ACTA ARITHMETICA
LXXV.1 (1996)

Non-congruent numbers, odd graphs and the Birch–Swinnerton-Dyer conjecture

by

KEQIN FENG (Hefei)

1. Introduction. The aim of this paper is twofold. One is to present more non-congruent numbers n with arbitrarily many prime factors. Another is to verify the (even part of) the Birch–Swinnerton-Dyer conjecture on the elliptic curve

$$E_n: \quad y^2 = x^3 - n^2 x$$

for several series of integer n.

Congruent numbers. A positive integer n is called a *congruent number* (CN) if n is the area of a rational right triangle. Otherwise n is called a *non-congruent number* (non-CN). It is well known that n is non-CN iff the rank of the rational point group $E_n(\mathbb{Q})$ is zero (see Koblitz [4], for instance). From now on we assume without loss of generality that n is square-free. The congruent number problem is very old and was discussed by Arab scholars in the tenth century. By the author's (incomplete) knowledge, the following CN and non-CN have been determined (p, q and r denote distinct prime numbers, p_i means a prime number congruent to i modulo 8).

For CN:

- $n = 2p_3$ (Heegner (1952), Birch (1968)),
- $n = p_5, p_7$ (Stephens, 1975),
- $n = p^u q^v \equiv 5, 6, 7 \pmod 8,\ 0 \le u, v \le 1$ (B. Gross, 1985),

$$\left.\begin{array}{l} \bullet\ n = 2p_3p_5, 2p_5p_7 \\ \bullet\ n = 2p_1p_7,\ \left(\frac{p_1}{p_7}\right) = -1 \\ \bullet\ n = 2p_1p_3,\ \left(\frac{p_1}{p_3}\right) = -1 \end{array}\right\} \text{(Monsky, 1990)},$$

where $\left(\frac{p}{q}\right)$ is the Legendre symbol.

Supported by the National Natural Science Foundation of China and the National Education Committee of China.

For non-CN:

$$\begin{aligned}
&\bullet\ n = p_3, p_3q_3, 2p_5, 2p_5q_5 \ \text{(Genocchi, 1855)},\\
&\left.\begin{aligned}
&\bullet\ n = p_1,\ p_1 = a^2+4b^2,\ \left(\tfrac{a+2b}{p_1}\right) = -1\\
&\bullet\ n = 2p,\ p \equiv 9 \pmod{16}
\end{aligned}\right\}\ \text{(Bastien, 1913)}.
\end{aligned}$$

Lagrange [5] (1974) presented many non-CN n with at most three odd prime factors by using the 2-descent method to prove $\operatorname{rank} E_n(\mathbb{Q}) = 0$. Some of them are:

- $n = p_1p_3$, $\left(\frac{p_1}{p_3}\right) = -1$,
- $n = 2p_1p_5$, $\left(\frac{p_1}{p_5}\right) = -1$,
- $n = p_1p_3q_1$, with the condition $(*)$ (see below),
- $n = 2p_1p_5q_1$, with the condition $(*)$.

Condition $(*)$. n can be written as $n = pqr$ or $2pqr$ such that $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = -1$.

A well-known conjecture made by Alter, Curtz and Kubota [1] says that n is CN if $n \equiv 5, 6, 7 \pmod 8$. Several particular cases of this conjecture has been verified (see the above-mentioned n). Moreover, the whole ACK conjecture can be derived from the BSD conjecture on the elliptic curve E_n.

Birch and Swinnerton-Dyer conjecture. Let $L_{E_n}(s)$ be the L-function of the elliptic curve E_n. The BSD conjecture says that:

(BSD1) $\operatorname{rank} E_n(\mathbb{Q}) = \operatorname{ord}_{s=1} L_{E_n}(s)$.

(BSD2) If $L_{E_n}(1) \neq 0$, then

$$L_{E_n}(1)/A = |Ш(E_n)|, \tag{1.1}$$

where $Ш(E_n)$ is the Tate–Shafarevich group of E_n, and A is a certain nonzero number which we do not want to describe exactly. K. Rubin ([8], [9]) proved that if $L_{E_n}(1) \neq 0$, then the group $Ш(E_n)$ is finite and the odd parts of both sides of (1.1) are equal.

It is well known that $L_{E_n}(1) = 0$ for $n \equiv 5, 6, 7 \pmod 8$. Therefore the Alter–Curtz–Kubota conjecture can be derived from the BSD conjecture (BSD1). A remarkable step was made by Tunnell [12] in 1983 who presented an elementary formula for $L_{E_n}(1)/A$ by using modular forms with weight 3/2. For n odd, let

$$a(n) = \frac{1}{2} \sum_{\substack{x^2+y^2+2z^2=n\\ 2\mid y}} \zeta(x+iy) \qquad (i = \sqrt{-1}), \tag{1.2}$$

where ζ is the character of $(\mathbb{Z}[i]/(4(1+i)))^\times$ such that

$$\zeta(\alpha) = \begin{cases} 1 & \text{for } \alpha = 1, 7, 3+2i, 1+2i, \\ -1 & \text{for } \alpha = 3, 5, 7+2i, 5+2i. \end{cases}$$

For $2 \parallel n$, let

$$b(n/2) = \frac{1}{2} \sum_{\substack{x^2+2y^2+z^2=n/2 \\ 2|z}} \zeta'(x+\sqrt{-2}\,y), \tag{1.3}$$

where ζ' is the character of $(\mathbb{Z}[\sqrt{-2}]/(4))^\times$ such that

$$\zeta'(\alpha) = \zeta'(-\alpha), \quad \zeta'(1) = 1, \quad \zeta'(1+2\sqrt{-2}) = \zeta'(3+2\sqrt{-2}) = -1.$$

Let $w(n)$ be the number of distinct prime factors of n. For the left-hand side of (1.1), Tunnell [12] proved that

$$L_{E_n}(1)/A = \begin{cases} (a(n)/2^{w(n)})^2 & \text{if } 2 \nmid n, \\ (b(n/2)/2^{w(n/2)})^2 & \text{if } 2 \parallel n. \end{cases} \tag{1.4}$$

We are now ready to explain the title and philosophy of this paper. The sums (1.2) and (1.3) extend over the solutions of $x^2+y^2+2z^2 = n$ (or $n/2$) with $2 \mid y$. We have a one-to-one correspondence between the solutions of $x^2+y^2+2z^2 = n$ and $X^2+Y^2+Z^2 = 2n$ (with $2 \mid Z$) as follows:

$$(X, Y, Z) = (x+y, x-y, 2z), \qquad (x, y, z) = \left(\tfrac{X+Y}{2}, \tfrac{X-Y}{2}, \tfrac{Z}{2}\right). \tag{1.5}$$

A well-known Gauss result says that the number of solutions of $X^2+Y^2+Z^2 = 2n$ (with $2 \mid Z$) is $4h(-2n)$, where $h(-2n)$ is the class number of $\mathbb{Q}(\sqrt{-2n})$. Since Rubin proved that the odd parts of both sides of (1.1) are equal provided $a(n) \neq 0$ or $b(n/2) \neq 0$, we need to determine the Sylow 2-subgroup $C_K^{(2)}$ of the class group C_K for $K = \mathbb{Q}(\sqrt{-2n})$. Gauss' genus theory says that

$$2\text{-rank}\, C_K = w(2n) - 1 = w(n).$$

For each n we can define a graph $G(n)$. Rédei and Reichardt ([6], [7]) essentially proved that $2^{w(n)} \parallel h(-2n)$ iff $G(n)$ is an odd graph (for the definition of $G(n)$ and odd graph see Section 2). It turns out that for a series of n we can show by the 2-descent method that $\operatorname{rank} E_n(\mathbb{Q}) = 0$ and the order of $Ш(E_n)$ is odd provided the graph $G(n)$ is odd (see Section 3). Therefore we present a series of non-congruent numbers n with arbitrarily many prime factors. By using the above-mentioned Rédei–Reichardt result we can show that $a(n)/2^{w(n)}$ or $b(n/2)/2^{w(n/2)}$ is an odd integer so that the BSD conjectures (BSD1) and (BSD2) are true for such n (see Section 4). This is the relation between non-congruent numbers, odd graphs, the 2-parts of the class numbers of imaginary quadratic fields and the BSD conjecture on E_n.

2. Odd graphs and the 2-class number of $\mathbb{Q}(\sqrt{-2n})$. We use standard terminology of graph theory. Let $G = (V, E)$ be a (simple) directed graph, $V = \{v_1, \ldots, v_m\}$ the vertices of G, and E ($\subseteq V \times V$) the arcs of G. The *adjacency matrix* of G is defined by $A(G) = (a_{ij})_{1\le i,j\le m}$, where

$$a_{ij} = \begin{cases} 1 & \text{if } i \ne j \text{ and } \overrightarrow{v_iv_j} \in E, \\ 0 & \text{otherwise.} \end{cases}$$

Let $d_i = \sum_{j=1}^m a_{ij}$ be the outdegree of the vertex v_i ($1 \le i \le m$), and $M(G) = \operatorname{diag}(d_1, \ldots, d_m) - A(G)$. Then the sum of each row of $M(G)$ is zero, so that $\det M(G) = 0$. Let $M_{ij} = M_{ij}(G)$ be the (i, j) co-factor of $M(G)$; we have $M_{ij} = (-1)^{j+k} M_{ik}$. If the matrix $A(G)$, and so $M(G)$, is symmetric, we view G as a non-directed graph and the "two-direction arc" $\overline{v_iv_j}$ as an edge. For a non-directed graph G, we have

$$M_{11} = (-1)^{i+k} M_{ik} \quad (1 \le i, k \le m)$$

and it is well known that the absolute value of M_{11} is the number of spanning trees of G.

DEFINITION 2.1. Let $G = (V, E)$ be a directed graph. A partition $V = V_1 \cup V_2$ is called *odd* if either there exists $v_1 \in V_1$ such that $\#\{v_1 \to V_2\}$ (the number of arcs from v_1 to vertices of V_2) is odd, or there exists $v_2 \in V_2$ such that $\#\{v_2 \to V_1\}$ is odd. Otherwise the partition is called *even*. G is called *odd* if each non-trivial partition of V is odd.

Let $r = \operatorname{rank}_{\mathbb{F}_2} M(G)$ be the rank of the matrix $M(G)$ over $\mathbb{F}_2$. Then $r \le \operatorname{rank}_{\mathbb{Q}} M(G) \le m - 1$. We have the following nice criterion for oddness of G.

LEMMA 2.2. *Let $G = G(V, E)$ be a directed graph with m vertices, $r = \operatorname{rank}_{\mathbb{F}_2} M(G)$. Then the number of even partitions of V is 2^{m-r-1}. In particular, G is an odd graph iff $r = m - 1$. For G non-directed, G is odd iff the number $t(G)$ of spanning trees of G is odd.*

Proof. Consider the following homogeneous linear equations over $\mathbb{F}_2$:

$$M(G)\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{2.1}$$

Each vector $(c_1, \ldots, c_m)$ over $\mathbb{F}_2$ corresponds to a partition of $V = \{v_1, \ldots, v_m\}$ by

$$V_1 = \{v_i : \ c_i = 0\}, \qquad V_2 = \{v_i : \ c_i = 1\}.$$

The vectors $(c_1, \ldots, c_m)$ and $(c_1 + 1, \ldots, c_m + 1)$ correspond to the same partition of V up to interchanging V_1 and V_2. A vector $(c_1, \ldots, c_m)$ is a solution of (2.1) iff $\sum_{j=1}^{m} a_{ij}c_j + d_ic_i = 0$ $(1 \le i \le m)$. But in $\mathbb{F}_2$ we have

$$\begin{aligned}\sum_{j=1}^{m} a_{ij}c_j + d_ic_i &= \sum_{j=1}^{m} a_{ij}(c_j + c_i)\\ &= \begin{cases} \sum_{j=1}^{m} a_{ij}c_j = \sum_{j=1, c_j=1}^{m} a_{ij} & \text{if } c_i = 0,\\ \sum_{j=1}^{m} a_{ij}(c_j+1) = \sum_{j=1, c_j=0}^{m} a_{ij} & \text{if } c_i = 1,\end{cases}\\ &= \begin{cases} \#\{v_i \to V_2\} & \text{if } v_i \in V_1,\\ \#\{v_i \to V_1\} & \text{if } v_i \in V_2.\end{cases}\end{aligned}$$

Therefore $(x_1, \ldots, x_m) = (c_1, \ldots, c_m)$ is a solution of (2.1) over $\mathbb{F}_2$ iff the partition $V = V_1 \cup V_2$ is even. So the number of even partitions of V is half of the number of solutions of (2.1) over $\mathbb{F}_2$, which is $\frac{1}{2} \cdot 2^{m-r} = 2^{m-r-1}$. For G non-directed, we know that $r = m-1$ iff $t(G) = M_{11} = 1 \in \mathbb{F}_2$. This completes the proof. ■

Many odd non-directed graphs can be found easily from Lemma 2.2.

Corollary 2.3. (1) *The following non-directed graphs are odd*:

- *a tree* T;
- *a cycle* C_n *with an odd number* n *of vertices*;
- *a perfect graph* K_n *with an odd number* n *of vertices* (*for each pair of distinct vertices* v_i *and* v_j *there exists an edge* $\overline{v_iv_j}$ *in* K_n).

(2) *Suppose that* G_1 *and* G_2 *are non-directed graphs. Let* G *be a "glue" of* G_1 *and* G_2 *as shown in Fig.* 1.

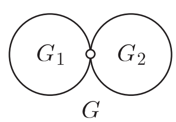

Fig. 1

Then G *is odd iff both* G_1 *and* G_2 *are odd.*

(3) *Every odd non-directed graph is connected.*

Proof. (1) follows from $t(T) = 1$, $t(C_n) = n$ and $t(K_n) = n^{n-2}$ by Cayley. (2) comes from $t(G) = t(G_1)t(G_2)$. (3) For a disconnected non-directed graph G, $t(G) = 0$. ■

The concept of odd graph has been used to determine the solvability of the Pell equation $x^2 - dy^2 = -1$ (see [2], for instance). For our purpose, we now describe a relation between an odd graph and the Sylow 2-subgroup C_K^2 of the class group C_K of an imaginary quadratic field K.

Let $K = \mathbb{Q}(\sqrt{-D})$ $(D \ge 2)$ be an imaginary quadratic field, $-D = \mathrm{disc}(K)$ the discriminant of K, $h_K = |C_K|$ the class number of K, $r_2 = \dim_{\mathbb{F}_2} C_K/C_K^2$ the 2-rank of C_K. Gauss' genus theory says that $r_2 = t-1$ so that $2^{t-1} \mid h_K$, where $t = w(D)$ is the number of distinct prime factors of D. Now we define the directed graph $G(D)$ in the following way. The vertices of $G(D)$ are all prime factors of D. For distinct vertices p_i and p_j, there is an arc $\overrightarrow{p_i p_j}$ in $G(D)$ iff $\left(\frac{p_j}{p_i}\right) = -1$, where $\left(\frac{p}{q}\right)$ is the Legendre symbol but we assume that $\left(\frac{n}{2}\right) = 1$ for each odd integer n.

THEOREM 2.4. *Let* $K = \mathbb{Q}(\sqrt{-D})$ $(D \geq 2)$ *be an imaginary quadratic field*, $-D = \operatorname{disc}(K)$, *and* t *the number of distinct prime factors of* D. *Then*

(1) $2^{t-1} \parallel h_K \;\Leftrightarrow$ *the directed graph* $G(D)$ *is odd.*

(2) *If* $D = 8p_2 \ldots p_t$ $(t \geq 2)$, $p_2 \equiv \pm 3 \pmod 8$ *and* $p_i \equiv 1 \pmod 8$ *for* $i \geq 3$, *then* $2^{t-1} \parallel h_K$ *iff* $G(D/8)$ *is odd.*

Proof. (1) Let $p_1, \ldots, p_t$ be the distinct prime factors of D. For each subset S of $\{1, \ldots, t\}$ with $1 \leq |S| \leq t-1$, let $Q_S = \prod_{i \in S} p_i$ and Q'_S be the square-free part of D/Q_S. We denote by α_S the ambiguous ideal in O_K with $N(\alpha_S) = Q_S$. Then genus theory says that the set

$$\{[\alpha_S] = [\alpha_{\overline{S}}] : \; S \subset \{1, \ldots, t\}, \; 1 \leq |S| \leq t-1\}$$

consists of $2^{r_2} - 1 = \frac{1}{2}(2^t - 2)$ ideal classes in C_K with order 2, where $[\alpha]$ denotes the class of the ideal α, and $\overline{S} = \{1, \ldots, t\} - S$. Rédei and Reichardt ([6], [7]) proved that $[\alpha_S] \in C_K^2$ iff the equation

$$u^2 Q_S + v^2 Q'_S - w^2 = 0$$

has a non-trivial $\mathbb{Q}$-solution $(u, v, w) \neq (0, 0, 0)$. By Legendre, the last statement is equivalent to the existence of $X, Y \in \mathbb{Z}$ such that

$$X^2 \equiv Q_S \pmod{Q'_S} \quad \text{and} \quad Y^2 \equiv Q'_S \pmod{Q_S}.$$

Therefore

$$\begin{aligned} 2^{t-1} \parallel h_K &\Leftrightarrow [\alpha_S] \notin C_K^2 \text{ for each } S \subset \{1, \ldots, t\} \text{ with } 1 \leq |S| \leq t-1, \\ &\Leftrightarrow \text{for each } S \subset \{1, \ldots, t\} \text{ with } 1 \leq |S| \leq t-1, \text{ either there} \\ &\qquad \text{exists a prime number } p \mid Q'_S \text{ such that } \left(\tfrac{Q_S}{p}\right) = -1, \text{ or there} \\ &\qquad \text{exists a prime number } q \mid Q_S \text{ such that } \left(\tfrac{Q'_S}{q}\right) = -1, \\ &\Leftrightarrow G(D) \text{ is an odd graph.} \end{aligned}$$

(2) In this case $G(D/8)$ is a non-directed graph by the quadratic reciprocity law and $G(D)$ is as in Fig. 2 since $\left(\frac{2}{p_2}\right) = -1$ and $\left(\frac{2}{p_i}\right) = 1$ for $i \geq 3$.

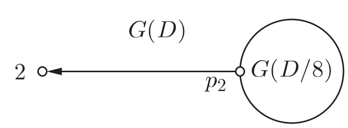

Fig. 2

It is easy to see that $G(D)$ is odd iff $G(D/8)$ is odd. This completes the proof of Theorem 2.4. ∎

3. 2-descent method. The aim of this section is to show more integers n with arbitrarily many prime factors to be non-congruent numbers and $2 \nmid \#(Ш(E_n))$ for these n by the 2-descent method. First, we describe the 2-descent method briefly. (For details see the last chapter of Silverman's book [11].)

Let $a, b \in \mathbb{Z}$ and $E : y^2 = x^3 + ax^2 + bx$ be an elliptic curve over $\mathbb{Q}$. The 2-dual curve of E is $E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X$. We have the 2-isogeny

$$\phi : E \to E', \qquad \phi(x, y) = (y^2/x^2, y(b - x^2)/x^2).$$

The kernel of ϕ is $E[\phi] = \{0, (0, 0)\}$, where 0 denotes the infinite point of E as the identity of the $\mathbb{Q}$-point group $E(\mathbb{Q})$. Let $\widehat{\phi} : E' \to E$ be the dual of ϕ so that $\phi\widehat{\phi} = [2]$ and $\widehat{\phi}\phi = [2]$. We have the following exact sequences:

$$0 \to \frac{E'(\mathbb{Q})[\widehat{\phi}]}{\phi(E(\mathbb{Q})[2])} \to \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \xrightarrow{\hat{\phi}} \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to \frac{E(\mathbb{Q})}{\widehat{\phi}(E'(\mathbb{Q}))} \to 0, \tag{3.1}$$

$$0 \to \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \to S^{(\phi)}(E) \xrightarrow{f} Ш(E)[\phi] \to 0, \tag{3.2}$$

$$0 \to \frac{E(\mathbb{Q})}{\widehat{\phi}(E'(\mathbb{Q}))} \to S^{(\hat{\phi})}(E') \xrightarrow{\hat{f}} Ш(E')[\widehat{\phi}] \to 0, \tag{3.3}$$

$$0 \to Ш(E)[\phi] \to Ш(E)[2] \xrightarrow{\phi} Ш(E')[\widehat{\phi}] \to 0, \tag{3.4}$$

where $S^{(\phi)}(E)$ is the ϕ-Selmer group of $E/\mathbb{Q}$ which is a finite subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ and can be calculated in the following way. Let

$$S = \{\infty\} \cup \{\text{prime factors of } 2b(a^2 - 4b)\}.$$

Let M be the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ generated by -1 and all prime factors of $2b(a^2 - 4b)$. For each $d \in M$, we have the curves (homogeneous spaces of $E/\mathbb{Q}$ and $E'/\mathbb{Q}$)

$$\begin{aligned} c_d : &\quad dw^2 = d^2t^4 - 2adt^2z^2 + (a^2 - 4b)z^4, \\ c'_d : &\quad dw^2 = d^2t^4 + adt^2z^2 + bz^4. \end{aligned}$$

Then we have the following isomorphisms of groups

$$\begin{aligned} S^{(\phi)}(E) &\cong \{d \in M : c_d(Q_v) \neq \emptyset \text{ for each } v \in S\}, \\ S^{(\hat{\phi})}(E) &\cong \{d \in M : c'_d(Q_v) \neq \emptyset \text{ for each } v \in S\}, \end{aligned}$$

where $c_d(Q_v) \neq \emptyset$ means that the curve c_d has a non-trivial solution $(w, t, y) \neq (0, 0, 0)$ in Q_v. With these isomorphisms, the kernels of f and $\widehat{f}$ in the exact sequences (3.2) and (3.3) are

$$\ker f = \{d \in M : c_d(Q) \neq \emptyset\}, \qquad \ker \widehat{f} = \{d \in M : c'_d(Q) \neq \emptyset\}. \tag{3.5}$$

For our case, the elliptic curve E_n and its dual E'_n have the equations

$$E_n: \quad y^2 = x^3 - n^2 x, \qquad E'_n: \quad Y^2 = X^3 + 4n^2 X$$

and

$$S = \{\infty\} \cup \{\text{prime factors of } 2n\}.$$

Moreover, M is the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ generated by -1 and the prime factors of $2n$. For each $d \in M$, the homogeneous spaces are

$$c_d: \quad dw^2 = d^2t^4 + 4n^2z^4, \qquad c'_d: \quad dw^2 = d^2t^4 - n^2z^4.$$

From (3.5) we know that

$$1 \in \ker f, \qquad \pm 1, \pm n \in \ker \widehat{f}. \tag{3.6}$$

Since $E_n(\mathbb{Q})[2] = \{0, (y,x) = (0,0), (0, \pm n)\}$ and $E'_n(\mathbb{Q})[\widehat{\phi}] = \phi(E_n(\mathbb{Q})[2]) = \{0, (0,0)\}$, the exact sequences (3.1)–(3.3) imply that

$$\begin{aligned} 2 + \operatorname{rank} E_n(\mathbb{Q}) &= \dim_{\mathbb{F}_2} \ker f + \dim_{\mathbb{F}_2} \ker \widehat{f} \\ &= \dim_{\mathbb{F}_2} S^{(\phi)}(E_n) - \dim_{\mathbb{F}_2} Ш(E_n)[\phi] \\ &\quad + \dim_{\mathbb{F}_2} S^{(\hat{\phi})}(E'_n) - \dim_{\mathbb{F}_2} Ш(E'_n)[\widehat{\phi}], \end{aligned} \tag{3.7}$$

which together with (3.6) implies that

$$\operatorname{rank} E_n(\mathbb{Q}) = 0 \iff \ker f = \{1\} \text{ and } \ker \widehat{f} = \{\pm 1, \pm n\}.$$

In particular, if $S^{(\phi)}(E_n) = \{1\}$ and $S^{(\hat{\phi})}(E'_n) = \{\pm 1, \pm n\}$, then we have $\operatorname{rank} E_n(\mathbb{Q}) = 0$ and $Ш(E_n)[\phi] = Ш(E'_n)[\widehat{\phi}] = \{1\}$. Then (3.4) implies $Ш(E_n)[2] = \{1\}$, which means that the order of the group $Ш(E_n)$ is odd.

Theorem 3.1. *We have $S^{(\phi)}(E_n) = \{1\}$ and $S^{(\hat{\phi})}(E'_n) = \{\pm 1, \pm n\}$ in the following two cases ($p_1, \ldots, p_t$ are distinct odd prime numbers).*

(I) $n = p_1 p_2 \ldots p_t$ $(t \geq 1)$, $p_1 \equiv 3 \pmod 8$, $p_i \equiv 1 \pmod 8$ *for* $i \geq 2$, *and $G(n)$ is an odd graph.*

(II) $n = 2p_1 p_2 \ldots p_t$ $(t \geq 1)$, $p_1 \equiv 5 \pmod 8$, $p_i \equiv 1 \pmod 8$ *for* $i \geq 2$, *and $G(n/2)$ is an odd graph.*

Therefore $\operatorname{rank} E_n(\mathbb{Q}) = 0$ *so that n is a non-congruent number, and the order of the Tate–Shafarevich group $Ш(E_n)$ is odd.*

Proof. (I) Note that the graph $G(n)$ is non-directed by the quadratic reciprocity law, and $G(n)$ odd implies that $G(2n)$ is odd. Moreover,

$$\begin{gathered} M = \langle -1, 2, p_1, \ldots, p_t \rangle \subseteq \mathbb{Q}^\times/\mathbb{Q}^{\times 2}, \qquad S = \{\infty, 2, p_1, \ldots, p_t\}, \\ c_d: \quad dw^2 = d^2t^4 + 4n^2z^4, \qquad c'_d: \quad dw^2 = d^2t^4 - n^2z^4. \end{gathered}$$

We need to show that:

(Ia) For each $d \in M$, $d \neq 1$, there exists $v \in S$ such that $c_d(Q_v) = \emptyset$.

(Ib) For each $d \in M$, $d \neq \pm 1, \pm n$, there exists $v \in S$ such that $c'_d(Q_v) = \emptyset$.

To prove (Ia), let $V = \{2, p_1, \ldots, p_t\}$. It is easy to see that $c_d(Q_\infty) = \emptyset$ for $d<0$. So we just need to consider the cases $d = \prod_{p \in V_1} p$ for each $V_1 \subseteq V$, $V_1 \neq \emptyset$. Suppose that $V_1 \neq V$. Then V_1 and $V_2 = V - V_1$ is a non-trivial partition of V. Since $G(2n)$ is an odd graph, we know that either there exists $q \in V_1$ such that $\left(\frac{2n/d}{q}\right) = -1$, or there exists $p \in V_2$ such that $\left(\frac{d}{p}\right) = -1$.

Now we prove $c_d(Q_p) = c_d(Q_q) = \emptyset$. Suppose that $(w,t,z) \neq (0,0,0)$ is a non-trivial solution of the curve c_d in Q_p. Let $w = dw'$. Then c_d has the form $dw'^2 = t^4 + (2n/d)^2 z^4$. For each $l \in \mathbb{Z}$, $(w'p^{2l}, tp^l, zp^l)$ is also a solution of the curve c_d in Q_p. So we can assume $w', t, z \in \mathbb{Z}_p$ and $v_p(w') = v_p(t) = 0$, where v_p is the exponential valuation of Q_p normalized by $v_p(p) = 1$. Since $p \nmid d$ and $p \mid \frac{2n}{d}$, we know that $dw'^2 \equiv t^4 \pmod p$, which contradicts $\left(\frac{d}{p}\right) = -1$. Therefore $c_d(Q_p) = \emptyset$.

On the other hand, $q \neq 2$ since we assume $\left(\frac{m}{2}\right) = 1$ for each odd m. If $q = p_1 \equiv 3 \pmod 4$, the equation of c_d implies that $t^4 \equiv -(2n/d)^2 z^4 \pmod q$ since $q \mid d$ and $q \nmid \frac{2n}{d}$. This contradicts $\left(\frac{-1}{q}\right) = -1$. If $q = p_i \equiv 1 \pmod 8$ $(i \geq 2)$, then

$$\left(\frac{-1}{p}\right)_4 = 1 \quad \text{and} \quad \left(\frac{2n/d}{q}\right) = \left(\frac{-(2n/d)^2}{q}\right)_4 = 1,$$

which contradicts the assumption $\left(\frac{2n/d}{q}\right) = -1$. Therefore $c_d(Q_q) = \emptyset$.

Next we consider the case $V_1 = V$ so that $d = 2n$. The curve c_{2n} is $2nw'^2 = t^4 + z^4$. By reduction $\bmod\, p_1$ we know that $c_{2n}(Q_{p_1}) = \emptyset$. This completes the proof of (Ia) so we have $S^{(\phi)}(E_n) = \{1\}$.

To prove (Ib) let $V = \{p_1, \ldots, p_t\}$. Since $\pm 1, \pm n \in S^{(\hat{\phi})}(E'_n)$, $S^{(\hat{\phi})}(E'_n)$ is a group, and $c'_2(Q_2) = \emptyset$, we need to show that $d \notin S^{(\hat{\phi})}(E'_n)$ for each $1 < d < n$, $d \mid n$. We have $d = \prod_{p \in V_1} p$ where V_1 is a subset of V such that $1 \leq |V_1| < t$. Since $G(n)$ is an odd graph, we know that either there exists $q \mid d$ such that $\left(\frac{n/d}{q}\right) = -1$ or there exists $p \mid n/d$ such that $\left(\frac{d}{p}\right) = -1$. Since $G(n)$ is a non-directed odd graph, there exist at least 2 prime factors of n having the above properties of p or q. Therefore we can assume $p \neq p_1$.

Suppose that $c'_d : dw^2 = d^2t^4 - n^2z^4$ has a solution $(w,t,z) \neq (0,0,0)$ in Q_p; we can assume that $\min\{v_p(w), v_p(t), v_p(z)\} = 0$. If $v_p(w) \geq 1$, then $v_p(t) \geq 1$. Let $w = \frac{n}{d}w'$ and $t = \frac{n}{d}t'$. Then c'_d has the equation $dw'^2 = n^2t'^4 - d^2z^4$. Therefore $\left(\frac{\pm d}{p}\right) = 1$, which contradicts $\left(\frac{d}{p}\right) = -1$, so we have $c'_d(Q_p) = \emptyset$. In the same way we can show that $c'_d(Q_q) = \emptyset$. This completes the proof of $S^{(\hat{\phi})}(E'_n) = \{\pm 1, \pm n\}$.

(II) It is easy to see that $c_d(Q_2) = c'_d(Q_2) = \emptyset$ for each $d \mid n, 2 \mid d, d > 0$. Therefore $d \notin S^{(\phi)}(E_n)$ and $d \notin S^{(\hat{\phi})}(E'_n)$ for such d. Since $G(n/2)$ is a non-directed odd graph, we can show $d \notin S^{(\phi)}(E_n)$ for each $d \mid n/2$, $1 < d \le n/2$, and $d \notin S^{(\hat{\phi})}(E'_n)$ for each $d \mid n/2$, $1 < d < n/2$, by the same argument as in the proof of (I). Therefore $S^{(\phi)}(E_n) = \{1\}$ and $S^{(\hat{\phi})}(E'_n) = \{\pm 1, \pm n\}$. This completes the proof of Theorem 3.1. ∎

Remark 3.2. From the quadratic reciprocity law and Dirichlet's theorem on prime numbers in arithmetic progressions it is easy to show that for each directed graph G there exist inifinitely many D such that $G(D) = G$. Therefore Theorem 2.4 yields many non-congruent numbers with any given number of prime factors. For the case of $t \le 3$, Theorem 3.1 was proved by Genocchi and Lagrange (see the list in Section 1).

4. BSD conjecture on $E_n : y^2 = x^3 - n^2 x$. For natural numbers a_1, $a_2, \ldots, a_n$, we denote by $N(n; a_1, a_2, \ldots, a_n)$ the number of integral solutions of the equation $n = a_1 x_1^2 + a_2 x_2^2 + \ldots + a_n x_n^2$.

THEOREM 4.1. (1) *Suppose that n satisfies the condition* (I) *of Theorem* 3.1. *Then the conjectures* (BSD1) *and* (BSD2) *are true for E_n iff* $N(n; 1, 64, 2) \equiv 0 \pmod{2^{t+1}}$.

(2) *Suppose that n satisfies the condition* (II) *of Theorem* 3.1. *Then* (BSD1) *and* (BSD2) *are true for E_n iff* $N(n/2; 1, 32, 4) \equiv 0 \pmod{2^{t+1}}$.

Proof. (1) By Tunnell's result stated in Section 1, we know that

$$L_{E_n}(1)/A = (a(n)/2^t)^2,$$

where $a(n)$ is given by (1.2). Since $n \equiv 3 \pmod 8$, it is easy to see that

$$\begin{aligned} a(n) &= \frac{1}{2} \sum_{x^2+16y^2+2z^2=n} \zeta(x+4y) = \frac{1}{2} \sum_{x^2+16y^2+2z^2=n} (-1)^{((x+4d)^2-1)/8} \\ &= \frac{1}{2} \sum_{x^2+16y^2+2z^2=n} (-1)^{(x^2-1)/8+y} \\ &= \frac{1}{2}\Big(\sum_{\substack{x^2+16y^2+2z^2=n \\ 2\mid y}} (-1)^{(x^2-1)/8} - \sum_{\substack{x^2+16y^2+2z^2=n \\ 2\nmid y}} (-1)^{(x^2-1)/8} \Big) \\ &= \sum_{x^2+64y^2+2z^2=n} (-1)^{(x^2-1)/8} - \frac{1}{2} \sum_{x^2+16y^2+2z^2=n} (-1)^{(x^2-1)/8}. \end{aligned}$$

For $n \equiv 3 \pmod{16}$, we have $3 \equiv n \equiv x^2 + 2z^2 \equiv x^2 + 2 \pmod{16}$. Therefore $x^2 \equiv 1 \pmod{16}$, and $(x^2 - 1)/8 \equiv 0 \pmod 2$. For $n \equiv 11 \pmod{16}$, we have $11 \equiv x^2 + 2 \pmod{16}$. Therefore $x^2 \equiv 9 \pmod{16}$ and

$(x^2-1)/8 \equiv 1 \pmod 2$. Thus we know that

$$a(n) = \pm\big(N(n;1,64,2) - \tfrac{1}{2}N(n;1,16,2)\big).$$

Since $n \equiv 3 \pmod 8$ we have

$$\begin{aligned} N(n;1,16,2) &= \#\{(x,y,z)\in\mathbb{Z}^3 :\ x^2+y^2+2z^2=n,\ 2\,|\,y\} \\ &= 2h(-2n) \quad \text{(see Section 1)} \\ &\equiv 2^{t+1} \pmod{2^{t+2}} \quad \text{(Theorem 2.4)}. \end{aligned}$$

Theorem 3.1 says that $\operatorname{rank} E_n(\mathbb{Q}) = 0$ and $2 \nmid \#(Ш(E_n))$. Therefore

(BSD1) and (BSD2) are true for E_n

$$\begin{aligned} &\Leftrightarrow\ a(n)/2^t \equiv 1 \pmod 2 \\ &\Leftrightarrow\ 2N(n;1,64,2) - N(n;1,16,2) \equiv 2^{t+1} \pmod{2^{t+2}} \\ &\Leftrightarrow\ N(n;1,64,2) \equiv 0 \pmod{2^{t+1}}. \end{aligned}$$

(2) In this case we have

$$L_{E_n}(1)/A = (b(n/2)/2^t)^2,$$

where $b(n/2)$ is given by (1.3). The congruence $n/2 \equiv 5 \pmod 8$ implies that

$$\begin{aligned} b(n/2) &= \frac{1}{2}\sum_{x^2+8y^2+4z^2=n/2} \zeta'(x+2\sqrt{-2}\,y) \\ &= \frac{1}{2}\Big(N(n/2;1,32,4) - \sum_{\substack{x^2+8y^2+4z^2=n/2 \\ 2\nmid y}} 1\Big) \\ &= N(n/2;1,32,4) - \frac{1}{2}N(n/2;1,8,4). \end{aligned}$$

But $n/2 \equiv 5 \pmod 8$ implies that

$$\begin{aligned} N(n/2;1,8,4) &= \#\{(x,y,z)\in\mathbb{Z}^3 :\ x^2+2y^2+z^2=n,\ 2\,|\,z\} \\ &= 2h(-n) \equiv 2^{t+1} \pmod{2^{t+2}} \quad \text{(by Theorem 2.4)}. \end{aligned}$$

Therefore

(BSD1) and (BSD2) are true for E_n

$$\begin{aligned} &\Leftrightarrow\ b(n/2)/2^t \equiv 1 \pmod 2 \\ &\Leftrightarrow\ N(n/2;1,32,4) - \tfrac{1}{2}N(n/2;1,8,4) \equiv 2^t \pmod{2^{t+1}} \\ &\Leftrightarrow\ N(n/2;1,32,4) \equiv 0 \pmod{2^{t+1}}. \end{aligned}$$

This completes the proof of Theorem 4.1. ■

R e m a r k 4.2. If n satisfies the condition (I) of Theorem 3.1, then $N(n;1,64) = 0$ since n has a prime factor $p_1 \equiv 3 \pmod 8$ and $N(n;1,2) =$

2^{t+1} by considering the decomposition of $p_1, \dots, p_t$ in $\mathbb{Z}[\sqrt{-2}]$. Therefore $N(n;1,64,2) \equiv \#\{(x,y,z) \in \mathbb{Z}^3 : x^2+64y^2+2z^2 = n, xyz \neq 0\} \pmod{2^{t+1}}$. In particular, $N(n;1,64,2) \equiv 0 \pmod 8$ and (BSD1) and (BSD2) are true for such E_n provided $t = 1$ and 2. Similarly, if n satisfies the condition (II) of Theorem 3.1, then $N(n;1,32,4) \equiv \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 32y^2 + 4z^2 = n, xyz \neq 0\} \pmod{2^{t+1}}$ and (BSD1) and (BSD2) are true for such E_n provided $t = 1, 2$.

For $t \geq 3$, we do not know in general how to prove the congruences $N(n;1,64,2) \equiv 0 \pmod{2^{t+1}}$ for n satisfying the condition (I) of Theorem 3.1, and $N(n/2;1,32,4) \equiv 0 \pmod{2^{t+1}}$ for n satisfying the condition (II) of Theorem 3.1.

The following formula is found in [3]:

$$N(n;1,1,16,32) = \sum_{d_1 d_2 = n} \left(\frac{2}{d_1}\right) d_2 + 8 \sum_{\substack{n=x^2+4y^2 \\ x,y \geq 1}} \left(\frac{2}{x}\right)\left(\frac{-1}{y}\right) y \quad \text{for } n \equiv 5 \pmod 8.$$

For n satisfying the condition (II) of Theorem 3.1 and $t = 3$, the above formula gives that $N(n/2;1,1,16,32) \equiv 16 \pmod{32}$. Therefore

$$\begin{aligned} 0 &\equiv \#\{(x,y,z,w) \in \mathbb{Z}^4 : \ x^2 + y^2 + 16z^2 + 32w^2 = n/2\} \pmod{32} \\ &= N(n/2;1,1,16,32) - N(n/2;1,1,16) - N(n/2;1,1,32) + N(n/2;1,1) \\ &\equiv 16 - \tfrac{1}{3}N(n/2;1,1,1) - 2N(n/2;1,4,32) + 16 \pmod{32} \\ &\equiv -4h(-n) - 2N(n/2;1,4,32) \pmod{32} \\ &\equiv -2N(n/2;1,4,32) \pmod{32}. \end{aligned}$$

This shows that $N(n/2;1,4,32) \equiv 0 \pmod{2^4}$ and (BSD1) and (BSD2) are true for n satisfying the condition (II) of Theorem 3.1 and $t = 3$.

Acknowledgements. The author thanks the referee for several corrections and the reference [10] where P. Serf finds several classes of noncongruent numbers with 4–6 odd prime factors.

References

[1] R. Alter, T. B. Curtz and K. K. Kubota, *Remarks and results on congruent numbers*, in: Proc. 3rd South Eastern Conf. Combin., Graph Theory and Comput., 1972, Florida Atlantic Univ., Boca Raton, Fla., 1972, 27–35.

[2] J. E. Cremona and R. W. Odoni, *Some density results for negative Pell equations; an application of graph theory*, J. London Math. Soc. 39 (1989), 16–28.

[3] G. P. Gogišvili, *The number of representations of numbers by positive quaternary diagonal quadratic forms*, Sakharth SSR Mecn. Math. Inst. Šrom. 40 (1971), 59–105 (MR 49#2536 (=E28-203)) (in Russian).

[4] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, 1984.

[5] J. Lagrange, *Nombres congruents et courbes elliptiques*, Sém. Delange–Pisot–Poitou, 16e année, 1974/75, no. 16.

[6] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. 171 (1934), 55–60.

[7] L. Rédei und H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, ibid. 170 (1933), 69–74.

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

[9] —, *The main conjecture for imaginary quadratic fields*, ibid. 103 (1991), 25–68.

[10] P. Serf, *Congruent numbers and elliptic curves*, in: Computational Number Theory, A. Pethő, M. Pohst, H. C. Williams and H. G. Zimmer (eds.), de Gruyter, 1991, 227–238.

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

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

Department of Mathematics
University of Science and Technology of China
Hefei, 230026, China

Received on 2.12.1994
and in revised form on 17.8.1995 (2705)