ACTA ARITHMETICA
112.3 (2004)

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* $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ 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 $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ is known to be finite for any n, and there is an injection from the quotient group $E(\mathbb{Q})/nE(\mathbb{Q})$ into $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$. Thus $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ gives an upper bound for the rank of $E(\mathbb{Q})$. Therefore, if $\mathrm{rank}(E(\mathbb{Q}))$ is unbounded when E varies over the elliptic curves over $\mathbb{Q}$, then the order of $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ with n fixed can be arbitrarily large. The converse, however, is not necessarily true because of the presence of the Tate–Shafarevich group

$$Ш(E/\mathbb{Q}) = \mathrm{Ker}\Big(H^1(\mathbb{Q}, E) \to \prod_p H^1(\mathbb{Q}_p, E)\Big).$$

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

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

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

$$\sup\{\#(Ш(E/\mathbb{Q})_n) \mid E \in \mathscr{E}\} = \infty$$

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 $\mathscr{E}$ be the set of elliptic curves $F_{(a,b)}$ defined above. Then*

$$\sup\{\#(\text{Ш}(F/\mathbb{Q})_3) \mid F \in \mathscr{E}\} = \infty.$$

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 $\Delta_F = (a^3 - 27b)^3 b$.) 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 $\text{Ш}(F/\mathbb{Q}(E_3))$ 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-rational) cyclic n-isogeny such that $E_\varphi := \mathrm{Ker}(\varphi) = \langle S \rangle$. Since S is rational over k, we have $E_\varphi \cong \mathbb{Z}/n\mathbb{Z}$ as $\mathrm{Gal}(\overline{k}/k)$-modules. Let $\psi : F \to E$ be the dual isogeny of φ. Then $F_\psi := \mathrm{Ker}(\psi)$ is isomorphic to μ_n as a $\mathrm{Gal}(\overline{k}/k)$-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 $\mathrm{Gal}(\overline{L}/L)$-modules. Taking Galois cohomology, we obtain the exact sequence

$$(1) \qquad 0 \to E(L)/\psi(F(L)) \xrightarrow{\delta_L^{(\psi)}} H^1(L, F_\psi) \to H^1(L, F)_\psi \to 0.$$

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

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

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

$$\begin{aligned}\mathrm{Sel}^{(\psi)}(F/k) &= \mathrm{Ker}\Big(H^1(k, F_\psi) \xrightarrow{\prod \mathrm{res}_v} \prod_{v \in M_k} H^1(k_v, F_\psi) \to \prod_{v \in M_k} H^1(k_v, F)\Big) \\ &= \{x \in H^1(k, F_\psi) \mid \mathrm{res}_v(x) \in \mathrm{Im}(\delta_v^{(\psi)}) \text{ for all } v \in M_k\}.\end{aligned}$$

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

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

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

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

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

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

$$Ш(F/k) = \mathrm{Ker}\Big(H^1(k, F) \to \prod_{v \in M_k} H^1(k_v, F)\Big).$$

It is conjectured that $Ш(F/k)$ is finite. Let

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

be the Cassels–Tate pairing on $Ш(F/k)$. (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 $Ш(F/k)$ is trivial. Let $Ш(F/k)_\psi$ be the kernel of the map $Ш(F/k) \to Ш(E/k)$ induced from ψ, and let

$$\langle\ ,\ \rangle_\psi : Ш(F/k)_\psi \times Ш(F/k)_\psi \to \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$$

be the restriction of $\langle\ ,\ \rangle$ to the subgroup $Ш(F/k)_\psi$. The group $Ш(F/k)_\psi$ fits into the exact sequence

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

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

$$\langle\ ,\ \rangle_\psi : \mathrm{Sel}^{(\psi)}(F/k) \times \mathrm{Sel}^{(\psi)}(F/k) \to \mathbb{Z}/n\mathbb{Z}. \tag{2}$$

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

$$y^2 + xy = x^3 + a_4(q)x + a_6(q), \tag{3}$$

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

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

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

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

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

$$X(u) = \frac{u}{(1-u)^2} + \sum_{n=1}^{\infty}\biggl(\frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\,\frac{q^n}{(1-q^n)^2}\biggr), \tag{4}$$

$$Y(u) = \frac{u^2}{(1-u)^3} + \sum_{n=1}^{\infty}\biggl(\frac{(q^n u)^2}{(1-q^n u)^3} - \frac{q^n u^{-1}}{(1-q^n u^{-1})^3} + \frac{q^n}{(1-q^n)^2}\biggr). \tag{5}$$

Let n be a prime number, and fix an nth root of unity $\zeta \in \mu_n$ and an nth 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 μ and ν 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*

$$\operatorname{Im}(\delta_k^{(\psi)}) = \begin{cases} k^\times/k^{\times n} & \text{if } \nu(S) \neq 0, \\ \{1\} & \text{if } \nu(S) = 0. \end{cases}$$

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:

$$\theta(u) = (1-u) \prod_{n=1}^{\infty} \frac{(1-q^n u)(1-q^n u^{-1})}{(1-q^n)^2} \qquad (u \in \overline{k}^\times).$$

LEMMA 3.2. *Let $x_1, \ldots, x_r \in \overline{k}^\times$ and $m_0, m_1, \ldots, m_r \in \mathbb{Z}$. Let f be a function on $\overline{k}^\times$ defined by*

$$f(u) = u^{-m_0} \prod_{i=1}^{r} \theta(u/x_i)^{m_i} \qquad (u \in \overline{k}^\times).$$

Then the equation $f(qu) = f(u)$ holds for all $u \in \overline{k}^\times$ 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*

$$\operatorname{div}(f \circ \tau^{-1}) = \sum_{i=1}^{r} m_i(\tau(x_i)).$$

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

$$f(\tau(u)) = u^{-\nu} \left(\frac{\theta(\zeta^{-\mu} q_1^{-\nu} u)}{\theta(u)} \right)^n \qquad (u \in \overline{k}^\times). \tag{6}$$

Then Lemma 3.2 implies that f is a rational function on E defined over k such that $\operatorname{div}(f) = n((S) - (O))$. 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

$$\delta_k^{(\psi)}(\tau(u)) \equiv f(\tau(u)) \equiv u^{-\nu} \pmod{k^{\times n}} \tag{7}$$

for all $u \in k^\times$. 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 $0 \le \nu(P) < n$.

PROPOSITION 3.3. *Suppose $q_1 \in k$. Let $f \in k(E)^\times$ be the rational function on E defined by* (6). *Then for any $P \in E(k)_n \setminus \{O, S\}$, $v(f(P))$ 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 $\alpha, \beta \in \overline{k}^\times$, we write $\alpha \sim \beta$ if $v(\alpha/\beta) = 0$. Take $u, z \in \overline{k}^\times$ such that $\tau(u) = S$, $\tau(z) = P$. Clearly one can take u, z so that $0 \le v(u), v(z) < v(q)$. 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

$$v(f(P)) = -\nu(S)\nu(P)v(q_1) + n \cdot v\left(\frac{\theta(u^{-1}z)}{\theta(z)} \right). \tag{8}$$

To calculate the second term, notice that $-v(q) < v(z/u) < v(q)$ and $0 \le v(z) < v(q)$. Hence $1 - q^n(z/u)^{\pm 1} \sim 1$ and $1 - q^n z^{\pm 1} \sim 1$ for all $n \ge 1$. Thus

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

First, suppose $\nu(P) \ne 0$. 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,

$$v\left(\frac{\theta(u^{-1}z)}{\theta(z)} \right) = -\max\{\nu(S) - \nu(P), 0\}v(q_1) + \delta_{\nu(S),\nu(P)} v(1-\zeta). \tag{9}$$

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*

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

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

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

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 $\mathrm{ord}_\mathfrak{p}(\alpha) \neq 0$. 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 $\mathrm{ord}_\mathfrak{p}(q) > 0$ 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 μ, ν and τ defined in the previous section for $E_q/k_\mathfrak{p}$. Let

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

Consider the following condition:

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

Clearly this is equivalent to requiring that $\mathrm{ord}_\mathfrak{p}(\Delta_E) > 0$ 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

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

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

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

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

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

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

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

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

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

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

Proof. Let $x\in V(A_k)$. Then $\mathrm{res}_{\mathfrak p}(x)\in\mathscr O_{\mathfrak p}^\times/\mathscr O_{\mathfrak p}^{\times n}$ for any $\mathfrak p\in B_k$. But, since n is a prime number, the assumption that $N\mathfrak p\not\equiv 1\pmod n$ implies that $\mathscr O_{\mathfrak p}^{\times n}=\mathscr O_{\mathfrak p}^\times$. Therefore, $x=1$ in $k_{\mathfrak p}^\times/k_{\mathfrak p}^{\times n}$. This proves that $V(A_k)\subset \mathrm{Sel}^{(\psi)}(F/k)$. Thus the assertion follows from Proposition 4.1. ∎

We will henceforth assume that k contains μ_n. For any $\mathfrak p\in M_{k,0}\setminus\Sigma_k(n)$ and $x\in k$ with $\mathrm{ord}_{\mathfrak p}(x)=0$, let $\left(\frac{x}{\mathfrak p}\right)_n$ be the nth power residue symbol, namely $\left(\frac{x}{\mathfrak p}\right)_n$ is the nth root of unity such that

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

Note that $\left(\frac{x}{\mathfrak p}\right)_n=1$ if and only if $x\in\mathscr O_{\mathfrak p}^{\times n}$. Thus the following corollary immediately follows from Proposition 4.1.

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

$$\mathrm{Sel}^{(\psi)}(F/k)=\left\{x\in V(A_k)\ \middle|\ \left(\frac{x}{\mathfrak p}\right)_n=1\ (\forall\mathfrak p\in B_k)\right\}.$$

Now, we will give an explicit description of the set A_k. For this purpose, divide the set $\Sigma(E/k)$ into two subsets:

$$\Sigma^{(1)}(E/k) = \{\mathfrak{p} \in \Sigma(E/k) \mid \mathrm{ord}_{\mathfrak{p}}(\Delta_E) \not\equiv 0 \pmod{n}\},$$
$$\Sigma^{(2)}(E/k) = \{\mathfrak{p} \in \Sigma(E/k) \mid \mathrm{ord}_{\mathfrak{p}}(\Delta_E) \equiv 0 \pmod{n}\}.$$

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

$$\phi_{\mathfrak{p}}^*(f_S) = c_{\mathfrak{p}} f_{\mathfrak{p},S} \qquad (c_{\mathfrak{p}} \in k_{\mathfrak{p}}^{\times}).$$

But in view of Proposition 2.1 the commutative diagram

$$\begin{tikzcd}
E(k) \arrow[r, "\delta_k^{(\psi)}"] \arrow[d] & H^1(k, F_\psi) \arrow[r, "\cong"] \arrow[d] & k^{\times}/k^{\times n} \arrow[d] \\
E(k_{\mathfrak{p}}) \arrow[r, "\delta_{k_{\mathfrak{p}}}^{(\psi)}"] & H^1(k_{\mathfrak{p}}, F_\psi) \arrow[r, "\cong"] & k_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times n}
\end{tikzcd}$$

shows that $c_{\mathfrak{p}} \in k_p^{\times n}$. Hence, when we compute $\mathrm{Im}(\delta_{\mathfrak{p}}^{(\psi)})$, we may use f_S instead of $f_{\mathfrak{p},S}$.

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

$$\mathrm{ord}_{\mathfrak{p}}(\phi_{\mathfrak{p}}^*(f_S(P))) = \mathrm{ord}_{\mathfrak{p}}(f_{\mathfrak{p},S})$$

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

$$i_{\mathfrak{p}}(S, P) = \frac{\mathrm{ord}_{\mathfrak{p}}(f_S(P))}{\frac{1}{n}\,\mathrm{ord}_{\mathfrak{p}}(\Delta_E)}.$$

Consider the following condition:

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

Obviously (12) implies (11).

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

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

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

$$i_{\mathfrak{p}}(S, P) \equiv -\nu_{\mathfrak{p}}(S)\nu_{\mathfrak{p}}(P) \pmod{n}$$

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

Proof. If $\mathrm{ord}_{\mathfrak{p}}(\Delta_E) \not\equiv 0 \pmod{n}$, then $q_1 = q^{1/n}$ does not belong to $k_{\mathfrak{p}}$. Let σ be an element of $\mathrm{Gal}(\overline{k}_{\mathfrak{p}}/k_{\mathfrak{p}})$ such that $q_1^{\sigma} \neq q_1$. Since the Tate parametrization $\tau_{\mathfrak{p}}$ is Galois equivariant and S is k-rational, we have

$$\tau_{\mathfrak{p}}(\zeta^{\mu_{\mathfrak{p}}(S)}\mathfrak{q}_1^{\nu_{\mathfrak{p}}(S)}) = \tau_{\mathfrak{p}}(\zeta^{\mu_{\mathfrak{p}}(S)}(\mathfrak{q}_1^{\sigma})^{\nu_{\mathfrak{p}}(S)}).$$

Hence $\nu_{\mathfrak{p}}(S)\tau_{\mathfrak{p}}(\mathfrak{q}_1^{\sigma-1}) = 0$. Since $\mathfrak{q}_1^{\sigma-1}$ is an nth root of unity other than 1, we have $\tau_{\mathfrak{p}}(\mathfrak{q}_1^{\sigma-1}) \neq 0$. Therefore, $\nu_{\mathfrak{p}}(S) = 0$. This proves (i).

To prove (ii), suppose that $\mathrm{ord}_{\mathfrak{p}}(\Delta_E) \equiv 0 \pmod{n}$ and $\mathfrak{p}$ does not divide n. Then Corollary 3.4 shows that

$$\frac{\mathrm{ord}_{\mathfrak{p}}(f_S(P))}{\mathrm{ord}_{\mathfrak{p}}(q_1)} \equiv -\nu_{\mathfrak{p}}(S)\nu_{\mathfrak{p}}(P) \pmod{n}.$$

Since $\frac{1}{n}\mathrm{ord}_{\mathfrak{p}}(\Delta_E) = \mathrm{ord}_{\mathfrak{p}}(q_1)$, (ii) follows. ■

Corollary 4.5. *Assume that k contains μ_n and the condition* (12) *holds. Then*

$$A_k = \{\mathfrak{p} \in \Sigma^{(2)}(E/k) \mid i_{\mathfrak{p}}(S, -S) \not\equiv 0 \pmod{n}\}.$$

Proof. By Proposition 4.4(i), A_k is a subset of $\Sigma^{(2)}(E/k)$. Let $\mathfrak{p} \in \Sigma^{(2)}(E/k)$. Applying Proposition 4.4(ii) for $P = -S$ and noticing that $\nu_{\mathfrak{p}}(-S) \equiv -\nu_{\mathfrak{p}}(S) \pmod{n}$, we obtain

$$i_{\mathfrak{p}}(S, -S) \equiv \nu_{\mathfrak{p}}(S)^2 \pmod{n}.$$

This implies that $\mathfrak{p} \in A_k$ if and only if $i_{\mathfrak{p}}(S, -S) \not\equiv 0 \pmod{n}$. 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 $\langle\ ,\ \rangle_{\psi}$ defined in (2) in terms of the Hilbert norm residue symbol

$$(\ ,\ )_{\mathfrak{p}} : k_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times n} \times k_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times n} \to \mu_n$$

of $k_{\mathfrak{p}}$.

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 $x, x' \in \mathrm{Sel}^{(\psi)}(F/k)$. For each $\mathfrak{p} \in M_k$ let $P_{\mathfrak{p}} \in E(k_{\mathfrak{p}})$ be a local point such that $\mathrm{res}_{\mathfrak{p}}(x) = \delta_{\mathfrak{p}}^{(\psi)}(P_{\mathfrak{p}})$. Then*

$$\langle x, x'\rangle_{\psi} = \sum_{\mathfrak{p} \in M_k} \mathrm{Ind}_{\zeta}(f_T(P_{\mathfrak{p}}), x')_{\mathfrak{p}},$$

where $\mathrm{Ind}_{\zeta} : \mu_n \to \mathbb{Z}/n\mathbb{Z}$ 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 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 $\mathfrak{p} \in A_k$ put $\lambda_{\mathfrak{p}} = \nu_{\mathfrak{p}}(T)/\nu_{\mathfrak{p}}(S) \in \mathbb{Z}/n\mathbb{Z}$. Then for $x, x' \in \mathrm{Sel}^{(\psi)}(F/k)$ we have*

$$\langle x, x' \rangle_{\psi} = \sum_{\mathfrak{p} \in A_k} \lambda_{\mathfrak{p}} \operatorname{Ind}_{\zeta}(x, x')_{\mathfrak{p}}.$$

Proof. Let $\tau_{\mathfrak{p}} : \overline{k}_{\mathfrak{p}}^{\times}/q_{\mathfrak{p}}^{\mathbb{Z}} \to E(\overline{k}_{\mathfrak{p}})$ be the Tate parametrization. For each $\mathfrak{p} \in M_k$ there exists a point $P_{\mathfrak{p}} \in E(k_{\mathfrak{p}})$ such that $\delta_{\mathfrak{p}}^{(\psi)}(P_{\mathfrak{p}}) = \mathrm{res}_{\mathfrak{p}}(x)$. Choose $u_{\mathfrak{p}} \in k_{\mathfrak{p}}^{\times}$ so that $\tau_{\mathfrak{p}}(u_{\mathfrak{p}}) = P_{\mathfrak{p}}$. Then by the same argument as in the proof of Proposition 3.1 one can prove that

$$f_T(P_{\mathfrak{p}}) = f_T(\tau_{\mathfrak{p}}(u_{\mathfrak{p}})) \equiv u_{\mathfrak{p}}^{-\nu_{\mathfrak{p}}(T)} \pmod{k_{\mathfrak{p}}^{\times n}}.$$

Hence by Theorem 5.1 we have

$$\langle x, x' \rangle_{\psi} = \sum_{\mathfrak{p} \in M_k} \operatorname{Ind}_{\zeta}(u_{\mathfrak{p}}^{-\nu_{\mathfrak{p}}(T)}, x')_{\mathfrak{p}}. \tag{13}$$

If $\nu_{\mathfrak{p}}(S) = 0$, then $\mathrm{Im}(\delta_{\mathfrak{p}}^{(\psi)}) = \{1\}$ by Proposition 3.1, and so $(u_{\mathfrak{p}}^{-\nu_{\mathfrak{p}}(T)}, x')_{\mathfrak{p}} = 1$. If $\nu_{\mathfrak{p}}(S) \neq 0$, then $u_{\mathfrak{p}}^{-\nu_{\mathfrak{p}}(T)} \equiv (u_{\mathfrak{p}}^{-\nu_{\mathfrak{p}}(S)})^{\lambda_{\mathfrak{p}}} \pmod{k_{\mathfrak{p}}^{\times n}}$. Therefore

$$(u_{\mathfrak{p}}^{-\nu_{\mathfrak{p}}(T)}, x')_{\mathfrak{p}} = (u_{\mathfrak{p}}^{-\nu_{\mathfrak{p}}(S)}, x')_{\mathfrak{p}}^{\lambda_{\mathfrak{p}}} = (x, x')_{\mathfrak{p}}^{\lambda_{\mathfrak{p}}}. \tag{14}$$

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

The following theorem shows that one can compute the value of $\lambda_{\mathfrak{p}}$ 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 $\mathfrak{p} \in A_k$ the value of $\lambda_{\mathfrak{p}}$ is given by the following formula*:

$$\lambda_{\mathfrak{p}} \equiv -\frac{i_{\mathfrak{p}}(S,T)}{i_{\mathfrak{p}}(S,-S)} \pmod{n}.$$

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

$$i_{\mathfrak{p}}(S,T) \equiv -\nu_{\mathfrak{p}}(S)\nu_{\mathfrak{p}}(T) \pmod{n}.$$

Since $i_{\mathfrak{p}}(S,-S) \equiv \nu_{\mathfrak{p}}(S)^2 \pmod{n}$, it follows that

$$\frac{i_{\mathfrak{p}}(S,T)}{i_{\mathfrak{p}}(S,-S)} \equiv -\lambda_{\mathfrak{p}} \pmod{n},$$

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 Weierstraß equation

$$y^2 + axy + by = x^3, \tag{15}$$

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 ζ. One can easily see that for any $\mathfrak{p} \in \Sigma(E/k)$ our elliptic curve E considered over $k_{\mathfrak{p}}$ is isomorphic to the Tate curve

$$E_q : \quad y^2 + xy = x^3 + \frac{b}{2a^3}\, x + \frac{b^2}{4a^6}$$

with a non-zero element $q = q_{\mathfrak{p}} \in k_{\mathfrak{p}}$ such that $j(E_q) = j(E)$. The isomorphism $\phi_{\mathfrak{p}} : E \to E_q$ is given by

$$\phi_{\mathfrak{p}}((x, y)) = (a^2x, a^3y - b/2). \tag{16}$$

Note that the rational function y on E has the divisor $\mathrm{div}(y) = 3((S) - (O))$. 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

$$y^2 + axy + by = x^3 - 5abx - a^3b - 7b^2. \tag{17}$$

Let $\psi : F \to E$ be the dual isogeny of the isogeny φ.

Proposition 6.1. *Let k be a number field containing μ_3 and assume that* $\mathrm{ord}_{\mathfrak{p}}(3) \not\equiv 0 \pmod 3$ *for all* $\mathfrak{p} \in \Sigma_k(3)$. *Then $A_k = \Sigma_k(b)$ and $B_k = \Sigma_k(a^3 - 27b)$. Moreover the ψ-Selmer group* $\mathrm{Sel}^{(\psi)}(F/k)$ *is given by*

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

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

$$i_{\mathfrak{p}}(S, -S) = \frac{\mathrm{ord}_{\mathfrak{p}}(b)}{\frac{1}{3}\,\mathrm{ord}_{\mathfrak{p}}(\Delta_E)}.$$

It follows that $i_{\mathfrak{p}}(S, -S) = 1$ or 0 according as $\mathfrak{p}$ 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* $\mathrm{ord}_3(b) \not\equiv 0 \pmod 3$, *then*

$$\mathrm{Sel}^{(\psi)}(F/\mathbb{Q}) = V(\Sigma_{\mathbb{Q}}(b)).$$

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 $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{a^3 - 27b})$. We remark that if $\mathrm{ord}_3(b) \not\equiv 0 \pmod 3$, then $\mathrm{ord}_{\mathfrak{p}}(b) \not\equiv 0 \pmod 3$ for all $\mathfrak{p} \in \Sigma_K(3)$ since the absolute ramification index of $\mathfrak{p}$ is 2.

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

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

Proof. The assertion follows from Proposition 6.1 and Corollary 4.3. ∎

Put $\ell = a^3 - 27b$, hence $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{\ell})$. 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 ξ is a cubic root of ℓ and ω is a primitive cubic root of unity. (*The number of possible choices of the pair (ξ, ω) 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 ξ such that $\xi^3 = \ell$. Here the second equality holds since

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

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 ξ and consider three (mutually disjoint) subsets $A_K^{(i)}$ $(i = 0, 1, 2)$ of A_K defined by

$$A_K^{(i)} = \{\mathfrak{p} \in A_K \mid a \equiv \omega^i\xi \pmod{\mathfrak{p}^{\varepsilon_{\mathfrak{p}}}}\},$$

where $\varepsilon_{\mathfrak{p}} = 2$ or 1 according as $\mathfrak{p}$ 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* $\mathrm{ord}_3(b) \not\equiv 0 \pmod 3$. *Let* $x, x' \in \mathrm{Sel}^{(\psi)}(F/K)$. *Then*

$$\langle x, x' \rangle_\psi = \sum_{\mathfrak{p} \in A_K^{(1)}} \mathrm{Ind}_\zeta(x, x')_{\mathfrak{p}} + 2 \sum_{\mathfrak{p} \in A_K^{(2)}} \mathrm{Ind}_\zeta(x, x')_{\mathfrak{p}},$$

where $\zeta = e_3(S, T)$.

Proof. It follows from Theorem 5.3 that

$$\lambda_{\mathfrak{p}} \equiv \frac{\mathrm{ord}_{\mathfrak{p}}(y(T))}{\mathrm{ord}_{\mathfrak{p}}(b)} \pmod 3 \tag{19}$$

for all $\mathfrak{p} \in A_K$. By Lemma 6.4 we have

$$\mathrm{ord}_{\mathfrak{p}}(y(T)) = 2\,\mathrm{ord}_{\mathfrak{p}}(a - \omega\xi) + \mathrm{ord}_{\mathfrak{p}}(a - \omega^2\xi).$$

First, suppose $\mathfrak{p}$ does not divide 3. Then $\mathfrak{p}$ does not divide simultaneously any two factors of the right hand side of (18). Therefore, if $a \equiv \xi \pmod{\mathfrak{p}}$, then $\mathrm{ord}_{\mathfrak{p}}(a - \omega\xi) = \mathrm{ord}_{\mathfrak{p}}(a - \omega^2\xi) = 0$. Hence $\mathrm{ord}_{\mathfrak{p}}(y(T)) = 0$. If $a \equiv \omega\xi \pmod{\mathfrak{p}}$, then $\mathrm{ord}_{\mathfrak{p}}(a - \xi) = \mathrm{ord}_{\mathfrak{p}}(a - \omega^2\xi) = 0$. Hence

$$\mathrm{ord}_{\mathfrak{p}}(y(T)) = 2\,\mathrm{ord}_{\mathfrak{p}}(a - \omega\xi) = 2\,\mathrm{ord}_{\mathfrak{p}}(b).$$

Similarly, if $a \equiv \omega^2\xi \pmod{\mathfrak{p}}$, then $\mathrm{ord}_{\mathfrak{p}}(a - \xi) = \mathrm{ord}_{\mathfrak{p}}(a - \omega\xi) = 0$. Hence

$$\mathrm{ord}_{\mathfrak{p}}(y(T)) = \mathrm{ord}_{\mathfrak{p}}(a - \omega\xi) = \mathrm{ord}_{\mathfrak{p}}(b).$$

Consequently, if $\mathfrak{p}$ does not divide 3, then

$$\mathrm{ord}_{\mathfrak{p}}(y(T)) = \begin{cases} 0 & \text{if } a \equiv \xi \pmod{\mathfrak{p}}, \\ 2\,\mathrm{ord}_{\mathfrak{p}}(b) & \text{if } a \equiv \omega\xi \pmod{\mathfrak{p}}, \\ \mathrm{ord}_{\mathfrak{p}}(b) & \text{if } a \equiv \omega^2\xi \pmod{\mathfrak{p}}. \end{cases} \tag{20}$$

Next, suppose $\mathfrak{p}$ divides 3. Then $\mathrm{ord}_{\mathfrak{p}}(a - \omega^i\xi) > 0$ for any $i = 0, 1, 2$ and equation (18) shows that

$$\mathrm{ord}_{\mathfrak{p}}(y(T)) = -6 + 2\,\mathrm{ord}_{\mathfrak{p}}(a - \omega\xi) + \mathrm{ord}_{\mathfrak{p}}(a - \omega^2\xi).$$

(Note that $\mathrm{ord}_{\mathfrak{p}}(3) = 3$.) Moreover, one of the three factors $a - \omega^i$ $(i = 0, 1, 2)$ of the right hand side of (18) is divisible by $\mathfrak{p}^2$ and the others are not. Therefore, if $a \equiv \xi \pmod{\mathfrak{p}^2}$, then $\mathrm{ord}_{\mathfrak{p}}(a - \omega\xi) = \mathrm{ord}_{\mathfrak{p}}(a - \omega^2\xi) = 1$. Hence $\mathrm{ord}_{\mathfrak{p}}(y(T)) = -3$. If $a \equiv \omega\xi \pmod{\mathfrak{p}^2}$, then $\mathrm{ord}_{\mathfrak{p}}(a - \xi) = \mathrm{ord}_{\mathfrak{p}}(a - \omega^2\xi) = 1$. Hence

$$\mathrm{ord}_{\mathfrak{p}}(a - \omega\xi) = \mathrm{ord}_p\left(\frac{27b}{(a - \xi)(a - \omega^2\xi)}\right) = \mathrm{ord}_{\mathfrak{p}}(b) + 4.$$

Therefore,

$$\mathrm{ord}_{\mathfrak{p}}(y(T)) = 2(\mathrm{ord}_{\mathfrak{p}}(b)+4)+1-6 = 2\,\mathrm{ord}_{\mathfrak{p}}(b)+3.$$

Similarly, if $a \equiv \omega^2\xi \pmod{\mathfrak{p}^2}$, then $\mathrm{ord}_{\mathfrak{p}}(a-\omega^2\xi) = \mathrm{ord}_{\mathfrak{p}}(b)+4$ and $\mathrm{ord}_{\mathfrak{p}}(a-\omega\xi)=1$. Hence

$$\mathrm{ord}_{\mathfrak{p}}(y(T)) = 2+\mathrm{ord}_{\mathfrak{p}}(b)+4-6 = \mathrm{ord}_{\mathfrak{p}}(b).$$

Consequently, if $\mathfrak{p}$ divides 3, then

$$\mathrm{ord}_{\mathfrak{p}}(y(T)) = \begin{cases} -3 & \text{if } a \equiv \xi \pmod{\mathfrak{p}^2}, \\ 2\,\mathrm{ord}_{\mathfrak{p}}(b)+3 & \text{if } a \equiv \omega\xi \pmod{\mathfrak{p}^2}, \\ \mathrm{ord}_{\mathfrak{p}}(b) & \text{if } a \equiv \omega^2\xi \pmod{\mathfrak{p}^2}. \end{cases} \tag{21}$$

By (20) and (21), for any $\mathfrak{p} \in A_K^{(i)}$ $(i=0,1,2)$ we have

$$\mathrm{ord}_{\mathfrak{p}}(y(T)) \equiv -i\cdot\mathrm{ord}_{\mathfrak{p}}(b) \pmod 3.$$

It then follows from (19) that

$$\lambda_{\mathfrak{p}} \equiv -i \pmod 3$$

for any $\mathfrak{p} \in A_K^{(i)}$. Moreover, if $\mathfrak{p} \in M_{K,0}\setminus A_K$, then $\mathrm{ord}_{\mathfrak{p}}(x) \equiv \mathrm{ord}_{\mathfrak{p}}(x') \equiv 0 \pmod 3$, and so $(x,x')_{\mathfrak{p}} = 1$. Therefore

$$\langle x,x'\rangle_{\psi} = \sum_{i=0}^{2} i \sum_{\mathfrak{p}\in A_K^{(i)}} \mathrm{Ind}_{\zeta}(x,x')_{\mathfrak{p}}.$$

This proves the theorem. ∎

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

$$\dim_{\mathbb{Z}/3\mathbb{Z}} Ш(F_{(a,b)}/\mathbb{Q})_3 \geq r. \tag{22}$$

Let ℓ be an odd prime number with $\ell \equiv -1 \pmod 9$. Thus ℓ remains prime in $k := \mathbb{Q}(\sqrt{-3})$. Let ξ be a cubic root of ℓ in $\overline{\mathbb{Q}}$ and put $K = \mathbb{Q}(\sqrt{-3},\xi)$. Since $\ell \equiv -1 \pmod 9$, ℓ 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 ℓ.

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 $\mathrm{Gal}(k(\sqrt[3]{p_i})/k)$ as a subgroup of

$\mathrm{Gal}(L/k)$, and we have an isomorphism

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

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

$$\sqrt[3]{p_i}^{\,g_i} = \omega \sqrt[3]{p_i}. \tag{23}$$

LEMMA 7.1. *There exist prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of K such that*

$$\left(\frac{\xi}{\mathfrak{q}_j}\right)_3 = 1 \quad \textit{and} \quad \left(\frac{p_i}{\mathfrak{q}_j}\right)_3 = \omega^{\delta_{ij}}$$

for all i, j, where $\left(\frac{*}{*}\right)_3$ denotes the cubic power residue symbol of K and δ_{ij} denotes Kronecker's delta.

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

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

Therefore, by Chebotarev's density theorem, there exist prime ideals $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$ of KL such that

$$\begin{cases} \mathrm{Frob}_{KL/k}(\mathfrak{Q}_i)|_K = 1, \\ \mathrm{Frob}_{KL/k}(\mathfrak{Q}_i)|_L = g_i. \end{cases} \tag{24}$$

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

$$\sqrt[3]{p_i}^{\,\mathrm{Frob}_{KL/k}(\mathfrak{Q}_j)} = \omega^{\delta_{ij}} \sqrt[3]{p_i},$$

which is equivalent to $\left(\frac{p_i}{\mathfrak{q}_j}\right)_3 = \omega^{\delta_{ij}}$. Thus the prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ have the desired properties. ∎

Letting $\mathfrak{p}_i$ and $\mathfrak{q}_i$ be as above, choose an integer a such that

$$\begin{cases} \mathrm{ord}_3(a - \xi) = 3, \\ a \equiv \xi \pmod{\mathfrak{p}_1 \ldots \mathfrak{p}_r}, \\ a \equiv \omega\xi \pmod{\mathfrak{q}_1 \ldots \mathfrak{q}_r}. \end{cases} \tag{25}$$

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

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

Since $\mathrm{ord}_{\mathfrak{p}}((a - \xi) - (a - \omega^i\xi)) = \mathrm{ord}_{\mathfrak{p}}((\omega^i - 1)) = 1$ for any $\mathfrak{p} \in \Sigma_K(3)$ and $i = 1, 2$, this shows that $\mathrm{ord}_{\mathfrak{p}}(a - \omega^i\xi) = 1$ for $i = 1, 2$. Therefore,

$\mathrm{ord}_{\mathfrak{p}}((a-\omega\xi)(a-\omega^2\xi)) = 2$. In particular, regarding $(a-\omega\xi)(a-\omega^2\xi)$ as an element of $\mathbb{Q}_3$, we have $\mathrm{ord}_3((a-\omega\xi)(a-\omega^2\xi)) = 1$. Hence the relation

$$\mathrm{ord}_3(a^3-\ell) = \mathrm{ord}_3(a-\xi) + \mathrm{ord}_3((a-\omega\xi)(a-\omega^2\xi))$$

shows that $\mathrm{ord}_3(a^3-\ell) = 4$. Therefore, if we put

$$b = \frac{a^3-\ell}{27},$$

then b is an integer such that $(a,b)=1$ and $\mathrm{ord}_3(b)=1$.

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 ω is the primitive cubic root of unity defined in (23). We claim that

$$\dim_{\mathbb{Z}/3\mathbb{Z}}(Ш(F/\mathbb{Q})_{\psi}) \ge r. \tag{26}$$

Since $Ш(F/\mathbb{Q})_{\psi}\subset Ш(F/\mathbb{Q})_3$, this proves the claim (22). To prove (26), let β_j be a generator of the principal ideal $\mathfrak{q}_j^h$ for each $j=1,\dots,r$. (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* $p_1,\dots,p_r\in \mathrm{Sel}^{(\psi)}(F/\mathbb{Q})$ *and* $\beta_1,\dots,\beta_r\in\mathrm{Sel}^{(\psi)}(F/K)$.

Proof. Since $\ell = a^3-27b$ is a prime number with $\ell\equiv\ 2 \pmod 3$, Corollary 6.2 shows that

$$\mathrm{Sel}^{(\psi)}(F/\mathbb{Q}) = V(\Sigma_{\mathbb{Q}}(b)).$$

In particular, $p_1,\dots,p_r\in\mathrm{Sel}^{(\psi)}(F/\mathbb{Q})$.

To prove the second statement, notice that $K\supset\mu_3$. Let $\mathfrak{l}=(\xi)$ denote the unique prime ideal in K lying above ℓ. Then by Corollary 6.3 we have

$$\mathrm{Sel}^{(\psi)}(F/K) = \left\{x\in V(\Sigma_K(b))\;\middle|\;\left(\frac{x}{\mathfrak{l}}\right)_3 = 1\right\}.$$

Thus, in order to prove that $\beta_i\in\mathrm{Sel}^{(\psi)}(F/K)$, we have to show that $\left(\frac{\beta_i}{\mathfrak{l}}\right)_3 = 1$. But this is equivalent to $(\xi,\beta_i)_{\mathfrak{l}}=1$. To compute $(\xi,\beta_i)_{\mathfrak{l}}$, note that

$$(\xi,\beta_i)_{\mathfrak{q}_i} = \left(\frac{\xi}{\mathfrak{q}_i}\right)_3^h = 1.$$

The first equality holds because $\mathrm{ord}_{\mathfrak{q}_i}(\xi)=0$ and $\mathrm{ord}_{\mathfrak{q}_i}(\beta_i)=h$, and the second one holds by Lemma 7.1. Moreover, since $\xi\equiv -1 \pmod 9$, we have $(\xi,\beta_i)_{\mathfrak{p}} = 1$ for all $\mathfrak{p}\in\Sigma_K(3)$. Then the product formula implies that $(\xi,\beta_i)_{\mathfrak{l}}=1$. This proves that $\beta_i\in\mathrm{Sel}^{(\psi)}(F/K)$, completing the proof. ∎

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

We first note that $(p_i, \beta_j)_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in \Sigma_K(3)$ because $p_i \equiv -1 \pmod 9$. For each i there are three conjugate ideals of $\mathfrak{p}_i$ in K. We number them so that

$$\Sigma_K(p_i) \cap A_K^{(\nu)} = \{\mathfrak{p}_i^{(\nu)}\} \quad (\nu = 0, 1, 2).$$

Thus $\mathfrak{p}_i^{(0)} = \mathfrak{p}_i$. Moreover, by the choice of the integer a in (25) we have

$$\begin{cases} \Sigma_K(\beta_i) \cap A_K^{(1)} = \{\mathfrak{q}_i\}, \\ \Sigma_K(\beta_i) \cap A_K^{(\nu)} = \emptyset \quad (\nu = 0, 2). \end{cases}$$

Therefore, applying Theorem 6.5, we obtain

$$\langle p_i, \beta_j\rangle_\psi = \mathrm{Ind}_\omega(p_i, \beta_j)_{\mathfrak{p}_i^{(1)}} + 2\,\mathrm{Ind}_\omega(p_i, \beta_j)_{\mathfrak{p}_i^{(2)}} + \mathrm{Ind}_\omega(p_i, \beta_j)_{\mathfrak{q}_j}. \tag{27}$$

Since p_i is in k, we have

$$(p_i, \beta_j)_{\mathfrak{p}_i^{(1)}} = (p_i, \beta_j)_{\mathfrak{p}_i^{(2)}} = (p_i, N_{K/k}(\beta_j))_{p_i}.$$

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

$$(p_i, \beta_j)_{\mathfrak{q}_j} = \left(\frac{p_i}{\mathfrak{q}_j}\right)_3^h = \omega^{h\delta_{ij}}$$

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 $p_1, \dots, p_r$ are independent in $\mathrm{Sel}^{(\psi)}(E/K)$. This proves (26), completing the proof of Theorem 1.1. ∎

References

[1] D. Atake, *On elliptic curves with large Tate–Shafarevich groups*, J. Number Theory 87 (2001), 282–300.

[2] C. D. Beaver, 5-*torsion in the Shafarevich–Tate group of a family of elliptic curves*, ibid. 82 (2000), 25–46.

[3] V. R. Bölling, *Die Ordnung der Schafarewitsch–Tate-Gruppe kann beliebig groß werden*, Math. Nachr. 67 (1975), 157–179.

[4] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. 44 (1977), 715–743.

[5] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. 211 (1962), 95–112.

[6] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *VI. The Tate–Shafarevich group can be arbitrarily large*, ibid. 214 (1963), 65–70.

[7] T. Fisher, *On* 5 *and* 7 *descents for elliptic curves*, PhD thesis, Cambridge, 2000.

[8] K. Kramer, *A family of semistable elliptic curves with large Tate–Shafarevich groups*, Proc. Amer. Math. Soc. 89 (1983), 379–386.

[9] F. Lemmermeyer, *On Tate–Shafarevich groups of some elliptic curves*, in: Algebraic Number Theory and Diophantine Analysis (Graz, 1998), F. Halter-Koch and R. F. Tichy (eds.), de Gruyter, 2000, 277–291.

[10] W. G. McCallum, *On the Shafarevich–Tate group of the Jacobian of a quotient of the Fermat curve*, Invent. Math. 93 (1988), 637–666.

[11] S. Milne, *Arithmetic Duality Theorems*, Perspect. Math. 1, Academic Press, 1986.

[12] P. Roquette, *Analytic Theory of Elliptic Functions over Local Fields*, Hamburger Math. Einzelschriften (N.F.) 1, Vandenhoeck & Ruprecht, Göttingen, 1970.

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[14] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994.

[15] J. Tate, *Duality theorems in Galois cohomology over number fields*, in: Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, 288–295.

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)