TORSION POINTS ON ELLIPTIC CURVES AND GALOIS MODULE STRUCTURE

A. Agboola

Version of June 17, 1995

§0. Introduction and statement of results. In this paper we shall study the Galois module structure of certain Kummer orders obtained by dividing torsion points on an elliptic curve.

Let E be an elliptic curve defined over a number field F. We suppose that all endomorphisms of E are defined over F, and that E/F has everywhere good reduction. For any field L, we write O_L for its ring of integers and L^c for an algebraic closure of L; we set $\Omega_L = Gal(L^c/L)$.

Let $p > 3$ be a rational prime, and write G_i for the subgroup of elements of $E(F^c)$ which are killed by the endomorphism $[p^i]$ of E. Let $\mathfrak{B}_i(F) = \mathfrak{B}_i$ denote the O_F-Hopf algebra which represents the O_F-group scheme of $[p^i]$-torsion on E, and let $\mathfrak{A}_i(F) = \mathfrak{A}_i$ be the Cartier dual of $\mathfrak{B}_i$. A detailed description of these algebras is given in [T] (see also [ST]). There it is shown that $\mathfrak{B}_i$ is an O_F-order in the algebra $B_i(F) = B_i = Map(G_i, F^c)^{\Omega_F}$, and $\mathfrak{A}_i$ is an O_F order in the algebra $A_i(F) = A_i = (F^c G_i)^{\Omega_F}$ (where here Ω_F acts upon both G_i and F^c). (Here and elsewhere we shall omit from our notation the dependence of our constructions on the underlying field F unless there is some danger of ambiguity.)

Partially supported by an NSF Postdoctoral Research Fellowship.

Suppose that $Q \in E(F)$, and write

$$G_Q(i) = \{Q' \in E(F^c) : [p^i]Q' = Q\} \tag{0.1}$$

Define the Kummer algebra $F_Q(i)$ by

$$F_Q(i) = Map(G_Q(i), F^c)^{\Omega_F} \tag{0.2}$$

Then $[F_Q(i) : F] = |G_i|$, and A_i acts on $F_Q(i)$ via

$$(f. \sum_{g \in G_i} a_g g)(Q') = \sum_{g \in G_i} a_g f(Q' + g) \tag{0.3}$$

for $f \in F_Q(i)$ and $\sum_{g \in G_i} a_g g \in A_i$.

Let $O_Q(i)$ denote the integral closure of O_F in $F_Q(i)$. In general $O_Q(i)$ does not admit an action of $\mathfrak{A}_i$. We define the Kummer order $\mathfrak{C}_Q(i)$ to be the maximal $\mathfrak{A}_i$-stable submodule of $O_Q(i)$, i.e.

$$\mathfrak{C}_Q(i) = \{x \in O_Q(i) | x.\mathfrak{A}_i \subseteq O_Q(i)\} \tag{0.4}$$

It is shown in [T] that $\mathfrak{C}_Q(i)$ is a twisted form of $\mathfrak{B}_i$, and that $\mathfrak{C}_Q(i)$ is a locally free $\mathfrak{A}_i$-module. Thus $\mathfrak{C}_Q(i)$ defines an element $(\mathfrak{C}_Q(i))$ in the locally free classgroup $Cl(\mathfrak{A}_i)$ of $\mathfrak{A}_i$. Hence we obtain a map

$$\psi_i : E(F) \longrightarrow Cl(\mathfrak{A}_i) \tag{0.5}$$

given by $\psi_i(Q) = (\mathfrak{C}_Q(i))$. Since E/F has everywhere good reduction, the map ψ_i is a group homomorphism (see Theorem 1 of [T]), and $\psi_i(Q) = 0$ if and only if $\mathfrak{C}_Q(i)$ is a globally free $\mathfrak{A}_i$-module. (We remark that in [T] it is assumed that E has complex multiplication. This assumption is not necessary for setting up the basic theory. See [BT] and [A1].) For an interesting geometric description of the homomorphism ψ_i in terms of line bundles on E and the connection with a Galois-module theoretic analogue of a now classical conjecture of Tate, we refer the reader to [A1].

The following result is a special case of Theorem 1 of [ST].

Theorem (Srivastav-Taylor). *Suppose that E is a CM elliptic curve. Then $E(F)_{torsion} \subseteq ker(\psi_i)$.*

This theorem gives information regarding the Galois module structure of rings of integers of certain abelian extensions of F. It may therefore be regarded as yielding an integral version of the Krönecker Jugendtraum.

The purpose of this paper is to prove the following result.

Theorem 1. *Suppose that E is an elliptic curve. Then $E(F)_{torsion} \subseteq ker(\psi_i)$.*

The proof of Theorem 1 depends upon the use of elementary intersection theory to prove integrality results concerning certain resolvent elements that arise as special functions on E. Our methods differ from those of previous authors (see e.g. [ST], [CNS], [CNT]) in that we avoid the use of modular functions and the q-expansion principle in obtaining such integrality statements. We remark that the techniques introduced in this paper may also be used to prove an analogue of Theorem 1 in the function field case, and we refer the reader to [A2] for further details. Finally, we mention that the situation in which $p \leq 3$ has been studied by several authors in the case of CM elliptic curves (see [CNS] and the references quoted therein). It seems almost certain that the intersection theoretic methods of this paper may also be used to obtain partial results similar to those contained in [CNS], although we have not carried out this project.

I would like to express my warmest thanks to Martin Taylor for his helpful comments on an earlier version of this paper. I am also extremely grateful to the referee for his very careful reading of the manuscript and for his many suggestions which have led to improvements in the exposition.

§**1. Preliminary results.** In this section we recall certain results from [T], [BT], [Sh] and [ST] that we shall require.

We begin by describing the relationship between $(\mathfrak{C}_Q(i)) \in Cl(\mathfrak{A}_i)$ and $(\mathfrak{C}_Q(j)) \in Cl(\mathfrak{A}_j)$ for $0 < j < i$, using the methods of §2 of [ST].

The natural surjection $[p^{i-j}] : G_i \to G_j$ induces a surjective homomorphism $A_i \to A_j$ of Hopf algebras (which we shall also denote by $[p^{i-j}]$) given by

$$[p^{i-j}](\sum_{g \in G_i} \alpha_g g) = \sum_{g \in G_i} \alpha_g([p^{i-j}]g). \tag{1.1}$$

Similarly, the inclusion $G_j \to G_i$ induces an inclusion $A_j \to A_i$ of Hopf algebras. Since these maps are induced by homomorphisms of group schemes, we can pass to the integral level and deduce that $\mathfrak{A}_j$ may be viewed as either a quotient algebra or a subalgebra of $\mathfrak{A}_i$.

Next, we observe that G_i acts on $Map(G_i, F^c)$ via translations, i.e.

$$f^g(h) = f(g+h) \quad \forall f \in Map(G_i, F^c), g, h \in G_i. \tag{1.2}$$

The isomorphism $G_i/G_j \simeq G_{i-j}$ induces identifications

$$F^c G_{i-j} = (F^c G_i)^{G_j} \tag{1.3}$$

and

$$Map(G_{i-j}, F^c) = Map(G_i, F^c)^{G_j}. \tag{1.4}$$

The identifications (1.3) and (1.4) in turn induce isomorphisms of $\mathfrak{A}_{i-j}$ with a subalgebra of $\mathfrak{A}_i$ and $\mathfrak{B}_{i-j}$ with a subalgebra of $\mathfrak{B}_i$.

Proposition 1.1. *There are isomorphisms*

$$F_Q(j) \simeq \Sigma_{i-j}.F_Q(i) \tag{1.5}$$

as A_j-modules, and

$$\mathfrak{C}_Q(j) \simeq \frac{\Sigma_{i-j}}{p^{i-j}}.\mathfrak{C}_Q(i) \tag{1.6}$$

as $\mathfrak{A}_j$-modules. These isomorphisms are compatible with the inclusions $\mathfrak{C}_Q(j) \hookrightarrow F_Q(j)$ and $\mathfrak{C}_Q(i) \hookrightarrow F_Q(i)$.

Here $\Sigma_{i-j} = \Sigma_{g \in G_{i-j}} g$ viewed as an element of A_i, and A_j (resp. $\mathfrak{A}_j$) acts on the right hand side of (1.5) (resp. (1.6)) via the homomorphism $[p^{i-j}]$.

Proof. See §2 of [ST], especially Proposition 1. (It is assumed in [ST] that E has complex multiplication, but this assumption is not necessary for this particular result.) $\square$

The following result is an immediate consequence of Proposition 1.1.

Proposition 1.2. *Suppose that $\mathfrak{C}_Q(i)$ is a globally free $\mathfrak{A}_i$-module. Then $\mathfrak{C}_Q(j)$ is $\mathfrak{A}_j$-globally free for all $0 < j < i$.* $\square$

Proposition 1.2 implies that, in order to prove Theorem 1, we may replace p^i by a higher power of p. Let l and l' be distinct odd primes not equal to p. Then, by replacing p^i by a higher power of p if necessary, we shall henceforth assume that

$$p^i \equiv 1 \quad mod(ll'). \tag{1.7}$$

We next observe that it follows from the definition of $\mathfrak{C}_Q(i)$ that $\psi_i(Q)$ in fact depends only upon the image of Q in $E(F)/p^iE(F)$. Hence, in order to prove

Theorem 1, we may assume that $Q \in E(F)$ is a p-power torsion point. We shall make this assumption from now on. Observe that, with this assumption, we have

$$p^i.(\mathfrak{C}_Q(i)) = 0 \tag{1.8}$$

in $Cl(\mathfrak{A}_i)$.

We shall now describe certain results concerning the algebras $\mathfrak{A}_i$ and $\mathfrak{B}_i$.

For each prime $\mathfrak{q}$ of O_F, let $G_{i,\mathfrak{q}}$ denote the $O_{F_\mathfrak{q}}$-group scheme obtained by localising and completing the O_F-group scheme afforded by G_i at $\mathfrak{q}$. Then there is an exact sequence

$$0 \longrightarrow G^0_{i,\mathfrak{q}} \longrightarrow G_{i,\mathfrak{q}} \longrightarrow G'_{i,\mathfrak{q}} \longrightarrow 0 \tag{1.9}$$

of $O_{F,\mathfrak{q}}$-group schemes, where $G^0_{i,\mathfrak{q}}$ is the connected component of the identity of $G_{i,\mathfrak{q}}$, and $G'_{i,\mathfrak{q}}$ is the maximal étale quotient $G_{i,\mathfrak{q}}/G^0_{i,\mathfrak{q}}$. The group scheme $G'_{i,\mathfrak{q}}$ is represented by the algebra $\mathfrak{B}'_{i,\mathfrak{q}} := Map(G'_{i,\mathfrak{q}}(F^c_\mathfrak{q}), O_{F^c_\mathfrak{q}})^{\Omega_{F_\mathfrak{q}}}$; we remark that $\mathfrak{B}'_{i,\mathfrak{q}}$ is the unique maximal order in the algebra $B'_{i,\mathfrak{q}} := Map(G'_{i,\mathfrak{q}}(F^c_\mathfrak{q}), F^c_\mathfrak{q})^{\Omega_{F_\mathfrak{q}}}$.

Let $\mathfrak{F}(X,Y) \in O_{F_\mathfrak{q}}[[X,Y]]$ denote the formal group afforded by the kernel of reduction modulo $\mathfrak{q}$ on $E(F_\mathfrak{q})$. If b is an endomorphism of E, we write $[b](X)$ for the power series corresponding to the induced endomorphism b of $\mathfrak{F}(X,Y)$. Define an $O_{F\mathfrak{q}}$-ideal $f_\mathfrak{q}$ of $O_{F_\mathfrak{q}}[[X]]$ by

$$f_\mathfrak{q} = [p^i](X).\mathfrak{O}_{F_\mathfrak{q}}[[X]]. \tag{1.10}$$

Then the algebra $\mathfrak{B}^0_{i,\mathfrak{q}} := O_{F_\mathfrak{q}}[[X]]/f_\mathfrak{q}$ represents the group scheme G^0_i (see e.g. II §7 of [BT]). Here $\mathfrak{B}^0_{i,\mathfrak{q}}$ is viewed as an order in the algebra $B^0_{i,\mathfrak{q}} := Map(G^0_{i,\mathfrak{q}}(F^c_\mathfrak{q}), F^c_\mathfrak{q})^{\Omega_{F_\mathfrak{q}}}$ via the rule that

$$[b](X)(g) = [b](\underline{g}) \tag{1.11}$$

for $g \in G^0_{i,\mathfrak{q}}(F^c_{\mathfrak{q}})$, where $\underline{g}$ denotes the parameter for g on the formal group $\mathfrak{F}$.

Let $\mathfrak{B}_{i,\mathfrak{q}}$ denote the local completion of the algebra $\mathfrak{B}_i$ at $\mathfrak{q}$, and set $B_{i,\mathfrak{q}}(F) = B_{i,\mathfrak{q}} = \mathfrak{B}_{i,\mathfrak{q}} \otimes_{O_{F_{\mathfrak{q}}}} F_{\mathfrak{q}}$. The exact sequence (1.9) splits when restricted to the closed fibre of $Spec(O_{F_{\mathfrak{q}}})$ (cf. e.g. [Sh] p.68). Hence there are isomorphisms of algebras

$$\mathfrak{B}_{i,\mathfrak{q}} \simeq \mathfrak{B}'_{i,\mathfrak{q}} \otimes \mathfrak{B}^0_{i,\mathfrak{q}} \tag{1.12}$$

and

$$B_{i,\mathfrak{q}} \simeq B'_{i,\mathfrak{q}} \otimes B^0_{i,\mathfrak{q}}. \tag{1.13}$$

Write $j : B_{i,\mathfrak{q}} \to B^0_{i,\mathfrak{q}}$ for the obvious projection map. We record the following result for future use.

Proposition 1.3. *Let $\mathfrak{M}_{i,\mathfrak{q}}$ denote the maximal order in the algebra $B_{i,\mathfrak{q}}$. Suppose that $\eta \in \mathfrak{M}_{i,\mathfrak{q}}$ is such that $j(\eta) \in \mathfrak{B}^0_{i,\mathfrak{q}}$. Then $\eta \in \mathfrak{B}_{i,\mathfrak{q}}$.*

Proof. This follows easily from the immediately preceding discusion together with the fact that $\mathfrak{B}'_{i,\mathfrak{q}}$ is the maximal order in $B'_{i,\mathfrak{q}}$. $\square$

It follows from the argument given in §2, Proposition 1 of [T] that the algebra $\mathfrak{A}_i$ is described explicitly by

$$\mathfrak{A}_i = \{p^{-i} \sum_{g \in G_i} f(g)g : f \in \mathfrak{B}_i\}. \tag{1.14}$$

If M/F is a finite extension, then, since E/F has everywhere good reduction, we have that

$$\mathfrak{B}_i(M) = \mathfrak{B}_i(F) \otimes_{O_F} O_M, \quad \mathfrak{A}_i(M) = \mathfrak{A}_i(F) \otimes_{O_F} O_M \tag{1.15}$$

and

$$\mathfrak{B}_i(F) = \mathfrak{B}_i(M)^{\Omega_F}, \quad \mathfrak{A}_i(F) = \mathfrak{A}_i(M)^{\Omega_F}. \tag{1.16}$$

We shall now give an alternative description of $\mathfrak{C}_Q(i)$ as a Q-twist of the algebra $\mathfrak{B}_i$ (see §4 of [T]).

Let N/F be a finite extension containing the coordinates of G_i and $G_Q(i)$. Then there is an isomorphism of N-algebras (and A_i-modules) $B_i(N) \simeq N_Q$ induced by translation by any $Q' \in G_Q(i)$. So there is an isomorphism of N-algebras and A_i-modules given by

$$\xi : B_i \otimes_F N \longrightarrow F_Q(i) \otimes_F N \tag{1.17}$$

where $\xi(b \otimes n)(Q' + g) = b(g)n$ for $b \in B_i$, $n \in N$, and $g \in G_i$. (Here Ω_F acts on both terms of (1.17) via the second factor.) Then we have

$$\mathfrak{C}_Q(i) = [\xi(\mathfrak{B}_i \otimes_{O_F} O_N)]^{\Omega_F}. \tag{1.18}$$

For any finite extension M/F, it follows that

$$\mathfrak{C}_Q(i)(M) = \mathfrak{C}_Q(i)(F) \otimes_{O_F} O_M, \quad \mathfrak{C}_Q(i)(F) = \mathfrak{C}_Q(i)(M)^{\Omega_F}. \tag{1.19}$$

We conclude this section by recalling the following result from [T] regarding a change of basefield. For any finite extension M/F, there is a commutative diagram

$$\begin{array}{ccc} E(M) & \xrightarrow{\psi_{i,M}} & Cl(\mathfrak{A}_i(M)) \\ {\scriptstyle Tr_{M/F}}\downarrow & & \downarrow{\scriptstyle Res} \\ E(F) & \xrightarrow{\psi_{i,F}} & Cl(\mathfrak{A}_i(F)) \end{array} \tag{1.20}$$

where $Tr_{M/F}$ is the trace map, and Res is the restriction map on classgroups defined in §4 of [T].

§**2. Néron symbols and intersection multiplicities.** In this section we shall recall some elementary facts concerning intersection theory on curves and arithmetic surfaces. For full details, we refer the reader to Chapter III of [L] and to [G].

Let N be a number field, and let v denote a non-archimedean absolute value on N. Write π_v for a uniformising parameter in O_{N_v}, and suppose that v is normalised so that $v(\pi_v) = 1$. We write q_v for the cardinality of the residue field of N_v, and for each $\alpha \in N_v$, we set $|\alpha|_v = q_v^{-v(\alpha)}$.

Suppose that C/N_v is a complete, non-singular, geometrically irreducible curve, and assume that $C(N_v)$ is non-empty. Write $Div^0(C(N_v))$ for the set of elements of degree zero in the free abelian group on $C(N_v)$, and view this as a subgroup of $Div^0(C/N_v)$.

If $Z \in Div^0(C/N_v)$ is the divisor of a rational function f, and $Z' = \sum n_i(P_i)$ is a 0-cycle in $Div^0(C/N_v)$ whose support is disjoint from that of Z, then we set

$$f(Z') = \prod_i f(P_i)^{n_i}. \tag{2.1}$$

(It is easy to see that this is well-defined.)

The following theorem is due to Néron (see §3 of [G] for a proof).

Theorem 2.1. *Let $Z \in Div^0(C(N_v))$, $Z' \in Div^0(C/N_v)$, and suppose that Z, Z' have disjoint supports. Then one can define (in precisely one way) a real number $< Z, Z' >_v$ satisfying the following properties:*

(1) The pairing $< Z, Z' >_v$ is bilinear.

(2) If $Z' = (f)$ is principal, then $< Z, Z' >_v = log|f(Z)|_v$.

(3) The pairing is symmetric, i.e. $< Z, Z' >_v = < Z', Z >_v$ if $Z' \in Div^0(C(N_v))$.

(4) Write $supp(Z')$ for the support of Z', and fix $P_0 \in C(N_v) \backslash supp(Z')$. Then the map

$$C(N_v) \backslash supp(Z') \longrightarrow \mathbb{R}$$

defined by $P \mapsto < (P) - (P_0), Z' >_v$ is continuous. $\square$

(We remark that the above pairing may also be defined when v is archimedean, but we shall not require this fact.)

Since we are assuming that v is non-archimedean, the pairing $< Z, Z' >_v$ may be described in terms of intersection multiplicities. In order to explain this, we shall first of all recall some basic facts concerning intersection theory on an arithmetic surface. (We refer the reader to Chapter III of [L] for further details.)

Set $Y = Spec(O_N)$, and let X be a regular arithmetic surface over Y, with $\pi : X \to Y$. Write $\mathfrak{O}$ for the structure sheaf of X. Suppose that W, W' are effective divisors on X without common component, and let x be a closed point of X. The intersection number $i_x(W, W')$ is defined by

$$i_x(W, W') = length(\mathfrak{O}_x/(f, g)), \tag{2.1}$$

where *length* is that of an $\mathfrak{O}_x$-module, and W (resp. W') is represented locally by a function f (resp. g) in a neighbourhood of x.

The intersection $W.W'$ is defined by

$$W.W' = \sum_x i_x(W.W')[x]; \tag{2.2}$$

this is a finite sum and should be viewed as a 0-cycle on X.

Let y be a closed point of Y, with associated valuation v. Then the number $i_y(W.W')$ (which we shall also sometimes write $i_v(W.W')$) is defined by

$$i_y(W.W') = \sum_x i_x(W.W')[k(x) : k(y)] \tag{2.3}$$

where the sum is taken over all $x \in supp(W) \cap supp(W')$ lying above y. (Here $k(x)$ (resp. $k(y)$) denotes the residue field at x (resp. y).)

Now write X_N for the generic fibre of X, and let $Div^0(X_N)$ denote the group of divisors on X_N of degree zero. For any irreducible divisor $Z \in Div(X_N)$, its Zariski closure $\mathbf{Z}$ in X is an irreducible horizontal divisor on X. Conversely, every irreducible horizontal divisor on X arises in this way. Extend the association $Z \mapsto \mathbf{Z}$ by linearity to all of $Div(X_N)$; if $Z = \sum_i n_i(P_i)$ is a divisor on X_N, we write $\mathbf{Z} = \sum_i n_i(\mathbf{P}_i)$ for the associated irreducible horizontal divisor on X.

Suppose that $Z, Z' \in Div^0(X_N)$ and that all the components of Z, Z' are rational over N. Write X_{N_v} for the generic fibre of $X \times_Y Spec(O_{N_v})$. Then Z, Z' may be regarded as elements of $Div^0(X_{N_v})$ with components rational over N_v. Hence, if in addition Z, Z' have disjoint supports, then we may refer to $< Z, Z' >_v$ as in Theorem 2.1 (cf. [L], Chapter III, Proposition 4.4).

Let $X_y := \pi^{-1}(y)$ denote the fibre of π above y. We are now in a position to describe the Néron pairing in terms of intersection multiplicities (see §3 (especially (3.7)) of [G]).

Theorem 2.2. *With the above notation, suppose that $Z, Z' \in Div^0(X_N)$ have disjoint supports and that all the components of Z, Z' are rational over N. Suppose further that X_y is smooth. Then,*

$$< Z, Z' >_v = -i_y(\mathbf{Z}.\mathbf{Z}')log(q_v). \qquad (2.4 \quad \square)$$

Remark. If X_y is not smooth, then the term $i_y(\mathbf{Z}.\mathbf{Z}')$ in (2.4) must be modified (cf.Chapter III, Theorem 5.2 of [L]).

§3. Intersection multiplicities on elliptic curves. We retain the notation of the previous section, and we suppose in addition that X is an elliptic surface over Y with X_y smooth for each closed point y of Y. (We continue to write v for the valuation attached to y.)

Suppose that P, Q_1, Q_2 are distinct points on X_N. We assume furthermore that these points are rational over N, and we set $P' = P + Q_2$, $Q' = Q_1 + Q_2$. Since the map $X \to X$ given by $T \mapsto T + Q_2$ is an automorphism of the surface X, it follows that we have

$$i_y(\mathbf{P}.\mathbf{Q}_1) = i_y(\mathbf{P}'.\mathbf{Q}'). \tag{3.1}$$

Hence

$$i_y(\mathbf{P}.\mathbf{Q}_1) = i_y(\underline{\mathbf{O}}.\mathbf{S}),$$

where $S = P - Q_1$ and $\underline{O}$ is the origin of the group law on X.

This enables us to apply the following technique (see [S] p.85-91). Let $\omega \neq 0$ be a differential of the first kind on X_N, and choose a parameter z such that $\omega = dz +$ (higher order terms) about $\underline{O}$. (So we may take $z = s/t$, in terms of Weierstrass coordinates s, t on X_N.) Write $\tilde{P}$ for the reduction of $P \in X_N$. Then

$$\begin{aligned} i_y(\underline{\mathbf{O}}.\mathbf{P}) &= 0 \quad \text{if} \quad \tilde{P} \neq \underline{\tilde{O}} \\ &= v(z(P)) \quad \text{otherwise.} \end{aligned}$$

So the local intersection multiplicity $i_y(\underline{\mathbf{O}}.\mathbf{P})$ is determined by the parameter $z(P)$ of P on the formal group about the origin. The following result is an immediate consequence of the preceding discussion.

Proposition 3.1. *Suppose that $Z = (P), Z' = (P')$ are divisors on X_N which are rational over N. Then $i_y(\mathbf{Z}.\mathbf{Z}')$ is non-zero only if the points P, P' coincide when reduced modulo v.* $\square$

§**4. Special functions.** We now return to the setup and notation established in §0 and §1. Thus, E/F is an elliptic curve with everywhere good reduction, l and

l' are distinct odd primes and $Q \in E(F)$ is a p-power torsion point. (Recall that $p > 3$ is a prime satisfying $p^i \equiv 1(\text{modulo} \quad ll')$.) The purpose of this section is to describe two special functions on E that will play a crucial role in the proof of Theorem 1.

Let E_l (resp.$E_{l'}$) denote the group of l (resp. l') torsion points of E, and write $F(E_l)$ for the field obtained by adjoining the coordinates of the points in E_l to F. Let θ and ϕ be two independent l-torsion points. Choose a function $D_{\theta,\phi}$, rational over $F(E_l)$ such that the divisor of $D_{\theta,\phi}$ is given by

$$(D_{\theta,\phi}) = \sum_{k=0}^{l-1}(k\theta) - \sum_{k=0}^{l-1}(\phi + k\theta). \tag{4.1}$$

(In what follows, we shall write D for $D_{\theta,\phi}$.) $D(z)$ and $D(z+\theta)$ have the same divisor, and so,

$$D(z+\theta) = \omega.D(z) \quad \omega \in F(E_l). \tag{4.2}$$

Since $l.\theta = \underline{O}$, it follows that $\omega^l = 1$.

We write

$$w : G_i \times G_i \longrightarrow \mu_{p^i} \tag{4.3}$$

for the Weil pairing on $G_i \times G_i$. Suppose that $\nu \in G_i$. Then we define a homomorphism $\chi_\nu : G_i \to \mu_{p^i}$ by

$$\chi_\nu(\gamma) = w(l.\gamma, \nu), \quad \gamma \in G_i. \tag{4.4}$$

It follows that the characters of G_i are precisely the χ_ν's.

Next, consider the function $H(z) = D(p^i z)/D(z)$. $H(z)$ has neither a zero nor a pole at $z = \underline{O}$ and $H(\underline{O}) = p^i$. The following result is immediate.

Lemma 4.1. *The divisor of the function $H(z)$ is given by*

$$(H(z)) = \sum_{g \in G_i \setminus \underline{O}} [\sum_{k=0}^{l-1}(k\theta + g) - \sum_{k=0}^{l-1}(\phi + k\theta + g)]. \quad \square$$

Define the resolvent function $R_\nu(z)$ by

$$R_\nu(z) = \frac{1}{p^i} \sum_{\gamma \in G_i} \frac{D(p^i z)}{D(z+\gamma)} \chi_\nu(-\gamma). \tag{4.5}$$

Note that $R_\nu(z)$ is well-defined independently of the choice of D, and that $R_\nu(\underline{O}) = 1$. Also we have (using the fact that $p^i \equiv 1(ll')$):

$$D(p^i(z+\theta)) = D(p^i z + \theta) = \omega . D(p^i \theta), \tag{4.6}$$

and

$$D(z+\gamma+\theta) = \omega D(z+\gamma). \tag{4.7}$$

Hence

$$R_\nu(z+\theta) = R_\nu(z). \tag{4.8}$$

We shall now determine the divisor of $R_\nu(z)$.

Proposition 4.2.

(a) If $\nu = \underline{O}$, then $R_\nu(z) = 1$.

(b) If $\nu \neq \underline{O}$, then

$$(R_\nu(z)) = \sum_{g \in G_i} [\sum_{k=0}^{l-1}(\nu' + k\theta + g + \phi) - \sum_{k=0}^{l-1}(k\theta + g + \phi)]$$

where ν' is any point in $E(F^c)$ satisfying $[p^i]\nu' = \nu$.

Remark. This is Theorem 3 of [ST]. We give an argument below (which is somewhat different from that in [ST]) for the convenience of the reader and because we believe that the more algebraic techniques used here may be of use in treating the case of higher dimensional abelian varieties.

Proof.

(a) We have that

$$(D(p^i z)) = \sum_{g\in G_i} [\sum_{k=0}^{l-1}(k\theta + g) - \sum_{k=0}^{l-1}(\phi + k\theta + g)] \tag{4.9}$$

and

$$(D(z+\gamma)) = \sum_{k=0}^{l-1}(k\theta - \gamma) - \sum_{k=0}^{l-1}(\phi + k\theta - \gamma). \tag{4.10}$$

Hence $D(p^i z)^{-1}$ and $\sum_{\gamma\in G_i} D(z+\gamma)^{-1}$ have the same polar divisor. It follows from (4.8) that $R_{\underline{O}}(z)$ gives a well-defined function on the elliptic curve $E/<\theta>$, with at worst a simple pole. This implies, via the Riemann-Roch theorem, that $R_{\underline{O}}(z)$ is constant. Thus we have

$$R_{\underline{O}}(z) = R_{\underline{O}}(\underline{O}) = 1. \tag{4.10a}$$

(b) Let $f_\nu(z)$ be a function on E whose divisor is given by

$$(f_\nu(z)) = \sum_{g\in G_i}(\nu' + g) - \sum_{g\in G_i}(g) \tag{4.11}$$

where ν' is any point in $E(F^c)$ satisfying $[p^i]\nu' = \nu$. Then we have

$$\frac{f_\nu(z+\lambda)}{f_\nu(z)} = w(\lambda,\nu) \tag{4.12}$$

for all $\lambda \in G_i$ (see e.g. [Si] Chapter III §8). Define

$$F_\nu(z) = \prod_{k=0}^{l-1} f_\nu(z + k\theta). \tag{4.13}$$

Then

$$(F_\nu(z)) = \sum_{k=0}^{l-1}[\sum_{g\in G_i}(\nu' + g + k\theta) - \sum_{g\in G_i}(g + k\theta)] \tag{4.14}$$

and furthermore we have that

$$\frac{F_\nu(z+\gamma)}{F_\nu(z)} = w(l.\gamma, \nu) = \chi_\nu(\gamma) \tag{4.15}$$

for all $\gamma \in G_i$. It follows from the definition of $F_\nu(z)$ that

$$F_\nu(z+\theta) = F_\nu(z). \tag{4.16}$$

We also have that

$$R_\nu(z+\gamma) = R_\nu(z).\chi_\nu(\gamma) \tag{4.17}$$

for all $\gamma \in G_i$.

Next, we observe that

$$(D(p^i z)^{-1}) = \sum_{g\in G_i}[\sum_{k=0}^{l-1}(\phi + k\theta + g) - \sum_{k=0}^{l-1}(k\theta + g)] \tag{4.18}$$

and

$$(F_\nu(z-\phi)) = \sum_{g\in G_i}[\sum_{k=0}^{l-1}(\nu' + \phi + k\theta + g) - \sum_{k=0}^{l-1}(k\theta + g + \phi)]. \tag{4.19}$$

Hence

$$\text{Polar divisor of } \frac{F_\nu(z-\phi)}{D(p^i z)} = \sum_{g\in G_i}\sum_{k=0}^{l-1}(k\theta + g). \tag{4.20}$$

Now

$$\begin{aligned}\text{Polar divisor of } \frac{R_\nu(z)}{D(p^i z)} &= \text{Polar divisor of } \sum_{\gamma\in G_i}\frac{1}{D(z+\gamma)}.\chi_\nu(-\gamma) \\ &= \sum_{g\in G_i}\sum_{k=0}^{l-1}(k\theta + g). \end{aligned} \tag{4.21}$$

Thus, it follows from (4.15)-(4.16) that the quotient $F_\nu(z-\phi)/R_\nu(z)$ yields a well-defined function on the elliptic curve $E/<G_i,\theta>$ with at worst a simple pole. This implies, via the Riemann-Roch theorem, that $F_\nu(z-\phi)/R_\nu(z)$ is constant. So,

$$F_\nu(z-\phi)=c_1.R_\nu(z), \tag{4.22}$$

and since $R_\nu(\underline{O})=1$, it follows that $c_1=F_\nu(-\phi)$. Thus we have

$$R_\nu(z)=F_\nu(-\phi)^{-1}.F_\nu(z-\phi), \tag{4.23}$$

and now part (b) of the proposition follows. □

§**5. Integrality results.** We shall now use the results in §2 and §3 to obtain integrality statements concerning special values of the functions $R_\nu(z)$ and $H(z)$.

For any finite extension N/F, let $\mathcal{E}/O_N$ denote the Néron minimal model of E/N. If $Z=\sum_i n_i(P_i)$ is a divisor on the generic fibre $\mathcal{E}_N$, then we write $\mathbf{Z}=\sum_i n_i(\mathbf{P}_i)$ for the Zariski closure of Z on $\mathcal{E}$. Our principal tool will be the following proposition.

Proposition 5.1. *Let f be a function on E with divisor Z, and suppose that $Z'\in Div^0(E)$. Assume also that all components of Z,Z' are rational over N. Then for each finite place v of N, we have that*

$$ord_v(f(Z'))=i_v(\mathbf{Z}.\mathbf{Z}').$$

In particular, $f(Z')$ is an algebraic integer if and only if $i_v(\mathbf{Z}.\mathbf{Z}')\geq 0$ for all finite v.

Proof. This follows immediately from Theorem 2.1(2) and Theorem 2.2. □

Fix a choice of $\nu\in\hat{G}_i$ with $\nu\neq\underline{O}$ and set $Z_1=(R_\nu(z))$, $Z_2=(H(z))$ (these are divisors on E); so

$$Z_1:=\sum_{g\in G_i}[\sum_{k=0}^{l-1}(\nu'+k\theta+\phi+g)-\sum_{k=0}^{l-1}(g+k\theta+\phi)] \tag{5.1}$$

and

$$Z_2 := \sum_{g \in G_i \setminus \underline{O}} [\sum_{k=0}^{l-1} (k\theta + g) - \sum_{k=0}^{l-1} (g + k\theta + \phi)]. \tag{5.2}$$

(Note that the divisor Z_1 depends upon our choice of ν, although we omit this dependence from our notation.)

Let ψ be a primitive l'-torsion point of E, and let β be any p-power torsion point of E. Define a divisor Z_3 on E by

$$Z_3 := (\beta + \psi) - (\underline{O}). \tag{5.3}$$

Now choose N/F to be a sufficiently large extension that all components of the Z_i's are rational over N, and regard each Z_i as being a divisor on $\mathcal{E}_N$. We observe that

(a) $supp(Z_3)$ is disjoint from $supp(Z_1) \cup supp(Z_2)$.

(b) $\mathbf{Z}_3$ and $\mathbf{Z}_i$ $(i = 1, 2)$ can only intersect on vertical fibres of $\mathcal{E}/O_N$ lying above places v dividing p, l or l'. This follows from Proposition 3.1 together with the fact that $\cup_{j=1}^{3} supp(Z_j)$ contains only points that are killed by l, l' or a power of p.

In this section, we shall evaluate $i_v(\mathbf{Z}_3.\mathbf{Z}_i)$ $(i = 1, 2)$ for all such finite places v of O_N.

Proposition 5.2. *If $v|l$, then*

$$i_v(\mathbf{Z}_1.\mathbf{Z}_3) = \sum_{k=0}^{l-1} i_v((k\boldsymbol{\theta} + \boldsymbol{\phi}).(\underline{\mathbf{O}})).$$

In all other cases, $i_v(\mathbf{Z}_1.\mathbf{Z}_3) = 0$.

Proof. Suppose that $v \nmid l$. Then $supp(\mathbf{Z}_1)$ and $supp(\mathbf{Z}_3)$ are disjoint when reduced modulo v, and so we deduce from Proposition 3.1 that $i_v(\mathbf{Z}_1.\mathbf{Z}_3) = 0$ in this case.

If $v|l$, then it follows from the fact that the local intersection multiplicity is both bilinear and translation invariant (see §2 and §3) that we have

$$i_v(\mathbf{Z}_1.\mathbf{Z}_3) = \sum_{k=0}^{l-1} i_v((k\boldsymbol{\theta} + \boldsymbol{\phi}).(\underline{\mathbf{O}})).$$

as asserted. $\square$

We observe from Proposition 5.2 that $i_v(\mathbf{Z}_1.\mathbf{Z}_3) \geq 0$ for all finite v, and that $i_v(\mathbf{Z}_1.\mathbf{Z}_3)$ is independent of the choice of β and of $\nu \neq \underline{O}$. For any two algebraic numbers a and b, write $a \sim b$ if a/b is a unit. The following result is an immediate consequence of Propositions 5.1 and 5.2 together with equation (4.10)(a).

Proposition 5.3.

(a) $R_\nu(\beta + \psi)$ is an algebraic integer for all p-power torsion points β of E and all $\nu \in \hat{G}_i$. Furthermore, $R_\nu(\beta + \psi)$ is a unit at all primes not dividing l.

(b) Let β_1, β_2 be any p-power torsion points of E. Then

$$R_\nu(\beta_1 + \psi) \sim R_\nu(\beta_2 + \psi)$$

for all $\nu \in \hat{G}_i$.

Proof. This follows from the immediately preceding discussion together with the fact that $R_{\underline{O}}(z) = 1$ for all z. $\square$

We now turn our attention to the function $H(z)$.

Proposition 5.4. *If $v|p$, then*

$$i_v(\mathbf{Z}_2.\mathbf{Z}_3) = -\sum_{g \in G_i \setminus \underline{O}} i_v((\mathbf{g}).(\underline{\mathbf{O}})).$$

In all other cases, $i_v(\mathbf{Z}_2.\mathbf{Z}_3) = 0$.

Proof. Suppose that $v \nmid p$. Then $supp(\mathbf{Z}_2)$ and $supp(\mathbf{Z}_3)$ are disjoint when reduced modulo v. Hence it follows from Proposition 3.1 that $i_v(\mathbf{Z}_2.\mathbf{Z}_3) = 0$ in this case.

If on the other hand $v|p$, then again it follows from Proposition 3.1 together with the fact that the local intersection multiplicity is both bilinear and translation invariant that

$$i_v(\mathbf{Z}_2.\mathbf{Z}_3) = -\sum_{g \in G_i \backslash \underline{O}} i_v((\mathbf{g}).(\underline{\mathbf{O}})). \quad \square$$

Proposition 5.5. *$H(\beta + \psi)$ is a global unit for all p-power torsion points β.*

Proof. Recall that $H(\underline{O}) = p^i$. From Proposition 5.1 applied to Z_2 and Z_3, we have, for each finite place v of N

$$ord_v\left(\frac{H(\beta + \psi)}{H(\underline{O})}\right) = i_v(\mathbf{Z}_2.\mathbf{Z}_3)$$

i.e

$$\begin{aligned} ord_v\left(\frac{H(\beta + \psi)}{p^i}\right) &= -\sum_{g \in G_i \backslash \underline{O}} i_v((\mathbf{g}).(\underline{\mathbf{O}})) \quad \text{if} \quad v|p \\ &= 0 \quad \text{otherwise.} \end{aligned} \tag{5.4}$$

for all p-power torsion points β.

Set $\beta = \underline{O}$. Then $H(\psi) = D(p^i\psi)/D(\psi) = 1$ (since $p^i \equiv 1(ll')$), and so we have

$$\begin{aligned} ord_v(p^{-i}) &= -\sum_{g \in G_i \backslash \underline{O}} i_v((\mathbf{g}).(\underline{\mathbf{O}})) \quad \text{if} \quad v|p \\ &= 0 \quad \text{otherwise.} \end{aligned} \tag{5.5}$$

From (5.4) and (5.5) we deduce that $ord_v(H(\beta + \psi)) = 0$ for all finite v and all p-power torsion points β. Hence $H(\beta + \psi)$ is a global unit, as asserted. $\square$

§6. Proof of Theorem 1. In this section we shall use our earlier results to give a proof of Theorem 1. Let us begin by recalling the salient facts concerning the situation with which we are dealing.

We assume that E/F is an elliptic curve with everywhere good reduction, and $Q \in E(F)$ is a p-power torsion point. The numbers l and l' are distinct odd primes, and we suppose further that $p^i \equiv 1(ll')$. We have that θ and ϕ are independent l-torsion points, while ψ is a primitive l'-torsion point of E.

Let M be the field $F(E_{ll'})$, and define a function h on E by

$$h(z) = \frac{D(p^i z + \psi)}{D(z + \psi)}. \tag{6.1}$$

Then the functions $D(z)$ and $h(z)$ both lie in the function field $M(E)$. Observe that $h(z) = H(z + \psi)$, since ψ is an l'-division point and $p^i \equiv 1(ll')$.

Lemma 6.1. *For the field M as above, we have*

$$[M : F] | [l(l+1)(l-1)^2][l'(l'+1)(l'-1)^2]$$

Proof. The group $Gal(M/F)$ is a subgroup of $GL_2(\mathbb{F}_l) \times GL_2(\mathbb{F}_{l'})$. The result now follows from the fact that for any prime q, the group $GL_2(\mathbb{F}_q)$ is of order $q(q+1)(q-1)^2$. □

Lemma 6.2. *Let $w = HCF\{l(l+1)(l-1)^2 | l \neq p \quad \text{is an odd rational prime}\}$. Suppose that $q > 3$ is a prime. Then $q \nmid w$.*

Proof. Choose a prime l_1 such that $l_1 \equiv 3(q)$ and $l_1 \neq p$.. (This may be done, via Dirichlet's theorem on primes in an arithmetic progression.) Then $q \nmid l_1(l_1+1)(l_1-1)^2$, and the result follows. □

Next, we observe that if Q is any p-power torsion point in $E(F)$, the function h defines an element h_Q of $M_Q(i)$ by the rule

$$h_Q(Q') = h(Q'), \quad Q' \in G_Q(i). \tag{6.2}$$

Note that $h_Q(Q')$ is always finite. If we take $Q = \underline{O}$, then we have that $G_{\underline{O}}(i) = G_i$, and (6.2) defines a function $h_{\underline{O}}$ on G_i. We define a resolvend element $\rho \in A_i(M)$ by

$$\rho = \frac{1}{p^i} \sum_{g \in G_i} h_{\underline{O}}(g) g^{-1}. \tag{6.3}$$

Proposition 6.3. *Let $Q \in E(F)$ be a p-power torsion point. Then $h_Q \in \mathfrak{C}_Q(i)(M)$.*

Proof. Let N be some large extension of M containing the coordinates of all points of G_i and $G_Q(i)$. From §1 (see (1.17)-(1.19)) it follows that $\mathfrak{C}_Q(i)(M) = \xi(\mathfrak{B}_i(N)) \cap M_Q(i)$. Hence, since $h_Q \in M_Q(i)$, the result will follow if we show that $h_Q \in \xi(\mathfrak{B}_i(N))$.

Let $\mathcal{M}_i(N)$ denote the maximal order in the algebra $B_i(N)$. Proposition 5.5 implies that $\xi^{-1}(h_Q) \in \mathcal{M}_i(N)^x$ (cf. (1.17)). We shall show that $\xi^{-1}(h_Q) \in \mathfrak{B}_i(N)_{\mathfrak{q}}$ for each prime $\mathfrak{q}$ of O_N.

Set $\eta = \xi^{-1}(h_Q)$ and suppose that $\mathfrak{q} \nmid p$. Then $\mathcal{M}_i(N)_{\mathfrak{q}} = \mathfrak{B}_i(N)_{\mathfrak{q}}$, and so we have that $\eta \in \mathfrak{B}_i(N)_{\mathfrak{q}}$, as required.

Suppose now that $\mathfrak{q}|p$. It follows from Proposition 1.3 that, in order to show that $\eta \in \mathfrak{B}_i(N)_{\mathfrak{q}}$, it suffices to show that $j(\eta) \in \mathfrak{B}^0_{i,\mathfrak{q}}(N)$. For this we use an argument motivated by that given in Proposition 5 of [ST]. I am grateful to the referee for supplying some of the details given below.

Set $Z_4 = (h(z))$, a divisor on $\mathcal{E}_N$, and write $\mathbf{Z}_4$ for the associated divisor on the Néron model $\mathcal{E}/O_N$. We claim that the fibre $\mathcal{E}_{\mathfrak{q}}$ of $\mathcal{E}$ over $\mathfrak{q}$ does not occur in $\mathbf{Z}_4$.

For observe that this is the same as saying that $ord_{w(\mathfrak{q})}(h(z)) = 0$, where $ord_{w(\mathfrak{q})}$ is the discrete valuation of the function field $N(E)$ corresponding to the generic point of $\mathcal{E}_{\mathfrak{q}}$. Now

$$h(z) = H(z+\psi) = \frac{D(p^i(z+\psi))}{D(z+\psi)} = \frac{[p^i]^*(D(z+\psi))}{D(z+\psi)},$$

where $[p^i]^* : N(E) \to N(E)$ is the algebra homomorphism induced by the morphism $[p^i] : \mathcal{E} \to \mathcal{E}$. Since $[p^i]^*$ fixes a uniformiser for $O_{N,\mathfrak{q}}$, which is also a uniformiser in $O_{\mathcal{E},w(\mathfrak{q})}$ (where $O_{\mathcal{E}}$ denotes the structure sheaf of $\mathcal{E}$), we see that $ord_{w(\mathfrak{q})}([p^i]^* f) = ord_{w(\mathfrak{q})}(f)$ for all $f \in N(E)$. Hence

$$ord_{w(\mathfrak{q})}(h(z)) = ord_{w(\mathfrak{q})}([p^i]^* D(z+\psi)) - ord_{w(\mathfrak{q})}(D(z+\psi)) = 0,$$

as asserted.

Now let $\tilde{E}$ denote the reduction of E modulo $\mathfrak{q}$, and write k for the residue field of O_N at $\mathfrak{q}$. Since $h(z) \in O^x_{\mathcal{E},w(\mathfrak{q})}$, we may define $\bar{h}(z) \in k^c(\tilde{E})$ to be the (non-zero) image of $h(z)$ in the residue field of $w(\mathfrak{q})$ (noting that this latter field is naturally contained in $k^c(\tilde{E})$). The divisor of $\bar{h}(z)$ on $\tilde{E}$ is contained in the intersection of the fibre $\mathcal{E}_{\mathfrak{q}}$ with the divisor $\mathbf{Z}_4$. All points appearing in the divisor of $\bar{h}(z)$ have order dividing ll', and so cannot be p-power torsion points.

Consider the formal group afforded by $E_1(N_{\mathfrak{q}})$, the kernel of reduction of E modulo $\mathfrak{q}$. Let $t = t(z)$ denote the parameter of a point $z \in E_1(N_{\mathfrak{q}})$ on this formal group, and write α' for the parameter of any p-power torsion point in $E_1(N_{\mathfrak{q}})$. For any point $z \in E_1(N_{\mathfrak{q}})$, we have the following expansion of $\bar{h}$ as a Laurent series in $k^c[[t]]$:

$$\bar{h}(z+\alpha') = \sum_{i=0}^{\infty} \bar{b}_i t^i$$

with $\bar{b}_0 \neq 0$, since the divisor of $\bar{h}$ contains no p-power torsion points. Hence we have that $h(z+\alpha')$ is a unit in $O_{N,\mathfrak{q}}[[t]]$, i.e.

$$h(z+\alpha') = \sum_{i=0}^{\infty} b_i t^i,$$

with $b_0 \in O^{x}_{N,\mathfrak{q}}$ and $b_i \in O_{N,\mathfrak{q}}$. It therefore follows that $j(\eta) \in \mathfrak{B}^0_{i,\mathfrak{q}}(N)$, as asserted. This completes the proof. $\square$

The following corollary is now an immediate consequence of (1.14).

Corollary 6.4. *The resolvend element ρ lies in $\mathfrak{A}_i(M)$.* $\square$

We now prove a special case of Theorem 1.

Theorem 6.5. *Let $Q \in E(F)$ be a p-power torsion point. Then*

$$\mathfrak{C}_Q(i)(M).\rho = h_Q.\mathfrak{A}_i(M),$$

and so $\mathfrak{C}_Q(i)(M)$ is $\mathfrak{A}_i(M)$-free.

Proof. The proof of this assertion is similar to that of Theorem 5 of [ST].

We shall show that the equality holds everywhere locally; this will imply the desired result. Let $\mathfrak{q}$ be a prime of O_M. Then we may write $\mathfrak{C}_Q(i)(M)_{\mathfrak{q}} = x_{\mathfrak{q}}.\mathfrak{A}_i(M)_{\mathfrak{q}}$. For some $\lambda_{\mathfrak{q}} \in A_i(M_{\mathfrak{q}})$, we have

$$x_{\mathfrak{q}}.\rho\lambda_{\mathfrak{q}} = h_Q. \tag{6.4}$$

We shall show that in fact $\lambda_{\mathfrak{q}} \in \mathfrak{A}_i(M)^{x}_{\mathfrak{q}}$; this will establish the result.

We begin by observing that, since $h_Q \in \mathfrak{C}_Q(i)(M)$ and $\mathfrak{A}_i(M)_{\mathfrak{q}} = \{x \in A_i(M_{\mathfrak{q}}) : \mathfrak{C}_Q(i)(M)_{\mathfrak{q}}.x \subseteq \mathfrak{C}_Q(i)(M)_{\mathfrak{q}}\}$, we have that

$$\rho\lambda_{\mathfrak{q}} \in \mathfrak{A}_i(M)_{\mathfrak{q}}. \tag{6.5}$$

Next, recall that if $x \in M_Q$ and $\nu \in G_i$, then we have the Lagrange resolvent

$$(x|\chi_\nu) = \sum_{g \in G_i} x^g \chi_\nu(g^{-1}). \tag{6.6}$$

If $g' \in G_i$, then $(x^{g'}|\chi_\nu) = (x|\chi_\nu).\chi_\nu(g')$, and so for each $\lambda \in \mathbb{Q}^c G_i$, we have

$$(x\lambda|\chi_\nu) = (x|\chi_\nu).\chi_\nu(\lambda). \tag{6.7}$$

Hence (6.4) implies that

$$(x_\mathfrak{q}|\chi_\nu).\chi_\nu(\rho).\chi_\nu(\lambda_\mathfrak{q}) = (h_Q|\chi_\nu). \tag{6.8}$$

Now the proof of Theorem 3 of [T] implies that if $Q' \in G_Q(i)$, then $(x_\mathfrak{q}|\chi_\nu)(Q') \sim p^i$. Also, we have that $\chi_\nu(\rho) = R_\nu(\psi)$, and $(h_Q|\chi_\nu)(Q') = p^i R_\nu(Q' + \psi)$. Hence, evaluating (6.8) at $Q' \in G_Q(i)$, we obtain

$$p^i R_\nu(\psi).\chi_\nu(\lambda_\mathfrak{q}) \sim p^i R_\nu(Q' + \psi). \tag{6.9}$$

Next, we recall (see Proposition 5.3) that

$$R_\nu(\psi) \sim R_\nu(Q' + \psi) \sim \begin{cases} 1 & \text{if} \quad \nu = \underline{O} \\ \\ \text{an} \quad l-\text{unit if} & \nu \neq \underline{O}. \end{cases} \tag{6.10}$$

This implies that $\chi_\nu(\lambda_\mathfrak{q})$ is always a unit, and that $\chi_\nu(\rho)$ is also a unit at $\mathfrak{q}$ unless $\nu \neq \underline{O}$ and $\mathfrak{q}|l$. There are now two cases to consider.

Case 1. Suppose that $\mathfrak{q} \nmid l$. Corollary 6.4 implies that $\rho \in \mathfrak{A}_i(M)_\mathfrak{q}$. Since also $\chi_\nu(\rho)$ is a unit for all ν in this case, it follows that in fact $\rho \in \mathfrak{A}_i(M)_\mathfrak{q}^x$. Thus, from (6.4), it follows that $\lambda_\mathfrak{q} \in \mathfrak{A}_i(M)_\mathfrak{q}$, and so we have that $\lambda_\mathfrak{q} \in \mathfrak{A}_i(M)_\mathfrak{q}^x$ since $\chi_\nu(\lambda_\mathfrak{q})$ is a unit for all $\nu \in G_i$.

Case 2. Suppose that $\mathfrak{q}|l$. Then, since $l \nmid |G_i|$, it follows that $\mathfrak{A}_i(M)_\mathfrak{q}$ is the maximal order. Now we deduce that $\lambda_\mathfrak{q} \in \mathfrak{A}_i(M)_\mathfrak{q}^x$ since the $\chi_\nu(\lambda_\mathfrak{q})$ are units for all $\nu \in G_i$. $\square$

We are now in a position to prove Theorem 1.

Consider the trace-restriction square (1.20):

$$\begin{array}{ccc} E(M) & \xrightarrow{\psi_{i,M}} & Cl(\mathfrak{A}_i(M)) \\ {\scriptstyle Tr_{M/F}}\Big\downarrow & & \Big\downarrow{\scriptstyle Res} \\ E(F) & \xrightarrow{\psi_{i,F}} & Cl(\mathfrak{A}_i(F)) \end{array} \tag{6.11}$$

If $Q \in E(F)$ is a p-power torsion point, we may regard Q as lying in $E(M)$, and Theorem 6.5 implies that

$$\psi_{i,F}(Tr(Q)) = Res(\psi_{i,M}(Q)) = 0 \tag{6.12}$$

Next, we observe that we also have

$$\psi_{i,F}(Tr(Q)) = \psi_{i,F}([M:F]Q) = [M:F].\psi_{i,F}(Q) \tag{6.13}$$

Hence we obtain that

$$[M:F]\psi_{i,F}(Q) = 0 \tag{6.14}$$

i.e.

$$[M:F](\mathfrak{C}_Q(i)) = 0. \tag{6.15}$$

Now let l and l' vary among all odd primes not equal to p. Then it follows from Lemmas 6.1 and 6.2 that $w^2\psi_{i,F}(Q) = 0$. Now recall that $|G_i|\psi_{i,F}(Q) = 0$ (see (1.8)). Since $p > 3$, we have that $(|G_i|, w) = 1$ by Lemma 6.2, and so finally we deduce that $(\mathfrak{C}_Q(i)(F)) = 0$ in $Cl(\mathfrak{A}_i(F))$. This completes the proof of Theorem 1. $\square$

References

[**A1**] A. Agboola, *A geometric interpretation of the class invariant homomorphism*, Journal des Théorie des Nombres de Bordeaux **6** (1994), 273-280.

[**A2**] A. Agboola, *A note on elliptic curves and Galois module structure in global function fields*, preprint.

[**BT**] N. Byott, M. J. Taylor, *Hopf orders and Galois module structure*, In: Group rings and classgroups, K. W. Roggenkamp, M. J. Taylor (eds), Birkhauser, 1992, pp. 153-210.

[**CNS**] Ph. Cassou-Noguès, A. Srivastav, *On Taylor's conjecture for Kummer orders*, Seminaire de Théorie des Nombres de Bordeaux **2** (1990), 349-363.

[**CNT**] Ph. Cassou-Noguès, M. J. Taylor, *Elliptic functions and rings of integers*, Birhauser, 1987.

[**G**] B. Gross, *Local heights on curves*, In: Arithmetic geometry, G. Cornell, S. Silverman (eds), Springer, 1986, pp. 327-339.

[**L**] S. Lang, *Introduction to Arakelov theory*, Springer, 1988.

[**S**] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Vieweg, 1989.

[**Sh**] S. Shatz, *Group schemes, formal groups and p-divisible groups*, In: Arithmetic geometry, G. Cornell, S. Silverman (eds), Springer, 1986, pp. 29-78.

[**Si**] J. Silverman, *The arithmetic of elliptic curves*, Springer, 1986.

[**ST**] A. Srivastav, M. J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math. **99** (1990), 165-184.

[**T**] M. J. Taylor, *Mordell-Weil groups and the Galois module structure of rings of integers*, Ill. J. Math. **32** (1988), 428-452.

Department of Mathematics, UC Berkeley, Berkeley, CA 94720, USA.
E-mail address: agboola@math.berkeley.edu