BULL. AUSTRAL. MATH. SOC. 11R29, 11G07, 14H52
VOL. 54 (1996) [267–274]

THE SELMER GROUPS AND THE AMBIGUOUS IDEAL CLASS GROUPS OF CUBIC FIELDS

YEN-MEI J. CHEN

In this paper, we study a family of elliptic curves with CM by $\mathbb{Q}(\sqrt{-3})$ which also admits a $\mathbb{Q}$-rational isogeny of degree 3. We find a relation between the Selmer groups of the elliptic curves and the ambiguous ideal class groups of certain cubic fields . We also find some bounds for the dimension of the 3-Selmer group over $\mathbb{Q}$, whose upper bound is also an upper bound of the rank of the elliptic curve.

0. INTRODUCTION

Let D be a cube-free integer. We consider the elliptic curve

$$E/\mathbb{Q} : y^2 = x^3 + D^2,$$

which has j-invariant 0 and has complex multiplication $\pi = \sqrt{-3}$. More precisely, π is the endomorphism

$$\begin{aligned} \pi : E/\mathbb{Q} &\longrightarrow E/\mathbb{Q} \\ (x,y) &\mapsto \left(-\frac{x^3+4D^2}{3x^2}, -\frac{y(x^3-8D^2)}{3\sqrt{-3}x^3}\right). \end{aligned}$$

We set the following notation.

$$\begin{aligned} S_1 &= \{p \text{ prime } : p \mid D \text{ and } p \equiv 1 \mod 3\} \\ S_2 &= \{p \text{ odd prime } : p \mid D \text{ and } p \equiv 2 \mod 3\} \\ l_1 &= |S_1| \\ l_2 &= |S_2| \\ k &= \mathbb{Q}(\omega),\ \omega = \frac{1+\sqrt{-3}}{2} \\ K &= k\left(\sqrt[3]{2D}\right) \\ U_k &= \text{the group of units of } k \\ U_K &= \text{the group of units of } K \\ C_K &= \text{the 3-class group of } K \\ C_K^{(\tau)} &= \{a \in C_K : a^\tau = a\}, \end{aligned}$$

Received 1st November, 1995.

where τ is a generator of the Galois group of the field extension K/k and $C_K^{(\tau)}$ is called the ambiguous ideal class group of K/k. We first define a map

$$\Psi : S^{(\pi)}(E/k) \longrightarrow C_K^{(\tau)},$$

then we can obtain an upper bound of the rank of the Selmer group $S^{(3)}(E/\mathbb{Q})$ by using the theorem of Gerth [**3**] which gives an explicit computation of the rank of the group $C_K^{(\tau)}$. On the other hand, we can obtain a lower bound by using the duality theorem of Cassels [**1**]. More precisely, we can obtain the following inequalities:

$$l_2 + \varepsilon_2 - 3 \leqslant \dim_{\mathbb{F}_3} S^{(3)}(E/\mathbb{Q}) \leqslant 2l_1 + l_2 - \varepsilon_1 + 1$$

where ε_1 and ε_2, both depending on D, are integers 0, 1, or 2. For the family of curves $E/\mathbb{Q} : y^2 = x^3 + D^3$, Frey [**2**] showed that the rank of the Selmer group of a 3-isogeny is closely related to the class number of the quadratic field $\mathbb{Q}\left(\sqrt{D}\right)$. Also Jan Nekevář [**4**] proved some analogous results for the elliptic curve given by $Dy^2 = 4x^3 - 27$ which is isomorphic to the curve given by $y^2 = x^3 - 432D^3$. Our result gives explicit bounds for the dimension of $S^{(3)}(E/k)$ and implies that the dimension can be arbitrarily large.

1. The Selmer Group $S^{(\pi)}(E/k)$

Definition: Let F be a number field and let $\phi : E/F \to E'/F$ be an isogeny defined over F. Then the ϕ-Selmer group of E/F is the subgroup of $H^1\left(G_{\overline{F}/F}, E[\phi]\right)$ defined by

$$S^{(\phi)}(E/F) \overset{def}{\equiv} \ker\{H^1\left(G_{\overline{F}/F}, E[\phi]\right) \to \prod_{v \in M_F} H^1\left(G_{\overline{F}_v/F_v}, E\right)\}.$$

Observe that the map $\pi : E/\mathbb{Q} \longrightarrow E/\mathbb{Q}$ given as above is defined over k but not over $\mathbb{Q}$ and that $E[\pi]$ is isomorphic to μ_3 as a $\mathrm{Gal}\left(\overline{k}/k\right)$-module, and thus we have

$$H^1\left(G_{\overline{k}/k}, E[\pi]\right) \cong k^*/k^{*3}.$$

Given an element $d \in k^*$, it corresponds to the homogeneous space of E which can be given by

$$C_d : dx^3 + d^2y^3 = 2Dz^3.$$

Then such d will be an element of the Selmer group $S^{(\pi)}(E/k)$ provided that C_d admits a k_v-rational point for all $v \in M_k$. For any such d, since $2D$ is a perfect cube in K

the principal divisor (d) must be a cube of some divisor in K, say $(d) = \mathfrak{a}^3$. It is clear that $\mathfrak{a}^\tau = \mathfrak{a}$, so $\mathfrak{a} \in C_K^{(\tau)}$. Thus we can define a homomorphism

$$\Psi : S^{(\pi)}(E/k) \longrightarrow C_K^{(\tau)}$$

by $\Psi(d) = \mathfrak{a}$. Then it is clear that $\ker \Psi = U_K \cdot K^{*3} \cap k^*/k^{*3}$. Note that Ψ induces two maps

$$\Psi^+ : S^{(\pi)}(E/k)^+ \longrightarrow C_K^{(\tau)^+},$$
$$\Psi^- : S^{(\pi)}(E/k)^- \longrightarrow C_K^{(\tau)^-}$$

where $+$ and $-$ refer to the action of $\mathrm{Gal}(k/\mathbb{Q})$. Observe that all of the groups mentioned above are $\mathbb{F}_3$-vector spaces.

Lemma 1.1. (Gerth)

(a) $\dim_{\mathbb{F}_3} C_K^{(\tau)} = 2l_1 + l_2 - \varepsilon_1$;

(b) $\dim_{\mathbb{F}_3} C_K^{(\tau)^+} = l_1$;

(c) $\dim_{\mathbb{F}_3} C_K^{(\tau)^-} = l_1 + l_2 - \varepsilon_1$;

where ε_1 (depending on D) is 0, 1 or 2.

Proof: See [3]. ∎

Lemma 1.2.

(a) $\dim_{\mathbb{F}_3} S^{(\pi)}(E/k) \leqslant \dim_{\mathbb{F}_3} C_K^{(\tau)} + 2$.

(b) $\dim_{\mathbb{F}_3} S^{(\pi)}(E/k)^+ \leqslant \dim_{\mathbb{F}_3} C_K^{(\tau)^+} + 1$.

(c) $\dim_{\mathbb{F}_3} S^{(\pi)}(E/k)^- \leqslant \dim_{\mathbb{F}_3} C_K^{(\tau)^-} + 1$.

Proof: (a) We already see that Ψ is a homomorphism from $S^{(\pi)}(E/k)$ to $C_K^{(\tau)}$ with $\ker\Psi = U_K \cdot K^{*3} \cap k^*/k^{*3}$. Since $U_K \cdot K^{*3} \cap k^* = U_k \cdot K^{*3} \cap k^*$, we have $U_K \cdot K^{*3} \cap k^*/k^{*3} = \{1, 2D, 4D^2\} \cdot U_k \cdot k^{*3}/k^{*3}$. The Dirichlet Unit Theorem implies that $U_k = \mu_6$. Hence $\dim_{\mathbb{F}_3} \ker\Psi = 2$ and and thus we have

$$\dim_{\mathbb{F}_3} S^{(\pi)}(E/k) \leqslant \dim_{\mathbb{F}_3} C_K^{(\tau)} + 2.$$

(b) Observe that $\ker\Psi^+$ is generated by $\{2D\}$, and thus $\dim_{\mathbb{F}_3} \ker\Psi^+ = 1$. Therefore (b) holds.

(c) Similar to (b) except that $\ker\Psi^-$ is generated by $\{\omega\}$. ∎

Proposition 1.3.

(a) $\dim_{\mathbb{F}_3} S^{(\pi)}(E/k) \leqslant l_1 + l_2 - \varepsilon_1 + 2$.

(b) $\dim_{\mathbb{F}_3} S^{(\pi)}(E/k)^+ \leqslant l_1 + 1$.

(c) $\dim_{\mathbb{F}_3} S^{(\pi)}(E/k)^- \leqslant l_1 + l_2 - \varepsilon_1 + 1$.

Proof: Follows immediately from Lemma 1.1 and Lemma 1.2. ∎

2. The Selmer Group $S^{(3)}(E/k)$

Recall that $\pi^2 = -3$, so we have the following exact sequence

$$0 \longrightarrow E[\pi] \hookrightarrow E[3] \xrightarrow{\pi} E[\pi] \longrightarrow 0.$$

Taking Galois cohomology as $G_{K/k}$, $G_{\overline{k}/k}$, and $G_{\overline{K}/K}$-modules respectively, we know that each row of the following commutative diagram is exact except at the end. Since we can view $G_{\overline{K}/K}$ as a subgroup of $G_{\overline{k}/k}$, the Inf-Res sequence implies that each column is also exact.

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 \to E[\pi] \to & & H^1(G_{K/k}, E[\pi]) & \to & H^1(G_{K/k}, E[3]) & \xrightarrow{\tilde{\pi}} & H^1(G_{K/k}, E[\pi]) \xrightarrow{?} 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 \to E[\pi] \to & & H^1\left(G_{\overline{k}/k}, E[\pi]\right) & \to & H^1\left(G_{\overline{k}/k}, E[3]\right) & \xrightarrow{\tilde{\pi}} & H^1\left(G_{\overline{k}/k}, E[\pi]\right) \xrightarrow{?} 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & 0 \to & H^1\left(G_{\overline{K}/K}, E[\pi]\right)^{G_{K/k}} & \to & H^1\left(G_{\overline{K}/K}, E[3]\right)^{G_{K/k}} & \xrightarrow{\tilde{\pi}} & H^1\left(G_{\overline{K}/K}, E[\pi]\right)^{G_{K/k}} \xrightarrow{?} 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & 0 \to & H^2(G_{K/k}, E[\pi]) & \to & H^2(G_{K/k}, E[\pi]) & \to & H^2(G_{K/k}, E[\pi]) \to \cdots \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \vdots & & \vdots & & \vdots
\end{array}$$

By routine computations, we have the following equalities:

$$H^1(G_{K/k}, E[\pi]) \cong H^2(G_{K/k}, E[\pi]) \cong \mathbb{Z}/3\mathbb{Z},$$
$$H^1(G_{K/k}, E[3]) \cong H^2(G_{K/k}, E[3]) \cong \mathbb{Z}/3\mathbb{Z}.$$

Then it is clear that the first row is exact. Note that $E[3]$ is isomorphic to $\mu_3 \times \mu_3$ as a Gal $(\overline{K}/K)$-module; thus we have

$$H^1\left(G_{\overline{K}/K}, E[3]\right) \cong K^*/K^{*3} \times K^*/K^{*3}.$$

The third row is equivalent to the following exact sequence, and therefore it is exact.

$$\begin{array}{ccccccc}
0 \longrightarrow K^*/K^{*3} & \longrightarrow & K^*/K^{*3} \times K^*/K^{*3} & \longrightarrow & K^*/K^{*3} \longrightarrow 0 \\
 & a \mapsto (a,1) & & (a,b) \mapsto b &
\end{array}$$

Combining all the observations above, we have the following lemma:

https://doi.org/10.1017/S000497270001772X Published online by Cambridge University Press

Lemma 2.1. *The $\mathbb{F}_3$-dimension of the cokernel of the map*

$$\widetilde{\pi}: H^1\left(G_{\overline{k}/k}, E[3]\right) \to H^1\left(G_{\overline{k}/k}, E[\pi]\right)$$

is less than or equal to 1.

Proposition 2.2. *The $\mathbb{F}_3$-dimension of the cokernel of the map*

$$\widetilde{\pi}: S^{(3)}(E/k) \longrightarrow S^{(\pi)}(E/k)$$

is less than or equal to 2.

Proof: Given arbitrary $a \in S^{(\pi)}(E/k)$ – in other words the corresponding homogeneous space is locally trivial everywhere — it is easy to check that at least one of a, $2Da$, $4D^2a$ is locally a cube everywhere except at v, $v \mid 3$. If a is in the image of the map $\widetilde{\pi}: H^1\left(G_{\overline{k}/k}, E[3]\right) \to H^1\left(G_{\overline{k}/k}, E[\pi]\right)$ and it is locally a cube at v, $v \mid 3$, then $(1, a) \in S^{(3)}(E/k)$ and $\widetilde{\pi}((1, a)) = a$. It is easy to see that given a finite set T of indepedent elements in k^*/k^{*3} one can find another set T' such that T and T' generate the same subgroup in k^*/k^{*3} and every element in T' is a cube at v, $v \mid 3$ with at most one exception. Therefore Lemma 2.1 implies that the $\mathbb{F}_3$-dimension of the cokernel of the map $S^{(3)}(E/k) \xrightarrow{\widetilde{\pi}} S^{(\pi)}(E/k)$ is less than or equal to 2. ∎

Corollary 2.3. *Assume that $Ш(E/k)[3^\infty]$ is finite. Assume that either D is not divisible by 3 or D is divisible by 9. Then the sequence*

$$0 \to E[\pi] \to S^{(\pi)}(E/k) \to S^{(3)}(E/k) \xrightarrow{\widetilde{\pi}} S^{(\pi)}(E/k) \to 0$$

is exact.

Proof: It suffices to show that

$$S^{(3)}(E/k) \xrightarrow{\widetilde{\pi}} S^{(\pi)}(E/k) \to 0$$

is exact. Given arbitrary $a \in S^{(\pi)}(E/k)$, the second hypothesis implies that a is locally a cube at v, $v \mid 3$. Thus $(1, a) \in S^{(3)}(E/k)$ and $\widetilde{\pi}((1, a)) = a$. Again according to Lemma 2.1, we know that $\mathbb{F}_3$-dimension of the cokernel of the map $S^{(3)}(E/k) \xrightarrow{\widetilde{\pi}} S^{(\pi)}(E/k)$ is less than or equal to 1. Now the first hypothesis implies that $S^{(3)}(E/k) \xrightarrow{\widetilde{\pi}} S^{(\pi)}(E/k)$ is surjective if and only if $\dim_{\mathbb{F}_3} S^{(3)}(E/k)$ is odd. Therefore we need the following lemma to complete the proof. ∎

Lemma. $\dim_{\mathbb{F}_3} S^{(3)}(E/k)$ *is odd.*

Proof: 1^0 There is an exact sequence

$$0 \longrightarrow E(k)/3(E(k)) \longrightarrow S^{(3)}(E/k) \longrightarrow Ш(E/k)[3] \longrightarrow 0$$

https://doi.org/10.1017/S000497270001772X Published online by Cambridge University Press

which implies $\dim_{\mathbb{F}_3} S^{(3)}(E/k)$ and $\dim_{\mathbb{F}_3} E(k)/3(E(k))$ have the same parity, thus it suffices to show that $\dim_{\mathbb{F}_3} E(k)/3(E(k))$ is odd.

2^0 Consider the following sequence:

$$\begin{gathered} 0 \longrightarrow E(\mathbb{Q}) \xrightarrow{\alpha} E'(k) \xrightarrow{\beta} E'(\mathbb{Q}) \longrightarrow 0 \\ (x,\, y) \mapsto P = \left(-3x, -3\sqrt{-3y}\right) \mapsto P + P^{\sigma} \end{gathered}$$

where E' is given by $E'/\mathbb{Q} : y^2 = x^3 - 27D^2$ and is isogeneous to the original curve E. We claim that the sequence is exact. It is clear that α is injective and that $\ker \beta = \operatorname{im} \alpha$. We show that β is surjective. Given any point $Q = (x, y) \in E'(\mathbb{Q})$, then $P = (x\omega, -y)$ and $P^{\sigma} = \left(x\omega^2, -y\right)$ are both k-rational points. By an easy computation, we have $Q = P + P^{\sigma} = \beta(P)$, and so β is surjective.

Since the group $E'(\mathbb{Q})$ is torsion-free and finitely generated, it is a projective $\mathbb{Z}$-module, and thus the above sequence splits. By taking tensor products with the group $\mathbb{Z}/3\mathbb{Z}$, we obtain another exact sequence

$$0 \to E(\mathbb{Q})/3E(\mathbb{Q}) \to E'(k)/3E'(k) \to E'(\mathbb{Q})/3E'(\mathbb{Q}) \to 0.$$

Therefore we have

$$\begin{aligned} \dim_{\mathbb{F}_3} E(k)/3(E(k)) &= \dim_{\mathbb{F}_3} E(\mathbb{Q})/3E(\mathbb{Q}) + \dim_{\mathbb{F}_3} E'(\mathbb{Q})/3E'(\mathbb{Q}) \\ &= 2 \dim_{\mathbb{F}_3} E'(\mathbb{Q})/3E'(\mathbb{Q}) + 1. \end{aligned}$$

(Since $E_{\mathrm{tors}}(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ and $\operatorname{rank}(E(\mathbb{Q})) = \operatorname{rank}(E'(\mathbb{Q}))$.) $\square$

3. Bounds for The Dimension of The Selmer Group $S^{(3)}(E/\mathbb{Q})$

Now we turn to consider the 3-isogeny

$$\begin{aligned} \lambda : E/\mathbb{Q} &\longrightarrow E'/\mathbb{Q} \\ (x, y) &\mapsto \left(\frac{x^3 + 4D^2}{x^2}, \frac{y\left(x^3 - 8D^2\right)}{x^3}\right) \end{aligned}$$

and its dual

$$\begin{aligned} \widehat{\lambda} : E'/\mathbb{Q} &\longrightarrow E/\mathbb{Q} \\ (x, y) &\mapsto \left(\frac{x^3 + 4D^2}{81x^2}, \frac{y\left(x^3 - 216D^2\right)}{729x^3}\right). \end{aligned}$$

Then we can identify

$$\begin{gathered} S^{(\lambda)}(E/\mathbb{Q}) = S^{(\pi)}(E/k)^{+}, \; S^{(\hat{\lambda})}(E'/\mathbb{Q}) = S^{(\pi)}(E/k)^{-}, \\ S^{(3)}(E/\mathbb{Q}) = S^{(3)}(E/k)^{+}. \end{gathered}$$

Denote the dimensions of $S^{(\lambda)}(E/\mathbb{Q})$, $S^{(\hat{\lambda})}(E'/\mathbb{Q})$, $S^{(3)}(E/\mathbb{Q})$ by s, s', t respectively. Now we state the duality theorem of Cassels, which will be used latter.

Theorem. (Cassels [1])

$$\frac{|S^{(\lambda)}(E/\mathbb{Q})|}{|S^{(\hat{\lambda})}(E'/\mathbb{Q})|}=\frac{|E_{\rm tors}(\mathbb{Q})|}{|E'_{\rm tors}(\mathbb{Q})|}\cdot\prod_p\frac{c'_p}{c_p}\cdot\frac{\int_{E'(\mathbb{R})}|\omega'_{min}|_\infty}{\int_{E(\mathbb{R})}|\omega_{min}|_\infty}.$$

Lemma 3.1. *$s-s'=-l_2-\varepsilon_2$ where ε_2 depending on D is -2, -1, 0 or 1.*

Proof: 1^0 By elementary calculation,

$$\frac{\int_{E'(\mathbb{R})}|\omega'_{min}|_\infty}{\int_{E(\mathbb{R})}|\omega_{min}|_\infty}=\frac{1}{3}.$$

2^0 By using the Tate's algorithm [5], we can obtain the following equalities :

$$\text{if } p\nmid 6D,\ c_p=c'_p=1;\quad \text{if } p\mid D,\ p\neq 2,3,\quad \frac{c_p}{c'_p}=\begin{cases}3 & \text{if } p\equiv 2 \mod 3,\\ 1 & \text{if } p\equiv 1 \mod 3;\end{cases}$$

$$\frac{c_2}{c'_2}=\begin{cases}3 & \text{if D is odd },\\ 1 & \text{if D is even };\end{cases}\qquad \frac{c_3}{c'_3}=\begin{cases}3 & \text{if } 3\mid D,\\ 1 & \text{if } D\equiv 1,2,4,8 \mod 9,\\ \dfrac{1}{3} & \text{if } D\equiv 5,7 \mod 9.\end{cases}$$

By combining all the above equalities, Lemma 3.1 will follow. ∎

Finally, we obtain an upper bound and a lower bound for the dimension of the Selmer group $S^{(3)}(E/\mathbb{Q})$.

Proposition 3.2. $l_2+\varepsilon_2-3\leqslant t\leqslant 2l_1+l_2-\varepsilon_1+1$

Proof: 1^0 According to Proposition 2.2 we already know that the sequence

$$0\to E[\pi]\to S^{(\pi)}(E/k)\to S^{(3)}(E/k)\xrightarrow{\widetilde{\pi}} S^{(\pi)}(E/k)$$

is exact and dim coker $\widetilde{\pi}\leqslant 2$. By considering the Galois group Gal$(k/\mathbb{Q})$ acting on each group, we obtain another exact sequence

$$0\to E[\lambda]\to S^{(\lambda)}(E/\mathbb{Q})\to S^{(3)}(E/\mathbb{Q})\xrightarrow{\widetilde{\lambda}} S^{(\hat{\lambda})}(E'/\mathbb{Q})$$

with dim coker $\widetilde{\lambda}\leqslant 2$. Thus

$$s+s'-3\leqslant t\leqslant s+s'-1.$$

2^0 By combining Lemma 3.1 and Proposition 1.3, we have

$$l_2+\varepsilon_2-3\leqslant t\leqslant 2l_1+l_2+\varepsilon_1+1.$$

Thus the proposition holds. ∎

https://doi.org/10.1017/S000497270001772X Published online by Cambridge University Press

REFERENCES

[1] J.W.S. Cassels, 'Arithmetic on Curves of Genus 1', *J. Reine Angew. Math.* **217** (1965), 180–199.

[2] G. Frey, 'Die Klassgruppe Quadratischer und Kubischer Zahlkörper und die Selmer Gruppen Gewisser Elliptische Kurven', *Manuscripta Math.* **16** (1975), 333–362.

[3] F. Gerth, 'On 3-class groups of pure cubic fields', *J. Reine Angew. Math.* **278/279** (1975), 52–62.

[4] J. Nekevář, 'Class number of quadratic fields and Shimura's correspondence', *Math. Ann.* **287** (1990), 577–594.

[5] J. Tate, 'Algorithm for determining the type of a singular fiber in an elliptic pencil', in *Lecture Notes Mathematics* **476** (Springer-Verlag, Berlin, Heidelberg, New York, 1975), pp. 33–52.

Department of Mathematics
Tamkang University
Tamshui, Taipei 25137
Taiwan
Republic of China
e-mail: ymjchen@mail.tku.edu.tw