_p)) \to H^1(G(L_p/K), E(L_p))$. As above, using the system $\{\beta_j\}$ we choose a cocycle $\psi_1: G(L_p/K) \to E(L_p)$ corresponding to c_{1p}. In particular, $\psi_1(t) = (\sum\beta_j)\varphi(t)$ and $\psi_1(t^{-1}) = (\sum\beta_j)\varphi(t^{-1})$. Let c_{2p} denote the restriction of c_{1p} to T. If we take $\{1,\sigma\}$ to be a system of representatives of $G(\mathscr{L}/\mathbf{Q}_p)/T$, then the corestriction of c_{2p} to $G(\mathscr{L}/\mathbf{Q}_p)$ is determined by a cocycle $\tilde\psi$ such that $\tilde\psi(t) = \psi_1'(t) + \psi_1'(t\sigma) = \psi_1(t) + \sigma\psi_1(t^{-1}) = \psi(t)$ and $\tilde\psi(\sigma) = \psi_1'(\sigma) + \psi_1'(1) = 0$. That is, $\tilde\psi = \psi$. Hence, the restriction c_{3p} of c_p to $G(\mathscr{L}/\mathbf{Q}_p)$ is the corestriction of c_{2p} from T to $G(\mathscr{L}/\mathbf{Q}_p)$. Further, we shall use the fact that

$$\langle s, \operatorname{cor}(x)\rangle_{D,\mathbf{Q}_p} = \langle s, x\rangle_{D,\mathscr{K}} \quad \forall x \in H^1(G(\mathscr{L}/\mathscr{K}), E(\mathscr{L})), \qquad s \in E(\mathbf{Q}_p)/D.$$

This general property of $\langle\ ,\ \rangle$ follows from the definition of $\langle\ ,\ \rangle$ (see above), the general properties of the $\smile$-product (see [7], p. 107), and the commutative diagram connecting the mapping inv in a tower of local fields (see [7], p. 139). In particular,

$$\langle s, c_p\rangle_{D,p} \overset{\text{def}}{=} \langle s, c_{3p}\rangle_{D,\mathbf{Q}_p} = \langle s, c_{2p}\rangle_{D,\mathscr{K}};$$

(4) will follow from (5) if we show that

$$\operatorname{red}\left(\left(\sum\beta_j\right)R_p\right) = -((p+1+a_p)/D)\operatorname{red}(y_K) + ((p-1)/D)h(\operatorname{red}(\gamma(0))).$$

In fact, from (3) it follows that

$$\operatorname{red}\left(\left(\sum\beta_j\right)R_p\right) = ((p+1)/D)\operatorname{Fr}(\operatorname{red}(y_K)) - (a_p/D)\operatorname{red}(y_K)$$
$$= ((p+1)/D)\operatorname{red}(y_K^\sigma) - (a_p/D)\operatorname{red}(y_K)$$
$$= -((p+1)/D)\operatorname{red}(y_K) + ((p+1)/D)h(\operatorname{red}(\gamma(0)))$$
$$- (a_p/D)\operatorname{red}(y_K)$$
$$= -((p+1+a_p)/D)\operatorname{red}(y_K) + ((p+1)/D)h(\operatorname{red}(\gamma(0))).$$

Proposition 7 is proved. ■

§4. The finiteness theorem

We introduce the notation needed for the statement of the theorem. Let K' denote the compositum of K and the field $k = \mathrm{End}(E) \otimes \mathbf{Q}$. For a rational prime number l we denote by G_{l^∞} the group $G(K'(E_{l^\infty})/K')$, where $E_{l^\infty} = \bigcup E_{l^n}$, and by G_{l^n} the group $G(K'(E_{l^n})/K')$. If $\mathrm{End}(E) = \mathscr{O}$ is an order in an imaginary quadratic extension k of $\mathbf{Q}$, then $\mathscr{O}$ has one class (since E is defined over $\mathbf{Q}$) and the choice of a projective system of generators $e_n \in E_{l^n}$ such that $E_{l^n} = (\mathscr{O}/l^n)e_n$, $le_{n+1} = e_n$, defines embeddings $\rho_n: G_{l^n} \hookrightarrow (\mathscr{O}/l^n)^*$ and $\rho: G_{l^\infty} \hookrightarrow \hat{\mathscr{O}}^*$, where $\hat{\mathscr{O}}$ is the l-completion of $\mathscr{O}$. If E does not have complex multiplication, i.e., $\mathrm{End}(E) = \mathbf{Z}$, then the choice of a projective system of generators $e_{1,n}, e_{2,n} \in E_{l^n}$ such that $E_{l^n} = (\mathbf{Z}/l^n)e_{1,n} + (\mathbf{Z}/l^n)e_{2,n}$, $le_{j,n+1} = e_{j,n}$ defines embeddings $\rho_n: G_{l^n} \hookrightarrow \mathrm{GL}_2(\mathbf{Z}/l^n)$ and $\rho: G_{l^\infty} \hookrightarrow \mathrm{GL}_2(\mathbf{Z}_l)$.

Suppose $\mathrm{End}(E) = \mathbf{Z}$. If $\rho(G_{l^\infty}) = \mathrm{GL}_2(\mathbf{Z}_l)$, then we set $m_{1l} = 0$. If $\rho(G_{l^\infty}) \neq \mathrm{GL}_2(\mathbf{Z}_l)$, then we define m_{1l} as the least $m \in \mathbf{N}$ such that $\rho(G_{l^\infty}) \supset I + l^m M_2(\mathbf{Z}_l)$ ($M_2(\mathbf{Z}_l)$ is the ring of 2×2 matrices over $\mathbf{Z}_l$, and I is the identity matrix). Suppose $\mathrm{End}(E) = \mathscr{O}$. We denote by $\Delta(\mathscr{O})$ the discriminant of $\mathscr{O}$. If $\rho(G_{l^\infty}) = \hat{\mathscr{O}}^*$, then we set $m_{1l} = 0$ if $l \neq 2$, and $m_{1l} = 0$ if $l = 2$ and either $2|\Delta(\mathscr{O})$ or 2 remains prime in k. If $2 \nmid \Delta(\mathscr{O})$ and 2 splits in k, we set $m_{12} = 1$. If $\rho(G_{l^\infty}) \neq \hat{\mathscr{O}}^*$, then we define m_{1l} as the least $m \in \mathbf{N}$ such that $\rho(G_{l^\infty}) \supset 1 + l^m \hat{\mathscr{O}}$. Further, we denote by m'_{2l} the least $m \in \mathbf{Z}_+$ such that l^m annihilates $H^1(G_{l^\infty}, E_{l^\infty})$. From classical results in case E has complex multiplication and from the results of Serre in the case $\mathrm{End}(E) = \mathbf{Z}$ (see [8], §5.1) it follows that m_{1l} and m'_{2l} exist for all l and are zero for almost all l. By $m''_{2l} \leq m'_{2l}$ we denote the least $m \in \mathbf{Z}_+$ such that l^m annihilates $H^2(G_{l^n}, E_{l^n}) \cap S_{l^n}(K')$ $\forall n$. Here $S_{l^n}(K')$ is the l^nth Selmer group of the field K' and the intersection is in $H^1(K', E_{l^n})$.

We set $m_{2l} = m''_{2l} + 1$ if $K = \mathbf{Q}(\sqrt{-1})$ and $l = 2$; or if $K = \mathbf{Q}(\sqrt{-3})$ and $l = 3$; we set $m_{2l} = m''_{2l}$ in the remaining cases. For an arbitrary rational q such that $q|N$ and $(q, \Delta) = 1$ (Δ is the discriminant of K), we denote by M_q the period of the finite group $H^1(\mathbf{Q}_q, E)_{\mathrm{nr}}$ (the subgroup of $H^1(\mathbf{Q}, E)$ of homogeneous spaces that split over the maximal unramified extension of $\mathbf{Q}_q$ (see [10], §2, Appendix 2, no. 1)). If $q|N$ and $q|\Delta$, then we denote by M_q the period of the finite group $H^1(\mathscr{K}', E)_{\mathrm{nr}}$, where $\mathscr{K}'$ is the completion of K with respect to a prime divisor $\delta|q$; M is the least common multiple of all the M_q.

We set $x_K = M(y_K - y_K^\sigma) = M(2y_K - h\gamma(0))$ if $l \neq 2$ or $l = 2$ and $Mh\gamma(0)$ is a point (in $E(\mathbf{Q})$) of even period, and $x_K = My_K$ if $l = 2$ and $Mh\gamma(0)$ is a point of odd period. We denote by $\varepsilon_l(n)$ the least $\varepsilon \in \mathbf{Z}_+$ such that $l^\varepsilon x_K \in l^n E(K)$. If y_K is a point of infinite order, then we denote by m'_{3l} the greatest $m \in \mathbf{Z}_+$ such that $x'_K \in l^m E(K)'$, where $E(K)'$ is the factor group of $E(K)$ by the subgroup of elements of finite order, so that $E(K)' \simeq \mathbf{Z}^{g_K}$, where g_K is the rank of E over K. Obviously, $n - \varepsilon_l \leq m'_{3l}$. If y_K is a point of infinite order, then we denote $\max_n(n - \varepsilon_l(n)) \leq m'_{3l}$ by m_{3l}; $m_{3l} = 0$ for almost all l. We set $\delta_l = 0$ if $l \neq 2$, and $\delta_2 = 1$. We set $\delta'_l = 0$ if $l \neq 2$, $\delta'_2 = 0$ if E has complex multiplication or the automorphism of complex conjugation σ acts nontrivially on E_2, and $\delta'_2 = 1$ otherwise.

We set $\delta''_l = 0$ if $l \neq 2$, $\delta''_2 = 0$ if $H^1(G(K/\mathbf{Q}), E(K) \cap E_{2^n}) \cap S_{2^n}$ are trivial for all n (intersection in $H^1(\mathbf{Q}, E_{2^n})$), and $\delta''_2 = 1$ otherwise. Let $\delta'''_l = \mathrm{ord}_l([k/\mathbf{Q}])$. We set $m_{4l} = 2\delta_l + 2\delta'_l + \delta''_l + 2\delta'''_l$. Finally, we set m_{5l} to be the exponent of the power of l in the expansion of the discriminant of the endomorphism ring of E. In particular, $m_{5l} = 0$ if E does not have complex multiplication. We set $m_l = 2m_{1l} + 2m_{2l} + m_{4l} + 2m_{5l}$; $m_l \in \mathbf{Z}_+$, and $m_l = 0$ for almost all l. If y_K is a point of infinite order, then we denote by $C = C(E, K)$ the natural number $\prod_l l^{m_{3l} + m_l}$; Z is the finite set of pairs (K, i) described in §2. We have

THEOREM 1. *Suppose $(K, i) \notin Z$. Then, for all n, $l^{n - \varepsilon_l(n) + m_l}$ annihilates S_{l^n} (the l^nth Selmer group of E over $\mathbf{Q}$). If y_K is a point of infinite order, then $l^{m_{3l} + m_l}$ annihilates S_{l^n} $\forall n$.*

The second assertion of the theorem follows from the first one, since if y_K is a point of infinite order, then by definition $n - \varepsilon_l(n) \leq m_{3l}$.

COROLLARY 1. *Suppose $(K, i) \notin Z$. If y_K is a point of infinite order, then $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ are finite groups, and the natural number $C(E, K)$ annihilates S_D $\forall D \in \mathbf{N}$, $E(\mathbf{Q})$, and $Ш(E, \mathbf{Q})$.*

PROOF OF COROLLARY 1. We have the exact sequence

$$0 \to E(\mathbf{Q})/D \to S_D \to Ш(E, \mathbf{Q})_D \to 0.$$

If y_K is a point of infinite order, then it follows from Theorem 1 that C annihilates S_D $\forall D$. In particular, C annihilates $E(\mathbf{Q})/D$. Hence, $E(\mathbf{Q})$ is finite, since by the Mordell-Weil theorem $E(\mathbf{Q}) \simeq A \times \mathbf{Z}^g$, where A is a finite group and $g \in \mathbf{Z}_+$ is the rank of E over $\mathbf{Q}$. Further, C annihilates $Ш_D$ for all D, and hence $Ш = Ш_C$. But $Ш_C$ is finite, since S_C is finite (as is well known, S_D is finite $\forall D$, which follows from the finiteness of the group of divisor classes of the field $\mathbf{Q}(E_D)$). ■

COROLLARY 2. *Suppose $(K, i) \notin Z$, and $(\Delta, 2N) = 1$. Then the groups $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ are finite if $L(E, \mathbf{Q}, 1)L'(E, \mathbf{Q}, \chi_K, 1) \neq 0$.*

PROOF OF COROLLARY 2. In [2] Gross and Zagier obtained the formula

$$b(K)L(E, \mathbf{Q}, 1)L'(E, \mathbf{Q}, \chi_K, 1) = \mathrm{height}(y_K), \qquad b(K) \neq 0,$$

where $\mathrm{height}(y_K)$ is the canonical height. Hence, if $L(E, \mathbf{Q}, 1)L'(E, \mathbf{Q}, \chi_K, 1) \neq 0$, then y_K is a point of infinite order. ■

Let f be a rational prime number, $(f, N) = 1$, $(f, a_f) = 1$, $\left(\frac{f}{K}\right) = 1$, and $(\Delta, 2N) = 1$. Suppose $\overline{\mathbf{Q}}$ is embedded in $\overline{\mathbf{Q}_f}$. According to [4], there is an f-adic analogue of the Gross-Zagier formula

$$b_f(K)L_f(E, \mathbf{Q}, 1)L'_f(E, \mathbf{Q}, \chi_K, 1) = \mathrm{height}_f(y_K)$$

with explicit $b_f(K) \neq 0$. If $L_f(E, \mathbf{Q}, 1)L'_f(E, \mathbf{Q}, \chi_K, 1) \neq 0$, we set

$$\nu_f(K) = \tfrac{1}{2}(\mathrm{ord}_f(b_f(K)) + \mathrm{ord}_f(L_f(E, \mathbf{Q}, 1)L'_f(E, \mathbf{Q}, \chi_K, 1))).$$

Since height_f is quadratic, we obviously have

COROLLARY 3. *Suppose $(K, i) \notin Z$, $(\Delta, 2N) = 1$, and f is a rational prime number such that $(f, N) = 1$, $(f, a_f) = 1$, and $\left(\frac{f}{K}\right) = 1$. If $L_f(E, \mathbf{Q}, 1)L'_f(E, \mathbf{Q}, \chi_K, 1) \neq 0$, then $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ are finite. Here $m_{3f} \leq \mathrm{ord}_f(M) + \nu_f(K)$ if $f \neq 2$ or $f = 2$ and $Mh\gamma(0) \in E(\mathbf{Q})_{\mathrm{tor}}$ is a point of odd period, and $m_{3f} \leq \mathrm{ord}_f(M) + \nu_f(K) + 1$ if $f = 2$ and $Mh\gamma(0)$ is a point of even period.* ■

COROLLARY 4. *The group $Ш(X_{17}, \mathbf{Q})$ is finite.*

PROOF OF COROLLARY 4. For a rational prime g, $g \equiv 3 \pmod 4$, $\left(\frac{-g}{17}\right) = 1$, it is known (Mazur [11], p. 237) that $y_{\mathbf{Q}(\sqrt{-g})}$ has a point of infinite order on the elliptic curve X_{17}. ■

We proceed to the proof of Theorem 1. First we outline it. We bound from below those p that remain prime in K. Let $D = l^n$, $D|((p+1)/u_p)$, and $D|a_p$. Replacing c_p by Mc_p reduces the equality $\sum_q \langle s, c_p\rangle_{D,q} = 0$ to $\langle s, Mc_p\rangle_{D,p} = 0$. We shall prove this. Assume first that $(q,\Delta) = 1$, i.e., that q does not ramify in K (in K only the divisors of Δ are ramified). If $q|N$, then $\langle s, Mc_p\rangle_{D,q} = 0$, since by definition M annihilates $H^1(\mathbf{Q}_q, E)_{\mathrm{nr}}$, and the q-localization of c_p belongs to $H^1(\mathbf{Q}_q, E)_{\mathrm{nr}}$, since q is not ramified in K_p (in K_p only divisors of Δ and p, $(p,N) = 1$, are ramified). Analogously, $\langle s, c_p\rangle_{D,q} = 0$ if $(q,N) = 1$, $q \neq p$, since $H^1(\mathbf{Q}_q, E)_{\mathrm{nr}} = 0$ in this case (see [10], §2, Appendix 2, no 1), since outside of N the curve E has good reduction. For $q|\Delta$, $q \neq p$, as before we have $\langle s, Mc_p\rangle_{D,q} = 0$, since $\langle s, Mc_p\rangle_{D,q} = \langle s, Mc'_p\rangle_{D,\delta}$, where c'_p is the corestriction of r_p in $H^1(G(L_p/K), E(L_p))$ and δ is a prime divisor of K dividing q (this is verified in the same way as above: see the end of §3). Further, $c'_p \in H^1(\mathcal{K}', E)_{\mathrm{nr}}$, where $\mathcal{K}'$ is the δ-completion of K, and M annihilates $H^1(\mathcal{K}', E)_{\mathrm{nr}}$. Thus $\langle s, Mc_p\rangle_{D,p} = 0$. Using the explicit formula (4), we shall prove

Proposition 9. *$\exists \alpha_p, \beta_p \in \mathbf{Z}_+$ such that $\alpha_p + \beta_p \le n + \rho_p$, where $\rho_p = 0$ if $l \neq 2$, $\rho_p = 1$ if $l = 2$ and $E(\mathbf{Z}/p)_2 \simeq \mathbf{Z}/2$, and $\rho_p = 2$ if $l = 2$ and $E(\mathbf{Z}/p)_2 \simeq \mathbf{Z}/2 + \mathbf{Z}/2$, such that $l^{\alpha_p} s = l^{\beta_p} x_K = 0$ in $E(\mathcal{K})/D$, where $s \in S_D$.*

Then, using the Chebotarev density theorem and information about the structure of $G(K'(E_{l^\infty})/K')$ (see above), from these estimates for the sums of the exponents of the local periods of s and x_K we derive an analogous estimate for the sum of the exponents of the periods of s and x_K in $S_{l^\infty}(K)$.

Proof of Proposition 9. We denote by Ta the Tate module of E corresponding to the number l, i.e., $\mathrm{Ta} = \varprojlim E_{l^n}$ (the reduction homomorphism identifies E_{l^n} with $E(\overline{\mathbf{Z}/p})_{l^n}$; we consider here points of E over $\overline{\mathbf{Z}/p}$); $\mathrm{Ta} \simeq \mathbf{Z}_l \oplus \mathbf{Z}_l$, and in a chosen basis the action of Fr (the Frobenius automorphism of $\overline{\mathbf{Z}/p}$ over $\mathbf{Z}/p$) is given by the matrix

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbf{Z}_l),$$

where $a_{11} + a_{22} = a_p$ and $a_{11}a_{22} - a_{21}a_{12} = p$. We denote by F a quadratic extension of $\mathbf{Z}/p$ which is the residue field of $\mathcal{K}$ ($\mathcal{K}$ is the p-completion of K). Let A denote $E(F)_{l^\infty}$, i.e., the l-component of $E(F)$. Since $a_{11} + a_{22} \equiv 0 \pmod D$ and $a_{11}a_{22} - a_{21}a_{12} \equiv -1 \pmod D$, we have $\mathrm{Fr}^2 \equiv I \pmod D$, where $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Hence, $E_D \subset A$. We denote by A_+ the kernel of $\mathrm{Fr} - 1$ on A, i.e., the l-component of $E(\mathbf{Z}/p)$, and by A_- the kernel of $\mathrm{Fr} + 1$ on A,

$$A_+ \simeq \mathrm{Ta}/(\mathrm{Fr} - 1)\mathrm{Ta}, \qquad A \simeq \mathrm{Ta}/(\mathrm{Fr}^2 - 1)\mathrm{Ta}.$$

Let $p + 1 + a_p = l^b r$, where $(r,l) = 1$, and $p + 1 - a_p = l^a v$, where $(v,l) = 1$. By the hypothesis $(D|((p+1)/u_p), D|a_p)$ $a, b \ge n$; $|A_+| = l^a$ and $|A| = l^{a+b}$. We have the exact sequence

$$0 \to A_+ \to A \to (\mathrm{Fr} - 1)A \to 0.$$

Since $\mathrm{Fr} \pm I$ are nondegenerate matrices, we have $A_- \simeq (\mathrm{Fr} - 1)A$ and $A_+ = (\mathrm{Fr} + 1)A$. Hence

$$|A_-| = |A|/|A_+| = l^b.$$

From the fact that $\langle s, Mc_p\rangle_{D,p} = 0$ and (4) it follows that $[e, e_-]_D = 1$, where $e = e(s) = (\mathrm{Fr} + 1)e'(s)$, $e'(s) \in E_D$, and $e_- = ((p + 1 + a_p)/D)\mathrm{red}(vx_K) \in E_{D-}$, since $\mathrm{Fr}(\mathrm{red}(vx_K)) = \mathrm{red}(vx_K^\tau) = -\mathrm{red}(vx_K)$. Let $\lambda \in \mathbf{Z}_+$ be such that $l^\lambda E_{D-} \subset [e_-]$, the

subgroup of E_{D-} generated by e_-. Then $l^\lambda e$ is orthogonal to E_{D-} relative to the Weil pairing $[\ ,\ ]_D$. In particular,

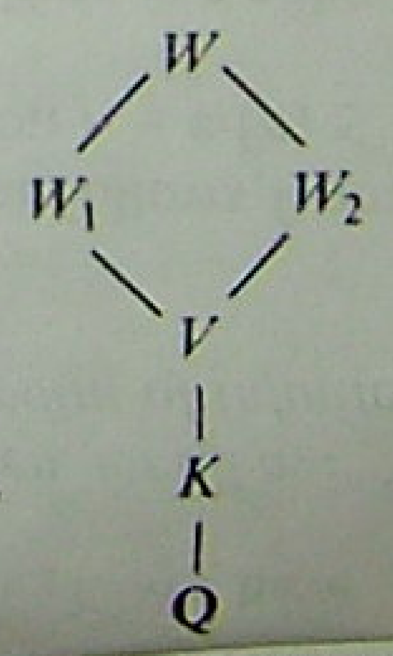
$$[l^\lambda e, (1 - \mathrm{Fr})\tilde{e}]_D = [(1 + \mathrm{Fr})l^\lambda e, \tilde{e}]_D = 1 \quad \forall \tilde{e} \in E_D.$$

Here we used the fact that $[\mathrm{Fr}(e), \mathrm{Fr}(\tilde{e})]_D = \mathrm{Fr}([e, \tilde{e}]_D)$ (see [5], p. 101), and $\mathrm{Fr}(\zeta) = \zeta^{-1}$ $\forall \zeta \in \mu_D$. Since the pairing $[\ ,\ ]_D$ is nondegenerate, we have $(1 + \mathrm{Fr})l^\lambda e = 0$, i.e., $l^\lambda e \in E_{D-}$. On the other hand, $l^\lambda e \in E_{D+}$. Thus, if $l^\lambda E_{D-} \subset [e_-]$, then $l^\lambda e \in E_{D+} \cap E_{D-}$.

We denote $r(\mathrm{red}(vx_K)) \in A_-$ by e_1. Suppose $l \neq 2$. Then A is the direct sum of A_+ and A_-, and hence $A_+ \simeq \mathbf{Z}/l^a$ and $A_- \simeq \mathbf{Z}/l^b$ (since A is a factor of $\mathbf{Z}_l + \mathbf{Z}_l$). Let $0 \le \beta \le n$ be the least integer such that $l^\beta e_1 \in l^n A_-$. We shall show that $l^{n-\beta} E_{D-} \subset [e_-]$ ($E_{D-} = E_D \cap A_-$; $E_{D+} = E_D \cap A_+$). If $\beta = 0$, the assertion is obvious. Suppose $\beta > 0$. Then $e_1 = l^{n-\beta} u \pmod{l^b}$, where $(u, l) = 1$, and $e_- = l^{b-n} e_1 = l^{b-\beta} u \pmod{l^b}$. The generator of E_{D-} is $l^{b-n} \pmod{l^b}$. Therefore $l^{n-\beta} E_{D-} \subset [e_-]$. Consequently, $l^{n-\beta} e \in E_{D+} \cap E_{D-}$. But $E_{D+} \cap E_{D-} = 0$. Hence $l^{n-\beta} e = 0$. Since the mapping red induces an isomorphism $E(\mathcal{K})/D \to A/D$, we have $l^\beta x_K = 0$ in $E(\mathcal{K})/D$. By definition $e = e(s)$ is $(\mathrm{Fr}^2 - 1)\overline{Q}$, where $D\overline{Q} = \mathrm{red}(P)$ and $P \in E(\mathbf{Q}_p)$ represents s in $E(\mathbf{Q}_p)/D$. The condition $l^{n-\beta} e = 0$ means that $l^{n-\beta} s = 0$ in $E(\mathcal{K})/D$, since the mapping (class of P) $\mapsto (\mathrm{Fr}^2 - 1)\overline{Q}$, where $D\overline{Q} = \mathrm{red}(P)$, gives an imbedding of $E(\mathcal{K})/D$ into E_D. Thus, Proposition 9 is proved for $l \neq 2$.

Now we consider the case $l = 2$. Obviously, $E_{D+} \cap E_{D-} = E_2 \cap A_+ = E_{2+}$. Therefore, if $0 \le \lambda \le n$ is such that $l^\lambda E_{D-} \subset [e_-]$, then $l^{\lambda+1} e = 0$. There are two possible cases: $E_{2+} \simeq \mathbf{Z}/2$ and $E_{2+} \simeq \mathbf{Z}/2 + \mathbf{Z}/2$. Suppose $E_{2+} \simeq \mathbf{Z}/2$. Then $A_- \simeq \mathbf{Z}/2^b$ and $A_+ \simeq \mathbf{Z}/2^a$. Let $0 \le \beta \le n$ be the minimal integer such that $2^\beta e_1 \in 2^n A_-$. Analogously, as above, we will obtain that $2^{n+1-\beta} s = 2^\beta x_K = 0$ in $E(\mathcal{K})/D$. Now we consider the case $E_{2+} = E_2 \simeq \mathbf{Z}/2 + \mathbf{Z}/2$. If $n = 1$, then we can take $\alpha + \beta = 1$ in Proposition 9. Suppose $n \ge 2$ and $b = n$. In this case $A_- = E_{D-} \simeq \mathbf{Z}/2^{n-1} + \mathbf{Z}/2$, since for any other structure of A_- we would have $E_{4-} = E_4$, which is impossible since $\mathrm{Fr} + I \not\equiv 0 \pmod 4$, which follows from the fact that $\det(\mathrm{Fr}) \equiv -1 \not\equiv 1 \pmod 4$. We note that $e_1 = e_-$ for $b = n$. Let $2^\beta e_1 = 0$, $0 \le \beta \le n - 1$. Then $2^{n-\beta} E_{D-} \subset [2e_1]$. Therefore we again have $2^{n+1-\beta} s = 2^\beta x_K = 0$ in $E(\mathcal{K})/D$. Suppose $b > n$. Then $A_- \simeq \mathbf{Z}/2^{b-1} + \mathbf{Z}/2$ and $E_{D-} \simeq \mathbf{Z}/2^n + \mathbf{Z}/2$. Let $0 \le \beta \le n$ be such that $2^\beta e_1 \in 2^n A_-$. If $\beta = 0$, then we can take $\alpha = n$ and $\beta = 0$ in Proposition 9. Suppose $\beta > 0$. Then the condition $2^\beta e_1 \in 2^n A_-$ is equivalent to the fact that $\overline{e}_1 = 2^{n-\beta} u \pmod{2^{b-1}}$, $(u, l) = 1$, where $\overline{e}_1$ is the projection of e_1 into $\mathbf{Z}/2^{b-1}$; $e_- = 2^{b-\beta} u \in \mathbf{Z}/2^{b-1}$; E_{D-} is generated by $2^{b-1-n} \in \mathbf{Z}/2^{b-1}$, and $1 \in \mathbf{Z}/2$. Hence, $2^{n+1-\beta} E_{D-} \in [e_-]$. Consequently, we can set $\alpha = n + 2 - \beta$ in Proposition 9. ■

We consider the tower of fields



where $V = K'(E_{D'})$, and D' is defined in the following way. $D' = 2D$ if $K = \mathbf{Q}(\sqrt{-1})$

From the fact that $\langle s, Mc_p\rangle_{D,p} = 0$ and (4) it follows that $[e, e_-]_D = 1$, where $e = e(s) = (\mathrm{Fr}+1)e'(s)$, $e'(s) \in E_D$, and $e_- = ((p+1+a_p)/D)\mathrm{red}(vx_K) \in E_{D-}$, since $\mathrm{Fr}(\mathrm{red}(vx_K)) = \mathrm{red}(vx_K^\sigma) = -\mathrm{red}(vx_K)$. Let $\lambda \in \mathbf{Z}_+$ be such that $l^\lambda E_{D-} \subset [e_-]$, the

K

Q

where $V = K'(E_{D'})$, and D' is defined in the following way: $D' = 2D$ if $K = \mathbf{Q}(\sqrt{-1})$ and $l = 2$, $D' = 3D$ if $K = \mathbf{Q}(\sqrt{-3})$ and $l = 3$, and $D' = D$ in the remaining cases; W_1 and W_2 are D-periodic abelian extensions of V, corresponding to $s_1, s_2 \in H^1(V, E_D) = \mathrm{Hom}(G(\overline{V}/V), E_D)$, where s_1 is the image (restriction) of s in $H^1(V, E_D)$ and s_2 corresponds to x_K; W is the compositum of W_1 and W_2. We have imbeddings $s_1: G(W_1/V) \hookrightarrow E_D$ and $s_2: G(W_2/V) \hookrightarrow E_D$. We denote $G(W/V)$ by H and $G(W_j/V)$ by H_j. The image of H_j in E_D relative to the imbeddings $s_j: \mathrm{H}_j \hookrightarrow E_D$ will be denoted by Λ_j. We recall that we assume $\overline{\mathbf{Q}}$ to be embedded into $\mathbf{C}$, and σ to be the automorphism of complex conjugation. Since s_1 and s_2 generate the eigenspaces relative to the action of $G(V/\mathbf{Q})$ in $H^1(V, E_D)$ ($s_1^g = s_1$; $s_2^g = s_2$ if $g = \mathrm{id}$ on K, and $s_2^\sigma = -s_2$), then $W_1/\mathbf{Q}$ and $W_2/\mathbf{Q}$ are Galois extensions; σ acts in a natural way on H, H_1, and H_2: $\eta^\sigma = \sigma\eta\sigma^{-1} = \sigma\eta\sigma$ ($\sigma^2 = 1$). We have

Proposition 10. *$\forall \eta \in \mathrm{H}\ \exists \alpha, \beta \in \mathbf{Z}_+$ such that $\alpha + \beta \le n$ if $l \ne 2$, $\alpha + \beta \le n+2$ if $l = 2$, and $(\eta_1^\sigma\eta_1)^\alpha = 1$, $(\eta_2^\sigma\eta_2)^\beta = 1$, where η_j is the restriction of η to W_j.*

Proof. By the Chebotarev density theorem there exist infinitely many rational primes p which are unramified in W and for some prime divisor v of the field W dividing p we have $g = \sigma\eta = \mathrm{Fr}_v$, i.e., g is continuous relative to the v-metric, and the automorphism of W_v over $\mathbf{Q}_p$ induced from it by continuity is the Frobenius automorphism. Throwing away a finite set of prime numbers, we may assume that p is relatively prime to $2\Delta_1$ and $Q_j(J_1(z_1), J_2(z_1))$, $j = 1, 2$ (see Proposition 6). Let $v|w$ and $w|p$, w a prime divisor of the field V. Since $g = \sigma$ on V, then V_w is a quadratic extension of $\mathbf{Q}_p$ and is also a completion of K. From this it follows that p remains prime in K, and $E(F) \supset E_D$, where F is the residue field of V_w (a quadratic extension of $\mathbf{Z}/p$). Hence $D^2|(p+1-a_p)(p+1+a_p)$. Let $D'' = Du_K$, where $u_K = |O_K^*/\mathbf{Z}^*|$. We have an inclusion $\mu_{D''} \subset V$. In fact, $\mu_{D'} \subset \mathbf{Q}(E_{D'})$, which follows from the nondegeneracy of the Weil pairing $[\ ,\ ]_D$ and the property $[e_1^f, e_2^f]_D = [e_1, e_2]^f$ $\forall f \in G(\overline{\mathbf{Q}}/\mathbf{Q})$, and $\mu_{2u_K} \subset K$. Since $\zeta^\sigma = \zeta^{-1}$, and, on the other hand, $\zeta^\sigma = \zeta^p$ ($\zeta \in \mu_{D''}$), it follows that $u_K D|(p+1)$. Granting that $u_p|u_K$, we will obtain that $D|((p+1)/u_p)$ and $D|a_p$.

Let $\mathscr{W}_1$ and $\mathscr{W}_2$ denote completions of W_1 and W_2; V_w coincides with $\mathscr{K}$, the completion of K, and $G(\mathscr{W}_1/\mathscr{K}) \subset \mathrm{H}_1$ is generated by g_1^2, where g_1 is the restriction of g to W_1. We note that $g_1^2 = \sigma\eta_1\sigma\eta_1 = \eta_1^\sigma\eta_1$. Analogously, $G(\mathscr{W}_2/\mathscr{K}) \subset \mathrm{H}_2$ is generated by $\eta_2^\sigma\eta_2$. But $\mathscr{W}_1 = \mathscr{K}(Q_1)$, where $DQ_1 = P \in E(\mathscr{K})$ and $s = P \pmod{DE(\mathscr{K})}$; also $\mathscr{W}_2 = \mathscr{K}(Q_2)$, where $DQ_2 = x_K$. Therefore $G(\mathscr{W}_1/\mathscr{K})$ is isomorphic to the subgroup generated by s in $E(\mathscr{K})/D$, and $G(\mathscr{W}_2/\mathscr{K})$ is isomorphic to the subgroup generated by x_K in $E(\mathscr{K})/D$. According to Proposition 9, $\exists \alpha, \beta$ such that $\alpha + \beta$ satisfies the hypothesis of Proposition 10, l^α annihilates $G(\mathscr{W}_1/\mathscr{K})$, and l^β annihilates $G(\mathscr{W}_2/\mathscr{K})$. This completes the proof of Proposition 10. ■

Lemma 1. *Let A, B, and C be groups, and let $\varphi_1: A \to B$ and $\varphi_2: A \to C$ be homomorphisms, where $\varphi_1(A)$ and $\varphi_2(A)$ are abelian groups. Assume that $\forall a \in A\ \exists \alpha, \beta \in \mathbf{Z}_+$ such that $\alpha + \beta \le n$ and $l^\alpha\varphi_1(a) = l^\beta\varphi_2(a) = 0$. Then $\exists \alpha, \beta \in \mathbf{Z}_+$ such that $\alpha + \beta \le n$ and, for all $a \in A$, $l^\alpha\varphi_1(a) = l^\beta\varphi_2(a) = 0$.*

Proof. We shall prove the lemma by induction on n. Suppose $n = 1$. Let $A_1 = \ker(\varphi_1)$ and $A_2 = \ker(\varphi_2)$. By hypothesis $A = A_1 \cup A_2$. We must show that $A_1 = A$ or $A_2 = A$. We assume that this is not so. Then A_1 and A_2 are proper subgroups of A. Since $A = A_1 \cup A_2$, neither of the groups A_1 and A_2 is contained in the other. Hence, $\exists a_1 \in A_1, a_1 \notin A_2$, and $\exists a_2 \in A_2$, $a_2 \notin A_1$. Then $a_1 = a_2 \notin A_1 \cup A_2$ is a

contradiction. Let $n = m > 1$. For $\varphi_1' = l^{m-1}\varphi_1$ and $\varphi_2' = l^{m-1}\varphi_2$ we can apply the lemma for $n = 1$. For example, let $l^{m-1}\varphi_1(A) = 0$. We consider the homomorphisms $\varphi_1' = \varphi_1$ and $\varphi_2' = l\varphi_2$. We shall show that the conditions of the lemma hold with $n = m-1$. In fact, if $\varphi_2(a) = 0$, then we can set $\alpha(a) = m-1$ and $\beta(a) = 0$, since $l^{m-1}\varphi_1(a) = 0$. If $\varphi_2(a) \ne 0$, then by the hypothesis $\exists \alpha'(a), \beta'(a) \ge 1$ such that $l^{\alpha'(a)}\varphi_1(a) = l^{\beta'(a)}\varphi_2(a) = 0$. Then we set $\alpha(a) = \alpha'(a)$ and $\beta(a) = \beta'(a) - 1$. By induction $\exists \alpha', \beta'$ such that $\alpha' + \beta' \le m-1$ and $l^{\alpha'}\varphi_1(A) = l^{\beta'}l\varphi_2(A) = 0$. Then we set $\alpha = \alpha'$ and $\beta = \beta' + 1$. ■

From Lemma 1 and Proposition 10 we get

Proposition 11. *$\exists \alpha, \beta \in \mathbf{Z}_+$ such that $\alpha + \beta \le n$ if $l \ne 2$, $\alpha + \beta \le n+2$ if $l = 2$, and, for all $\eta \in \mathrm{H}$, $(\eta_1^\sigma\eta_1)^\alpha = 1$ and $(\eta_2^\sigma\eta_2)^\beta = 1$, where η_j is the restriction of η to H_j.* ■

Since $s_1^\sigma = s_1$ and $s_2^\sigma = -s_2$, we have $s_1(\eta_1^\sigma) = \sigma(s_1(\eta_1))$ and $s_2(\eta_2^\sigma) = -\sigma(s_2(\eta_2))$. Therefore we have

Corollary 5. *$\exists \alpha, \beta \in \mathbf{Z}_+$ such that $\alpha + \beta \le n$ if $l \ne 2$, $\alpha + \beta \le n+2$ if $l = 2$, and l^α annihilates $(\sigma+1)\Lambda_1$ and l^β annihilates $(1-\sigma)\Lambda_2$.* ■

Proposition 12. *$\exists \alpha, \beta \in \mathbf{Z}_+$ such that $\alpha + \beta \le n + 2m_{1l} + 2\delta_l + 2\delta_l' + 2m_{5l}$ and l^α annihilates Λ_1, while l^β annihilates Λ_2.*

Proof. Let α' and β' be the same as in Corollary 5. Obviously we may assume that $\alpha' \le n$ and $\beta' \le n$. Let $\Lambda_1' \subset E_{l^{n-\alpha'}}$ be the image of Λ_1 under the homomorphism of multiplication by $l^{\alpha'}$, and let $\Lambda_2' \subset E_{l^{n-\beta'}}$ be the image of Λ_2 under the homomorphism of multiplication by $l^{\beta'}$. We consider $G_{l^n} = G(K'(E_{l^n})/K')$ as a subgroup of $\mathrm{GL}_2(\mathbf{Z}/l^n)$ or $(\mathscr{O}/l^n)^*$ if $\mathrm{End}(E) = \mathbf{Z}$ or $\mathscr{O}$ respectively. Here $\mathscr{O}$ is an order in an imaginary quadratic extension $k/\mathbf{Q}$. If A is a σ-module, then by A_+ and A_- we denote the kernel of $\sigma - 1$ and $\sigma + 1$, respectively. From Corollary 5 it follows that $\Lambda_1' \subset (E_{l^{n-\alpha'}})_-$ and $\Lambda_2' \subset (E_{l^{n-\beta'}})_+$. Moreover, Λ_1' and Λ_2' are G_{l^n}-invariant (since W_1/K' and W_2/K' are Galois extensions).

Lemma 2. *Let $e \in E_{l^m}$ be such that the G_{l^m}-orbit of e belongs to $(E_{l^m})_-$ or $(E_{l^m})_+$. Then $l^\lambda e = 0$, where $\lambda = m_{1l} + m_{5l} + \delta_l'$.*

Proof of Lemma 2. If $m \le m_{1l}$, then the assertion is trivial. Suppose $m > m_{1l}$. We consider first the case when $m_{1l} = 0$. Then, by definition, $G_{l^m} = \mathrm{GL}_2(\mathbf{Z}/l^m)$ or $(\mathscr{O}/l^m)^*$ and if $l = 2$, then either $\mathrm{End}(E) = \mathbf{Z}$ or $\mathrm{End}(E) = \mathscr{O}$ and 2 divides the discriminant $\Delta(\mathscr{O})$ of the order $\mathscr{O}$ or remains prime in k. We shall show that in all these cases the linear hull of G_{l^m} is $M_2(\mathbf{Z}/l^m)$ or $\mathscr{O}/l^m$ respectively. It suffices to verify this for $m = 1$. Suppose $\mathrm{End}(E) = \mathbf{Z}$. We have

$$\mathrm{GL}_2(\mathbf{Z}/l) = M_2(\mathbf{Z}/l) \Big\backslash \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Big| (ad - bc) = 0 \right\};$$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Big| (ad - bc) = 0 \right\} = \left\{ \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}; \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix}; \begin{pmatrix} a & b \\ c & (bc)/a \end{pmatrix}, a \ne 0 \right\}$$

and has order $2l^2 - l + (l-1)l^2 = l^3 + l^2 - l$. Hence $\mathrm{GL}_2(\mathbf{Z}/l)$ contains $l^4 - l^3 - l^2 + l$ elements. Since $l^4 - l^3 - l^2 + l > l^3$ for $l > 2$, the linear hull of $\mathrm{GL}_2(\mathbf{Z}/l)$ is $M_2(\mathbf{Z}/l)$ for $l > 2$. If $l = 2$, this is verified directly.

Suppose $\mathrm{End}(E) = \mathscr{O} = \mathbf{Z} + cO_k$, where $O_k = [1, \tau]$ is the ring of integers of k. Suppose $l \nmid \Delta(\mathscr{O})$. Then $|(\mathscr{O}/l)^*| = l^2 - 1 > l$ if $\left(\frac{l}{k}\right) = -1$. Hence, the linear hull of $(\mathcal{O}/l)^*$ is $\mathcal{O}/l$. If $\left(\frac{l}{k}\right) = 1$, then $|(\mathcal{O}/l)^*| = (l-1)^2 > l$ since $l > 2$ in this case by hypothesis. Hence, the linear hull of $(\mathcal{O}/l)^*$ is $\mathcal{O}/l$. Suppose $l \mid \Delta(\mathcal{O})$. Then $|(\mathcal{O}/l)^*| = l^2 - 1 > l$ if $l > 2$. If $l = 2$, then $(\mathcal{O}/2)^*$ consists of the classes 1 and $1 + c\tau$ or τ, which are linearly independent in $\mathcal{O}/2$. Hence, again the linear hull of $(\mathcal{O}/2)^*$ is equal to $\mathcal{O}/2$. Since, by the definition of m_{1l}, for $m_{1l} > 0$

$$G_{l^m} \supset 1 + l^{m_{1l}} M_2(\mathbf{Z}/l^m), \qquad G_{l^m} \supset 1 + l^{m_{1l}}(\mathcal{O}/l^m),$$

when $\mathrm{End}(E) = \mathbf{Z}$ or $\mathcal{O}$, the linear hull of G_{l^m} obviously always contains $l^{m_{1l}} M_2(\mathbf{Z}/l^m)$ or $l^{m_{1l}}(\mathcal{O}/l^m)$, respectively. Therefore Lemma 2 will follow from Lemma 3.

LEMMA 3. *Let $e \in E_{l^m}$ be such that the $M_2(\mathbf{Z}/l^m)(\mathcal{O}/l^m)$-orbit of e belongs to $(E_{l^m})_-$ or $(E_{l^m})_+$. Then $l^\lambda e = 0$, where $\lambda = m_{5l} + \delta_l'$.*

PROOF OF LEMMA 3. First we consider the case when $\mathrm{End}(E) = \mathbf{Z}$. Then $M_2(\mathbf{Z}/l^m)e = E_{l^\mu}$, where $\lambda \in \mathbf{Z}_+$ is the least such that $l^\lambda e = 0$. Hence, either $E_{l^\mu} = (E_{l^\mu})_-$ or $E_{l^\mu} = (E_{l^\mu})_+$. Since σ is represented in $\mathrm{GL}_2(\mathbf{Z}/l^\lambda)$ by a matrix with determinant -1, then $(-1) \equiv 1 \pmod{l^\lambda}$. Hence $\lambda = 0$ if $l \neq 2$. If $l = 2$, then obviously $\lambda = 0$ if σ acts nontrivially on E_2 (i.e., $E_{2+} = E_{2-} \neq E_2$), and $\lambda \leq 1$ otherwise. Thus, Lemmas 2 and 3 are proved in the case $\mathrm{End}(E) = \mathbf{Z}$. We now consider the case $\mathrm{End}(E) = \mathcal{O} = \mathbf{Z} + cO_k$, $O_k = [1, \tau]$; $E_{l^m} = (\mathcal{O}/l^m)e_m$, where e_m is the generator of E_{l^m} as an $\mathcal{O}/l^m$-module; $\sigma(e_m) = \alpha e_m$, where $\alpha\alpha^\sigma = 1$ in $\mathcal{O}/l^m$. Suppose $e = be_m$. By hypothesis $(\sigma \pm 1)e = 0$ and $(\sigma \pm 1)(c\tau e) = 0$. Hence, $b^\sigma\alpha \pm b = 0$ and $c(\tau^\sigma b^\sigma \alpha \pm \tau b) = 0$. From this, $b^\sigma\alpha = \mp b$ and $bc(\tau^\sigma - \tau) = 0$. If b_1 is a representative of b in $\mathcal{O}$, then we have $b_1 c(\tau^\sigma - \tau) = l^m y$, where $y \in \mathcal{O}$. Hence,

$$b_1 = l^m(1/(c(\tau^\sigma - \tau)))y = l^m(c(\tau^\sigma - \tau)y)/(c^2(\tau^\sigma - \tau)^2) = (l^m/\Delta(\mathcal{O}))z,$$

where $z \in \mathcal{O}$. Here $\Delta(\mathcal{O}) = c^2\Delta(O_k)$ is the discriminant of the ring $\mathcal{O}$. In fact, if $\tau^2 + A\tau + B = 0$, then

$$\begin{aligned}(\tau^\sigma - \tau)^2 &= (\tau^\sigma)^2 - 2\tau^\sigma\tau + \tau^2 = -A\tau^\sigma - B - 2B - A\tau - B \\ &= A(-\tau - \tau^\sigma) - 4B = A^2 - 4B = \Delta(O_k).\end{aligned}$$

Since by definition $\Delta(\mathcal{O}) = l^{m_{5l}} r$, $(r, l) = 1$, obviously $l^{m_{5l}} e = 0$. This proves Lemmas 2 and 3. ■

Applying Lemma 2, we obtain that $l^{m_{1l} + m_{5l} + \delta_l'} \Lambda_1' = 0$ and $l^{m_{1l} + m_{5l} + \delta_l'} \Lambda_2' = 0$. We set $\alpha = \alpha' + m_{1l} + m_{5l} + \delta_l'$ and $\beta = \beta' + m_{1l} + m_{5l} + \delta_l'$. Then $l^\alpha \Lambda_1 = 0$, $l^\beta \Lambda_2 = 0$, and

$$\alpha + \beta = \alpha' + \beta' + 2m_{1l} + 2m_{5l} + 2\delta_l' \leq n + 2m_{1l} + 2m_{5l} + 2\delta_l + 2\delta_l'.$$

Proposition 12 is proved. ■

We complete the proof of the theorem. From the definition of m_{2l}, δ_l'', and δ_l''' it follows that if l^α annihilates s in $H^1(V, E_D)$, then $l^{\alpha + m_{2l} + \delta_l'' + \delta_l'''}$ annihilates s in $S_D = S_D(\mathbf{Q})$. Analogously, if l^β annihilates x_K in $H^1(V, E_D)$, then $l^{\beta + m_{2l} + \delta_l'''}$ annihilates x_K in $S_D(K)$. By the definition of $\varepsilon_l(n)$, $\beta + m_{2l} + \delta_l''' \geq \varepsilon_l(n)$. Since $\alpha + \beta \leq n + 2m_{1l} + 2\delta_l + 2\delta_l' + 2m_{5l}$, we have

$$\begin{aligned}\alpha + m_{2l} + \delta_l'' + \delta_l''' &\leq n - (\beta + m_{2l} + \delta_l''') + 2m_{1l} + 2m_{2l} + 2\delta_l \\ &\quad + 2\delta_l' + \delta_l'' + 2\delta_l''' + 2m_{5l} \\ &\leq n - \varepsilon_l(n) + m_l,\end{aligned}$$

which completes the proof of Theorem 1. ■

Received 25/JUNE/87

BIBLIOGRAPHY

1. J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 223–251.
2. Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), 225–320.
3. B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. 25 (1974), 1–61.
4. Bernadette Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, C. R. Acad. Sci. Paris Sér. I Math. 303 (1986), 165–168.
5. Gorô Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton, N.J., and Univ. of Tokyo Press, Tokyo, 1971.
6. John T. Tate, *The arithmetic of elliptic curves*, Invent Math. 23 (1974), 179–206.
7. J. W. S. Cassels and A. Fröhlich (editors), *Algebraic number theory* (Proc. Instructional Conf., Brighton, 1965), Academic Press, London, and Thompson, Washington, D.C., 1967.
8. M. I. Bashmakov, *Cohomology of abelian varieties over a number field*, Uspekhi Mat. Nauk 27 (1972), no. 6(168), 25–66; English transl. in Russian Math. Surveys 27 (1972).
9. H. Koch, *Galoissche Theorie der p-Erweiterungen*, Springer-Verlag, 1970.
10. Yu. I. Manin, *Cyclotomic fields and modular curves*, Uspekhi Mat. Nauk 26 (1971), no. 6(162), 7–71; English transl. in Russian Math. Surveys 26 (1971).
11. B. Mazur, *On the arithmetic of special values of L-functions*, Invent. Math. 55 (1979), 207–240.

Translated by J. S. JOEL