On the Tate–Shafarevich group of semistable elliptic curves with a rational 3-torsion

by

Noboru Aoki (Tokyo)

1. Introduction. Let $E$ be an elliptic curve defined over the rational number field $\mathbb{Q}$ and $E(\mathbb{Q})$ the Mordell–Weil group of $\mathbb{Q}$-rational points on $E$. Let $n$ be an integer greater than one and $E_n$ the group of $n$-torsion points on $E$. The $n$-Selmer group $\text{Sel}^{(n)}(E/\mathbb{Q})$ of $E/\mathbb{Q}$ is defined to be the kernel of the composite map

$$H^1(\mathbb{Q}, E_n) \to \prod_p H^1(\mathbb{Q}_p, E_n) \to \prod_p H^1(\mathbb{Q}_p, E),$$

where the first map is the direct product of restriction maps for all places $p$ of $\mathbb{Q}$ and the second map is the one induced from the inclusion $E_n \hookrightarrow E$. Then $\text{Sel}^{(n)}(E/\mathbb{Q})$ is known to be finite for any $n$, and there is an injection from the quotient group $E(\mathbb{Q})/nE(\mathbb{Q})$ into $\text{Sel}^{(n)}(E/\mathbb{Q})$. Thus $\text{Sel}^{(n)}(E/\mathbb{Q})$ gives an upper bound for the rank of $E(\mathbb{Q})$. Therefore, if rank$(E(\mathbb{Q}))$ is unbounded when $E$ varies over the elliptic curves over $\mathbb{Q}$, then the order of $\text{Sel}^{(n)}(E/\mathbb{Q})$ with $n$ fixed can be arbitrarily large. The converse, however, is not necessarily true because of the presence of the Tate–Shafarevich group

$$\text{III}(E/\mathbb{Q}) = \text{Ker} \left( H^1(\mathbb{Q}, E) \to \prod_p H^1(\mathbb{Q}_p, E) \right).$$

The $n$-torsion subgroup $\text{III}(E/\mathbb{Q})_n$ of $\text{III}(E/\mathbb{Q})$ fits into the exact sequence

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to \text{Sel}^{(n)}(E/\mathbb{Q}) \to \text{III}(E/\mathbb{Q})_n \to 0.$$

Thus we are naturally led to the following problem: Given a prime number $n$ and a family $\mathcal{E}$ of elliptic curves over $\mathbb{Q}$, determine whether

$$\sup\{ \#(\text{III}(E/\mathbb{Q})_n) \mid E \in \mathcal{E} \} = \infty$$

or not. This problem has been studied for $n = 2$ by Bölling [3], Kramer [8], Lemmermeyer [9] and Atake [1], for $n = 3$ by Cassels [6], and for $n = 5$ by Fisher [7]. The families of elliptic curves considered in those works may

2000 Mathematics Subject Classification: 11G05, 11G07, 14H52.
be divided into two types: one is the family of (quadratic ([3], [9], [1]) or cubic ([6])) twists of a fixed elliptic curve, and the other is a one-parameter family of semistable elliptic curves with non-constant \( j \)-invariant ([8], [7]).

In this paper we will be mainly interested in two types of elliptic curves:

\[
E = E_{(a,b)} : \quad y^2 + axy + by = x^3,
\]

\[
F = F_{(a,b)} : \quad y^2 + axy + by = x^3 - 5abx - a^3b - 7b^2,
\]

where \( a, b \) are relatively prime non-zero integers such that \( a^3 - 27b \neq 0 \). One can easily see that \( E \) has a rational point \( S = (0, 0) \in E(\mathbb{Q}) \) of order 3, and \( F \) is the quotient of \( E \) by the cyclic subgroup \( \langle S \rangle \) generated by \( S \). We consider the problem above for \( n = 3 \) and the family of such elliptic curves \( F_{a,b} \). We should remark that the assumption on \( a \) and \( b \) ensures that \( E \) and \( F \) are semistable elliptic curves, and so CM elliptic curves are excluded from our family in contrast to the work of Cassels mentioned above, where he treated the CM elliptic curves \( x^3 + y^3 + dz^3 = 0 \). The purpose of this paper is to prove the following theorem.

**Theorem 1.1.** Let \( \mathcal{E} \) be the set of elliptic curves \( F_{(a,b)} \) defined above. Then

\[
\sup \{ \#(\mathrm{III}(F/\mathbb{Q})_3) \mid F \in \mathcal{E} \} = \infty.
\]

In the proof of Theorem 1.1 we will assume that \( a^3 - 27b \) is a prime number and \( b \) is not a cube in \( \mathbb{Q} \), hence neither \( E_3 \) nor \( F_3 \) splits over \( \mathbb{Q} \). (Note that the discriminants of our curves are given by \( \Delta_E = (a^3 - 27b)b^3 \) and \( \Delta_F = (a^3 - 27b)^3b \).) Therefore we cannot use the method of [4] and [7] to prove Theorem 1.1. We will instead compute a restriction of the Cassels–Tate pairing to a subgroup of \( \mathrm{III}(F/\mathbb{Q}(E_3)) \) using McCallum’s formula (see Theorem 6.5). This part was strongly influenced by the recent work of Beaver [2] and Fisher [7].

**2. The Selmer group and the Tate–Shafarevich group.** Let \( n \) be a positive integer greater than one. Let \( E \) be an elliptic curve defined over a number field \( k \). Suppose \( E(k) \) contains a point \( S \) of order \( n \) and let \( F = E/\langle S \rangle \) be the quotient of \( E \) by the cyclic group generated by \( S \). Then \( F \) is also defined over \( k \) and the natural surjection \( \varphi : E \to F \) is a \((k\text{-rational})\) cyclic \( n \)-isogeny such that \( E_\varphi := \text{Ker}(\varphi) = \langle S \rangle \). Since \( S \) is rational over \( k \), we have \( E_\varphi \cong \mathbb{Z}/n\mathbb{Z} \) as \( \text{Gal}(\overline{k}/k) \)-modules. Let \( \psi : F \to E \) be the dual isogeny of \( \varphi \). Then \( F_\psi := \text{Ker}(\psi) \) is isomorphic to \( \mu_n \) as a \( \text{Gal}(\overline{k}/k) \)-module.

Now, let \( L \) be a field containing \( k \) and consider the exact sequence

\[
0 \to F_\psi \to F \xrightarrow{\psi} E \to 0
\]

of \( \text{Gal}(\overline{L}/L) \)-modules. Taking Galois cohomology, we obtain the exact sequence
Let $M_k$ be the set of places of $k$. For each $v \in M_k$, we denote by $k_v$ the completion of $k$ at $v$. Taking $k_v$ for $L$, we then obtain the exact sequence

$$0 \to E(k_v)/\psi(F(k_v)) \xrightarrow{\delta_v^{(\psi)}} H^1(k_v, F_\psi) \to H^1(L, F_\psi) \to 0,$$

where $\delta_v^{(\psi)} = \delta_{k_v}^{(\psi)}$. Let $\text{res}_v : H^1(k, \ast) \to H^1(k_v, \ast)$ denote the restriction map. We define the $\psi$-Selmer group by

$$\text{Sel}^{(\psi)}(F/k) = \text{Ker} \left( H^1(k, F_\psi) \prod_{v \in M_k} H^1(k_v, F_\psi) \to \prod_{v \in M_k} H^1(k_v, F) \right)$$

$$= \{ x \in H^1(k, F_\psi) | \text{res}_v(x) \in \text{Im}(\delta_v^{(\psi)}) \text{ for all } v \in M_k \}.$$ 

Since $F_\psi \cong \mu_n$, Kummer theory implies that $H^1(k, F_\psi) \cong \mathbb{k}^\times/k^\times n$. In what follows we will identify $H^1(k, F_\psi)$ with $\mathbb{k}^\times/k^\times n$ by this isomorphism. Thus $\text{Sel}^{(\psi)}(F/k)$ may be viewed as a subgroup of $\mathbb{k}^\times/k^\times n$. The following proposition will be useful when we give an explicit description of $\text{Im}(\delta_k^{(\psi)})$.

**Proposition 2.1.** There exists a rational function $f \in k(E)^\times$ such that

$$\text{div}(f) = n((S) - (O)) \quad \text{and} \quad f \circ [n] \in (k(E)^\times)^n,$$

where $[n]$ denotes the multiplication-by-$n$ map. Then

$$\delta_k^{(\psi)}(P) \equiv f(P) \pmod{\mathbb{k}^\times n}$$

for any $P \in E(k) \setminus \{O, S\}$.

**Proof.** See [13, Chapter X, Theorem 1.1].

Define the Tate–Shafarevich group of $F/k$ by

$$\text{III}(F/k) = \text{Ker} \left( H^1(k, F) \to \prod_{v \in M_k} H^1(k_v, F) \right).$$

It is conjectured that $\text{III}(F/k)$ is finite. Let

$$\langle \ , \ \rangle : \text{III}(F/k) \times \text{III}(F/k) \to \mathbb{Q}/\mathbb{Z}$$

be the Cassels–Tate pairing on $\text{III}(F/k)$. (See [5], [15] or [11] for the definition.) It is well known that this pairing is non-degenerate if and only if the divisible part of $\text{III}(F/k)$ is trivial. Let $\text{III}(F/k)_\psi$ be the kernel of the map $\text{III}(F/k) \to \text{III}(E/k)$ induced from $\psi$, and let

$$\langle \ , \ \rangle_\psi : \text{III}(F/k)_\psi \times \text{III}(F/k)_\psi \to \frac{1}{n} \mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$$
be the restriction of $\langle \ , \ \rangle$ to the subgroup $\text{III}(F/k)_\psi$. The group $\text{III}(F/k)_\psi$ fits into the exact sequence

$$0 \to E(k)/\psi(F(k)) \xrightarrow{\delta_k^{(\psi)}} \text{Sel}^{(\psi)}(F/k) \to \text{III}(F/k)_\psi \to 0.$$ 

Pulling back the pairing to $\text{Sel}^{(\psi)}(F/k)$ using the surjection $\text{Sel}^{(\psi)}(F/k) \to \text{III}(F/k)_\psi$, we obtain a pairing on $\text{Sel}^{(\psi)}(F/k)$, which we denote by the same symbols:

$$\langle \ , \ \rangle_\psi : \text{Sel}^{(\psi)}(F/k) \times \text{Sel}^{(\psi)}(F/k) \to \mathbb{Z}/n\mathbb{Z}.$$ 

In Section 6 we will prove an explicit formula for the pairing $\langle \ , \ \rangle_\psi$ when $E$ is a semistable elliptic curve satisfying a certain condition on the discriminant of $E$.

### 3. Tate curves.

Let $p$ be a prime number. Throughout this section $k$ will denote a $p$-adic field, that is, a finite extension of $\mathbb{Q}_p$. Let $v$ denote the valuation of $k$ such that $v(k^\times) = \mathbb{Z}$ and $q$ a non-zero element of $k$ with $v(q) > 0$. Let $E = E_q$ be the Tate curve over $k$ defined by the equation

$$y^2 + xy = x^3 + a_4(q)x + a_6(q),$$

where $a_4(q)$ and $a_6(q)$ are convergent power series in $k[[u]]$ defined by

$$a_4 = -\sum_{n=1}^\infty \frac{n^4q^n}{1-q^n}, \quad a_6 = -\frac{1}{12} \left(5 \sum_{n=1}^\infty \frac{n^3q^n}{1-q^n} + 7 \sum_{n=1}^\infty \frac{n^5q^n}{1-q^n}\right).$$

(For more details on the Tate curve see [14, Chapter V].) Then we have an isomorphism of $\text{Gal}(\overline{k}/k)$-modules called the Tate parametrization:

$$\tau : \overline{k}^\times/q\mathbb{Z} \to E(\overline{k}), \quad u \mapsto (X(u), Y(u)),$$

where $X(u)$ and $Y(u)$ are convergent power series in $k[[u]]$ defined by

$$X(u) = \frac{u}{(1-u)^2} + \sum_{n=1}^\infty \left( \frac{q^n u}{(1-q^nu)^2} + \frac{q^n u^{-1}}{(1-q^nu^{-1})^2} - 2 \frac{q^n}{(1-q^n)^2} \right),$$

$$Y(u) = \frac{u^2}{(1-u)^3} + \sum_{n=1}^\infty \left( \frac{(q^n u)^2}{(1-q^nu)^3} - \frac{q^n u^{-1}}{(1-q^nu^{-1})^3} + \frac{q^n}{(1-q^n)^2} \right).$$

Let $n$ be a prime number, and fix an $n$th root of unity $\zeta \in \mu_n$ and an $n$th root $q_1 = q^{1/n}$ of $q$ in $\overline{k}$. Then for any $P \in E_n$, we define two elements $\mu(P)$ and $\nu(P)$ of $\mathbb{Z}/n\mathbb{Z}$ by

$$\tau(\zeta^{\mu(P)} q_1^{\nu(P)}) = P.$$ 

Clearly both $\mu$ and $\nu$ are homomorphisms from $E_n$ to $\mathbb{Z}/n\mathbb{Z}$.

Now, let $S$ be a $k$-rational point of $E$ of order $n$. As in the preceding section we consider the quotient $F$ of $E$ by the cyclic subgroup generated by $S$ and the cyclic isogeny $\psi : F \to E$. 
PROPOSITION 3.1. Let $\delta_k^{(\psi)} : E(k) \to H^1(k, F_\psi) = k^\times/k^{\times n}$ be the map defined in (1). Then
\[
\text{Im}(\delta_k^{(\psi)}) = \begin{cases} 
  k^\times/k^{\times n} & \text{if } \nu(S) \neq 0, \\
  \{1\} & \text{if } \nu(S) = 0.
\end{cases}
\]

This fact is well known; for example it is proved in [2] in the case of $n = 5$ and the proof works for any $n$. However, we will give another proof using an explicit description of the rational function $f$ defined in Proposition 2.1. This proof is a generalization of that of Brumer and Kramer [4], where the case $n = 2$ is treated. We consider the following theta function:
\[
\theta(u) = (1 - u) \prod_{n=1}^{\infty} \frac{(1 - q^nu)(1 - q^n u^{-1})}{(1 - q^n)^2} \quad (u \in \bar{k}^\times).
\]

LEMMA 3.2. Let $x_1, \ldots, x_r \in \bar{k}^\times$ and $m_0, m_1, \ldots, m_r \in \mathbb{Z}$. Let $f$ be a function on $\bar{k}^\times$ defined by
\[
f(u) = u^{-m_0} \prod_{i=1}^{r} \theta(u/x_i)^{m_i} \quad (u \in \bar{k}^\times).
\]

Then the equation $f(qu) = f(u)$ holds for all $u \in \bar{k}^\times$ if and only if the following two conditions are satisfied:
\[
\sum_{i=1}^{r} m_i = 0 \quad \text{and} \quad \prod_{i=1}^{r} x_i^{m_i} = q^{m_0}.
\]

Moreover, if these conditions are satisfied (hence $f \circ \tau^{-1}$ may be viewed as a rational function on the Tate curve $E$), then the divisor of the rational function $f$ on $E$ is given by
\[
div(f \circ \tau^{-1}) = \sum_{i=1}^{r} m_i(\tau(x_i)).
\]

Proof. See [12, §1, Proposition 1].

Proof of Proposition 3.1. We want to construct a rational function $f$ on $E$ which satisfies the condition of Proposition 2.1. Let $\mu = \mu(S), \nu = \nu(S)$ and define a function $f$ on $E$ by
\[
f(\tau(u)) = u^{-\nu} \left( \frac{\theta(\zeta^{-\mu} q_1^{-\nu} u)}{\theta(u)} \right)^n \quad (u \in \bar{k}^\times).
\]

Then Lemma 3.2 implies that $f$ is a rational function on $E$ defined over $k$ such that $\text{div}(f) = n((S) - (O))$. Moreover, we define a function $g$ on $E$ by
\[
g(\tau(u)) = u^{-\nu} \frac{\theta(\zeta^{-\mu} q_1^{-\nu} u^n)}{\theta(u^n)}.
\]
Then \( g \) is also a rational function on \( E \) defined over \( k \) and satisfies the relation

\[
f(\tau(u^n)) = g(\tau(u))^n.
\]

Therefore \( f \circ [n] = g^n \), so \( f \) satisfies the condition in Proposition 2.1. Hence

\[
\delta^{(\psi)}_k(\tau(u)) \equiv f(\tau(u)) \equiv u^{-v} \pmod{k^x}
\]

for all \( u \in k^x \). Proposition 3.1 now easily follows from (7).

In the next proposition we identify \( \mathbb{Z}/n\mathbb{Z} \) with the subset \( \{0, 1, \ldots, n-1\} \) of \( \mathbb{Z} \). Thus we regard \( \nu(P) \) as an integer such that \( 0 \leq \nu(P) < n \).

**Proposition 3.3.** Suppose \( q_1 \in k \). Let \( f \in k(E)^x \) be the rational function on \( E \) defined by (6). Then for any \( P \in E(k)[O, S] \), \( v(f(P)) \) is given by the formula

\[
v(f(P)) = -(\nu(S)\nu(P) - n\max\{\nu(S) - \nu(P), 0\})v(q_1) - \delta_{\nu(S),\nu(P)}v(1 - \zeta),
\]

where \( \delta_{*,*} \) denotes Kronecker’s delta.

**Proof.** For any \( \alpha, \beta \in \overline{k}^x \), we write \( \alpha \sim \beta \) if \( v(\alpha/\beta) = 0 \). Take \( u, z \in \overline{k}^x \) such that \( \tau(u) = S, \tau(z) = P \). Clearly one can take \( u, z \) so that \( 0 \leq v(u), v(z) < v(q) \). Then by (6) we have

\[
f(P) = z^{-\nu(S)} \left( \frac{\theta(u^{-1}z)}{\theta(z)} \right)^n.
\]

Since \( v(z) = \nu(P)v(q_1) \), this shows that

\[
v(f(P)) = -\nu(S)\nu(P)v(q_1) + n \cdot v\left( \frac{\theta(u^{-1}z)}{\theta(z)} \right).
\]

To calculate the second term, notice that \(-v(q) < v(z/u) < v(q)\) and \( 0 \leq v(z) < v(q) \). Hence \( 1 - q^n(z/u)^{\pm1} \sim 1 \) and \( 1 - q^nz^{\pm1} \sim 1 \) for all \( n \geq 1 \). Thus

\[
\frac{\theta(u^{-1}z)}{\theta(z)} \sim \frac{1 - u^{-1}z}{1 - z}.
\]

First, suppose \( \nu(P) \neq 0 \). Then \( 1 - z \sim 1 \) and

\[
1 - u^{-1}z \sim \begin{cases} 
1 & \text{if } \nu(P) > \nu(S), \\
u^{-1}z & \text{if } \nu(P) < \nu(S), \\
1 - \zeta & \text{if } \nu(P) = \nu(S).
\end{cases}
\]

Here we have used the fact that \( 1 - \zeta^s \sim 1 - \zeta \) for any \( 0 < s < n \). Therefore,

\[
v\left( \frac{\theta(u^{-1}z)}{\theta(z)} \right) = -\max\{\nu(S) - \nu(P), 0\}v(q_1) + \delta_{\nu(S),\nu(P)}v(1 - \zeta).
\]

From (8) and (9) we obtain the desired formula.
Next, suppose $\nu(P) = 0$. Then $\mu(P) \neq 0$, hence $1 - z \sim 1 - \zeta^{\mu(P)} \sim 1 - \zeta$. Moreover, if $\nu(P) = 0$, then $\mu(S) \neq \mu(P)$, and

$$1 - u^{-1}z \sim \begin{cases} u^{-1} & \text{if } \nu(S) \neq 0, \\ 1 - \zeta & \text{if } \nu(S) = 0. \end{cases}$$

Therefore,

$$v\left( \frac{\theta(u^{-1}z)}{\theta(z)} \right) = -\max\{\nu(S), 0\}v(q_1) + \delta_{\nu(S),0}v(1 - \zeta). \tag{10}$$

From (8) and (10), we find that the formula of the proposition also holds in this case. This completes the proof. □

**Corollary 3.4.** Suppose $n$ is a prime and $q_1 \in k$. If $v(n) = 0$, then $v(f(P))$ is divisible by $v(q_1)$ and the integer $v(f(P))/v(q_1)$ satisfies the congruence

$$\frac{v(f(P))}{v(q_1)} \equiv -\nu(S)v(P) \pmod{n}.$$ 

Further, if $v(n) > 0$ and $v(q_1) \not\equiv 0 \pmod{n}$ (hence $v(q_1)$ is an $n$-adic unit), then the same congruence holds.

**Proof.** If $v(n) = 0$, then Proposition 3.3 implies that

$$v(f(P)) = -[\nu(S)v(P) + n \cdot \max\{\nu(S) - \nu(P), 0\}]v(q_1).$$

Hence the assertion of the proposition holds. If $v(n) > 0$ and $v(q_1) \not\equiv 0 \pmod{n}$, then $v(q_1)$ is an $n$-adic unit, hence we get the congruence of the proposition again. □

### 4. The Selmer group of a semistable elliptic curve.

We return to the situation where $k$ is a number field. In the remainder of this paper we will assume that $n$ is an odd prime number. Let $M_{k,0}$ denote the set of prime ideals of $k$. For any $\alpha \in k^\times$ let $\Sigma_k(\alpha)$ denote the set of prime ideals $\mathfrak{p}$ of $k$ such that $\text{ord}_\mathfrak{p}(\alpha) \neq 0$. Let $E$ be a semistable elliptic curve defined over $k$. Thus $\Sigma(E/k) := \Sigma_k(\Delta_E)$ is the set of bad prime ideals for $E$. We assume that $E$ has split multiplicative reduction at every prime in $\Sigma(E/k)$. For $\mathfrak{p} \in \Sigma(E/k)$, let $q = q_\mathfrak{p}$ be a non-zero element of $k_\mathfrak{p}$ with $\text{ord}_\mathfrak{p}(q) > 0$ such that $E$ is isomorphic to the Tate curve $E_q/k_\mathfrak{p}$ defined by (3). We fix an isomorphism $\phi_\mathfrak{p} : E_q \to E$. We write $\mu_\mathfrak{p}$, $\nu_\mathfrak{p}$ and $\tau_\mathfrak{p}$ for $\mu$, $\nu$ and $\tau$ defined in the previous section for $E_q/k_\mathfrak{p}$. Let

$$A_k = \{ \mathfrak{p} \in \Sigma(E/k) \mid \nu_\mathfrak{p}(S) \neq 0 \}, \quad B_k = \Sigma(E/k) \setminus A_k.$$ 

Consider the following condition:

$$\Sigma_k(n) \subset \Sigma(E/k). \tag{11}$$

Clearly this is equivalent to requiring that $\text{ord}_\mathfrak{p}(\Delta_E) > 0$ for all $\mathfrak{p} \in \Sigma_k(n)$.
For any subset $X$ of $M_{k,0}$, we define a subgroup $V(X)$ of $k^\times/k^{\times n}$ by

$$V(X) = \{ x \in k^\times/k^{\times n} \mid \text{ord}_p(x) \equiv 0 \pmod{n} \ (\forall p \in M_{k,0} \setminus X) \}.$$  

Moreover, if $Y$ is another subset of $M_{k,0}$ such that $X \cap Y = \emptyset$, we define a subgroup $V(X, Y)$ of $k^\times/k^{\times n}$ by

$$V(X, Y) = \{ x \in V(X) \mid x = 1 \in k_p^\times/k_p^{\times n} \ (\forall p \in Y) \}.$$  

**Proposition 4.1.** If the condition (11) holds, then

$$\text{Sel}^{(\psi)}(F/k) = V(A_k, B_k).$$  

**Proof.** Let $x \in k^\times/k^{\times n}$. Then $x$ belongs to $\text{Sel}^{(\psi)}(F/k)$ if and only if $x \in \text{Im}(\delta_p^{(\psi)})$ for all $p \in M_k$. Since we are assuming that $n$ is odd, it is not necessary to consider the local condition at infinite places. If $p$ is a finite place not in $\Sigma(E/k)$ and therefore not dividing $n$, then it is well known that $\text{Im}(\delta_p^{(\psi)}) = \mathcal{O}_p^\times / \mathcal{O}_p^{\times n} \subset k_p^\times/k_p^{\times n}$, where $\mathcal{O}_p$ denotes the integer ring of $k_p$. This shows that $\text{Sel}^{(\psi)}(F/k)$ is a subgroup of $V(\Sigma(E/k))$. If $p \in \Sigma(E/k)$, then $E$ has split multiplicative reduction at $p$, and so by Proposition 3.1 we have

$$\text{Im}(\delta_p^{(\psi)}) = \begin{cases} k_p^\times/k_p^{\times n} & \text{if } p \in A_k, \\ \{1\} & \text{if } p \in B_k. \end{cases}$$

Therefore the equality $\text{Sel}^{(\psi)}(F/k) = V(A_k, B_k)$ holds. \(\blacksquare\)

**Corollary 4.2.** Assume that the condition (11) holds. If $Np \not\equiv 1 \pmod{n}$ for all $p \in B_k$, then

$$\text{Sel}^{(\psi)}(F/k) = V(A_k).$$  

**Proof.** Let $x \in V(A_k)$. Then $\text{res}_p(x) \in \mathcal{O}_p^\times/\mathcal{O}_p^{\times n}$ for any $p \in B_k$. But, since $n$ is a prime number, the assumption that $Np \not\equiv 1 \pmod{n}$ implies that $\mathcal{O}_p^{\times n} = \mathcal{O}_p^\times$. Therefore, $x = 1$ in $k_p^\times/k_p^{\times n}$. This proves that $V(A_k) \subset \text{Sel}^{(\psi)}(F/k)$. Thus the assertion follows from Proposition 4.1. \(\blacksquare\)

We will henceforth assume that $k$ contains $\mu_n$. For any $p \in M_{k,0} \setminus \Sigma_k(n)$ and $x \in k$ with $\text{ord}_p(x) = 0$, let $(\overline{x})_n$ be the $n$th power residue symbol, namely $(\overline{x})_n$ is the $n$th root of unity such that

$$\left( \frac{x}{p} \right)_n \equiv x^{(Np-1)/n} \pmod{p}.$$  

Note that $(\overline{x})_n = 1$ if and only if $x \in \mathcal{O}_p^{\times n}$. Thus the following corollary immediately follows from Proposition 4.1.

**Corollary 4.3.** Assume that $k$ contains $\mu_n$ and the condition (11) holds. Then

$$\text{Sel}^{(\psi)}(F/k) = \left\{ x \in V(A_k) \mid \left( \frac{x}{p} \right)_n = 1 \ (\forall p \in B_k) \right\}.$$
Now, we will give an explicit description of the set $A_k$. For this purpose, divide the set $\Sigma(E/k)$ into two subsets:

$\Sigma^{(1)}(E/k) = \{ p \in \Sigma(E/k) \mid \text{ord}_p(\Delta_E) \not\equiv 0 \pmod{n} \}$,

$\Sigma^{(2)}(E/k) = \{ p \in \Sigma(E/k) \mid \text{ord}_p(\Delta_E) \equiv 0 \pmod{n} \}$.

Let $f_S$ be a rational function on $E$ satisfying the condition of Proposition 3.1. For any $p \in \Sigma(E/k)$ let $f_{p,S}$ denote the rational function on $E$ defined by (6). Since two rational functions $\phi_p^*(f_S)$ and $f_{p,S}$ on $E$ have the same divisor, they differ only by non-zero constant multiple:

$$\phi_p^*(f_S) = c_p f_{p,S} \quad (c_p \in k_p^\times).$$

But in view of Proposition 2.1 the commutative diagram

$$
\begin{array}{ccc}
E(k) & \xrightarrow{\delta_k^{(\psi)}} & H^1(k, F_\psi) \\
\downarrow & & \Downarrow \cong \\
E(k_p) & \xrightarrow{\delta_k^{(\psi)}} & H^1(k_p, F_\psi)
\end{array}
$$

shows that $c_p \in k_p^\times$. Hence, when we compute $\text{Im}(\delta_k^{(\psi)})$, we may use $f_S$ instead of $f_{p,S}$.

Let $P \in E_n \setminus \{O, S\}$. Then the above remark shows that

$$\text{ord}_p(\phi_p^*(f_S(P))) = \text{ord}_p(f_{p,S})$$

for any $p \in \Sigma(E/k)$. For each $p \in \Sigma^{(2)}(E/k)$, define the rational number

$$i_p(S, P) = \frac{\text{ord}_p(f_S(P))}{1/n \text{ord}_p(\Delta_E)}.$$

Consider the following condition:

(12) $\text{ord}_p(\Delta_E) \not\equiv 0 \pmod{n}$ for all $p \in \Sigma_k(n)$.

Obviously (12) implies (11).

**Proposition 4.4.** Assume that $k$ contains $\mu_n$ and the condition (12) holds. Then for any prime $p \in \Sigma(E/k)$ the following assertions hold:

(i) If $p \in \Sigma^{(1)}(E/k)$, then $\nu_p(S) = 0$.

(ii) If $p \in \Sigma^{(2)}(E/k) \setminus \Sigma_k(n)$ (resp. $p \in \Sigma_k(n)$), then $i_p(S, P)$ is an integer (resp. an $n$-adic integer) and the congruence

$$i_p(S, P) \equiv -\nu_p(S)\nu_p(P) \pmod{n}$$

holds for any $P \in E(k)_n \setminus \{O, S\}$.

**Proof.** If $\text{ord}_p(\Delta_E) \not\equiv 0 \pmod{n}$, then $q_1 = q_1^{1/n}$ does not belong to $k_p$. Let $\sigma$ be an element of $\text{Gal}(k_p/k_p)$ such that $q_1^{\sigma} \neq q_1$. Since the Tate
parametrization $\tau_p$ is Galois equivariant and $S$ is $k$-rational, we have
\[
\tau_p(\zeta^\mu_p(S), q_1^\mu_p(S)) = \tau_p(\zeta^\mu_p(S), q_1^\sigma(S)).
\]
Hence $\nu_p(S)\tau_p(q_1^\sigma) = 0$. Since $q_1^\sigma$ is an $n$th root of unity other than 1, we have $\tau_p(q_1^\sigma) \neq 0$. Therefore, $\nu_p(S) = 0$. This proves (i).

To prove (ii), suppose that $\text{ord}_p(\Delta_E) \equiv 0 \pmod{n}$ and $p$ does not divide $n$. Then Corollary 3.4 shows that
\[
\text{ord}_p(f_{\tau(p)}(P)) \equiv -\nu_p(S)\nu_p(P) \pmod{n}.
\]
Since $\frac{1}{n} \text{ord}_p(\Delta_E) = \text{ord}_p(q_1)$, (ii) follows.

**Corollary 4.5.** Assume that $k$ contains $\mu_n$ and the condition (12) holds. Then
\[
A_k = \{ p \in \Sigma^{(2)}(E/k) \mid i_p(S, -S) \not\equiv 0 \pmod{n} \}.
\]

**Proof.** By Proposition 4.4(i), $A_k$ is a subset of $\Sigma^{(2)}(E/k)$. Let $p \in \Sigma^{(2)}(E/k)$. Applying Proposition 4.4(ii) for $P = -S$ and noticing that $\nu_p(-S) \equiv -\nu_p(S) \pmod{n}$, we obtain
\[
i_p(S, -S) \equiv \nu_p(S)^2 \pmod{n}.
\]
This implies that $p \in A_k$ if and only if $i_p(S, -S) \not\equiv 0 \pmod{n}$. The corollary then follows.

**5. The Cassels–Tate pairing.** We begin with a theorem proved by McCallum [10], which is fundamental in our calculation. It enables us to describe the Cassels–Tate pairing $\langle \cdot, \cdot \rangle_{\psi}$ defined in (2) in terms of the Hilbert norm residue symbol
\[
(\cdot, \cdot)_p : k_p^\times/k_p^{x_n} \times k_p^\times/k_p^{x_n} \to \mu_n
\]
of $k_p$.

**Theorem 5.1.** Suppose $E(k)_n \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and let $\{S, T\}$ be a basis of $E(k)_n$. Let $e_n$ denote the Weil pairing on $E_n$ and put $\zeta = e_n(S, T)$. Let $F = E/\langle S \rangle$ be the cyclic quotient of $E$ by the subgroup $\langle S \rangle$ generated by $S$. Let $x, x' \in \text{Sel}^{(\psi)}(F/k)$. For each $p \in M_k$ let $P_p \in E(k_p)$ be a local point such that $\text{res}_p(x) = \delta_{\psi}^p(P_p)$. Then
\[
\langle x, x' \rangle_{\psi} = \sum_{p \in M_k} \text{Ind}_\zeta(f_T(P_p), x')_p,
\]
where $\text{Ind}_\zeta : \mu_n \to \mathbb{Z}/n\mathbb{Z}$ denotes the isomorphism sending $\zeta \in \mu_n$ to $1 \in \mathbb{Z}/n\mathbb{Z}$ and $f_T$ is a rational function on $E$ defined in Proposition 2.1.

**Proof.** One can prove this in a quite similar way to [10, Theorem 1.4]. See also [2] and [7], where the case $n = 5$ is treated.
The Tate–Shafarevich group

The next theorem is proved by Beaver [2] when \( n = 5 \), but the proof works for general \( n \). Here we will give a proof based on the result in Section 2.

**Theorem 5.2.** Let the notation and assumption be as in Theorem 5.1. Suppose \( E/k \) (and hence \( F/k \)) is a semistable elliptic curve with split multiplicative reduction at every prime in \( \Sigma(E/k) \). Let \( A_k \) be as in Section 3 and assume that the condition (11) holds. For each \( p \in A_k \) put \( \lambda_p = \nu_p(T)/\nu_p(S) = \mathbb{Z}/n\mathbb{Z} \). Then for \( x, x' \in \text{Sel}^{(\psi)}(F/k) \) we have

\[
\langle x, x' \rangle_\psi = \sum_{p \in A_k} \lambda_p \text{Ind}_\xi(x, x')_p.
\]

**Proof.** Let \( \tau_p : \overline{k}_p^\times / q_p^\mathbb{Z} \to E(\overline{k}_p) \) be the Tate parametrization. For each \( p \in M_k \) there exists a point \( P_p \in E(k_p) \) such that \( \delta_p^{(\psi)}(P_p) = \text{res}_p(x) \). Choose \( u_p \in k_p^\times \) so that \( \tau_p(u_p) = P_p \). Then by the same argument as in the proof of Proposition 3.1 one can prove that

\[
f_T(P_p) = f_T(\tau_p(u_p)) \equiv u_p^{-\nu_p(T)} (\text{mod } k_p^\times n).
\]

Hence by Theorem 5.1 we have

\[
\langle x, x' \rangle_\psi = \sum_{p \in M_k} \text{Ind}_\xi(u_p^{-\nu_p(T)}, x')_p.
\]

If \( \nu_p(S) = 0 \), then \( \text{Im}(\delta_p^{(\psi)}) = \{1\} \) by Proposition 3.1, and so \( u_p^{-\nu_p(T), x'}_p = 1 \). If \( \nu_p(S) \neq 0 \), then \( u_p^{-\nu_p(T)} \equiv (u_p^{-\nu_p(S)})^{\lambda_p} (\text{mod } k_p^\times n) \). Therefore

\[
(u_p^{-\nu_p(T), x'}_p, x')_p = (u_p^{-\nu_p(S), x'}_p, x')_p = (x, x')_p^{\lambda_p}.
\]

The assertion now immediately follows from (13) and (14).

The following theorem shows that one can compute the value of \( \lambda_p \) once the values of the function \( f_S \) on \( E_n \) have been known.

**Theorem 5.3.** Let the notation and assumption be as in Theorem 5.1. Assume, in addition, that the condition (12) holds. Then for any \( p \in A_k \) the value of \( \lambda_p \) is given by the following formula:

\[
\lambda_p \equiv -i_p(S, T) i_p(S, -S) (\text{mod } n).
\]

**Proof.** Applying Proposition 4.4(ii) for \( P = T \), we obtain

\[
i_p(S, T) \equiv -\nu_p(S)\nu_p(T) (\text{mod } n).
\]

Since \( i_p(S, -S) \equiv \nu_p(S)^2 (\text{mod } n) \), it follows that

\[
\frac{i_p(S, T)}{i_p(S, -S)} \equiv -\lambda_p (\text{mod } n),
\]

which proves the theorem.
6. The case of \( n = 3 \). Let \( E \) be a semistable elliptic curve defined over \( \mathbb{Q} \) with a rational point \( S \) of order 3. After a change of coordinates, we may assume that \( S = (0,0) \) and \( E \) is defined by the Weierstra\ss equation

\[
y^2 + axy + by = x^3,
\]

where \( a \) and \( b \) are integers such that \( (a, b) = 1 \) and \( (a^3 - 27b)b \neq 0 \). The discriminant of \( E \) is given by \( \Delta_E = (a^3 - 27b)b^3 \), and \( E \) has split multiplicative reduction at every prime in \( \Sigma(E/\mathbb{Q}) = \Sigma_\mathbb{Q}((a^3 - 27b)b) \). Let \( k \) be a number field containing a cubic root of unity \( \zeta \). One can easily see that for any \( p \in \Sigma(E/k) \) our elliptic curve \( E \) considered over \( k_p \) is isomorphic to the Tate curve

\[
y^2 + xy = x^3 + \frac{b}{2a^3} x + \frac{b^2}{4a^6}
\]

with a non-zero element \( q = q_p \in k_p \) such that \( j(E_q) = j(E) \). The isomorphism \( \phi_p : E \to E_q \) is given by

\[
\phi_p((x, y)) = (a^2 x, a^3 y - b/2).
\]

Note that the rational function \( y \) on \( E \) has the divisor \( \text{div}(y) = 3((S) - (O)) \). Thus we can take \( y \) for the rational function \( f_S \) on \( E \).

Now, let \( F = E/\langle S \rangle \) be the quotient of \( E \) by the cyclic group generated by \( S \) and \( \varphi : E \to F \) the natural surjection. Then \( F \) is defined over \( \mathbb{Q} \) by

\[
y^2 + axy + by = x^3 - 5abx - a^3b - 7b^2.
\]

Let \( \psi : F \to E \) be the dual isogeny of the isogeny \( \varphi \).

**Proposition 6.1.** Let \( k \) be a number field containing \( \mu_3 \) and assume that \( \text{ord}_p(3) \neq 0 \mod 3 \) for all \( p \in \Sigma_k(3) \). Then \( A_k = \Sigma_k(b) \) and \( B_k = \Sigma_k(a^3 - 27b) \). Moreover the \( \psi \)-Selmer group \( \text{Sel}^{(\psi)}(F/k) \) is given by

\[
\text{Sel}^{(\psi)}(F/k) = V(\Sigma_k(b), \Sigma_k(a^3 - 27b)).
\]

**Proof.** The assumption on \( k \) ensures that the condition (12) is satisfied. Let \( p \in \Sigma^{(2)}(E/k) \). Since \( f_S(-S) = y(-S) = -b \), we have

\[
i_p(S, -S) = \frac{\text{ord}_p(b)}{3\text{ord}_p(\Delta_E)}.
\]

It follows that \( i_p(S, -S) = 1 \) or 0 according as \( p \) divides \( b \) or not. Therefore \( A_k = V_k(b) \) (hence \( B_k = V_k(a^3 - 27b) \)) by Corollary 4.5. Thus the proposition follows from Proposition 4.1.

**Corollary 6.2.** If every prime factor of \( a^3 - 27b \) is congruent to 2 modulo 3 and \( \text{ord}_3(b) \neq 0 \mod 3 \), then

\[
\text{Sel}^{(\psi)}(F/\mathbb{Q}) = V(\Sigma_\mathbb{Q}(b)).
\]

**Proof.** The assertion follows from Proposition 6.1 and Corollary 4.2.
Let $K = \mathbb{Q}(E_3)$. Then it is easy to see that $K = \mathbb{Q}(\sqrt[3]{-3}, \sqrt[3]{a^3 - 27b})$.

We remark that if $\text{ord}_3(b) \not\equiv 0 \pmod{3}$, then $\text{ord}_p(b) \not\equiv 0 \pmod{3}$ for all $p \in \Sigma_K(3)$ since the absolute ramification index of $p$ is 2.

**Corollary 6.3.** Assume that $\text{ord}_3(b) \not\equiv 0 \pmod{3}$. Then

$$\text{Sel}^{(\psi)}(F/K) = \left\{ x \in V(\Sigma_K(b)) \left| \left( \frac{x}{p} \right)_3 = 1 \text{ for all } p \in \Sigma_K(a^3 - 27b) \right\}.$$

**Proof.** The assertion follows from Proposition 6.1 and Corollary 4.3. ■

Put $\ell = a^3 - 27b$, hence $K = \mathbb{Q}(\sqrt[3]{-3}, \sqrt[3]{\ell})$. It is not hard to compute all the points of $E_3$ explicitly. First, note that

$$\langle S \rangle = \{O, (0, 0), (0, -b)\}.$$

The coordinates of the points of $E_3 \setminus \langle S \rangle$ are given as follows:

**Lemma 6.4.** Let $T$ be a point of order 3 which does not belong to $\langle S \rangle$. Then we have

$$T = \left( -\frac{(a - \omega \xi)(a - \omega^2 \xi)}{9}, -\frac{(a - \omega \xi)^2(a - \omega^2 \xi)}{27} \right),$$

where $\xi$ is a cubic root of $\ell$ and $\omega$ is a primitive cubic root of unity. (The number of possible choices of the pair $(\xi, \omega)$ is 6 = $\#(E_3 \setminus \langle S \rangle)$.)

**Proof.** Let $P \in E_3 \setminus \{O\}$. Then the $x$-coordinate $x(P)$ of $P$ is a root of the quadric equation

$$3x^4 + a^2x^3 + 3abx^2 + 3b^2x = 0.$$

The trivial root $x = 0$ of this equation corresponds to the points $S = (0, 0)$ and $2S = (0, -b)$. Thus $x(T)$ is a root of the cubic equation

$$3x^3 + a^2x^2 + 3abx + 3b^2 = 0.$$

Solving this equation, we obtain

$$x(T) = -\frac{3b}{a - \xi} = -\frac{(a - \omega \xi)(a - \omega^2 \xi)}{9}$$

with some $\xi$ such that $\xi^3 = \ell$. Here the second equality holds since

(18) $$27b = (a - \xi)(a - \omega \xi)(a - \omega^2 \xi).$$

Solving the quadratic equation $y^2 + (ax(T) + b)y - x(T)^3 = 0$, we obtain the description of the $y$-coordinate $y(T)$ of $T$ in the lemma. ■

In the following we fix $\xi$ and consider three (mutually disjoint) subsets $A^{(i)}_K$ ($i = 0, 1, 2$) of $A_K$ defined by

$$A^{(i)}_K = \{ p \in A_K \mid a \equiv \omega^i \xi \pmod{p^{e_p}} \},$$
where \( \varepsilon_p = 2 \) or 1 according as \( p \) divides 3 or not. If \( b \equiv 0 \pmod{3} \), then
\[ A_K = A_K^{(0)} \cup A_K^{(1)} \cup A_K^{(2)} \]
by (18).

**Theorem 6.5.** Suppose \( \text{ord}_3(b) \not\equiv 0 \pmod{3} \). Let \( x, x' \in \text{Sel}^{(\psi)}(F/K) \).
Then
\[ \langle x, x' \rangle_\psi = \sum_{p \in A_K^{(1)}} \text{Ind}_\zeta(x, x')_p + 2 \sum_{p \in A_K^{(2)}} \text{Ind}_\zeta(x, x')_p, \]
where \( \zeta = e_3(S, T) \).

**Proof.** It follows from Theorem 5.3 that
\[ \lambda_p \equiv \frac{\text{ord}_p(y(T))}{\text{ord}_p(b)} \pmod{3} \]
for all \( p \in A_K \). By Lemma 6.4 we have
\[ \text{ord}_p(y(T)) = 2 \text{ord}_p(a - \omega \xi) + \text{ord}_p(a - \omega^2 \xi). \]

First, suppose \( p \) does not divide 3. Then \( p \) does not divide simultaneously any two factors of the right hand side of (18). Therefore, if \( a \equiv \xi \pmod{p} \), then \( \text{ord}_p(a - \omega \xi) = \text{ord}_p(a - \omega^2 \xi) = 0 \). Hence \( \text{ord}_p(y(T)) = 0 \). If \( a \equiv \omega \xi \pmod{p} \), then \( \text{ord}_p(a - \xi) = \text{ord}_p(a - \omega^2 \xi) = 0 \). Hence
\[ \text{ord}_p(y(T)) = 2 \text{ord}_p(a - \omega \xi) = 2 \text{ord}_p(b). \]
Similarly, if \( a \equiv \omega^2 \xi \pmod{p} \), then \( \text{ord}_p(a - \xi) = \text{ord}_p(a - \omega \xi) = 0 \). Hence
\[ \text{ord}_p(y(T)) = \text{ord}_p(a - \omega \xi) = \text{ord}_p(b). \]
Consequently, if \( p \) does not divide 3, then
\[ \text{ord}_p(y(T)) = \begin{cases} 0 & \text{if } a \equiv \xi \pmod{p}, \\ 2 \text{ord}_p(b) & \text{if } a \equiv \omega \xi \pmod{p}, \\ \text{ord}_p(b) & \text{if } a \equiv \omega^2 \xi \pmod{p}. \end{cases} \]

Next, suppose \( p \) divides 3. Then \( \text{ord}_p(a - \omega^i \xi) > 0 \) for any \( i = 0, 1, 2 \) and equation (18) shows that
\[ \text{ord}_p(y(T)) = -6 + 2 \text{ord}_p(a - \omega \xi) + \text{ord}_p(a - \omega^2 \xi). \]
(Note that \( \text{ord}_p(3) = 3 \).) Moreover, one of the three factors \( a - \omega^i \xi \) \( (i = 0, 1, 2) \) of the right hand side of (18) is divisible by \( p^2 \) and the others are not. Therefore, if \( a \equiv \xi \pmod{p^2} \), then \( \text{ord}_p(a - \omega \xi) = \text{ord}_p(a - \omega^2 \xi) = 1 \). Hence \( \text{ord}_p(y(T)) = -3 \). If \( a \equiv \omega \xi \pmod{p^2} \), then \( \text{ord}_p(a - \xi) = \text{ord}_p(a - \omega^2 \xi) = 1 \). Hence
\[ \text{ord}_p(a - \omega \xi) = \text{ord}_p\left(\frac{27b}{(a - \xi)(a - \omega^2 \xi)}\right) = \text{ord}_p(b) + 4. \]
Therefore,
\[ \ord_p(y(T)) = 2(\ord_p(b) + 4) + 1 - 6 = 2\ord_p(b) + 3. \]
Similarly, if \( a \equiv \omega^2 \xi \pmod{p^2} \), then
\[ \ord_p(a - \omega^2 \xi) = \ord_p(b) + 4 \]
and \( \ord_p(a - \omega \xi) = 1 \). Hence
\[ \ord_p(y(T)) = 2 + \ord_p(b) + 4 - 6 = \ord_p(b). \]
Consequently, if \( p \) divides 3, then
\[ \ord_p(y(T)) = 2 + \ord_p(b) + 4 \]
\[ 6 = \ord_p(b). \]
By (20) and (21), for any \( p \in A_K^{(i)} \) \( (i = 0, 1, 2) \) we have
\[ \ord_p(y(T)) \equiv -i \cdot \ord_p(b) \pmod{3}. \]
It then follows from (19) that
\[ \lambda_p \equiv -i \pmod{3} \]
for any \( p \in A_K^{(i)} \). Moreover, if \( p \in M_{K,0} \setminus A_K \), then
\[ \ord_p(x) \equiv \ord_p(x') \equiv 0 \pmod{3}, \]
and so \( (x, x')_p = 1 \). Therefore
\[ \langle x, x' \rangle_\psi = \sum_{i=0}^{2} \sum_{p \in A_K^{(i)}} \Ind_\psi(x, x')_p. \]
This proves the theorem. \( \blacksquare \)

7. Proof of Theorem 1.1. We want to show that for a given positive integer \( r \) we can find two integers \( a \) and \( b \) with \( (a, b) = 1 \) and \( (a^3 - 27b)b \neq 0 \) for which
\[ \dim_{\mathbb{Z}/3\mathbb{Z}} \text{III}(F_{(a,b)}/\mathbb{Q})_3 \geq r. \]
Let \( \ell \) be an odd prime number with \( \ell \equiv -1 \pmod{9} \). Thus \( \ell \) remains prime in \( k := \mathbb{Q}(\sqrt{-3}) \). Let \( \xi \) be a cubic root of \( \ell \) in \( \overline{\mathbb{Q}} \) and put \( K = \mathbb{Q}(\sqrt{-3}, \xi) \). Since \( \ell \equiv -1 \pmod{9} \), \( \ell \) is a cube in \( \mathbb{Q}_3 \), hence \( \xi \in \mathbb{Q}_3 \). Moreover, by genus theory we know that the class number \( h \) of \( K \) is not divisible by 3, since the base field \( k \) has class number one and \( K/k \) is a cyclic extension of degree 3 unramified outside the prime ideal generated by \( \ell \).

We choose \( r \) prime numbers \( p_1, \ldots, p_r \) with \( p_i \equiv -1 \pmod{9} \) so that the unique prime ideal of \( k \) lying above \( p_i \) decomposes completely in \( K \). This is possible because \( \mathbb{Q}(\zeta_9) \cap K = k \). Let
\[ L = k(\sqrt[3]{p_1}, \ldots, \sqrt[3]{p_r}). \]
Then \( L/k \) is a Kummer extension whose Galois group may be described as follows: For each \( i \), we can naturally view \( \text{Gal}(k(\sqrt[3]{p_i})/k) \) as a subgroup of
Gal(L/k), and we have an isomorphism

$$\text{Gal}(L/k) \cong \prod_{i=1}^{r} \text{Gal}(k(\sqrt[3]{p_i})/k).$$

Choose and fix a primitive cubic root of unity $\omega$, and let $g_i$ be the generator of $\text{Gal}(k(\sqrt[3]{p_i})/k)$ such that

$$\sqrt[3]{p_i}^{g_i} = \omega \sqrt[3]{p_i}.$$  \hspace{1cm} (23)

**Lemma 7.1.** There exist prime ideals $q_1, \ldots, q_r$ of $K$ such that

$$\left(\frac{\xi}{q_j}\right)_3 = 1 \quad \text{and} \quad \left(\frac{p_i}{q_j}\right)_3 = \omega^{\delta_{ij}}$$

for all $i, j$, where $(\frac{\cdot}{3})$ denotes the cubic power residue symbol of $K$ and $\delta_{ij}$ denotes Kronecker’s delta.

**Proof.** The extension $KL/k$ is a Kummer extension of exponent 3. Since $\ell$ is relatively prime to $p_1, \ldots, p_r$, we have an isomorphism

$$\text{Gal}(KL/k) \cong \text{Gal}(K/k) \times \text{Gal}(L/k).$$

Therefore, by Chebotarev’s density theorem, there exist prime ideals $\Omega_1, \ldots, \Omega_r$ of $KL$ such that

$$\left\{ \begin{array}{l}
\text{Frob}_{KL/k}(\Omega_i)|_K = 1, \\
\text{Frob}_{KL/k}(\Omega_i)|_L = g_i.
\end{array} \right. \hspace{1cm} (24)$$

Let $q_i$ be the prime ideal of $K$ lying under $\Omega_i$. The first condition of (24) implies that $\text{Frob}_{K/k}(q_i) = 1$ since $\text{Frob}_{K/k}(q_i) = \text{Frob}_{KL/k}(\Omega_i)|_K$. This shows that $\left(\frac{\xi}{q_j}\right)_3 = 1$. Moreover the second condition of (24) implies that

$$\sqrt[3]{p_i}^{\text{Frob}_{KL/k}(\Omega_j)} = \omega^{\delta_{ij}} \sqrt[3]{p_i},$$

which is equivalent to $\left(\frac{p_i}{q_j}\right)_3 = \omega^{\delta_{ij}}$. Thus the prime ideals $q_1, \ldots, q_r$ have the desired properties.

Letting $p_i$ and $q_i$ be as above, choose an integer $a$ such that

$$\left\{ \begin{array}{l}
\text{ord}_3(a - \xi) = 3, \\
a \equiv \xi \pmod{p_1 \ldots p_r}, \\
a \equiv \omega \xi \pmod{q_1 \ldots q_r}.
\end{array} \right. \hspace{1cm} (25)$$

The existence of such an integer is ensured by the fact that $\xi \in \mathbb{Q}_3$ and the prime ideals $p_i, q_i$ $(i = 1, \ldots, r)$ decompose completely in $K$ for all $i$. Moreover the first condition of (25) shows that

$$\Sigma_K(3) \subset A^{(1)}_K.$$ 

Since $\text{ord}_p((a - \xi) - (a - \omega^i \xi)) = \text{ord}_p((\omega^i - 1)) = 1$ for any $p \in \Sigma_K(3)$ and $i = 1, 2$, this shows that $\text{ord}_p(a - \omega^i \xi) = 1$ for $i = 1, 2$. Therefore,
ord_p((a - \omega \xi)(a - \omega^2 \xi)) = 2. In particular, regarding (a - \omega \xi)(a - \omega^2 \xi) as an element of \mathbb{Q}_3, we have ord_3((a - \omega \xi)(a - \omega^2 \xi)) = 1. Hence the relation
\[ \text{ord}_3(a^3 - \ell) = \text{ord}_3(a - \xi) + \text{ord}_3((a - \omega \xi)(a - \omega^2 \xi)) \]
shows that ord_3(a^3 - \ell) = 4. Therefore, if we put
\[ b = \frac{a^3 - \ell}{27}, \]
then b is an integer such that (a, b) = 1 and ord_3(b) = 1.

Let \( E = E(a, b) \) and \( F = F(a, b) \) be two elliptic curves defined by the equation in (15) and (17) respectively. Then \( K \) coincides with \( \mathbb{Q}(E_3) \). Let \( S = (0, 0) \in E_3 \) and choose \( T \in E_3 \setminus \langle S \rangle \) so that \( e_3(S, T) = \omega \), where \( \omega \) is the primitive cubic root of unity defined in (23). We claim that
\[ \dim_{\mathbb{Z}/3\mathbb{Z}}(\text{III}(F/\mathbb{Q})_\psi) \geq r. \]
Since \( \text{III}(F/\mathbb{Q})_\psi \subset \text{III}(F/\mathbb{Q})_3 \), this proves the claim (22). To prove (26), let \( \beta_j \) be a generator of the principal ideal \( q_j^3 \) for each \( j = 1, \ldots, r \). (Recall that \( h \) is the class number of \( K \).) Before proving (26) itself, we prove a lemma.

**Lemma 7.2.** Let the notation be as above. Then \( p_1, \ldots, p_r \in \text{Sel}(\psi)(F/\mathbb{Q}) \) and \( \beta_1, \ldots, \beta_r \in \text{Sel}(\psi)(F/K) \).

**Proof.** Since \( \ell = a^3 - 27b \) is a prime number with \( \ell \equiv 2 \pmod{3} \), Corollary 6.2 shows that
\[ \text{Sel}(\psi)(F/\mathbb{Q}) = V(\Sigma_\mathbb{Q}(b)). \]
In particular, \( p_1, \ldots, p_r \in \text{Sel}(\psi)(F/\mathbb{Q}) \).

To prove the second statement, notice that \( K \supset \mu_3 \). Let \( I = (\xi) \) denote the unique prime ideal in \( K \) lying above \( \ell \). Then by Corollary 6.3 we have
\[ \text{Sel}(\psi)(F/K) = \left\{ x \in V(\Sigma_K(b)) \mid \left( \frac{x}{I} \right)_3 = 1 \right\}. \]
Thus, in order to prove that \( \beta_i \in \text{Sel}(\psi)(F/K) \), we have to show that \( \left( \frac{\beta_i}{I} \right)_3 = 1 \). But this is equivalent to \( (\xi, \beta_i)_I = 1 \). To compute \( (\xi, \beta_i)_I \), note that
\[ (\xi, \beta_i)_{q_i} = \left( \frac{\xi}{q_i} \right)_3^h = 1. \]
The first equality holds because \( \text{ord}_{q_3}(\xi) = 0 \) and \( \text{ord}_{q_i}(\beta_i) = h \), and the second one holds by Lemma 7.1. Moreover, since \( \xi \equiv -1 \pmod{9} \), we have \( (\xi, \beta_i)_p = 1 \) for all \( p \in \Sigma_K(3) \). Then the product formula implies that \( (\xi, \beta_i)_I = 1 \). This proves that \( \beta_i \in \text{Sel}(\psi)(F/K) \), completing the proof. \( \blacksquare \)

We return to the proof of (26). For this, it suffices to show that the images of \( p_1, \ldots, p_r \in \text{Sel}(\psi)(F/\mathbb{Q}) \) in \( \text{III}(F/\mathbb{Q})_\psi \) are linearly independent. Since we have a homomorphism \( \text{Sel}(\psi)(F/\mathbb{Q}) \to \text{Sel}(\psi)(F/K) \) induced from
the natural map \( \mathbb{Q}^\times / \mathbb{Q}^\times 3 \to K^\times / K^\times 3 \), it is enough to show that the images of \( p_1, \ldots, p_r \in \text{Sel}(\psi)(F/K) \) in \( III(F/K) \) are linearly independent. For this purpose, we calculate the Cassels–Tate pairing \( \langle p_i, \beta_j \rangle_\psi \) on \( \text{Sel}(\psi)(E/K) \) for all \( i, j \).

We first note that \( \langle p_i, \beta_j \rangle_p = 1 \) for all \( p \in \Sigma_K(3) \) because \( p_i \equiv -1 \pmod{9} \). For each \( i \) there are three conjugate ideals of \( p_i \) in \( K \). We number them so that
\[
\Sigma_K(p_i) \cap A^{(\nu)}_K = \{ p_i^{(\nu)} \} \quad (\nu = 0, 1, 2).
\]
Thus \( p_i^{(0)} = p_i \). Moreover, by the choice of the integer \( a \) in (25) we have
\[
\begin{cases}
\Sigma_K(\beta_i) \cap A^{(1)}_K = \{ q_i \}, \\
\Sigma_K(\beta_i) \cap A^{(\nu)}_K = \emptyset \quad (\nu = 0, 2).
\end{cases}
\]
Therefore, applying Theorem 6.5, we obtain
\[
\langle p_i, \beta_j \rangle_\psi = \text{Ind}_\omega(p_i, \beta_j)_{p_i^{(1)}} + 2 \text{Ind}_\omega(p_i, \beta_j)_{p_i^{(2)}} + \text{Ind}_\omega(p_i, \beta_j)_{q_j}.
\]
Since \( p_i \) is in \( k \), we have
\[
\langle p_i, \beta_j \rangle_{p_i^{(1)}} = \langle p_i, \beta_j \rangle_{p_i^{(2)}} = (p_i, N_{K/k}(\beta_j))_{p_i}.
\]
Hence the sum of the first two terms of the right hand side of (27) is equal to zero. On the other hand, we have
\[
\langle p_i, \beta_j \rangle_{q_j} = \left( \frac{p_i}{q_j} \right)_3^h = \omega^{h \delta_{ij}}
\]
by Lemma 7.1. Consequently, we obtain the following simple description of the pairing \( \langle p_i, \beta_j \rangle_\psi \):
\[
\langle p_i, \beta_j \rangle_\psi \equiv h \delta_{ij} \pmod{3}.
\]
Since \( h \) is not divisible by 3, the equality \( \langle p_i, \beta_j \rangle_\psi = 0 \) holds if and only if \( i \neq j \), which proves that \( p_1, \ldots, p_r \) are independent in \( \text{Sel}(\psi)(E/K) \). This proves (26), completing the proof of Theorem 1.1. \( \blacksquare \)

References

The Tate–Shafarevich group


Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Toshima-ku
Tokyo 171-8501, Japan
E-mail: aoki@rkmath.rikkyo.ac.jp

Received on 11.2.2002
and in revised form on 14.2.2003 (4216)