TOKYO J. MATH.
VOL. 20, NO. 1, 1997

# The Order of the $p$-Selmer Groups and the Rank of Elliptic Curves

Hisayoshi SATO

*Kyushu University*

(Communicated by K. Katayama)

## 1. Introduction.

Let $E$ be an elliptic curve defined over a number field $k$. Then the set $E(k)$ of all $k$-rational points of $E$ is a finitely generated abelian group. By the rank of $E/k$ we mean the rank of the free part of $E(k)$. The rank is deeply connected with the order of the Selmer group. In this paper, we give an upper bound of the order of the $p$-Selmer group of $E/k$ for a prime number $p$ in terms of the ideal class group of certain finite extension of $k$. There are various results about the order of the Selmer groups. Brumer-Kramer [2], Washington [11], and Kawachi-Nakano [3] studied the case for $p=2$. For a cyclic isogeny $\phi$ of prime degree $p$, Aoki [1] estimated the order of the $\phi$-Selmer group by using the genus formula.

We here follow Aoki's method in order to estimate the order of the Selmer group for the multiplication-by-$p$ map.

In Section 2, we recall the general facts about the Selmer group and define some maps which will be needed later. In Section 3, we embed the $p$-Selmer group for an odd prime $p$ in some Galois cohomology groups and estimate the order of the Selmer group by making use of the genus formula under some assumptions. For $p=2$, we discuss in Section 4. In Section 5, we show that the assumptions in Section 3 hold for an elliptic curve without complex multiplication whenever we choose a suitable prime number $p$ and replace the base field $k$ by some finite extension of $k$.

## 2. Preliminaries.

Let $k$ be an algebraic number field of finite degree and $E$ be an elliptic curve defined over $k$. For any integer $m\geq 2$, $E[m]$ denotes the kernel of the multiplication-by-$m$ map $[m]$. Let $S$ be a finite set of places of $k$ consisting of the infinite places, those which divide $m$ and those at which $E$ has bad reductions, and $k_S$ be the maximal Galois

Received September 27, 1995

extension of $k$ which is unramified outside $S$. Then it is known that there is an exact sequence

$$0 \longrightarrow H^1(k_S/k, E[m]) \longrightarrow H^1(k, E[m]) \longrightarrow \bigoplus_{v \in M_k \setminus S} H^1(k_v, E),$$

where $M_k$ means the set of all (finite, infinite) places of $k$ and $k_v$ denotes the completion of $k$ at $v \in M_k$ [5]. From the above sequence, the Selmer group $S^{(m)}(E/k)$ of $E/k$ for $[m]$ is given by

$$\begin{aligned} S^{(m)}(E/k) &= \mathrm{Ker}\{H^1(k, E[m]) \to \prod_{v \in M_k} H^1(k_v, E)\} \\ &= \mathrm{Ker}\{H^1(k, E[m]) \to \prod_{v \in S} H^1(k_v, E)\} \cap \mathrm{Ker}\{H^1(k, E[m]) \to \prod_{v \notin S} H^1(k_v, E)\} \\ &= \mathrm{Ker}\{H^1(k_S/k, E[m]) \to \prod_{v \in S} H^1(k_v, E)\}. \end{aligned}$$

The following diagram is commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(k)/mE(k) & \xrightarrow{\delta} & H^1(k, E[m]) & \longrightarrow & H^1(k, E)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \prod res_v & & \downarrow \prod res_v & & \\ 0 & \longrightarrow & \prod_{v \in S} E(k_v)/mE(k_v) & \xrightarrow{\prod \delta_v} & \prod_{v \in S} H^1(k_v, E[m]) & \longrightarrow & \prod_{v \in S} H^1(k_v, E)[m] & \longrightarrow & 0, \end{array}$$

where $res_v$ means the restriction map of cohomology groups. Then, from the above discussion, the Selmer group is given by

$$S^{(m)}(E/k) = \{\xi \in H^1(k_S/k, E[m]) \mid res_v(\xi) \in \mathrm{Im}\,\delta_v \text{ for any } v \in S\}.$$

Next suppose that $E[m] = \langle P \rangle \times \langle P' \rangle \subset E(k)$, where $P$, $P'$ are some generators over $\mathbf{Z}/m\mathbf{Z}$. Let $\mu_m \subset k^\times$ be the group of $m$-th roots of unity and $e_m$ be the Weil pairing

$$e_m : E[m] \times E[m] \longrightarrow \mu_m.$$

For fixed generators $P$, $P'$ of $E[m]$ over $\mathbf{Z}/m\mathbf{Z}$, it is easily seen that $e_m$ gives an isomorphism

$$\begin{aligned} i : H^1(k, E[m]) &\xrightarrow{\sim} H^1(k, \mu_m) \times H^1(k, \mu_m), \\ \xi &\longmapsto ([\sigma \mapsto e_m(\xi(\sigma), P')], [\tau \mapsto e_m(P, \xi(\tau))]). \end{aligned}$$

Let $\kappa$ be the isomorphism given by the Kummer sequence for the field $k$:

$$\kappa : H^1(k, \mu_m) \xrightarrow{\sim} k^\times / k^{\times m}.$$

Then using the isomorphisms $\kappa$ and $i$, we define an isomorphism

$$j\colon H^1(k, E[m]) \xrightarrow{\sim} (k^\times/k^{\times m})^2\,,$$
$$j=(\kappa\times\kappa)\circ i\,.$$

For any place $v$ of $k$, let $i_v$, $\kappa_v$, $j_v$ denote the maps which are defined over $k_v$ in a similar way as $i$, $\kappa$, $j$ respectively. Moreover, $e_m$ defines a cup product

$$\langle\ ,\ \rangle_v\colon H^1(k_v, E[m])\times H^1(k_v, E[m]) \xrightarrow{\cup_{e_m}} H^2(k_v, \mu_m) \underset{\sim}{\xrightarrow{inv_v}} \tfrac{1}{m}\mathbf{Z}/\mathbf{Z}\,,$$

where $inv_v$ denotes the invariant map.

Finally, let $(\ ,\ )_v\colon k_v^\times/k_v^{\times m}\times k_v^\times/k_v^{\times m}\to\mu_m$ be the Hilbert norm residue symbol. Then we define a bilinear map $\Phi$ as follows:

$$\Phi\colon (k_v^\times/k_v^{\times m})^2\times(k_v^\times/k_v^{\times m})^2\to\mu_m\,,$$
$$((a, b), (c, d))\longmapsto (a, d)_v(b, c)_v^{-1}\,.$$

LEMMA 1. *The following diagram is commutative*:

$$\begin{array}{ccc} H^1(k_v, E[m]) \times H^1(k_v, E[m]) & \xrightarrow{\langle\ ,\ \rangle_v} & \frac{1}{m}\mathbf{Z}/\mathbf{Z} \\ \Big\downarrow {\scriptstyle j_v\times j_v} & & \Big\downarrow {\scriptstyle \imath} \\ (k_v^\times/k_v^{\times m})^2 \times (k_v^\times/k_v^{\times m})^2 & \xrightarrow{\Phi} & \mu_m\,, \end{array}$$

*where* $\imath(n/m)=e_m(P, P')^n$.

PROOF. If we define a pairing

$$f\colon H^1(k_v, \mu_m)^2\times H^1(k_v, \mu_m)^2\longrightarrow H^2(k_v, \mu_m)\,,$$
$$((\xi, \eta), (\phi, \psi))\longmapsto [(\sigma, \tau)\mapsto(\xi\cup\psi)(\sigma, \tau)((\eta\cup\phi)(\sigma, \tau))^{-1}]\,,$$

then by the definition, it is easily checked that the following diagram is commutative:

$$\begin{array}{ccc} H^1(k_v, E[m]) \times H^1(k_v, E[m]) & \xrightarrow{\cup_{e_m}} & H^2(k_v, \mu_m) \\ \Big\downarrow {\scriptstyle i_v\times i_v} & & \Big\downarrow {\scriptstyle id} \\ H^1(k_v, \mu_m)^2 \times H^1(k_v, \mu_m)^2 & \xrightarrow{f} & H^2(k_v, \mu_m)\,. \end{array}$$

On the other hand, by [7] Ch. XIV Proposition 5, we have a commutative diagram

$$\begin{array}{ccc} H^1(k_v, \mu_m) \times H^1(k_v, \mu_m) & \xrightarrow{\cup} & H^2(k_v, \mu_m) \\ \Big\downarrow {\scriptstyle \kappa_v\times\kappa_v} & & \Big\downarrow {\scriptstyle \nu} \\ k_v^\times/k_v^{\times m} \times k_v^\times/k_v^{\times m} & \xrightarrow{(\ ,\ )_v} & \mu_m\,, \end{array}$$

where $\nu$ stands for the composition of $inv_v$ and $\iota: \frac{1}{m}\mathbf{Z}/\mathbf{Z} \xrightarrow{\sim} \mu_m$. Hence for $((\xi, \eta), (\phi, \psi)) \in H^1(k_v, \mu_m)^2 \times H^1(k_v, \mu_m)^2$, we have

$$\nu \circ f((\xi, \eta), (\phi, \psi)) = \nu((\xi \cup \psi)(\eta \cup \phi)^{-1}) = \nu(\xi \cup \psi)\nu(\eta \cup \phi)^{-1}$$
$$= (\kappa_v\xi, \kappa_v\psi)_v(\kappa_v\eta, \kappa_v\phi)_v^{-1} = \Phi((\kappa_v\xi, \kappa_v\eta), (\kappa_v\phi, \kappa_v\psi)) = \Phi \circ \kappa_v^4((\xi, \eta), (\phi, \psi)) .$$

Therefore the diagram

$$\begin{array}{ccc} H^1(k_v, \mu_m)^2 \times H^1(k_v, \mu_m)^2 & \xrightarrow{f} & H^2(k_v, \mu_m) \\ \downarrow \kappa_v^4 & & \downarrow \nu \\ (k_v^\times/k_v^{\times m})^2 \times (k_v^\times/k_v^{\times m})^m & \xrightarrow{\Phi} & \mu_m \end{array}$$

is commutative.

Moreover, the composite map $\frac{1}{m}\mathbf{Z}/\mathbf{Z} \xrightarrow{inv_v^{-1}} H^2(k_v, \mu_m) \xrightarrow{\nu} \mu_m$ coincides with $\iota$ by the definition of $\nu$. This gives the desired result.

Taking account of Lemma 1, let $\mathrm{Im}\,\delta_v^\perp$ be the annihilator of $\mathrm{Im}\,\delta_v$ with respect to $\langle\ ,\ \rangle_v$, namely

$$\mathrm{Im}\,\delta_v^\perp = \{\xi \in H^1(k_v, E[m]) \mid \langle \eta, \xi \rangle_v = 0 \text{ for any } v \in \mathrm{Im}\,\delta_v\} .$$

Then by the definition of $e_m$, it can be shown that $\mathrm{Im}\,\delta_v \subset \mathrm{Im}\,\delta_v^\perp$ [4].

On the other hand, the Tate pairing $E(k_v) \times H^1(k_v, E) \to \mathbf{Q}/\mathbf{Z}$ [10], [12] induces a perfect pairing

$$E(k_v)/mE(k_v) \times H^1(k_v, E)[m] \to \tfrac{1}{m}\mathbf{Z}/\mathbf{Z} ,$$

and this pairing is commutative with $\langle\ ,\ \rangle_v$, namely the diagram

$$\begin{array}{ccc} E(k_v)/mE(k_v) \times H^1(k_v, E)[m] & \longrightarrow & \frac{1}{m}\mathbf{Z}/\mathbf{Z} \\ \uparrow \delta_v \times lift & & \downarrow id \\ H^1(k_v, E[m]) \times H^1(k_v, E[m]) & \longrightarrow & \frac{1}{m}\mathbf{Z}/\mathbf{Z} \end{array}$$

is commutative.

Hence, for any $\xi \in \mathrm{Im}\,\delta_v^\perp \subset H^1(k_v, E[m])$, the image $\bar{\xi}$ in $H^1(k_v, E)[m]$ is an annihilator for $E(k_v)/mE(k_v)$. But the pairing is perfect, hence we have $\bar{\xi} = \bar{0}$. Therefore $\xi$ is in the kernel of $H^1(k_v, E[m]) \to H^1(k_v, E)[m]$ which is equal to $\mathrm{Im}\,\delta_v$, hence $\mathrm{Im}\,\delta_v^\perp \subset \mathrm{Im}\,\delta_v$, consequently we have

(1) $$\mathrm{Im}\,\delta_v = \mathrm{Im}\,\delta_v^\perp .$$

### 3. The cases for odd primes.

In this section, we will embed the Selmer group $S^{(p)}(E/k)$ for an odd prime number $p$ in some Galois cohomology group under some assumptions, and estimate the order of $S^{(p)}(E/k)$ by making use of the genus formula.

Let assume that $E(k)$ contains the $p$-torsion subgroup $E[p]$. Moreover we assume that the following condition (A) holds.

(A) There are such generators $P_1$, $P_2$ of $p^2$-torsion subgroup $E[p^2]$ over $\mathbf{Z}/p^2\mathbf{Z}$ that the definition fields $K_1=k(P_1)$, $K_2=k(P_2)$ of $P_1$, $P_2$ over $k$ are both cyclic extensions of degree $p$ over $k$, and if we put

$$G_i=\mathrm{Gal}(K_i/k)=\langle\tau_i\rangle \qquad (i=1,2),$$

then

$$P=P_1^{\tau_1}-P_1, \qquad P'=P_2^{\tau_2}-P_2$$

generate $E[p]$ over $\mathbf{Z}/p\mathbf{Z}$.

We take the above generators $P$, $P'$ of $E[p]$ in order to define the map $j$ in Section 2 and consider the following maps

$$E(k)/pE(k)\xrightarrow{\delta}H^1(k,E[p])\xrightarrow[\sim]{j}(k^\times/k^{\times p})^2 .$$

Then by the definition of $\delta$ and the condition (A), for any $\sigma\in\mathrm{Gal}(\bar{k}/k)$

$$\delta([p]P_1)(\sigma)=P_1^\sigma-P_1\in\langle P\rangle .$$

Hence, the second component of the image $i\circ\delta([p]P_1)$ becomes always trivial:

$$(i\circ\delta([p]P_1))_2(\sigma)=e_p(P,P_1^\sigma-P_1)=1 \qquad \text{for any } \sigma\in\mathrm{Gal}(\bar{k}/k).$$

Therefore the image $j\circ\delta([p]P_1)$ is always in the form

$$j\circ\delta([p]P_1)=(a_1,1)\in(k^\times/k^{\times p})^2$$

for some $a_1\in k^\times/k^{\times p}$. Similarly, the image of $[p]P_2$ is in the form

$$j\circ\delta([p]P_2)=(1,a_2)\in(k^\times/k^{\times p})^2$$

for some $a_2\in k^\times/k^{\times p}$. For any $v\in M_k$, the images of $j_v\circ\delta_v$ are also given by

$$\begin{cases} j_v\circ\delta_v([p]P_1)=(a_1,1)\in(k_v^\times/k_v^{\times p})^2 , \\ j_v\circ\delta_v([p]P_2)=(1,a_2)\in(k_v^\times/k_v^{\times p})^2 . \end{cases}$$

On the other hand, let $L/K$ be an arbitrary field extension. Then for an elliptic curve $E/K$, the following diagram is commutative:

$$\begin{array}{ccccc} E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E[p]) & \xrightarrow{\sim} & (K^\times/K^{\times p})^2 \\ \downarrow & & \downarrow{\scriptstyle res} & & \downarrow \\ E(L)/pE(L) & \xrightarrow{\delta_L} & H^1(L, E[p]) & \xrightarrow{\sim} & (L^\times/L^{\times p})^2 . \end{array}$$

For any $P \in E(K)$, $K([p]^{-1}P)$ is contained in $L$ if and only if $P$ is contained in $pE(L)$, and it is equivalent to that $\delta(P)$ is an element of the kernel of the map $(K^\times/K^{\times p})^2 \to (L^\times/L^{\times p})^2$. Since the kernel is $((K^\times \cap L^{\times p})/K^{\times p})^2$, if we put $\delta(P) = (\delta(P)_1, \delta(P)_2)$, it is equivalent to that $K(\sqrt[p]{\delta(P)_1}, \sqrt[p]{\delta(P)_2})$ is contained in $L$. Therefore we have

$$K([p]^{-1}P) = K(\sqrt[p]{\delta(P)_1}, \sqrt[p]{\delta(P)_2} \qquad \text{for any } P \in E(K) .$$

Consequently, we have

$$K_1 = k(P_1) = k(\sqrt[p]{a_1}), \qquad K_2 = k(P_2) = k(\sqrt[p]{a_2}) .$$

Moreover, it is clear that the subgroups of $(k_v^\times/k_v^{\times p})^2$ generated by $(a_1, 1)$, $(1, a_2)$, denoted by $\langle(a_1, 1)\rangle_v$, $\langle(1, a_2)\rangle_v$ respectively, are contained in $\operatorname{Im}\delta_v$. Hence, taking the annihilators with respect to the bilinear map $\Phi$: $(k_v^\times/k_v^{\times p})^2 \times (k_v^\times/k_v^{\times p})^2 \to \mu_p$ and by (1), we have

$$\operatorname{Im}\delta_v = \operatorname{Im}\delta_v^\perp \subset \langle(a_1, 1)\rangle_v^\perp , \qquad \operatorname{Im}\delta_v = \operatorname{Im}\delta_v^\perp \subset \langle(1, a_2)\rangle_v^\perp .$$

Let $(c, d) \in (k_v^\times/k_v^{\times p})^2$ be an annihilator of $(a_1, 1)$. Then by the definition we see

$$1 = \Phi((a_1, 1), (c, d)) = (a_1, d)_v (1, c)_v^{-1} = (a_1, d)_v .$$

Hence $d$ must be an annihilator of $a_1$ with respect to the Hilbert norm residue symbol and $c$ is arbitrary. In $k_v^\times/k_v^{\times p}$ the Kummer group for $K_{1,\omega} = k_v(\sqrt[p]{a_1})$ is the subgroup generated by $a_1$, denoted by $\langle a_1\rangle_v$, and its annihilator with respect to the Hilbert norm residue symbols is the norm of $K_{1,\omega}^\times$, namely $NK_{1,\omega}^\times k_v^{\times p}/k_v^{\times p}$. Therefore we have

$$\langle(a_1, 1)\rangle_v^\perp = k_v^\times/k_v^{\times p} \times NK_{1,\omega}^\times k_v^{\times p}/k_v^{\times p} .$$

Similarly

$$\langle(1, a_2)\rangle_v^\perp = NK_{2,\omega'}^\times k_v^{\times p}/k_v^{\times p} \times k_v^\times/k_v^{\times p} ,$$

where $K_{2,\omega'} = k_v(\sqrt[p]{a_2})$. Hence we have an inclusion

(2)
$$\begin{aligned} \operatorname{Im}\delta_v &\subseteq \langle(a_1, 1)\rangle_v^\perp \cap \langle(1, a_2)\rangle_v^\perp \\ &= NK_{2,\omega'}^\times k_v^{\times p}/k_v^{\times p} \times NK_{1,\omega}^\times k_v^{\times p}/k_v^{\times p} . \end{aligned}$$

Let $\mathcal{O}_{1,\omega}$ denote the ring of integers of $K_{1,\omega}$. Then if $K_{1,\omega}/k_v$ is unramified, we have

(3)
$$NK_{1,\omega}^\times \equiv N\mathcal{O}_{1,\omega}^\times \qquad (\operatorname{mod} k_v^{\times p}) .$$

Similarly, if $K_{2,\omega'}^\times/k_v$ is unramified, then

(4)
$$NK_{2,\omega'}^\times \equiv N\mathcal{O}_{2,\omega'}^\times \qquad (\operatorname{mod} k_v^{\times p}) .$$

Let $R_i$ be the set of places of $k$ which are ramified in $K_i$ $(i=1, 2)$. Moreover we put $T_i = R_i \cap S$ $(i=1, 2)$, where $S$ means the same set as in Section 2. Let $T'_i$ be the set of places of $K_i$ lying above places of $T_i$. Then $T'_i$-idèle group $J_{K_i,T'_i}$ of $K_i$ is defined by

$$J_{K_i,T'_i} := \prod_{\omega \in M_{K_i} \setminus T'_i} \mathcal{O}_{i,\omega}^{\times} \times \prod_{\omega \in T'_i} K_{i,\omega}^{\times},$$

where for an infinite place $\omega$, $\mathcal{O}_{i,\omega}^{\times}$ denotes $\mathbf{C}^{\times}$. Note that by the assumption, $k$ contains $\mu_p$, hence $k$ and $K_i$ are totally imaginary.

For each places $v$ of $k$, we choose and fix a place $\omega$ of $K_i$ lying above $v$ once for all. Then by the semi-local theory, there exists an isomorphism

$$\hat{H}^0(K_i/k, J_{K_i,T'_i}) \cong \bigoplus_{v \notin T_i} \hat{H}^0(K_{i,\omega}/k_v, \mathcal{O}_{i,\omega}^{\times}) \oplus \bigoplus_{v \in T_i} \hat{H}^0(K_{i,\omega}/k_v, K_{i,\omega}^{\times}),$$

where $\hat{H}$ means the Tate cohomology.

Let $f$ be the composition of the following maps.

$$\begin{aligned} \prod_{i=1,2} H^1(k_{T_i}/k, \mu_p) &\xrightarrow{\prod(\prod_{v \in T_i} res_v)} \prod_{i=1,2} \Big( \sum_{v \in T_i} H^1(k_{T_i,v}/k_v, \mu_p) \Big) \\ &\longrightarrow \prod_{i=1,2} \Big( \prod_{v \in T_i} \hat{H}^0(K_{i,\omega}/k_v, K_{i,\omega}^{\times}) \Big) \\ &\hookrightarrow \prod_{i=1,2} (\hat{H}^0(K_i/k, J_{K_i,T'_i})) . \end{aligned}$$

Then we have

LEMMA 2. *There is an inclusion*

$$S^{(p)}(E/k) \hookrightarrow \mathrm{Ker}\Big\{ \prod_{i=1,2} H^1(k_{T_i}/k, \mu_p) \xrightarrow{f} \prod_{i=1,2} \hat{H}^0(K_i/k, J_{K_i,T'_i}) \Big\} .$$

PROOF. Looking at the following diagram

$$\begin{array}{ccccc} E(k)/pE(k) & \xrightarrow{\delta} & H^1(k_S/k, E[p]) & \xrightarrow{\simeq} & H^1(k_S/k, \mu_p) \times H^1(k_S/k, \mu_p) \\ \downarrow & & \downarrow{\scriptstyle resoinf} & & \downarrow \\ \prod_{v \in S} E(k_v)/pE(k_v) & \longrightarrow & \prod_{v \in S} H^1(k_v, E[p]) & \xrightarrow{\simeq} & \prod_{v \in S} \{H^1(k_v, \mu_p) \times H^1(k_v, \mu_p)\} , \end{array}$$

the Selmer group $S^{(p)}(E/k)$ can be expressed as

$$S^{(p)}(E/k) = \{(\xi_1, \xi_2) \in H^1(k_S/k, \mu_p)^2 \mid res_v(\xi_1, \xi_2) \in \mathrm{Im}(i_v \circ \delta_v) \text{ for any } v \in S\} .$$

Since the map $i_v$ is an isomorphism, we identify $\mathrm{Im}\,\delta_v$ with $\mathrm{Im}(i_v \circ \delta_v)$. Then, by (2), (3) and (4), we have for each $(\xi_1, \xi_2) \in S^{(p)}(E/k)$

$$res_v \xi_1 \in N\mathcal{O}_{2,\omega'}^{\times} k_v^{\times p}/k_v^{\times p} \qquad (v \in S \setminus T_2) ,$$

$$res_v \xi_2 \in N\mathcal{O}_{1,\omega}^{\times} k_v^{\times p}/k_v^{\times p} \qquad (v \in S \setminus T_1) .$$

On the other hand, by Kummer theory, there is an isomorphism

$$H^1(k_S/k, \mu_p) \cong \{x \in k^\times/k^{\times p} \mid \mathrm{ord}_v(x) \equiv 0 \pmod p \text{ for any } v \notin S\}\,.$$

Hence we have

$$\begin{cases} \mathrm{ord}_v(res_v\xi_1) \equiv 0 \pmod p & \text{for any } v \in T_2\,, \\ \mathrm{ord}_v(res_v\xi_2) \equiv 0 \pmod p & \text{for any } v \notin T_1\,. \end{cases}$$

Therefore we have an inclusion

$$\begin{aligned} S^{(p)}(E/k) &\hookrightarrow H^1(k_{T_2}/k, \mu_p) \times H^1(k_{T_1}/k, \mu_p) \\ &\cong \{x \in k^\times/k^{\times p} \mid \mathrm{ord}_v(x) \equiv 0 \pmod p \text{ for any } v \notin T_2\} \\ &\quad \times \{x \in k^\times/k^{\times p} \mid \mathrm{ord}_v(x) \equiv 0 \pmod p \text{ for any } v \notin T_1\}\,. \end{aligned}$$

Moreover, for $v \in T_2$

$$res_v\xi_1 \in NK_{2,\omega'}^\times k_v^{\times p}/k_v^{\times p} = \mathrm{Ker}\{k_v^\times/k_v^{\times p} \to \hat{H}^0(K_{2,\omega'}/k_v, K_{2,\omega'}^\times)\}\,.$$

Similarly, for $v \in T_1$

$$res_v\xi_2 \in NK_{1,\omega}^\times k_v^{\times p}/k_v^{\times p} = \mathrm{Ker}\{k_v^\times/k_v^{\times p} \to \hat{H}^0(K_{1,\omega}/k_v, K_{1,\omega}^\times)\}\,.$$

This gives the desired inclusion.

In general, let $K/k$ be any finite Galois extension and $G = \mathrm{Gal}(K/k)$ be the Galois group. Then for a finite subset $T$ of $M_k$, $T$-unit group $U_{k,T}$ of $k$ is defined by

$$\begin{aligned} U_{k,T} = \{u \in k^\times \mid\ & v(u) > 0 \text{ for all real } v \in M_k^\infty \backslash T \text{ and} \\ & \mathrm{ord}_v(u) = 0 \text{ for all } v \in M_k^0 \backslash T\}\,, \end{aligned}$$

where $M_k^\infty$ (resp. $M_k^0$) is the set of all infinite (resp. finite) places of $k$. Let $T'$ be the set of places of $K$ lying above the places of $T$. Then the $T'$-unit group $U_{K,T'}$ is also defined in a similar way. Let $J_{K,T'}$ be the $T'$-idèle group of $K$, and $C_{K,T'}$ be a group defined by the following exact sequence

$$0 \longrightarrow U_{K,T'} \xrightarrow{\alpha} J_{K,T'} \xrightarrow{\beta} C_{K,T'} \longrightarrow 0\,, \tag{5}$$

where $\alpha$ denotes the diagonal embedding.

Taking the Tate cohomology we obtain a long exact sequence

$$\begin{aligned} \cdots &\longrightarrow \hat{H}^0(G, U_{K,T'}) \xrightarrow{\alpha_0} \hat{H}^0(G, J_{K,T'}) \xrightarrow{\beta_0} \hat{H}^0(G, C_{K,T'}) \\ &\longrightarrow H^1(G, U_{K,T'}) \xrightarrow{\alpha_1} H^1(G, J_{K,T'}) \xrightarrow{\beta_1} H^1(G, C_{K,T'}) \\ &\longrightarrow H^2(G, U_{K,T'}) \xrightarrow{\alpha_2} H^2(G, J_{K,T'}) \xrightarrow{\beta_2} H^2(G, C_{K,T'}) \\ &\longrightarrow \qquad \cdots\,. \end{aligned} \tag{6}$$

Let $Cl_{k,T}$ (resp. $Cl_{K,T'}$) be the group $J_k/k^{\times}J_{k,T}$ (resp. $J_K/K^{\times}J_{K,T'}$). Suppose that $T$ contains all the places which ramify in $K/k$, and that $K/k$ is a cyclic extension, then Aoki [1] shows the following genus formula:

Suppose that $K/k$ is a cyclic extension. Then it holds that

$$|\operatorname{Ker}\alpha_2| = \frac{[K:k]\,|\hat{H}^0(G, U_{K,T'})|}{ef_T}\,\frac{|(Cl_{K,T'})^G|}{|Cl_{k,T}|}, \tag{7}$$

where $e=\prod_{v\in M_k} e_v$ is the product of the relative ramification indeces in $K/k$ and $f_T=\prod_{v\in T} f_v$ is the product of the relative degree of $v\in T$ in $K/k$ [1].

In our case, the $T_i$-unit group of $k$ is given by

$$U_{k,T_i}=\{u\in k^{\times} \mid \operatorname{ord}_v(u)=0 \text{ for any } v\in M_k^0\backslash T_i\} \qquad (i=1, 2).$$

The $T_i'$-unit group of $K_i$ is also given in a similar form.

We define a map

$$\lambda_i: U_{k,T_i}k^{\times p}/k^{\times p} \longrightarrow \hat{H}^0(K_i/k, J_{K_i,T_i'})$$

by the composition of the natural surjection

$$U_{k,T_i}k^{\times p}/k^{\times p}(\cong U_{k,T_i}/U_{k,T_i}\cap k^{\times p}) \longrightarrow U_{k,T_i}/NU_{K_i,T_i'}(\cong \hat{H}^0(K_i/k, U_{K_i,T_i'})),$$

where $N$ is the norm map from $K_i^{\times}$ to $k^{\times}$, and

$$\alpha_0^{(i)}: \hat{H}^0(K_i/k, U_{K_i,T_i'}) \longrightarrow \hat{H}^0(K_i/k, J_{K_i,T_i'}),$$

where $\alpha_r^{(i)}$'s are the maps obtained from taking cohomology groups for the exact sequence

$$0 \longrightarrow U_{K_i,T_i'} \xrightarrow{\alpha^{(i)}} J_{K_i,T_i'} \xrightarrow{\beta^{(i)}} C_{K_i,T_i'} \longrightarrow 0$$

as in (5), (6). Note that, since $K_i/k$ is a cyclic extension by the condition (A), $\hat{H}^0=H^2$ and $\alpha_0^{(i)}=\alpha_2^{(i)}$. Using the genus formula (7) in order to estimate the orders of the kernels of $\lambda_i$'s, we obtain the following upper bound of the order of the Selmer group.

THEOREM 1. *Assume that $E(k)$ contains $E[p]$ and the condition (A) holds. Then*

$$|S^{(p)}(E/k)| \le p^{2+d-r}\,\frac{|(Cl_{K_1,T_1'})^{G_1}|}{|(Cl_{k,T_1})^p|}\,\frac{|(Cl_{K_2,T_2'})^{G_2}|}{|(Cl_{k,T_2})^p|},$$

*where $d=[k:\mathbf{Q}]$ and $r=|R_1\backslash T_1|+|R_2\backslash T_2|$.*

PROOF. By the definition, the order of the kernel of $\lambda_i$ can be written as

$$|\operatorname{Ker}\lambda_i| = \frac{|U_{k,T_i}/U_{k,T_i}{}^p|}{|\hat{H}^0(K_i/k, U_{K_i,T_i'})|}\,|\operatorname{Ker}\alpha_2^{(i)}| \qquad (i=1, 2).$$

By the Dirichlet's unit theorem, we have $|U_{k,T_i}/U_{k,T_i}{}^p|=p^{d/2+|T_i|}$ where $d=[k:\mathbf{Q}]$.

Let $Cl_{k,T_i}$, be the group $J_k/k^\times J_{k,T_i}$ as above. Then, there exists an exact sequence

$$0\longrightarrow U_{k,T_i}k^{\times p}/k^{\times p}\longrightarrow H^1(k_{T_i}/k,\mu_p)\longrightarrow (Cl_{k,T_i})_p\longrightarrow 0$$

where $(\ )_p$ denotes the $p$-torsion subgroup. Moreover the next diagram is commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \prod_{i=1,2} U_{K_i,T_i'}k^{\times p}/k^{\times p} & \longrightarrow & \prod_{i=1,2} H^1(k_{T_i}/k,\mu_p) & \longrightarrow & \prod_{i=1,2}(Cl_{k,T_i})_p & \longrightarrow & 0 \\ & & \big\downarrow \lambda:=\prod\lambda_i & & \big\downarrow f & & \big\downarrow & & \\ 0 & \longrightarrow & \prod_{i=1,2}\hat{H}^0(K_i/k,J_{K_i,T_i'}) & \xrightarrow{id.} & \prod_{i=1,2}\hat{H}^0(K_i/k,J_{K_i,T_i'}) & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

where $f$ is defined in Lemma 2. Then, by the Snake Lemma we see

$$|\operatorname{Ker} f|=\frac{|\operatorname{Coker} f|\,|(Cl_{k,T_1})_p|\,|(Cl_{k,T_2})_p|\,|\operatorname{Ker}\lambda|}{|\operatorname{Coker}\lambda|}.$$

Since $|\operatorname{Coker}\lambda|\geq|\operatorname{Coker} f|$, we obtain

$$|S^{(p)}(E/k)|\leq|\operatorname{Ker} f|\leq|(Cl_{k,T_1})_p|\,|(Cl_{k,T_2})_p|\,|\operatorname{Ker}\lambda|.$$

On the other hand, by the genus formula, we have

$$|\operatorname{Ker}\alpha_2^{(i)}|=\frac{[K:k]\,|\hat{H}^0(K_i/k,U_{K_i,T_i'})|}{e_i}\,\frac{|(Cl_{K_i,T_i'})^{G_i}|}{|Cl_{k,T_i}|}\qquad(i=1,2),$$

where $e_i=\prod_{v\in M_k}e_v$ is the product of relative ramification indices in $K_i/k$. Note that, since $K_i/k$ is a cyclic extension of degree $p$ by condition (A), the residue class degrees are equal to 1 for any $v\in T_i$. Hence we have

$$\begin{aligned}|\operatorname{Ker}\lambda|&=|\operatorname{Ker}\lambda_1|\,|\operatorname{Ker}\lambda_2|\\ &=\frac{p^{2+d+|T_1|+|T_2|}}{e_1e_2}\,\frac{|(Cl_{K_1,T_1'})^{G_1}|}{|Cl_{k,T_1}|}\,\frac{|(Cl_{K_2,T_2'})^{G_2}|}{|Cl_{k,T_2}|}.\end{aligned}$$

Since $|Cl_{k,T_i}|/|(Cl_{k,T_i})_p|=|(Cl_{k,T_i})^p|$, and $e_i=p^{|R_i|}$, we obtain the desired estimate

$$|S^{(p)}(E/k)|\leq p^{2+d-r}\frac{|(Cl_{K_1,T_1'})^{G_1}|}{|(Cl_{k,T_1})^p|}\,\frac{|(Cl_{K_2,T_2'})^{G_2}|}{|(Cl_{k,T_2})^p|}.$$

Let $\dim_p$ denote the dimension over $\mathbf{Z}/p\mathbf{Z}$. By the assumption, we have $\operatorname{rank} E(k)=\dim_p E(k)/pE(k)-2$, and there is an injection $\delta: E(k)/pE(k)\to S^{(p)}(E/k)$. Hence we have the following

COROLLARY. *We have an inequality*

$$\operatorname{rank} E(k)\leq d-r+\operatorname{ord}_p\frac{|(Cl_{K_1,T_1'})^{G_1}|}{|(Cl_{k,T_1})^p|}+\operatorname{ord}_p\frac{|(Cl_{K_2,T_2'})^{G_2}|}{|(Cl_{k,T_2})^p|}.$$

## 4. The case for $p=2$.

In the case of $p=2$, the situation on the infinite places of $k$ is slightly different from the one for odd primes. For an odd prime $p$, the condition $E[p]\subset E(k)$ implies that $k$ is a totally imaginary number filed. On the other hand, we deduce nothing about the infinite places $k$ from the condition $E[2]\subset E(k)$. However, if we make some assumption on the infinite places in order to simplify the situation (for example, $k$ is totally imaginary), then we can estimate the 2-Selmer group for $E/k$ in a similar way for odd primes. In the case that $k$ is a totally real number field, we also obtain a similar estimate as follows.

Let $k$ be a totally real number field, $E$ be an elliptic curve defined over $k$. Let assume that $E[2]\subset E(k)$ and the following condition (B) holds.

(B) There are such generators $P_1$, $P_2$ of 4-torsion subgroup $E[4]$ over $\mathbf{Z}/4\mathbf{Z}$ that the definition fields $K_1=k(P_1)$, $K_2=k(P_2)$ of $P_1$, $P_2$ over $k$ are both cyclic extensions of degree 2 over $k$, and if we put

$$G_i=\mathrm{Gal}(K_i/k)=\langle\tau_i\rangle \qquad (i=1, 2),$$

then

$$P=P_1^{\tau_1}-P_1, \qquad P'=P_2^{\tau_2}-P_2$$

generate $E[2]$ over $\mathbf{Z}/2\mathbf{Z}$.

This is the same condition as (A) for $p=2$ in Section 3.

Let $R_i$ be the set of places of $k$ which ramify in $K_i$ $(i=1, 2)$, and put

$$T_i^{(2)}:=(R_i\cap S)\cup\{\text{the places lying above } 2\}\cup M_k^{\infty}.$$

THEOREM 2. *Under the above conditions we have*

$$|S^{(2)}(E/k)|\le 2^{2+r}\frac{|(Cl_{K_1,T_1'^{(2)}})^{G_1}|}{|(Cl_{k,T_1^{(2)}})^2|}\frac{|(Cl_{K_2,T_2'^{(2)}})^{G_2}|}{|(Cl_{k,T_2^{(2)}})^2|}$$

*where* $r:=|T_1^{(2)}|+|T_2^{(2)}|-|R_1|-|R_2|$.

PROOF. Each element of $S\backslash T_i^{(2)}$ $(i=1, 2)$ is a finite place. Hence the argument is completely similar to the one for odd primes. Note that since $T_i^{(2)}$ contains all infinite places of $k$, for the $T_i^{(2)}$-unit group $U_{k,T_i^{(2)}}$, the order of the group $U_{k,T_i^{(2)}}/U_{k,T_i^{(2)}}^2$ is equal to $2^{|T_i^{(2)}|}$ by Dirichlet's theorem.

## 5. Elliptic curves without complex multiplication.

In this section, we show that if an elliptic curve has no complex multiplication, then choosing some prime number $p$ and replacing $k$ by its finite extension if necessary, we can make the condition (A) in Section 3 to be valid.

Let $E/k$ be an elliptic curve defined over a number field of finite degree. For any integer $m\geq 2$, $E[m]$ is a free $(\mathbf{Z}/m\mathbf{Z})$-module of rank 2, and $G(m)=\mathrm{Gal}(k(m)/k)$ acts on $E[m]$ where $k(m)=k(E[m])$. Hence by taking some generators of $E[m]$ over $\mathbf{Z}/m\mathbf{Z}$, there exists a homomorphism $G(m)\rightarrow GL_2(\mathbf{Z}/m\mathbf{Z})$. Let us assume that $E$ has no complex multiplication. Then by Serre [6], [8], we know that for all but finitely many prime numbers $p$, the above homomorphisms are isomorphisms:

$$G(p^n) \xrightarrow{\sim} GL_2(\mathbf{Z}/p^n\mathbf{Z}) \qquad \text{for any } n\geq 1\,. \tag{8}$$

From an elementary fact, the orders of $GL_2(\mathbf{Z}/p\mathbf{Z})$ and $GL_2(\mathbf{Z}/p^2\mathbf{Z})$ can be given by

$$|GL_2(\mathbf{Z}/p\mathbf{Z})|=p(p^2-1)(p-1)\,, \qquad |GL_2(\mathbf{Z}/p^2\mathbf{Z})|=p^5(p^2-1)(p-1)\,.$$

Hence, for any prime $p$ which satisfies (8), $[k(p^2):k(p)]=p^4$. Let $P_1, P_2\in E[p^2]$ be any generators of $E[p^2]$ over $\mathbf{Z}/p^2\mathbf{Z}$. Then it is easily seen that for $\sigma\in G(p^2)$, $\sigma$ fixes $E[p]$ and $\mu_{p^2}$ if and only if $([p]P_1)^\sigma=[p]P_1$, $([p]P_2)^\sigma=[p]P_2$ and $\sigma\in SL_2(\mathbf{Z}/p^2\mathbf{Z})$, because $[p]P_1$ and $[p]P_2$ generate $E[p]$ over $\mathbf{Z}/p\mathbf{Z}$. We rewrite this condition in terms of matrices. First, since $\sigma$ fixes $[p]P_1$ and $[p]P_2$, putting $\sigma=\begin{pmatrix} a & b \\ c & d\end{pmatrix}$, $a, b, c, d\in\mathbf{Z}/p^2\mathbf{Z}$,

$$\begin{pmatrix} p \\ 0\end{pmatrix}=\begin{pmatrix} a & b \\ c & d\end{pmatrix}\begin{pmatrix} p \\ 0\end{pmatrix}=\begin{pmatrix} ap \\ cp\end{pmatrix}, \qquad \begin{pmatrix} 0 \\ p\end{pmatrix}=\begin{pmatrix} a & b \\ c & d\end{pmatrix}\begin{pmatrix} 0 \\ p\end{pmatrix}=\begin{pmatrix} bp \\ dp\end{pmatrix}.$$

Hence we have $a\equiv d\equiv 1 \pmod{p}$ and $b\equiv c\equiv 0 \pmod{p}$. Then if we put $\sigma=\begin{pmatrix} 1+p\alpha & p\beta \\ p\gamma & 1+p\eta\end{pmatrix}$ for some $\alpha$, $\beta$, $\gamma$, $\eta\in\mathbf{Z}/p^2\mathbf{Z}$, since $\sigma$ is in $SL_2(\mathbf{Z}/p^2\mathbf{Z})$, $\eta$ must be equal to $-\alpha$. Therefore $\sigma\in H:=\mathrm{Gal}(k(p^2)/(k(p))(\mu_{p^2}))$ if and only if it is in the form

$$\sigma=\begin{pmatrix} 1+p\alpha & p\beta \\ p\gamma & 1-p\alpha\end{pmatrix} \qquad \text{for some } \alpha,\ \beta,\ \gamma\in\mathbf{Z}/p^2\mathbf{Z}\,.$$

The number of such $\sigma$'s is $p^3$, namely $|H|=p^3$, hence $[(k(p))(\mu_{p^2}):k(p)]=p$. Moreover, the subgroup of $H$ consisting of the elements which fix $P_1$ is a group generated by $\sigma_1=\begin{pmatrix} 1 & p \\ 0 & 1\end{pmatrix}$. Similarly the subgroup which fixes $P_2$ is generated by $\sigma_2=\begin{pmatrix} 1 & 0 \\ p & 1\end{pmatrix}$ and their orders are both $p$. Hence if we put

$$K=(k(p))(\mu_{p^2}, P_1)\cap(k(p))(\mu_{p^2}, P_2)\,,$$

then $K(P_1)$ and $K(P_2)$ are both cyclic extensions of $K$ whose Galois Groups are generated by $\sigma_2$ and $\sigma_1$ respectively:

$$G_1=\mathrm{Gal}(K(P_1)/K)=\langle\sigma_2\rangle=\langle\sigma_2|_{K(P_1)}\rangle\,,$$
$$G_2=\mathrm{Gal}(K(P_2)/K)=\langle\sigma_1\rangle=\langle\sigma_1|_{K(P_2)}\rangle\,.$$

Moreover,

$$P_1^{\sigma_2}=\begin{pmatrix}1 & 0\\ p & 1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\begin{pmatrix}1\\ p\end{pmatrix}=P_1+[p]P_2\,,$$

$$P_2^{\sigma_1}=\begin{pmatrix}1 & p\\ 0 & 1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=\begin{pmatrix}p\\ 1\end{pmatrix}=[p]P_1+P_2\,.$$

Hence $P_1^{\sigma_2}-P_1=[p]P_2$ and $P_2^{\sigma_1}-P_2=[p]P_1$ generate $E[p]$ over $\mathbf{Z}/p\mathbf{Z}$. Therefore we obtain the following.

PROPOSITION. *Let $E/k$ be an elliptic curve without complex multiplication, and $p$ be a prime number which satisfies the condition* (8). *Then there exists a finite extension field $K$ of $k$ such that the condition* (A) *holds for $E/K$ and $p$.*

## References

[1] N. AOKI, Selmer groups and ideal class groups, Comment. Math. Univ. St. Paul. **42** (1993), 209–229.
[2] A. BRUMER and K. KRAMER, The rank of elliptic curves, Duke Math. J. **44** (1977), 715–743.
[3] M. KAWACHI and S. NAKANO, The 2-class groups of cubic fields and 2-descents on elliptic curves, Tôhoku Math. J. **44** (1992), 557–565.
[4] W. G. MCCALLUM, On the Shafarevich-Tate group of the jacobian of a quotient of the Fermat curve, Invent. Math. **93** (1988), 637–666.
[5] J. S. MILNE, *Arithmetic Duality Theorems*, Academic Press (1986).
[6] J.-P. SERRE, *Abelian l-Adic Representation and Elliptic Curves*, Benjamin (1968).
[7] J.-P. SERRE, *Local Fields*, Springer (1979).
[8] J.-P. SERRE, Propriétés galoisiennes des points d'order fini des courbes elliptiques, Invent. Math. **15** (1972), 259–331.
[9] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Springer (1986).
[10] J. TATE, Duality theorems in Galois cohomology over number fields, *Proc. Internat. Cong. Math. Stockholm* (1962), 288–295.
[11] L. C. WASHINGTON, Class numbers of the simplest cubic fields, Math. Computation **48** (1987), 371–384.
[12] L. C. WASHINGTON, Number fields and elliptic curves, *Number Theory and Applications* (R. A. Mollin ed.), Kluwer Academic Publishers (1989), 245–278.

*Present Address*:
GRADUATE SCHOOL OF MATHEMATICS, KYUSHU UNIVERSITY 33,
HAKOZAKI, FUKUOKA, 812 JAPAN.