COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 49, No. 1 2000

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

On the Equation $y^2 = x^3 + pqx$

by

Shin-ichi YOSHIDA

(Received June 21, 1999)
(Revised January 13, 2000)

1. Introduction

Let E be an elliptic curve defined over a number field K, and let $E(K)$ be its Mordell-Weil group, which is a finitely generated abelian group. In this paper, we study the elliptic curve defined over $\boldsymbol{Q}$ of the form

$$E_{pq} : y^2 = x^3 + pqx\,,$$

where p and q are distinct odd primes. Especially we are concerned with determining the rank and the structure of the Mordell-Weil group $E_{pq}(\boldsymbol{Q})$.

It is very difficult to determine the Mordell-Weil rank for a general elliptic curves and, there is no established algorithm to find it. As for the above type curves there is an approach given in the book of Silverman [Sil].

Set

$$E_D : y^2 = x^3 + Dx\,,$$

where D is a fourth power free integer. Then it holds

$$\operatorname{rank}(E_D(\boldsymbol{Q})) \leq 2\#\{l \text{ prime}; l \text{ divides } 2D\} - 1\,.$$

If D is an odd prime p, the rank of $E_p(\boldsymbol{Q})$ is much more restricted:

$$\operatorname{rank}(E_p(\boldsymbol{Q})) + \dim_2 Ш(E_p/\boldsymbol{Q})[2] = \begin{cases} 0 & \text{if } p \equiv 7,\ 11 \pmod{16} \\ 1 & \text{if } p \equiv 3, 5, 13, 15 \pmod{16} \\ 2 & \text{if } p \equiv 1 \pmod{8}\,. \end{cases}$$

Here we use the following notation:

– $Ш(E_p/\boldsymbol{Q})$ is the Shafarevich-Tate group of $E_p/\boldsymbol{Q}$,

– $M[\mu]$ is defined to be the kernel of μ for a group homomorphism $\mu : M \to M'$,

– $\dim_2 V$ is the dimension of an $\boldsymbol{F}_2$-vector space V.

In case D is a composite of two different odd primes p and q, the general information tells only

$$\operatorname{rank}(E_{pq}(\boldsymbol{Q})) \leq 5\,.$$

1991 *Mathematics Subject Classification.* Primary 11G05.

But if we put some additional conditions, we can determine the rank$(E_{pq}(\boldsymbol{Q}))$ as the following.

THEOREM 1. *If the Legendre symbol* $(q/p) = -1$ *and* $q - p \equiv \pm 6 \pmod{16}$, *then*

$$E_{pq}(\boldsymbol{Q}) = \{O, (0,0)\} \cong \boldsymbol{Z}/2\boldsymbol{Z}, \quad \textit{and} \quad Ш(E_{pq}/\boldsymbol{Q})[2] = 0.$$

If p and q are twin prime numbers, then $E_{pq}(\boldsymbol{Q})$ has a non-torsion point $(1, (p+q)/2)$. Moreover we have

THEOREM 2. *Let p and q be twin prime numbers with* $(q/p) = -1$. *Then we have the following.*

(a) $E_{pq}(\boldsymbol{Q}) \cong \boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$, *and* $Ш(E_{pq}/\boldsymbol{Q})[2] = 0$.

(b) *A generator of the free part of* $E_{pq}(\boldsymbol{Q})$ *is* $(1, (p+q)/2)$.

(c) *All integral points on* E_{pq} *are*

$$\left(1, \pm\frac{p+q}{2}\right), \quad \left(pq, \pm\frac{pq(p+q)}{2}\right), \quad \textit{and} \quad (0,0).$$

REMARK. We will discuss the case that p and q are twin prime numbers with $(q/p) = 1$ in Section 6. For example, we have the following.

THEOREM 3. *For* $(p,q) = (311, 313)$, *or* $(521, 523)$, *we have the same result as Theorem* 2 *except that*

$$Ш(E_{pq}/\boldsymbol{Q})[2] \cong \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z},$$

and we obtain $Ш(E_{pq}/\boldsymbol{Q})$ *is finite. Further, if the (full version of) Birch and Swinnerton-Dyer conjecture (see Section* 6) *is true, then* $Ш(E_{pq}/\boldsymbol{Q}) \cong \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$.

To proceed our study, we use the two-descent method, which we recall in the next section.

2. Two-descent method

In this section, we prepare fundamental concepts and tools according to [Sil]. Let E and E' be elliptic curves defined over a number field K. Let $\phi : E \to E'$ be an isogeny defined over K, and $E[\phi]$ its kernel. If L is a field containing K, the exact sequence of $G_L(= Gal(\bar{L}/L))$-modules

$$0 \to E(\bar{L}[\phi] \to E(\bar{L}) \xrightarrow{\phi} E'(\bar{L}) \to 0$$

gives rise to the short exact sequence in cohomology:

$$0 \to E'(L)/\phi(E(L)) \xrightarrow{\delta} H^1(G_L, E(\bar{L})[\phi]) \to WC(E/L)[\phi] \to 0.$$

Here we use the fact that $H^1(G_L, E(\bar{L}))$ is isomorphic to the Weil-Châtelet group $WC(E/L)$, which consists of certain equivalence classes of (smooth) curves C/K together with a simply transitive algebraic action of E on C defined over K. (See [Sil, Chap. X, 3.6].) We shall apply this situation to $L = K$ or $L = K_v$ (the completion of K at a (finite

or infinite) place v of K). If we fix an embedding $\bar{K} \subset \bar{K}_v$, then the inclusions $G_{K_v} \subset G_K$ and $E(\bar{K}) \subset E(\bar{K}_v)$ give the following commutative diagram.

$$\begin{array}{ccccccccc} 0 \to & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(G_K, E(\bar{K})[\phi]) & \to & WC(E/K)[\phi] & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & \prod_v E'(K_v)/\phi(E(K_v)) & \xrightarrow{\prod_v \delta_v} & \prod_v H^1(G_{K_v}, E(\bar{K}_v)[\phi]) & \to & \prod_v WC(E/K_v)[\phi] & \to 0\,. \end{array}$$

We define the ϕ-Selmer group $S^{(\phi)}(E/K)$ to be the kernel of the homomorphism $H^1(G_K, E(\bar{K})[\phi]) \to \prod_v WC(E/K_v)$, and the Shafarevich-Tate group $Ш(E/K)$ to be the kernel of the homomorphism $WC(E/K) \to \prod_v WC(E/K_v)$. By definition, the sequences

$$0 \to E'(K)/\phi(E(K)) \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0\,, \tag{1}$$

$$0 \to E(K)/\hat{\phi}(E'(K)) \to S^{(\hat{\phi})}(E'/K) \to Ш(E'/K)[\hat{\phi}] \to 0 \tag{2}$$

are exact, and $S^{(\hat{\phi})}(E'/K)$ are finite ([Sil, Chap. X, 4.2]), where $\hat{\phi}$ is the dual isogeny of ϕ. If $\deg \phi = m$, we also use the following exact sequences:

$$0 \to \frac{E'(K)[\hat{\phi}]}{\phi(E(K)[m])} \to \frac{E'(K)}{\phi(E(K))} \xrightarrow{\hat{\phi}} \frac{E(K)}{m(E(K))} \to \frac{E(K)}{\hat{\phi}(E'(K))} \to 0\,, \tag{3}$$

$$0 \to Ш(E/K)[\phi] \to Ш(E/K)[m] \to Ш(E'/K)[\hat{\phi}]\,. \tag{4}$$

Take the elliptic curves E and E' as

$$\begin{aligned} E = E[a,b]: &\quad y^2 = x^3 + ax^2 + bx \\ E' = E'[a,b]: &\quad Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X\,, \end{aligned} \tag{5}$$

where $a, b \in R_K$ (= the ring of integers of K) with $b(a^2 - 4b) \neq 0$, and take the isogeny ϕ as

$$\phi : E \to E' \quad (x, y) \mapsto (y^2/x^2, y(b - x^2)/x^2) \tag{6}$$

with the kernel $E(\bar{K})[\phi] = \{O, (0,0)\}$. ($O = O_E$ denotes the identity element of E.) As G_K-modules, we have $E(\bar{K})[\phi] \cong \mu_2 (= \{\pm 1\} \subset K^*)$ since $E(\bar{K})[\phi] \subset E(K)$, so we get the isomorphism

$$H^1(G_K, E(\bar{K})[\phi]) \cong H^1(G_K, \mu_2) \cong K^*/K^{*2}$$

by Hilbert's theorem 90. Using this isomorphism, we have the following (cf. [Sil, Chap. X, 4.9]):

THEOREM 4 (Descent via Two-Isogeny). *Let E/K, E'/K and ϕ be the elliptic curves and the two-isogeny defined as above* (5) *and* (6), *and let*

$$S = \{\text{all infinite places of } K\} \cup \{\text{all finite places of } K \text{ dividing } 2b(a^2 - 4b)\}$$

$$K(S,2) = \{d \in K^*/K^{*2};\ \mathrm{ord}_v(d) \equiv 0 \pmod 2 \text{ for all } v \notin S\}\,.$$

(*Here* ord_v *means the normalized valuation for a finite place* v.) *Then, there is an exact sequence*

$$\begin{array}{rcccl} 0 \to E'(K)/\phi(E(K)) & \xrightarrow{\delta} & K(S,2) & \to & WC(E/K)[\phi] \\ O_{E'} & \longmapsto & 1 & & \\ (0,0) & \longmapsto & a^2-4b & & \\ P=(X,Y) & \longmapsto & X(P\neq O,(0,0)) & & \\ & & d & \mapsto & \{C_d/K\}, \end{array}$$

where C_d/K *is the curve given by the equation*

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2-4b)z^4 .$$

The ϕ*-Selmer group is then*

$$S^{(\phi)}(E/K) \cong \{d \in K^*/K^{*2};\ C_d(K_v) \neq \emptyset \text{ for all } v \in S\} .$$

The map

$$\begin{aligned} \psi : C_d &\to E' \\ (z,w) &\mapsto (d/z^2, -dw/z^3) \end{aligned}$$

has the property that if $P \in C_d(K)$, *then*

$$\delta(\psi(P)) = d \text{ in } K^*/K^{*2} .$$

In this paper, we treat the case $a = 0$, $b = pq$ (and $K = \boldsymbol{Q}$), where p, q are distinct odd primes. We denote $E[0, D]$ (resp. $E'[0, D]$) by E_D (resp. E'_D), for short.

To compute the Selmer groups, we often use Hensel's lemma (cf. [Sil, Chap. X, exer. 10.12]):

LEMMA 1. *Let* R *be a complete ring for a discrete valuation* v, $F(X_1, \cdots, X_N) \in R[X_1, \cdots, X_N]$, $(a_1, \cdots, a_N) \in R^N$, *and suppose*

$$v(F(a_1, \cdots, a_N)) > 2v\left(\frac{\partial F}{\partial X_i}(a_1, \cdots, a_N)\right)$$

for some $1 \leq i \leq N$. *Then* $F(X_1, \cdots, X_N) = 0$ *has a root in* R^N.

3. Computation of $S^{(\phi)}(E_{pq}/\boldsymbol{Q})$, $S^{(\hat{\phi})}(E'_{pq}/\boldsymbol{Q})$

Let $E = E_{pq}$ and $E' = E'_{pq}$. In this section, we compute the Selmer groups $S^{(\phi)}(E/\boldsymbol{Q})$ and $S^{(\hat{\phi})}(E'/\boldsymbol{Q})$, where ϕ is the isogeny given by

$$\phi : E \to E' \quad (x, y) \mapsto (y^2/x^2, y(pq - x^2)/x^2) ,$$

and $\hat{\phi}$ is its dual isogeny. In this case, by Theorem 3, we have the following natural identifications:

$$S^{(\phi)}(E/\boldsymbol{Q}) = \{d \in \boldsymbol{Q}(S,2);\ C_d(\boldsymbol{Q}_l) \neq \emptyset\ (\forall l \in S)\},$$

$$S^{(\hat{\phi})}(E'/\boldsymbol{Q}) = \{d \in \boldsymbol{Q}(S,2);\ C'_d(\boldsymbol{Q}_l) \neq \emptyset\ (\forall l \in S)\}.$$

Where

$$S = \{\infty, 2, p, q\}$$

$$\boldsymbol{Q}(S,2) = \{\pm 1, \pm 2, \pm p, \pm q, \pm 2p, \pm 2q, \pm pq, \pm 2pq\} \subset \boldsymbol{Q}^*/\boldsymbol{Q}^{*2}$$

$$C_d:\quad dw^2 = d^2 - 4pqz^4$$

$$C'_d:\quad dW^2 = d^2 + pqZ^4,$$

and we put $\boldsymbol{Q}_\infty = \boldsymbol{R}$.

PROPOSITION 1. *The notation is as above. Then, we have the following*:

(1.1) $1, -pq \in S^{(\phi)}(E/\boldsymbol{Q})$.

(1.2) *The following equivalences hold.*

(a) $-1 \in S^{(\phi)}(E/\boldsymbol{Q})$ *if and only if* $p \equiv q \equiv 1 \pmod 4$.

(b) $p \in S^{(\phi)}(E/\boldsymbol{Q})$ *if and only if* $(p/q) = (-q/p) = 1$.

(c) $2 \in S^{(\phi)}(E/\boldsymbol{Q})$ *if and only if* $(2/p) = (2/q) = 1$, *and* $pq \equiv 1, 9, 15 \pmod{16}$.

(d) $-2 \in S^{(\phi)}(E/\boldsymbol{Q})$ *if and only if* $(-2/p) = (-2/q) = 1$, *and* $pq \equiv 1, 3, 9 \pmod{16}$.

(e) $2p \in S^{(\phi)}(E/\boldsymbol{Q})$ *if and only if* $(2p/q) = (-2q/p) = 1$, *and* $p - q \equiv 0, 2, 8 \pmod{16}$.

(2.1) $\{1, pq\} \subset S^{(\hat{\phi})}(E'/\boldsymbol{Q}) \subset \{1, p, q, pq\}$.

(2.2) $p \in S^{(\hat{\phi})}(E'/\boldsymbol{Q})$ *if and only if* $(p/q) = 1$, *and one of the following conditions holds.*

· p *or* q *is congruent to* $1 \pmod 8$, *or*

· $p + q$ *is congurent to* 0 *or* $4 \pmod{16}$.

Where $(*/*)$ *is the Legendre symbol.*

Note. Since the condition on p and q is symmetric, the groups $S^{(\phi)}(E/\boldsymbol{Q})$ and $S^{(\hat{\phi})}(E'/\boldsymbol{Q})$ can be determined completely from Proposition 1.

Proof. The method is the same as that in [Sil, Chap. X, 6.2], so we compute some parts in the proposition.

By Theorem 4, (1, 1) is quite trivial. Let $d \in \boldsymbol{Q}(S,2)$. It is easy to see that $C_d(\boldsymbol{R}) \neq \emptyset$. Hence, d is in $S^{(\phi)}(E/\boldsymbol{Q})$ if and only if $C_d(\boldsymbol{Q}_p)$, $C_d(\boldsymbol{Q}_q)$ and $C_d(\boldsymbol{Q}_2)$ are not empty.

$$d = -1 \quad C_{-1} : -w^2 = 1 - 4pqz^4.$$

If $(z_0, w_0) \in C_{-1}(\boldsymbol{Q}_p)$, then it is easy to see that $\mathrm{ord}_p z_0, \mathrm{ord}_p w_0 \geq 0$ and so $w_0^2 \equiv -1 \pmod p$. Conversely, by Hensel's lemma, any solution to $w^2 \equiv -1 \pmod p$ lifts to a point in $C_{-1}(\boldsymbol{Q}_p)$. Therefore

$$C_{-1}(\boldsymbol{Q}_p) \neq \emptyset \Leftrightarrow p \equiv 1 \pmod 4.$$

Similarly,

$$C_{-1}(\boldsymbol{Q}_q) \neq \emptyset \Leftrightarrow q \equiv 1 \pmod 4 .$$

From above, to see whether -1 is in $S^{(\phi)}(E/\boldsymbol{Q})$ or not, we may assume that $p \equiv q \equiv 1 \pmod 4$. If $(z_0, w_0) \in C_{-1}(\boldsymbol{Q}_2)$, then we must have $\mathrm{ord}_2 w_0 < 0$, and $s = -\mathrm{ord}_2 z_0 > 0$ (so $\mathrm{ord}_2 w_0 = 1 - 2s$). If we write

$$z_0 = 2^{-s} z_1,\ w_0 = 2^{1-2s} w_1 \quad (z_1, w_1 \in \boldsymbol{Q}_2,\ \mathrm{ord}_2 z_2 = \mathrm{ord}_2 w_1 = 0) ,$$

then we have

$$-{w_1}^2 = 2^{4s-2} - pq{z_1}^4 .$$

Hence, the condition that $C_{-1}(\boldsymbol{Q}_2) \neq \emptyset$ is equivalent to the condition that there exists $s \in \boldsymbol{Z}$, $s > 0$ such that

$$-1 \equiv 2^{4s-2} - pq \pmod 8 ,$$

by Hensel's lemma. (Note that z_1, w_1 are 2-adic units.) If $pq \equiv 1$ (resp. $pq \equiv 5$) $(\mathrm{mod}\, 8)$, the last congruence has a solution $s = 2$ (resp. $s = 1$). Hence we have (1.2a)

$$d = p \quad C_p : w^2 = p - 4qz^4 .$$

If $(z_0, w_0) \in C_p(\boldsymbol{Q}_q)$, then $\mathrm{ord}_q z_0$, $\mathrm{ord}_q w_0 \geq 0$ and $w_0^2 \equiv p \pmod q$. Conversely, a solution to $w^2 \equiv p \pmod q$ lifts to a point of $C_p(\boldsymbol{Q}_q)$. Therefore

$$C_p(\boldsymbol{Q}_q) \neq \emptyset \Leftrightarrow \left(\frac{p}{q}\right) = 1 .$$

Similarly,

$$C_p(\boldsymbol{Q}_p) \neq \emptyset \Leftrightarrow \left(\frac{-q}{p}\right) = 1 .$$

We must determine whether $C_p(\boldsymbol{Q}_2)$ is empty or not, under the assumption that $(p/q) = (-q/p) = 1$ (so we have $p \equiv 1 \pmod 4$) or $p \equiv q \equiv 3 \pmod 4$. Let $(z_0, w_0) \in C_p(\boldsymbol{Q}_2)$. Then there are three cases which we must consider:

(i) $\mathrm{ord}_2 w_0 > 0,\ \mathrm{ord}_2 z_0 \geq 0$
(ii) $\mathrm{ord}_2 w_0 = 0,\ s = \mathrm{ord}_2 z_0 \geq 0$
(iii) $\mathrm{ord}_2 w_0 < 0,\ -s = \mathrm{ord}_2 z_0 < 0,\ \mathrm{ord}_2 w_0 = 1 - 2s$

It is easy to see that the case (i) cannot occur.

Case (ii): Put $z_0 = 2^s$, with a non-negative integer s. Then we have

$$w_0^2 = p - 2^{4s+2} q z_1^4 ,$$

where z_1 is a 2-adic unit or 0, and w_0 is a 2-adic unit. If $p \equiv 1 \pmod 4$, the following table gives solutions (z_1, w_0, s) of the congruence

$$w_0^2 \equiv p - 2^{4s+2} q z_1^4 \pmod 8 ,$$

and the solutions lift points in $C_p(\boldsymbol{Q}_2)$ by Hensel's lemma.

$p \equiv 1 \pmod 8$	$(1, 1, 1)$
5	$(1, 1, 0)$

Hence, we see that $C_p(\boldsymbol{Q}_2) \neq \emptyset$ if $p \equiv 1 \pmod 4$.

Case (iii): If we set $z_0 = 2^{-s} z_1$, $w_0 = 2^{1-2s} w_1$ ($z_1, w_1 \in \boldsymbol{Q}_2$ $\mathrm{ord}_2 z_1 = \mathrm{ord}_2 w_1 = 0$; $s \in \boldsymbol{Z}$, $s > 0$), then we get

$$w_1{}^2 = 2^{4s-2} p - q z_1{}^4 .$$

If $p \equiv q \equiv 3 \pmod 4$, the following table gives solutions (z_1, w_1, s) of the congruence

$$b^2 \equiv 2^{4s-2} p - q a^4 \pmod 8 ,$$

and the solutions lift points in $C_p(\boldsymbol{Q}_2)$.

$p \equiv 3 \pmod 8$	$(1, 1, 1)$
7	$(1, 1, 2)$

So, we obtain that $C_p(\boldsymbol{Q}_2) \neq \emptyset$ if $p \equiv q \equiv 3 \pmod 4$. After all, we have

$$\left(\frac{p}{q}\right) = 1 \left(\frac{-q}{p}\right) = 1 \Rightarrow C_p(\boldsymbol{Q}_2) \neq \emptyset$$

and

$$p \in S^{(\phi)}(E/\boldsymbol{Q}) \Leftrightarrow \left(\frac{p}{q}\right) = \left(\frac{-q}{p}\right) = 1 .$$

This proves (1.2b). Similar calculations for other $d \in \boldsymbol{Q}(S, 2)$ give the desired result. □

Theorem 1 follows easily from Proposition 1 and exact sequences (1) through (4).

4. The proof of Theorem 2(a), (b)

PROOF (of Theorem 2(a), (b)). (a) Let $E = E_{pq}$ and $E' = E'_{pq}$. Without loss of generality, we may assume $q = p + 2$. Then we have $(2/p) = (q/p) = -1$, so we have

$$S^{(\phi)}(E/\boldsymbol{Q}) = \{1, -pq, -2p, 2q\} \cong \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}, \quad \text{and}$$
$$S^{(\hat{\phi})}(E'/\boldsymbol{Q}) = \{1, pq\} \cong \boldsymbol{Z}/2\boldsymbol{Z} .$$

By Proposition 1. Hence we obtain inequalities

$$\dim_2 E'(\boldsymbol{Q})/\phi(E(\boldsymbol{Q})) \leq 2 , \quad \dim_2 E(\boldsymbol{Q})/\hat{\phi}(E'(\boldsymbol{Q})) \leq 1 . \tag{7}$$

from the exact sequences (1) and (2).

Let r be the rank of $E(\boldsymbol{Q})$. Since the torsion subgroup of $E(\boldsymbol{Q})$ is $\{O, (0, 0)\} (\cong \boldsymbol{Z}/2\boldsymbol{Z})$ by [Sil, Chap. X, 6.1], we have

$$\dim_2 E'(\boldsymbol{Q})[\hat{\phi}]/\phi(E(\boldsymbol{Q})[2]) = 1 , \quad \dim_2 E(\boldsymbol{Q})/2(E(\boldsymbol{Q})) = r + 1 . \tag{8}$$

Using (7), (8) and (3), we have $r \leq 1$. In fact, we obtain $r = 1$ since $E(\boldsymbol{Q})$ contains a non-torsion point $P_0 = (1, (p+q)/2)$. Then $Ш(E/\boldsymbol{Q})[2] = 0$ can be proved easily by (1), (2) and (4). So we obtain (a).

(b) Let P be a generator of free part of $E(\boldsymbol{Q})$ and put $P' = P + (0, 0)$. From (a), the integral point P_0 is a multiple of P or P', thus P or P' is also an integral point by [Sil,

Chap. IX, exer. 9.12]. We may suppose that P_0 is a multiple of P. By (2) and the injection (in fact, isomorphism)

$$\begin{aligned} \delta : E(\boldsymbol{Q})/\hat{\phi}(E'(\boldsymbol{Q})) &\to S^{(\hat{\phi})}(E'/\boldsymbol{Q}) = \{1, pq\} \subset \boldsymbol{Q}^*/\boldsymbol{Q}^{*2} \\ O &\mapsto 1 \\ (0,0) &\mapsto pq \\ Q = (x, y) &\mapsto x(Q \neq O, (0,0)), \end{aligned} \tag{9}$$

any integral point has the form (u^2, v) or (pqu^2, v) $(u, v \in \boldsymbol{Z})$. We need the following claim.

CLAIM. If $Q = (u^2, v) \in E(\boldsymbol{Q})$ $(u, v \in \boldsymbol{Z}, u \neq 0)$, then $u = \pm 1$, hence $Q = \pm P_0$.

Proof (of the claim). Since $Q \in E(\boldsymbol{Q})$, we have $v^2 = u^2(u^4 + pq)$. Then, $u^4 + pq$ becomes a square, we can write $t^2 = u^4 + pq$ with a positive integer t, and we get $(t - u^2)(t + u^2) = pq$. Since p, q $(p < q)$ are primes, we obtain

$$\begin{aligned} &\text{(i)} \quad t - u^2 = 1 \text{ and } t + u^2 = pq\,, \text{ or} \\ &\text{(ii)} \quad t - u^2 = p \text{ and } t + u^2 = q\,. \end{aligned}$$

In the case (i), we have $2u^2 = pq - 1$ and $(2u)^2 = 2pq - 2 \equiv -2 \pmod{p}$, hence $(-2/p) = 1$. On the other hand, we also have $(2/p) = -1$ by assumption, we must obtain $p \equiv 3 \pmod 8$. Using $2u^2 = pq - 1$ again, we have $2u^2 \equiv 3 \cdot (3+2) - 1 \equiv 6 \pmod 8$. It is easy to see that it is impossible. In the case (ii), we get $2u^2 = q - p = 2$, $2t = p + q$, thus $u = \pm 1$.

We return to the proof of Theorem 2. If P is of the form (u^2, v), then we have nothing to prove from above claim. It suffices to show that P can not be of the form (pqu^2, v). If P is of the form (pqu^2, v) and if we can write $P_0 = mP$ with $m \in \boldsymbol{Z}$ (We may assume m is positive.), then m must be even. Otherwise, we write $m = 2k + 1$ $(k \in \boldsymbol{Z})$, and get $(1, (p+q)/2) = P_0 = 2kP + P = \hat{\phi}(\phi(kP)) + (pqu^2, v)$, hence we would have $1 = pq$ in $\boldsymbol{Q}^*/\boldsymbol{Q}^{*2}$ by using the homomorphism δ in (9), which leads a contradiction. Since m is even, $mP' = mP = P_0$, thus P' is an integral point. On the other hand, since $P' = P + (0,0) = (1/u^2, *)$, we get $u^2 = 1$ from above claim, and $P' = \pm P_0$, which is impossible because m is even. □

REMARK. When p, q are twin prime numbers with $(q/p) = 1$, similar argument of above proof gives $1 \leq r \leq 3$, where $r =$ the rank of $E_{pq}(\boldsymbol{Q})$. In this case, the sign of the functional equation of the L-series $L(E_{pq}, s)$ is -1 by Proposition 1 and the result of Birch and Stephens [BS], so we can expect r is odd. Both the cases $r = 1$ and $r = 3$ can occur (see Section 6 and 7).

REMARK. Using an argument similar to the above proof, we can generalize Theorem 2:

THEOREM 5. *Let p and q be distinct odd prime numbers with the properties that*

(i) $(q/p) = -1$,
(ii) $|(q-p)/2| \equiv 1 \pmod 8$, *and*
(iii) $2|q-p|$ *is a square*.

(*For example*, $(p, q) = (11, 29), (23, 601), (419, 997)$, *etc.*) *Then we have*

$$E_{pq}(\boldsymbol{Q}) \cong \mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$$

with generators $P_0 = (|q-p|/2, \sqrt{2|q-p|}(p+q)/4)$ *and* $(0, 0)$.

Further, integral points are $\pm P_0$ *and* $(0, 0)$ *only.*

REMARK. Suppose that we knew, a priori, that the group $Ш(E_{pq}/\boldsymbol{Q})$ were finite, or more generally, that its 2-primary component were finite. Then the existence of the Cassels-Tate pairing ([Ca], [Ta]) would imply that $\dim_2 Ш(E_{pq}/\boldsymbol{Q})[2]$ is even. Hence, it is easy to prove that if p, q are distinct prime numbers with $(q/p) = -1$ and $q - p \equiv \pm 2 \pmod{16}$, then the rank of $E_{pq}(\boldsymbol{Q})$ is 1 if the 2-primary component of $Ш(E_{pq}/\boldsymbol{Q})$ is finite.

5. Integral points

Let p and $q = p + 2$ be twin prime numbers with $(q/p) = -1$. In this section, we prove Theorem 2(c):

All integral points on the curve

$$E : y^2 = x^3 + pqx$$

are $(1, \pm(p+q)/2)$, $(pq, \pm pq(p+q)/2)$ and $(0, 0)$.

By the argument of the proof of Theorem 2(a) (b), it suffices to consider integral points (x, y) of the form $x = pqU^2$ and $y = \pm pqUT$, where U and T are positive integers. So we must solve the equation

$$(T-1)(T+1) = pqU^4 \quad (U, T \in \mathbf{Z};\ U, T > 0). \tag{10}$$

Let $(U, T) = (v, t)$ be a solution, we want to show that $u = 1$. There are several cases which we must consider:

Case 1, t is even.

$$\begin{aligned}
&(1.1) \quad t-1 = u_1^4, && t+1 = pqu_2^4;\\
&(1.2) \quad t-1 = pu_1^4, && t+1 = qu_2^4;\\
&(1.3) \quad t-1 = qu_1^4, && t+1 = pu_2^4;\\
&(1.4) \quad t-1 = pqu_1^4, && t+1 = u_2^4,
\end{aligned}$$

where, in each case, u_1 and u_2 are relatively prime positive odd integers.

Case 2, t is odd.

$$\begin{aligned}
&(2.1)\quad t \mp 1 = 2u_3^4, \qquad t \pm 1 = 8pqu_4^4;\\
&(2.2)\quad t \mp 1 = 2pu_3^4, \qquad t \pm 1 = 8qu_4^4;\\
&(2.3)\quad t \mp 1 = 2qu_3^4, \qquad t \pm 1 = 8pu_4^4;\\
&(2.4)\quad t \mp 1 = 2pqu_3^4, \qquad t \pm 1 = 8u_4^4,
\end{aligned}$$

where, u_3 and u_4 are relatively prime positive integers with u_3 odd, and u_4 even.

LEMMA 2. *The cases* (1.1), (1.3), (1.4), (2.2), *and* (2.3) *cannot occur.*

Proof. If the case (1.1) can occur, then we have $pqu_2^4 - u_1^4 = 2$, and hence $(-2/q) = 1$. However, since p or $q = p + 2$ is $\equiv 1 \pmod 4$, we have

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{q-2}{q}\right) = \left(\frac{-2}{q}\right) = 1.$$

It contradicts the assumption on p and q. Impossibility of (1.4) is quite similar.

If the case (1.3) occur, then we have $pu_2^4 - qu_1^4 = 2$. Since u_1 and u_2 are odd, we must obtain $p - q \equiv 2 \pmod 8$. This is impossible because $q - p = 2$.

If the case (2.2) occur, we have $4qu_4^4 - pu_3^4 = \pm 1$ and so we obtain $(\pm q/p) = (\mp p/q) = 1$. But, since $(q/p) = (p/q) = -1$, we must have $(\pm 1/p) = (\mp 1/q) = -1$. It is clearly impossible. Similarly, (2.3) does not occur. □

For the case (1.2), we have $qu_2^4 - pu_1^4 = 2$, which has a solution $u_1 = u_2 = 1$ that gives the desired point $(u, t) = (1, (p+q)/2)$. The following proposition is a special case of the result of Siegel [Sie]:

PROPOSITION 2. *Let p and $q = p + 2$ be as above, and suppose that*

$$pq \geq (188 \cdot 4 \cdot 2^4)^2 \quad (= 144769024).$$

Then the equation

$$qU_2^4 - pU_1^4 = 2 \quad (U_1, U_2 \in \mathbf{Z}, > 0)$$

has the only solution $(U_1, U_2) = (1, 1)$.

This proposition is also used to prove the next two lemmas.

LEMMA 3. *Under the assumption in Proposition* 2, *the case* (2.4) *does not occur.*

Proof. If the case (2.4) occur, then we must obtain $4u_4^4 - pqu_3^4 = 1$ since u_3 is odd and $pq \equiv 3 \pmod 4$. This means that $(U, T) = (u_3, 2u_4^2)$ is a solution of the equation (10) with even T. By Lemma 2 and Proposition 2, we have $2u_4^2 = (p + q)/2$. Hence we have $(p/q) = 1$, which gives a contradiction. □

LEMMA 4. *Under the assumption in Proposition* 2, *the case* (2.1) *does not occur.*

Proof. If (2.1) is satisfied, we obtain $4pqu_4^4 - u_3^4 = \pm 1$. By the consideration in modulo 8, we must have

$$4pqu_4^4 - u_3^4 = -1$$

and $t + 1 = 2u_3^4$, $t - 1 = 8pqu_4^4$, and u_4 is even. Because u_3 is odd, we easily obtain

$$u_3^2 + 1 = 2\alpha u_5^4 \quad \text{and} \quad u_3^2 - 1 = 2\beta u_6^4,$$

for some positive integers α, β, u_5, u_6 such that $\alpha\beta = pq$, $u_4 = u_5u_6$, and such that u_5 is odd and u_6 is even with $(u_5, u_6) = 1$. Eliminating u_3^2, we have

$$\alpha u_5^4 - \beta u_6^4 = 1\,.$$

Since u_5 is odd and u_6 is even, $\alpha \equiv 1 \pmod 8$. So we have $\alpha = 1$ because $p, q = p + 2$, and pq is not congruent to 1 modulo 8 by the assumption that $(q/p) = (2/p) = -1$. Hence we get

$$(u_5^4 - 1)(u_5^4 + 1) = pqu_6^4, \tag{11}$$

which means $(U, T) = (u_6, u_5^2)$ is a solution of the equation (10) with odd T. From (11), we see that $u_5 < u_6$, so we have

$$u_5^2 < u_5u_6 = u_4 < 8pqu_4^4 = t - 1\,,$$

and $u_5^2 < t$. Lemma 2, Lemma 3, and the infinite descent argument gives the desired result. □

Proof of Theorem 2(c). If $pq > 144769024$, Theorem 2(c) is true by the above argument. On the other hand, if $pq \leq 144769024$, we can use the algorithm of Gebel, Pethö and Zimmer [GPZ] or Smart [Sm].

By the proof of Theorem 2(b), it suffices to show that if integral points $Q \in E$ of the form

$$Q = M\left(1, \frac{p+q}{2}\right) + (0, 0)\,,$$

where M is an integer, then $M = \pm 1$. (We may assume M is positive.) The algorithm of Gebel, Pethö and Zimmer [GPZ] gives an upper bound on M. In our case, we can check that M is at most 5 for each p, $q = p + 2$ with $(q/p) = -1$ and $pq \leq 144769024$, and then, by direct computation, we have the desired result $M = 1$. □

6. Special values of L-series and the conjecture of Birch and Swinnerton-Dyer

In this section, we give some examples such that the group $E_{pq}(\boldsymbol{Q})$ has rank one and the group $Ш(E_{pq}/\boldsymbol{Q})$ is non-trivial for twin prime numbers p, q with the Legendre symbol $(q/p) = 1$. First, we recall the definition and facts about L-series $L(E, s)$ for an elliptic curve E over $\boldsymbol{Q}$ briefly. For more details, see [Sil].

Let $E/\boldsymbol{Q}$ be an elliptic curve. We set

– R_E: the elliptic regulator of $E(\boldsymbol{Q})/E_{\text{tors}}(\boldsymbol{Q})$ computed using the canonical height pairing.

– N_E: the conductor of $E/\boldsymbol{Q}$.

– Ω_E: the real period of E.

For each rational prime l, let c_l denote the number of connected components, rational over $\boldsymbol{F}_l$, of the closed fiber of the Néron model of E at l, and put

$$L_l(E,s) = \begin{cases} 1 - a_l l^{-s} + l^{1-2s} & \text{if } E \text{ has good reduction at } l\,, \\ 1 - l^{-s} & \text{if } E \text{ has split multiplicative reduction at } l\,, \\ 1 + l^{-s} & \text{if } E \text{ has non-split multiplicative reduction at } l\,, \\ 1 & \text{if } E \text{ has additive reduction at } l\,, \end{cases}$$

where

$$a_l = 1 + l - \#\tilde{E}(\boldsymbol{F}_l)\,.$$

The L-function is defined by the Euler product

$$L(E,s) = \prod_l L_l(E,s)^{-1}\,,$$

which is convergent and gives an analytic function for $\Re e(s) > 3/2$ by the Hasse-Weil bound $|a_l| \leq 2\sqrt{l}$.

CONJECTURE 1 (*Hasse-Weil*). *If we put*

$$\Lambda(E,s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)\,,$$

then $\Lambda(E,s)$ has an analytic continuation to the entire complex plane and it satisfies the functional equation

$$\Lambda(E,s) = \varepsilon\Lambda(E,2-s)$$

with $\varepsilon = \pm 1$.

The above ε is called the sign of the functional equation of $L(E,s)$.

If $E/\boldsymbol{Q}$ is modular (i.e. $E/\boldsymbol{Q}$ is parametrized by modular functions), then the above conjecture is known to be true. In our case $E = E_D$ which has complex multiplication by the ring of Gaussian integers, Shimura's result (cf. [Shi], [Shi2]) gives that E_D is modular.

The Birch and Swinnerton-Dyer conjecture gives a misterious relation between an analytic object $L(E,s)$ and arithmetic objects $E(\boldsymbol{Q})$, Ш$(E/\boldsymbol{Q})$, etc.

CONJECTURE 2 (*Birch and Swinnerton-Dyer*). *Assuming the analytic continuation for $L(E,s)$, we have*

(a) $\operatorname{ord}_{s=1}L(E,s) =$ *the* rank of $E(\boldsymbol{Q})$ $(= r,$ *say*$)$.

(b) $\lim_{s\to 1}(s-1)^{-r}L(E,s) = \Omega_E R_E \#Ш(E/\boldsymbol{Q}) \prod_l c_l/(\#E_{\mathrm{tors}}(\boldsymbol{Q}))^2$.

In particular, the above conjecture (b) says that

(b_0) If $L(E,1) \neq 0$, then the rank of $E(\boldsymbol{Q})$ is zero and

$$\frac{L(E,1)}{\Omega_E}\,\frac{(\#E_{\mathrm{tors}}(\boldsymbol{Q}))^2}{\prod_l c_l} = \#Ш(E/\boldsymbol{Q})\,. \tag{12}$$

(b_1) If $L(E,1) = 0$ and $L'(E,1) \neq 0$, then the rank of $E(\boldsymbol{Q})$ is one and

$$\frac{L'(E,1)}{2\Omega_E \hat{h}(P_1)}\,\frac{(\#E_{\mathrm{tors}}(\boldsymbol{Q}))^2}{\prod_l c_l} = \#Ш(E/\boldsymbol{Q})\,, \tag{13}$$

where $\hat{h}(P_1)$ is the height of a generator P_1 of a free part of the Mordell-Weil group $E(\boldsymbol{Q})$. (See [Sil]).

On the Birch and Swinnerton-Dyer conjecture, known results is as follows.

FACT 1 (*Coates and Wiles, Rubin*) ([CW], [Ru], [Ru2]). *Let $E/\boldsymbol{Q}$ be an elliptic curve with complex multiplication. Suppose that $L(E, 1) \neq 0$. Then*

(i) *$E(\boldsymbol{Q})$ and $Ш(E/\boldsymbol{Q})$ are finite.*

(ii) *The l-part of both sides of* (12) *in* (b_0) *are equal for each prime $l \geq 5$, and the 3-part of bothsides of* (12) *in* (b_0) *are equal if $E/\boldsymbol{Q}$ doesn't have complex multiplication by $\boldsymbol{Z}[(-1+\sqrt{-3}/2]$.*

FACT 2 (*Gross and Zagier, Kolyvagin*) ([GZ], [Kol]). *Let $E/\boldsymbol{Q}$ be a modular elliptic curve, and assume $L(E, s)$ has simple zero at $s = 1$. Then $E(\boldsymbol{Q})$ has rank 1 and $Ш(E/\boldsymbol{Q})$ is finite.*

Next, we give a method to compute the quantities as above for $E = E_{pq}$. (p, q are distinct odd prime numbers.)

The real period $\Omega_{E_{pq}}$ is given by

$$\Omega_{E_{pq}} = \frac{\sqrt{2}\pi}{(pq)^{1/4}\mathrm{AGM}(\sqrt{2}, 1)},$$

where AGM means the arithmetic geometric mean of Gauss (c.f. [Cre]).

The quantities $N_{E_{pq}}$ and c_l can be computed by Tate's algorithm [Ta2].

$$N_{E_{pq}} = \begin{cases} 2^6 p^2 q^2 & \text{if } pq \equiv 1 \pmod 4, \\ 2^5 p^2 q^2 & \text{if } pq \equiv 3 \pmod 4, \end{cases}$$

$$c_l = \begin{cases} 1 & \text{if } l \neq 2, p, q, \\ 2 & \text{if } l = p, q, \\ 1 & \text{if } l = 2 \text{ and } pq \equiv 1 \pmod 4, \\ 2 & \text{if } l = 2 \text{ and } pq \equiv 3 \pmod 4. \end{cases}$$

Since E_{pq} has complex multiplication by $\boldsymbol{Z}[\sqrt{-1}]$, we have

$$L_l(E_{pq}, s) = \begin{cases} 1 & \text{if } l = 2, p, q, \\ 1 - a_l l^{-s} + l^{1-2s} & \text{if } l \neq 2, p, q, \end{cases}$$

where a_l can be computed as follows.

If $l \equiv 3 \pmod 4$ and $l \neq p, q$, then

$$a_l = 0.$$

If $l \equiv 1 \pmod 4$ and $l \neq p, q$, factor l in $\boldsymbol{Z}[\sqrt{-1}]$:

$$l = \lambda\bar{\lambda} \text{ with } \lambda \equiv 1 \pmod{2 + 2\sqrt{-1}}.$$

Then

$$a_l = \overline{\left(\frac{-pq}{\lambda}\right)_4}\lambda + \left(\frac{-pq}{\lambda}\right)_4 \bar{\lambda},$$

where $(\alpha/\lambda)_4$ is the 4^{th}-power residue symbol. (see [IR].)

For a method to compute heights (and hence the regulator $R_{E_{pq}}$), see [Cre] or [Sil2].

To compute $L(E_{pq}, 1)$ and $L'(E_{pq}, 1)$, we use the following formula. (See [Ma])

FACT 3. *Let $E/\boldsymbol{Q}$ be a modular elliptic curve,*

$$L(E, s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

its L-function, ε the sign of functional equation for $L(E, s)$, then

$$L(E, 1) = 2\sum_{n=1}^{\infty} \frac{a_n}{n} \exp\left(\frac{-2\pi n}{\sqrt{N_E}}\right)$$

if $\varepsilon = 1$, and

$$L'(E, 1) = 2\sum_{n=1}^{\infty} \frac{a_n}{n} H\left(\frac{2\pi n}{\sqrt{N_E}}\right)$$

if $\varepsilon = -1$ where

$$H(s) = \int_s^{\infty} \frac{\exp(-x)}{x} dx\,.$$

We use the following approximation of $L(E, 1)$ and $L'(E, 1)$. (See Gebel and Zimmer [GeZi].)

Put

$$S_m = 2\sum_{n=1}^{m} \frac{a_n}{n} \exp\left(\frac{-2\pi n}{\sqrt{N_E}}\right)$$

and

$$S'_m = 2\sum_{n=1}^{m} \frac{a_n}{n} H\left(\frac{2\pi n}{\sqrt{N_E}}\right).$$

If $\varepsilon = 1$, then

$$|L(E, 1) - S_m| < 10^{-k}$$

for

$$m > \frac{\sqrt{N_E}}{2\pi n}(2\log 2 + k\log 10 - \log(1 - \exp(-2\pi/\sqrt{N_E})))\,.$$

If $\varepsilon = -1$, then

$$|L'(E, 1) - S'_m| < 10^{-k}$$

for

$$m > \frac{\sqrt{N_E}}{2\pi n} \max\{4, 2\log 2 + k\log 10 - \log(1 - \exp(-2\pi/\sqrt{N_E}))\}\,.$$

Here the integrals $H(2\pi n/\sqrt{N_E})$ must be approximated to within an error of size $10^{-k}/(8m)$.

The sign ε can be computed by the result of Birch and Stephens [BS] (and Proposition 1): If we write $\#S^{(\phi)}(E_{pq}/\boldsymbol{Q}) = 2^{r_1}$ and $\#S^{(\hat{\phi})}(E'_{pq}/\boldsymbol{Q}) = 2^{r_2}$, then

$$\varepsilon = (-1)^{r_1+r_2-2}\,.$$

EXAMPLES.

(i) $p = 311$, $q = 313$. This is the smallest example which satisfies the following property:

p, q are twin prime numbers with $(q/p) = 1$, $E_{pq}(\boldsymbol{Q})$ has rank one (not three) and $Ш(E_{pq}/\boldsymbol{Q})$ is a non-trivial finite group.

Since $\varepsilon = -1$, $L(E_{pq}, 1) = 0$ and

$$S'_m \doteq 9.06556996293884$$

for $m = 2200000$ (with error less than 10^{-5}). Hence it follows from Fact 2 that $E_{pq}(\boldsymbol{Q})$ has rank 1. Then the same argument of the proof of Theorem 2(b) shows that a generator of the free part is $(1, (p+q)/2) = (1, 312)$. (Further, when we use the algorithm in [GPZ], all integral points of E_{pq} are $(1, \pm 312)$, $(97343, \pm 30371016)$ and $(0, 0)$.)

One can compute

$$\hat{h}((1, 312)) \doteq 2.698945375060464\,, \quad \Omega_{E_{pq}} \doteq 0.20993315682460675255\,.$$

Then the left hand side of (13) is

$$\frac{L'(E_{pq}, 1)}{2\Omega_{E_{pq}}\hat{h}((1, 312))} \frac{(\#E_{pq,\mathrm{tors}}(\boldsymbol{Q}))^2}{\prod_l c_l} \doteq 4.000000000000436984\,.$$

So we can expect that $\#Ш(E_{pq}/\boldsymbol{Q}) = 4$. From the facts that the rank of $E_{pq}(\boldsymbol{Q})$ is 1, and Proposition 1, the following commutative diagram with exact rows and columns gives $\#Ш(E_{pq}/\boldsymbol{Q})[2] = 4$.

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \downarrow & & & & \\
 & & E'_{pq}(\boldsymbol{Q})[\hat{\phi}]/\phi(E_{pq}(\boldsymbol{Q})[2]) & & & & 0 & & \\
 & & \downarrow & & & & \downarrow & & \\
0 & \to & E'_{pq}(\boldsymbol{Q})/\phi(E_{pq}(\boldsymbol{Q})) & \xrightarrow{\delta_\phi} & S^{(\phi)}(E_{pq}/\boldsymbol{Q}) & \to & Ш(E_{pq}/\boldsymbol{Q})[\phi] & \to & 0 \\
 & & \downarrow & & & & \downarrow & & \\
0 & \to & E_{pq}(\boldsymbol{Q})/2E_{pq}(\boldsymbol{Q}) & \xrightarrow{\delta_2} & S^{(2)}(E_{pq}/\boldsymbol{Q}) & \to & Ш(E_{pq}/\boldsymbol{Q})[2] & \to & 0 \\
 & & \downarrow & & & & \downarrow & & \\
0 & \to & E_{pq}(\boldsymbol{Q})/\hat{\phi}(E'_{pq}(\boldsymbol{Q})) & \xrightarrow{\delta_{\hat{\phi}}} & S^{(\hat{\phi})}(E'_{pq}/\boldsymbol{Q}) & \to & Ш(E'_{pq}/\boldsymbol{Q})[\hat{\phi}] & \to & 0 \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

(ii) $p = 521$, $q = 523$. Similar computations as example (i) gives the following quantities. (The sign ε of functional equation is -1, and $L(E_{pq}, 1) = 0$.)

$$S'_m \doteq 7.676167412213061$$

for $m = 6300000$ (with error less than 10^{-5}). (So we have $L'(E_{pq}, 1) \neq 0$, the rank of $E_{pq}(\boldsymbol{Q})$ is 1, and $\#(E_{pq}/\boldsymbol{Q})[2] = 4$.)

$$\hat{h}((1, 522)) \doteq 2.955984075921569\,, \quad \Omega_{E_{pq}} \doteq 0.16230143699733870890 46592\,.$$

Then the left hand side of (13) is

$$\frac{L'(E_{pq}, 1)}{2\Omega_{E_{pq}}\hat{h}((1, 522))} \frac{(\#E_{pq,\mathrm{tors}}(\boldsymbol{Q}))^2}{\prod_l c_l} \doteq 3.999999999999961364\,,$$

and we can also expect that $\#Ш(E_{pq}/\boldsymbol{Q}) = 4$.

Theorem 3 follows from the above computations. (For integral points, using the algorithm in [GPZ], we can obtain the desired result.)

7. Tables

In the following tables, we compute the various invariants for the elliptic curves $E = E_{pq}$ for primes p, q with $p < q < 100$.

Table 1. $\mathrm{rank}(E_{pq}(\boldsymbol{Q})) = 0$, $Sha = 1$

p, q	$L(E_{pq}, 1)$								
13, 7	2.401	29, 19	1.531	59, 37	1.085	73, 47	0.969	89, 31	1.023
17, 7	2.245	41, 3	2.227	61, 7	1.631	79, 37	1.009	89, 83	0.800
17, 11	2.006	41, 19	1.404	61, 23	1.212	79, 41	0.983	97, 7	1.453
19, 3	5.398	43, 5	1.937	67, 13	1.365	79, 53	0.922	79, 23	1.079
19, 13	1.871	43, 37	1.174	71, 13	1.346	83, 13	1.294	97, 59	0.853
23, 7	4.164	47, 5	1.894	71, 17	1.258	83, 73	0.841		
23, 17	1.668	47, 41	1.119	71, 61	0.914	89, 3	1.835		
29, 3	2.428	53, 31	1.165	73, 31	1.075	89, 19	1.157		

Table 2. $\mathrm{rank}(E_{pq}(\boldsymbol{Q})) = 0$, $Sha = 9$

p, q	$L(E_{pq}, 1)$				
67, 41	9.220	67, 61	8.348	97, 71	7.327

Table 3. $\mathrm{rank}(E_{pq}(\boldsymbol{Q})) = 0$, $Sha \doteq 4.0$

p, q	$L(E_{pq}, 1)$								
29, 13	3.366	47, 7	3.483	59, 19	2.563	73, 17	2.499	83, 67	1.718
29, 23	5.837	47, 23	2.587	59, 43	2.090	73, 19	4.861	89, 41	1.908
31, 7	3.865	47, 31	2.401	59, 53	3.967	79, 23	2.272	89, 79	3.240
37, 11	6.605	53, 5	3.676	61, 5	3.549	79, 31	2.108	97, 11	5.190
37, 13	3.167	53, 29	2.369	67, 11	2.847	79, 73	3.404	97, 43	3.691
41, 31	4.968	53, 37	2.229	71, 23	2.333	83, 3	3.734		
43, 19	2.774	59, 3	4.067	71, 47	1.952	83, 29	4.235		

Table 4. $\operatorname{rank}(E_{pq}(\boldsymbol{Q})) = 0$, $Sha \doteq 16.0$

p, q	$L(E_{pq}, 1)$				
83, 19	9.415	83, 59	7.092	89, 73	6.608

Table 5. $\operatorname{rank}(E_{pq}(\boldsymbol{Q})) = 1$, $L'(E_{pq}, 1) \neq 0$

p, q	$x(P)$	$L'(E_{pq}, 1)$	Sha				
5, 3	1	4.276	1.0	43, 31	$\frac{81}{4}$	3.234	1.0
7, 3	$\frac{25}{4}$	6.238	1.0	47, 3	$\frac{3025}{64}$	8.758	1.0
7, 5	1	4.612	1.0	47, 11	$\frac{9631107673174849}{361754694022500}$	28,976	1.0
11, 7	$\frac{6889}{1600}$	12.269	1.0	47, 13	$\frac{14161}{225}$	14.037	1.0
13, 11	1	4.663	1.0	47, 17	17	10.545	4.0
17, 3	25	8.364	1.0	47, 19	$\frac{169}{4}$	3.730	1.0
17, 5	$\frac{81}{4}$	5.651	1.0	47, 29	9	4.128	1.0
17, 13	52	10.812	4.0	47, 43	?	27.667	?
19, 5	$\frac{1}{4}$	8.730	1.0	53, 3	25	6.540	1.0
19, 7	$\frac{9}{4}$	4.287	1.0	53, 7	$\frac{25}{4}$	7.615	1.0
23, 3	$\frac{169}{16}$	7.128	1.0	53, 17	$\frac{4225}{36}$	22.944	4.0
23, 5	9	5.580	1.0	53, 19	$\frac{1022272729}{54686025}$	27.953	1.0
23, 11	$\frac{81}{4}$	4.467	1.0	53, 23	$\frac{5041}{225}$	11.240	1.0
23, 19	$\frac{11881}{4900}$	9.4014	1.0	53, 41	$\frac{1849}{36}$	4.342	1.0
29, 11	9	4.904	1.0	59, 7	$\frac{2209}{36}$	6.470	1.0
29, 17	$\frac{169}{36}$	5.341	1.0	59, 13	$\frac{76729}{3025}$	16.159	1.0
31, 3	$\frac{121}{4}$	5.917	1.0	59, 23	$\frac{977624543473542441}{31555344310297600}$	25.682	1.0
31, 11	$\frac{5329}{8100}$	10.296	1.0	59, 29	$\frac{724201}{8100}$	15.831	1.0
31, 13	9	4.770	1.0	59, 31	$\frac{6477025}{226576}$	9.319	1.0
31, 17	$\frac{49}{25}$	9.359	1.0	59, 47	$\frac{305809}{144}$	6.460	1.0
31, 19	$\frac{81}{1600}$	7.955	1.0	61, 11	25	4.969	1.0
31, 29	1	4.157	1.0	61, 17	$\frac{2209}{36}$	25.997	1.0
37, 3	$\frac{25}{4}$	9.249	1.0	61, 31	$\frac{1225}{9}$	7.787	1.0
37, 7	$\frac{9}{4}$	7.823	1.0	61, 41	$\frac{1}{100}$	17.865	4.0
37, 17	$\frac{625}{4}$	4.824	1.0	61, 43	9	3.808	1.0
37, 19	9	4.467	1.0	61, 47	$\frac{471801841}{2528100}$	20.386	1.0
37, 23	$\frac{582169}{225}$	17.759	1.0	61, 59	1	3.596	1.0
41, 5	20	10.050	4.0	67, 5	$\frac{169}{9}$	9.171	1.0
41, 7	$\frac{169}{25}$	10.638	1.0	67, 7	$\frac{3721}{144}$	6.900	1.0
41, 11	225	8.230	1.0	67, 23	$\frac{25}{4}$	3.038	1.0
41, 13	$\frac{529}{4}$	4.905	1.0	67, 31	$\frac{3954475055236689}{2207245062400}$	19.733	1.0
41, 29	$\frac{221841}{36100}$	8.917	1.0	67, 37	$\frac{81}{4}$	5.781	1.0
41, 37	$\frac{3700}{9}$	15.342	4.0	67, 47	$\frac{121}{4}$	2.817	1.0
43, 7	$\frac{27225}{3136}$	9.936	1.0	67, 53	$\frac{1261129}{11025}$	13.420	1.0
43, 13	$\frac{9}{4}$	7.007	1.0	71, 3	$\frac{121}{16}$	5.551	1.0
43, 23	$\frac{49}{4}$	3.327	1.0	71, 5	$\frac{121}{36}$	11.286	1.0
43, 29	$\frac{7882065961}{114383025}$	28.336	1.0	71, 11	$\frac{16129}{900}$	7.341	1.0

Table 6. $\mathrm{rank}(E_{pq}(\boldsymbol{Q})) = 1$, $L'(E_{pq}, 1) \neq 0$ (continued)

p, q	$x(P)$	$L'(E_{pq}, 1)$	*Sha*				
71, 19	$\frac{2275385401}{4928400}$	13.206	1.0	83, 23	$\frac{9}{4}$	2.910	1.0
71, 37	$\frac{121}{900}$	11.126	1.0	83, 31	$\frac{141698792041}{30248862084}$	14.632	1.0
71, 41	$\frac{25150225}{370881}$	17.274	1.0	83, 37	$\frac{912025}{93636}$	15.488	1.0
71, 43	$\frac{52441}{7056}$	6.454	1.0	83, 47	$\frac{314885025}{3444736}$	9.348	1.0
71, 53	9	3.636	1.0	83, 53	$\frac{1352569}{81225}$	13,912	1.0
71, 59	$\frac{225}{4}$	2.770	1.0	83, 71	$\frac{16220506545961}{375558157584}$	13.240	1.0
71, 67	?	37.501	?	83,79	?	37.839	?
73, 5	$\frac{361}{4}$	5.084	1.0	89, 7	$\frac{1}{25}$	9.041	1.0
73, 7	$\frac{3025}{81}$	12.450	1.0	89, 11	11	11.001	4.0
73, 11	$\frac{361}{9}$	8.234	1.0	89, 13	$\frac{37746167851681}{13560602500}$	19.880	1.0
73, 13	$\frac{625}{36}$	4.879	1.0	89, 23	$\frac{191660572287409}{122202680625}$	35.893	1.0
73, 29	$\frac{30151856407852780 81}{4425678074092000}$	23.278	1.0	89, 29	$\frac{81}{100}$	4.443	1.0
73, 37	$\frac{5328}{121}$	15.190	4.0	89, 37	$\frac{13446889}{3034564}$	9.306	1.0
73, 43	$\frac{3374569}{301401}$	16.242	1.0	89, 43	$\frac{5405043361}{3404025}$	20.822	1.0
73, 53	$\frac{1369}{100}$	4.158	1.0	89, 53	$\frac{84800}{289}$	16.963	4.0
73, 59	$\frac{201276047978041}{543765267500625}$	34.577	1.0	89, 59	$\frac{496175625}{1453361129}$	21.812	1.0
73, 61	$\frac{244}{9}$	8.259	4.0	89, 61	$\frac{564001}{841000}$	6.775	1.0
79, 3	$\frac{606841}{44100}$	13.131	1.0	97, 3	3	14.550	4.0
79, 11	$\frac{625}{16}$	4.665	1.0	97, 5	$\frac{6355441}{925444}$	13.422	1.0
79, 13	$\frac{1681}{32400}$	18.150	1.0	97, 13	$\frac{10201}{44100}$	8.878	1.0
79, 17	$\frac{529}{49}$	8.935	1.0	97, 19	$\frac{73441}{441}$	12.434	1.0
79, 19	$\frac{4553685361}{6969600}$	13.265	1.0	97, 29	$\frac{2809}{4}$	4.061	1.0
79, 29	25	4.063	1.0	97, 31	$\frac{31}{225}$	29.476	4.0
79, 43	$\frac{1894039290081}{1478388492100}$	15.590	1.0	97, 37	$\frac{1089}{100}$	4.209	1.0
79, 59	$\frac{192721}{900}$	5.533	1.0	97, 53	$\frac{508016448}{395641}$	31.682	4.0
79, 61	9	3.521	1.0	97, 61	?	41.047	?
79, 67	$\frac{1051899489}{11587216}$	9.213	1.0	97, 67	3429	6.402	1.0
83, 5	$\frac{1521}{25}$	11.746	1.0	97, 79	9	13.235	4.0
83, 7	$\frac{403225}{4356}$	9.846	1.0	97, 83	$\frac{6962448042451225}{2597699613622689}$	31.049	1.0
83, 17	17	10.134	4.0				

In tables, *Sha* is the conjectural value of the order the Shafarevich-Tate group. Note that if $L(E, 1) \neq 0$ then the result of Rubin says that the l-part of Ш = the l-part of *Sha* for all odd primes l, hence *Sha* is the correct value of Ш in Tables 1 and 2.

In Tables 5, 6, 7 and 8, $x(P)$ (or $x(P_i)$) is the x-coordinate of a set of generator(s) P (or P_i's) for the free part of the Mordell-Weil group $E(\boldsymbol{Q})$.

In Tables 5 and 6 we could not find a rational point of E for the four cases $(p, q) = (47, 43)$, $(71, 67)$, $(83, 79)$ and $(97, 61)$, but the results of Gross-Zagier and Rubin give $\mathrm{rank}(E(\boldsymbol{Q})) = 1$.

In Table 9, we could not determine the rank of $E(\boldsymbol{Q})$, but if the Birch and Swinnerton conjecture is correct, we have $\mathrm{rank}(E(\boldsymbol{Q})) = 2$ and P_1, P_2 are generators of the free part.

Table 7. $\mathrm{rank}(E_{pq}(\boldsymbol{Q})) = 2, L^{(2)}(E_{pq}, 1) \neq 0$ ($Sha \doteq 1.0$)

p, q	$x(P_1), x(P_2)$	$L^{(2)}(E_{pq}, 1)/2$			
11, 3	4, 16	8.234	61, 29	16, $\frac{21904}{3969}$	26.555
11, 5	5, $\frac{9}{4}$	10.865	61, 37	$\frac{19044}{25}$, $\frac{83521}{57600}$	71.393
13, 3	3, 27	8.659	61, 53	$\frac{2116}{9}$, $\frac{2209}{64}$	14.209
13, 5	4, $\frac{1}{16}$	13.884	67, 3	100, $\frac{25}{36}$	28.784
19, 11	$\frac{25}{4}$, $\frac{8464}{9}$	10.773	67, 19	$\frac{9}{4}$, $\frac{324}{25}$	19.120
23, 13	13, $\frac{13}{289}$	19.068	67, 29	1421, $\frac{49}{4}$	24.536
29, 5	$\frac{81}{16}$, $\frac{289}{36}$	20.758	67, 43	$\frac{225}{4}$, $\frac{102400}{1521}$	35.305
29, 7	7, $\frac{175}{9}$	11.667	67, 59	$\frac{169}{4}$, $\frac{1936}{9}$	10.826
31, 5	5, $\frac{289}{16}$	18.873	71, 7	$\frac{64}{25}$, $\frac{676}{25}$	39.929
31, 23	$\frac{121}{144}$, $\frac{13924}{169}$	19.255	71, 29	29, $\frac{344549}{8281}$	26.205
37, 5	$\frac{121}{16}$, $\frac{64}{225}$	18.152	71, 31	$\frac{100}{49}$, $\frac{2765569}{19600}$	57.132
37, 29	$\frac{1156}{9}$, $\frac{49}{64}$	14.975	73, 3	12, 48	17.171
41, 17	$\frac{36}{25}$, $\frac{24964}{225}$	46.184	73, 67	$\frac{225}{4}$, $\frac{2412}{121}$	37.986
43, 3	64, $\frac{100}{9}$	19.323	79, 5	45, $\frac{2809}{100}$	26.816
43, 11	$\frac{1}{4}$, $\frac{196}{9}$	11.403	79, 7	36, $\frac{36}{25}$	18.769
43, 17	$\frac{17}{16}$, $\frac{25}{4}$	27.286	79, 47	$\frac{8248384}{247009}$, $\frac{229552801}{9363600}$	33.797
47, 37	$\frac{37}{9}$, $\frac{2809}{36}$	27.724	79, 71	$\frac{305219786089}{2504001600}$, $\frac{1153677920836}{12917004409}$	48.882
53, 11	11, $\frac{9}{4}$	12.521	83, 11	36, $\frac{144}{25}$	17.233
53, 13	$\frac{625}{16}$, $\frac{841}{36}$	19.796	83, 41	$\frac{41}{4}$, $\frac{81}{4}$	19.989
53, 43	$\frac{169}{4}$, $\frac{5203}{169}$	41.346	83, 43	$\frac{289}{4}$, $\frac{4624}{4761}$	35.012
53, 47	47, $\frac{65853225}{15382084}$	43.544	83, 61	61, $\frac{112789}{9409}$	22.530
59, 5	5, $\frac{169}{36}$	20.496	89, 47	188, $\frac{210681}{784}$	37.752
59, 17	$\frac{17}{4}$, $\frac{9}{2}$	22.037	89, 67	$\frac{268}{9}$, $\frac{289}{4}$	21.354
61, 3	3, 75	12.482	97, 17	$\frac{784}{9}$, $\frac{625}{64}$	28.252
61, 13	$\frac{729}{16}$, $\frac{11449}{1764}$	22.902	97, 41	$\frac{657721}{67600}$, $\frac{21325924}{354025}$	98.399
61, 19	171, $\frac{225}{4}$	22.326			

Table 8. $\mathrm{rank}(E_{pq}(\boldsymbol{Q})) = 3, L^{(3)}(E_{pq}, 1) \neq 0$ ($Sha \doteq 1.0$)

p, q	$x(P_1), x(P_2), x(P_3)$	$L^{(3)}(E_{pq}, 1)/6$			
19, 17	17, $\frac{49}{4}$, $\frac{121}{9}$	29.495	73, 71	71, 1, $\frac{1369}{144}$	68.659
41, 23	23, $\frac{729}{49}$, $\frac{2601}{16}$	41.820	89, 5	20, 80, $\frac{49}{36}$	48.759
59, 41	41, $\frac{1025}{64}$, $\frac{4961}{10}$	52.764	89, 71	284, $\frac{121}{81}$, $\frac{5625}{16}$	63.141
73, 23	92, $\frac{361}{49}$, $\frac{2809}{144}$	71.640	97, 47	47, $\frac{1692}{289}$, $\frac{86903}{121}$	59.432

Table 9. $\mathrm{rank}(E_{pq}(\boldsymbol{Q})) = ?, \mathrm{ord}_{s=1} L(E_{pq}, s) = 2$ ($Sha \doteq 4.0$)

p, q	$x(P_1), x(P_2)$	$L^{(2)}(E_{pq}, 1)/2$			
73, 41	16, 164	23.239	97, 73	$\frac{292}{9}$, $\frac{30276}{25}$	48.933
89, 17	68, 36	27.621	97, 89	356, 4	22.929

References

[BS] B. J. BIRCH and N. M. STEPHENS, The parity of the rank of the Mordell-Weil group, *Topology* **5** (1966), 295–299.

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

[Cre] J. E. CREMONA, *Algorithms for Modular Elliptic Curves*, (*2nd ed.*) Cambridge Univ. Press, Cambridge, 1996.

[CW] J. COATES and A. WILES, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 233–251.

[GPZ] J. GEBEL, A. PETHÖ and H. G. ZIMMER, Computing integral points on elliptic curves, *Acta Arith.* **LXVIII** (1994), 171–192.

[GrZa] B. H. GROSS and D. B. ZAGIER, Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986), 225–320.

[GeZi] J. GEBEL and H. G. ZIMMER, Computing the Mordell-Weil group of an elliptic curve over $\boldsymbol{Q}$, in: *Elliptic Curve and Related Topics*, (H. Kisilevski and M. R. Murty, eds.), AMS, 1994, pp. 61–83.

[IR] K. IRELAND and M. ROSEN, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1982.

[Kol] V. A. KOLYVAGIN, Finiteness of $E(\boldsymbol{Q})$ and Ш$(E/\boldsymbol{Q})$ for a subclass of Weil curves, *Math. USSR. Izv.* **32** (1989), 523–542.

[Ma] Yu. I. MANIN, Cyclotomic fields and modular curves, *Russian Math. Surveys* **26** (1971) no. 6, 7–78.

[Ru] K. RUBIN, Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, *Invent. Math.* **89** (1987), 527–560.

[Ru2] K. RUBIN, The main conjecture for imaginary quadratic fields, *Invent. Math.* **103** (1991), 25–68.

[Shi] G. SHIMURA, On the zeta-function of an abelian variety with complex multiplication, *Ann. Math.* **94** (1971), 504–533.

[Shi2] G. SHIMURA, On elliptic curves with complex multiplication as factor of the jacobians of modular function fields, *Nagoya Math. J.* **43** (1971), 199–208.

[Sie] C. L. SIEGEL, Die Gleichung $ax^n - by^n = c$, *Math. Ann.* **114** (1937), 57–68.

[Sil] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1985.

[Sil2] J. H. SILVERMAN, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

[Sm] N. P. SMART, S-integral points on elliptic curves, *Math. Proc. Camb. Phil. Soc.* **116** (1994), 391–397.

[Ta] J. TATE, Duality theorems in Galois cohomology over number fields, *Proc. Intern. Cong. Math., Stockholm*, 1962, pp. 234–241.

[Ta2] J. TATE, Algorithm for determining the type of a singular fiber in an elliptic pencil, in: *Modular Functions of One Variable IV*, Lect. Notes in Math. 476, (B. J. Birch and W. Kuyk, eds.), Springer-Verlag, Berlin, 1975, pp. 33–52.

Department of Mathematics and Informatics
Graduate School of Science and Technology
Chiba University
1–33 Yayoi-cho, Inage-ku, Chiba-shi, 263
Japan
E-mail address: myoshida@math.s.chiba-u.ac.jp