On the Structure of Shafarevich-Tate Groups

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

1989

Contents

1 Introduction

Let E be a Weil elliptic curve over the fied of rational numbers $\mathbb{Q}$. Note that, according to the Weil-Taniyama conjecture, ever 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 R. According to the Mordell-Weil theorem, $E(R)$ is a finitey generated (abelian) group, that is, $E(R)_{\text{tor}}$ is finite and $E(R) \cong E(R)_{\text{tor}} \times \mathbb{Z}^{g(R,E)}$, 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:

$$Ш(R,E) = \ker\left(H^1(R,E) \to \prod_v H^1(R(v),E)\right)$$

(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 torsion group and for all natural M its subgroup $Ш(E,R)_M$ of M-torsion 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 1.2 below). Let $[Ш(R,E)]^?$ denote the hypothetical order of $Ш(R,E)$; then, according to BS, we have the quality $[Ш(R,E)] = [Ш(R,E)]^?$.

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 $\gamma : X_N \to E$ a Weil parametrization. here X_N is the modular curve over $\mathbb{Q}$ which parameterizes isomorphism classes of isogenies $E' \to E''$ of elliptic curves with cyclic kernel of order N. The field $K = \mathbb{Q}(\sqrt{D})$ has discriminant D satisfying $0 > D \equiv$ square $\pmod{4N}$)., where $D \neq -3$ or -4. Fix an ideal i_1 of the ring of integers O_1 of K for which $O_1/i_1 \cong \mathbb{Z}/N$. 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 $\mathbb{C}/O_\lambda \to \mathbb{C}/i_\lambda^{-1}$ (here $i_\lambda^{-1} \supset O_\lambda$ is the inverse of I_λ in the group of proper $O_{|lambda}$-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 $\mathcal{O} = \mathrm{End}(E)$ and $Q = \mathcal{O} \otimes \mathbb{Q}$. Let ℓ be a rational prime, $T = \varprojlim E_{\ell^n}$ the Tate module, and $\hat{\mathcal{O}} = \mathcal{O} \otimes \mathbb{Z}_\ell$. Let $B(E)$ denote the set of odd rational primes which do not divide the discriminant of $\mathcal{O}$ and for which the natural representation $\rho : G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathcal{O}} T$ 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 $\mathcal{O} = \mathbb{Z}$ and N is square-free, then all $\ell \geq 11$ belong to $B(E)$.

If the point P_1 has infinite order, (that is, $P_1 \notin E(K)_{\mathrm{tor}}$) 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 1.1. *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 $\ell \in B(E)$ we have $\mathrm{ord}_\ell(d) = 0$.*

In Theorem 1.1, d is an integer which depends upon E but not upon K. The application of Theorem **??** to BS is clear from the following result of Gross and Zagier [5] for $(D, 2N) = 1$.

Theorem 1.2. *The function $L(E, K, s)$ vanishes at $s = 1$. The point P_1 has infinite order $\iff$ $L'(E, K, 1) \neq 0$. 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 $[Ш(K, E)] = \left(C_K / \left(c \prod_{q|N} b\langle q \rangle\right)\right)^2$.*

In Theorem 1.2, the integer c is defined in terms of the parameterization γ (cf. [5]), and the integer $b\langle q \rangle$, where $q \mid N$ 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 $\mathrm{Re}(s) > 3/2$ 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 $\ell \in B(E)$. Let $n(p) = \mathrm{ord}_\ell(p+1, a_p)$, 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 $P_0 := 1$, and $\Lambda = \bigcup_{r \geq 0} \Lambda^r$. If $r > 0$ and $\lambda \in \Lambda^r$, let $n(\lambda)$ denote $\min_{p|\lambda} n(p)$; then $M_\lambda = \ell^{n(\lambda)}$ and $n(1) = \infty$. Let $\lambda \in \Lambda$, $1 \leq n \leq n(\lambda)$, and $M = \ell^n$. 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 1.1.

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

$$0 \to E_M \to E(\overline{R}) \to \xrightarrow{\times M} 0$$

induces the exact squence

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

If R/L is a Galois extension, then

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

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 $\ell \in B(E)$ 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 $1 \leq \lambda \in \Lambda$, then the natural homomorphism $G(K_\lambda/K_1) \to \prod_{p|\lambda} G(K_p/K_1)$ is an isomorphism, and we also have the isomorphisms

$$G(K_\lambda/K_{\lambda/p}) \xrightarrow{\cong} G(K_p/K_1) \xrightarrow{\cong} \mathbb{Z}/(p+1).$$

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.

2 Statement of Main Theorem of [?]

Let ℓ be an odd prime and A a finite abelian group of ℓ-power order. The *sequence of invariants* of A is the nonincreasing sequence of nonnegative integers $\{n_1, n_2, \ldots\}$ such that

$$A \approx \bigoplus_{i\geq 1} \mathbb{Z}/\ell^{n_i}\mathbb{Z}.$$

Fix an elliptic curve E over $\mathbb{Q}$ and let ε denote the *negative* of the sign of the functional equation of E, and let K be a field that satisfies the Heegner hypothesis.

Suppose A is equipped with an action of complex conjugation σ. For $\nu = 0, 1$ let A^ν denote the submodule $(1 - (-1)^\nu \varepsilon\sigma)A$. Since ℓ is odd, $A = A^0 \oplus A^1$, and σ acts on A^ν as multiplication by $(-1)^{\nu-1}\varepsilon$. Proof:

$$\sigma(1 - (-1)^\nu \varepsilon\sigma)x = (\sigma - (-1)^\nu\varepsilon)x = (-1)^{\nu-1}\varepsilon x + \sigma x,$$

and

$$(-1)^{\nu-1}\varepsilon(1-(-1)^\nu\varepsilon\sigma)x = ((-1)^{\nu-1}\varepsilon - (-1)^{2\nu-1}\sigma)x = ((-1)^{\nu-1}\varepsilon + \sigma)x.$$

Let $X = Ш(E/K)[\ell^\infty]$, and for $\nu = 0, 1$, let $\{x_i^\nu\}$ be the sequence of invariants of X^ν. If $r \in \mathbb{N}$, let $\nu(r) \in \{0, 1\}$ be such that $r - \nu(r) - 1$ is even. Set

$$\xi(r, \nu) = r - |\nu - \nu(r)|.$$

Let $B(E)$ denote the set of odd rational primes which do not divide the discriminant of $\mathcal{O} = \mathrm{End}(E)$ and for which $\rho : G_\mathbb{Q} \to \mathrm{Aut}_\mathcal{O}(T_\ell(E))$ is surjective. Fix $\ell \in B(E)$ and for any prime p let $n(p) = \mathrm{ord}_\ell(\gcd(p+1, a_p))$. Let Λ^r denote the set of all products of r distinct primes $p \nmid N$ such that p is inert in K, and for which $n(p) > 0$. Let Λ be the union of the Λ^r, and for any $\lambda \in \Lambda$ let $n(\lambda) = \min_{p|\lambda} n(p)$.

Suppose $\lambda \in \Lambda$. Let $m'(\lambda)$ be the exponent of the highest power of ℓ that divides P_λ in $E(K_\lambda)$. Let

$$m(\lambda) = \begin{cases} m'(\lambda) & \text{if } m'(\lambda) < n(\lambda), \\ \infty & \text{otherwise.} \end{cases}$$

Let $m_r = \min_{\lambda\in\Lambda^r} m(\lambda)$. For example, $m_0 = \mathrm{ord}_\ell([E(K) : \mathbb{Z}P_1])$. Let

$$m = \min_{\lambda\in\Lambda} m(\lambda).$$

Theorem 2.1 (Kolyvagin). *If $\nu \in \{0,1\}$ and $r \geq 1+\nu$, then*

$$x^{\nu}_{r-\nu} = m_{\xi(r,\nu)-1} - m_{\xi(r,\nu)}.$$

Theorem 2.2 (Kolyvagin). $\#\text{Ш}(E/K)[\ell^\infty] = \ell^{2(m_0-m)}$

Theorem 2.3 (Kolyvagin). *The full Birch and Swinnerton-Dyer conjecture is true for E over K if and only if $m = \mathrm{ord}_\ell\left(c\prod_{q|N} c_q\right)$, where c is the Manin constant, and the c_q are the Tamagawa numbers.*

3 Notation

Let ℓ be a prime and A an abelian group of ℓ-power order.

$$\begin{aligned}
\ell &= \text{ a prime}\\
A &= \text{ abelian group of } \ell\text{-power order}\\
M &= \ell^n\\
A[M] &= \text{ kernel of multiplication by } M\\
A/MA &= \text{ cokernel of multiplication by } M\\
\overline{L} &= \text{ algebraic closure of } L\text{, embedded in } \mathbb{C}\\
\mathrm{Gal}(R/L) &= \text{ Galois group of } R/L\text{, when defined}\\
H^1(L,A) &= H^1(\mathrm{Gal}(\overline{L}/L),A)\\
\mathcal{O}^* &= \text{ units in the ring } \mathcal{O}\\
R(v) &= \text{ completion of } R \text{ at the place } v\\
K_\lambda &= \text{ ring class field of } K \text{ of conductor } \lambda\\
\mathcal{K} &= \text{ the unramified quadratic extension of } \mathbb{Q}_p\\
H^1(R,A) \ni \tau \mapsto \tau_v &= \tau(v) \in H^1(R_v,A)\\
\overline{\mathbb{Q}}_p \approx \overline{K}(\mathfrak{p}) &= \bigcup_{\mathfrak{p}|v} R_v, \text{ where } \mathfrak{p} \text{ is a fixed place over } p \in \Lambda^1\\
H_{p,n} &= \text{ (see page 12)}\\
X &= Ш(E/K)[\ell^\infty]\\
n(\lambda) &= \min_{p|\lambda} \mathrm{ord}_\ell(\gcd(p+1,a_p))\\
m'(\lambda) &= \mathrm{ord}_\ell(P_\lambda \in E(K_\lambda))\\
m(\lambda) &= \begin{cases} m'(\lambda) & \text{if } m'(\lambda) < n(\lambda),\\ \infty & \text{otherwise}\end{cases}\\
m_r &= \min_{\lambda\in\Lambda^r} m(\lambda)\\
m_0 &= \mathrm{ord}_\ell([E(K):\mathbb{Z}P_1])\\
\nu &\in \{0,1\} \text{ (fixed)}\\
\nu(r) &\in \{0,1\} \text{ has opposite parity to that of } r\\
\xi(r,\nu) &= r - |\nu-\nu(r)|\\
\Lambda^r &= \{ \text{ all products of } r \text{ distinct } p\nmid N \text{ s.t. } p \text{ is inert in } K \text{ and } n(p)>0 \text{ }\}\\
\Lambda &= \cup_{r\geq 0}\Lambda^r\\
\Lambda^r_n &= \{\lambda\in\Lambda^r : n(\lambda)\geq n\}\\
\Lambda_n &= \bigcup_{r\geq 0}\Lambda^r_n
\end{aligned}$$

$$\begin{aligned}
e(A) &= e_\ell(A) = \min\{k\geq 0 : \ell^k A = 0\} \text{ (here } A \text{ is a torsion } \mathbb{Z}_\ell\text{-module)}\\
e(a) &= e_\ell(a) = e(\mathbb{Z}_\ell\cdot a) = \log_\ell(\mathrm{order}(a))\\
\psi^\nu_{p,n} &= \text{ (see page 14)}\\
u(\nu) &= \text{ (see page 28)}
\end{aligned}$$

We use n, n', n'' for natural numbers and M, M', M'', resp., for ℓ^n, $\ell^{n'}$, and $\ell^{n''}$.

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

4.1 The Definition of the Classes $\tau_{\lambda,n}$

Fix $\lambda \in \Lambda$ and $\ell \in B(E)$. Let $M = \ell^n$, where $1 \leq n \leq n(\lambda)$. We construct a class $\tau_{\lambda,n} \in H^1(K, E[M])$.

Let K_λ be the ring class field of K with conductor λ. Thus K_1 is the Hilbert class field of K and if $\lambda > 1$, then

$$\mathrm{Gal}(K_\lambda/K_1) \longrightarrow \prod_{p|\lambda} \mathrm{Gal}(K_p/K_1)$$

is an isomorphism and

$$\mathrm{Gal}(K_\lambda/K_{\lambda/p}) \xrightarrow{\cong} \mathrm{Gal}(K_p/K_1) \xrightarrow{\cong} \mathbb{Z}/(p+1)\mathbb{Z}.$$

For each $p \mid \lambda$, fix a generator $t_p \in \mathrm{Gal}(K_\lambda/K_{\lambda/p})$.

Let $\mathcal{O}_\lambda = \mathbb{Z} + \lambda\mathcal{O}_K$ and $\mathcal{I}_\lambda = \mathcal{N} \cap \mathcal{O}_\lambda$, where $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Let $z_\lambda \in X_0(N)(K_\lambda)$ be the point corresponding to the cyclic N-isogeny

$$(\mathbb{C}/\mathcal{O}_\lambda \to \mathbb{C}/\mathcal{I}_\lambda^{-1}).$$

Set

$$y_\lambda = \pi_E(z_\lambda) \in E(K_\lambda).$$

Since $\ell \in B(E)$,

$$\mathrm{res}_K^{K_\lambda} : H^1(K, E[M]) \to H^1(K_\lambda, E[M])^{\mathrm{Gal}(K_\lambda/K)}$$

is an *isomorphism*. Thus to construct an element of $H^1(K, E[M])$, it suffices to give an element of $H^1(K_\lambda, E[M])^{\mathrm{Gal}(K_\lambda/K)}$, which is what we now do.

Let

$$I_p = -\sum_{i=1}^{p} i t_p^i$$

and

$$I_\lambda = \prod_{p\mid\lambda} I_p \in \mathbb{Z}[\mathrm{Gal}(K_\lambda/K_1)].$$

Let $J_\lambda = \sum g$, where g runs through a set of coset representatives for $\mathrm{Gal}(K_\lambda/K_1)$ inside $\mathrm{Gal}(K_\lambda/K)$. Then $J_\lambda I_\lambda \in \mathbb{Z}[\mathrm{Gal}(K_\lambda/K)]$ and we let

$$P_\lambda = J_\lambda I_\lambda y_\lambda \in E(K_\lambda).$$

Then

$$\mathrm{res}_K^{K_\lambda}(\tau_{\lambda,n}) = P_\lambda \pmod{ME(K_\lambda)} \in E(K_\lambda)/ME(K_\lambda) \hookrightarrow H^1(K_\lambda, E[M]). \tag{4.1}$$

Remark 4.1. If P_1 has infinite order, then Kolyvagin proved that

$$\#\text{Ш}(E/K)[\ell^\infty] \mid \ell^{2m_0},$$

where $m_0 = \mathrm{ord}_\ell([E(K) : \mathbb{Z}P_1])$.

4.2 Properties of the Points y_λ

Suppose $p \mid \lambda$ and set $\mathrm{Tr}_p = \sum_{i=0}^{p} t_p^i$. Then

$$\mathrm{Tr}_p\, y_\lambda = a_p y_{\lambda/p}.$$

Let $\overline{\mathbb{F}}_p$ denote the residue class field of $\overline{K}_\mathfrak{p}$, and set $\tilde{E} = E_{/\mathbb{F}_p}$.

$$E(\overline{K}_\mathfrak{p}) \ni \alpha \mapsto \tilde{\alpha} \in \tilde{E}(\overline{\mathbb{F}}_p).$$

Let $\mathrm{Fr}_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ be the pth power automorphism. For all $g \in \mathrm{Gal}(K_\lambda/\mathbb{Q})$, we have

$$\widetilde{gy_\lambda} = \mathrm{Fr}_p(\widetilde{gy_{\lambda/p}}).$$

Let θ_λ be the Artin reciprocity homomorphism from the group of classes of $\mathcal{O}_\lambda$ ideals to $\mathrm{Gal}(K_\lambda/K)$, and let σ denote complex conjugation. We have

$$\sigma(y_\lambda) \equiv \varepsilon\theta_\lambda(\mathcal{I}_\lambda)y_\lambda \pmod{E(\mathbb{Q})_{\mathrm{tor}}}. \tag{4.2}$$

We have

$$(t_p - 1)I_p = \mathrm{Tr}_p - (p+1).$$

If $M \mid \gcd(p+1, a_p)$, then for all $g \in \mathrm{Gal}(K_\lambda/\mathbb{Q})$, we have

$$gP_\lambda \equiv P_\lambda \pmod{ME(K_\lambda)},$$

so (4.1) really does defines an element $\tau_{\lambda,n} \in H^1(K, E[M])$.

Since $\sigma g = g^{-1}\sigma$ for all $g \in \mathrm{Gal}(K_\lambda/K)$, it follows that

$$\sigma I_p \equiv -I_p \sigma \pmod{M}.$$

This and (4.2) imply that if $\lambda \in \Lambda^r$, then

$$\begin{aligned} \sigma P_\lambda &= \varepsilon(-1)^r P_\lambda \pmod{ME(K_\lambda)}, \quad \text{and} \\ \sigma \tau_{\lambda,n} &= \varepsilon(-1)^r \tau_{\lambda,n}. \end{aligned}$$

4.3 Properties of the Localization of $\tau_{\lambda,n}$

Recall that p is a prime of good reduction for E which is inert in K and that

$$a_p \equiv p + 1 \equiv 0 \pmod{M}.$$

The primes p that we will actually use to prove things will be given by a Chebaterov density argument, so we can safely assume that $p > 2$ (so that the appropriate reduction maps are injective). For all $M = \ell^{n'}$, we have

$$E[M] \subset E(\mathbb{Q}_p^{\mathrm{un}})$$

and reduction induces a $G_p = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{un}}/\mathbb{Q}_p)$ isomorphism

$$E[M] \xrightarrow{\cong} \tilde{E}(\overline{\mathbb{F}}_p)[M].$$

We have

$$\mathrm{Fr}_p^2 - a_p \, \mathrm{Fr}_p + p = 0$$

on $E[M]$ and $\tilde{E}(\overline{\mathbb{F}}_p)[M]$. Since $a_p \equiv p + 1 \equiv 0 \pmod{M}$,

$$\mathrm{Fr}_p^2 - 1 = 0 \qquad \text{on } E[M],$$

so $E[M] \subset E[\mathcal{K}]$, where $\mathcal{K}$ is the unramified quadratic extension of $\mathbb{Q}_p$. Since p is inert in K, it follows that $\mathcal{K} = K(p)$.

Let $F = \mathbb{F}_{p^2}$ denote the residue class field of $\mathcal{K}$.

Lemma 4.2. *We have a commutative square of isomorphisms*

$$\begin{tikzcd}
E(\mathcal{K})/ME(\mathcal{K}) \arrow[r, "\cong", "f_{p,n}"'] \arrow[d, "\cong"] & E[M] \arrow[d, "\cong"] \\
\tilde{E}(F)/M\tilde{E}(F) \arrow[r, "\cong", "\tilde{f}_{p,n}"'] & \tilde{E}[M],
\end{tikzcd}$$

where

$$f_{p,n} = \frac{\mathrm{Fr}_{p^2} - 1}{M}, \qquad \tilde{f}_{p,n} = \frac{a_p}{M}\,\mathrm{Fr}_p - \frac{p+1}{M}.$$

(The meaning of $f_{p,n}$ is "first make a choice of Mth root, then apply $\mathrm{Fr}_{p^2} - 1$"; this is well defined since different choices differ by an Mth root, and the Mth roots are fixed by Fr_{p^2}, since they are rational over $\mathcal{K}$.)

Proof. Suppose $f_{p,n}(P) = 0$, so there is $Q \in E(\overline{\mathbb{Q}}_p)$ such that $MQ = P$ and $(\mathrm{Fr}_p^2 - 1)(Q) = 0$. Thus $Q \in E(\mathcal{K})$, so $P \pmod{ME(\mathcal{K})} = 0$, and $f_{p,n}$ is injective. The diagram commutes because $\mathrm{Fr}_p^2 - 1 = a_p \mathrm{Fr}_p - (p+1)$ on $E(\overline{\mathbb{F}}_p)[\ell^\infty]$. The leftmost vertical map is surjective, by Hensel's lemma, and hence an isomorphism because, as mentioned above, the rightmost vertical map is an isomorphism (and $f_{p,n}$ is injective). Because $f_{p,n}$ is injective so is $\tilde{f}_{p,n}$, so to complete the proof it suffices to show that $\tilde{f}_{p,n}$ is surjective. Since $\#\tilde{E}(F)$ is *finite*,

$$\#\left(\frac{\tilde{E}(F)}{M\tilde{E}(F)}\right) = \frac{\#\tilde{E}(F)}{\#M\tilde{E}(F)} = \frac{\#\tilde{E}(F)}{\#\tilde{E}(F)/\#\tilde{E}[M]} = \#\tilde{E}[M].$$

Thus $\tilde{f}_{p,n}$ and hence $f_{p,n}$ must be surjective. □

Let

$$[\,,\,]_M : E[M] \times E[M] \longrightarrow \mu_M$$

denote the Weil pairing. We have

$$[\gamma(e_1), \gamma(e_2)]_M = \gamma([e_1, e_2]_M) \tag{4.3}$$

for all $\gamma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let $E[M] = E[M]^0 \oplus E[M]^1$ be the decomposition of $E[M]$ with respect to the involution Fr_p, as described in Section 2.

Lemma 4.3. *$E[M]^\nu \approx \mathbb{Z}/M\mathbb{Z}$ for $\nu = 0, 1$.*

Proof. If the lemma is false, then $\mathrm{Fr}_p = 1$ or $\mathrm{Fr}_p = -1$ on $E[\ell]$ (I don't 100% see this, though I don't see how it could be wrong either), and we have for any $e_1, e_2 \in E[M]$,

$$\begin{aligned}[e_1, e_2]_\ell &= [\mathrm{Fr}_p(e_1), \mathrm{Fr}_p(e_2)]_\ell = \mathrm{Fr}_p[e_1, e_2]_\ell \\ &= ([e_1, e_2]_\ell)^p = [e_1, e_2]_\ell^{-1},\end{aligned}$$

so $[e_1, e_2]_\ell = 1$, since ℓ is odd. (In the last equality, we used that $p \equiv -1 \pmod{\ell}$.) This is impossible, because $[\,,\,]_\ell$ is nondegenerate. $\square$

Let

$$H_{p,n} := H^1(\mathcal{K}, E[M]) = \mathrm{Hom}(G_p^{\mathrm{ab}}/(G_p^{\mathrm{ab}})^M, E[M]) \cong \mathrm{Hom}(\mathcal{K}^*/(\mathcal{K}^*)^M, E[M]),$$

where we have used the isomorphism $\theta_p : \mathcal{K}^*/(\mathcal{K}^*)^M \to G_p^{\mathrm{ab}}/(G_p^{\mathrm{ab}})^M$ from local class field theory. We have

$$\mathcal{K}^*/(\mathcal{K}^*)^M = \mathcal{A}_n \oplus \mathcal{B}_n$$

where $\mathcal{A}_n = \langle p \rangle = p^{\mathbb{Z}}/p^{M\mathbb{Z}}$ and $\mathcal{B}_n = \mathcal{O}_\mathcal{K}^*/(\mathcal{O}_\mathcal{K}^*)^M$. Then

$$H_{p,n} = A_{p,n} \oplus B_{p,n}$$

where $A_{p,n}$ (resp., $B_{p,n}$) is the subgroup of $H_{p,n}$ of homomorphisms that are trivial on $\mathcal{B}_n$ (resp., $\mathcal{A}_{p,n}$). Note that $A_{p,n} = E(\mathcal{K})/ME(\mathcal{K})$, since

$$E(\mathcal{K})/ME(\mathcal{K}) \subset A_{p,n} = H_{p,n}^{\mathrm{un}}$$

and $\#(E(\mathcal{K})/ME(\mathcal{K})) = M^2 = \#A_{p,n}$ (see Lemma 4.2).

If $\mathcal{L}_{p,n}$ is the class field of $\mathcal{K}$ that 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

$$G_{p,n} = \mathrm{Gal}(\mathcal{L}_{p,n}/\mathcal{K}).$$

Because $H_{p,n} = A_{p,n} \oplus B_{p,n}$, it follows that $H_{p,n}^\nu$ decomposes into a direct sum of the cyclic subgroups $A_{p,n}^\nu$ and $B_{p,n}^\nu$ of order M.

Let $\mathcal{K}_p$ be the class field of $\mathcal{K}$ corresponding to the subgroup $p^{\mathbb{Z}}(\mathbb{Z}_p^* + p\mathcal{O}_\mathcal{K})$. 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 $\lambda \in \Lambda$ is a multiple of p. The completion of $K_{\lambda/p}$ in $\overline{K}(\mathfrak{p})$ is the field $\mathcal{K}$, the completion of K_λ is the field $\mathcal{K}_p$, and the embedding (as decomposition group)

$$\mathrm{Gal}(\overline{\mathcal{K}}(\mathfrak{p})/\mathcal{K}) \hookrightarrow \mathrm{Gal}(\overline{K}/K_{\lambda/p})$$

induces an isomorphism between $\mathrm{Gal}(\mathcal{K}_p/\mathcal{K})$ and $\mathrm{Gal}(K_\lambda/K_{\lambda/p})$. Thus the generator $t_p \in \mathrm{Gal}(K_\lambda/K_{\lambda/p})$ can also be viewed as a generator of $\mathrm{Gal}(\mathcal{K}_p/\mathcal{K})$. Let $t_{p,n}$ denote the generator of $G_{p,n}$ which is the image of t_p.

For $e \in E[M]$, let $b_{p,n}(e)$ be the element of $H_{p,n}$ which sends $t_{p,n} \in G_{p,n}$ to e. We define a nondegenerate alternating pairing

$$\langle\, , \rangle'_{p,n} : H_{p,n} \times H_{p,n} \longrightarrow Z/M\mathbb{Z}$$

by the following conditions: the group $H^0_{p,n}$ is orthogonal to the group $H^1_{p,n}$, and for $s \in A_{p,n}$ and all $e \in E[M]$ we have

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

where

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

Let

$$\langle\, , \rangle_{p,n} : H_{p,n} \times H_{p,n} \to \mathbb{Z}/M\mathbb{Z}$$

be the alternating pairing induced by cup product, the pairing $[\, ,]_M$, and the canonical isomorphism $H^2(\mathcal{K}, \mu_M) \to \mathbb{Z}/M\mathbb{Z}$. This is a pairing of $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$ modules, hence $H^0_{p,n}$ is orthogonal to $H^1_{p,n}$. According to formula (5) of [**?**],

$$\langle s, b_{p,n}(e)\rangle_{p,n} = \langle s, b_{p,n}(e)\rangle'_{p,n}$$

for all s and e, it follows that

$$\langle\, , \rangle_{p,n} = \langle\, , \rangle'_{p,n}.$$

Fix generators e_p^ν of the groups $E^\nu_{M_p}$, where $M_p = \ell^{n(p)}$, such that

$$[e_p^0, e_p^1]_M = \zeta_{p,n(p)}.$$

Set

$$e^\nu_{p,n} = \frac{M_p}{M} e^\nu_p.$$

Then $[e^0_{p,n}, e^1_{p,n}] = \zeta_{p,n}$, since $[N\beta, N\alpha]_M = [\alpha, \beta]^N_{M_p}$ for all $\alpha, \beta \in E[M_p]$ and $N = M_p/M$. (I'm not sure this makes any sense, but it's my best guess at what Kolvagin means; what he writes makes no sense.)

Definition 4.4 ($\psi_{p,n}^{\nu}$)**.** Define a homomorphism

$$\psi_{p,n}^{\nu} : H_{p,n}^{\nu} \to \mathbb{Z}/M\mathbb{Z}$$

by $\psi_{p,n}^{\nu}(x) = \langle x, b_{p,n}^{\nu} \rangle_{p,n}$, where $b_{p,n}^{\nu} = b_{p,n}(e_{p,n}^{1-\nu})$.

Then $\psi_{p,n}^{\nu}$ is trivial on $B_{p,n}^{\nu} = \langle b_{p,n}^{\nu} \rangle$ and induces an isomorphism between $A_{p,n}^{\nu}$ and $\mathbb{Z}/M\mathbb{Z}$ such that for all $s \in A_{p,n}^{\nu}$ we have

$$\psi_{p,n}^{\nu}(s) e_{p,n}^{\nu} = (-1)^{\nu} f_{p,n}(s). \tag{4.4}$$

Let $\psi_{p,n} = \psi_{p,n}^{0} + \psi_{p,n}^{1}$ and, abusing notation, let $\psi_{p,n}$ also denote the homomorphism $H^1(K, E[M]) \to \mathbb{Z}/M\mathbb{Z}$ which is the composition of $\psi_{p,n}$ and the localization homomorphism $H^1(K, E[M]) \to H_{p,n}$.

Let $S_{\lambda,n}$ be the subgroup of $\alpha \in H^1(K, E[M])$ such that $\alpha(v) \in E(K(v))/ME(K(v))$ for all places v of K that do not divide λ. (Equivalently, the image of α in $H^1(K(v), E)$ is trivial for all $v \nmid \lambda$.) Thus $S_{\lambda,n}$ contains $\mathrm{Sel}^{(M)}(E/K)$, but $S_{\lambda,n}$ might be bigger because there is no local condition at places that divide λ.

Proposition 4.5. *Let $\lambda \in \Lambda^r$. Then $\tau_{\lambda,n} \in S_{\lambda,n}^{\nu(r)}$. If $\xi(p, \lambda) = 1$, then*

$$\tau_{p,n}(p) = P_\lambda \,(\mathrm{mod}\ ME(K_p)) \in E(K_p)/ME(K_p).$$

If $p \mid \lambda$, then

$$\tau_{\lambda,n}(p) = \varepsilon \cdot \psi_{p,n}(\tau_{\lambda/p,n}) \cdot b_{p,n}^{\beta}, \qquad \textit{where } \beta = \nu(r) \tag{4.5}$$

$$\varepsilon \cdot \psi_{p,n}(\tau_{\lambda/p,n}) \cdot e_{p,n}^{\beta'} = \left((-1)^{\beta} \cdot \frac{p+1}{M} \cdot \varepsilon - \frac{a_p}{M} \right) \widetilde{P_{\lambda/p}}. \tag{4.6}$$

Proof. The cohomology class $\tau_{\lambda,n}$ contains the cocycle

$$k_{\lambda,n}(\gamma) = \left(\gamma \left(\frac{P_\lambda}{M} \right) - \frac{P_\lambda}{M} \right) + \frac{(1-\gamma)P_\lambda}{M}, \tag{4.7}$$

where

$$\frac{(1-\gamma)P_\lambda}{M} \in E(K_\lambda)$$

is the unique (since $E(K_\lambda)[\ell^\infty]$ is trivial) solution to the equation $Mx = (1-\gamma)P_\lambda \in ME(K_\lambda)$. If $\xi(p, \lambda) = 1$, then $K_\lambda \subset \mathcal{K}$ and $\mathrm{Gal}(\overline{K}(\mathfrak{p})/\mathcal{K}) \subset \mathrm{Gal}(\overline{K}/K_\lambda)$, hence, in view of (4.7), we see that $\tau_{\lambda,n}(p) = P_\lambda (\mathrm{mod}\ ME(\mathcal{K}))$.

If R is a field and $\alpha \in H^1(R, E[M])$, denote by (α) the image of α in $H^1(R, E)[M]$. Again, in view of (4.7), we see that the class $(\tau_{\lambda,n})$ contains the cocycle

$$k'_{\lambda,n}(\gamma) = \frac{(1-\gamma)P_\lambda}{M}.$$

In particular,

$$(\tau_{\lambda,n}) \in H^1(\mathrm{Gal}(K_\lambda/K), E(K_\lambda)).$$

Let v be a place of K that does not divide λ. Then since K_λ/K is unramified outside λ, it follows that $(\tau_{\lambda,n})_v \in H^1(K_v, E)^{\mathrm{un}}$. This group is always finite and is trivial if $(v, N) = 1$. Gross observed that in the case $v \mid \lambda$, we have $(\tau_{\lambda,n})_v = 0$ as well. (Huh?) Hence $\tau_{\lambda,n} \in S^\beta_{\lambda,n}$.

Suppose that $p \mid \lambda$. Since reduction induces an isomorphism between $E[M]$ and $E(F)[M]$, the elment $k_{\lambda,n}(\gamma)$ may be defined by its reduction. We shall show that if

$$\gamma \in \mathrm{Gal}(\overline{K}(\mathfrak{p})/\mathcal{K}) \subset \mathrm{Gal}(\overline{K}/K_{\lambda/p}),$$

then the eduction of the first term of (4.7) is trivial. Indeed, it is equal to

$$\tilde{\gamma}\frac{\tilde{P}_\lambda}{M} - \frac{\tilde{P}_\lambda}{M} = 0,$$

since, by virtue of ... and the definition of P_λ, we have

$$\tilde{P}_\lambda = -(1 + 2 + \cdots + p)\,\mathrm{Fr}_p\,\tilde{P}_{\lambda/p} \in ME(F).$$

Hence

$$\tau_{\lambda,n}(p) \in H^1(\mathrm{Gal}(\mathcal{K}_p/\mathcal{K}), E[M]) = B_{p,n}.$$

It remains to calculate the value of $\tau_{\lambda,n}(p)$ at t_p. We have

$$\begin{aligned}
\frac{(1-t_p)P_\lambda}{M} &= \frac{(1-t_p)I_p I_{\lambda/p} J_\lambda y_\lambda}{M} \\
&= \frac{(p+1-\mathrm{Tr}_p)I_{\lambda/p} J_\lambda y_\lambda}{M} \\
&= \frac{p+1}{M} I_{\lambda/p} J_\lambda y_\lambda - \frac{a_p}{M} P_{\lambda/p},
\end{aligned}$$

and for its reduction, in view of ...., we have the expression

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

□

5 The Orthoganality 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

$$0 \to E[M] \to E[M'] \xrightarrow{M} E[M''] \to 0$$

induces the exact sequence

$$E(R)[M'']/ME(R)[M'] \hookrightarrow H^1(R, E[M]) \xrightarrow{\alpha_{n,n'}} H^1(R, E[M']) \xrightarrow{\alpha_{n',n''}} H^1(R, E[M'']).$$

Suppose that for all integer n, n' with $n \le n'$ we have $E(R)[M''] = ME(R)[M']$. Then the maps $\alpha_{n,n'}$ are injections and the image of $\alpha_{n,n'}$ 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. (This is sneaky. Here $\alpha_{n'',n'} : H^1(R, E[M'']) \to H^1(R, E[M'])$ is defined because $n'' = n' - n \le n'$, and by hypothesis $\alpha_{n'',n'}$ is an injection.) 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 in which the hypothesis assumed at the beginning of this paragraph is satisfied. First, suppose that $R = K$. In this case, since $E(K)[\ell^\infty] = 0$, we identify $H^1(R, E[M])$ with $H[M]$, where

$$H := H^1(K, E[\ell^\infty]) = \varinjlim_{M'\to\infty} H^1(K, E[M']).$$

Note that $S_{\lambda,n}$ coincides with $S_{\lambda,n'}[M]$ under this identification. The second case is when $R = K(p)$ (completion of K at prime over p) and $n' \le n(p) = \mathrm{ord}_\ell(\gcd(a_p, p+1))$. Then $E(R)[M'] = E[M']$, hence, $ME(R)[M'] = E[M''] = E(R)[M'']$.

Let $n \leq n' \leq n(\lambda)$. It follows from (4.1) that

$$\tau_{\lambda,n} = \alpha_{n',n}\tau_{\lambda,n'}$$

or

$$\tau_{\lambda,n} = M''\tau_{\lambda,n''},$$

in view of the identifications. From (4.4) and Proposition 4.5, for p a prime with $p \nmid \lambda$ and $s \in S_{\lambda,n}$, we obtain the relations

$$\psi_{p,n'}(\tau_{\lambda,n'}) = \psi_{p,n}(\tau_{\lambda,n}) \pmod{M} \tag{5.1}$$

and

$$\psi_{p,n'}(s) = M''\psi_{p,n}(s) \pmod{M'}. \tag{5.2}$$

If A is a torsion $\mathbb{Z}_\ell$-module, then $e(A) = e_\ell(A)$ denotes the minimum nonnegative integer k such that $\ell^k A = 0$, so $e(A)$ is $\log_\ell$ of the exponent of A. If $a \in A$, then $e(a) = e_\ell(a) = e(\mathbb{Z}_\ell \cdot a)$, i.e., $\log_\ell$ of the order of a. For example, when $m(\lambda) < \infty$ then

$$m(\lambda) = n(\lambda) - e_\ell(P_\lambda \,(\mathrm{mod}\ \ell^{n(\lambda)}E(K_\lambda)).$$

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

$$\begin{aligned} e(\tau_{\lambda,n'}) &= e(P_\lambda(\mathrm{mod}\ \ell^{n'}E(K_\lambda))) && (5.3)\\ &= e(P_\lambda(\mathrm{mod}\ \ell^{n(\lambda)}E(K_\lambda))) \;-\; (n(\lambda) - n') && (5.4)\\ &= n' - m(\lambda). && (5.5) \end{aligned}$$

Suppose $n' \in [m(\lambda), n(\lambda)]$ and let $n \in [n' - m(\lambda),\, n']$, so

$$n' - m(\lambda) \leq n \leq n' \leq n(\lambda).$$

Let $p \mid \lambda \in \Lambda^r$. Then $\tau_{\lambda,n'} \in S^{\nu(r)}_{\lambda,n}$. From (4.5), in view of the equalities $M\tau_{\lambda,n'} = 0$ and $b^{\nu(r)}_{p,n} = M''b^{\nu(r)}_{p,n}$, it follows that $M'' \mid \psi_{p,n'}(\tau_{\lambda/p}, n')$ and

$$\tau_{\lambda,n'}(p) = \varepsilon(\psi_{p,n'}(\tau_{\lambda/p,n'})/M'')b^{\nu(r)}_{p,n}.$$

If $s \in S^{\nu(r)}_{\lambda,n}$, 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

$$\sum_{p|\lambda} \left(\psi_{p,n'}(\tau_{\lambda/p,n'})/M'' \right) \cdot \psi_{p,n}(s) \equiv 0 \pmod{M}. \tag{5.6}$$

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

Proposition 5.1. *Let A^0 and A^1 be finite subgroups of $H^0[M]$ and $H^1[M]$, respectively. For $i = 0$ or $i = 1$, let $\psi^i \in \mathrm{Hom}(A^i, \mathbb{Z}/M\mathbb{Z})$ and $n' \geq n$. Then there are infinitely many primes p such that $M' \mid M_p$ (i.e., $n' \leq n(p)$) and*

$$\mathbb{Z}/M\mathbb{Z} \left(\text{restriction of } \psi^i_{p,n} \text{ to } A^i\right) = (\mathbb{Z}/M\mathbb{Z})\psi^i.$$

Proof. We consider in detail the case where E does not have complex multiplication. The other case is handled analogously.

Let $E[M] = E[M]^0 \oplus E[M]^1$ 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 follows that $E[M]^i \approx \mathbb{Z}/M\mathbb{Z}$ for $i = 0, 1$ (cf. (4.3) and below). Let e^i be a generator of $E[M]^i$. Let $V = K(E[M'])$, where $M' = \ell^{n'}$. Note that $\mu_{M'} \subset V$ because of nondegeneracy of the Weil pairing.

Define the homomorphism

$$f : H[M] \to H^1(V, \mu_m) \cong \mathrm{Hom}(G_V^{\mathrm{ab}}, \mu_M)$$

as follows: for all $z \in G_V^{\mathrm{ab}}$ and $h = h^0 + h^1 \in H[M]$, we have

$$f(h) : \ z \mapsto [h^0(z), e^1]_M^2 \cdot [h^1(z), e^0]_M^2. \tag{5.7}$$

I have to check that this is well-defined and is a homomorphism, and I also have to figure out *what* this is! It might be res^V composed with cupping with two elements of $H^0(V, E[M])$, and ?

Suppose that f is an injection. Let W be the abelian extension of V corresponding to $f(A)$, where $A = A^0 \oplus A^1$. That is, W is the fixed field of

$$\ker f(A) = \bigcap_{\varphi \in f(A)} \ker \varphi \subset G_V^{\mathrm{ab}}.$$

By Kummer theory, the natural homomorphism

$$\mathrm{Gal}(W/V) \to \mathrm{Hom}(f(A), \mu_M)$$

is an isomorphism, hence, in view of the isomorphism $f : A \to f(A)$, we have the isomorphism

$$\mathrm{Gal}(W/V) \to \mathrm{Hom}(A, \mu_M).$$

Suppose that $\eta \in \mathrm{Gal}(W/V)$ 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 $\beta = \eta\sigma_1 \in \mathrm{Gal}(W/\mathbb{Q})$, where σ_1 is the restriction of complex conjugation to W. According to the Chebotarev density theorem, there exists infinitely many rational primes q which do not divide $N\ell$, are unramified in W, and such that

$$\beta = \mathrm{Fr} := \mathrm{Fr}_{W(w)/\mathbb{Q}_q}$$

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, $M' \mid (q+1)$, 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, $M' \mid a_q$. Therefore $M' \mid M_q$.

Let $g \in \mathrm{Gal}(V/\mathbb{Q})$ and let $\alpha(g) = 1$ if $g \in \mathrm{Gal}(V/K)$, and $\alpha(g) = -1$, otherwise. If $(-1)^{\nu-1}\varepsilon = 1$, then, by definition, σ acts trivially on $H[M]^\nu$, hence $h^\nu(z^g) = gh^\nu(z)$. If $(-1)^{\nu-1}\varepsilon = -1$, then σ acts on $H[M]^\nu$ by multiplication by -1, hence $h^\nu(z^g) = \alpha(g)gh^\nu(z)$. Using (4.3) as well, for $h^\nu \in A^\nu$, we have

$$[h^\nu(\mathrm{Fr}^2), e^{\nu'}]_M = [h^\nu(\eta), e^{\nu'}]_M^2 = \chi^\nu(h^\nu) = [e^0, e^1]_M^b,$$

where $b = \psi^\nu(h^\nu)$. Hence, considering (4.4), we see that $\psi_{q,n}^\nu$ is proportional to ψ^ν by a factor from $(\mathbb{Z}/M\mathbb{Z})^*$.

Now we shall prove that f is an injection. Let $h \in \ker(f)$. Then it follows from (5.7) that for all $z \in G_V^{\mathrm{ab}}$ we have

$$[h^0(z), e^1]_M = [h^1(z), e^0]_M^{-1}. \tag{5.8}$$

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

$$[h^0(z), ge^1]_M = [h^1(z), ge^0]_M^{-\alpha(g)}. \tag{5.9}$$

For $i = 0, 1$, let e^i be the generator of E^i such that $(M'/M)e_1^i = e^i$. Define the homomorphism $\varphi : \mathrm{Gal}(V/K) \to \mathrm{GL}_2(\mathbb{Z}/M'\mathbb{Z})$ so that $g(e_1^0, e_1^1) = \rho(g)(e_1^0, e_1^1)$. Since $\ell \in B(E)$, it follows that $\mathrm{Im}(\rho) = \mathrm{GL}_2(\mathbb{Z}/M'\mathbb{Z})$. Furthermore, the homorphism $\rho : \mathrm{Gal}(V/K) \to \mathrm{GL}_2(\mathbb{Z}/M'\mathbb{Z})$ 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 $\ell \equiv 3 \pmod 4$ and $K = \mathbb{Q}(\sqrt{-1})$, in which case $\rho(\mathrm{Gal}(V/K)) = \ker(\delta')$, where the homomorphism $\delta' : \mathrm{GL}_2(\mathbb{Z}/M'\mathbb{Z}) \to \{\pm 1\}$ is induced by $\det : \mathrm{GL}_2(\mathbb{Z}/M'\mathbb{Z}) \to (\mathbb{Z}/M'\mathbb{Z})^*$ and the unique nontrivial homomorphism $\delta : (\mathbb{Z}/M'\mathbb{Z})^* \to \{\pm 1\}$ (cf. [**?**, §4]).

Let $g_0 \in \mathrm{Gal}(V/K)$ be such that $\rho(g_0) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Substituting gg_0 for g in (5.9), we obtain the equality

$$[h^0(z), ge^0]_M = [h^1(z), ge^1]_M^{\alpha(g)}. \tag{5.10}$$

Let $K \subset \mathbb{Q}(E[M'])$. Then there exists an element $g_1 \in \mathrm{Gal}(V/\mathbb{Q}(E[M']))$ such that $\alpha(g_1) = -1$. The relations (5.9) and (5.10) for $g = 1$ and $g = g_1$, respectively, together imply that for $i = 0, 1$, $[h^0(z), e^i]_M = 1$ and $[h^1(z), e^i]_M = 1$, hence $h^0(z) = h^1(z) = 0$.

Suppose that $K \subset Q(E[M'])$. Then $K = \mathbb{Q}(\sqrt{-1})$, hence $\ell > 3$, since we are assuming that $K \neq \mathbb{Q}(\sqrt{-3})$. Since $\ell > 3$, there exists an element $a \in \mathbb{Z}/M'\mathbb{Z}$ such that $\delta(a) = 1$ but $a \not\equiv 1 \pmod{\ell}$. Let $g_2 \in \mathrm{Gal}(V/K)$ be such that $\rho(g_2) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right)$. Comparing (5.9) and (5.10) for $g = 1$ and $g = g_2$, respectively, we obtain $h^0(z) = h^1(z) = 0$.

Thus $\mathrm{res}_K^V(h) = 0$. It remains to show that

$$\mathrm{res}_K^V : H[M] \to H^1(V, E[M])$$

is an injection. Let $g_3 \in \mathrm{Gal}(V/K)$ 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 $\mathrm{Gal}(V/K)$. We have $E[M] = 0$ and $H^1(G_3, E[M]) = 0$. In view of inf-res-transgression applied to the group $\mathrm{Gal}(V/K)$ and its normal subgroup G_3, we see that $\ker(\mathrm{res}_K^V) = H^1(\mathrm{Gal}(V/K), E[M])$ is the trivial group. $\square$

We need the following corollary to Proposition 5.1.

Corollary 5.2. *Let A^0 and A^1 be finite subgroups of $H[M]^0$ and $H[M]^1$. For $i = 0, 1$ and $j = 1, 2$, let*

$$f_j^i : \mathrm{Hom}(A^i, \mathbb{Z}/M) \to C_j^i$$

be four surjective homomorphisms, and suppose that $n' \geq n$. Then there are infinitely many primes p such that $M' \mid M_p$ and

$$\# f_j^i \left(\text{restriction of } \psi_{p,n}^i \text{ to } A^i\right) = \# C_j^i.$$

Proof. By virtue of Proposition 5.1, it is enough to prove the existence of characters $\psi^i \in Hom(A^i, \mathbb{Z}/M\mathbb{Z})$ such that $e(f_j^i(\psi^i)) = e(C_j^i)$. There exists a character ψ^ν, since otherwise $\mathrm{Hom}(A^\nu, \mathbb{Z}/M\mathbb{Z})$ 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 $\delta = 1$, and denote the intersection of $S_{\lambda,n}$ with the kernels of the characters $\psi_{p,n}$ for all $p \mid \delta$ when $\delta > 1$. We have the following proposition.

Proposition 5.3. *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 order ℓ^{n-1}, it is sufficient to prove the equality

$$\# \left(\frac{S_{\lambda,\delta,n}^\nu}{S_{\lambda,\delta,n-1}^\nu} \right) \geq \ell^{r-k}. \tag{5.11}$$

Note that (5.11) implies that the multiplicity of n in the sequence of invariants of $S_{\lambda,\delta,n}^\nu$ is $\geq (r-k)/n$.

If v is a place of K, let $H_{v,n}$ denote $H^1(K(v), E[M])$ and $A_{v,n}$ denote $E(K(v))/ME(K(v))$. If β is a set of places of K, let $H_{\beta,n}$ denote the locally-compact group $\coprod_{v|\beta} H_{v,n}$. 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: $v \mid \beta$ signifies that $v \in \beta$ and $\beta_1\beta_2$ denotes the cup product $\beta_1 \cup \beta_2$. 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

$$\#Z_n = \sqrt{\#H_{\beta,n}} = M^{r-k}$$

and $\#Z_{n-1}^\nu = (M/\ell)^{r-k}$ (the latter equality holds since, in the previous equality, n is any natural number $\leq n(\lambda)$). Thus, $\#(Z_n^\nu/Z_{n-1}^\nu) = \ell^{r-k}$, whence follows (5.11).

Let α be the set of all places of K. By Poitou-Tate duality, the image Y_1 of the group $H[M]$ in $H_{\alpha,n}$ is an isotropic subgroup of $H_{\alpha,n}$. Let

$$Y_3 := \prod_{p|\delta} B_{p,n} \cdot \prod_{\gcd(v,\lambda)=1} A_{v,n}.$$

By local Tate duality $A_{v,n}$ is an isotropic subgroup of $H_{v,n}$, and $B_{p,n}$ is an isotropic subgroup of $H_{p,n}$, so Y_3 is an isotropic subgroup of $H_{\alpha/\beta,n}$.

Let $Y_2 = H_{\beta,n} \times Y_3$. We have $Z_n = \pi_\beta(Y_1 \cap Y_2)$. (I do not know for certain exactly what Kolyvagin means by π_β, and he doesn't bother to say.) 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 $\pi_\beta(z') = z$ and $\pi_{\alpha/\beta}(z') = 0$. Since z' is orthogonal to $Y_1 \cap Y_2$, by Pontrjagin theory, $z' = z_1 + z_2$, where $z_1 \in Y_1^\perp = Y_1$ and $z_2 \in Y_2^\perp$. We have $\pi_\beta(z_2) \in H_{\beta,n}^\perp = 0$ and $\pi_{\alpha/\beta}(z_2) \in Y_3^\perp = Y_3$. Hence $z' - z_2 = z_1 \in Y_1 \cap Y_2$ and $\pi_\beta(z' - z_2) = z$, so $z \in Z_n$. $\square$

We now have all that is necessary for the study of the group $X = Ш(E/K)[\ell^\infty]$.

6 A Structure Theorem for $Ш(E/K)[\ell^\infty]$

Let Λ_n^r denote the subset of Λ^r consisting of all elements λ such that $n(\lambda) \geq n$; then

$$\Lambda_n = \bigcup_{r\geq 0} \Lambda_n^r.$$

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 $\mathrm{Hom}(S_M^\nu, \mathbb{Z}/M\mathbb{Z})$ generated by $\varphi_{p,n}^\nu$ for all $p \mid \lambda$.

In the sequel, we shall assume that $n'' \geq n' \geq n$.

Proposition 6.1. *Let $\delta \in \Lambda^k_{n''}$, $n > m(\delta)$, $\delta q \in \Lambda^{k+1}_{n''}$, and $e(\Psi_{q,n}(\tau_{\delta,n})) = e(\tau_{\delta,n})$. Then $m(\delta q) \leq m(\delta)$. If, moreover, $n'' - n \geq m(\delta q)$ and $\iota = 1 - \nu(k)$, then*

$$e(\varphi^{\iota}_{q,n} \pmod{\psi^{\iota}_{\delta,n}}) \leq m(\delta) - m(\delta q).$$

Proof. By Proposition 4.5,

$$\tau_{\delta q,n}(q) = \varepsilon \psi_{q,n}(\tau_{\delta,n}) b^{\iota}_{q,n}.$$

Then, in view of (5.3) and our assumptions, we have

$$n - m(\delta q) = e(\tau_{\delta q,n}) \geq e(\psi_{q,n}(\tau_{\delta,n})) = e(\tau_{\delta,n}) = n - m(\delta).$$

Hence $m(\delta q) \leq m(\delta)$.

It is a consequence of (5.6) that $a\varphi^{\iota}_{q,n} \in \Phi^{\iota}_{\delta,n}$, where

$$a = \frac{\psi_{q,n'}(\tau_{\delta,n'})}{\ell^{m(\delta q)}} \in \mathbb{Z}/M\mathbb{Z}$$

and $n' = n + m(\delta q)$. Since

$$\mathrm{ord}_{\ell}(\psi_{q,n}(\tau_{\delta,n})) = n - e(\tau_{\delta,n}) = m(\delta)$$

and (5.1) holds, it follows that $\mathrm{ord}_{\ell}(a) = m(\delta) - m(\delta q)$. ∎

If $\delta \in \Lambda^k$, where $r \geq k$, let

$$m_r(\delta) = \min_{\lambda \in \Lambda^r,\, \delta | \lambda} m(\lambda).$$

Proposition 6.2. *If $\delta \in \Lambda^k$ is such that $m(\delta) < \infty$, then $m_{k+1}(\delta) \leq m(\delta)$.*

Proof. Let $n = n(\delta)$; then $n > m(\delta)$, since $m(\delta) < \infty$. Accoding to Corollary 5.2, there exists q such that $\delta q \in \Lambda^{k+1}_n$ and $e(\psi_{q,n}(\tau_{\delta,n}) = e(\tau_{\delta,n})$. The, by Proposition 6.1, we have the inequality $m(\delta q) \leq m(\delta)$. ∎

Recall that, for $r \geq 0$, m_r denotes $m_r(1)$.

Proposition 6.3. *The sequence $\{m_r\}$ is such that $m_r \geq m_{r+1}$.*

Proof. By assumption the point P_1 has infinite order. Hence $m_0 < \infty$, since m_0 is the exponent of the highest powe of ℓ dividing P_1 in $E(K)$. Now apply Proposition 6.2 and use induction on r. ∎

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

Proposition 6.4. *Let $k \geq 0$, $r \geq k$, $\alpha = \nu(k)$, $\beta = \nu(r)$, and $n'' \geq n' \geq n$. Let $\delta \in \Lambda^{k}_{n''}$ be such that $x := m_r(\delta) < n$ and $\lambda \in \Lambda^{r}_{n}$ such that $m(\lambda) = x$. Then there exists $q \in \Lambda^1$ satisfying the following conditions:*

1. *$\xi(q, \lambda) = 1$ and $M'' \mid M_q$;*
2. *$e(\psi^{\beta}_{q,n'}(\tau_{\lambda,n'})) = e(\tau_{\lambda,n'})$;*
3. *at our discretion, one of the following two conditions is fullfilled:*
   (a) *$e(\psi^{\alpha'}_{q,n'}(\mathrm{mod}\ \Phi^{\alpha'}_{\delta,n'})) = e(T^{\alpha'}_{\delta,n'})$;*
   (b) *if $k \geq 1$, then for a preassigned $p_1 \mid \delta$,*
   $$e(\varphi^{\alpha'}_{q,n'}(\tau_{\delta/p_1,n'})) = e(\tau_{\delta/p_1,n'});$$
4. *$e(\psi^{\alpha}_{q,n'}(\tau_{\delta,n'})) = e(\tau_{\delta,n'})$;*
5. *there exists $p \mid (\lambda/\delta)$ such that $m(\lambda q/p) = x$.*

Moreover, if $\alpha = \beta'$ and $n'' - n \geq y := m(\delta)$, then we may choose a p satisfying condition 5 so that the following condition is fulfilled:

6. *$e(\psi^{\alpha}_{p,n}(\tau_{\delta,n})) = e(\tau_{\delta,n})$.*

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

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

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

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

It follows from () and () that conditions (2) and (7) are satisfied as well after the substitution $n' \mapsto n$. Hence $e(z) = n - x > 0$. By the definition of x, we have

$$e(\psi^{\beta}_{p,n}(\tau_{\lambda q/p,n}) \leq e(\tau_{\lambda q/p,n}) \leq n - x.$$

Thus, there exists $p \mid (\lambda/\delta)$ such that the following conditions are fulfilled:

8. $e(\psi^{\beta}_{p,n}(\tau_{\lambda q/p,n}) = n - x$ and, hence, $m(\lambda q/p) = x$;
9. $e(\psi^{\beta'}_{p,n}(s) = n$.

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 (6) holds. Otherwise $e(\tau_{\delta,n}) = n - y > 0$, and (6) follows from (9), since $\tau_{\delta,n} = \ell^y \tau_{\delta,n+y}$. □

Proposition 6.5. *Let $n > m_0$ and $n' = n + m_0$. (It says "$m + m_0$" in [**?**], but m isn't defined anywhere.) Suppose that $r = k + 1 \geq 1$, $\delta \in \Lambda^k_{n'}$, and $m(\delta) = m_{r-1}$. Then there exists a prime number 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*

$$e(\varphi^{\beta}_{p_r,n} \,(\mathrm{mod}\ \Phi^{\beta}_{\delta,n})) = e(T^{\beta}_{\delta,n}) = m_{r-1} - m_r(\delta), \tag{6.1}$$

$$e(\psi_{p_r,n}(\tau_{\delta,n})) = e(\tau_{\delta,n}), \tag{6.2}$$

$$e(\phi^{\beta'}_{p_r,n} \,(\mathrm{mod}\ \Phi^{\beta'}_{\delta,n})) \geq m_{r-2} - m_{r-1}, \quad \textit{where } r \geq 2. \tag{6.3}$$

Proof. Let $\lambda \in \Lambda^r_{x+1}$, where $x = m(\delta)$, be such that $m(\lambda) = x$. The existence of p_r follows from Proposition 6.4 applied to δ and λ (and $n'' = n'$, $n' = n$, $n = x + 1$).

Now apply Proposition 6.4 to δ and $\lambda = \delta p_r$ (where $n'' = n'$ and $n' = n$). Select a q corresponding to condition (3a)). From conditions (2) and (3a), and Proposition 6.1, it follows that $e(T^{\beta}_{\delta,n}) \leq y - x$, where $y = m(\delta) = m_{r-1}$. The element $a = \tau_{\delta q,y}$ belongs to $S^{\beta}_{1,y} \subset S^{\beta}_{1,n}$, by virtue of Proposition 4.5 and the relation $\tau_{\delta',y'} = 0$ for all $\delta' \in \Lambda^{r-1}_y$ (by definition of $m_{r-1} = y$). Since $a = \ell^{n-y}\tau_{\delta,n}$, it then follows from (8) that

$$e(\varphi^{\beta}_{p_r,n}(a)) = e(\varphi^{\beta}_{p_r,n}(\tau_{\delta q,n})) - (n - y) = y - x.$$

Since $a \perp \Phi_{\delta,n}$, we have that

$$e(\varphi^{\beta}_{p_r,n} \,(\mathrm{mod}\ \Phi^{\beta}_{\delta,n})) \geq y - x,$$

hence (6.1) is true.

Analogously, the element $b = \tau_{\delta,m_{r-2}}$ lies in $S^{\beta'}_{1,n}$ and $b \perp \Phi^{\beta'}_{\delta,n}$. According to (6), (6.2) is true, hence $e(\varphi^{\beta'}_{p_r,n}(b) = m_{r-2} - y$, and (6.3) holds. □

If ω is a sequence $(p_0, \dots, p_r)$ of integers, for $0 \le i \le r$ let $\omega(i) = p_0 \cdots p_i$. [Note, this is not how Kolyvagin defines $\omega(i)$, but his definition doesn't make any sense.] Define Ω_n^r to be the set of sequences $\omega = (p_0, \dots, p_r)$ 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 $(p_0) := (1)$.

A priori, by the Mordell-Weil theorem, and because $E(K)[\ell^\infty]$ is trivial, $(E(K)/ME(K))^\nu \cong (\mathbb{Z}/M\mathbb{Z})^{g^\nu}$, where $g^0 + g^1$ is the rank of E over K. The sequence

$$0 \to E(K)/ME(K) \to H^1(K, E[M]) \to H^1(K, E)[M] \to 0.$$

induces the exact sequence

$$0 \to (E(K)/ME(K))^\nu \to S_{1,n}^\nu \to X_{1,n}^\nu \to 0. \tag{6.4}$$

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 $P_1 = \ell^{m_0}\mathbf{x}$ where $\mathbf{x} \in E(K) - \ell E(K)$ (set-theoretic difference).

Let $n > m_0$, $r = 1$, $\omega = p_0 = 1$, and choose p_1 as in Proposition 6.5. Then $T_{\delta,n}^0 = \mathrm{Hom}(S_{1,n}^0, \mathbb{Z}/M\mathbb{Z})$ and $m_1(\delta) = m_1$. According to (6.1), we have

$$e(S_{1,n}^0) = e(T_{\delta,n}^0) = m_0 - m_1 < n.$$

Hence, in view of (6.4), it follows that $g^0 = 0$, $S_{1,n}^0 = S_{1,m_0-m_1}^0$, and $X^0 = X_{1,n}^0 = X_{1,m_0-m_1}^0$ is a finite group. In particular, the invariants x_i^0 of X^0 coincide with the invariants of $T_{1,n}^0$.

Moreover, it follows from (6.2) that

$$e(\varphi_{p_1,n}^1(\mathbf{x} \pmod{ME(K)})) = n,$$

hence, $S_{1,n}^1$ is the direct sum of $\mathbb{Z}/M\mathbf{x}\mathbb{Z} \pmod{ME(K)} = \mathbb{Z}/M\mathbb{Z}$ and $Y = \ker \varphi_{p_1,n}^1$.

Let $r = 2$, $\omega = (1, p_1)$, and $\delta = p_1$. Then $T_{\delta,n}^1$ is the dual group for Y. Hence, it follows from 6.1 that

$$e(Y) = e(T_{\delta,n}^1) = m_1 - m_2(\delta)$$

and by (6.4), we have $g^1 = 1$ and $X^1 = X_{1,n}^1 = X_{1,m_1-m_2}^1(\delta)$ is finite and isomorphic to Y. In particular, the invariants x_i^1 of the group X^1 coincide with the invariants of the group $T_{p_1,n}^1$.

In [**?**] it was proved that $g^0 = 0$, and in [**?**] that $g^1 = 1$ and $\#X \mid \ell^{2m_0}$.

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 $\xi(j, \nu) = j - |\nu - \nu(j)|$.

Theorem 6.6. *Let $r > 0$, $n > m_0$, and $n' = n + m_0$. Then $\Omega^r_{n'} \neq \emptyset$. Moreover, for all $\omega \in \Omega^{r-1}_{n'}$, there exists $p_r \mid \xi(\omega, p_r) \in \Omega^r_{n'}$. Let $\omega \in \Omega^r_{n'}$. Then for $1 \leq j \leq r$,*

$$e\left(\varphi_{p,n}\left(\tau_{\omega(j-1),n}\right)\right) = e(\tau_{\omega(j-1),n'}),$$

and if $\nu \in \{0, 1\}$ is such that $r - \nu > 0$, then for $1 + \nu \leq j \leq r$ we have

$$e\left(\phi^{\nu}_{p_j,n} \left(\operatorname{mod} \Phi^{\nu}_{\omega(j-1),n}\right)\right) = m_{\xi(j,\nu)-1} - m_{\xi(j,\nu)} = x^{\nu}_{j-\nu}.$$

Proof. For $r = 1$ the theorem was proved above. Therefore, by induction, it suffices to prove the theorem for $r \geq 2$, assume it is true for all $r' < r$. Let $\omega \in \Omega^{r-1}_{n'}$, $\delta = \omega(r-1)$, and choose p_r as in Proposition 6.5 so that, in particular, the relations (6.1)–(6.3) hold. Since the theorem is true for $r - 1$, it follows that $e(T^{\nu}_{\delta,n}) = x^{\nu}_{r-\nu}$, 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 (6.3) and the inequality $x^{\beta'}_{r-\beta'} \leq x^{\beta'}_{r-1-\beta'}$. In view of (6.1), (6.2), and the induction hypothesis, it remains only to prove that $m_r(\delta) = m_r$. This will be done if we prove that $\Omega^r_{n'} \neq \emptyset$. Indeed, using the fact that $\xi(\omega', p') \in \Omega^r_{n'}$, 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 $0 \leq k \leq r$, let U^k be the set of pairs $\omega \in \Omega^k_{n'}$, $\lambda \in \Lambda^r_u$ such that $\omega(k) \mid \lambda$ and $m(\lambda) = m_r$. It follows from Proposition 6.5 that $\Omega^r_{n'}$ 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 $\xi(\omega, \lambda) \in U^k$. Apply Proposition 6.4 to $\delta = \omega(k)$, λ (and $n'' = n'$, $n = u$), and choose a q corresponding to condition (3a). 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 6.6 for $k + 1 \leq r - 1$, we have

$$m_k - m_{k+1} = x^{\alpha'}_{k+1-\alpha'} = e(T^{\alpha'}_{\delta,n}),$$

where $\alpha = \nu(k)$. On the other hand, in view of Proposition 6.1 and condition (3a), we see that $e(T_{\delta,n}) \leq m_k - m(\delta q)$. Hence $m(\delta q) \leq m_{k+1}$, but, by the definition of m_{k+1}, we have $m_{k+1} \leq m(\delta q)$. Thus $m(\delta q) = m_{k+1}$. $\square$

7 Parametrization of $\text{Ш}(E/K)[\ell^\infty]$

The purpose of this section 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 $\varphi_{p,n}$.

Let n' be a nonnegative integer (I think). For $r \geq 0$ let $\Pi^r_{n'}$ be the set of sequence $\pi = (p_0, \ldots, p_r)$ such that $\pi(r) \in \Lambda^r_{n'}$; if $r > 0$ and $1 \leq j \leq r$, then

$$e(\Psi_{p_j,n'}(\tau_{\pi(j-1),n'})) = e(\tau_{\pi(j-1),n'}) \tag{7.1}$$

and, if $r \geq 2$ and $2 \leq j \leq r$, moreover,

$$e(\Psi_{p_j,n'}(\tau_{\pi(j-1)/p_1,n'}) = e(\tau_{\pi(j-1)/p_1,n'}). \tag{7.2}$$

Recall that

$$m = \min_{r\geq 0} m_r = \lim_{r\to\infty} m_r.$$

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 6.4, condition (3b), and induction, we shall prove that for all n' there exists $\pi \in \Pi^r_{n'}$ such that $m(\pi(r)) = m$. We shall say that $\pi \in \Pi^r_{n'}$ is *minimal* if $m(\pi(r)) = m$. From Proposition 6.1 and 6.4 it follows that if $\pi' \in \Pi^{r-1}_{n'}$ is minimal, then there exists p_r such that $(\pi', p_r) \in \Pi^r_{n'}$ is minimal.

Let $n > m_0$ and $n' \geq n + m_0$. Assume that $r \geq 2$, that $\pi \in \Pi^r_{n'}$ is minimal, and $\pi - p_r$ is minimal as well.

Definition 7.1 $(u(\nu))$**.** 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 $\nu = \nu(r)$), $u(v) = r - \nu - 1$.

Let $\lambda^\nu = \pi(u(\nu) + \nu)$. By Proposition 6.5, $T^\nu_{\lambda^\nu,n} = 0$, that is, $\varphi^\nu_{p_j,n}$, $1 \leq j \leq u(\nu) + \nu$, generate $\mathrm{Hom}(S^\nu_M, \mathbb{Z}/M\mathbb{Z})$. In particular, the homomorphism α^ν_2 in (**??**) below is an isomorphism. For $1 - \nu \leq i \leq u(\nu)$, set

$$\lambda^\nu_i = \pi(i + \nu)/p_{\nu(i)}$$

and

$$z^\nu_i = \tau_{\lambda^\nu_i, n+m(\lambda^\nu_i)} \in S_{\lambda^\nu_i,n}.$$

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

$$a^{\nu}_{ij} = 0, \tag{7.3}$$

and for the remaining pairs ij:

$$a^{\nu}_{ij} = \psi_{p_{j+\nu}, n+m(\lambda^{\nu}_i)} \left(\tau_{\lambda^{\nu}_i / p_{j+\nu}, n+m(\lambda^{\nu}_i)}\right) / \ell^{m(\lambda^{\nu}_i)}. \tag{7.4}$$

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

$$\sum_{j=1-\nu}^{u(\nu)} a_{ij} \varphi_{p_{j+\nu}, n} = 0. \tag{7.5}$$

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

Let $r \geq 2+\nu$, $a^{\nu} = \{a^{\nu}_{ij}\}$ for $1 \leq i, j \leq u(\nu)$, and $A^{\nu} = A(a^{\nu})$. Sending 1_j to $\varphi^{\nu}_{p_{j+\nu}, n} (\mathrm{mod}\ \varphi^{\nu}_{p_{\nu}, n})$ and taking (7.5) into account, we define the surjective homomorphisms α^{ν}_i in () below. We have the isomorphisms

$$\begin{tikzcd} A^{\nu} \arrow[r, "\alpha^{\nu}_1", "\cong"'] & \Phi^{\nu}_{\lambda^{\nu}, n}/(\varphi^{\nu}_{p_{\nu}, n}) \arrow[r, "\alpha^{\nu}_2", "\cong"'] & \mathrm{Hom}(S^{\nu}_M, \mathbb{Z}/M\mathbb{Z})/(\varphi^{\nu}_{p_{\nu}, n}) \\ X^{\nu} \arrow[rr, "\alpha^{\nu}_4", "\cong"'] & & \mathrm{Hom}(X^{\nu}, \mathbb{Z}/M\mathbb{Z}). \arrow[u, "\alpha^{\nu}_3"'] \end{tikzcd} \tag{7.6}$$

Here $\varphi^{0}_{p_0, n} := 1$ and $(\varphi^{\nu}_{p_{\nu}, n})$ is the subgroup generated by $\varphi^{\nu}_{p_{\nu}, n}$. We proved above that the natural injection α^{ν}_2 is an isomorphism. The isomorphism α^{ν}_3 is induced by the exact sequence (?), and α^{ν}_4 is any isomorphism between X^{ν} and its dual group. We shall prove below that α^{ν}_1 is an isomorphism as well.

If $b \in \mathbb{Z}/M\mathbb{Z}$, then $\mathrm{ord}_{\ell}(b) := n - e(b)$. Using Proposition **??**, (?), and (?), we obtain the relation

$$\mathrm{ord}_{\ell}(a^{\nu}_{ii}) = m(\lambda^{\nu}_i / p_{i+\nu}) - m(\lambda^{\nu}_i) \leq m_0 < n. \tag{7.7}$$

Since $a_{ij} = 0$ if $j > i$, it then follows that

$$\mathrm{ord}_\ell(A^\nu) \leq z^\nu := \sum_{i=1}^{u(\nu)} \mathrm{ord}_\ell(a_{ii}^\nu).$$

Equation (7.7) 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

$$\mathrm{ord}_\ell([A^0][A^1]) \leq z^0 + z^1 = 2m_0 - 2m. \tag{7.8}$$

Let $\lambda = \pi(r)$. Since $\tau_{\lambda,n+m}$ and $s = \tau_{\lambda/(p_1 p_r),n+m}$ are orthogonal, considered as elements of $S_{\lambda,n}$ (cf. (?)), then if

$$\theta_1 = \psi_{p_1,n+m}\left(\tau_{\lambda/p_1,n+m}\right)/\ell^m,$$

it follows that

$$\theta_1 \psi_{p_1,n}(s) = \theta_2 := -(\varphi_{p_r,n+m}(\tau_{\lambda/p_r,n+m})/\ell^m)\psi_{p_r,n}(s).$$

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

Since $\mathrm{ord}_\ell([X^0][X^1]) = 2m_0 - 2m$ (cf. **??**) and **??** 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 $1 \leq j \leq i$, because then, by Proposition **??**, $z_i^\nu(p_{j+\nu}) \in B^\nu_{p_{j+\nu},n}$ and $\psi_{p,n}(B_{p,n}) = 0$ (cf. Section **??**). We see from **??** and **??** that, if $u(\nu) \geq 2$ and $i < u(\nu)$, then $\varphi_{p_{i+1+\nu}}(z_i^\nu) \in (\mathbb{Z}/M\mathbb{Z})^*$. According to (**??**),

$$e(z_i^\nu) = n + m(\lambda_i^\nu) - m(\lambda_i^\nu) = n.$$

We shall show that if $(c_1, \ldots, c_{u(\nu)}) \in (\mathbb{Z}/M\mathbb{Z})^{u(\nu)}$ is such that

$$\sum_{i=1}^{u(\nu)} c_i z_i^\nu = 0, \tag{7.9}$$

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 (7.9). By the properties of z^ν noted above, we obtain $c_1 = \cdots = c_{u(\nu)-1} = 0$ and, hence, $c_{u(\nu)} = 0$ as well.

Then, from the definition of z_i^ν and Proposition **??**, it follows that

$$z_i^\nu(p_{j+\nu}) = a_{ij}^\nu b_{j+\nu,n}^\nu \pmod{E(K(p_{j+\nu}))/M}.$$

Thus

$$w = \sum_{i=1}^{u(\nu)} c_i z_i^\nu \in S_{p_\nu,n}^\nu$$

and the following relation holds for $1 \le j \le u(\nu)$:

$$\sum_{i=1}^{u(\nu)} c_i a_{ij}^\nu = 0. \tag{7.10}$$

Note that the orthogonality between elements of $S_{p_1,n}^1$ and $\mathbf{x} \pmod{ME(K)}$, in view of the fact that

$$\varphi_{p_1,n}(\mathbf{x} \pmod{ME(K)} \in (\mathbb{Z}/M\mathbb{Z})^*$$

and (**??**), implies that $S_{p_1,n}^1 = S_M^1$. Therefore, (**??**) is the condition that w belongs to the group S_M^ν. Let $B^\nu = \{c_1, \ldots, c_{u(v)}\}$ be the subgroup of $(\mathbb{Z}/M\mathbb{Z})^{u(\nu)}$ defined by (7.10). If a is a matrix, then a^{tr} denotes the transpose of the matrix a.

The pairing

$$(\mathbb{Z}/M\mathbb{Z})^{u(\nu)} \times (\mathbb{Z}/M\mathbb{Z})^{u(\nu)} \to \mathbb{Z}/M\mathbb{Z},$$

under which $(1_j, 1_j) = \delta_{ij}$ (the Kronecker symbol), induces the isomorphism β_2^ν in (**??**). The isomorphism β_1^ν is any isomorphism of the dual groups. The β_3^ν is an injection $(c_1, \ldots, c_{u(\nu)}) \mapsto w$. The isomorphism β_4^ν is induced by the homomorphism $S_M^\nu \to X^\nu$ in (**??**). We have

$$A(a^{\nu\,\mathrm{tr}}) \xrightarrow[\cong]{\beta_1^\nu} \mathrm{Hom}(A(a^{\nu\,\mathrm{tr}}), \mathbb{Z}/M\mathbb{Z}) \xrightarrow[\cong]{\beta_2^\nu} B^\nu \xrightarrow[\cong]{\beta_3^\nu} \ker(\psi_{p_{2\nu}}^\nu) \xrightarrow[\cong]{\beta_4^\nu} X^\nu. \tag{7.11}$$

We shall show that, for $n > 2m_0$, β_3^ν is also an isomorphism. Let a be a $u \times u$ matrix over $\mathbb{Z}/M\mathbb{Z}$ such that $a_{ij} = 0$ for $j > i$ and

$$\xi = \sum_{i=1}^{u} \mathrm{ord}_\ell(a_{ii}) \le n.$$

Using induction on u and our assumption, we see that $\mathrm{ord}_\ell(A(a)) = \xi$.

In particular, if $n > 2m$ and $a = a^{\nu\,\mathrm{tr}}$, then $\xi \le n$, by virtue of (?), and hence, $\mathrm{ord}_{\ell_0}(B^\nu) = \xi = z^\nu$. Thus, since $\mathrm{ord}_\ell([X^0][X^1]) = z^0 + z^1 = 2m_0 - 2m$, 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 $\ell^{m_0}X^\nu = 0$, for $n = m_0$ and $n' > 2m_0$, we have the isomorphism 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 the Birch and Swinnerton-Dyer conjecture for 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 (?), 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 $a_{ij}^\nu \in \mathbb{Z}/M_0\mathbb{Z}$, where $M_0 \in \ell^{m_0}$. Then for $n = m_0$, we obtain the isomorphism (?), in particular, the isomorphism $A^\nu \cong X^\nu$ and the parametrization of the dual group of X^ν by the characters ψ_{p,m_0}^ν for $p \mid (\lambda^\nu/p)$. If $\theta = 3$, then we also obtain the isomorphisms in (?), 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

$$\psi_{p_r,m+1}(\tau_{\lambda/p,m+1}) = 0. \tag{7.12}$$

It follows from (7.12) that $m(\lambda/p) = m$ and, in view of Proposition 6.1, that $m(\lambda) = m$. If $r = 1$, then (7.12) implies that $m_0 = m$, hence $X = 0$, since $\#X = \ell^{2m-2m_0}$, and we complete the calculations. If $r > 1$, then we verify the conditions

$$\frac{n'-1}{\theta} \ge m_0' := \min_{1 \le j \le u(1)+1} \mathrm{ord}_\ell(\psi_{p_j,n}(\tau_{1,n'})) \tag{7.13}$$

and

$$\psi_{p_2,m_0'+1}(\tau_{1,m_0+1}) \ne 0. \tag{7.14}$$

It follows from (7.13) that $m_0 = m_0'$. If $r > 2$, then we verify the condition

$$\psi_{p_1,m_0+1}(\tau_{1,m_0+1}) \neq 0. \tag{7.15}$$

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

$$m(\lambda_i^\nu) = \min_{j=\nu(i)-\nu, i<j\leq u(\nu)} \operatorname{ord}_\ell \psi_{p_{j+\nu},m_0+1}(\tau_{\lambda_i^\nu,m_0+1}). \tag{7.16}$$

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

$$\psi_{p_{i+\nu+1},m(\lambda_i^\nu)+1}\left(\tau_{\lambda_i^\nu,m(\lambda_i^\nu)+1}\right) \neq 0. \tag{7.17}$$

The conditions (7.12), (7.14), and (7.13) if $r = 2$, or (7.15) and (7.17) if $r > 2$, are equivalent to the conditions (7.1) and (7.2); thus, we require a triple n', r, π for which (7.12) and (7.13) hold, and, if $r = 2$, (7.15) and (7.17) hold as well (for the case $r = 1$, see above).

The coefficients of a^ν for $r - \nu \geq 2$ are calculated using (7.3) and (7.4).

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 $\operatorname{ord}_\ell(a_{11}^0) = m_0 - m(p_1)$. In view of Theorem ? and (?), we obtain that $m_1 = m(p_1)$ and $\operatorname{ord}_\ell(a_{22}^0) = m_0 - m(p_1)$. Then (?), as well as (?), holds already (if $n = m_0$) for $\theta = 2$. In particular, $X^0 \cong S_{M_0}^0 \cong (\mathbb{Z}/\ell^{m_0-m_1})^2$; 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 $\operatorname{Hom}(S_{M_0}^0, \mathbb{Z}/M_0\mathbb{Z})$. If $r = 2$, then $m_1 = m(p_1) = m$; if $r = 3$, then $p_1 = \lambda_1^0$ and, according to (7.16),

$$m_1 = \operatorname{ord}_\ell(\psi_{p_2,m_0+1}(\tau_{p_1,m_0+1})).$$

If $r = 2$, then

$$e(X^1) = m_1 - m_2 = m - m = 0,$$

so $X^1 = 0$. Suppose that $r = 3$. Then

$$Y = \ker(\varphi_{p_1,m_0}) \cong X^1 \cong (\mathbb{Z}/\ell^{m(p_1)-m})^2,$$

and φ_{p_2,m_0}^1 and φ_{p_3,m_0}^1, restricted to Y, form a basis of $\operatorname{Hom}(Y, \mathbb{Z}/M_0\mathbb{Z})$.

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

Recall (cf. Theorem ?) that the ℓ-component of the Birch and Swinnerton-Dyer conjecture 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 procedure 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 order 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
- for all $\ell \mid M$ and $p \in \Lambda^1$ we can calculate the value $z(p) \in E(K(p))/ME(K(p))$.

Adding to z, if necessary, the element $T\left(\sum_{\ell \mid M} \ell^{-m_0}\right) P_1 \pmod{ME(K)}$, with the corresponding $T \subset \mathbb{N}$, we may assume that for all $\ell \mid M$ we have

$$z(p_1)^1 \equiv 0 \pmod{\ell^{m_0 - m}}.$$

Then we have the following effective criterion (necessary and sufficient) for the curve C to have a point over K (with m, m_0, and λ, of course, corresponding to ℓ):

$$\text{for all } \ell \mid M, \text{ for all } p \mid \lambda,\ z(p) \equiv 0 \pmod{\ell^{m_0 - m} E(K(p))}. \tag{7.18}$$

If the curve C is defined over $\mathbb{Q}$ and has a point over $\mathbb{Q}(v)$ for all places of $\mathbb{Q}$, then the effective criterion for C to have a point over $\mathbb{Q}$ is the criterion (7.18) with $z(p)^\nu$ in place of $z(p)$, where $(1)^{\nu-1}\varepsilon = 1$.