On the equation $y^2 = (x+m)(x^2+m^2)$

Shin-ichi Yoshida

1 Introduction

Let m be a square-free integer. Throughout this paper E_m will denote the elliptic curve given by the equation $y^2 = (x+m)(x^2+m^2)$.

Stroeker and Top [StTo] have consider the Mordell-Weil group $E_m(\mathbb{Q})$ when m is a prime by computing Selmer groups. Schmitt [Sch] also use the same method to obtain an upper bound for the rank of $E_m(\mathbb{Q})$ for square-free m. Lemmermeyer [Lem] has shown that the 2-ranks of the Tate-Shafarevich groups of E_m can be arbitrarily large. MacLeod [MLe] computes some Heegner points for rank 1 curves in the case where m is prime congruent ro 7 (mod 8).

In this paper, first, we will use Heegner points to obtain the rank of $E_m(\mathbb{Q})$ is 1 for various m which contains the truth of the conjecture in the paper of Stroeker and Top [StTo]. Secondly, we will give an analogue result of Tunnell [Tun]. All the methods used in this paper have already appeared in [Yo1], [Yo2].

Some of our results are stated as follows.

Theorem 1.1. (1) *Let p be a prime with $p \equiv -1 \pmod 8$. Then the rank of the Mordell-Weil group $E_m(\mathbb{Q})$ is 1 for $m = p, \pm 2p$.*
(2) *Let formal power series in the variable q be given by*

$$\Phi_{1,3} = \frac{1}{2}\left\{ \sum_{x,y,z\in\mathbb{Z}} q^{3x^2+16y^2+43z^2-2xz} - \sum_{x,y,z\in\mathbb{Z}} q^{11x^2+12y^2+16z^2-4xy} \right\}.$$

Set $\Phi_{1,3} = \sum_{m=1}^{\infty} a_{1,3}(m)q^m$. Let d be a square-free positive integer $\equiv 3 \pmod 8$. If $a_{1,3}(d) \neq 0$ then $E_d(\mathbb{Q})$ is finite. Moreover, under the conjecture of Birch and Swinnerton-Dyer [BiSw], the converse is also true.

The paper is organized as follows. In Section 2, we will use Heegner points to prove Theorem 1.1(1). In Section 3, we will introduce several theta series and give its properties. And then, we will show an analogue of the result of Tunnell [Tun] on the congruent number elliptic curve $y^2 = x^3 - m^2x$. As a corollary, we will obtain Theorem 1.1(2). In Section 4, using the results in Section 3, we will give some finiteness result of $E_m(\mathbb{Q})$ for various m. In particular, we will obtain a stronger result of [StTo].

2 Heegner points

At first, we give some notation and recall some facts.

Given a positive integer N, let $\Gamma_0(N)$ be the group of matrices in $SL_2(\mathbb{Z})$ which are upper triangular modulo N. It acts as a discrete group of Möbius transformation on the Poincaré upper half-plane $\mathfrak{H}$. The group $\Gamma_0(N)$ also acts on cusps $\mathbb{Q} \cup \{i\infty\}$ in the same manner. Let $\mathfrak{H}^*$ denotes $\mathfrak{H} \cup \mathbb{Q} \cup \{i\infty\}$. The modular curve $X_0(N) = \Gamma_0(N)\backslash\mathfrak{H}^*$ is defined over $\mathbb{Q}$. For a $\tau \in \mathfrak{H}^*$, let $[\tau]$ be its corresponding point of $X_0(N)$. The cusps $[i\infty]$ and $[0]$ are $\mathbb{Q}$-rational points of $X_0(N)$. (See [Shi1], [Ogg].)

Let $S_2(N)$ denote the $\mathbb{C}$-vector space of cusp forms of weight two and level $\Gamma_0(N)$ with the trivial character. Let $\varphi(\tau)$ be a normalized newform in $S_2(N)$. Suppose that all the Fourier coefficients of φ are integers. Then the function

$$\begin{aligned} I_\varphi : \mathfrak{H}^* &\longrightarrow \mathbb{C} \\ \tau_0 &\mapsto 2\pi i \int_{\tau_0}^{i\infty} \varphi(\tau) d\tau \end{aligned}$$

is well-defined. Also, the map

$$\begin{aligned} P_\varphi : \Gamma_0(N) &\longrightarrow \mathbb{C} \\ M &\mapsto I_\varphi(\tau_1) - I_\varphi(M(\tau_1)) \end{aligned}$$

is well-defined (independent of $\tau_1 \in \mathfrak{H}^*$) and is a group homomorphism (see Knapp [Kna]). The image Λ_φ of P_φ defines a lattice of rank two in $\mathbb{C}$. By an assumption on φ, the elliptic curve $E_\varphi = \mathbb{C}/\Lambda_\varphi$ is defined over $\mathbb{Q}$ and the map I_φ induces a morphism

$$\widetilde{I}_\varphi : X_0(N) \longrightarrow E_\varphi$$

defined over $\mathbb{Q}$. By definition, we have $\widetilde{I}_\varphi([i\infty])$ is the zero of E_φ and $\widetilde{I}_\varphi([0])$ is in $E_\varphi(\mathbb{Q})$. (Moreover, the point $\widetilde{I}_\varphi([0])$ is a torsion point, but we do not use this fact since we use only newforms φ such that the groups $E_\varphi(\mathbb{Q})$ are finite.)

For $t = \pm 1, \pm 2$, let φ_t be the normalized newform such that the corresponding elliptic curve E_{φ_t} is isogenous to our elliptic curve E_t. In fact, each of φ_t's is in $S_2(128)$ and the corresponding elliptic curve E_{φ_t} is isomorphic to the elliptic curve E_t from Table 1 in [Cre]. Also we have the following table. (Here we use the codes in [Cre].)

t	$E_{\varphi_t} \cong E_t$	$E_t(\mathbb{Q})$
1	128A1(C)	$\mathbb{Z} \times \mathbb{Z}/2$
-1	128C1(A)	$\mathbb{Z}/2$
2	128D1(G)	$\mathbb{Z}/2$
-2	128B1(F)	$\mathbb{Z}/2$

Let $\Omega(\varphi_t)$ be the least positive real period of Λ_{φ_t}. Since $E_t(\mathbb{R}) \cong E_{\varphi_t}(\mathbb{R})$ is connected, we see that $\Omega(\varphi_t)$ is also the real period $\Omega(E_t)$ of E_t.

Let $L(E_t, s)$ denote the L-series of E_t, which is defined on $\mathrm{Re}(s) > 3/2$. (cf. App.C of [Sil]). Since E_t is modular, $L(E_t, s)$ has an analytic continuation to all $\mathbb{C}$.

From the Table 4 in [Cre] and using the fact that

$$L(E_t, 1) = -\int_0^{i\infty} 2\pi i \varphi_t(\tau) d\tau = -I_{\varphi_t}(0)$$

(cf. [Cre], p.30, 37), we have

$$I_{\varphi_t}(0) = \begin{cases} -\Omega(\varphi_t)/2 & \text{if } t = -1, \pm 2. \\ 0 & \text{for } t = 1. \end{cases}$$

In particular, we have proved

Lemma 2.1. *The point $\widetilde{I}_{\varphi_t}([0])$ is a torsion point of exact order two in $E_t(\mathbb{Q})$.*

We also use the following lemma.

Lemma 2.2. *Let W_{128} be the involution of $X_0(128)$ induced by $\tau \mapsto -1/128\tau$. Then, for any $\tau_0 \in \mathfrak{H}^*$, we have*

$$\widetilde{I}_{\varphi_t}([\tau_0]) = \widetilde{I}_{\varphi_t}([0]) - \widetilde{I}_{\varphi_t}(W_{128}[\tau_0])$$

for $t = -1, \pm 2$.

For a proof, we can use the same argument as Lemma 4.3 of [Yo1]. □

Proof (of Theorem 1.1(1)). Since $p \equiv -1 \pmod 8$, the prime 2 splits in the quadratic field $K = \mathbb{Q}(\sqrt{-p})$. Write $128 = \mathfrak{n}\overline{\mathfrak{n}}$ with $(\mathfrak{n}, \overline{\mathfrak{n}}) = 1$, where $\mathfrak{n}$ is an ideal of the ring $\mathcal{O}_K$ of integers in K and the bar denotes the (complex) conjugation. The inclusion $\mathcal{O}_K \subset \mathfrak{n}^{-1}\mathcal{O}_K$ induces an isogeny $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathfrak{n}^{-1}\mathcal{O}_K$ whose kernel is $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/128$. Hence the pair $(\mathbb{C}/\mathcal{O}_K, \mathbb{C}/\mathfrak{n}^{-1}\mathcal{O}_K)$ represents a 'Heegner' point $[\tau_p]$ (say) of $X_0(128)$ ($\tau_p \in \mathfrak{H}$). Moreover, by the theory of complex multiplication, $[\tau_p]$ is rational over the Hilbert class field $K(1)$ of K. Set

$$Q = \sum_{\sigma \in \mathrm{Gal}(K(1)/K)} \sigma \widetilde{I}_{\varphi_t}([\tau_p]) \in E_t(K).$$

By using the well-known fact that the involution W_{128} induces the complex conjugation on E_t, Lemma 2.2 gives

$$\begin{aligned} \overline{Q} &= \sum_{\sigma \in \mathrm{Gal}(K(1)/K)} \sigma \widetilde{I}_{\varphi_t}(W_{128}[\tau_p]) \\ &= h(-p)\widetilde{I}_{\varphi_t}([0]) - Q, \end{aligned}$$

where $h(-p) = [K(1) : K]$ is the class number of K. In particular

$$Q - \overline{Q} = h(-p)\widetilde{I}_{\varphi_t}([0]) - 2\overline{Q}.$$

Since $p \equiv -1 \pmod 4$, the class number $h(-p)$ is odd. By a direct computation, we can easily check that every rational torsion point of exact order two in E_t is not divisible by two in $E_t(K)$ if $t = -1, \pm 2$. Therefore the point $h(-p)\widetilde{I}_{\varphi_t}([0]) \in E_m$ $(t = -1, \pm 2)$ is not divisible by two in $E_t(K)$ by using the duplication formula, and then we obtain that the point $Q - \overline{Q}$ of $E_t(K)$ is of the form $(u_0, v_0\sqrt{-p})$ with $u_0, v_0 \in \mathbb{Q}, v_0 \neq 0$. Hence we have the point

$$(-pu_0, p^2 v_0) \in E_{-tp}(\mathbb{Q}) \quad (t = -1, \pm 2)$$

of infinite order. So we have a rational point of E_{-tp} which is not torsion $(t = -1, \pm 2)$. Since it is known that $\mathrm{rank} E_{-tp}(\mathbb{Q}) \leq 1$ ([StTo]), we obtain that the rank of $E_{-tp}(\mathbb{Q})$ is exactly 1. Moreover, the result of Gross and Zagier [GrZa] gives $\mathrm{ord}_{s=1} L(E_{-tp}, s) = 1$. This completes the proof of Theorem 1.1(1). □

3 Analogue of the result of Tunnell

As in the previous section, for each $t = \pm 1, \pm 2$ let $\varphi_t \in S_2(128)$ be the newform corresponding to the (modular) elliptic curve E_t. In particular, φ_t is a common eigenfunction of the Hecke operator $T_2(p)$ for all odd primes p (say, $T_2(p)\varphi_t = \lambda_{t,p}\varphi_t$).

We also use the following notation.

By χ_c, we denote the Dirichlet character corresponding to $\mathbb{Q}(\sqrt{c})/\mathbb{Q}$ $(c \in \mathbb{Z}, c \neq 0)$.

Let N be a positive integer divisible by 4 and χ a quadratic Dirichlet character modulo N such that $\chi(-1) = 1$. Let $S_{3/2}(N, \chi)$ denote the $\mathbb{C}$-vector space of modular cusp forms of weight $3/2$ with character χ, $S^{\circ}_{3/2}(N, \chi)$ the subspace generated by the forms of types

$$\theta_{\psi,c}(\tau) = \sum_{m \in \mathbb{Z}} \psi(m) m q^{cm^2},$$

where c is any positive integer and ψ is any quadratic character with conductor r_ψ such that $4r_\psi^2 c \mid N$ and $\chi = \psi\chi_c\chi_{-1}$.(See [Shi2].) Let $S^{\perp}_{3/2}(N, \chi)$ denote the orthogonal complement of $S^{\circ}_{3/2}(N, \chi)$ with respect to the Petersson inner product and $S^{\perp}_{3/2}(N, \chi, \varphi_t)$ the subspace of $S^{\perp}_{3/2}(N, \chi)$ which consists of elements Φ such that $T_{3/2}(p^2)\Phi = \lambda_{t,p}\Phi$ for all primes $p \nmid N$, where $T_{3/2}(p^2)$ is the p^2-th Hecke operator which acts on $S_{3/2}(N, \chi)$ (see [Shi2]).

Definition 3.1. Let us define several quadratic forms $Q^{(k)}_{t,\alpha} = Q^{(k)}_{t,\alpha}(x, y, z)$ as

follows.

(1) $Q^{(1)}_{1,3} = 3x^2 + 16y^2 + 43z^2 - 2xz,\ Q^{(2)}_{1,3} = 11x^2 + 12y^2 + 16z^2 - 4xy$

(2) $Q^{(1)}_{1,5} = 5x^2 + 5y^2 + 44z^2 + 4yz + 4xz + 2xy,$
$Q^{(2)}_{1,5} = 8x^2 + 12y^2 + 13z^2 - 4yz - 8xz$

(3) $Q^{(1)}_{-1,1} = x^2 + 16y^2 + 128z^2,\ Q^{(2)}_{-1,1} = 4x^2 + 16y^2 + 33z^2 - 4xz,$
$Q^{(3)}_{-1,1} = 9x^2 + 16y^2 + 16z^2 - 8xy$

(4) $Q^{(1)}_{-1,7} = 7x^2 + 7y^2 + 44z^2 - 4yz - 4xz - 2xy,$
$Q^{(2)}_{-1,7} = 12x^2 + 15y^2 + 15z^2 + 14yz + 4xz + 4xy$

(5) $Q^{(1)}_{2,1} = x^2 + 10y^2 + 26z^2 - 4yz,\ Q^{(2)}_{2,1} = 4x^2 + 9y^2 + 10z^2 - 8yz - 4xy,$
$Q^{(3)}_{2,1} = 3x^2 + 9y^2 + 11z^2 + 6yz + 2xz + 2xy$

(6) $Q^{(1)}_{2,3} = 3x^2 + 7y^2 + 27z^2 + 6yz + 2xz + 2xy,$
$Q^{(2)}_{2,3} = 7x^2 + 8y^2 + 12z^2 + 8yz + 4xz + 4xy$

(7) $Q^{(1)}_{-2,1} = x^2 + 8y^2 + 128z^2,\ Q^{(2)}_{-2,1} = 4x^2 + 8y^2 + 33z^2 - 4xz,$
$Q^{(3)}_{-2,1} = 8x^2 + 9y^2 + 16z^2 - 8yz$

(8) $Q^{(1)}_{-2,3} = 3x^2 + 5y^2 + 19z^2 - 2yz - 2xz - 2xy,$
$Q^{(2)}_{-2.3} = 5x^2 + 6y^2 + 10z^2 - 4yz - 4xz$

From Preposition 3 and Proposition 4 of [Leh] (see also [Dic], [Jon]) we can check the following lemma by using a computer.

Lemma 3.2. *The quadratic forms in each of (1) $\sim$ (8) of Definition 3.1 form a genus.*

We use the abbreviation $\Theta(Q)$ for the Θ-series corresponding to a positive definite quadratic form Q. For $(t, \alpha) = (1,3), (1,5), (-1,1), (-1,7), (\pm 2, 1)$ or $(\pm 2, 3)$, set

$$\Phi_{t,\alpha} = \left\{\Theta(Q^{(1)}_{t,\alpha}) - \Theta(Q^{(2)}_{t,\alpha})\right\} \times \begin{cases} 1/4 & \text{if } (t,\alpha) = (1,5), (-1,7), \\ 1/2 & \text{otherwise.} \end{cases}$$

Theorem 3.3. *With the above notation, we have the following.*

(1-1) $\Phi_{1,3} \in S^{\perp}_{3/2}(512, \chi_2, \varphi_{-2})$.

(1-2) $\Phi_{1,5} \in S^{\perp}_{3/2}(512, \chi_1, \varphi_{-1})$.

(2) $\Phi_{-1,1}, \Phi_{-1,7} \in S^{\perp}_{3/2}(512, \chi_2, \varphi_2)$.

(3-1) $\Phi_{2,1} \in S^{\perp}_{3/2}(512, \chi_1, \varphi_{-2})$.

(3-2) $\Phi_{2,3} \in S^{\perp}_{3/2}(512, \chi_2, \varphi_{-1})$.

(4) $\Phi_{-2,1}, \Phi_{-2,3} \in S^{\perp}_{3/2}(512, \chi_1, \varphi_2)$.

Proof. We use the notation from section 1 of [Yo2]. Each statement of this theorem can be proved similarly, so we only give the proof for the part (1-1).

From Lemma 3.2, one sees that $\Phi_{1,3}$ is an element of $S_{3/2}(512, \chi_2)$. Moreover, by comparing the Fourier coefficients of $T_{3/2}(p^2)\Phi_{1,3}$ with those of $\Phi_{1,3}$, we see that $\Phi_{1,3}$ is eigenfunction of $T_{3/2}(p^2)$ for $p = 3, 5$ with eigenvalue $-2, 2$, respectively.

$S^{\circ}_{3/2}(512, \chi_2)$ is generated by $\theta_{\chi_{-1},2}, \theta_{\chi_{-1},8}$, and $\theta_{\chi_{-2},1}$. In the same way, we obtain that $\theta_{\chi_{-1},2}$, $\theta_{\chi_{-1},8}$, $\theta_{\chi_{-2},1}$ are eigenfunctions of $T_{3/2}(3^2)$ with eigenvalue $-4, -4, 4$, respectively.

Therefore $\Phi_{1,3}$ is in $S^{\perp}_{3/2}(512, \chi_2)$ since the adjoint of $T_{3/2}(3^2)$ with respect to the Petersson inner product (on $S_{3/2}(512, \chi_2)$) is $\overline{\chi_2(3)}T_{3/2}(3^2) = -T_{3/2}(3^2)$.

From Table 3 of [Cre], the newform $\varphi_{-2} \in S_2(128)$ has eigenvalues $\lambda_{-2,3} = -2, \lambda_{-2,5} = 2$ for $T_2(3), T_2(5)$, respectively. Hence $\Phi_{1,3}$ is an elements of $S^{\perp}_{3/2}(512, \chi_2, \varphi_{-2})$ by the algorithm of Antoniadis, Bungert and Frey [ABF], [Fre] (see also the last remark in the section 2 of [Yo2]). This proves (1-1). □

Remark. There are various relations between theta function. For instance, we can find that

$$\tilde{\Phi}_{2,3} = \frac{1}{4}\left\{\Theta(\tilde{Q}^{(1)}_{2,3}) - \Theta(\tilde{Q}^{(2)}_{2,3})\right\},$$

where

$$\begin{aligned} \tilde{Q}^{(1)}_{2,3} &= 2x^2 + 3y^2 + 26z^2 + 2yz + 2xy, \\ \tilde{Q}^{(2)}_{2,3} &= 2x^2 + 7y^2 + 10z^2 + 2yz + 2xy. \end{aligned}$$

Let $\Phi_{t,\alpha} = \sum_{m=1}^{\infty} a_{t,\alpha}(d)q^m$ $(q = e^{2\pi i\tau}, \tau \in \mathfrak{H})$ denote the modular form defined as above. Using the theorem of Waldspurger [Wal], we obtain the following.

Theorem 3.4. *Let $d > 0$ be a square-free odd integer. Then we have*

$$(1) \quad L(E_d, 1)/\Omega(E_d) = \begin{cases} a_{1,3}(d)^2 & \text{if } d \equiv 3 \pmod 8 \\ 2a_{1,5}(d)^2 & \text{if } d \equiv 5 \pmod 8 \\ 0 & \text{otherwise,} \end{cases}$$

$$(2) \quad L(E_{-d}, 1)/\Omega(E_{-d}) = \begin{cases} \frac{1}{2}a_{-1,1}(d)^2 & \text{if } d \equiv 1 \pmod 8 \\ 4a_{-1,7}(d)^2 & \text{if } d \equiv 7 \pmod 8 \\ 0 & \text{otherwise,} \end{cases}$$

$$(3) \quad L(E_{\pm 2d}, 1)/\Omega(E_{\pm 2d}) = \begin{cases} \frac{1}{2}a_{\pm 2,1}(d)^2 & \text{if } d \equiv 1 \pmod 8 \\ a_{\pm 2,3}(d)^2 & \text{if } d \equiv 3 \pmod 8 \\ 0 & \text{otherwise,} \end{cases}$$

Proof. (1) From Theorem 3.3(1), the main theorem of Waldspurger [Wal] in our case says that

$$\frac{L(E_d,1)}{\Omega(E_d)} \times a_{1,\alpha}(\alpha)^2 = \frac{L(E_\alpha,1)}{\Omega(E_\alpha)} \times a_{1,d}(d)^2$$

if $d \equiv \alpha \pmod 8$ for $\alpha = 3, 5$. By a computer calculation, we obtain that $\frac{L(E_3,1)}{\Omega(E_3)} = 1$ and $\frac{L(E_5,1)}{\Omega(E_5)} = 2$. It is easy to see that $a_{1,3}(3) = a_{1,5}(5) = 1$. If $d \equiv 1, 7 \pmod 8$ then $L(E_d, 1)$ vanishes from the fact that the sign of functional equation for $L(E_d, s)$ is -1 by Theorem 1.3 of [Sch]. Hence (1) of the theorem is proved. (2) and (3) can be proved by the same argument. □

Let d be a square-free positive odd integer. Put

$$\begin{aligned} u_1(d) &= \sharp\{p : \text{prime} |\ \ p \mid d,\ p \equiv 1 \pmod 4\} \\ u_3(d) &= \sharp\{p : \text{prime} |\ \ p \mid d,\ p \equiv 3 \pmod 4\}. \end{aligned}$$

We also denote

$$\begin{aligned} (1)\quad \text{Ш}_d &= \begin{cases} a_{1,3}(d)^2/2^{2u_1(d)+u_3(d)-1} & \text{if } d \equiv 3 \pmod 8 \\ a_{1,5}(d)^2/2^{2u_1(d)+u_3(d)-2} & \text{if } d \equiv 5 \pmod 8, \end{cases} \\ (2)\quad \text{Ш}_{-d} &= \begin{cases} a_{-1,1}(d)^2/2^{2u_1(d)+u_3(d)} & \text{if } d \equiv 1 \pmod 8 \\ a_{-1,7}(d)^2/2^{2u_1(d)+u_3(d)-3} & \text{if } d \equiv 7 \pmod 8, \end{cases} \\ (3)\quad \text{Ш}_{\pm 2d} &= \begin{cases} a_{\pm 2,1}(d)^2/2^{2u_1(d)+u_3(d)} & \text{if } d \equiv 1 \pmod 8 \\ a_{\pm 2,3}(d)^2/2^{2u_1(d)+u_3(d)-1} & \text{if } d \equiv 3 \pmod 8. \end{cases} \end{aligned}$$

As a corollary, we have the following by the result of Kolyvagin [Kol1], [Kol2] with Tate's algorithm [Tat].

Corollary 3.5. *Let $(t, \alpha) = (1,3), (1,5), (-1, \pm 1), (2,1)$ or $(2,3)$. Let $d > 0$ be a square-free integer with $d \equiv \alpha \pmod 8$. Assume that $a_{t,\alpha}(d) \neq 0$. Then both the Mordell-Weil group $E_{td}(\mathbb{Q})$ and the Tate-Shafarevich group $\text{Ш}(E_{td})$ are finite. Moreover, assuming the Birch and Swinnerton-Dyer conjecture [BiSw], we have $\sharp\text{Ш}(E_{td}) = \text{Ш}_{td}$.*

Theorem 1.1(2) follows from this corollary at once.

4 Application

In this section, we will give various non-vanishing results of $L(E_m, 1)$.

For a positive definite quadratic form Q and a positive integer d, let $N(d, Q)$ denote the number of representations of d by Q. As before, let $h(D)$ be the class number of $\mathbb{Q}(\sqrt{D})$ of discriminant $D < 0$.

Theorem 4.1. *Let p is a prime such that $p \equiv 3 \pmod 8$. Then $L(E_p, 1) \neq 0$ Therefore $E_p(\mathbb{Q})$ and $Ш(E_p)$ are finite. Moreover, the 2-torsion part of the conjecture of Birch and Swinnerton-Dyer is true.*

Proof. By Lemma 3.2 and Theorem 86 of [Jon], one can obtain that

$$N(p, Q_{1,3}^{(1)}) + N(p, Q_{1,3}^{(2)}) = h(-8p).$$

Therefore we have

$$\begin{aligned} 2a_{1,3}(p) &= N(p, Q_{1,3}^{(1)}) - N(p, Q_{1,3}^{(2)}) \\ &= 2N(p, Q_{1,3}^{(1)}) - N(p, Q_{1,3}^{(1)}) - N(p, Q_{1,3}^{(2)}) \\ &= 2N(p, Q_{1,3}^{(1)}) - h(-8p). \end{aligned}$$

by definition of $a_{1,3}(p)$. From a result of Pizer [Piz], we see that $h(-8p) \equiv 2 \pmod 4$ since p is prime congruent to 3 (mod 4). It is trivial that $N(p, Q_{1,3}^{(1)})$ is even. Therefore $a_{1,3}(p)$ is odd. In particular, $L(E_p, 1)/\Omega(E_p) = a_{1,3}(p)^2 \neq 0$ and both $E_p(\mathbb{Q})$ and $Ш(E_p)$ are finite. On the one hand, by two-descent method (see [StTo]), the 2-torsion part of $Ш(E_p)$ is trivial. On the other hand, we see that $Ш_p = a_{1,3}(p)^2$ is odd by Corollary 3.5. So the 2-torsion part of the conjecture of Birch and Swinnerton-Dyer is true. □

Remark. By the same argument, we also obtain the same result holds for all primes $p \equiv 5 \pmod 8$. Hence, we have a generalization of [StTo].

Theorem 4.2. *If p is a prime such that $p \equiv 7 \pmod{16}$, then $a_{-1,7}(p) \neq 0$. (So $L(E_{-p}, 1) \neq 0$.) In particular, both $E_{-p}(\mathbb{Q})$ and $Ш(E_{-p})$ are finite. Moreover, the 2-torsion part of $Ш(E_{-p})$ is non-trivial.*

Proof. The same argument as the proof of Theorem 4.1 gives

$$N(p, Q_{-1,7}^{(1)}) + N(p, Q_{-1,7}^{(2)}) = h(-8p).$$

Therefore we have

$$\begin{aligned} 4a_{-1,7}(p) &= N(p, Q_{-1,7}^{(1)}) - N(p, Q_{-1,7}^{(2)}) \\ &= N(p, Q_{-1,7}^{(1)}) + N(p, Q_{-1,7}^{(2)}) - 2N(p, Q_{-1,7}^{(2)}) \\ &= h(-8p) - 2N(p, Q_{-1,7}^{(2)}) \end{aligned}$$

by definition of $a_{-1,7}(p)$. From a result of Pizer [Piz], we see that $h(-8p) \equiv 4 \pmod 8$ since p is prime congruent to 7 (mod 16). Since
$N(p, Q_{-1,7}^{(2)})$

$$\begin{aligned} &= \sharp\left\{(x,y,z) \in \mathbb{Z}^3 : 12x^2 + 15y^2 + 15z^2 + 14yz + 4xz + 4yz = p\right\} \\ &= \sharp\left\{(x,y,z) \in \mathbb{Z}^3 : 12x^2 + 15y^2 + 15z^2 + 14yz + 4xz + 4yz = p, x(y-z) \neq 0\right\} \\ &\quad + \sharp\left\{(y,z) \in \mathbb{Z}^2 : 15y^2 + 15z^2 + 14yz = p\right\} \\ &\equiv 0 \pmod 4, \end{aligned}$$

we find that $4a_{-1,7}(p) \equiv 4 \pmod 8$. In particular, $a_{-1,7}(p) \neq 0$ and the finiteness of $E_{-p}(\mathbb{Q})$ and $Ш(E_{-p})$ follows from Corollary 3.5. Moreover, by two-descent method (see [Sch]), the 2-torsion part of $Ш(E_{-p})$ is non-trivial. We also note that $4 \mid\mid Ш_{-p}$ since $a_{-1,7}(p)$ is odd. □

References

[ABF] J. A. Antoniadis, M. Bungert and G. Frey, Properties of twists of elliptic curves, *J. reine angew. Math.* **405** (1990), 1–28.

[BiSw] B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves II, *J. reine angew. Math.* **218** (1965), 79–108.

[Cre] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, (2nd ed.), Cambridge Univ. Press, Cambridge, 1997.

[Dic] L. E. Dickson, *Studies in the Theory of Numbers* Chelsea Pub.Co., 1957.

[Fre] G. Frey, Construction and arithmetical applications of modular forms of low weight, in: *Elliptic Curves and Related Topics*, (H.Kisilevsky and M.R.Murty, eds.), CRM Proceedings and Lecture Notes vol.4, American Math.Soc., 1994, pp.1–21.

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

[Jon] B. W. Jones, The Arithmetic Theory of Quadratic Forms, Mathematical Association of America, 1950.

[Kna] A. W. Knapp, *Elliptic Curves*, Princeton Univ. Press, Princeton, NJ., 1992.

[Kol1] V. A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a subclass of Weil curves, *Math. USSR. Izv.* **32** (1989), 523–542.

[Kol2] ———, Euler systems, in: *The Grothendieck Festschrift vol.II*, (P. Cartier, L. Illusie, et al, eds.), Progr. in Math. 87, Birkhäuser, 1990, pp.435–483.

[Leh] J. L. Lehman, Levels of positive definite ternary quadratic forms, *Math. Comp.* **58** (1992), 399–417.

[Lem] F. Lemmermeyer, On Tate-Shafarevich groups of some elliptic curves, in; *Algebraic Number Theory and Diophantine Analysis*, de Gruyter, Berlin, 2000, 277–291.

[MLe] A. J. MacLeod, A note on the curve $Y^2 = (X+p)(X^2+p^2)$, *Rocky Mountain J. Math.* **34** (2004), 263–267.

[Ogg] A. P. Ogg, Rational points on certain elliptic modular curves, in: *Analytic Number Theory*, Proc. Symp. in Pure. Math. **XXIV,** Amer. Mat. Soc., 1973, pp.221–231.

[Piz] A. Pizer, On the 2-part of the class number of imaginary quadratic number fields, *Journal of Number Theory* **8** (1976), 184–192.

[Sch] S. Schmitt, Computation of the Selmer groups of certain parametrized elliptic curves, *Acta Arith.* **LXXVIII.3** (1997), 241–254.

[Shi1] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten, Tokyo, and Princeton Univ. Press, Princeton, N.J., 1971.

[Shi2] ———, On modular forms of half-integral weight, *Math. Ann.* **97** (1973), 440–481.

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

[StTo] R. J. Stroeker and T. Top, On the equation $Y^2 = (X + p)(X^2 + p^2)$, *Rocky Mountain J. Math.* **27** (1994), 1135–1161.

[Tat] 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.

[Tun] J. B. Tunnell, A classical diophantine problem and moduler forms of weight 3/2, *Invent. Math.* **72** (1983), 323–334.

[Wal] J.-L. Waldspurger, Sur les coefficients de Fourier des forms modulaires de poids demi-entier, *J. de Math. pures et appl.* **60** (1981), 375–484.

[Yo1] S. Yoshida, Some variants of the congruent number problem I, *Kyushu J. of Math.* **55** (2001), 387-404.

[Yo2] ———, Some variants of the congruent number problem II, *Kyushu J. of Math.* **56** (2002), 147-165.

Department of Mathematics and Informatics
Graduate School of Science and Technology
Chiba University
1-33 Yayoi-cho, Inage-ku, Chiba-shi, 263-8522
Japan

E-mail address: myoshida@math.s.chiba-u.ac.jp