A note on the Selmer group of the elliptic curve $y^2 = x^3 + Dx$

By Takeshi GOTO

Graduate School of Mathematics, Kyushu University 33, 6-10-1, Hakozaki, Higashi-ku, Fukuoka 812-8581

(Communicated by Heisuke HIRONAKA, M. J. A., Sept. 12, 2001)

Abstract: We present an explicit formula for the Selmer rank of the elliptic curve $y^2 = x^3 + Dx$. Using this formula, we give some results analogous to Iskra's theorem.

Key words: Selmer group; elliptic curve; congruent number.

1. Introduction. In this note, we study the $\mathbf{Q}$-rank of the elliptic curve defined by

$$E_D : y^2 = x^3 + Dx \quad (D \in \mathbf{Q}).$$

We can suppose without loss of generality that D is a fourth-power free integer and not divided by 4 (if necessary, we must consider the dual curve E_{-4D}, whose $\mathbf{Q}$-rank is equal to that of E_D). Bremner and Cassels [4] studied the rank of E_D when D is a prime, and Yoshida [9] did when D is a product of two distinct primes. In both cases, one can obtain the upper bound for the rank by the 2-descent method via 2-isogeny. In this note, we call this upper bound the *Selmer rank*. It is believed that the parity of the Selmer rank is equal to that of the actual rank of the curve. Birch and Stephens [3] give the formula for the parity of the Selmer rank of E_D. The purpose of this note is to give a formula for the Selmer rank of E_D for general D.

Since E_{-n^2} is the elliptic curve connected with the congruent number problem, many mathematicians have studied this curve. For example, Iskra [5] proved the following theorem.

Theorem 1 (Iskra). *Let primes $p_1, \dots, p_r$ satisfy the following two conditions*:

- $p_i \equiv 3 \pmod 8$ *for* $\forall i$.
- $(p_i/p_j) = 1$ *for* $i < j$, *where* $(\ /\ )$ *is the Legendre symbol.*

And let $D = -p_1^2 \cdots p_r^2$. Then the rank of the curve E_D is 0.

The complete 2-descent method gives the better upper bound than the Selmer rank. Aoki [1] and Monsky (appendix in Heath-Brown [7]) give each formula for this upper bound of the curve E_{-n^2}. Iskra's theorem can be proven by Monsky's formula.

The main result of this note is an explicit formula for the Selmer rank of the curve E_D (see (2) and Theorems 4 and 5). Applying the main result, we have the following facts analogous to Iskra's theorem.

Theorem 2. *When D has one of the following forms, the rank of the curve E_D is* 0.

(a) $D = 2p_1 \cdots p_r$, *where*
$p_i \equiv 5 \pmod 8$, $(p_j/p_i) = 1$ *for* $i \neq j$.
(b) $D = 2p_1 \cdots p_r$, *where r is even and*
$p_i \equiv 5 \pmod 8$, $(p_j/p_i) = -1$ *for* $i \neq j$.
(c) $D = p_1^2 \cdots p_r^2$, *where*
$p_i \equiv 5 \pmod 8$, $(p_j/p_i) = 1$ *for* $i \neq j$.
(d) $D = p_1^2 \cdots p_r^2$, *where r is even and*
$p_i \equiv 5 \pmod 8$, $(p_j/p_i) = -1$ *for* $i \neq j$.
(e) $D = 2p_1^2 \cdots p_r^2$, *where* $p_i \equiv 5 \pmod 8$.
(f) $D = 2p_1^3 \cdots p_r^3$, *where*
$p_i \equiv 5 \pmod 8$, $(p_j/p_i) = 1$ *for* $i \neq j$.
(g) $D = 2p_1^3 \cdots p_r^3$, *where r is even and*
$p_i \equiv 5 \pmod 8$, $(p_j/p_i) = -1$ *for* $i \neq j$.

We have three remarks. Firstly, (c) and (d) are the cases of the congruent number problem with $n = 2p_1 \cdots p_r$. Secondly, calculating the Selmer rank is sufficient to deduce Theorem 2, but not sufficient to give Theorem 1. Iskra's theorem can be proven by the complete 2-descent method. Thirdly, applying the main result, we can also give the sequence of E_D whose Selmer rank can be arbitrary large. For example, if r is odd, $p_i \equiv 5 \pmod 8$, $(p_j/p_i) = -1$ for $i \neq j$, and $D = 2p_1 \cdots p_r$, then the Selmer rank of E_D is $2r - 2$.

2. Notations and some basic facts. In this section, we recall some basic facts on the Selmer group of elliptic curve with at least one rational 2-torsion. For details, we refer [8, Chapter X]. Assume that $E/\mathbf{Q}$ has a rational 2-torsion and E' is the dual curve of E. Let $\varphi : E \to E'$ be the isogeny of degree

1991 Mathematics Subject Classification. Primary 11G05; Secondary 14H52.

2, and φ' the dual isogeny of φ. In this note, we use the following notation:

- $S^{(\varphi)}(E/\mathbf{Q})$, $S^{(\varphi')}(E'/\mathbf{Q})$ are the Selmer groups associated to φ, φ'.
- $\delta_k : E'(k)/\varphi(E(k)) \to k^\times/k^{\times 2}$ is the connecting homomorphism. When $k = \mathbf{Q}_p$, we simply write δ_p for δ_k (we suppose $\mathbf{Q}_\infty = \mathbf{R}$). Similarly, we denote by δ'_k the connecting homomorphism: $E(k)/\varphi'(E'(k)) \to k^\times/k^{\times 2}$.

Then we have the formula

$$\operatorname{rank} E(\mathbf{Q}) \le \dim_{\mathbf{F}_2} S^{(\varphi)}(E/\mathbf{Q}) + \dim_{\mathbf{F}_2} S^{(\varphi')}(E'/\mathbf{Q}) - 2.$$

In this note, we call the value of the right hand side the *Selmer rank*.

We now explain the method of calculating the Selmer group. From the definition of the Selmer group, we have the equivalent definition

$$\text{(1)} \qquad \begin{cases} S^{(\varphi)}(E/\mathbf{Q}) = \bigcap_{p \in M_\mathbf{Q}} \operatorname{Im}(\delta_p), \\ S^{(\varphi')}(E'/\mathbf{Q}) = \bigcap_{p \in M_\mathbf{Q}} \operatorname{Im}(\delta'_p), \end{cases}$$

where $M_\mathbf{Q} = \{\text{primes}\} \cup \{\infty\}$ and the groups $\operatorname{Im}(\delta_p)$, $\operatorname{Im}(\delta'_p)$ are regarded as the subgroups of the group $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$.

In view of the following theorem, if one of the groups $\operatorname{Im}(\delta'_p)$ and $\operatorname{Im}(\delta_p)$ is given, the other group is automatically determined (see for example Aoki [2]).

Theorem 3. *Let $p \in M_\mathbf{Q}$ and $(\ ,\ )_p$ be the Hilbert symbol. For a subgroup $V \subset \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, we define $V^\perp = \{x \in \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} \mid (x, y)_p = 1$ for all $y \in V\}$. Then it holds that $\operatorname{Im}(\delta_p) = \operatorname{Im}(\delta'_p)^\perp$.*

3. Main result and some examples. The Selmer group is defined as the intersection of all images of connecting homomorphisms (see (1)). In the case that $p = \infty$, it clearly holds that

$$\begin{cases} D > 0 \Rightarrow \operatorname{Im}(\delta'_\infty) = \{1\},\ \operatorname{Im}(\delta_\infty) = \{\pm 1\}. \\ D < 0 \Rightarrow \operatorname{Im}(\delta'_\infty) = \{\pm 1\},\ \operatorname{Im}(\delta_\infty) = \{1\}. \end{cases}$$

The following theorems give the images of the connecting homomorphisms δ'_p and δ_p for the bad primes of E_D. In this note, we denote by $\langle c_1, \ldots, c_n \rangle$ the subgroup of $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ or $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for some $p \in M_\mathbf{Q}$ generated by $c_1, \ldots, c_n \in \mathbf{Q}$, and u represents a non-square element modulo p.

Theorem 4. *Let p be an odd prime dividing D, and $\operatorname{ord}_p(D) = a$, $D = p^a D'$. Then the images $\operatorname{Im}(\delta'_p)$ and $\operatorname{Im}(\delta_p)$ are determined as follows:*

(a) *If $a = 1$ or 3, then $\operatorname{Im}(\delta'_p) = \langle D \rangle$ and $\operatorname{Im}(\delta_p) = \langle -D \rangle$.*

(b) *Let $a = 2$ and $p \equiv 1 \pmod 4$.*
  (i) *If D is a p-adic square, then*
  - $(-D')^{(p-1)/4} \equiv 1 \pmod p$ $\Rightarrow \operatorname{Im}(\delta'_p) = \langle p \rangle$, $\operatorname{Im}(\delta_p) = \langle p \rangle$.
  - $(-D')^{(p-1)/4} \equiv -1 \pmod p$ $\Rightarrow \operatorname{Im}(\delta'_p) = \langle pu \rangle$, $\operatorname{Im}(\delta_p) = \langle pu \rangle$.

  (ii) *If D is a p-adic non-square, then $\operatorname{Im}(\delta'_p) = \mathbf{Z}_p^\times\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ and $\operatorname{Im}(\delta_p) = \mathbf{Z}_p^\times\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$.*

(c) *Let $a = 2$ and $p \equiv 3 \pmod 4$.*
  (i) *If D is a p-adic square, then $\operatorname{Im}(\delta'_p) = \{1\}$ and $\operatorname{Im}(\delta_p) = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$.*
  (ii) *If D is a p-adic non-square, then $\operatorname{Im}(\delta'_p) = \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ and $\operatorname{Im}(\delta_p) = \{1\}$.*

Note that $(-D')^{(p-1)/4} \equiv 1 \pmod p$ if and only if $-D'$ is a quartic residue modulo p.

Theorem 5. *The images $\operatorname{Im}(\delta'_2)$ and $\operatorname{Im}(\delta_2)$ are determined as follows:*

(a) *If $D \equiv 1 \pmod 8$, then $\operatorname{Im}(\delta'_2) = \{1\}$ and $\operatorname{Im}(\delta_2) = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.*
(b) *If $D \equiv 5 \pmod 8$, then $\operatorname{Im}(\delta'_2) = \langle 5 \rangle$ and $\operatorname{Im}(\delta_2) = \langle -1, 5 \rangle$.*
(c) *If $D \equiv 3 \pmod{16}$, then $\operatorname{Im}(\delta'_2) = \langle -5 \rangle$ and $\operatorname{Im}(\delta_2) = \langle -2, 5 \rangle$.*
(d) *If $D \equiv 7, 11 \pmod{16}$, then $\operatorname{Im}(\delta'_2) = \langle -1, 5 \rangle$ and $\operatorname{Im}(\delta_2) = \langle 5 \rangle$.*
(e) *If $D \equiv 15 \pmod{16}$, then $\operatorname{Im}(\delta'_2) = \langle -1 \rangle$ and $\operatorname{Im}(\delta_2) = \langle 2, 5 \rangle$.*
(f) *If D is even, then $\operatorname{Im}(\delta_2) = \langle -D \rangle$ and $\operatorname{Im}(\delta'_2)$ is determined by Theorem 3.*

Example 1. Let $D = 775 = 5^2 \cdot 31$. Note that 31 is a quartic residue modulo 5. By Theorems 4 and 5, the images of the connecting homomorphisms are determined as follows:

p	$\operatorname{Im}(\delta'_p)$	$\operatorname{Im}(\delta_p)$
∞	$\{1\}$	$\{\pm 1\}$
2	$\langle -1, 5 \rangle$	$\langle 5 \rangle$
5	$\langle 10 \rangle$	$\langle 10 \rangle$
31	$\langle 31 \rangle$	$\langle -31 \rangle$

We define some notations:

$$S = \{p \mid \operatorname{Im}(\delta'_p) - \mathbf{Z}_p^\times\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} \ne \phi\} \cup S_\infty,$$
$$T = \{p \mid \operatorname{Im}(\delta_p) - \mathbf{Z}_p^\times\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} \ne \phi\} \cup T_\infty,$$

where S_∞, T_∞ are the sets defined by

$$\begin{cases} D > 0 \Rightarrow S_\infty = \phi,\ T_\infty = \{-1\}, \\ D < 0 \Rightarrow S_\infty = \{-1\},\ T_\infty = \phi. \end{cases}$$

For the set X, we denote by V_X the subgroup of $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ generated by all elements of X. In the case that $D = 775$,

$$S = \{5, 31\},$$
$$T = \{-1, 5, 31\},$$
$$V_S = \langle 5, 31 \rangle,$$
$$V_T = \langle -1, 5, 31 \rangle.$$

It is clear that $V_S \subset S^{(\varphi')}(E_D/\mathbf{Q})$ and $V_T \subset S^{(\varphi)}(E_D/\mathbf{Q})$. Using the representation of [6], we obtain the matrices

$$\Lambda' = \begin{array}{c} \\ 5 \\ 31 \end{array} \!\! \begin{array}{c} \begin{array}{cc} 5 & 31 \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \end{array},$$

$$\Lambda = \begin{array}{c} \\ -1 \\ 5 \\ 31 \end{array} \!\! \begin{array}{c} \begin{array}{ccc} 2 & 5 & 31 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \end{array},$$

where the numbers outside the matrices represent the meanings of these matrices. For example, that $(1, 1)$-entry of Λ' is 1 means $5 \notin \mathrm{Im}(\delta'_5)$, and that $(1, 2)$-entry is 0 means $5 \in \mathrm{Im}(\delta'_{31})$. Then that the entries in the second row are all 0 means $31 \in S^{(\varphi')}(E_D/\mathbf{Q})$. From the matrix Λ, it is clear that $-1, 5, 31 \notin S^{(\varphi)}(E_D/\mathbf{Q})$. And it follows that $-31 \in S^{(\varphi)}(E_D/\mathbf{Q})$ since the first row and the third row are the same. Note that $V_T/(\mathrm{Im}(\delta_p) \cap V_T)$ are groups of order 2 for $p = 2, 5, 31$, where the group V_T is regarded as the subgroup of $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$. But this order may be 4 for $p = 2$, and hence the definitions of Λ' and Λ are rather complicated (see [6] Table 4.) Consequently, $S^{(\varphi')}(E_D/\mathbf{Q}) = \langle 31 \rangle$, $S^{(\varphi)}(E_D/\mathbf{Q}) = \langle -31 \rangle$, and the Selmer rank of E_{775} is 0. In general, we have an useful formula

$$\text{(2)} \qquad \text{Selmer rank} = |S| + |T| - \operatorname{rank}\Lambda' - \operatorname{rank}\Lambda - 2.$$

Example 2. Let $D = 1975 = 5^2 \cdot 79$. Note that the *types* of 1975 and 775 are almost the same, but 79 is a quartic non-residue modulo 5. In the case that $D = 1975$, the Selmer rank is 2 by (2), and the rank is also 2.

Theorem 2 can be also proven by (2). We give only the short proof of (a).

Proof of Theorem 2 (a). In the case that r is even,

l	$\mathrm{Im}(\delta'_l)$	$\mathrm{Im}(\delta_l)$
∞	$\{1\}$	$\{\pm 1\}$
2	$\langle 2, -5 \rangle$	$\langle -2 \rangle$
p_1	$\langle 2p_1 \rangle$	$\langle 2p_1 \rangle$
$\vdots$	$\vdots$	$\vdots$
p_r	$\langle 2p_r \rangle$	$\langle 2p_r \rangle$

$$\Lambda' = \begin{array}{c} \\ 2 \\ p_1 \\ \vdots \\ p_r \end{array} \!\! \begin{array}{c} \begin{array}{cccc} 2 & p_1 & \cdots & p_r \end{array} \\ \left(\begin{array}{c|c} 0 & 1 \ \cdots \ 1 \\ \hline 1 & \\ \vdots & I_r \\ 1 & \end{array}\right) \end{array},$$

$$\Lambda = \begin{array}{c} \\ -1 \\ 2 \\ p_1 \\ \vdots \\ p_r \end{array} \!\! \begin{array}{c} \begin{array}{ccccc} 2 & 2' & p_1 & \cdots & p_r \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & & & \\ \vdots & \vdots & & I_r & \\ 1 & 0 & & & \end{pmatrix} \end{array},$$

where I_r is the identity matrix of degree r. Since $\mathrm{Im}(\delta_2) = \langle -2 \rangle$, the group $V_T/(\mathrm{Im}(\delta_2) \cap V_T)$ is Klein's four group. Therefore the definition of the matrix Λ is rather complicated. For example, that $(1, 1)$-entry of Λ is 0 means $-1 \in \{\pm 1, \pm 2\} (\subset \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2})$, and that $(1, 2)$-entry is 1 means $-1 \notin \{1, 5, -2, -10\}$. Such a definition validates the formula (2). Hence we have

$$\begin{aligned} \text{Selmer rank} &= (r + 1) + (r + 2) \\ &\quad - r - (r + 1) - 2 \\ &= 0, \end{aligned}$$

and $\operatorname{rank} E_D(\mathbf{Q}) = 0$. We can similarly prove the case that r is odd. But since $\mathrm{Im}(\delta_2) = \langle -10 \rangle$ in the case, we must reconsider the definition of the matrix Λ. □

4. Proof of Theorem 4. In this section, we give the proof of Theorem 4. From the definition of the connecting homomorphism, it follows that $\delta_k(P) = x(P)$ unless the order of P divides 2. Therefore in order to determine $\mathrm{Im}(\delta_k)$, we must check what numbers (modulo square) appear in the x-coordinates of the k-rational points on the elliptic curve E'. Similarly, we must check the x-coordinates of the k-rational points of the elliptic curve E to determine the image of the connecting homomorphism δ'_k. But, in view of Theorem 3, it is sufficient that we calculate one of the images $\mathrm{Im}(\delta'_p)$ and $\mathrm{Im}(\delta_p)$.

Proof of Theorem 4. Let p be an odd prime dividing D, and $\mathrm{ord}_p(D) = a$, $D = p^a D'$. For $(x, y) \in E(\mathbf{Q}_p)$, we let $\mathrm{ord}_p(x) = e$, $x = p^e w (w \in \mathbf{Z}_p^\times)$, then

$$\begin{aligned} y^2 &= p^{3e} w^3 + p^{e+a} D' w \\ &= p^{3e} w^3 (1 + p^{-2e+a} w^{-2} D') \qquad (3) \\ &= p^{e+a} w (p^{2e-a} w^2 + D') \qquad (4) \end{aligned}$$

from the equation of E_D. If $e \leq (a-1)/2$, then e must be even and $w \equiv 1 (\mathrm{mod}\ \mathbf{Q}_p^{\times 2})$ by (3), hence $x \equiv 1 (\mathrm{mod}\ \mathbf{Q}_p^{\times 2})$. Similarly, if $e \geq (a+1)/2$, then $x \equiv D\ (\mathrm{mod}\ \mathbf{Q}_p^{\times 2})$ by (4).

In the case that $\underline{a = 1 \text{ or } 3}$, the points with $(a-1)/2 < e < (a+1)/2$ do not exist, hence we have proved (a).

From now on, we assume that $\underline{a = 2}$, then we must investigate the set

$$H = \{(x, y) \in E_D(\mathbf{Q}_p) \mid \mathrm{ord}_p(x) = 1\}.$$

We set $a = 2, e = 1$, then

$$y^2 = p^3 w (w^2 + D') \qquad (5)$$

from (4). Therefore when $\underline{(-D'/p) = -1}$, $H = \phi$ and hence $\mathrm{Im}(\delta'_p) = \langle D \rangle$. Now we have proved (b),(ii) and (c),(i).

Next, we assume that $\underline{(-D'/p) = 1}$. Let $-D = p^2 c^2$ $(c \in \mathbf{Z}_p^\times)$, then

$$y = p^3 w (w + c)(w - c)$$

from (5). Hence w must be congruent to c or $-c$ modulo p. For example, if $w - c = p^{2n-3} z$ $(n \geq 2, z \in \mathbf{Z}_p^\times)$, then

$$y^2 = p^{2n} z (p^{2n-3} z + c)(p^{2n-3} z + 2c).$$

From this representation, $y \in \mathbf{Q}_p$ exists if and only if $z \equiv 2\ (\mathrm{mod}\ \mathbf{Q}_p^{\times 2})$. In this case, $x = pw = p(p^{2n-3} z + c) \equiv pc\ (\mathrm{mod}\ \mathbf{Q}_p^{\times 2})$. While $w + c = p^{2n-3} z$, then $x \equiv -pc\ (\mathrm{mod}\ \mathbf{Q}_p^{\times 2})$. Hence we have $\delta'_p(H) = \{\pm pc\}$ and $\mathrm{Im}(\delta'_p) = \{1, D, pc, -pc\}$. Therefore $\mathrm{Im}(\delta'_p) = \mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$ in the case that $\underline{p \equiv 3 \pmod 4}$. We have proved (c), (ii). When $\underline{p \equiv 1 \pmod 4}$, it follows that $\mathrm{Im}(\delta'_p) = \{1, pc\} = \langle p \rangle$ or $\langle pu \rangle$ according as c is a quadratic residue modulo p or not, i.e. $-D'$ is a quartic residue modulo p or not. We have proved (b),(i) and the proof is complete. □

Theorem 5 can be similarly proved. When D is even, it is easier to study $\mathrm{Im}(\delta_2)$ than $\mathrm{Im}(\delta'_2)$ because the structure of $E_{-4D}(\mathbf{Q}_2)$ is simpler than that of $E_D(\mathbf{Q}_2)$.

References

[1] Aoki, N.: On the 2-Selmer groups of elliptic curves arising from the congruent number problem. Comment. Math. Univ. St. Paul., **48**, 77–101 (1999).

[2] Aoki, N.: Selmer groups and ideal class groups. Comment. Math. Univ. St. Paul., **42**, 209–229 (1993).

[3] Birch, B. J., and Stephens, N. M.: The parity of the rank of the Mordell-Weil group. Topology, **5**, 295–299 (1966).

[4] Bremner, A., and Cassels, J. W. S.: On the equation $Y^2 = X(X^2 + p)$. Math. Comp., **42**, 257–264 (1984).

[5] Iskra, B.: Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8. Proc. Japan Acad., **72A**, 168–169 (1996).

[6] Goto, T.: Calculation of Selmer groups of elliptic curves with rational 2-torsions and θ-congruent number problem. Comment. Math. Univ. St. Paul (to appear).

[7] Heath-Brown, D. R.: The size of Selmer groups for the congruent number problem. II. Invent. Math., **118**, 331–370 (1994).

[8] Silverman, J. H.: The Arithmetic of Elliptic Curves. Graduate Texts in Math., vol. 106, Springer, New York (1986).

[9] Yoshida, S.: On the equation $y^2 = x^3 + pqx$. Comment. Math. Univ. St. Paul., **49**, 23–42 (2000).