ACTA ARITHMETICA
170.4 (2015)

On second 2-descent and non-congruent numbers

by

Yi Ouyang and Shenxing Zhang (Hefei)

1. Introduction and main results. Let n be a fixed positive square-free integer and let E_i and E_i' $(i = 1, 2, 3)$ be the elliptic curves

$$\begin{aligned} E_1 &: \quad y^2 = x^3 - n^2x, & E_1' &: \quad y^2 = x^3 + 4n^2x,\\ E_2 &: \quad y^2 = x(x+n)(x+2n), & E_2' &: \quad y^2 = x^3 - 6nx^2 + n^2x,\\ E_3 &: \quad y^2 = x(x-n)(x-2n), & E_3' &: \quad y^2 = x^3 + 6nx^2 + n^2x. \end{aligned}$$

It is well known that n is a non-congruent number if and only if one (or equivalently all) of the above elliptic curves has Mordell–Weil rank zero. In this paper we shall use the so-called second 2-descent to bound the rank of the image of 2-Selmer groups in the Selmer groups of the isogenies. As a consequence we find several series of non-congruent numbers.

We start with an overview of notation. For p a prime and x a rational or p-adic number such that $\operatorname{ord}_p(x)$ is even, the *modified Legendre symbol* is

$$\left(\frac{x}{p}\right) := \left(\frac{xp^{-\operatorname{ord}_p(x)}}{p}\right). \tag{1.1}$$

Thus $\left(\frac{\cdot}{p}\right)$ defines a homomorphism from $\{x \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \operatorname{ord}_p(x) \text{ is even}\}$ to $\{\pm 1\}$. Similarly, for an integer $m \geq 2$, the Jacobi symbol $\left(\frac{\cdot}{m}\right)$ is modified to be a multiplicative homomorphism from $\{x \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \operatorname{ord}_p(x) \text{ is even for all } p \mid m\}$ to $\{\pm 1\}$. Let

$$\left[\frac{x}{m}\right] := \left(1 - \left(\frac{x}{m}\right)\right)/2. \tag{1.2}$$

The symbol $\left[\frac{\cdot}{m}\right]$ defines an additive homomorphism from $\{x \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \operatorname{ord}_p(x) \text{ is even for all } p \mid m\}$ to $\mathbb{F}_2$, which we call the *additive Jacobi* (or *Legendre* if $m = p$) *symbol*.

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11D25.
Key words and phrases: non-congruent number, 2-descent.

DOI: 10.4064/aa170-4-3

We let m be the odd part of n, i.e., $n = (2, n)m$, where (a, b) denotes the greatest common divisor of non-zero integers a and b. Suppose $m = p_1 \cdots p_k$ is the prime decomposition of m.

We let A be the $k \times k$ matrix with (i, j)-entries $\left[\frac{p_j}{p_i}\right]$ for $i \neq j$ and with (i, i)-entries $\left[\frac{m/p_i}{p_i}\right]$, and

$$C = \operatorname{diag}\left\{\left[\frac{-1}{p_1}\right], \ldots, \left[\frac{-1}{p_k}\right]\right\}, \quad D = \operatorname{diag}\left\{\left[\frac{2}{p_1}\right], \ldots, \left[\frac{2}{p_k}\right]\right\},$$
$$\vec{0} = (0, \ldots, 0)^{\mathrm{T}}, \quad \vec{1} = (1, \ldots, 1)^{\mathrm{T}}.$$

Moreover, all matrices and vectors in this paper are defined over $\mathbb{F}_2$. For $\vec{v} = (v_1, \ldots, v_k)^{\mathrm{T}} \in \mathbb{F}_2^k$, we set

$$d(\vec{v}) := \prod_{i:\, v_i = 1} p_i.$$

In particular, $d(\vec{0}) = 1$ and $d(\vec{1}) = m$. Conversely, for d a factor of $2m$, we let $\vec{v}(d) := (v_1, \ldots, v_k)^{\mathrm{T}}$ be such that $v_i = 1$ if $p_i \mid d$.

THEOREM 1.1.

(1) *Assume $n \equiv 1 \bmod 8$, $p_i \equiv 1 \bmod 4$ and $\operatorname{rank} A = k - 1$. Assume $\vec{v}$ is a root of the equation $A\vec{x} = D\vec{1}$ and let $d = d(\vec{v})$. Write $2d = \tau^2 + \mu^2$ and choose $\sqrt{-1}$ in $\mathbb{Z}/n\mathbb{Z}$ such that $p \mid \tau - \sqrt{-1}\,\mu$ for all $p \mid d$. If $\left[\frac{\tau + \sqrt{-1}\,\mu}{n}\right] + \left[\frac{2}{d}\right] = 1$, then n is a non-congruent number. In particular, if $p_i \equiv 1 \bmod 8$, $\operatorname{rank} A = k - 1$ and $\left(\frac{1+\sqrt{-1}}{n}\right) = -1$, then n is a non-congruent number.*

(2) *Assume $m \equiv 1 \bmod 8$, $p_i \equiv \pm 1 \bmod 8$, and*

$$\operatorname{rank} A = \operatorname{rank}(A + C) = k - 1.$$

Write $m = 2\mu^2 - \tau^2$. If the odd part of $|\mu|$ is $\equiv 3 \bmod 4$, then $n = m$ is a non-congruent number. If $\left(\frac{2+\sqrt{2}}{m}\right) = -1$, then $n = 2m$ is a non-congruent number.

REMARK 1.2. Note that A is singular since $A\vec{1} = 0$. Thus the condition $\operatorname{rank} A = k - 1$ in (1) implies that the image of A in $\mathbb{F}_2^k$ is the hyperplane $x_1 + \cdots + x_k = 0$, in which $D\vec{1}$ lies. Hence the equation $A\vec{x} = D\vec{1}$ is solvable and $\vec{v}$ and $\vec{v} + \vec{1}$ are its two roots. If we replace $\vec{v}$ by $\vec{v}' = \vec{v} + \vec{1}$, then $d, \tau, \mu, i = \sqrt{-1}$ will be replaced by $d' = n/d$, τ', μ' and $i' = \sqrt{-1}$ respectively. One can check that

$$\left[\frac{\tau' + i'\mu'}{n}\right] + \left[\frac{2}{d'}\right] = \left[\frac{\tau + i\mu}{n}\right] + \left[\frac{2}{d}\right]$$

(see [5, Remark 4.7]).

EXAMPLE 1.3. In (1), let $n = 5 \times 13 \times 41$. Then

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

is of rank 2, $\vec{0}d = (1,0,0)^{\mathrm{T}}$, $d = 5$, $n/d = 533$, $2d = 3^2+1^2$, $2n/d = 29^2+15^2$, and

$$\left[\frac{3+\sqrt{-1}}{5}\right] = 0, \qquad \left[\frac{3+\sqrt{-1}}{13}\right] = 1, \qquad \left[\frac{3+\sqrt{-1}}{41}\right] = 1,$$

$$\left[\frac{29+15\sqrt{-1}}{5}\right] = 0, \quad \left[\frac{29+15\sqrt{-1}}{13}\right] = 1, \quad \left[\frac{29+15\sqrt{-1}}{41}\right] = 1.$$

Thus

$$\left[\frac{3+\sqrt{-1}}{n}\right] + \left[\frac{2}{5}\right] = \left[\frac{29+15\sqrt{-1}}{n}\right] + \left[\frac{2}{533}\right] = 1$$

and $5 \times 13 \times 41$ is non-congruent.

In (2), let $n = 7 \times 23 \times 41$. Then

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{and} \quad A + \operatorname{diag}\{1,1,0\} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

are of rank 2, $n = 6601 = 2 \times 59^2 - 19^2$, thus $7 \times 23 \times 41$ is non-congruent. Let $n = 2 \times 23 \times 31$. Then

$$A = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad A + \operatorname{diag}\{1,1\} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

are of rank 1,

$$\left(\frac{2+\sqrt{2}}{m}\right) = \left(\frac{7}{23}\right)\left(\frac{10}{31}\right) = -1,$$

thus $2 \times 23 \times 31$ is non-congruent.

THEOREM 1.4. *Let $n = (2,n)m \equiv 1,2,3 \bmod 8$ and $m = p_1 \cdots p_k$.*

(1) *Assume $p_i \equiv 3 \bmod 4$. If the equations $(A^2 + A + D)\vec{x} = \vec{0}, \vec{1}$ have together at most two solutions, then m is non-congruent. If the equations $((A+D)^2 + A)\vec{x} = \vec{0}, \vec{1}, D\vec{1}, D\vec{1} + \vec{1}$ have together at most two solutions, then $n = 2m$ is non-congruent.*

(2) *Assume $p_i \equiv \pm 3 \bmod 8$. If the equations $(A^2 + AC + C)\vec{x} = \vec{0}, \vec{1}, C\vec{1}, C\vec{1} + \vec{1}$ have together at most two solutions, then $n = m$ is non-congruent. If the equations $(A^2 + AC + I)\vec{x} = \vec{0}, \vec{1}, C\vec{1}, C\vec{1} + \vec{1}$ have together at most two solutions, then $n = 2m$ is non-congruent.*

(3) *Assume $p_i \equiv \pm 3 \bmod 8$. If the equations $(A^2 + CA + C)\vec{x} = \vec{0}, \vec{1}$ have together at most two solutions, then $n = m$ is non-congruent. If the equations $(A^2 + CA + I)\vec{x} = \vec{0}, C\vec{1}$ have together at most two solutions, then $n = 2m$ is non-congruent.*

A special case of the above theorem is the following result:

THEOREM 1.5. *Suppose* $n = (2, n)m \equiv 1, 2, 3 \bmod 8$ *and* $m = p_1 \cdots p_k$.

(1) *If* $p_i \equiv 3 \mod 4$ *and* $A^2 + A + D$ *is invertible, then* $n = m$ *is a non-congruent number.*
(2) *If* $p_i \equiv \pm 3 \mod 8$ *and* $A^2 + CA + C$ *is invertible, then* $n = m$ *is a non-congruent number.*
(3) *If* $p_i \equiv \pm 3 \mod 8$ *and* $A^2 + CA + I$ *is invertible, then* $n = 2m$ *is a non-congruent number.*

EXAMPLE 1.6. Suppose $p_i \equiv 3 \bmod 8$ in the above theorem. Then $n = m$ or $2m$ are non-congruent numbers if $A^2 + A + I$ is invertible. In particular, if $\left(\frac{p_i}{p_j}\right) = 1$ for $1 \le i < j \le k$, then A is upper triangular and $A^2 + A + I$ is invertible, thus m is a non-congruent number and so is $2m$ if k is even. The odd case was first discovered by Iskra [3].

Moreover, in this way, we can construct an infinite set T of primes congruent to 3 modulo 8 and such that the product of any finite subset of primes in T is a non-congruent number, for example,

$$T = \{3, 11, 83, 107, 347, 2939, 3539, 10667, 12539, 29147, \dots\}.$$

2. Computation of the Selmer groups

2.1. Second 2-descent method. We first recall the second 2-descent method of computing the Selmer groups of elliptic curves (cf. [4, pp. 232–233], [1, §5] and [7, X.4]).

For an isogeny $\varphi : E \to E'$ of elliptic curves defined over a number field K, the Mordell–Weil group, the Selmer group and the Shafarevich–Tate group are related by the fundamental exact sequence

$$0 \to E'(K)/\varphi E(K) \to S^{(\varphi)}(E/K) \to Ш(E/K)[\varphi] \to 0. \tag{2.1}$$

Moreover, if $\psi : E' \to E$ is another isogeny, for the composition $\psi \circ \varphi : E \to E$, we have a commutative diagram of exact sequences (cf. [8, p. 24]):

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & E'(K)/\varphi E(K) & \longrightarrow & S^{(\varphi)}(E/K) & \longrightarrow & Ш(E/K)[\varphi] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi_S} & & \downarrow & & \\
0 & \longrightarrow & E(K)/\psi\varphi E(K) & \longrightarrow & S^{(\psi\varphi)}(E/K) & \longrightarrow & Ш(E/K)[\psi\varphi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow & & \\
0 & \longrightarrow & E(K)/\psi E'(K) & \longrightarrow & S^{(\psi)}(E'/K) & \longrightarrow & Ш(E'/K)[\psi] & \longrightarrow & 0 \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array} \tag{2.2}$$

We denote by $\tilde{S}^{(\psi)}(E'/K)$ the image of res : $S^{(\psi\varphi)}(E/K) \to S^{(\psi)}(E'/K)$. If φ is of degree n and ψ is its dual isogeny, then by the above diagram, the computation of the Selmer groups S and $\tilde{S}$ provides a way to obtain the (weak) Mordell–Weil groups and Shafarevich–Tate groups of E and E'.

In what follows, we suppose $K = \mathbb{Q}$, and for $a, b \in \mathbb{Q}$, suppose

$$\begin{aligned} E = E_{a,b} : &\qquad y^2 = x^3 + ax^2 + bx, \\ E' = E_{-2a,a^2-4b} : &\qquad y^2 = x^3 - 2ax^2 + (a^2 - 4b)x. \end{aligned}$$

Then

$$\varphi = \varphi_{a,b} : E \to E', \qquad (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right),$$

is an isogeny of degree 2. Let ψ be the dual isogeny of φ. Then $\psi = \lambda \circ \varphi_{-2a,a^2-4b}$ where $\lambda : E_{4a,16b} \to E_{a,b}, (x, y) \mapsto (x/4, y/8)$, is an isomorphism.

REMARK 2.1. We shall compute the Selmer groups $S^{(\varphi)}(E/\mathbb{Q})$, $\tilde{S}^{(\varphi)}(E/\mathbb{Q})$ (for the isogeny $\varphi \circ \psi$ in the above diagram), $S^{(\psi)}(E'/\mathbb{Q})$ and $\tilde{S}^{(\psi)}(E'/\mathbb{Q})$ (for the isogeny $\psi \circ \varphi$) below. However, since $\psi = \lambda \circ \varphi_{-2a,a^2-4b}$, the computation for ψ is more or less the same as for φ, just interchanging (a, b) with $(-2a, a^2 - 4b)$.

Let S be the finite set of places $\{\infty, p \,|\, 2b(a^2 - 4b)\}$ and $\mathbb{Q}(S, 2) := \{b \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \mathrm{ord}_p(b) \equiv 0 \bmod 2 \text{ for all } p \notin S\}$. The set $\mathbb{Q}(S, 2)$ is represented by the set of squarefree factors of $2b(a^2 - 4b)$. From now on we identify these two sets.

LEMMA 2.2 ([7, X.4]). *Let C_d and C'_d be the curves*

$$C_d : \quad dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4, \qquad C'_d : \quad dw^2 = d^2 + adz^2 + bz^4.$$

Then the Selmer groups $S^{(\varphi)}(E/\mathbb{Q})$ and $S^{(\psi)}(E'/\mathbb{Q})$ can be identified as follows:

$$\begin{aligned} S^{(\varphi)}(E/\mathbb{Q}) &= \{d \in \mathbb{Q}(S, 2) : C_d(\mathbb{Q}_v) \neq \emptyset, \forall v \in S\}, \\ S^{(\psi)}(E'/\mathbb{Q}) &= \{d \in \mathbb{Q}(S, 2) : C'_d(\mathbb{Q}_v) \neq \emptyset, \forall v \in S\}. \end{aligned}$$

LEMMA 2.3. *Let $d \in S^{(\varphi)}(E_{a,b}/\mathbb{Q})$. Suppose (σ, τ, μ) is a non-zero integer solution of $d\sigma^2 = d^2\tau^2 - 2ad\tau\mu + (a^2 - 4b)\mu^2$ which is guaranteed by Hasse–Minkowski's Theorem (cf. [6]). Let $\mathcal{M}_s$ be the curve corresponding to $s \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ defined by*

$$\mathcal{M}_s : \quad \begin{cases} dw^2 = d^2t^4 - 2adt^2z^2 + (a^2 - 4b)z^4, \\ d\sigma w - (d\tau - a\mu)(dt^2 - az^2) - 4b\mu z^2 = su^2. \end{cases} \tag{2.3}$$

Then $d \in \tilde{S}^{(\varphi)}(E/\mathbb{Q})$ if and only if there exists $s \in \mathbb{Q}(S, 2)$ such that $\mathcal{M}_s$ is locally solvable everywhere.

Proof. Let

$$w = \frac{1}{\sqrt{d}}\left(x_1 - \frac{b}{x_1}\right), \quad t = \frac{y_1}{\sqrt{d}x_1}, \quad z = 1$$

where $(x_1, y_1) \in E$. Then the homogeneous space of $d \in S^{(\varphi)}(E/\mathbb{Q})$ is

$$C_d: \quad dw^2 = d^2t^4 - 2adt^2z^2 + (a^2 - 4b)z^4,$$

and we have a diagram

$$\begin{array}{ccccc} E' & \xrightarrow{\psi} & E & \xrightarrow{\varphi} & E' \\ & & \updownarrow & \nearrow & \\ & & C_d & & \end{array} \tag{2.4}$$

If $d \in \tilde{S}^{(\varphi)}(E/\mathbb{Q})$, assume ψ maps (x_2, y_2) to (x_1, y_1). Then $x_1 = y_2^2/(4x_2^2)$. Take

$$u = \sqrt{\frac{\sqrt{d}\,\sigma - (d\tau - a\mu)}{s}} \cdot \frac{x_2(2x_1\mu + \sqrt{d}\,\sigma + d\tau - a\mu)}{\mu y_2}.$$

Then after some calculations, we get (2.3). The remaining assertions follow from [1, §5, Lemma 8 and 10]. ∎

2.2. Our situation. Let $(a, b) = (0, -n^2), (3n, 2n^2)$ or $(-3n, 2n^2)$. Then $(-2a, a^2 - 4b) = (0, 4n^2)$, $(-6n, n^2)$ or $(6n, n^2)$ respectively, and we get the elliptic curves E_i and E_i' from the beginning of this paper. In our case, $S = \{\infty, \text{prime factors of } 2m\}$ and $\mathbb{Q}(S, 2)$ is identified with the factor set of $2m$. Let $C_{i,d}$ (resp. $C'_{i,d}$) be the curve C_d corresponding to E_i (resp. E_i').

We apply the diagram (2.2) to the isogenies $\psi \circ \varphi : E_i \to E_i$ and $\varphi \circ \psi : E_i' \to E_i'$ respectively. For the first one, ψ and ψ_S are both injective; for the second one,

$$\ker\left(\varphi : \frac{E(\mathbb{Q})}{\psi E'(\mathbb{Q})} \to \frac{E'(\mathbb{Q})}{2E'(\mathbb{Q})}\right) = \ker(\varphi_S : S^{(\psi)}(E'/\mathbb{Q}) \to S^{(2)}(E'/\mathbb{Q}))$$

is $\mathbb{Z}/2\mathbb{Z}$. The proposition below shows that if the images of the Selmer groups are minimal, then n is a non-congruent number.

PROPOSITION 2.4. *Let $E = E_i$ and $E' = E_i'$.*

(1) *If $\#\tilde{S}^{(\varphi)}(E/\mathbb{Q}) = 1$ and $\#\tilde{S}^{(\psi)}(E'/\mathbb{Q}) = 4$, then*

$$\operatorname{rank} E(\mathbb{Q}) = \operatorname{rank} E'(\mathbb{Q}) = 0. \tag{2.5}$$

Moreover, if $\#S^{(\varphi)}(E/\mathbb{Q}) = 1$, then

$$Ш(E/\mathbb{Q})[2^\infty] = 0, \quad Ш(E'/\mathbb{Q})[2^\infty] \cong S^{(\psi)}(E'/\mathbb{Q})/(\mathbb{Z}/2\mathbb{Z})^2; \tag{2.6}$$

if $\#S^{(\psi)}(E'/\mathbb{Q}) = 4$, then

$$Ш(E/\mathbb{Q})[2^\infty] \cong S^{(\varphi)}(E/\mathbb{Q}), \quad Ш(E'/\mathbb{Q})[2^\infty] = 0. \tag{2.7}$$

(2) *If* $\#\tilde{S}^{(\varphi)}(E/\mathbb{Q})<4$ *and* $\operatorname{rank}_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q})$ *is even, then* $\#\tilde{S}^{(\varphi)}(E/\mathbb{Q}) = 1$*; if* $\#\tilde{S}^{(\psi)}(E'/\mathbb{Q}) < 16$ *and* $\operatorname{rank}_{\mathbb{F}_2} S^{(\psi)}(E'/\mathbb{Q})$ *is even, then* $\#\tilde{S}^{(\psi)}(E'/\mathbb{Q}) = 4$.

Proof. (1) Since $E(\mathbb{Q})_{\mathrm{tor}} \cap \psi E'(\mathbb{Q}) = \{O\}$ and $\#E(\mathbb{Q})_{\mathrm{tor}} = 4$, by (2.2), we have

$$4 \le \#E(\mathbb{Q})/\psi E'(\mathbb{Q}) \le \#\tilde{S}^{(\psi)}(E'/\mathbb{Q}),$$
$$1 \le \#E'(\mathbb{Q})/\varphi E(\mathbb{Q}) \le \#\tilde{S}^{(\varphi)}(E/\mathbb{Q}).$$

Now if $\#\tilde{S}^{(\varphi)}(E/\mathbb{Q}) = 1$ and $\#\tilde{S}^{(\psi)}(E'/\mathbb{Q}) = 4$, then all inequalities above become equalities, which implies $\#E(\mathbb{Q})/2E(\mathbb{Q}) = 4$ and $\operatorname{rank} E(\mathbb{Q}) = \operatorname{rank} E'(\mathbb{Q}) = 0$.

If moreover $\#S^{(\varphi)}(E/\mathbb{Q}) = 1$, then

$$S^{(2)}(E/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2, \qquad Ш(E/\mathbb{Q})[2] = 0,$$
$$S^{(2)}(E'/\mathbb{Q}) = \frac{S^{(\psi)}(E'/\mathbb{Q})}{\mathbb{Z}/2\mathbb{Z}}, \quad Ш(E'/\mathbb{Q})[2] = \frac{S^{(\psi)}(E'/\mathbb{Q})}{(\mathbb{Z}/2\mathbb{Z})^2}.$$

Hence $Ш(E/\mathbb{Q})[2^\infty] = 0$ and $Ш(E/\mathbb{Q})[2^k\varphi] = 0$. By the exact sequence

$$0 \to Ш(E'/\mathbb{Q})[\psi] \to Ш(E'/\mathbb{Q})[2^k] \to Ш(E/\mathbb{Q})[2^{k-1}\varphi],$$

we have $Ш(E'/\mathbb{Q})[2^k] \cong Ш(E'/\mathbb{Q})[\psi]$ for every $k \in \mathbb{N}_+$, and thus

$$Ш(E'/\mathbb{Q})[2^\infty] \cong Ш(E'/\mathbb{Q})[\psi] \cong S^{(\psi)}(E'/\mathbb{Q})/(\mathbb{Z}/2\mathbb{Z})^2.$$

Ditto for $\#S^{(\psi)}(E'/\mathbb{Q}) = 4$.

(2) By the existence of Cassels' skew-symmetric bilinear form on Ш (cf. [1, p. 95] or [2]), the $\mathbb{F}_2$-ranks of $S^{(\varphi)}(E/\mathbb{Q})$ and $\tilde{S}^{(\varphi)}(E/\mathbb{Q})$ have the same parity, which implies $\tilde{S}^{(\varphi)}(E) = \{1\}$. Ditto for $S^{(\psi)}(E'/\mathbb{Q})$. ∎

Proposition 2.4 is crucial in this paper. In the following we shall give an explicit computation of the Selmer groups such that the assumptions of the proposition are satisfied in the cases corresponding to our main theorems.

2.3. The Selmer groups $S^{(\varphi)}$ and $S^{(\psi)}$. For any $d \mid 2m$, we let $d' = d/(2,d)$ be the odd part of d. We list the conditions for $C_{i,d}, C'_{i,d}$ to be locally solvable below. For the computation, one only needs to consider the valuations and use Hensel's Lemma. We omit the details (for these refer to [5, 8]).

Proposition 2.5.

(1) *The sets* $C_{1,d}(\mathbb{Q}_\infty), C_{2,d}(\mathbb{Q}_\infty)$ *and* $C'_{3,d}(\mathbb{Q}_\infty)$ *are non-empty if and only if* $d > 0$*, the sets* $C'_{1,d}(\mathbb{Q}_\infty)$*,* $C'_{2,d}(\mathbb{Q}_\infty)$ *and* $C_{3,d}(\mathbb{Q}_\infty)$ *are always non-empty.*

(2) *The conditions on d for $C_d(\mathbb{Q}_2) \neq \emptyset$ are listed as follows:*

	n	d *odd*	d *even*
$C_{1,d}$	*odd*	$d \equiv 1 \bmod 4$	$d' \equiv 1 \bmod 4$, $n \equiv \pm 1 \bmod 8$
	even	$d \equiv 1 \bmod 8$	*impossible*
$C_{2,d}$	*odd*	$n \equiv 1 \bmod 4$, $d \equiv 1 \bmod 8$ *or* $n \equiv 3 \bmod 4$, $d \equiv \pm 1 \bmod 8$	*impossible*
	even	$d \equiv 1 \bmod 8$	$m \equiv 7$, $d' \equiv 1 \bmod 8$ *or* $m \equiv 5$, $d' \equiv 7 \bmod 8$
$C_{3,d}$	*odd*	$n \equiv 3 \bmod 4$, $d \equiv 1 \bmod 8$ *or* $n \equiv 1 \bmod 4$, $d \equiv \pm 1 \bmod 8$	*impossible*
	even	$d \equiv 1 \bmod 8$	$m \equiv 1 \bmod 4$, $d' \equiv 1 \bmod 8$

The conditions on d for $C'_d(\mathbb{Q}_2) \neq \emptyset$ are listed as follows:

	n	d *odd*	d *even*
$C'_{1,d}$	*odd*	d *or* $n/d \equiv \pm 1 \bmod 8$	*impossible*
	even	*arbitrary*	*arbitrary*
$C'_{2,d}$	*odd*	d' *or* $-n/d' \equiv 1 \bmod 4$	
	even	$m \equiv 1, 3$ *or* $m \equiv 5$, $d' \equiv 1, 3$ *or* $m \equiv 7$, $d' \equiv \pm 1 \bmod 8$	
$C'_{3,d}$	*odd*	d' *or* $n/d' \equiv 1 \bmod 4$	
	even	$m \equiv 5, 7$ *or* $m \equiv 3$, $d' \equiv 1, 3$ *or* $m \equiv 1$, $d' \equiv \pm 1 \bmod 8$	

(3) *The conditions on d for $C_d(\mathbb{Q}_p) \neq \emptyset$ or $C'_d(\mathbb{Q}_p) \neq \emptyset$ for an odd prime $p \,|\, n$ are listed as follows:*

	$p \,|\, d$	$p \,|\, 2n/d$
$C_{1,d}$	$p \equiv 1 \bmod 4$, $\left(\frac{n/d}{p}\right) = 1$	$\left(\frac{d}{p}\right) = 1$
$C_{2,d}$	$p \equiv \pm 1 \bmod 8$, $\left(\frac{n/d}{p}\right) = 1$	
$C_{3,d}$	$p \equiv \pm 1 \bmod 8$, $\left(\frac{-n/d}{p}\right) = 1$	
$C'_{1,d}$	$\left(\frac{n/d}{p}\right) = 1$ *for all* $p \equiv 1 \bmod 4$	$\left(\frac{d}{p}\right) = 1$ *for all* $p \equiv 1 \bmod 4$
$C'_{2,d}$	$\left(\frac{-n/d}{p}\right) = 1$ *for all* $p \equiv \pm 1 \bmod 8$	$\left(\frac{d}{p}\right) = 1$ *for all* $p \equiv \pm 1 \bmod 8$
$C'_{3,d}$	$\left(\frac{n/d}{p}\right) = 1$ *for all* $p \equiv \pm 1 \bmod 8$	$\left(\frac{d}{p}\right) = 1$ *for all* $p \equiv \pm 1 \bmod 8$

Corollary 2.6.

(1) *Assume $n \equiv 1 \bmod 8$, $p_i \equiv 1 \bmod 4$ and $\operatorname{rank} \mathsf{A} = k - 1$. Assume $\vec{v}$ is a root of the equation $\mathsf{A}\vec{x} = \mathsf{D}\vec{1}$ and let $d = d(\vec{v})$. Then*

$$S^{(\varphi)}(E_1/\mathbb{Q}) = \{1, n, 2d, 2n/d\}, \qquad S^{(\psi)}(E'_1/\mathbb{Q}) = \{\pm 1, \pm n\}.$$

(2) *Assume* $m \equiv 1 \bmod 8$, $p_i \equiv \pm 1 \bmod 8$, *and* $\operatorname{rank} \mathsf{A} = \operatorname{rank}(\mathsf{A}+\mathsf{C}) = k-1$. *Assume* $\vec{v}$ *is the non-zero root of the equation* $(\mathsf{A}+\mathsf{C})\vec{x} = \vec{0}$ *and let* $d = d(\vec{v})$.

(i) *If* $n = m$, *then*

$$S^{(\varphi)}(E_3/\mathbb{Q}) = \{1, d, -n, -n/d\}, \qquad S^{(\psi)}(E_3'/\mathbb{Q}) = \{1, 2, n, 2n\}.$$

(ii) *If* $n = 2m$, *then*

$$S^{(\varphi)}(E_3/\mathbb{Q}) = \begin{cases} \{1, 2, d, 2d\} & \text{if } d \equiv 1 \bmod 8, \\ \{1, 2, -m/d, -n/d\} & \text{if } d \equiv -1 \bmod 8, \end{cases}$$

and $S^{(\psi)}(E_3'/\mathbb{Q}) = \{1, 2, m, n\}$.

Proof. We only show (1). The rest is similar.

Suppose $d \in S^{(\varphi)}(E_1/\mathbb{Q})$. As $C_{1,d}(\mathbb{Q}_\infty)$ and $C_{1,d}(\mathbb{Q}_2)$ are both non-empty, $0 < d \,|\, 2n$. If d is odd, then Proposition 2.5(3) implies $\mathsf{A}\vec{v}(d) = \vec{0}$. Thus $\vec{v} = \vec{0}$ or $\vec{1}$ and $d = 1, n$. If $d = 2d'$ is even, Proposition 2.5(3) implies that $\mathsf{A}\vec{v}(d') = \mathsf{D}\vec{1}$, thus $d = 2d(\vec{v})$ or $2n/d(\vec{v})$ for $\vec{v}$ a solution of $\mathsf{A}\vec{x} = \mathsf{D}\vec{1}$.

Suppose $d \in S^{(\psi)}(E_1'/\mathbb{Q})$. By Proposition 2.5(1) & (2), $d \,|\, n$ and $d \equiv \pm 1 \bmod 8$. By Proposition 2.5(3), $\mathsf{A}\vec{v}(d) = \vec{0}$. Hence $\vec{v}(d) = \vec{0}$ or $\vec{1}$ as $\operatorname{rank} \mathsf{A} = k-1$ and $d = \pm 1$ or $\pm n$. ∎

Corollary 2.7. *Suppose* $m = p_1 \cdots p_k$ *is a squarefree odd positive integer and* $n = m$ *or* $2m$ *such that* $n \equiv 1, 2$ *or* $3 \bmod 8$.

(1) *Assume* $p_i \equiv 3 \bmod 4$. *If* $n = m$ *and* $\mathsf{D} \neq \mathsf{O}$, *then* $S^{(\varphi)}(E_1/\mathbb{Q}) = \{1\}$ *and*

$$S^{(\psi)}(E_1'/\mathbb{Q}) = \begin{cases} \{d : d \,|\, n,\ d \equiv \pm 1 \bmod 8\} & \text{if } n \equiv 1 \bmod 8, \\ \langle -1, p_i \rangle & \text{if } n \equiv 3 \bmod 8. \end{cases}$$

If $n = 2m$, *then* $S^{(\varphi)}(E_1/\mathbb{Q}) = \{1\}$ *and* $S^{(\psi)}(E_1'/\mathbb{Q}) = \langle -1, 2, p_i \rangle$.

(2) *Assume* $p_i \equiv \pm 3 \bmod 8$. *If* $n = m$, *then* $S^{(\varphi)}(E_2/\mathbb{Q}) = \{1\}$ *and*

$$S^{(\psi)}(E_2'/\mathbb{Q}) = \begin{cases} \langle -1, 2, p_i \rangle & \text{if } n \equiv 1 \bmod 8, \\ \{d, 2d : d \equiv 1 \bmod 4,\ d \,|\, n\} & \text{if } n \equiv 3 \bmod 8. \end{cases}$$

If $n = 2m$, *then* $S^{(\varphi)}(E_2/\mathbb{Q}) = \{1\}$ *and*

$$S^{(\psi)}(E_2'/\mathbb{Q}) = \begin{cases} \langle -1, 2, p_i \rangle & \text{if } m \equiv 1 \bmod 8, \\ \{d, 2d : d \equiv 1, 3 \bmod 8,\ d \,|\, n\} & \text{if } m \equiv 5 \bmod 8. \end{cases}$$

(3) *Assume* $p_i \equiv \pm 3 \bmod 8$. *If* $n = m$, $m \equiv 3 \bmod 8$ *or* $\mathsf{C} \neq \mathsf{O}$, *then* $S^{(\varphi)}(E_3/\mathbb{Q}) = \{1\}$ *and*

$$S^{(\psi)}(E_3'/\mathbb{Q}) = \begin{cases} \{d, 2d : 0 < d \,|\, n,\ d \equiv 1 \bmod 4\} & \text{if } n \equiv 1 \bmod 8, \\ \langle 2, p_i \rangle & \text{if } n \equiv 3 \bmod 8. \end{cases}$$

If $n = 2m$, then $S^{(\varphi)}(E_3/\mathbb{Q}) = \{1\}$ and

$$S^{(\psi)}(E_3'/\mathbb{Q}) = \begin{cases} \langle 2, p_i\rangle & \text{if } m \equiv 5 \bmod 8, \\ \langle 2, p_1p_2, p_1p_3, \dots, p_1p_k\rangle & \text{if } m \equiv 1 \bmod 8. \end{cases}$$

In particular, in all cases, $S^{(\varphi)} = \{1\}$ and $S^{(\psi)}$ has even $\mathbb{F}_2$-rank.

Proof. We only pick one case to prove, the remaining cases being similar. In (1), if $n = m$ is odd, by Proposition 2.5, $S^{(\varphi)}(E_1/\mathbb{Q}) \subseteq \{1, 2\}$. But if $2 \in S^{(\varphi)}(E_1/\mathbb{Q})$, then $C_{1,2}(\mathbb{Q}_p) \neq \emptyset$ implies $\left(\frac{2}{p}\right) = 1$ and so $D = O$. By the same proposition, $d \in S^{(\psi)}(E_1'/\mathbb{Q})$ if and only if d is odd and d or $n/d \equiv \pm 1 \bmod 8$. If $n = 2m$ is even, then $S^{(\varphi)}(E_1/\mathbb{Q}) = \{1\}$ and $S^{(\psi)}(E_1'/\mathbb{Q}) = \langle -1, 2, p_i\rangle$ follow from Proposition 2.5 directly. ∎

2.4. The images $\tilde{S}^{(\varphi)}$ and $\tilde{S}^{(\psi)}$. We first suppose $(a, b) = (a_1n, b_1n^2)$ where $a_1, b_1 \in \mathbb{Z}$ and $b_1 \mid 2^\infty$. Let $E = E_{a,b}$ and $d \in S^{(\varphi)}(E/\mathbb{Q})$. We want to find a necessary condition for $d \in \tilde{S}^{(\varphi)}(E/\mathbb{Q})$.

By abuse of notation, write $d = \tau^2 - b_1\mu^2$ and select the triple (σ, τ, μ) in Lemma 2.3 to be $\big(d, \tau + \frac{1}{2}a_1\mu, \frac{d\mu}{2n}\big)$. Then the defining equations in (2.3) can be written as

$$\mathcal{M}_s: \quad \begin{cases} w^2 = d\big((t^2 - a_1(nz^2/d))^2 - 4b_1(nz^2/d)^2\big), \\ w - \tau(t^2 - a_1(nz^2/d)) - 2b_1\mu(nz^2/d) = su^2. \end{cases} \tag{2.8}$$

Proposition 2.8. *Suppose $d \in S^{(\varphi)}(E/\mathbb{Q})$ and $p \mid m$ is an odd prime number. If $p \mid d$, then $\sqrt{b_1} \in \mathbb{Q}_p$. The curve $\mathcal{M}_s$ is locally solvable:*

(1) *at $p \mid d$ if and only if for $\sqrt{b_1} \in \mathbb{Q}_p$ is chosen such that $p \mid \tau - \sqrt{b_1}\,\mu$, either*

$$p \mid s, \quad \left(\frac{n/d}{p}\right) = \left(\frac{a_1 - 2\sqrt{b_1}}{p}\right), \quad \left(\frac{n/s}{p}\right) = \left(\frac{\mu}{p}\right),$$

or

$$p \nmid s, \quad \left(\frac{n/d}{p}\right) = \left(\frac{a_1 + 2\sqrt{b_1}}{p}\right), \quad \left(\frac{s}{p}\right) = \left(\frac{-\mu}{p}\right)\left(\frac{n/d}{p}\right);$$

(2) *at $p \mid \frac{2m}{d}$ if and only if either*

$$p \mid s, \quad \left(\frac{d}{p}\right) = \left(\frac{a_1^2 - 4b_1}{p}\right),$$
$$\left(\frac{n/s}{p}\right) = \left(\frac{d}{p}\right)\left(\frac{\pm\sqrt{d(a_1^2 - 4b_1)} + a_1\tau - 2b_1\mu}{p}\right),$$

or

$$p \nmid s, \quad \left(\frac{d}{p}\right) = 1, \quad \left(\frac{s}{p}\right) = \left(\frac{\pm\sqrt{d} - \tau}{p}\right).$$

Here $\pm$ means one of them.

Proof. The proof and calculation are similar to [5, §3.2]. We use the notation $x = O(y)$ if the p-adic valuations satisfy $v(x) \geq v(y)$.

THE CASE $p \,|\, d$. We may assume $z = 1$, $v(t) = 0$, $v(w) > 0$. It is easy to see $t^2 \equiv (a_1 \pm 2\sqrt{b_1})\frac{n}{d} \pmod{p}$.

(i) If $v(su^2) \geq 3$, then by combining the two expressions of w^2, we obtain

$$\left(\mu\left(t^2 - \frac{a_1 n}{d}\right) + \frac{2n\tau}{d}\right)^2 = O(su^2).$$

Then

$$t^2 \equiv \frac{(a_1\mu - 2\tau)n}{d\mu} \equiv (a_1 - 2\sqrt{b_1})\frac{n}{d} \pmod{p} \quad \text{and} \quad \left(\frac{n/d}{p}\right) = \left(\frac{a_1 - 2\sqrt{b_1}}{p}\right).$$

Set $\beta = t^2 - \frac{(a_1\mu - 2\tau)n}{d\mu}$. Then

$$w^2 = d\left(\frac{4\tau^2 n^2}{\mu^2 d^2} - \frac{4n\tau\beta}{d\mu} + \beta^2 - 4b_1\left(\frac{n}{d}\right)^2\right) = \frac{4n^2}{\mu^2}\left(1 - \frac{\tau\mu\beta}{n} + \frac{d\mu^2\beta^2}{4n^2}\right).$$

Take the square root on both sides to get

$$w = \pm\left(\frac{2n}{\mu} - \tau\beta - b_1 n\mu\left(\frac{\mu\beta}{2n}\right)^2 + O(\beta^3/p^2)\right).$$

On the other hand, $w = -\frac{2n}{\mu} + \tau\beta + su^2$. Hence the sign must be negative and $su^2 = b_1 n\mu\left(\frac{\mu\beta}{2n}\right)^2 + O(\beta^3/p^2)$, thus $p \,|\, s$, $\left(\frac{n/s}{p}\right) = \left(\frac{\mu}{p}\right)$.

(ii) If $v(bu^2) \leq 2$ and $t^2 \equiv \frac{(a_1 - 2\sqrt{b_1})n}{d} \pmod{p}$, then $\left(\frac{n/d}{p}\right) = \left(\frac{a_1 - 2\sqrt{b_1}}{p}\right)$. Let

$$t^2 = \frac{(a_1 - 2\sqrt{b_1})n}{d} - \frac{p^2\alpha}{n\sqrt{b_1}},$$

then one can see

$$w^2 = 4p^2\alpha\left(1 + \frac{p^2 d\alpha}{4n^2 b_1}\right),$$

$$w = \pm 2p\sqrt{\alpha}\left(1 + \frac{p^2 d\alpha}{8n^2 b_1} + O(p^2)\right),$$

and

$$su^2 = \frac{p^2\tau}{n\sqrt{b_1}}\left(\sqrt{\alpha} \pm \frac{n\sqrt{b_1}}{p\tau}\right)^2 + \frac{n\sqrt{b_1}}{d\tau}(\tau - \sqrt{b_1}\,\mu)^2 \pm \frac{p^3 d}{4n^2 b_1}\alpha^{3/2} + O(p^3).$$

If $v(su^2) = 2$, then $\sqrt{\alpha} \equiv \mp\frac{n\sqrt{b_1}}{p\tau} \pmod{p}$, and

$$su^2 = \frac{n\sqrt{b_1}}{4d\tau^3}(\tau - \sqrt{b_1}\,\mu)^3(3\tau + \sqrt{b_1}\,\mu) + O(p^3) = O(p^3),$$

a contradiction. Thus $v(su^2) = 1$ and $p \,|\, s$, $\left(\frac{n/s}{p}\right) = \left(\frac{\tau\sqrt{b_1}}{p}\right) = \left(\frac{\mu}{p}\right)$.

(iii) If $v(su^2) \le 2$ and $t^2 \equiv \frac{(a_1+2\sqrt{b_1})n}{d} \pmod p$, then $\left(\frac{n/d}{p}\right) = \left(\frac{a_1+2\sqrt{b_1}}{p}\right)$ and

$$su^2 = -2\sqrt{b_1}\,\tau n/d - 2b_1\mu n/d + O(p) = -4b_1 n\mu/d + O(p),$$

thus $p \nmid s$, $\left(\frac{s}{p}\right) = \left(\frac{-\mu}{p}\right)\left(\frac{n/d}{p}\right)$.

The case $p \mid \frac{2m}{d}$.

(i) If $v(z) \ge v(t) = v(w)/2$, we may assume $t = 1$, $v(w) = 0$, $v(z) \ge 0$. Then $\left(\frac{d}{p}\right) = 1$ and

$$\begin{aligned} w &= \pm\sqrt{d}\,(1 - a_1(nz^2/d) - 2b_1(nz^2/d)^2 + \cdots) \\ &= \tau - (a_1\tau + 2b_1\mu)\frac{nz^2}{d} + su^2. \end{aligned}$$

Notice that $(\sqrt{d}-\tau)(-\sqrt{d}-\tau) = b_1\mu^2$ and $\pm\sqrt{d}-\tau$ are coprime. Choose suitable $\sqrt{d}$ or τ such that $\sqrt{d}-\tau \ne 0$. Then $v(\sqrt{d}-\tau)$ is even and $\left(\frac{\sqrt{d}-\tau}{p}\right)$ is well defined.

We may assume that $p \nmid (\sqrt{d}+\tau)$. If $w \equiv -\sqrt{d} \bmod p$ or $p \nmid \mu$, then $su^2 = -\sqrt{d} - \tau + O(p)$. Otherwise $w \equiv \sqrt{d} \bmod p$ and $v(\mu) \ge 1$, and so

$$b_1\left(\mu\left(1 - \frac{a_1 nz^2}{d}\right) + 2\tau\frac{nz^2}{d}\right)^2 = -su^2(2\tau + O(p)),$$

thus $p \nmid s$ and $\left(\frac{s}{p}\right) = \left(\frac{-2\tau}{p}\right) = \left(\frac{\pm\sqrt{d}-\tau}{p}\right)$.

(ii) If $v(z) < v(t)$, we may assume $z = 1$, $w = pw_1$, $t = pt_1$; then

$$w_1^2 = (a_1^2 - 4b_1)d\left(\frac{n}{pd}\right)^2 + O(p),$$

thus $\left(\frac{d}{p}\right) = \left(\frac{a_1^2-4b_1}{p}\right)$ and

$$\begin{aligned} w_1 &= \pm\sqrt{(a_1^2-4b_1)d}\left(\frac{n}{pd}\right) + O(p), \\ su^2 &= \frac{n}{d}(a_1\tau - 2b_1\mu \pm \sqrt{(a_1^2-4b_1)d} + O(p)). \end{aligned}$$

Notice that

$$(a_1\tau - 2b_1\mu + \sqrt{(a_1^2-4b_1)d})(a_1\tau - 2b_1\mu - \sqrt{(a_1^2-4b_1)d}) = b_1(a_1\mu - 2\tau)^2.$$

Thus

$$p \mid s, \quad \left(\frac{n/s}{p}\right) = \left(\frac{d}{p}\right)\left(\frac{a_1\tau - 2b_1\mu \pm \sqrt{(a_1^2-4b_1)d}}{p}\right). \ \blacksquare$$

To compute $\tilde{S}^{(\varphi_i)}(E_i/\mathbb{Q})$, we are in the cases $(a_1, b_1) = (0, -1)$, $(3, 2)$ and $(-3, 2)$ respectively.

COROLLARY 2.9. *Suppose* $d \in S^{(\varphi_i)}(E_i/\mathbb{Q})$. *Write* $d = \tau^2 - b_1\mu^2$, *and assume*

$$\left(\frac{b_1}{p}\right) = 1 \quad \textit{and} \quad \left(\frac{-a_1 + 2\sqrt{b_1}}{p}\right) = \left(\frac{-a_1 - 2\sqrt{b_1}}{p}\right) = 1 \quad \textit{for all } p \,|\, m.$$

Choose $\sqrt{b_1} \in \mathbb{Z}/m\mathbb{Z}$ *such that* $p \,|\, \tau - \sqrt{b_1}\,\mu$ *for all* $p \,|\, d'$. *Then* $\mathcal{M}_s$ *is locally solvable:*

(1) *at* $p \,|\, d'$ *only if either*

$$p \,|\, s, \quad \left(\frac{n/d}{p}\right) = \left(\frac{-1}{p}\right), \quad \left(\frac{n/s}{p}\right) = \left(\frac{-2(\tau + \sqrt{b_1}\,\mu)}{p}\right)\left(\frac{-\sqrt{b_1}}{p}\right),$$

or

$$p \nmid s, \quad \left(\frac{n/d}{p}\right) = \left(\frac{-1}{p}\right), \quad \left(\frac{s}{p}\right) = \left(\frac{-2(\tau + \sqrt{b_1}\,\mu)}{p}\right)\left(\frac{-\sqrt{b_1}}{p}\right);$$

(2) *at* $p \,|\, \frac{m}{d'}$ *only if either*

$$p \,|\, s, \quad \left(\frac{d}{p}\right) = 1, \quad \left(\frac{n/s}{p}\right) = \left(\frac{-2(\tau + \sqrt{b_1}\,\mu)}{p}\right),$$

or

$$p \nmid s, \quad \left(\frac{d}{p}\right) = 1, \quad \left(\frac{s}{p}\right) = \left(\frac{-2(\tau + \sqrt{b_1}\,\mu)}{p}\right).$$

In particular, if $E_i = E_1$ *or* E_3 *for* n *as in Theorem* 1.1(1) *or* (3) *respectively, then*

$$\left[\frac{-\sqrt{b_1}}{d'}\right] + \left[\frac{-2(\tau + \sqrt{b_1}\,\mu)}{m}\right] = 1 \quad \textit{implies} \quad d \notin \tilde{S}^{(\varphi)}(E_i/\mathbb{Q}).$$

Proof. For $p \,|\, d$, we have

$$\left(\frac{\mu}{p}\right) = \left(\frac{4b_1\mu}{p}\right) = \left(\frac{-\sqrt{b_1}}{p}\right)\left(\frac{-2(\tau + \sqrt{b_1}\,\mu)}{p}\right).$$

For $p \,|\, \frac{n}{d}$, if $p \,|\, s$, then

$$\begin{aligned} &-2(\sqrt{d} - \tau)(\tau + \sqrt{b_1}\,\mu) = (\tau + \sqrt{b_1}\,\mu - \sqrt{d})^2, \\ &\left(\frac{n/s}{p}\right) = \left(\frac{-2(\tau + \sqrt{b_1}\,\mu)}{p}\right). \end{aligned} \tag{2.9}$$

If $p \nmid s$, notice that

$$(a_1^2 - 4b_1)d = (-a_1\tau + 2b_1\mu)^2 - b_1(2\tau - a_1\mu)^2,$$
$$\left(\frac{s}{p}\right) = \left(\frac{-2(-a_1\tau + 2b_1\mu + \sqrt{b_1}\,(2\tau - a_1\mu))}{p}\right) = \left(\frac{-2(\tau + \sqrt{b_1}\,\mu)}{p}\right).$$

Then the local solvability follows from Proposition 2.8.

If $E_i = E_1$, $(a_1, b_1) = (0, -1)$, then for any $p \mid d$, $p \equiv 1 \bmod 4$, $\left(\frac{2\sqrt{-1}}{p}\right) = 1$; if $E_i = E_3$, $(a_1, b_1) = (-3, 2)$, then for any $p \mid d$, $p \equiv \pm 1 \bmod 8$, $\left(\frac{3 \pm 2\sqrt{2}}{p}\right) = 1$. If $d \in \tilde{S}^{(\varphi_i)}(E_i/\mathbb{Q})$, then there exists $s \in \mathbb{Q}(S, 2)$ satisfying the above conditions. Write $\varepsilon = s/d(\vec{v}(s)) = \pm 1, \pm 2$. Then

$$\text{the } i\text{th entry of } \mathsf{A}\vec{v}(s) = \begin{cases} \left[\frac{-2(\tau+\sqrt{b_1}\,\mu)}{p}\right] + \left[\frac{-\sqrt{b_1}}{p}\right] + \left[\frac{\varepsilon}{p}\right] & \text{if } p_i \mid d, \\ \left[\frac{-2(\tau+\sqrt{b_1}\,\mu)}{p}\right] + \left[\frac{\varepsilon}{p}\right] & \text{if } p_i \mid \frac{m}{d}. \end{cases}$$

But the image space of A is a subspace of $x_1 + \cdots + x_k = 0$ and notice that $m \equiv 1 \bmod 8$, $\sum \left[\frac{\varepsilon}{p}\right] = \left[\frac{\varepsilon}{m}\right] = 0$; thus

$$\left[\frac{-\sqrt{b_1}}{d'}\right] + \left[\frac{-2(\tau + \sqrt{b_1}\,\mu)}{m}\right] = 0. \ \blacksquare$$

To compute $\tilde{S}^{(\psi_i)}(E_i'/\mathbb{Q})$, we are in the cases $(a_1, b_1) = (0, 4)$, $(-6, 1)$ and $(6, 1)$ respectively. In these cases b_1 is a square number. We will fix the pair (τ, μ).

COROLLARY 2.10. *Suppose $d \in S^{(\psi_i)}(E_i'/\mathbb{Q})$ and $p \mid m$ is an odd prime number.*

(1) *If $i = 1$, then $\mathcal{M}_s$ for $(\tau, \mu) = (\frac{d+1}{2}, \frac{d-1}{4})$ is locally solvable:*

(i) *at $p \mid d$ if and only if either*

$$p \mid s, \quad \left(\frac{n/d}{p}\right) = 1, \quad \left(\frac{n/s}{p}\right) = \left(\frac{-1}{p}\right),$$

or

$$p \nmid s, \quad \left(\frac{n/d}{p}\right) = \left(\frac{-1}{p}\right), \quad \left(\frac{s}{p}\right) = \left(\frac{-1}{p}\right);$$

(ii) *at $p \mid \frac{n}{d}$ if and only if either*

$$p \mid s, \quad \left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right), \quad \left(\frac{n/s}{p}\right) = \left(\frac{-2}{p}\right),$$

or

$$p \nmid s, \quad \left(\frac{d}{p}\right) = 1, \quad \left(\frac{s}{p}\right) = \left(\frac{-2}{p}\right).$$

(2) *If $i = 2$, then $\mathcal{M}_s$ for $(\tau, \mu) = \left(\frac{d+1}{2}, \frac{d-1}{2}\right)$ is locally solvable:*

(i) *at $p \mid d$ if and only if either*

$$p \mid s, \quad \left(\frac{n/d}{p}\right) = \left(\frac{-1}{p}\right), \quad \left(\frac{n/s}{p}\right) = \left(\frac{-2}{p}\right),$$

or

$$p \nmid s, \quad \left(\frac{n/d}{p}\right) = \left(\frac{-2}{p}\right), \quad \left(\frac{s}{p}\right) = \left(\frac{-1}{p}\right);$$

(ii) *at* $p \mid \frac{n}{d}$ *if and only if either*

$$p \mid s, \quad \left(\frac{d}{p}\right) = \left(\frac{2}{p}\right), \quad \left(\frac{n/s}{p}\right) = \left(\frac{-1}{p}\right),$$

or

$$p \nmid s, \quad \left(\frac{d}{p}\right) = 1, \quad \left(\frac{s}{p}\right) = \left(\frac{-2}{p}\right).$$

(3) *If* $i = 3$, *then* $\mathcal{M}_s$ *for* $(\tau, \mu) = (\frac{d+1}{2}, \frac{d-1}{2})$ *is locally solvable:*

(i) *at* $p \mid d$ *if and only if either*

$$p \mid s, \quad \left(\frac{n/d}{p}\right) = \left(\frac{2}{p}\right), \quad \left(\frac{n/s}{p}\right) = \left(\frac{-2}{p}\right),$$

or

$$p \nmid s, \quad \left(\frac{n/d}{p}\right) = 1, \quad \left(\frac{s}{p}\right) = \left(\frac{2}{p}\right);$$

(ii) *at* $p \mid \frac{n}{d}$ *if and only if either*

$$p \mid s, \quad \left(\frac{d}{p}\right) = \left(\frac{2}{p}\right), \quad \left(\frac{n/s}{p}\right) = \left(\frac{2}{p}\right),$$

or

$$p \nmid s, \quad \left(\frac{d}{p}\right) = 1, \quad \left(\frac{s}{p}\right) = \left(\frac{-2}{p}\right).$$

Proof. This follows from Proposition 2.8 easily, one only needs to use the fact that $-2d(\pm\sqrt{d} - \tau) = (d \mp \sqrt{d})^2$. ∎

3. Proof of the main theorems

Proof of Theorem 1.1. (1) One can find a detailed argument in [5]. Under the assumption, by Corollary 2.6(1),

$$S^{(\varphi)}(E_1/\mathbb{Q}) = \{1, n, 2d, 2n/d\}, \quad S^{(\psi)}(E_1'/\mathbb{Q}) = \{\pm 1, \pm n\}$$

where $d = d(\vec{v})$ for $A\vec{v} = D\vec{1}$. Write $2d = \tau^2 + \mu^2$ and choose $\sqrt{-1}$ in $\mathbb{Z}/n\mathbb{Z}$ such that $p \mid \tau - \sqrt{-1}\mu$ for all $p \mid d$. By Corollary 2.9, if $\left[\frac{\tau+\sqrt{-1}\,\mu}{n}\right] + \left[\frac{2}{d}\right] = 1$, then $2d \notin \tilde{S}^{(\varphi)}(E_1/\mathbb{Q})$. By Proposition 2.4, $\tilde{S}^{(\varphi)}(E_1/\mathbb{Q}) = \{1\}$ and n is non-congruent.

(2) For $n = m$ odd, by Corollary 2.6(2),

$$S^{(\varphi)}(E_3/\mathbb{Q}) = \{1, d, -n, -n/d\}, \quad S^{(\psi)}(E_3'/\mathbb{Q}) = \{1, 2, n, 2n\}$$

where $d = d(\vec{v})$ for $\vec{v} \neq 0$ and $(A + C)\vec{v} = \vec{0}$. Write $-n = \tau^2 - 2\mu^2$, choose $\sqrt{2}$ such that $p \mid \tau - \sqrt{2}\,\mu$ for all $p \mid n$. Then $\left[\frac{-\sqrt{2}}{n}\right] + \left[\frac{-2(\tau+\sqrt{2}\,\mu)}{n}\right] = \left[\frac{\mu}{n}\right] = \left[\frac{n}{\mu'}\right] = \left[\frac{-1}{\mu'}\right]$ where μ' is the positive odd part of μ. By Corollary 2.9, $\mu' \equiv 3 \bmod 4$ implies $-n \notin \tilde{S}^{(\varphi)}(E_3/\mathbb{Q})$. By Proposition 2.4, $\tilde{S}^{(\varphi)}(E_3/\mathbb{Q}) = \{1\}$ and n is non-congruent.

For $n = 2m$ even, by Corollary 2.6(2),

$$S^{(\varphi)}(E_3/\mathbb{Q}) = \begin{cases} \{1,2,d,2d\} & \text{if } d \equiv 1 \bmod 8, \\ \{1,2,-m/d,-n/d\} & \text{if } d \equiv -1 \bmod 8 \end{cases}$$

and $S^{(\psi)}(E_3'/\mathbb{Q}) = \{1,2,m,n\}$ where $d = d(\vec{v})$ for $\vec{v} \neq 0$ and $(A+C)\vec{v} = \vec{0}$. Write $2 = 2^2 - 2 \times 1^2$, $\tau = 2$, $\mu = 1$, $\left[\frac{-2(2+\sqrt{2})}{m}\right] = \left[\frac{2+\sqrt{2}}{m}\right]$. By Corollary 2.9, $\left(\frac{2+\sqrt{2}}{m}\right) = -1$ implies $2 \notin \tilde{S}^{(\varphi)}(E_3/\mathbb{Q})$. By Proposition 2.4, $\tilde{S}^{(\varphi)}(E_3/\mathbb{Q}) = \{1\}$ and n is non-congruent. ∎

Proof of Theorem 1.4. (1) For $n = m$ odd, if $(A^2 + A + D)\vec{x} = \vec{0}, \vec{1}$ has together at most two solutions, then $D \neq O$. Indeed, if $D = O$, then $p_i \equiv 7 \bmod 8$ and k is even. If $\operatorname{rank} A < k-1$, then $A\vec{x} = \vec{0}$ and $(A^2+A)\vec{x} = \vec{0}$ have together more than four solutions. If $\operatorname{rank} A = k-1$, let $\vec{v}$ be a solution of $A\vec{x} = \vec{1}$; then $\vec{0}$, $\vec{1}$, $\vec{v}$ and $\vec{v} + \vec{1}$ all satisfy $(A^2 + A)\vec{x} = \vec{0}$ or $\vec{1}$. Hence we can apply Corollary 2.7(1).

Suppose $d \in \tilde{S}^{(\psi)}(E_1'/\mathbb{Q})$. If $d > 0$, let $\vec{v} = \vec{v}(d)$. Then

$$\text{the } i\text{th entry of } A\vec{v} = \begin{cases} \left[\frac{d}{p_i}\right] & \text{if } p_i \nmid d, \\ \left[\frac{n/d}{p_i}\right] & \text{if } p_i \mid d. \end{cases}$$

Suppose $s \in \mathbb{Q}(S,2)$ is such that $\mathcal{M}_s$ is locally solvable everywhere. Let $\vec{s} = \vec{v}(s)$ and $s_0 = d(\vec{s})$. Then $2 \nmid s_0 > 0$ and $s = \pm s_0, \pm 2s_0$. If $s = s_0$, then by Corollary 2.10(1):

- if $p \mid d$, $\left[\dfrac{n/d}{p}\right] = 0$, then $p \mid s$, $\left[\dfrac{n/s}{p}\right] = 1$;
- if $p \mid d$, $\left[\dfrac{n/d}{p}\right] = 1$, then $p \nmid s$, $\left[\dfrac{s}{p}\right] = 1$;
- if $p \nmid d$, $\left[\dfrac{d}{p}\right] = 1$, then $p \mid s$, $\left[\dfrac{n/s}{p}\right] = 1 + \left[\dfrac{2}{p}\right]$;
- if $p \nmid d$, $\left[\dfrac{d}{p}\right] = 0$, then $p \nmid s$, $\left[\dfrac{s}{p}\right] = 1 + \left[\dfrac{2}{p}\right]$.

So $\vec{s} = (A+I)\vec{v}$ and $A\vec{s} = \vec{1} + D(\vec{1} + \vec{v})$. Thus $(A^2 + A + D)\vec{v} = \vec{1} + D\vec{1}$. Similarly, for $s = -s_0, 2s_0, -2s_0$, we have $(A^2 + A + D)\vec{v} = D\vec{1}, \vec{1}, \vec{0}$ respectively. If $d < 0$, then $\vec{s} = (A+I)\vec{v} + \vec{1}$; but $A\vec{1} = \vec{0}$, so we still have $(A^2 + A + D)\vec{v} = \vec{0}, \vec{1}, D\vec{1}, D\vec{1} + \vec{1}$ respectively for $s = s_0, -s_0, 2s_0, -2s_0$. Hence $\pm d, \pm n/d \in \tilde{S}^{(\psi)}(E_1'/\mathbb{Q})$ only if

$$(A^2 + A + D)\vec{v} = \vec{0}, \vec{1}.$$

If the equations have together at most two solutions, then there are together at most eight elements in $\tilde{S}^{(\psi)}(E_1'/\mathbb{Q})$. By Proposition 2.4 and Corollary 2.7, $\#\tilde{S}^{(\psi)}(E_1'/\mathbb{Q}) = 4$ and n is a non-congruent number.

For $n = 2m$ even, similarly for odd $d = d_0 = d(\vec{v})$, if $s = s_0$, then $\vec{s} = (A + D + I)\vec{v}$ and $A\vec{s} = \vec{1} + D(\vec{v} + \vec{s} + \vec{1})$. Thus $((A + D)^2 + A)\vec{v} = \vec{1} + D\vec{1}$; if $s = -s_0, 2s_0, -2s_0$, then $((A+D)^2 + A)\vec{v} = D\vec{1}, \vec{1}, \vec{0}$. For $d = -d_0$, $((A+D)^2+A)\vec{v} = \vec{0}, \vec{1}, D\vec{1}, D\vec{1}+\vec{1}$ if $s = \pm s_0, \pm 2s_0$ respectively; for $d = \pm 2d_0$, $((A + D)^2 + A)(\vec{v} + \vec{1}) = \vec{0}, \vec{1}, D\vec{1}, D\vec{1} + \vec{1}$ respectively. Hence $\pm d, \pm 2n/d \in \tilde{S}^{(\psi)}(E_1'/\mathbb{Q})$ only if

$$((A + D)^2 + A)\vec{v} = \vec{0}, \vec{1}, D\vec{1}, D\vec{1} + \vec{1}.$$

If the equations have together at most two solutions, then there are together at most eight elements in $\tilde{S}^{(\psi)}(E'/\mathbb{Q})$. By Proposition 2.4 and Corollary 2.7, $\#\tilde{S}^{(\psi)}(E_1'/\mathbb{Q}) = 4$ and n is a non-congruent number.

The proofs of (2) and (3) are similar to that of (1). We suppose $2 \nmid d > 0$ and $\vec{v} = \vec{v}(d)$ in the following.

(2) If $n = m$, then $d, 2d, -n/d, -2n/d \in \tilde{S}^{(\psi)}(E_2'/\mathbb{Q})$ only if

$$(A^2 + AC + C)\vec{v} = \vec{0}, \vec{1}, C\vec{1}, C\vec{1} + \vec{1}.$$

If the equations have together at most two solutions, then $\#\tilde{S}^{(\psi)}(E_2'/\mathbb{Q}) \le 8$ and n is a non-congruent number.

If $n = 2m$, then $d, 2d, -m/d, -n/d \in \tilde{S}^{(\psi)}(E_2'/\mathbb{Q})$ only if

$$(A^2 + AC + I)\vec{v} = \vec{0}, \vec{1}, C\vec{1}, C\vec{1} + \vec{1}.$$

If the equations have together at most two solutions, then $\#\tilde{S}^{(\varphi)}(E_2/\mathbb{Q}) \le 8$ and n is a non-congruent number.

(3) For $n = m$, if the equations $(A^2 + CA + C)\vec{x} = \vec{0}, \vec{1}$ have together at most two solutions, then $C \ne O$ or $n \equiv 3 \bmod 8$. Indeed, if $C = O$ and $n \equiv 1 \bmod 8$, then $p_i \equiv 5 \bmod 8$ and k is even. Similar to the proof of $D \ne O$ in (1), one can show $A^2\vec{x} = 0$ has at least four solutions.

Thus $d, 2d, n/d, 2n/d \in \tilde{S}^{(\psi)}(E_3'/\mathbb{Q})$ only if

$$(A^2 + CA + C)\vec{v} = \vec{0}, \vec{1}.$$

If the equations have together at most two solutions, then $\#\tilde{S}^{(\psi)}(E_3'/\mathbb{Q}) \le 8$ and n is a non-congruent number.

For $n = 2m$ even, $d, 2d, m/d, n/d \in \tilde{S}^{(\psi)}(E_3'/\mathbb{Q})$ only if

$$(A^2 + CA + I)\vec{v} = \vec{0}, C\vec{1}.$$

If the equations have together at most two solutions, then $\#\tilde{S}^{(\psi)}(E_3'/\mathbb{Q}) \le 8$ and n is a non-congruent number. ∎

Acknowledgements. This research was partially supported by National Key Basic Research Program of China (grant no. 2013CB834202) and National Natural Science Foundation of China (grant no. 11171317). The authors would like to thank AMSS and MCM of Chinese Academy of Sciences, and Purdue University for hospitality during the preparation of this paper.

References

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

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

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

[4] D. Li and Y. Tian, *On the Birch–Swinnerton–Dyer conjecture of elliptic curves* E_D : $y^2 = x^3 - D^2x$, Acta Math. Sinica (English Ser.) 16 (2000), 229–236.

[5] Y. Ouyang and S. X. Zhang, *On non-congruent numbers with 1 modulo 4 prime factors*, Sci. China Math. 57 (2014), 649–658.

[6] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, New York, 1973.

[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

[8] M. Xiong and A. Zaharescu, *Selmer groups and Tate–Shafarevich groups for the congruent number problem*, Comment. Math. Helv. 84 (2009), 21–56.

Yi Ouyang, Shenxing Zhang
Wu Wen-Tsun Key Laboratory of Mathematics
School of Mathematical Sciences
University of Science and Technology of China
Hefei, Anhui 230026, China
E-mail: yiouyang@ustc.edu.cn
zsxqq@mail.ustc.edu.cn

Received on 19.9.2014
and in revised form on 11.3.2015 and 26.7.2015 (7935)