Can. J. Math., Vol. XL, No. 3, 1988, pp. 649-665

ON THE SELMER GROUP OF TWISTS OF ELLIPTIC CURVES WITH Q-RATIONAL TORSION POINTS

G. FREY

1. Notations and results. (1) The symbols p and q stand for prime numbers and throughout the paper we assume that p is fixed and contained in $\{3, 5, 7\}$. Let L be an algebraic number field (i.e., L is a finite extension of $\mathbf{Q}$). Then prime divisors of L dividing p (resp. q) are denoted by $\mathfrak{p}_L$ (resp. $\mathfrak{q}_L$). The completion of L with respect to $\mathfrak{q}_L$ is denoted by $L_{\mathfrak{q}}$. Let S be a finite set of prime numbers, and let M/L be a Galois extension with abelian Galois group of exponent p.

Definition. M/L is said to be *little ramified outside* S if for primes $q \notin S$ and all $\mathfrak{q}_L | q$ one has

$$M \cdot L_{\mathfrak{q}}(\zeta_p) = L_{\mathfrak{q}}(\zeta_p)(\sqrt[p]{u_1}, \dots, \sqrt[p]{u_k})$$

with $k \in \mathbf{N}$ and $v_{\mathfrak{q}_L}(u_i) = 0$. Here ζ_p is a pth root of unity, $u_1, \dots, u_k$ are elements in $L_{\mathfrak{q}}(\zeta_p)$ and $v_{\mathfrak{q}_L}$ is the normed valuation belonging to $\mathfrak{q}_L$. In particular M/L is unramified at all divisors of primes $q \notin S \cup \{p\}$.

We denote by L_S the maximal abelian extension of exponent p of L which is little ramified outside S, and by $L_{S,u}$ the maximal subfield of L_S which is unramified outside S.

$H_S(L)$ (resp. $H_{S,u}(L)$) denotes the Galois group of L_S/L (resp. $L_{S,u}/L$) and $\mathrm{cl}_S(L)_p$ (resp. $\mathrm{cl}_{S,u}(L)_p$) denotes the order of these Galois groups. If $S = \emptyset$ we see that $\mathrm{cl}_{\phi,u}(L)_p$ is equal to the order of the subgroup of the divisor class group of L consisting of elements of order p which we denote by $\mathrm{cl}(L)_p$.

Now assume that $L/\mathbf{Q}$ is normal with cyclic Galois group generated by an element γ of order $p - 1$. Take an extension $\tilde{\gamma}$ to $L(\zeta_p)$. Let χ_p be the cyclotomic character induced by the action of $G(L(\zeta_p)/\mathbf{Q})$ on $\langle \zeta_p \rangle$. Then $\chi_p(\tilde{\gamma})$ is determined by

$$\tilde{\gamma}(\zeta_p) = \zeta_p^{\chi_p(\tilde{\gamma})}.$$

Let M be normal over $\mathbf{Q}$ containing L such that $G(M/L)$ is abelian of exponent p. Then $\tilde{\gamma}$ operates by conjugation on

$$G(M(\zeta_p)/L(\zeta_p)) \cong G(M/L),$$

Received June 25, 1987 and in revised form December 1, 1987. The research described in this paper was supported by the Deutsche Forschungsgemeinschaft and the Natural Sciences and Engineering Research Council of Canada. It was performed in part at the University of Toronto and at the Mathematical Sciences Research Institute at Berkeley. The author wants to thank these institutions for their help and their hospitality.

and this operation does not depend on the choice of $\tilde{\gamma}$. Hence the subgroup

$$H(\chi_p) := \{\alpha \in G(M/L);\ \tilde{\gamma}\alpha\tilde{\gamma}^{-1} = \alpha^{\chi_p(\tilde{\gamma})}\} \subset G(M/L)$$

is well defined.

In the special case that $M = L_S$ we denote by $\mathrm{cl}_S(L)_p(\chi_p)$ the order of $H_S(L)(\chi_p)$.

(2) Now we shall consider an elliptic curve $E/\mathbf{Q}$ given by a Weierstrass equation $F(x, y) = 0$ with coefficients in $\mathbf{Z}$ and minimal discriminant Δ_E. For any extension field L of $\mathbf{Q}$ we denote the L-rational points of E (including ∞) by $E(L)$.

Let j_E be the absolute invariant of E, and denote by N_E the conductor of E. Let $\tilde{S}_E$ be the set of odd primes $q|N_E$ with $q \equiv -1 \bmod p$ and $v_q(\Delta_E) \not\equiv 0 \bmod p$ and $S_E \subset \tilde{S}_E$ the subset of primes with $v_q(j_E) < 0$. Let d be a square free integer and let E_d be the twist of E with d, i.e., if E is given by

$$y^2 = x^3 - g_2x - g_3$$

then E_d is given by

$$y^2 = x^3 - g_2d^2x - g_3d^3.$$

E_d is isomorphic to E over $\mathbf{Q}(\sqrt{d})$ but not over $\mathbf{Q}$. Let $\mathfrak{W}(E_d, \mathbf{Q})_p$ be the set of elements of order p in the kernel of

$$\rho: H^1(G(\bar{\mathbf{Q}}/\mathbf{Q}), E_d(\bar{\mathbf{Q}})) \to \bigoplus_{q \text{ prime}} H^1(G(\bar{\mathbf{Q}}_q/\mathbf{Q}_q), E_d(\bar{\mathbf{Q}}_q)).$$

Then the group of elements of order p in the Selmer group of E_d, denoted by $S(E_d, \mathbf{Q})_p$, is given as pre-image of $\mathfrak{W}(E_d, \mathbf{Q})_p$ of the map

$$\alpha: H^1(G(\bar{\mathbf{Q}}/\mathbf{Q}), E_d(\bar{\mathbf{Q}})_p) \to H^1(G(\bar{\mathbf{Q}}/\mathbf{Q}), E_d(\bar{\mathbf{Q}})).$$

The aim of this paper is to get some information about $S(E_d, \mathbf{Q})_p$ if $E(\mathbf{Q})$ contains an element of order p. It is obvious that to get this one has to look at the behaviour of E over the local fields $\mathbf{Q}_q$ and their algebraic closures $\bar{\mathbf{Q}}_q$.

Case 1. Assume that $v_q(j_E) \geqq 0$. Then there is a finite extension N of $\mathbf{Q}$ such that E has good reduction modulo all $\mathfrak{q}_N|q$, i.e., we find an elliptic curve $\tilde{E}$ over N such that $\tilde{E}$ modulo $\mathfrak{q}_N$ is an elliptic curve over the residue field of $\mathfrak{q}_N$. $\tilde{E}(\bar{N}_{\mathfrak{q}})$ contains a subgroup $\tilde{E}_-(\bar{N}_{\mathfrak{q}})$ consisting of points $(\tilde{x}, \tilde{y})$ with $v_{\mathfrak{q}_N}(\tilde{x}) < 0$. $\tilde{E}_-$ is the *kernel of the reduction modulo* $\mathfrak{q}_N$, and $v_{\mathfrak{q}_N}(\tilde{x}/\tilde{y})$ is the *level* of $(\tilde{x}, \tilde{y})$. We will have to use some facts about $\tilde{E}_-$ which are essentially due to E. Lutz and which can be found in [**2**]. To have a simple notation we say: A point $(x, y) \in E(\bar{N}_{\mathfrak{q}})$ is in the kernel of the reduction modulo $\mathfrak{q}$ if its image $(\tilde{x}, \tilde{y})$ is in $\tilde{E}_-(\bar{N}_{\mathfrak{q}})$.

Case 2. $v_q(j_E) < 0$. Then after an extension K of $\mathbf{Q}_q$ of degree $\leqq 2$ E becomes a Tate curve (cf. [5]); in particular, one has a parametrization

$$\phi:\bar{K}^*/\langle Q\rangle \rightarrow E(\bar{K})$$

where Q is the q-adic period of E. One has

$$j_E = \frac{1}{Q} + \sum_{i=0}^{\infty} a_i Q^i \quad \text{with } a_i \in \mathbf{Z},$$

and points of order p of $E(\bar{K})$ are of the form $\phi(\zeta_p^\alpha(Q^{1/p})^\beta)$.

If L is as number field and $\mathfrak{q}_L|q$ we say: A point $(x, y) \in E(L_\mathfrak{q})$ is in the connected component of the unity modulo $\mathfrak{q}_L$ if it is of the form $\phi(u)$ with u a $\mathfrak{q}_L$-adic unit, and (x, y) is in the kernel of the reduction modulo $\mathfrak{q}_L$ if $u - 1 \in \mathfrak{q}_L$. One should notice that if E is not a Tate curve over $\mathbf{Q}_q$ but over an extension of degree 2 of $\mathbf{Q}_q$, then for all points P in $E(\mathbf{Q}_q)$, $2P$ is in the connected component of the unity modulo q.

(3) We want to prove the following:

THEOREM. *Let E be an elliptic curve defined over $\mathbf{Q}$ with a point P of order $p > 2$ rational over $\mathbf{Q}$. Assume that either E is given by the equation $y^2 = x^3 + 1$ (hence $p = 3$) or that P is not contained in the kernel of the reduction modulo p, in particular this means that E is not supersingular modulo p if $v_p(j_E) \geqq 0$.*

Let d be a square free integer prime to $p \cdot N_E$ such that:

(i) *If $2|N_E$ then $d \equiv 3 \bmod 4$.*

(ii) *If $q \notin \{2, p, S_E\}$ but $q|N_E$ then $(d/q) = -1$ if E is a Tate curve over $\mathbf{Q}_q$ or $v_q(j_E) \geqq 0$ (hence $p = 3$), and $(d/q) = 1$ otherwise.*

(iii) *If $v_p(j_E) < 0$ then $(d/p) = -1$.*

Then one has

$$(*) \quad \mathrm{cl}_{S_{E,u}}(\mathbf{Q}(\sqrt{d}))_p | \#S(E_d, \mathbf{Q})_p | \mathrm{cl}_{\tilde{S}_{E,u}}(\mathbf{Q}(\sqrt{d}))_p \cdot \mathrm{cl}_{S_E}(K)_p(\chi_p)$$

where K is the subfield of $\mathbf{Q}(\sqrt{d}, \zeta_p)$ of index 2 containing neither ζ_p nor $\sqrt{d}$. (If $d < 0$ then K is the maximal real subfield of $\mathbf{Q}(\sqrt{d}, \zeta_p)$.)

For $p = 7$ the condition $v_p(j_E) \geqq 0$ is no restriction at all. For $p > 3$ and $v_p(j_E) < 0$ again this is no restriction. One could work with a weaker condition but then the technical problems would increase considerably.

We remark that

$$\mathrm{cl}_{\tilde{S}_{E,u}}(\mathbf{Q}(\sqrt{d}))_p \cdot \mathrm{cl}_{S_E}(K)_p(\chi_p)$$

divides

$$\mathrm{cl}(\mathbf{Q}(\sqrt{d}))_p \cdot \mathrm{cl}_\emptyset(K)(\chi_p) \cdot s_E$$

where s_E is a number depending only on $\tilde{S}_E$, with $s_E = 1$ if $\tilde{S}_E = \emptyset$.

Now we use

LEMMA 1. $\mathrm{cl}_\phi(K)_p(\chi_p)\,|\,\mathrm{cl}(\mathbf{Q}(\sqrt{d}))_p$ *if d is negative.*

So we get

COROLLARY. $\mathrm{cl}(\mathbf{Q}(\sqrt{d})_p\,|\,\#\mathrm{S}(E_d, \mathbf{Q})_p\,|\,\mathrm{cl}(\mathbf{Q}(\sqrt{d})_p^2 s_E$ *if* $d < 0$.

In many interesting cases one has $\widetilde{S}_E = \emptyset$ and hence $p\,|\,\#S(E_d, \mathbf{Q})_p$ if and only if p divides the class number of $\mathbf{Q}(\sqrt{d})$. In particular the rank of E_d is equal to 0 if

$$p \nmid \mathrm{cl}(\mathbf{Q}(\sqrt{d})_p).$$

Examples of such curves are $E{:}y^2 = x^3 + 1$ for $p = 3$ (cf. [**1**]), and $X_0(11)$ (for $p = 5$) (cf. [**3**]).

We end this section by proving Lemma 1. Let $M/\mathbf{Q}$ be a Galois extension containing K with $\langle\alpha\rangle = G(M/K)$,

$$\alpha^p = \mathrm{id} \quad \text{and} \quad \overline{\gamma}\alpha\overline{\gamma}^{-1} = \alpha^{\chi_p(\overline{\gamma})} \text{ where } \langle\overline{\gamma}\rangle = G(K/\mathbf{Q}).$$

We assume that M is unramified outside p and little ramified at p; hence

$$M(\zeta_p) = K(\sqrt{d})(\sqrt[p]{c}) \quad \text{with } c \in M(\sqrt{d})$$

and the principal divisor of c is a pth power. Let $\widetilde{\gamma}$ be an extension of $\overline{\gamma}$ to $G(M(\sqrt{d})/\mathbf{Q})$ with $\widetilde{\gamma}^{p-1} = \mathrm{id}$; $\widetilde{\gamma}|\mathbf{Q}(\zeta_p)$ generates $G(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ and $\widetilde{\gamma}|\mathbf{Q}(\sqrt{d}) = \mathrm{id}$. Since $M(\sqrt{d})/\mathbf{Q}$ is normal we have

$$\widetilde{\gamma}(c) = c^i \cdot e^p$$

with $1 \leqq i \leqq p - 1$ and $e \in K(\sqrt{d})$. Hence

$$\widetilde{\gamma}(\sqrt[p]{c}) = (\sqrt[p]{c})^i \cdot e \cdot \xi_{\widetilde{\gamma}}$$

with $\zeta_{\widetilde{\gamma}}^p = 1$. Let $\widetilde{\alpha}$ be an extension of α to $M(\sqrt{d})$ of order p again. Then

$$\widetilde{\gamma}\widetilde{\alpha}(\sqrt[p]{c}) = \zeta_{\widetilde{\alpha}}^{\chi_p(\overline{\gamma})}\widetilde{\gamma}(\sqrt[p]{c})$$

and

$$\widetilde{\alpha}^{\chi_p(\gamma)}\widetilde{\gamma}(\sqrt[p]{c}) = \widetilde{\alpha}^{\chi_p(\gamma)}(\zeta_{\widetilde{\gamma}}(\sqrt[p]{c})^i \cdot e) = \zeta_{\widetilde{\alpha}}^{i \cdot \chi_p(\overline{\gamma})} \cdot \widetilde{\gamma}(\sqrt[p]{c})$$

and hence $i = 1$. That gives

$$\widetilde{c} = N_{\langle\widetilde{\gamma}\rangle}(c) = c^{p-1} \cdot e'^p$$

with $e' \in K(\sqrt{d})$ and hence

$$M(\sqrt{d}) = \mathbf{Q}(\sqrt{d}, \sqrt[p]{c}, \zeta_p).$$

The divisor of $\widetilde{c}$ is a pth power, but since $\pm\widetilde{c}$ is not a pth power in $\mathbf{Q}(\sqrt{d})$, it is an element of order p in the divisor class group of $\mathbf{Q}(\sqrt{d})$, and this proves the lemma.

Remark. For $p = 3$ one recovers the well known fact that the class number of $\mathbf{Q}(\sqrt{-3d})$ is divisible by 3 only if the class number of $\mathbf{Q}(\sqrt{d})$ is divisible by 3.

2. Proof of the theorem. In this section we always assume that $E/\mathbf{Q}$ is an elliptic curve satisfying the conditions imposed in the theorem, and that d is a square free integer satisfying (i)-(iii) as stated in the theorem. Let P be a point of order p of E rational over $\mathbf{Q}$.

(1) Firstly we want to prove the divisibility of $S(E_d, \mathbf{Q})_p$ by

$$\mathrm{cl}_{S_{E,u}}(\mathbf{Q}(\sqrt{d}))_p.$$

LEMMA 2. *Let $M/\mathbf{Q}$ be a non abelian Galois extension of degree $2p$ containing $\mathbf{Q}(\sqrt{d})$ and unramified over this field outside S_E. Let α be a generator of $G(M/\mathbf{Q}(\sqrt{d}))$ and ϕ the element in*

$$H^1(G(M/\mathbf{Q}), E_d(M)_p)$$

determined by $\phi(\alpha) = P$. Then ϕ is an element of $S(E_d, \mathbf{Q})_p$.

Proof. One sees at once that there is one element

$$\phi \in H^1(G(M/\mathbf{Q}), E_d(M)_p)$$

whose restriction $\bar{\phi}$ to $G(M/\mathbf{Q}(\sqrt{d})) = \langle\alpha\rangle$ is given by $\bar{\phi}(\alpha) = P$: We identify $E_d(M)_p$ with $E(M)_p = \langle P\rangle$. Since

$$E_d(\mathbf{Q}(\sqrt{d}))_p = \langle P\rangle \quad \text{and } \delta P = -P \quad \text{with } \langle\delta\rangle = G(\mathbf{Q}(\sqrt{d})/\mathbf{Q}),$$

we get invariance of ϕ under δ from the fact that $\delta\alpha\delta = \alpha^{-1}$, and since

$$H^1(G(M/\mathbf{Q}), E_d(M)_p) = H^1(G(M/\mathbf{Q}(\sqrt{d})), E_d(M)_p)^{\delta},$$

our assertion follows.

Hence it remains to show that $\bar{\phi}$ is locally trivial regarded as an element of

$$H^1(G(M/\mathbf{Q}(\sqrt{d})), E(M)).$$

We can restrict ourselves to primes $\mathfrak{q}_M | p \cdot N_E$. By condition (i) divisors of 2 are split in $M/\mathbf{Q}(\sqrt{d})$ if $2|N_E$, and hence we may assume that $\mathfrak{q}_M \nmid 2$.

Assume that $(d/q) = -1$. In this case $\mathfrak{q}_M$ is either fully ramified or decomposed (since $M/\mathbf{Q}$ is not abelian). So assume that $\mathfrak{q}_M$ is ramified and divides q. Then $q \in S_E$ and in particular $q \neq p$ and $v_q(\Delta_E) \not\equiv 0 \bmod p$. It follows that $E_d/\mathbf{Q}_q(\sqrt{d})$ is a Tate curve and that P is contained in the connected component of the unity over $\mathbf{Q}_q(\sqrt{d})$ corresponding to a pth root of unity ζ_p. $\bar{\phi}$ is locally trivial if $\zeta_p = \alpha x/x$ with some $x \in M_{\mathfrak{q}}$, and since $M_{\mathfrak{q}}/\mathbf{Q}_q(\sqrt{d})$ is cyclic of degree p such an x certainly exists.

Next assume that $(d/q) = 1$ and $q \neq p$. Then $v_q(j_E) < 0$ and E is not a Tate curve over $\mathbf{Q}_q$, and so again P corresponds to some pth root of unity ζ_p under the Tate parametrization of $E = E_d$ over $\mathbf{Q}_q(\zeta_p)$ and hence $\bar{\phi}$ is split by $\mathbf{Q}_q(\zeta_p)$ as seen above. But since the degree of $\mathbf{Q}_q(\zeta_p)$ over $\mathbf{Q}_q$ is prime to p, $\bar{\phi}$ is split over $\mathbf{Q}_q$ already.

So there is only one remaining case: $q = p$ and $v_p(j_E) \geqq 0$. Let $\mathfrak{p}_M | p$. By assumption $M/\mathbf{Q}$ is unramified at $\mathfrak{p}_M$. We find a normal extension $N/\mathbf{Q}$ of degree prime to p such that E has good reduction modulo all primes $\mathfrak{p}_N | p$. For $p = 3$ we can take

$$N = \mathbf{Q}(\sqrt{-1}, \sqrt[4]{-3})$$

by hypothesis; for $p > 3$ take

$$N = \mathbf{Q}(\zeta_{12}, \sqrt[12]{p}).$$

Now

$$H^1(G(M_{\mathfrak{p}} \cdot N/\mathbf{Q}_p \cdot N), E_d(M_{\mathfrak{p}} \cdot N)) = 0$$

since the reduction of E_d modulo $\mathfrak{p}$ is good and $M_{\mathfrak{p}}N/\mathbf{Q}_pN$ is unramified, and hence it follows that

$$H^1(G(M_{\mathfrak{p}}/\mathbf{Q}_p), E_d(M)) = 0$$

also, and so Lemma 2 is proven.

Next we look at the action of

$$\langle \delta \rangle = G(\mathbf{Q}(\sqrt{d})/\mathbf{Q})$$

on $H_{S_{E,u}}(\mathbf{Q}(\sqrt{d}))$, the Galois group of the maximal abelian extension of $\mathbf{Q}(\sqrt{d})$ of exponent p unramified outside S_E, and we assert that δ acts as $-\mathrm{id}$ on this group. This assertion together with Lemma 2 gives the desired divisibility of $\# S(E_d, \mathbf{Q})_p$.

Proof of the assertion.

$$H_{S_{E,u}}(\mathbf{Q}(\sqrt{d})) = H^- \oplus H^+$$

where H^- is the part where δ acts as $-\mathrm{id}$, and H^+ the part with $\delta = \mathrm{id}$. Take

$$\tilde{M} := M_{S_{E,u}}^{H^-}$$

and assume that M_1 is a subfield of $\tilde{M}$ cyclic over $\mathbf{Q}(\sqrt{d})$. Hence $M_1/\mathbf{Q}$ is cyclic of degree $2 \cdot [M_1:\mathbf{Q}(\sqrt{d})]$. Let M_2 be the cyclic extension $\mathbf{Q}$ of degree $[M_1:\mathbf{Q}(\sqrt{d})]$ contained in M_1. Then M_2 is unramified outside S_E, but since for $q \in S_E$ one has $q \equiv -1 \bmod p$ and since $[M_2:\mathbf{Q}] | p$, it follows that M_2 is unramified in all primes and hence $M_1 = \mathbf{Q}$ and $\tilde{M} = \mathbf{Q}(\sqrt{d})$. So our assertion is proven.

(2) *Galois structure of splitting fields of p-covers of E.* Next we determine the Galois group structure of splitting fields of elements in

$$H^1(G(\bar{\mathbf{Q}}/\mathbf{Q}), E(\bar{\mathbf{Q}})_p)$$

for elliptic curves having a $\mathbf{Q}$-rational point P of order p. Denote by $\mathbf{Q}(E_p)$ the field obtained by adjunction of the coordinates of all points of order p of E to $\mathbf{Q}$. Then $\mathbf{Q}(E_p)$ is a Galois extension of $\mathbf{Q}$ containing $\mathbf{Q}(\zeta_p)$. It is cyclic over $\mathbf{Q}(\zeta_p)$ of degree dividing p. Hence its Galois group is generated by two elements $\bar{\gamma}$, $\bar{\epsilon}$ with $\bar{\gamma}^{p-1} = \mathrm{id}$, $\bar{\epsilon}^p = \mathrm{id}$, $\bar{\gamma}|\mathbf{Q}(\zeta_p)$ generating $G(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ and

$$\overline{\gamma\epsilon\gamma}^{-1} = \bar{\epsilon}^{\chi_p(\bar{\gamma})^{-1}}.$$

To see this we choose a base of the form $\{P, Q\}$ of $E(\bar{\mathbf{Q}})_p = E_p$ such that for $\sigma \in G(\mathbf{Q}(E_p)/\mathbf{Q})$ the action of E_p induces a matrix

$$\rho_\sigma = \begin{pmatrix} 1 & b \\ 0 & a \end{pmatrix} \in Gl(2, \mathbf{Z}/p)$$

with

$$a = \det(\rho_\sigma) \equiv \chi_p(\sigma) \text{ modulo } p.$$

Now choose $\bar{\gamma}$ such that

$$\rho_{\bar{\gamma}} = \begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix}$$

with w a generator of $(\mathbf{Z}/p)^*$, and take $\bar{\epsilon} = \mathrm{id}$ if $\mathbf{Q}(E_p) = \mathbf{Q}(\zeta_p)$, and $\bar{\epsilon}$ such that

$$\rho_{\bar{\epsilon}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

otherwise. Then $\bar{\gamma}$ and $\bar{\epsilon}$ generate $G(\mathbf{Q}(E_p)/\mathbf{Q})$ and since

$$\begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & w^{-1} \end{pmatrix} = \begin{pmatrix} 1 & w^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{w^{-1}}$$

we get the relation

$$\overline{\gamma\epsilon\gamma}^{-1} = \bar{\epsilon}^{\chi_p(\bar{\gamma})^{-1}}.$$

We should keep in mind that the choice of $\bar{\epsilon}$ and $\bar{\gamma}$ is closely related to the choice of the base $\{P, Q\}$. In particular we have

$$\bar{\epsilon}(Q) = P + Q \text{ if } \epsilon \neq \mathrm{id} \quad \text{and} \quad \bar{\gamma}(Q) = \chi_p(\bar{\gamma}) \cdot Q.$$

In the rest of this paper P and Q and $\bar{\epsilon}$ and $\bar{\gamma}$ always satisfy these relations.

Now take a square free integer d prime to $p \cdot N_E$.

$$L_d := \mathbf{Q}(E_{d,p})$$

is a quadratic extension of $\mathbf{Q}(E_p)$. It is equal to $\mathbf{Q}(\sqrt{d}) \cdot \mathbf{Q}(E_p)$. Its Galois group over $\mathbf{Q}$ is generated by three elements δ, γ, ϵ with

$$\delta^2 = \mathrm{id}, \quad \delta(\sqrt{d}) = -\sqrt{d}, \quad \gamma^{p-1} = \mathrm{id}, \quad \gamma|\mathbf{Q}(E_p) = \overline{\gamma}, \quad \epsilon^p = \mathrm{id},$$
$$\epsilon|\mathbf{Q}(E_p) = \overline{\epsilon}, \quad \gamma^i\epsilon^j|\mathbf{Q}(\sqrt{d}) = \mathrm{id},$$

δ commuting with ϵ and γ and

$$\gamma\epsilon\gamma^{-1} = \epsilon^{\chi_p(\gamma)^{-1}}.$$

In particular we get that δ operates as $-\mathrm{id}$ on $E_{d,p}$, the points of order p of E_d. The fixed field of ϵ is $\mathbf{Q}(\sqrt{d}, \zeta_p)$ and the fixed field of $\langle \epsilon, \delta\gamma^{(p-1)/2} \rangle$ is K.

We describe the elements in $H^1(G(\overline{\mathbf{Q}}/\mathbf{Q}), E_{d,p})$. We have the exact inf-res-sequence

$$0 \rightarrow H^1(G(L_d/\mathbf{Q}), E_{d,p}) \overset{\inf}{\rightarrow} H^1(G(\overline{\mathbf{Q}}/\mathbf{Q}), E_{d,p})$$
$$\overset{\mathrm{res}}{\rightarrow} H^1(G(\overline{\mathbf{Q}}/L_d), E_{d,p})^{G(L_d/\mathbf{Q})} = \mathrm{Hom}_{G(L_d/\mathbf{Q})}(G(\overline{\mathbf{Q}}/L_d), E_{d,p}).$$

ASSERTION. $H^1(G(L_d/\mathbf{Q}), E_{d,p}) = 0.$

Proof. If $\epsilon = \mathrm{id}$ the degree of $L_d/\mathbf{Q}$ is prime to p, and the assertion follows. Now let ϵ be of order p. Using again the inflation-restriction-sequence one gets

$$H^1(G(L_d/\mathbf{Q}), E_{d,p}) = H^1(\langle \epsilon \rangle, E_{d,p})^{\langle \delta, \gamma \rangle}.$$

Let P_d, Q_d be the points of order p of $E_{d,p}$ corresponding to $P, Q \in E_p$. Then

$$P_d = \epsilon Q_d - Q_d,$$

and hence $H^1(\langle \epsilon \rangle, E_{d,p})$ is generated by the class of the cocycle ψ which sends ϵ to Q_d. But $\delta\epsilon\delta = \epsilon$ and $\delta Q_d = -Q_d$ and hence

$$\psi \notin H^1(\langle \epsilon \rangle, E_{d,p})^{\langle \delta \rangle},$$

and we have proved the assertion.

Hence we have an embedding of

$$H^1(G(\overline{\mathbf{Q}}/\mathbf{Q}), E_{d,p})$$

into

$$\mathrm{Hom}_{G(L_d/\mathbf{Q})}(G(\overline{\mathbf{Q}}/\mathbf{Q}), E_{d,p}).$$

Take an element $\widetilde{\Phi}$ in $H^1(G(\overline{\mathbf{Q}}/\mathbf{Q}), E_{d,p})$ with

$$\mathrm{res}\ \widetilde{\Phi} = \phi \in \mathrm{Hom}_{G(L_d/\mathbf{Q})}(G(\overline{\mathbf{Q}}/L_d), E_{d,p})$$

and denote by M the fixed field of the kernel of ϕ. $M/\mathbf{Q}$ is normal, and $G(M/L_{-d})$ is generated by two elements α_1, α_2 with $\alpha_i^p = \mathrm{id}$, which we may choose in such a way that

$$\Phi(\alpha_1) = \mu_1 P,\ \phi(\alpha_2) = \mu_2 Q.$$

We may also assume that $\mu_i = 1$ if $\alpha_i \neq \mathrm{id}$.

We extend $\delta, \gamma, \epsilon \in G(L_{-d}/\mathbf{Q})$ to elements $\tilde{\delta}, \tilde{\gamma}, \tilde{\epsilon} \in G(M/\mathbf{Q})$ and compute the actions of these elements on α_i. We assume that $\tilde{\delta}^2 = \tilde{\gamma}^{p-1} = \mathrm{id}$. Since

$$\phi(\beta\alpha_i\beta^{-1}) = \beta\phi(\alpha_i) \quad \text{for all } \beta \in G(M/\mathbf{Q})$$

we get:

$$\begin{aligned}
\tilde{\delta}\alpha_i\tilde{\delta} &= \alpha_i^{-1} && (\text{since } \tilde{\delta}|E_{d,p} = -\mathrm{id}),\\
\tilde{\gamma}\alpha_1\tilde{\gamma}^{-1} &= \alpha_1 && (\text{since } \tilde{\gamma}P = P),\\
\tilde{\gamma}\alpha_2\tilde{\gamma}^{-1} &= \alpha_2^{\chi_p(\tilde{\gamma})} && (\text{since } \tilde{\gamma}Q = \chi_p(\tilde{\gamma})Q),\\
\tilde{\epsilon}\alpha_1\tilde{\epsilon}^{-1} &= \alpha_1 && (\text{since } \tilde{\epsilon}P = P), \text{ and}\\
\tilde{\epsilon}\alpha_2\tilde{\epsilon}^{-1} &= \alpha_1\alpha_2 && \text{if } \epsilon \neq \mathrm{id} \text{ and } \alpha_2 \neq \mathrm{id} \text{ (since then } \epsilon\phi(\alpha_2) =\\
&&& \epsilon Q = P + Q = \phi(\alpha_1\alpha_2); \text{ necessarily } \alpha_1 \neq \mathrm{id}\\
&&& \text{in this case).}
\end{aligned}$$

In particular it follows that $\langle\alpha_1\rangle$ is a normal subgroup of $G(M/\mathbf{Q})$ and that $\langle\alpha_2\rangle$ is normal if either $\alpha_2 = \mathrm{id}$ or $\epsilon = \mathrm{id}$.

Now we distinguish two cases:

Case 1. $\epsilon = \mathrm{id}$. In this case $\langle\alpha_1\rangle$ and $\langle\alpha_2\rangle$ are both normal in $G(M/\mathbf{Q})$ and hence

$$M_i := M^{\langle\alpha_i\rangle}$$

are normal extensions of $\mathbf{Q}$. The Galois group of $M_2/\mathbf{Q}(\sqrt{d})$ is abelian and generated by the restriction of $\langle\tilde{\gamma}, \alpha_1\rangle$ to M_2. Hence

$$\bar{M}_2 := M^{\langle\alpha_2,\tilde{\gamma}\rangle}$$

is Galois over $\mathbf{Q}$ containing $\mathbf{Q}(\sqrt{d})$ and if $\alpha_1 \neq \mathrm{id}$ then $G(\bar{M}_2/\mathbf{Q})$ is non abelian of order $2p$. Since

$$\tilde{\delta}\tilde{\gamma}^{(p-1)/2}\alpha_2\tilde{\gamma}^{(p-1)/2}\tilde{\delta} = \alpha_2$$

it follows that M_1 is abelian over K and hence

$$\bar{M}_1 := M^{\langle\alpha_1,\tilde{\delta}\tilde{\gamma}^{(p-1)/2}\rangle}$$

is normal over $\mathbf{Q}$. Its Galois group is generated by

$$\bar{\alpha}_2 = \alpha_2|\bar{M}_1 \text{ and } \bar{\gamma} = \tilde{\gamma}|\bar{M}_1,$$

its order is equal to order $(\alpha_2) \cdot (p - 1)$, and one has the relation

$$\overline{\gamma\alpha\gamma}^{-1} = \bar{\alpha}_2^{\chi_p(\tilde{\gamma})}.$$

Case 2. order $(\epsilon) = p$. In this case we may assume that $\alpha_1 \neq \mathrm{id}$, for $\alpha_1 = \mathrm{id}$ implies that $\alpha_2 = \mathrm{id}$, too.

Subcase (i). $\alpha_2 = \mathrm{id}$. We assert that $G(M/\mathbf{Q}(\zeta_p, \sqrt{d}))$ is not cyclic.

https://doi.org/10.4153/CJM-1988-028-9 Published online by Cambridge University Press

Otherwise $\tilde{\epsilon}$ would be an element of order p^2 with $\tilde{\epsilon}^p = \alpha_1$ (without loss of generality). So $\tilde{\delta}\tilde{\epsilon}^p\tilde{\delta} = \tilde{\epsilon}^{-p}$ and hence

$$\tilde{\delta}\tilde{\epsilon}\tilde{\delta} = \tilde{\epsilon}^k \text{ with } k \equiv -1 \text{ modulo } p.$$

But since $\delta\epsilon\delta = \epsilon$ we would get

$$\delta\tilde{\epsilon}\delta = \tilde{\epsilon} \cdot (\tilde{\epsilon}^p)^l = \tilde{\epsilon}^{(1+p^l)}$$

which gives a contradiction. Hence we can choose $\tilde{\epsilon}$ so that

$$\tilde{\epsilon}^p = \tilde{\alpha}_1^p = \text{id and } \tilde{\delta}\tilde{\epsilon}\tilde{\delta} = \tilde{\epsilon}.$$

(This determines $\tilde{\epsilon}$ uniquely.) $\bar{M}_2 := M^{\langle \epsilon, \tilde{\gamma} \rangle}$ is normal over $\mathbf{Q}$, contains $\mathbf{Q}(\sqrt{d})$ and its Galois group is dihedral of order $2p$.

Subcase (ii). $\alpha_2 \neq \text{id}$. $M_1 := M^{\langle \alpha_1 \rangle}$ is normal over $\mathbf{Q}$ and of degree p over L_d. Since

$$\tilde{\delta}\alpha_2\tilde{\delta} = \alpha_2^{-1}$$

we conclude as above that ϵ has an extension $\tilde{\epsilon}$ to M_1 of order p with

$$\tilde{\delta}\tilde{\epsilon}\tilde{\delta} = \tilde{\epsilon}.$$

Since $\tilde{\delta}\tilde{\gamma}^{(p-1)/2}$ acts trivially on α_2 and $\tilde{\epsilon}$ acts trivially on $\alpha_2|M_1$,

$$\langle \tilde{\delta}\tilde{\gamma}^{(p-1)/2}, \tilde{\epsilon} \rangle$$

is a normal subgroup of $G(M_1/\mathbf{Q})$. So

$$\bar{M}_1 := M_1^{\langle \tilde{\delta}\tilde{\gamma}^{(p-1)/2}, \tilde{\epsilon} \rangle}$$

is normal over $\mathbf{Q}$ containing K, and its Galois group over K is generated by $\bar{\alpha}_2 = \alpha_2|\bar{M}_1$ which is of order p and satisfies the relation

$$\bar{\gamma}\bar{\alpha}_2\bar{\gamma}^{-1} = \bar{\alpha}_2^{\chi_p(\tilde{\gamma})} \text{ with } \bar{\gamma} = \tilde{\gamma}|K.$$

In order to simplify notation we define:

$$\bar{M}_2(\phi) := \mathbf{Q}(\sqrt{d})$$

if either $\epsilon \neq \text{id}$ or $\alpha_2 \neq \text{id}$.

Hence for a given

$$\phi \in H^1(G(\bar{\mathbf{Q}}/\mathbf{Q}), E_{d,p})$$

we have a field $M = M(\phi)$ which determines $\langle \phi \rangle$ completely. What information do we get from the pair $(\bar{M}_1(\phi), \bar{M}_2(\phi))$? If $\epsilon = \text{id}$ or if $\alpha_2 = \text{id}$ then of course we get $M(\phi)$ back from $(\bar{M}_1(\phi), \bar{M}_2(\phi))$. In these cases we shall say that Φ is of first type. What happens if $\epsilon \neq \text{id}$ and $\alpha_2 \neq \text{id}$? Assume that

$$\phi \neq \tilde{\phi} \in H^1(G(\bar{\mathbf{Q}}/\mathbf{Q}), E_{d,p})$$

have the fields $M(\phi)$ and $M(\tilde{\phi})$ with Galois groups $\langle \alpha_1, \alpha_2 \rangle$ resp. $\langle \tilde{\alpha}_1, \tilde{\alpha}_2 \rangle$ as above such that

$$M(\phi)^{\langle\alpha_1\rangle} = M(\tilde{\phi})^{\langle\tilde{\alpha}_1\rangle}.$$

Let N be the composite of $M(\phi)$ and $M(\tilde{\phi})$. Then the Galois group $G(N/L_d)$ is generated by three elements $\langle\alpha'_1, \alpha'_2, \alpha'_3\rangle$ which we can choose in such a way that

$$\alpha'_2|M(\phi) = \alpha_2,\ \alpha'_2|M(\tilde{\phi}) = \tilde{\alpha}_2^{\lambda}$$

with $\lambda \in \{1, \ldots, p-1\}$ and

$$\alpha'_1|M(\phi) = \alpha_1,\ \alpha'_1|M(\tilde{\phi}) = \alpha_1^{\lambda}.$$

N is a splitting field for ϕ and $\tilde{\phi}$, and

$$(\phi - \lambda^{-1}\tilde{\phi})(\alpha'_1) = 0 = (\phi - \lambda^{-1}\tilde{\phi})(\alpha'_2).$$

Hence the fixed field of the kernel of $\phi - \lambda\tilde{\phi}$ is a cyclic extension of L_d which is normal over $\mathbf{Q}$, and $\phi - \lambda^{-1}\tilde{\phi}$ is of first type. Hence $\bar{M}_1(\phi)$ determines $\langle\phi\rangle$ up to elements of first type, and in order to determine all elements in

$$H^1(G(\bar{\mathbf{Q}}/\mathbf{Q}), E_{d,p}),$$

it is enough to determine all dihedral extensions of $\mathbf{Q}$ of degree $2p$ containing $\mathbf{Q}(\sqrt{d})$ and all extensions M_1 of degree p over K which are normal over $\mathbf{Q}$ such that conjugation by $\bar{\gamma}$ on $G(\bar{M}_1/K)$ is equal to $\chi_p(\bar{\gamma})$.

To prove the theorem one has to show that for $\phi \in S(E_d, \mathbf{Q})_p$ the field $\bar{M}_2(\phi)$ is unramified over $\mathbf{Q}(\sqrt{d})$ outside $\tilde{S}_E$, and $\bar{M}_1(\phi)$ is unramified over K outside $S_E \cup \{p\}$ and little ramified at divisors of p, and this we will do step by step in the next section.

(3) *Splitting fields of elements in* $S(E_d, \mathbf{Q})_p$. We continue to use the assumptions and the notations of the theorem.

LEMMA 3. *Let ϕ be an element in $S(E_d, \mathbf{Q})_p$. Then $\bar{M}_1(\phi) =: \bar{M}_1$ is unramified outside of $S_E \cup \{p\}$ over K and $\bar{M}_2(\phi) =: \bar{M}_2$ is unramified outside $\tilde{S}_E \cup \{p\}$ over $\mathbf{Q}(\sqrt{d})$.*

Proof. We have to test prime numbers $q \neq p$ that divide N_E.

(i) If $q = 2$ then $d \equiv 3 \bmod 4$ and so $\mathbf{Q}(\sqrt{d})$ and K are ramified at 2 over $\mathbf{Q}$. Hence the norm of $\mathfrak{q}|2$ in $\mathbf{Q}(\sqrt{d})$ is equal to 2 and so $\mathbf{Q}(\sqrt{d})$ has no cyclic extension of degree p in which $\mathfrak{q}$ ramifies, and the same argument can be applied to $\mathfrak{q}_K|2$ over K for $p = 3$ and 5. Now take $p = 7$. By assumption 2 has only one extension $\mathfrak{q}_K$ to K which is ramified of order 2 and has norm 8. Assume that $\mathfrak{q}_K$ is ramified in $\bar{M}_1|K$ and let $\mathfrak{q}_{\bar{M}_1}$ be the unique extension of $\mathfrak{q}_K$ to $\bar{M}_1$. Let M_t be the subfield of $\bar{M}_1$ in which $\mathfrak{q}_{\bar{M}_1}$ is tamely ramified. Then M_t is a cyclic extension of degree 7 of $\mathbf{Q}(\zeta_7 + \zeta_7^{-1})$, and $\bar{M}_1$ is the composite of M_t with K over $\mathbf{Q}(\zeta_7 + \zeta_7^{-1})$; hence

https://doi.org/10.4153/CJM-1988-028-9 Published online by Cambridge University Press

$$G(\bar{M}_1/\mathbf{Q}(\zeta_7 + \zeta_7^{-1}))$$

is abelian. But this contradicts the fact that

$$\bar{\gamma}^3\bar{\alpha}\bar{\gamma}^3 = \bar{\alpha}^{\chi_7(\bar{\gamma}^3)} = \bar{\alpha}^{-1}$$

where $\langle\bar{\alpha}\rangle = G(\bar{M}_1/K)$ and $\langle\bar{\gamma}\rangle = G(K/\mathbf{Q})$. So we can assume that $q \nmid 2p$ but $q|N_E$.

(ii) If $v_q(j_E) \geqq 0$ it follows from Néron's list of minimal models of elliptic curves with potentially good reduction that p has to be equal to 3 ([**4**], p. 124). By assumption we have $(d/q) = -1$. If $q \equiv 1 \bmod 3$ then $(-3d/p) = -1$ too, and hence extensions of $\mathbf{Q}(\sqrt{d})$ resp. $K = \mathbf{Q}(\sqrt{-3d})$ which are normal over $\mathbf{Q}$ with Galois group S_3 have to be unramified in divisors of q for

$$\mathbf{Q}_q^*/\mathbf{Q}_q^{*3} \cong \mathbf{Q}_q(\sqrt{d})^*/(\mathbf{Q}_q(\sqrt{d}))^{*3} \cong \mathbf{Q}_q(\sqrt{-3d})^*/(\mathbf{Q}_q(\sqrt{-3d})^*)^3.$$

If $q \equiv -1 \bmod 3$ we see that $q \in \tilde{S}_E$ for E has bad reduction modulo q but good reduction modulo all divisors of q over L_d, whence

$$v_q(\Delta_E) \equiv 4 \text{ modulo } 12.$$

Since $(-3d/q) = 1$ the norm of $\mathfrak{q}_K|q$ is congruent to $-1 \bmod 3$ and so $K_\mathfrak{q}$ has no ramified extension of degree 3.

(iii) Now we assume that $v_q(j_E) < 0$. If

$$v_q(j_E) \equiv 0 \bmod p$$

we have that $q \notin S_E$ and so E_d is not a Tate curve over $\mathbf{Q}_q$. Moreover, $\mathbf{Q}_q(E_p)$ is unramified over $\mathbf{Q}_q$ and hence $\bar{M}_1/K$ and $\bar{M}_2/\mathbf{Q}(\sqrt{d})$ are unramified at all divisors of q if and only if M_1/L_d resp. M_2/L_d are unramified at all divisors of q.

Now we use the triviality of ϕ over $\mathbf{Q}_q$. There is a $\tilde{Q} \in E_d(M_\mathfrak{q})$ (where $\mathfrak{q}_M|q$) such that for all σ in the decomposition group of $\mathfrak{q}_M$ we have $\sigma\tilde{Q} - \tilde{Q} = \phi(\sigma)$. Hence

$$Q' := p \cdot \tilde{Q} \in E_d(\mathbf{Q}_q)$$

and so $2 \cdot Q'$ is in the connected component of the unity modulo q. Hence $\tilde{Q} = \tilde{Q}_1 + Q_2$ with $Q_2 \in E_{d,p}$ and $2\tilde{Q}_1$ in the component of the unity of $E \bmod \mathfrak{q}_M$, so $\tilde{Q}_1$ corresponds to a $\mathfrak{q}_M$-adic unit u under the Tate parametrization. Now take

$$\alpha \in \langle\alpha_1, \alpha_2\rangle I_{\mathfrak{q}_M}$$

($I_{\mathfrak{q}_M}$ the inertia group of $\mathfrak{q}_M$). Then $2(\alpha\tilde{Q} - \tilde{Q})$ corresponds to $\alpha u/u$ and is a pth root of unity. Since $q \neq p$ we conclude that $\alpha u/u = 1$ and hence $\alpha = \mathrm{id}$. So $\mathfrak{q}_M$ is unramified over L_d.

If $v_q(j_E) \not\equiv 0 \bmod p$ it follows that either $q \equiv 1 \bmod p$ and E is a Tate curve over $\mathbf{Q}_q$, or that $q \equiv -1 \bmod p$ and then $q \in S_E$. Consider the first possibility. We have $(d/q) = -1$ and so q is not completely decomposed in $\mathbf{Q}(\sqrt{d})$ and K. Since

$$\mathbf{Q}_q^*/\mathbf{Q}_q^{*p} \cong \mathbf{Q}_q(\sqrt{d})^*/\mathbf{Q}_q(\sqrt{d})^{*p} = K_{\mathfrak{q}}/K_{\mathfrak{q}}^{*p}$$

for $\mathfrak{q}_K|q$ we see that for all cyclic extensions $\bar{M}_1$ of $\mathbf{Q}(\sqrt{d})$ and $\bar{M}_2/K$ of degree p and divisors $\mathfrak{q}_{M_i}$ of q, one has that $G(\bar{M}_{i,\mathfrak{q}}/\mathbf{Q}_q)$ is abelian of even order. But this implies that

$$\bar{M}_{1,\mathfrak{q}} = \mathbf{Q}_q(\sqrt{d}) \quad \text{and} \quad \bar{M}_{2,\mathfrak{q}} = K_{\mathfrak{q}},$$

and we have proven the lemma.

The next step is to describe the behaviour of $\bar{M}_i$ at divisors of p.

LEMMA 4. *Assume that $v_p(j_E) < 0$ and $\phi \in S(E_d, \mathbf{Q})_p$. Then $\bar{M}_2$ is unramified at p and $\bar{M}_1/K$ is little ramified at divisors of p.*

Proof. The assumptions imposed on E imply that $E/\mathbf{Q}_p$ is a Tate curve but that $E_d/\mathbf{Q}_p$ is not a Tate curve. Since

$$\mathbf{Q}_p(E_p) = \mathbf{Q}_p(\zeta_p)$$

the behaviour of $\bar{M}_i$ at p is determined by the behaviour of M at p. So let $\mathfrak{p}_M|p$ and let $I_{\mathfrak{p}_M}$ be the inertia group of $\mathfrak{p}_M$. Take

$$\alpha \in \langle \alpha_1, \alpha_2 \rangle \cap I_{\mathfrak{p}_M}.$$

As in the proof of Lemma 3 we can use the fact that $E_d/\mathbf{Q}_p$ is not a Tate curve to show that $\phi(\alpha) = \alpha\tilde{Q} - \tilde{Q}$ where $2\tilde{Q}$ is in the connected component of the unity of E_d modulo $\mathfrak{q}_M$. This gives

$$M_{\mathfrak{p}} = M_{\mathfrak{p}}^{\langle\alpha\rangle}(\sqrt[p]{u})$$

where u is a $\mathfrak{p}_M$-adic unit corresponding to $2\tilde{Q}$ under Tate's parametrization, and so in particular M_1/L_d is little ramified.

Now assume moreover that $\alpha_2 = \text{id}$ or $\epsilon = \text{id}$. Then $\bar{M}_2/\mathbf{Q}(\sqrt{d})$ is of degree p. We have to show that $\bar{M}_2/\mathbf{Q}(\sqrt{d})$ is unramified at $\mathfrak{p}_{\bar{M}_2}|p$. We recall the choice of the point Q. Since

$$\gamma Q = \chi_p(\gamma)Q \text{ and } \langle\gamma\rangle = G(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$$

it follows that Q is in the kernel of the reduction of E modulo all divisors of p, and hence $P + \lambda Q$ is not in this kernel. But for $\alpha \in I_{\mathfrak{p}_M}$ we saw that $\phi(\alpha) = \alpha\tilde{Q} - \tilde{Q}$ is in the kernel of the reduction modulo $\mathfrak{p}_M$ and hence

$$\alpha_1\alpha_2^\lambda \notin I_{\mathfrak{p}_M} \quad \text{for all } \lambda \in \mathbf{N} \text{ and } \mathfrak{p}_M|p.$$

It follows that $M^{\langle\alpha_2\rangle}/L_d$ is unramified at $\mathfrak{p}_M$ and hence $\bar{M}_2/\mathbf{Q}(\sqrt{d})$ is unramified at p.

Next we look at the case that $v_p(j_E) \geqq 0$. First let us assume $p > 3$.

LEMMA 5. *Assume that $E/\mathbf{Q}$ has a point P of order $p > 3$ rational over $\mathbf{Q}$, that $v_p(j_E) \geqq 0$ and that P is not in the kernel of the reduction modulo p. (If $p \nmid N_E$ this always holds.) Let ϕ be an element in $S(E_d, \mathbf{Q})_p$ with corresponding fields $\bar{M}_1$ and $\bar{M}_2$. Then $\bar{M}_1/K$ is little ramified at p, and $\bar{M}_2/\mathbf{Q}(\sqrt{d})$ is unramified at p.*

Proof. Let N be an extension field of $\mathbf{Q}(\zeta_p)$ such that E has good reduction modulo all primes $\mathfrak{p}_N | p$ and such that

$$[N:\mathbf{Q}(\zeta_5)]\,|3 \quad \text{for } p = 5 \quad \text{and}$$

$$[N:\mathbf{Q}(\zeta_7)]\,|2 \quad \text{for } p = 7.$$

From our assumptions it follows that $N_{\mathfrak{p}}$ contains $\mathbf{Q}(E_p)$ and that $\langle Q \rangle$ is the subgroup of order p of the kernel of the reduction modulo $\mathfrak{p}_N$. Hence all divisors of p are decomposed in $\mathbf{Q}(E_p)/\mathbf{Q}(\zeta_p)$ and so again we can prove the lemma by looking at the behaviour of p in M/L_d.

So assume that $\mathfrak{p}_M | p$ and let $I_{\mathfrak{p}_M}$ be the inertia group of $\mathfrak{p}_M$. Assume that

$$\alpha_1^{\mu}\alpha_2^{\lambda} \in I_{\mathfrak{p}_M}.$$

Then there is a $\widetilde{Q} \in E(M_{\mathfrak{p}})$ with

$$(\alpha_1^{\mu}\alpha_2^{\lambda})\widetilde{Q} - \widetilde{Q} = \mu P + \lambda Q.$$

But we know that for $\mu \neq 0$ the point $\mu P + \lambda Q$ is not in the kernel of the reduction modulo $\mathfrak{p}_M$ and since

$$(I_{\mathfrak{p}_M} - \mathrm{id})\widetilde{E}(N \cdot M_{\mathfrak{p}})$$

is contained in this kernel ($\widetilde{E}$ is a model of E over N having good reduction modulo $\mathfrak{p}_M | p$) we must have $\mu = 0$ and hence

$$I_{\mathfrak{p}_M} \cap G(M/L_d) \subset \langle \alpha_2 \rangle.$$

So $M^{\langle \alpha_2 \rangle}/L_d$ is unramified at $\mathfrak{p}_M$ and hence $\bar{M}_2/\mathbf{Q}(\sqrt{d})$ is unramified at all divisors of p.

Now assume that $I_{\mathfrak{p}_M} = \langle \alpha_2 \rangle$. Then $Q = \alpha_2\widetilde{Q} - \widetilde{Q}$ and since $\langle \alpha_2 \rangle$ acts trivially on $\widetilde{E}(N \cdot M_{\mathfrak{p}})/\widetilde{E}_{-}(N \cdot M_{\mathfrak{p}})$ we may assume that

$$\widetilde{Q} \in \widetilde{E}_{-}(N \cdot M_{\mathfrak{p}})$$

and hence

$$p \cdot \widetilde{Q} \in \widetilde{E}_{-}(N \cdot Q_p).$$

$\widetilde{E}$ has ordinary reduction modulo $\mathfrak{p}_M$, and so Lutz's parametrization of $\widetilde{E}_{-}$ shows that $N \cdot \mathbf{Q}_p(\widetilde{Q})$ is little ramified at divisors of p, and the lemma follows.

Now we come to $p = 3$ to end the proof of the theorem.

LEMMA 6. *Assume that E has a point of order 3 rational over $\mathbf{Q}$ and that $v_p(j_E) \geqq 0$. Assume moreover that either P is not contained in the kernel of the reduction modulo p or that E is given by the equation $y^2 = x^3 + 1$. Let d be a square free integer prime to 3, and ϕ an element in $S(E_d, \mathbf{Q})_3$ with corresponding fields $\bar{M}_i$. Then $\bar{M}_1/\mathbf{Q}(\sqrt{-3d})$ is little ramified at 3 and $\bar{M}_2/\mathbf{Q}(\sqrt{d})$ is unramified at 3.*

Proof. Assume at first that E is not given by $y^2 = x^3 + 1$. Since E is not supersingular modulo 3 it follows that

$$v_3(j_E) = 0 = 3 + 3v_3(g_2) - v_3(\Delta_E)$$

and hence $v_3(\Delta_E) \equiv 0 \bmod 3$ and E has good reduction over $\mathbf{Q}(\sqrt[4]{-3})$. Since P is not contained in the kernel of the reduction modulo 3 we have

$$\mathbf{Q}_3(E_3) \subset \mathbf{Q}_3(\sqrt{-3})$$

and hence 3 is decomposed in $\mathbf{Q}_3(E_3)/\mathbf{Q}_3(\zeta_3)$. Again we only have to look at the behaviour of 3 in M/L_d, and by repeating the argument of Lemma 4 we get the desired result.

Now assume that E is given by $y^2 = x^3 + 1$. Then E has good reduction modulo prime divisors of 3 in $\mathbf{Q}(\sqrt[4]{-3})$. An equation $\widetilde{E}$ with good reduction is obtained by the transformation

$$x' := \frac{x + d}{\sqrt{-3}}, \quad y' = \frac{y}{(\sqrt[4]{-3})^3}.$$

Since $L_d = \mathbf{Q}(\zeta_3, \sqrt{2})$ we have that $\epsilon \neq \mathrm{id}$. So $\bar{M}_2|\mathbf{Q}(\sqrt{d})$ is nontrivial only if $\alpha_2 = \mathrm{id}$. Assume, therefore, to begin with, that $\alpha_2 = \mathrm{id}$. Then

$$\phi = \inf_M^{\bar{M}_2}(\bar{\phi})$$

with

$$\bar{\phi} \in H^1(G(\bar{M}_2/\mathbf{Q}), \langle P \rangle)$$

determined by $\bar{\phi}(\bar{\alpha}_1) = P$. Hence $\bar{\phi}$ is an element of $S(E_d, \mathbf{Q})_3$ with splitting field $\bar{M}_2$, and for $\mathfrak{p}_{\bar{M}_2}|3$ there is a point $\widetilde{Q} \in E_d(\bar{M}_{2,\mathfrak{p}})$ with $\bar{\alpha}_1\widetilde{Q} - \widetilde{Q} = P$ if $\mathfrak{p}_{\bar{M}_2}$ is ramified. Assume that $\widetilde{Q}$ has coordinates (x', y') satisfying

$$y'^2 = x'^3 + d^3.$$

Adding $(-d, 0)$ if necessary, we may assume that

$$v_{\mathfrak{p}_{\bar{M}_2}}(x' + d) \leqq 0.$$

The coordinates of $\widetilde{Q}$ with respect to $\widetilde{E}$ are

$$(\bar{x}, \bar{y}) := \left(\frac{x' + d}{\sqrt{-3}}, \frac{y'}{(\sqrt[4]{-3})^3}\right)$$

and hence $\widetilde{Q}$ is in the kernel of the reduction modulo $\mathfrak{p}_{N\cdot\bar{M}_2}|3$ and since

$$v_{\mathfrak{p}_{N\cdot\bar{M}_2}}(\bar{x}) \leqq v_{\mathfrak{p}_{N\cdot\bar{M}_2}}(x' + d) - v_{\mathfrak{p}_{N\cdot\bar{M}_2}}(\sqrt{-3})$$

the level of $\widetilde{Q}$ with respect to the Lutz parametrization of $\widetilde{E}_-$, is at least equal to the level of P given by coordinates

$$\left(\frac{d}{\sqrt{-3}}, \frac{(\sqrt{d})^3}{(\sqrt[4]{-3})^3}\right).$$

We obtain a contradiction and so $\mathfrak{p}_{\bar{M}_2}$ is unramified over $\mathbf{Q}(\sqrt{d})$. Now let us consider the case $\alpha_2 \neq \mathrm{id}$. We must show that

$$\bar{M}_1(\zeta_3) = \mathbf{Q}(\sqrt{d}, \zeta_3)(\sqrt[3]{u})$$

with u a $\mathfrak{p}$-adic unit for all $\mathfrak{p}|3$.

Definition. Let L be a number field, $\mathfrak{p}_L$ a prime divisor and π_L a uniformizing element of $\mathfrak{p}_L$. Let σ be an element in $\mathrm{Aut}(L/\mathbf{Q})$ with $\sigma\mathfrak{p}_L = \mathfrak{p}_L$. Then

$$f_{\mathfrak{p}_L}(\sigma) := v_{\mathfrak{p}_L}(\sigma\pi_L - \pi_L).$$

We see that our assertion is equivalent to the inequality

$$v_{\mathfrak{p}_{M'}}(\alpha_2') \leqq 4$$

for all prime divisors $\mathfrak{p}_{M'}$ of $M' := M_1^{\langle\tilde{\epsilon}\rangle}$ which divide 3 and for $\alpha_2' = \alpha_2|M'$. We begin with a prime $\mathfrak{p}_{M(\sqrt[4]{-3})}$ of $M(\sqrt[4]{-3})$ dividing 3 and with $\tilde{\alpha}_2\tilde{\alpha}_1^\lambda$ generating

$$G(M(\sqrt[4]{-3})/M^{\langle\alpha_2\alpha_1^\lambda\rangle}(\sqrt[4]{-3})).$$

Assertion 1.

$$f_{\mathfrak{p}_{M(\sqrt[4]{-3})}}(\tilde{\alpha}_2\tilde{\alpha}_1^\lambda) \leqq 9 \text{ if } \tilde{\alpha}_2\tilde{\alpha}_1^\lambda \in I_{\mathfrak{p}_{M(\sqrt[4]{-3})}}.$$

Assume that this is true. By a formula which can be found in [**6**, p. 71], one gets, with

$$\mathfrak{p}_{M_1(\sqrt[4]{-3})} = \mathfrak{p}_{M(\sqrt[4]{-3})}|M_1(\sqrt[4]{-3}) \quad \text{and} \quad \alpha_2^0 = \tilde{\alpha}_2|M_1(\sqrt[4]{-3}),$$

$$f_{\mathfrak{p}_{M_1(\sqrt[4]{-3})}}(\alpha_2^0) = \frac{1}{3}\left(\sum_{\lambda=0}^{2} f_{\mathfrak{p}_{M(\sqrt[4]{-3})}}(\tilde{\alpha}_2\tilde{\alpha}_1^\lambda)\right) \leqq 9.$$

Using this formula again we get, by restriction to M_1,

$$f_{\mathfrak{p}_{M_1}}(\bar{\alpha}_2) \leqq \frac{1}{2}(9 + 1) = 5.$$

Assertion 2. $f_{\mathfrak{p}_{M_1}}(\tilde{\epsilon}) = 2$.

Assuming that this is true and again using the formula mentioned above, we get, with $\mathfrak{p}_{M'} = \mathfrak{p}_{M_1}|M'$,

$$f_{\mathfrak{p}_{M'}}(\alpha_2') \leqq \frac{1}{3}(5 + 2 + 2) \leqq 3.$$

This completes the proof of the lemma except for Assertions 1 and 2.

Proof of Assertion 1. The point $Q + \lambda P$ is in the kernel of the reduction modulo $\mathfrak{p}_{M(\sqrt[4]{-3})} =: \tilde{\mathfrak{p}}$ and has a level equal to the order of the ramification of this prime in

$$M(\sqrt[4]{-3})/L_d(\sqrt[4]{-3})$$

which divides 9.

Assuming that $\tilde{\alpha}_1^\lambda \tilde{\alpha}_2$ is in the ramification group of $\tilde{\mathfrak{p}}$ we have that

$$Q + \lambda P = \tilde{\alpha}_2 \tilde{\alpha}_1^\lambda \tilde{Q} - \tilde{Q} \quad \text{with } \tilde{Q} \in \tilde{E}_-(M(\sqrt[4]{-3})_{\tilde{\mathfrak{p}}}).$$

If

$$v_{\tilde{\mathfrak{p}}}(\pi_{\tilde{\mathfrak{p}}} - \tilde{\alpha}_2 \tilde{\alpha}_1^\lambda \pi_{\tilde{\mathfrak{p}}}) =: \tilde{f}$$

one sees at once that the level of $\tilde{\alpha}_2 \tilde{\alpha}_1^\lambda Q' - Q'$ is at most equal to (level of Q') + $\tilde{f}$ for all

$$Q' \in \tilde{E}_-(M(\sqrt[4]{-3})_{\tilde{\mathfrak{p}}});$$

hence $\tilde{f}$ has to be $\leqq 9$ in our case, and this proves Assertion 1.

Proof of Assertion 2. Since $L_d = \mathbf{Q}(\sqrt{d}, \zeta_3)(\sqrt[3]{2})$ one has

$$f_{\mathfrak{p}_{L_d}}(\epsilon) = 2$$

and one obtains by the formula used several times already,

$$2 = \frac{1}{3}(f_{\mathfrak{p}_{M_1}}(\tilde{\epsilon}) + f_{\mathfrak{p}_{M_1}}(\tilde{\epsilon}\overline{\alpha}_2) + f_{\mathfrak{p}_{M_1}}(\tilde{\epsilon}\overline{\alpha}_2^2)).$$

Since

$$f_{\mathfrak{p}_{M_1}}(\tilde{\epsilon}\overline{\alpha}_2) = f_{\mathfrak{p}_{M_1}}(\tilde{\epsilon}\overline{\alpha}_2^2) \geqq 2$$

the only possibility is

$$2 = f_{\mathfrak{p}_{M_1}}(\tilde{\epsilon}) = f_{\mathfrak{p}_{M_1}}(\tilde{\epsilon}\overline{\alpha}_2) = f_{\mathfrak{p}_{M_1}}(\tilde{\epsilon}\overline{\alpha}_2^2),$$

and this proves Assertion 2.

References

1. G. Frey, *A relation between the value of the L-series of the curve $y^2 = x^3 - k^3$ in $s = 1$ and its Selmer group*, Archiv der Math. *45* (1985), 232-238.
2. E. Lutz, *Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques*, J. reine angew. Math. *177* (1937), 238-247.
3. B. Mazur, *On the arithmetic of special values of L-functions*, Invent. Math. *55* (1979), 207-240.
4. A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Inst. Hautes Études Sci. Publ. Math. *21* (1964).
5. P. Roquette, *Analytic theory of elliptic functions over local fields*, Hamburger Mathematische Einzelschriften (Neue Folge), Heft *1* (Vandenhoech and Ruprecht, Göttingen, 1970).
6. J. P. Serre, *Corps locaux* (Hermann, Paris, 1962).

Universität des Saarlandes,
Saarbrücken, West Germany