Cambridge Journal of Mathematics
Volume 2, Number 1, 117–161, 2014

Congruent numbers and Heegner points*

Ye Tian

1. Introduction and main results

A positive integer is called a *congruent number* if it is the area of a right-angled triangle, all of whose sides have rational length. The problem of determining which positive integers are congruent is buried in antiquity (see Chapter 9 of Dickson [6]), with it long being known that the numbers 5, 6, and 7 are congruent. Fermat proved that 1 is not a congruent number, and similar arguments show that also 2 and 3 are not congruent numbers. No algorithm has ever been proven for infallibly deciding whether a given integer $n \geq 1$ is congruent. The reason for this is that it can easily be seen that an integer $n \geq 1$ is congruent if and only if there exists a point (x, y), with x and y rational numbers and $y \neq 0$, on the elliptic curve $ny^2 = x^3 - x$. Moreover, assuming n to be square free, a classical calculation of root numbers shows that the complex L-function of this curve has zero of odd order at the center of its critical strip precisely when n lies in one of the residue classes of 5, 6, or 7 modulo 8. Thus, in particular, the unproven conjecture of Birch and Swinnerton-Dyer predicts that every positive integer lying in the residue classes of 5, 6, and 7 modulo 8 should be a congruent number. The aim of this paper is to prove the following partial results in this direction.

Theorem 1.1. *For any given integer $k \geq 0$, there are infinitely many square-free congruent numbers with exactly $k+1$ odd prime divisors in each residue class of $5, 6,$ and 7 modulo 8.*

Remark 1.2. The above result when $k = 0$ is due to Heegner [11], Birch [1], Stephens [24], and completed by Monsky [19], and that when $k = 1$ is due to Monsky [19] and Gross [26]. Actually Heegner is the first mathematician who found (in [11]) a method to construct fairly general solutions to cubic Diophantine equations. The method of this paper is based on his construction.

*The author was supported by NSFC grant 11325106, 973 Program 2013CB834202, NSFC grant 11031004, and The Chinese Academy of Sciences The Hundred Talents Program.

In addition to Theorem 1.1, we have the following result on the conjecture of Birch and Swinnerton-Dyer. For any abelian group A and an integer $d \geq 1$, we write $A[d]$ for the kernel of multiplication by d on A.

Theorem 1.3. *Let $m \equiv 5, 6, 7 \bmod 8$ be a square-free positive integer such that its odd part $n = p_0 p_1 \cdots p_k, k \geq 0$, has prime factors $p_i \equiv 1 \bmod 8$ for $1 \leq i \leq k$, and satisfies the condition that the field $\mathbb{Q}(\sqrt{-n})$ has no ideal classes of exact order 4. Then for the elliptic curve $E^{(m)}$ over $\mathbb{Q}$: $my^2 = x^3 - x$, we have*

$$\mathrm{rank}_{\mathbb{Z}} E^{(m)}(\mathbb{Q}) = 1 = \mathrm{ord}_{s=1} L(E^{(m)}, s).$$

Moreover, the Shafarevich-Tate group of $E^{(m)}$ is finite and has odd cardinality.

We will often work with the field $K = \mathbb{Q}(\sqrt{-2n})$. For the integer n in Theorem 1.3, the condition that $\mathbb{Q}(\sqrt{-n})$ has no ideal classes of exact order 4 is equivalent to the condition that the ideal class group $\mathcal{A}$ of the field K satisfies:

$$\dim_{\mathbb{F}_2}(\mathcal{A}[4]/\mathcal{A}[2]) = \begin{cases} 0, & \text{if } n \equiv \pm 3 \bmod 8, \\ 1, & \text{if } n \equiv 7 \bmod 8. \end{cases} \tag{1.1}$$

Remark 1.4. The work of Perrin-Riou [21] and Kobayshi [13] shows that the order of the p-primary subgroup of the Tate-Shafarevich group of $E^{(m)}$ is as predicted by the conjecture of Birch and Swinnerton-Dyer for all primes p with $(p, 2m) = 1$. At present, it is unknown whether the same statement holds for the primes p dividing $2m$, so that the full Birch-Swinnerton-Dyer conjecture is still not quite completely known for the curves $E^{(m)}$. However, toward to the conjecture for $p = 2$ we have Theorem 1.5 below in view of Gross-Zagier formula.

The condition (1.1) on $\mathcal{A}[4]/\mathcal{A}[2]$ in Theorem 1.3 allows us to complete the first 2-descent and to show that the 2-Selmer group of $E^{(m)}$ modulo the 2-torsion subgroup of $E^{(m)}$ is $\mathbb{Z}/2\mathbb{Z}$ (see Lemma 5.1). It follows that

$$\mathrm{rank}_{\mathbb{Z}} E^{(m)}(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(E^{(m)}/\mathbb{Q})[2] = 1,$$

and therefore that $\mathrm{rank}_{\mathbb{Z}} E^{(m)}(\mathbb{Q})$ is either 0 or 1. Any one of the parity conjecture for Mordell-Weil group and the finiteness conjecture for Shafarevich-Tate group predicts that the elliptic curve $E^{(m)}$ has Mordell-Weil group of rank 1. Therefore the BSD conjecture predicts that the analytic rank is 1.

Then the generalization of Gross-Zagier formula predicts that the height of a Heegner divisor is non-zero, so this Heegner divisor class should have infinite order. However, we shall follow a different path, and, always assuming (1.1), we shall prove independently of any conjectures that this Heegner divisor does indeed have infinite order, and the Tate-Shafarevich group is finite of odd order. Our method uses induction on the number of primes dividing the congruent number m, Kolyvagin's Euler system, and a generalization of the Gross-Zagier formula.

Let E be the elliptic curve $y^2 = x^3 - x$ so that $E^{(m)}$ is a quadratic twist of E. It is not difficult to see that the only rational torsion on $E^{(m)}$ is the subgroup $E^{(m)}[2]$ of 2-torsion. Let $E(\mathbb{Q}(\sqrt{m}))^-$ denote the subgroup of those points in $E(\mathbb{Q}(\sqrt{m}))$ which are mapped to their negative by the non-trivial element of the Galois group of $\mathbb{Q}(\sqrt{m})$ over $\mathbb{Q}$. Then the map which sends (x, y) to $(x, \sqrt{m}y)$ defines an isomorphism from $E^{(m)}(\mathbb{Q})$ onto $E(\mathbb{Q}(\sqrt{m}))^-$. Thus m will be congruent if and only if we can show that $E(\mathbb{Q}(\sqrt{m}))^-$ is strictly larger than $E[2]$. Note that $E^{(m)}$ and $E^{(-m)}$ are isomorphic over $\mathbb{Q}$.

The modular curve $X_0(32)$ of level $\Gamma_0(32)$ has genus 1 and is defined over $\mathbb{Q}$. Its associated Riemann surface structure is given by the complex uniformization

$$X_0(32)(\mathbb{C}) = \Gamma_0(32)\backslash(\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})),$$

where $\mathcal{H}$ is the upper half complex plane, and we write $[z]$ for the point on the curve defined by any $z \in \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. It is easy to see that $[\infty]$ is defined over $\mathbb{Q}$. The elliptic curve E has conductor 32 and there is a degree 2 modular parametrization $f : X_0(32) \to E$ mapping $[\infty]$ to 0. Such f is unique up to multiplication by -1 because the elliptic curve $(X_0(32), [\infty])$ has only one rational torsion point of order 2 (see Proposition 2.2). Let $n = p_0p_1 \cdots p_k$ and m be integers as in Theorem 1.3. Let $K = \mathbb{Q}(\sqrt{-2n})$ and H its Hilbert class field. Let $m^* = (-1)^{\frac{n-1}{2}}m$ and χ the abelian character over K defining the unramified extension $K(\sqrt{m^*})$. Define the point $P \in X_0(32)$ to be $[i\sqrt{2n}/8]$ if $n \equiv 5 \bmod 8$, and to be $[(i\sqrt{2n}+2)/8]$ if $n \equiv 6$ or $7 \bmod 8$. Both Theorem 1.1 and Theorem 1.3 will follow from the following main theorem of the paper.

Theorem 1.5. *Let $n = p_0p_1 \cdots p_k$ and m be the integers as in Theorem 1.3. Then the point $f(P) \in E$ is defined over $H(i)$; and the χ-component of $f(P)$, defined by*

$$P^\chi(f) := \sum_{\sigma \in \mathrm{Gal}(H(i)/K)} f(P)^\sigma \chi(\sigma),$$

satisfies

$$P^\chi(f) \in 2^{k+1}E(\mathbb{Q}(\sqrt{m^*}))^- \quad \textit{and} \quad P^\chi(f) \notin 2^{k+2}E(\mathbb{Q}(\sqrt{m^*}))^- + E[2].$$

In particular, $P^\chi(f) \in E(\mathbb{Q}(\sqrt{m^*}))^- \cong E^{(m)}(\mathbb{Q})$ *is of infinite order and* m *is a congruent number.*

We now explain our method in the case $n \equiv 5 \bmod 8$ in details. Other cases are similar. Let $p_0 \equiv 5 \bmod 8$ and $p_i \equiv 1 \bmod 8$, $1 \le i \le k$, be distinct primes. Let $n = p_0 p_1 \cdots p_k$ and $K = \mathbb{Q}(\sqrt{-2n})$. The theory of complex multiplication implies that

$$z := f(P) + (1+\sqrt{2}, 2+\sqrt{2})$$

is a point on E defined over the Hilbert class field H of K, even though neither $f(P)$ nor the 4-torsion point $(1+\sqrt{2}, 2+\sqrt{2})$ on E is defined over H. Note that if we use $-f$ instead of f, then we still obtain an H-rational point $-f(P)+(1+\sqrt{2}, 2+\sqrt{2}) = -z + (1,0)$. The desired Heegner point is defined by taking trace of z from H to $K(\sqrt{n})$

$$y_n := \mathrm{Tr}_{H/K(\sqrt{n})} z \in E(K(\sqrt{n})). \tag{1.2}$$

It turns out that y_n is actually defined over $\mathbb{Q}(\sqrt{n})$. Moreover, y_n (resp. $2y_n$) belongs to $E(\mathbb{Q}(\sqrt{n}))^-$ if $k \ge 1$ (resp. $k = 0$). Now it is easy to see that the point $P^\chi(f)$, defined in Theorem 1.5, is equal to $4y_n$.

The condition (1.1) in Theorem 1.3, in the case $p_0 \equiv 5 \bmod 8$, is equivalent to that the Galois group $\mathrm{Gal}(H/H_0) \cong 2\mathcal{A}$ has odd cardinality where $H_0 = K(\sqrt{p_0}, \ldots, \sqrt{p_k})$ is the genus field of K. We will show that the point y_n is of infinite order for $n = p_0 p_1 \cdots p_k$ satisfying the condition (1.1) in Theorem 1.3. When $k = 0$, classical arguments show that y_n is of infinite order (see, for example, [19]). However, when k is at least 1, we will prove by induction on k that, provided $n = p_0 p_1 \cdots p_k$ satisfies condition (1.1) in Theorem 1.3, the point y_n belongs to $2^{k-1}E(\mathbb{Q}(\sqrt{n}))^- + E[2]$, but does not belong to $2^k E(\mathbb{Q}(\sqrt{n}))^- + E[2]$. This clearly shows that y_n must be of infinite order. (Note that condition (1.1) holds automatically when $k = 0$). We now give some more details on how these arguments are carried through in detail.

In fact, we find a relation of y_n with other Heegner divisors. Now assume that $k \ge 1$ and let $y_0 = \mathrm{Tr}_{H/H_0} z \in E(H_0)$. It turns out that $y_0 \in E(H_0^+)$ where $H_0^+ = H_0 \cap \mathbb{R}$. For any positive divisor d of n divisible by p_0, let

$y_d = \mathrm{Tr}_{H/K(\sqrt{d})} z$, which actually belongs to $E(\mathbb{Q}(\sqrt{d}))^-$. The points y_d's with $p_0|d|n$ and y_0 are related by the following relation:

$$\sum_{p_0|d|n} y_d = \begin{cases} 2^k y_0, & \text{if } k \geq 2, \\ 2^k y_0 + \#2\mathcal{A} \cdot (0,0), & \text{if } k = 1. \end{cases} \tag{1.3}$$

Next, for any proper divisor d of n divisible by p_0, we need to know the 2-divisibility of y_d in the Mordell-Weil group $E(\mathbb{Q}(\sqrt{d}))^-$. To do this, we similarly construct a point $y_d^0 \in E(\mathbb{Q}(\sqrt{d}))$ with K replaced by $K_0 = \mathbb{Q}(\sqrt{-2d})$, whose 2-divisibility is understood by induction hypothesis. We can reduce the comparison of 2-divisibilities of y_d and y_d^0 to the comparison of their heights via Kolyvagin's result. The heights of these two points are related to central derivative L-values via Gross-Zagier formula Theorem 1.2 in [27]. The comparison of heights of these two points is further reduced to the comparison of two central L-values, which is given by Zhao in [28]. It turns out from the comparison and induction hypothesis that $y_d \in 2^k E(\mathbb{Q}(\sqrt{d}))^- + E[2]$ for all proper divisors d of n. It follows from the equality (1.3) that

$$y_n = 2^k \left(y_0 - \sum_{p_0|d|n, d \neq n} y_d' \right) + t$$

for some $y_d' \in E(\mathbb{Q}(\sqrt{d}))^-$ and $t \in E[2]$. It can then be shown by additional arguments (see the proof of Theorem 4.1) that this implies that $y_n \in 2^{k-1} E(\mathbb{Q}(\sqrt{n}))^- + E[2]$. The fact that $y_n \notin 2^k E(\mathbb{Q}(\sqrt{n}))^- + E[2]$ with n satisfying the condition (1.1) follows from the same algebraic ingredient as in the initial case $k = 0$ and some ramification argument. Note that $4y_n = P^\chi(f)$ and then Theorem 1.5 follows in the case $n \equiv 5 \bmod 8$.

Remark 1.6. By a conjecture of Goldfeld [8] or Katz-Sarnak [12], combined with Coates-Wiles' result [4], almost all positive integers $n \equiv 1, 2, 3 \bmod 8$ are non-congruent numbers.

It is known ([7] and [18]) that for any given integer $k \geq 0$, there are infinitely many square-free non-congruent positive integers with exactly $k+1$ odd prime divisors in each residue class of 1, 2, and 3 modulo 8. In fact, let $n = p_0 p_1 \cdots p_k$ be a product of distinct odd primes with $p_i \equiv 1 \bmod 8$ for $1 \leq i \leq k$ satisfying the condition (1.1) in Theorem 1.3. Let $m = n$ or $2n$ such that $m \equiv 1, 2, 3 \bmod 8$. Then m is non-congruent if $p_0 \not\equiv 1 \bmod 8$. Moreover, if $p_0 \equiv 1 \bmod 8$, then n is non-congruent provided the additional assumption $\left(\frac{2}{n}\right)_4 = -(-1)^{(n-1)/8}$.

The above non-congruent numbers are constructed easily by minimizing the 2-Selmer groups attached to 2-isogenies of $E^{(m)}$ and taking 2-part of the Shafarevich-Tate group into account in the case $p_0 \equiv 1 \bmod 8$.

Notations and Conventions. We often work with the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-2n})$ where n is a square-free positive odd integer. We fix an embedding of the algebraic closure $\bar{K}$ of K in $\mathbb{C}$. Let $\mathcal{O}_K$ denote the ring of integers in K. Then $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}w$ with $w = i\sqrt{2n}$. Let K^{ab} denote the maximal abelian extension of K. Let $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ and $\widehat{K} = K \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ the finite adéles of K. Denote by

$$[\quad, K^{ab}/K] : \quad \widehat{K}^\times / K^\times \longrightarrow \mathrm{Gal}(K^{ab}/K),$$

the Artin reciprocity law, and similarly for $[\quad, \mathbb{Q}^{ab}/\mathbb{Q}]$. We also often write $\sigma_t = [t, K^{ab}/K]$. For each prime $p|2n$, let ϖ_p be a uniformizer $\sqrt{-2n}$ of the local field K_p of K at the unique prime above p; for each $0 < d|n$, let $\varpi_d = \prod_{p|d} \varpi_p \in \widehat{K}^\times$. We often use the convention $\varpi = \varpi_2 \in K_2^\times$. For $t \in \widehat{K}^\times$ (resp. $\widehat{\mathbb{Q}}^\times$), we denote by $t_2 \in K_2^\times$ (resp. $\mathbb{Q}_2$) its component at 2.

We will also need Gauss' genus theory for the imaginary quadratic field K. Denote by H the Hilbert class field of K and $\mathcal{A}$ the ideal class group of K. Suppose that n has exact $k+1$ prime divisors: $n = \prod_{j=0}^{k} p_j$. Let $H_0 = K(\sqrt{p_0^*}, \sqrt{p_1^*}, \ldots, \sqrt{p_k^*}) \subset H$ be its genus field of K, where $p^* = (-1)^{(p-1)/2} p$ so that $p^* \equiv 1 \bmod 4$. Sometimes we identify the ideal class group $\mathcal{A}$ of K with the class group $\widehat{K}^\times / K^\times \widehat{\mathcal{O}}_K^\times$. Consider the exact sequence

$$0 \longrightarrow \mathcal{A}[2] \longrightarrow \mathcal{A} \xrightarrow{\times 2} \mathcal{A} \longrightarrow \mathcal{A}/2\mathcal{A} \longrightarrow 0.$$

Gauss' genus theory says the following

(i) the subgroup $\mathcal{A}[2]$ consists of the ideal classes of $(d, \sqrt{-2n})$, corresponding to the classes of ϖ_d in $\widehat{K}^\times / K^\times \widehat{\mathcal{O}}_K^\times$, where d runs over all positive divisors of n. Therefore $\mathcal{A}[2]$ has cardinality 2^{k+1}.

(ii) under the class field theory isomorphism $\sigma : \mathcal{A} \simeq \mathrm{Gal}(H/K)$, the subgroup $2\mathcal{A} \simeq \mathrm{Gal}(H/H_0)$, i.e. the class of $t \in 2\mathcal{A}$ if and only if σ_t fixes all $\sqrt{p_j^*}, 0 \leq j \leq k$.

By Gauss' quadratic reciprocity law, for each $0 < d|n$ and $p|n$, σ_{ϖ_d} fixes $\sqrt{p^*}$ iff $(\frac{d}{p}) = 1$ for $p \nmid d$ and $(\frac{2n/d}{p}) = 1$ for $p|d$.

It is easy to see that $i \notin H$ and therefore the restriction map gives the natural isomorphism $\mathrm{Gal}(H(i)/K(i)) \cong \mathrm{Gal}(H/K)$. Let $\mathcal{O}_2$ denote the ring of integers in the local field K_2. Its unit group $\mathcal{O}_2^\times$ is generated by $-1, 5, 1+\varpi$ as a $\mathbb{Z}_2$-module. We often need the structure of the Galois group $\mathrm{Gal}(H(i)/\mathbb{Q}) \cong \mathrm{Gal}(H(i)/K) \rtimes \{1, c\}$, where c is the complex conjugation and

$$\mathrm{Gal}(H(i)/K) \cong \widehat{K}^\times/K^\times\widehat{\mathcal{O}}_K^{\times(2)}U_2, \quad \text{with} \quad U_2 = \mathbb{Z}_2^\times(1 + 2\varpi\mathcal{O}_2).$$

Here the supscript in $\widehat{\mathcal{O}}_K^{\times(2)}$ means the component above 2 is removed. Note that $U_2 \subset \mathcal{O}_2^\times$ is generated by $-1, 5, (1+\varpi)^2$. Thus the Galois group $\mathrm{Gal}(H(i)/H)$ is generated by $\sigma_{1+\varpi}$. The group $\mathrm{Gal}(H(i)/\mathbb{Q})$ is generated by $\mathrm{Gal}(H(i)/H_0(i)) \cong 2\mathcal{A}$, the complex conjugation c, and elements representing $\mathrm{Gal}(H_0(i)/K)$. For example, when $2\mathcal{A} \cap \mathcal{A}[2] = 0$, $\mathrm{Gal}(H_0(i)/K)$ is represented by $\sigma_{1+\varpi}$ and σ_{ϖ_d} with all $0 < d|n$.

Acknowledgment. The author thanks John Coates, Xinyi Yuan, Shouwu Zhang, Wei Zhang for many useful discussions and comments. In the original version of this paper, the author used the construction of Heegner points given by employing the modular parametrization of E via the modular curve $X(8)$, following the original work of Heegner and Monsky. The current simpler construction using the curve $X_0(32)$ arose out of discussions with Xinyi Yuan.

The author thanks Keqin Feng, Delang Li, Mingwei Xu, and Chunlai Zhao for bringing him to this beautiful topic when he was in a master degree program. The author thanks John Coates, Benedict Gross, Victor Kolyvagin, Yuan Wang, Lo Yang, Shing-Tung Yau, and Shouwu Zhang for constant encouragement during the preparation of this work.

2. Modular parametrization and CM points

Let E be the elliptic curve with Weierstrass equation $y^2 = x^3 - x$. It is known that E has conductor 32. Let $f : X_0(32) \longrightarrow E$ be a fixed modular parametrization over $\mathbb{Q}$ of degree 2 mapping the cusp $[\infty]$ at the infinity on $X_0(32)$ to the zero element $0 \in E$. In this section, we will construct suitable CM points on E associated to the modular parametrization f and the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-2n})$ with n a positive square-free odd integer. We will show that $E' := (X_0(32), [\infty])$ is an elliptic curve with Weierstrass equation $y^2 = x^3 + 4x$. Before giving construction of points on E, we need set up the correspondence of torsion points of E' over $\mathbb{Q}(i)$ between their (x, y)-coordinates and their modular expressions.

We now recall the following standard notation. Let $\mathcal{H}$ be the upper half complex plane, on which the subgroup $\mathrm{GL}_2^+(\mathbb{R})$ of elements of $\mathrm{GL}_2(\mathbb{R})$ with positive determinant acts by linear fractional transformations. Let $\Gamma_0(32)$ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c \equiv 0 \bmod 32$, which acts on $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}$ by linear fractional transformation. Denote by $Y_0(32)$ the modular curve of level $\Gamma_0(32)$ over $\mathbb{Q}$ and $X_0(32)$ its projective closure over $\mathbb{Q}$. Then the underlying compact Riemann surface of $X_0(32)$ is given as:

$$X_0(32)(\mathbb{C}) = Y_0(32)(\mathbb{C}) \cup S,$$

where

$$Y_0(32)(\mathbb{C}) = \Gamma_0(32)\backslash\mathcal{H}, \qquad S = \Gamma_0(32)\backslash\mathbb{P}^1(\mathbb{Q}).$$

For each $z \in \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, let $[z]$ denote the point on $X_0(32)(\mathbb{C})$ represented by z. The set S consists of 8 cusps:

$$[\infty], \quad [0], \quad [-1/2], \quad [-1/16], \quad [-1/4], \quad [-3/4], \quad [1/8], \quad [-1/8],$$

where the first 4 cusps are defined over $\mathbb{Q}$ and the later 4 ones have the field of definition $\mathbb{Q}(i)$. The curve $X_0(32)$ has genus one and thus we have an elliptic curve $E' := (X_0(32), [\infty])$ over $\mathbb{Q}$ with the cusp $[\infty]$ as its zero element.

Proposition 2.1. *The elliptic curve $E' = (X_0(32), \infty)$ has complex multiplication by $\mathbb{Z}[i]$ and Weierstrass equation $y^2 = x^3 + 4x$ such that the cusp $[0] = (2, 4)$ in (x, y)-coordinates. Moreover, the set S of cusps on $X_0(32)$ is exactly $E'[(1+i)^3]$.*

Proof. Define N to be the normalizer of $\Gamma_0(32)$ in $\mathrm{GL}_2^+(\mathbb{R})$ and let $Z(\mathbb{R})$ denote the center of $\mathrm{GL}_2^+(\mathbb{R})$. Let $\mathrm{Aut}(X_0(32)(\mathbb{C}))$ denote the group of automorphisms of $X_0(32)(\mathbb{C})$ and $\mathrm{Aut}(X_0(32)(\mathbb{C}), S)$ its subgroup of automorphisms t satisfying $t(S) = S$. Then the action of $N \subset \mathrm{GL}_2^+(\mathbb{R})$ on $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ induces a homomorphism

$$T : N \longrightarrow \mathrm{Aut}(X_0(32)(\mathbb{C}), S)$$

with kernel $Z(\mathbb{R})\Gamma_0(32)$.

Now, as is very well known, every element of $\mathrm{Aut}(X_0(32)(\mathbb{C}))$ is of form

$$t_{\alpha,\epsilon}(x) = \epsilon(x) + \alpha,$$

where ϵ belongs to the group $\mathrm{Aut}(E'_{\mathbb{C}})$ of automorphisms of the elliptic curve $E'_{\mathbb{C}}$ (i.e. ones with $\epsilon([\infty]) = [\infty]$), and α is some point in $E'(\mathbb{C})$.

Now consider the matrices

$$A = \begin{pmatrix} 0 & 1 \\ -32 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1/4 \\ 0 & 1 \end{pmatrix}, \quad C = AB^2 = \begin{pmatrix} 0 & 1 \\ -32 & -16 \end{pmatrix}.$$

One verifies immediately that A, B, and C belong to N, and that their classes in $N/Z(\mathbb{R})\Gamma_0(32)$ have exact orders $2, 4, 4$, respectively. Thus $T(A), T(B)$, $T(C)$ have exact orders $2, 4, 4$, respectively. Also $T(B)$ maps $[\infty]$ to itself. Thus $T(B) \in \mathrm{Aut}(E'_{\mathbb{C}})$ is an automorphism of $E'_{\mathbb{C}}$ of exact order 4, proving that $E'_{\mathbb{C}}$ has complex multiplication by $\mathbb{Z}[i]$. Since $T(A)$ has fixed point $[i\sqrt{2}/8]$, it is not translation. It now follows immediately from that $T(A)^2 = 1$ that $T(A) = t_{\alpha,-1}$ for some point α in $E'(\mathbb{C})$. Therefore, $T(C) = T(AB^2) = t_{\alpha,1}$. But $T(C)$ has exact order 4, whence we see that α must have order 4. Finally, $T(A)$ is defined over $\mathbb{Q}$ since it is the Atkin-Lehner involution. As $T(B^2)$ is the multiplication by -1 and then is clearly defined over $\mathbb{Q}$. Hence $\alpha = T(AB^2)([\infty]) = [0]$ must be a rational point of exact order 4.

Since every elliptic curve over $\mathbb{Q}$ is known to be parametrized by the modular curve of the same level as its conductor, it follows that $E' = (X_0(32), [\infty])$ must be isogenous to the elliptic curve $y^2 = x^3 + 4x$. However, there are just two isomorphism classes of curves defined over $\mathbb{Q}$ in the isogeny class of E', and $y^2 = x^3 + 4x$ is the unique one with a rational point of order 4. Thus E' must be isomorphic to $y^2 = x^3 + 4x$ over $\mathbb{Q}$. Since rational points on $y^2 = x^3 + 4x$ of exact order 4 are $(2, \pm 4)$, the isomorphism is unique if we require the order 4 point $[0]$ on E' is mapped to $(2, 4)$. Thus E' has Weierstrass equation $y^2 = x^3 + 4x$ for unique modular functions x, y such that the cusp $[0]$ has coordinate $(2, 4)$.

Let ψ denote the unique Grossencharacter of any elliptic curve defined over $\mathbb{Q}$ with conductor 32 and complex multiplication by $\mathbb{Z}[i]$. Then the conductor of ψ must be $(1+i)^3\mathbb{Z}[i]$ because the norm of this conductor times the absolute value 4 of the discriminant of $\mathbb{Q}(i)$ must be 32. It then follows easily from the main theorem of complex multiplication that $E'[(1+i)^3] = E'(\mathbb{Q}(i))_{\mathrm{tor}}$. But we know that $S \subset E'(\mathbb{Q}(i))_{\mathrm{tor}}$ and has cardinality 8, thus $S = E'(\mathbb{Q}(i))_{\mathrm{tor}} = E'[(1+i)^3]$. □

For any field extension F over $\mathbb{Q}$, let $X_0(32)_F$ be the base change of $X_0(32)$ to F and write $\mathrm{Aut}(X_0(32)_F)$ for the group of automorphisms of $X_0(32)_F$. Similarly one defines $\mathrm{Aut}(E'_F)$. Then it is easy to see that

$$\mathrm{Aut}(X_0(32)_F) \cong E'(F) \rtimes \mathrm{Aut}(E'_F).$$

Using the notations in the proof of Proposition 2.1, we have seen above that there is a natural homomorphism

$$T : N \longrightarrow \mathrm{Aut}(X_0(32)(\mathbb{C}), S) \subset \mathrm{Aut}(X_0(32)_{\mathbb{C}}),$$

with kernel $Z(\mathbb{R})\Gamma_0(32)$. Now we have that $\mathrm{Aut}(E'_{\mathbb{C}}) \cong \mathbb{Z}[i]^\times$ and $T(B) \in \mathrm{Aut}(E'_{\mathbb{C}})$ is of order 4. One can see that $T(B)$ maps (x, y) to $(-x, iy)$ by looking at actions of $T(B)$ at 0 and B at $[\infty]$: at $[\infty]$, the differential is represented by dq with $q = e^{2\pi i z}$. It is clear that $B^*dq = dB^*q = idq$; at $0 \in E'$, the morphism $(x, y) \mapsto (-x, iy)$ brings the Neron differential dx/y to idx/y.

Proposition 2.2. *With the notations above, the normalizer N of $\Gamma_0(32)$ is generated by $Z(\mathbb{R})\Gamma_0(32), A$ and B. The homomorphism T induces an isomorphism*

$$N/Z(\mathbb{R})\Gamma_0(32) \xrightarrow{\sim} \mathrm{Aut}(X_0(32)_{\mathbb{Q}(i)}) \cong E'(\mathbb{Q}(i)) \rtimes \mathrm{Aut}(E'_{\mathbb{Q}(i)}).$$

Moreover, if write $t_\alpha \in \mathrm{Aut}(E'_{\mathbb{C}})$ for the translation by $\alpha \in E'(\mathbb{C})$, then the following relations hold:

$$t_{(2,4)} = T\begin{pmatrix} 0 & 1 \\ -32 & -16 \end{pmatrix}, \quad t_{(2,-4)} = T\begin{pmatrix} -16 & -1 \\ 32 & 0 \end{pmatrix}, \quad t_{(0,0)} = T\begin{pmatrix} -2 & -1 \\ 32 & 14 \end{pmatrix},$$
$$t_{(-2,4i)} = T\begin{pmatrix} -24 & -7 \\ 32 & 8 \end{pmatrix}, \quad t_{(-2,-4i)} = T\begin{pmatrix} 8 & 7 \\ -32 & -24 \end{pmatrix},$$
$$t_{(2i,0)} = T\begin{pmatrix} -4 & -3 \\ 32 & 20 \end{pmatrix}, \quad t_{(-2i,0)} = T\begin{pmatrix} 4 & 1 \\ 32 & 12 \end{pmatrix}.$$

Proof. Since $E'(\mathbb{Q})$ has rank 0, we see that $E'(\mathbb{Q}(i)) = E'[(1+i)^3]$ consists of the following 8 points:

$$[\infty], \quad (0,0), \quad (2, \pm 4), \quad (\pm 2i, 0), \quad (-2, \pm 4i).$$

Note that $T(C) = t_{(2,4)}$ and $T(B)$ generate $E'(\mathbb{Q}(i)) \rtimes \mathrm{Aut}(E'_{\mathbb{Q}(i)})$. It follows that the image of T contains $\mathrm{Aut}(X_0(32)_{\mathbb{Q}(i)})$. But any t in the image of T, $t([\infty]) \in S = E'(\mathbb{Q}(i))$. It follows that $\mathrm{Im}(T) \subseteq E'(\mathbb{Q}(i)) \rtimes \mathrm{Aut}(E'_{\mathbb{Q}(i)})$. Thus the image of T is $\mathrm{Aut}(X_0(32)_{\mathbb{Q}(i)}$ and the homomorphism T induces an isomorphism $N/Z(\mathbb{R})\Gamma_0(32) \xrightarrow{\sim} \mathrm{Aut}(X_0(32)_{\mathbb{Q}(i)})$. It also follows that N is generated by $Z(\mathbb{R})\Gamma_0(32)$, A, and B.

Note that $\alpha = (2,4)$ and $i\alpha$ generate $E'(\mathbb{Q}(i))$ and

$$t_{-i\alpha} = [-i] \circ [t_\alpha] \circ [i] = T(B^{-1}) \circ T(C) \circ T(B) = T(B^{-1}CB).$$

The verifying of remaining relations is then straightforward. □

There is a well known alternative adelic expression for the complex points of $X_0(32)$, which we will also need. Let $\mathbb{A}$ be the adeles of $\mathbb{Q}$ and $\mathbb{A}_f$ its finite part. Let $G = \mathrm{GL}_{2,\mathbb{Q}}$, $G(\mathbb{A}_f)$ its finite-adelic points, and $U_0(32) \subset G(\mathbb{A}_f)$ the open compact subgroup defined by

$$U_0(32) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \;\middle|\; c \equiv 0 \bmod 32\widehat{\mathbb{Z}} \right\}.$$

The complex uniformization of $X_0(32)$ has the following adelic form

$$X_0(32)(\mathbb{C}) = G(\mathbb{Q})_+ \backslash (\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})) \times G(\mathbb{A}_f)/U_0(32).$$

For any $z \in \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ and any $g \in G(\mathbb{A}_f)$. we denote by $[z, g]$ its image in $X_0(32)(\mathbb{C})$.

The matrix $B^2 \in G(\mathbb{Q}) \subset G(\mathbb{A}_f)$ normalizes both $\Gamma = \Gamma_0(32)$ and $U_0(32)$. The morphism $T(B^2)$ is represented by the Hecke action

$$[z, g] \mapsto [z, gB^{-2}], \quad \forall z \in \mathcal{H}, g \in G(\mathbb{A}_f)$$

which is defined over $\mathbb{Q}$ by the functriality of canonical models of Shimura varieties. However, the matrix B does not normalize $U_0(32)$, though it normalizes $\Gamma_0(32)$. The morphism $T(B)$ on $X_0(32)$ can be written as

$$[z, \gamma] \mapsto [z, \gamma B^{-1}], \quad \forall \gamma \in G(\mathbb{Q})_+, z \in \mathcal{H},$$

but we can not conclude that it is defined over $\mathbb{Q}$. In fact, it is defined over $\mathbb{Q}(i)$.

We now construct suitable points on E from CM points on $X_0(32)$. We first consider the case with $n \equiv 1 \bmod 4$ and the case with $n \equiv 3 \bmod 4$ will be considered later in Theorem 2.8. Note that the set of torsion points with exact order 4 on E is the union of the following subsets:

$$(i, 1-i) + E[2], \quad \left(1+\sqrt{2}, 2+\sqrt{2}\right) + E[2], \quad \text{and} \quad \left(-1-\sqrt{2}, i\left(2+\sqrt{2}\right)\right) + E[2],$$

whose doubles are $(0,0), (1,0)$, and $(-1,0)$, respectively.

Definition 2.3. *Let $n \equiv 1 \bmod 4$ be a positive integer and $K = \mathbb{Q}(\sqrt{-2n})$. Let $P \in X_0(32)(K^{ab})$ be the image of $\frac{i\sqrt{2n}}{8}$ under the complex uniformization $\mathcal{H} \to X_0(32)$. Define the CM point on E*

$$z := f(P) + (1+\sqrt{2}, 2+\sqrt{2}) \in E(K^{ab}).$$

For each $t \in \widehat{K}^\times$, let z_t denote the Galois conjugation z^{σ_t} of z.

Theorem 2.4. *Assume that $n \equiv 1 \bmod 4$ is a positive integer. Then, for each $t \in \widehat{K}^\times$, we have*

1. *the point z_t is defined over the Hilbert class field H of K and only depends on the class of t modulo $K^\times \widehat{\mathcal{O}}_K^\times$;*
2. *the complex conjugation of z_t, denoted by $\bar{z}_t$, is equal to $z_{t^{-1}}$; and*
3. *$z_{\varpi t} + z_t = 0$ or $(0,0)$ according to $n \equiv 1 \bmod 8$ or $\equiv 5 \bmod 8$.*

Remark 2.5. The CM points z_t above are essentially the same as those Monsky studied in [19] using modular functions on $X(8)$. Theorem 2.4 still holds if we replace z by any CM point $\pm f(P) + Q$ where Q is any 4-torsion point of E with $2Q = (1,0)$.

We will prove Theorem 2.4 by showing the following corresponding result on $X_0(32)$ via the modular parametrization f.

Proposition 2.6. *Let $n \equiv 1 \bmod 4$ be a positive integer and $K = \mathbb{Q}(\sqrt{-2n})$. Let $P \in X_0(32)$ be the point defined by $i\sqrt{2n}/8 \in \mathcal{H}$ via the complex uniformization. Let H' be the defining field of P. The following hold:*

1. *the field $H' \subset K^{ab}$ of P over K is characterized by*

$$\mathrm{Gal}(H'/K) \xrightarrow{\sim} \widehat{K}^\times / K^\times (\mathbb{Z}_2^\times (1 + 4\mathcal{O}_2)) \widehat{\mathcal{O}}_K^{\times(2)}$$

   via Artin reciprocity law. Here the supscript in $\widehat{\mathcal{O}}_K^{\times(2)}$ means the component at the unique place of K above 2 is removed.
2. *The extension H'/K is anticyclotomic in the sense that H' is Galois over $\mathbb{Q}$ such that the nontrivial involution on K over $\mathbb{Q}$ acts on $\mathrm{Gal}(H'/K)$ by the inverse.*
3. *The field H' is a cyclic extension of degree 4 over H with $\mathrm{Gal}(H'/H)$ generated by $\sigma_{1+\varpi}$, where recall that $\varpi \in K_2^\times$ is the uniformizer $\sqrt{-2n}$.*
4. *Moreover,*

$$P^{\sigma_{1+\varpi}} = P + (-2i, 0), \quad P^{\sigma_\varpi} + P = (2,4).$$

Proof. Recall Shimura's reciprocity law (for example, see [17]). Let $w = i\sqrt{2n} \in K^\times$ and view $K^\times$ as a sub-torus of $\mathrm{GL}_{2,\mathbb{Q}}$ via the $\mathbb{Q}$-embedding of $K^\times$ into $\mathrm{GL}_{2,\mathbb{Q}}$: $a + bw \mapsto \left(\begin{smallmatrix} a & -2nb \\ b & a \end{smallmatrix}\right)$. Then $w \in \mathcal{H}$ is the unique point on $\mathcal{H}$ fixed by $K^\times$. For any point

$$x = [w, g] \in X_0(32)(\mathbb{C}) = G(\mathbb{Q})_+ \backslash (\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})) \times G(\mathbb{A}_f)/U_0(32), \quad g \in G(\mathbb{A}_f)$$

and any $t \in \widehat{K}^\times \subset G(\mathbb{A}_f)$, the action of σ_t on x is given by: $[w, g]^{\sigma_t} = [w, tg]$. It follows that the defining field $K(x)$ of x is characterized by

$$\mathrm{Gal}(K(x)/K) \simeq \widehat{K}^\times / K^\times (\widehat{K}^\times \cap gU_0(32)g^{-1})$$

via the reciprocity law.

Write the point $P = \left[w, \left(\begin{smallmatrix} 8 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right] \in X_0(32)$ in adelic form. Then H' corresponds to the open compact subgroup

$$\widehat{K}^\times \cap \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix} U_0(32) \begin{pmatrix} 8^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{Z}_2^\times (1 + 4\mathcal{O}_2) \widehat{\mathcal{O}}_K^{\times (2)}.$$

It gives the statement (1) and

$$\begin{aligned} \mathrm{Gal}(H'/H) \xrightarrow{\sim} K^\times \widehat{\mathcal{O}}_K^\times / K^\times (\mathbb{Z}_2^\times (1 + 4\mathcal{O}_2)) \widehat{\mathcal{O}}_K^{\times (2)} &= \mathcal{O}_2^\times / \mathbb{Z}_2^\times (1 + 4\mathcal{O}_2) \\ &= (1 + \varpi)^{\mathbb{Z}/4\mathbb{Z}}. \end{aligned}$$

Here we use the fact that $\mathcal{O}_2^\times = \{\pm 1\} \times 5^{\mathbb{Z}_2} \times (1 + \varpi)^{\mathbb{Z}_2}$ as a $\mathbb{Z}_2$-module. Moreover, since

$$\widehat{\mathbb{Q}}^\times \subset K^\times \cdot (\mathbb{Z}_2^\times (1 + 4\mathcal{O}_2) \widehat{\mathcal{O}}_K^{\times (2)}),$$

the non-trivial involution of K acts on $\mathrm{Gal}(H'/K)$ by the inverse. The statements (2) and (3) are now proved.

By Proposition 2.2, $t_{(-2i,0)} = T\left(\begin{smallmatrix} 4 & 1 \\ 32 & 12 \end{smallmatrix}\right)$. Note that $(-2i, 0)$ is of order 2. Thus the relation $P^{\sigma_{1+\varpi}} = P + (-2i, 0)$ is equivalent to

$$P^{\sigma_{1+\varpi}} = T \begin{pmatrix} 4 & 1 \\ 32 & 12 \end{pmatrix} P,$$

which is just

$$\left[w, (1 + \varpi) \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix}\right] = \left[w, \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 32 & 12 \end{pmatrix}\right] \tag{2.1}$$

It is further equivalent to

$$(1+\varpi)\begin{pmatrix}8&0\\0&1\end{pmatrix}\in K^\times\begin{pmatrix}8&0\\0&1\end{pmatrix}\begin{pmatrix}4&1\\32&12\end{pmatrix}U_0(32),$$

and then to

$$(1+\varpi)\in K^\times(V\cap\widehat{K}^\times),\quad V=\begin{pmatrix}1&2\\1&3\end{pmatrix}\begin{pmatrix}8&0\\0&1\end{pmatrix}U_0(32)\begin{pmatrix}8^{-1}&0\\0&1\end{pmatrix}.$$

It follows easily from $n\equiv 1 \bmod 4$ that

$$V\cap\widehat{K}^\times=\widehat{\mathcal{O}}_K^{\times(2)}\mathbb{Z}_2^\times(1+\varpi+4\mathcal{O}_2).$$

Then (2.1) is equivalent to

$$1+\varpi\in K^\times\widehat{\mathcal{O}}_K^{\times(2)}\mathbb{Z}_2^\times(1+\varpi+4\mathcal{O}_2),$$

which is obvious.

By proposition 2.2, $t_{(2,4)}=T\left(\begin{smallmatrix}-16&-1\\32&0\end{smallmatrix}\right)^{-1}$, thus the relation $P^{\sigma_\varpi}+P=(2,4)$ is equivalent to

$$P^{\sigma_\varpi}=T\begin{pmatrix}-16&-1\\32&0\end{pmatrix}^{-1}(T(B^2)P),$$

which is just

$$\left[w,\varpi\begin{pmatrix}8&0\\0&1\end{pmatrix}\right]=\left[w,\begin{pmatrix}8&0\\0&1\end{pmatrix}\begin{pmatrix}1&1/2\\0&1\end{pmatrix}\begin{pmatrix}-16&-1\\32&0\end{pmatrix}\right]\tag{2.2}$$

It is further equivalent to

$$\varpi\begin{pmatrix}8&0\\0&1\end{pmatrix}\in K^\times\begin{pmatrix}8&0\\0&1\end{pmatrix}\begin{pmatrix}0&-1\\32&0\end{pmatrix}U_0(32)$$

and then to

$$\varpi\in K^\times(V\cap\widehat{K}^\times),\quad V=\begin{pmatrix}0&-2\\1&0\end{pmatrix}\begin{pmatrix}8&0\\0&1\end{pmatrix}U_0(32)\begin{pmatrix}8^{-1}&0\\0&1\end{pmatrix}.$$

It is easy to have that

$$V\cap\widehat{K}^\times=\widehat{\mathcal{O}}_K^{\times(2)}\mathbb{Z}_2^\times(\varpi+8\mathcal{O}_2).$$

Then (2.2) is equivalent to $\varpi \in K^\times \widehat{\mathcal{O}}_K^{\times(2)} \mathbb{Z}_2^\times(\varpi + 8\mathcal{O}_2)$, which is obvious. The proof of (4) is complete. □

Proof of Theorem 2.4. Recall that the defining field $H' = K(P)$ of P over K corresponds to the subgroup $K^\times \widehat{\mathcal{O}}_K^{\times(2)} \mathbb{Z}_2^\times(1 + 4\mathcal{O}_2) \subset \widehat{K}^\times$. The norm of this subgroup over the extension $K/\mathbb{Q}$ is $\mathbb{Q}^\times \widehat{Z}^{\times(2)} \mathbb{Z}_2^{\times 2}(1 + 8\mathbb{Z}_2)$, which corresponds to the abelian extension $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$. Thus $\sqrt{2}, i \in H'$.

For any $t \in \widehat{K}^\times$, let $P_t = \left[w, t\begin{pmatrix} 8 & \\ & 1\end{pmatrix}\right] = P_1^{\sigma_t} \in X_0(32)$, then

$$z_t := z^{\sigma_t} = f(P_t) + (1 + \sqrt{2}, 2 + \sqrt{2})^{\sigma_t} \in E(H').$$

Since H'/K is anti-cyclotomic and $P \in X_0(32)(\mathbb{R})$, the complex conjugation of $f(P_t)$ is $f(P_{t^{-1}})$ and therefore the complex conjugation of z_t is equal to $z_{t^{-1}}$. This proves (2).

To show (1), we only need to consider the case with $t = 1$, i.e. $z := z_1 \in E(H)$. Note that

$$\sigma_{1+\varpi}(\sqrt{2}) = [1 + \varpi, K^{ab}/K](\sqrt{2}) = [(1 + 2n)_2, \mathbb{Q}^{ab}/\mathbb{Q}](\sqrt{2}) = -\sqrt{2}.$$

Since $\sigma_{1+\varpi}$ generates $\mathrm{Gal}(H'/H)$, $z \in E(H)$ is equivalent to the relation $z^{\sigma_{1+\varpi}} = z$, and therefore is equivalent to

$$\begin{aligned} f(P^{\sigma_{1+\varpi}}) &= f(P) + (1 + \sqrt{2}, 2 + \sqrt{2}) - (1 + \sqrt{2}, 2 + \sqrt{2})^{\sigma_{1+\varpi}} \\ &= f(P) + (0, 0) = f(P + (-2i, 0)) \end{aligned}$$

which follows from the first equality in Proposition 2.6 (4).

To show (3), we only need to show that $z_\varpi + z = 0$ or $(0, 0)$ according to $n \equiv 1 \bmod 8$ or $\equiv 5 \bmod 8$. Note that

$$[\varpi, K^{ab}/K](\sqrt{2}) = [(2n)_2, \mathbb{Q}^{ab}/\mathbb{Q}](\sqrt{2}) = [n_2, \mathbb{Q}^{ab}/\mathbb{Q}](\sqrt{2}) = (-1)^{(n-1)/4}\sqrt{2}$$

and that $f((2, 4)) = (1, 0)$. It follows that

$$\begin{aligned} z^{\sigma_\varpi} + z &= f(P^{\sigma_\varpi} + P) + \begin{cases} (1, 0), & \text{if } n \equiv 1 \bmod 8, \\ (-1, 0), & \text{if } n \equiv 5 \bmod 8. \end{cases} \\ &= f(P^{\sigma_\varpi} + P - (2, 4)) + \begin{cases} 0, & \text{if } n \equiv 1 \bmod 8, \\ (0, 0), & \text{if } n \equiv 5 \bmod 8. \end{cases} \end{aligned}$$

Thus the desired follows then from the second equality in Proposition 2.6 (4). □

We now consider the case with $n \equiv 3 \bmod 4$.

Definition 2.7. *Let $n \equiv 3 \bmod 4$ be a positive integer and $K = \mathbb{Q}(\sqrt{-2n})$. Let $P \in X_0(32)$ be the image of $\frac{2+i\sqrt{2n}}{8}$ under the complex uniformization and define a CM point*

$$z := f(P) + (1+\sqrt{2}, 2+\sqrt{2}) \in E(K^{ab}).$$

For any $t \in \widehat{K}^\times$ satisfying σ_t fixing i, define $z_t := z^{\sigma_t}$.

Theorem 2.8. *Assume that $n \equiv 3 \bmod 4$ is a positive integer. Then, for each $t \in \widehat{K}^\times$ with σ_t fixing i, we have*

1. *the point $z_t \in E(H(i))$ and the involution $\sigma_{1+\varpi}$ of $\mathrm{Gal}(H(i)/H)$ maps z_t to $z_t + (0,0)$;*
2. *the complex conjugation of z_t, denoted by $\bar{z}_t$, is equal to $-z_{t^{-1}} + (1,0)$;*
3. *let $\varpi' = \varpi(1+\varpi) \in K_2^\times$ (so that $\sigma_{\varpi'}$ fixes i), then $z_{\varpi' t} - z_t = (1,0)$ or $(-1,0)$ according to $n \equiv 7 \bmod 8$ or $3 \bmod 8$.*

We will give the proof of Theorem 2.8 after we prove the following

Proposition 2.9. *Let $n \equiv 3 \bmod 4$ be a positive integer and $P \in X_0(32)$ be the CM point corresponding to $\frac{2+i\sqrt{2n}}{8} \in \mathcal{H}$ via complex uniformization. The defining field $H' \subset K^{ab}$ of P over K is characterized by*

$$\mathrm{Gal}(H'/K) \xrightarrow{\sim} \widehat{K}^\times / K^\times (\mathbb{Z}_2^\times (1+4\mathcal{O}_2)) \widehat{\mathcal{O}}_K^{\times(2)}$$

via Artin reciprocity law so that $\mathrm{Gal}(H'/H)$ is generated by $\sigma_{1+\varpi}$. Moreover,

$$P^{\sigma_{1+\varpi}} = P + (2i, 0), \qquad P^{\sigma_{\varpi'}} - P = (2,4).$$

Here $\varpi' = \varpi(1+\varpi) \in K_2^\times$ so that $\sigma_{\varpi'}$ fixes i.

Proof. The proof of the first part is the same as in the case $n \equiv 1 \bmod 4$. By Proposition 2.2, $t_{(2i,0)} = T\left(\begin{smallmatrix} -4 & -3 \\ 32 & 20 \end{smallmatrix}\right)$. The relation $P^{\sigma_{1+\varpi}} = P + (2i, 0)$ is equivalent to

$$P^{\sigma_{1+\varpi}} = T \begin{pmatrix} -4 & -3 \\ 32 & 20 \end{pmatrix} P$$

which is

$$\left[w, (1+\varpi) \begin{pmatrix} 8 & -2 \\ 0 & 1 \end{pmatrix} \right] = \left[w, \begin{pmatrix} 8 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -4 & -3 \\ 32 & 20 \end{pmatrix}^{-1} \right]. \tag{2.3}$$

It is further equivalent to,

$$(1+\varpi)\begin{pmatrix}8 & -2\\ 0 & 1\end{pmatrix} \in K^\times \begin{pmatrix}8 & -2\\ 0 & 1\end{pmatrix}\begin{pmatrix}20 & 3\\ -32 & -4\end{pmatrix} U_0(32),$$

and then to

$$(1+\varpi) \in K^\times (V \cap \widehat{K}^\times),$$
$$V = \begin{pmatrix}7 & 8\\ -1 & -1\end{pmatrix}\begin{pmatrix}8 & 0\\ 0 & 1\end{pmatrix} U_0(32) \begin{pmatrix}8 & 0\\ 0 & 1\end{pmatrix}^{-1}\begin{pmatrix}1 & -2\\ 0 & 1\end{pmatrix}^{-1}.$$

But it is easy to see that $V \cap \widehat{K}^\times = \widehat{\mathcal{O}}_K^{\times(2)} \mathbb{Z}_2^\times (1+\varpi+4\mathcal{O}_2)$ provided that $n \equiv 3 \bmod 4$. Therefore (2.3) is equivalent to

$$1+\varpi \in K^\times \widehat{\mathcal{O}}_K^{\times(2)} \mathbb{Z}_2^\times (1+\varpi+4\mathcal{O}_2),$$

which is obvious.

By Proposition 2.2, $t_{(2,4)} = T\left(\begin{smallmatrix}0 & 1\\ -32 & -16\end{smallmatrix}\right)$. Thus the relation $P^{\sigma_{\varpi'}} - P = (2,4)$ is equivalent to

$$\left[w, \varpi(1+\varpi)\begin{pmatrix}8 & -2\\ 0 & 1\end{pmatrix}\right] = \left[w, \begin{pmatrix}8 & -2\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ -32 & -16\end{pmatrix}^{-1}\right]. \tag{2.4}$$

It is further equivalent to,

$$\varpi(1+\varpi)\begin{pmatrix}8 & -2\\ 0 & 1\end{pmatrix} \in K^\times \begin{pmatrix}8 & -2\\ 0 & 1\end{pmatrix}\begin{pmatrix}-16 & -1\\ 32 & 0\end{pmatrix} U_0(32),$$

and then to

$$\varpi(1+\varpi) \in K^\times (V \cap \widehat{K}^\times),$$
$$V = \begin{pmatrix}-6 & -2\\ 1 & 0\end{pmatrix}\begin{pmatrix}8 & 0\\ 0 & 1\end{pmatrix} U_0(32) \begin{pmatrix}8 & 0\\ 0 & 1\end{pmatrix}^{-1}\begin{pmatrix}1 & -2\\ 0 & 1\end{pmatrix}^{-1}.$$

But it is easy to see that $V \cap \widehat{K}^\times = \widehat{\mathcal{O}}_K^{\times(2)} \mathbb{Z}_2^\times (2+\varpi+8\mathcal{O}_2)$. Therefore (2.4) is equivalent to

$$\varpi(1+\varpi) \in K^\times \widehat{\mathcal{O}}_K^{\times(2)} \mathbb{Z}_2^\times (2+\varpi+8\mathcal{O}_2),$$

which is obvious since $n \equiv 3 \bmod 4$. $\square$

Proof of Theorem 2.8. It is clear that $\sqrt{2} \in H$ but $i \notin H$ and that the Galois group $\mathrm{Gal}(H'/H(i)) = \{1, \sigma_{1+\varpi}^2\}$. Thus the item (1) follows from the relation $z^{\sigma_{1+\varpi}} = z + (0,0)$. It is clearly that the relation is equivalent to $f(P^{\sigma_{1+\varpi}} - P - (2i,0)) = 0$ by noting $f((2i,0)) = (0,0)$, which is given in Proposition 2.9.

Note that the point $[i\sqrt{2n}/8]$ is real. Then the complex conjugation of $f(P)$ is $-f(P)$ and therefore the complex conjugation $\overline{z}$ of z is equal to $-z + (1,0)$. Thus we have that for any $t \in \widehat{K}^\times$ fixing i, $\overline{z_t} = \overline{z}^{t^{-1}} = -z_{t^{-1}} + (1,0)$. This proves the item (2).

For item (3), it is enough to show the case with $t = 1$. Now $\sigma_{\varpi'}(\sqrt{2}) = \sigma_\varpi(\sqrt{2}) = [(2n)_2, \mathbb{Q}^{ab}/\mathbb{Q}](\sqrt{2}) = (-1)^{(n^2-1)/8}\sqrt{2}$. By the relation $P^{\sigma_{\varpi'}} - P = (2,4)$ and $f((2,4)) = (1,0)$, we have

$$\begin{aligned} z_{\varpi'} - z &= f(P^{\sigma_{\varpi'}} - P) + (1+\sqrt{2}, 2+\sqrt{2})^{\sigma_\varpi} - (1+\sqrt{2}, 2+\sqrt{2}) \\ &= (1,0) + \begin{cases} (0,0), & \text{if } n \equiv 3 \bmod 8, \\ 0, & \text{if } n \equiv 7 \bmod 8, \end{cases} \end{aligned}$$

which is equal to $(-1,0)$ or $(1,0)$ according to $n \equiv 3 \bmod 8$ or $\equiv 7 \bmod 8$, $\square$

3. Comparison of Heegner points

Let $n = p_0 p_1 \cdots p_k$ be a product of distinct odd primes with $p_i \equiv 1 \bmod 8$ for $1 \le i \le k$ and $p_0 \not\equiv 1 \bmod 8$. Let m_0 be a positive divisor of $2n$ such that $m_0 \equiv 5, 6,$ or $7 \bmod 8$. In this section, we will generalize the construction in Theorem 1.5 to define a point $P^\chi(f) \in E(\mathbb{Q}(\sqrt{m^*}))^-$, where $m^* = (-1)^{(n-1)/2} m$. With n replaced by the odd part n_0 of m_0, this construction gives a point $P^{\chi_0}(f)$ already define in Theorem 1.5 for $n = n_0$. By Gross-Zagier and Kolyvagin, these two points are actually linearly dependent modulo $E[2]$. The main result of this section is a comparison of 2-divisibility of these two points using the generalized Gross-Zagier formula and the 2-divisibility of special values of L-series. The comparison will be a key ingredient in the induction argument of proving Theorem 1.5 in the next section. Let us begin with some notations.

Put

$$K = \mathbb{Q}(\sqrt{-2n}), \qquad K_0 = \mathbb{Q}(\sqrt{-2n_0}),$$

and write η, η_0 for the abelian characters of $\mathbb{Q}$ defining these two quadratic fields. Let $m_0^* = (-1)^{\frac{n_0-1}{2}} m_0$ and we will also consider the two extensions

$$J = K(\sqrt{m_0^*}), \qquad J_0 = K_0(\sqrt{m_0^*})$$

and write χ, χ_0 for the abelian characters of K and K_0, respectively, defining them. These two extensions are both unramified. In fact, it is easy to see that they are contained in genus subfields of K, K_0, respectively. For any non-zero integer d, let us write $L(E^{(d)}, s)$ for the complex L-function of the elliptic curve $E^{(d)} : dy^2 = x^3 - x$ over $\mathbb{Q}$. On the other hand, we write $L(E/K, \chi, s), L(E/K_0, \chi_0, s)$ for the complex L-functions of E over K, K_0, twisted by the characters χ, χ_0, respectively.

Lemma 3.1. *Let $c \in \{1, 2\}$ denote the integer $2n_0/m_0$. Then the following equalities hold:*

$$L(E/K, \chi, s) = L(E^{(cn/n_0)}, s)L(E^{(m_0)}, s),$$
$$L(E/K_0, \chi_0, s) = L(E^{(c)}, s)L(E^{(m_0)}, s).$$

The proof is an immediate consequence of the Artin formalism applied to the L-functions of E for the extensions J, J_0 of $\mathbb{Q}$, which are quartic when $m_0^* \neq -2n$. For example, the first equality follows on noting that the induced character of χ is the sum of the characters defining the two quadratic extensions $\mathbb{Q}(\sqrt{m_0^*})$ and $\mathbb{Q}(\sqrt{-2n/m_0^*})$. We hope that the usefulness of such a Lemma in an inductive argument is immediately clear. Indeed, it is very well known (see [2] p.87) that $L(E^{(c)}, s)$ does not vanish at $s = 1$. Thus $L(E/K, \chi, s)$ and $L(E/K_0, \chi_0, s)$ will have a zero of the same order at $s = 1$ if and only if $L(E^{(cn/n_0)}, s)$ does not vanish at $s = 1$. We note that this latter assertion does not always hold. For example, if we take $n = p_0p_1$, $n_0 = p_0 \equiv 5 \bmod 8$ to be any prime, and $p_1 = 17$, then $2n/n_0 = 34$ and $L(E^{(34)}, s)$ has a zero of order 2 at $s = 1$ (indeed, 34 is the smallest square free congruent number which does not lie in the residue classes of $5, 6, 7 \bmod 8$). Nevertheless, the work of Zhao (See Proposition 3.8) always provides a lower bound of the power of 2 dividing the algebraic part of $L(E^{(cn/n_0)}, 1)$, which is precisely what we will need to carry out an induction argument on k, via the comparison of the heights of two Heegner points on E, which we now construct.

View K as a $\mathbb{Q}$-subalgebra of $M_2(\mathbb{Q})$ via the embedding

$$K \longrightarrow M_{2\times 2}(\mathbb{Q}), \quad a + b\sqrt{-2n}/8 \longmapsto \begin{pmatrix} a & -2nb/64 \\ b & a \end{pmatrix}, \quad \forall a, b \in \mathbb{Q},$$

with which $K^\times$ is a $\mathbb{Q}$-subtorus of $\mathrm{GL}_{2,\mathbb{Q}}$ such that $i\sqrt{2n}/8$ is the unique fixed point of $K^\times$ on the upper half complex plane $\mathcal{H}$. Define a CM point $P \in X_0(32)$ to be $[w/8, 1]$ if $n \equiv 1 \bmod 4$ and $[(w + 2)/8, 1]$ if $n \equiv 3 \bmod 4$. Let $f : X_0(32) \to E$ be a modular parametrization of degree 2 of the elliptic curve $E : y^2 = x^3 - x$. By Theorem 2.4 and 2.8, we have that $f(P) + (1 + \sqrt{2}, 2 + \sqrt{2}) \in E(H(i))$. Thus $f(P) \in E(H(i))$ since $\sqrt{2} \in H(i)$. Here H is the Hilbert class field of K. Define

$$P^{\chi}(f) = \sum_{\sigma \in \mathrm{Gal}(H(i)/K)} f(P)^{\sigma} \chi(\sigma) \in E(K(\sqrt{m_0^*}))^-,$$

where $E(K(\sqrt{m_0^*}))^-$ is the subgroup of points in $E(K(\sqrt{m_0^*}))$ which are mapped to their inverses under the involution of $K(\sqrt{m_0^*})$ over K. Similarly, let $E(\mathbb{Q}(\sqrt{m_0^*}))^-$ denote the subgroup of points in $E(\mathbb{Q}(\sqrt{m_0^*}))$ which are mapped to their inverses under the non-trivial involution of $\mathbb{Q}(\sqrt{m_0^*})$ over $\mathbb{Q}$. Note that χ in this section is the character defining the extension $K(\sqrt{m_0^*})$ over K, but is not the one in the introduction defining $K(\sqrt{m^*})$ if $m_0 \neq m$.

Lemma 3.2. *The point $P^{\chi}(f)$ belongs to $E(\mathbb{Q}(\sqrt{m_0^*}))^-$.*

Proof. Note that when $m_0^* \neq -2n$, the extension $K(\sqrt{m_0^*})$ over $\mathbb{Q}$ is quartic and its Galois group is generated by complex conjugation and the non-trivial element in $\mathrm{Gal}(K(\sqrt{m_0^*})/K)$. In this case, we only need to check that $P^{\chi}(f) \in E(\mathbb{Q}(\sqrt{m_0^*}))$.

If $n \equiv 5 \bmod 8$, then $m_0^* = m_0 = n_0$ is positive. Note that $P = [i\sqrt{2n}/8, 1]$ is defined over $\mathbb{R}$ since $i\sqrt{2n}$ is pure imaginary. Note also that the complex conjugation acts on $\mathrm{Gal}(H(i)/K)$ by the inverse. It follows that $P^{\chi}(f)$ is invariant under complex conjugation, and therefore belongs to $E(\mathbb{Q}(\sqrt{m_0^*}))$.

Now assume $n \equiv 3 \bmod 4$, then $m_0^* = -m_0$. Note that P is the multiplication of a real point by $[i]$ and therefore is mapped to its negative under the complex conjugation. It follows that $P^{\chi}(f)$ is mapped to $-P^{\chi}(f)$ under the complex conjugation. If $m_0 = 2n$, it is now clear that $P^{\chi}(f) \in E(\mathbb{Q}(\sqrt{-m_0}))^-$. When $m_0 \neq 2n$, choose $\sigma \in \mathrm{Gal}(H(i)/K(i))$ mapping $\sqrt{-m_0}$ to $-\sqrt{-m_0}$, then both σ and the complex conjugation take $P^{\chi}(f)$ to $-P^{\chi}(f)$. Therefore their composition fixes $P^{\chi}(f)$ and has fixed field $\mathbb{Q}(\sqrt{-m_0})$ in $K(\sqrt{-m_0})$. This shows that $P^{\chi}(f) \in E(\mathbb{Q}(\sqrt{-m_0}))$. □

Analogously for K_0, let $P_0 \in X_0(32)(K_0^{ab})$ be the point $[\sqrt{-2n_0}/8, 1]$ if $n_0 \equiv 1 \bmod 4$ and $[(\sqrt{-2n_0} + 2)/8, 1]$ if $n_0 \equiv 3 \bmod 4$. Replacing K, P, χ by K_0, P_0, χ_0, we similarly obtain another point $P^{\chi_0}(f) \in E(\mathbb{Q}(\sqrt{m_0^*}))^-$.

The main goal of this section is to compare 2-divisibilities of the two points $P^{\chi}(f)$ and $P^{\chi_0}(f)$ in the group $E(\mathbb{Q}(\sqrt{m_0^*}))^-$, which is given by the following result.

Theorem 3.3. *Let $n = p_0 p_1 \cdots p_k$ and n_0, m, and m_0 be integers as above. Assume that $n_0 = p_0 p_{i_1} \cdots p_{i_{k-s}}$ is a proper divisor of n, i.e. $s > 0$, and that $P^{\chi_0}(f)$ belongs to $2^t E(\mathbb{Q}(\sqrt{m_0^*}))^- + E[2]$ for some integer $t \geq 0$. Then*

$$P^{\chi}(f) \in 2^{t+s+1} E(\mathbb{Q}(\sqrt{m_0^*}))^- + E[2].$$

The proof of Theorem 3.3 is divided into three steps. First, reduce the comparison of the two points in Mordell-Weil group to the comparison of their heights via Kolyvagin's result; second, further reduce to the comparison of two Special L-values via generalized Gross-Zagier formula; third, estimate 2-adic valuations of these special L-values.

Proposition 3.4. *If either $P^{\chi_0}(f)$ or $P^{\chi}(f)$ is not torsion, then $E(\mathbb{Q}(\sqrt{m_0^*}))^- \otimes_{\mathbb{Z}} \mathbb{Q}$ is one dimensional $\mathbb{Q}$-vector space. In this case, the ratio $[P^{\chi}(f) : P^{\chi_0}(f)] \in \mathbb{Q} \cup \{\infty\}$ of the two points in this one dimensional space is given by*

$$[P^{\chi}(f) : P^{\chi_0}(f)]^2 = [\widehat{h}(P^{\chi}(f)) : \widehat{h}(P^{\chi_0}(f))], \tag{3.1}$$

where $\widehat{h} : E(\bar{\mathbb{Q}}) \to \mathbb{R}$ denotes the Néron-Tate height function.

Proof. Note that Heegner hypothesis is not satisfied for (E, K, χ), but one can still use Kolyvagin's Euler system method to see that $E(K(\sqrt{m_0^*}))^-$ is of rank one if $P^{\chi}(f)$ is not torsion (for example, see Theorem 3.2 of [20]) and therefore $E(\mathbb{Q}(\sqrt{m_0^*}))^-$ is of rank one by Lemma 3.2. Another argument with Kolyvagin's original result is as follows. Using the generalized Gross-Zagier formula (Theorem 1.2 in [27]), we know the L-series $L(s, E, \chi) = L(s, E^{(2n/m_0)}) L(s, E^{(m_0)})$ has vanishing order 1 at the central point $s = 1$. Considering ϵ-factors, we then know that $L(s, E^{(m_0)})$ has vanishing order 1 at $s = 1$. Taking an imaginary quadratic field K' such that the Heegner hypothesis is satisfied for $(E^{(m_0)}, K')$ and $L(s, E_{K'}^{(m_0)})$ has vanishing order 1 at $s = 1$, then Kolyvagin's original result shows that $E^{(m_0)}(\mathbb{Q}) \cong E(\mathbb{Q}(\sqrt{m_0^*}))^-$ is of rank one. Similarly, if $P^{\chi_0}(f)$ is not torsion then $E(\mathbb{Q}(\sqrt{m_0^*}))^-$ is of rank one.

The equality (3.1) now follows from the fact that the height function $\widehat{h}$ is quadratic. ☐

Using the generalized Gross-Zagier formula (Theorem 1.2 in [27]), we further express this ratio in term of special L-values. For any square-free integer $d \geq 1$, let $\Omega^{(d)}$ denote the real period of $E^{(d)}$, defined by

$$\Omega^{(d)} := \frac{2}{\sqrt{d}} \int_1^{\infty} \frac{dx}{\sqrt{x^3 - x}}.$$

It is known that the algebraic part of L-values

$$L^{\mathrm{alg}}(E^{(d)},1) := L(E^{(d)},1)/\Omega^{(d)}$$

is a rational number. Note again that $L^{\mathrm{alg}}(E^{(c)},1) \neq 0$ for $c=1$ and 2.

Proposition 3.5. *We have that*

$$\widehat{h}(P^{\chi}(f)) = \frac{L^{\mathrm{alg}}(E^{(cn/n_0)},1)}{L^{\mathrm{alg}}(E^{(c)},1)} \cdot \widehat{h}(P_0^{\chi_0}(f)). \tag{3.2}$$

Remark 3.6. In the proof of this proposition, we will use the language of automorphic representation. Let $\pi^{(d)}$ denote the automorphic representation associated to the elliptic curve $E^{(d)}$. Let $L(s,\pi^{(d)})$ denote its complete L-series and $L^{(\infty)}(s,\pi^{(d)})$ its finite part. Then

$$L^{(\infty)}\big(s,\pi^{(d)}\big) = L\Big(E^{(d)}, s+\frac{1}{2}\Big).$$

Moreover, we have that

$$\frac{L^{\mathrm{alg}}(E^{(cn/n_0)},1)}{L^{\mathrm{alg}}(E^{(c)},1)} = \frac{L(1/2,\pi^{(cn/n_0)})/\Omega^{(cn/n_0)}}{L(1/2,\pi^{(c)})/\Omega^{(c)}}.$$

Before the proof of this proposition, we need to recall the generalized Gross-Zagier formula in [27].

Let $G=\mathrm{GL}_{2,\mathbb{Q}}$. Let $X = \varprojlim_U X_U$ be the projective limit of modular curves indexed by open compact subgroups $U \subset G(\mathbb{A}_f)$. Let $\xi=(\xi_U)$ be the compatible system of Hodge classes such that ξ_U is represented by ∞ on each geometric irreducible component of X_U. For the elliptic curve $E: y^2=x^3-x$, define

$$\pi_E := \mathrm{Hom}^0_{\xi}(X,E) := \varinjlim_U \mathrm{Hom}^0_{\xi_U}(X_U,E)$$

where $\mathrm{Hom}^0_{\xi_U}(X_U,E)$ is the group of the morphisms f in $\mathrm{Hom}_{\mathbb{Q}}(X_U,E)\otimes\mathbb{Q}$ satisfying $f(\infty)=0$. The $\mathbb{Q}$-vector space π_E is endowed with the natural $G(\mathbb{A}_f)$-structure. Let $\mathbb{H}$ be the division quaternion algebra over $\mathbb{R}$ and let $\pi_\infty=\mathbb{Q}$ be the trivial representation of $\mathbb{H}^\times$. Then the representation $\pi=\pi_E$ is a restricted tensor product $\pi=\otimes_{v\le\infty}\pi_v$ (with respect to a spherical family f_v°) as a representation of the incoherent group $\mathbb{G}=G(\mathbb{A}_f)\times\mathbb{H}^\times$. We call π_E the rational automorphic representation associated to the elliptic curve E.

The representation $\pi = \pi_E$ is self-dual via the perfect $\mathbb{G}$-invariant pairing

$$(\ , \ ) : \pi \times \pi \longrightarrow \mathbb{Q}$$

given by

$$(f_1, f_2) = \mathrm{Vol}(X_U)^{-1} f_{1,U} \circ f_{2,U}^{\vee}, \qquad \mathrm{Vol}(X_U) = \int_{X_U(\mathbb{C})} \frac{dxdy}{2\pi y^2}$$

where f_i is represented by $f_{i,U} \in \mathrm{Hom}_{\xi_U}(X_U, E) = \mathrm{Hom}^0(J_U, E)$ with J_U the Jacobian of X_U, and $f_{2,U}^{\vee} : E \to J_U$ is the dual of $f_{2,U}$ so that $f_{1,U} \circ f_{2,U}^{\vee} \in \mathbb{Q} = \mathrm{End}^0(E)$. For each place v, let $(\ , \ )_v$ be a $G(\mathbb{Q}_v)$-invariant pairing such that for almost all unramified $v \nmid \infty$, $(f_v^0, f_v^0)_v = 1$ and such that for $f = \otimes_v f_v \in \pi_E$, $(f, f) = \prod_v (f_v, f_v)_v$.

Let $\eta : \widehat{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \to \{\pm 1\}$ be the character associated to the quadratic extension $K/\mathbb{Q}$. Let $K^1 = K^{\times}/\mathbb{Q}^{\times}$. Fix a Haar measure dt_v on $K^1(\mathbb{Q}_v) = K_v^{\times}/\mathbb{Q}_v^{\times}$ for each place v of $\mathbb{Q}$ such that the product measure over all v is the Tamagawa measure on $K^1 \backslash K^1(\mathbb{A})$ multiplied by $L(1, \eta)$. Define

$$\beta_v(f_v) = \frac{L(1, \eta_v) L(1, \pi_v, \mathrm{ad})}{\zeta_{\mathbb{Q}_v}(2) L(1/2, \pi_v, \chi_v)} \int_{K_v^{\times}/\mathbb{Q}_v^{\times}} (\pi_v(t) f_v, f_v)_v \chi_v(t) dt_v.$$

The Gross-Zagier formula ([27] Theorem 1.2) says:

$$(3.3) \quad (2h_K)^{-2} \widehat{h}(P^{\chi}(f)) = \frac{\zeta_{\mathbb{Q}}(2) L'(1/2, \pi, \chi)}{4L(1, \eta)^2 L(1, \pi, \mathrm{ad})} \prod_v \beta_v(f_v), \quad \forall\ f = \otimes_v f_v$$

where all L-functions, including $\zeta_{\mathbb{Q}}$, are all complete L-series and $L(s, \pi, \chi)$ (resp $L(s, \pi, \mathrm{ad})$) is L-series defined for Jacquet-Langlands lift of π, and h_K is the ideal class number of K. Similarly,

$$(3.4) \quad (2h_{K_0})^{-2} \widehat{h}(P^{\chi_0}(f)) = \frac{\zeta_{\mathbb{Q}}(2) L'(1/2, \pi, \chi_0)}{4L(1, \eta_0)^2 L(1, \pi, \mathrm{ad})} \prod_v \beta_{0,v}(f_v), \quad \forall\ f = \otimes_v f_v$$

where the subscript 0 corresponds to $K_0 = \mathbb{Q}(\sqrt{-2n_0})$.

We use the formulae (3.3) and (3.4) to compute the ratio of $P^{\chi}(f)$ and $P_0^{\chi_0}(f)$. It is more convenient to fix Haar measures as follows (which are used in [27]).

- for each place v of $\mathbb{Q}$, the Haar measure dx_v on $\mathbb{Q}_v$ is self dual with respect to the standard additive character ψ_v on $\mathbb{Q}_v$: $\psi_\infty(x) = e^{2\pi i x}$ and

$\psi_v(x) = e^{-2\pi i \iota_v(x)}$ for $v \nmid \infty$ where $\iota_v : \mathbb{Q}_v/\mathbb{Z}_v \to \mathbb{Q}/\mathbb{Z}$ is the natural embedding. The Haar measure $dx_v^\times$ on $\mathbb{Q}_v^\times$ is given by $\zeta_{\mathbb{Q}_v}(1)|x|_v^{-1}dx_v$, where $|\ |_v$ is the normalized absolute value on $\mathbb{Q}_v$.

- the Haar measure dy on K_v is such that the Fourier transform

$$\widehat{\Phi}(x) = \int_{K_v} \Phi(y)\psi_v(\langle x, y\rangle)dy$$

satisfies $\widehat{\widehat{\Phi}}(x) = \Phi(-x)$ where the pairing is

$$\langle x, y\rangle = \mathrm{N}_{K_v/\mathbb{Q}_v}(x+y) - \mathrm{N}_{K_v/\mathbb{Q}_v}(x) - \mathrm{N}_{K_v/\mathbb{Q}_v}(y).$$

The Haar measure $d^\times y$ on $K_v^\times$ is given by

$$d^\times y = \zeta_{K_v}(1)|\mathrm{N}_{K_v/\mathbb{Q}_v}(y)|_v^{-1}dy$$

where $\zeta_{K_v}(s) = \zeta_{\mathbb{Q}_v}(s)^2$ for v splits in K. For any $v \nmid \infty$, let D be the discriminant of K_v in $\mathbb{Z}_p$, then

$$\mathrm{Vol}(\mathcal{O}_{K_v}, dy) = \mathrm{Vol}(\mathcal{O}_{K_v^\times}, d^\times x) = |D|_v^{1/2}.$$

- take the quotient Haar measure dt_v on $K_v^1 = K_v^\times/\mathbb{Q}_v^\times$ and the product Haar measure $\otimes_v dt_v$ on $K^1(\mathbb{A})$ such that the total volume of $K^1(\mathbb{Q})\backslash K^1(\mathbb{A})$ is equal to $2L(1,\eta)$. Then these measures satisfy the requirement in the Gross-Zagier formula above. Then

$$\mathrm{Vol}(K_v^1, dt_v) = \begin{cases} 2, & \text{if } v = \infty, \\ 1, & \text{if } v \text{ is inert in } K, \\ 2|D|_v^{1/2}, & \text{if } K_v/\mathbb{Q}_p \text{ is ramified.} \end{cases}$$

Lemma 3.7. *Let $f : X_0(32) \to E$ be a degree 2 modular parametrization. With the above fixed Haar measure, we have*

$$\beta_v(f_v)/\beta_{0,v}(f_v) = \begin{cases} p^{-1/2}, & \textit{if } v = p \Big| \dfrac{n}{n_0}, \\ 1, & \textit{otherwise.} \end{cases}$$

Proof. Note that $\beta_v(f_v)/(f_v, f_v) = 1$ in the following spherical case: $K_v/\mathbb{Q}_v$, π_v, χ_v are all unramified and $f \in \pi^{G(\mathbb{Z}_v)}$ and $\mathcal{O}_{K_v}^\times/\mathbb{Z}_v^\times$ has volume one. Thus

$$\beta_v(f_v)/(f_v, f_v) = 1,\ \forall v \nmid 2n\infty, \qquad \beta_{0,v}(f_v)/(f_v, f_v) = 1,\ \forall v \nmid 2n_0\infty$$

and therefore $\beta_v(f_v)\big/\beta_{0,v}(f_v) = 1$ for any $v \nmid 2n\infty$.

Now let p be an odd prime. Then π_p is unramified and f_p is a non-zero (spherical) vector in the one-dimensional space $\pi_p^{G(\mathbb{Z}_p)}$. Then the normalized matrix coefficient

$$\Psi_p(g) := (\pi_p(g)f_p, f_p)/(f_p, f_p), \qquad g \in G(\mathbb{Q}_p)$$

is bi-$G(\mathbb{Z}_p)$-invariant and satisfies the Macdonald formula (See [3] Theorem 4.6.6):

$$\Psi_p\left(\begin{pmatrix} p^m & \\ & 1 \end{pmatrix}\right) = \frac{p^{-m/2}}{1+p^{-1}}\left(\alpha^m \frac{1-p^{-1}\alpha^{-2}}{1-\alpha^{-2}} + \alpha^{-m}\frac{1-p^{-1}\alpha^2}{1-\alpha^2}\right), \quad m \geq 0.$$

Here (α, α^{-1}) are the Satake parameters of π_p.

For $p|n$ which is then ramified in K and ϖ_p a uniformizer of K_p, using the above formula and the decomposition

$$K_p^\times/\mathbb{Q}_p^\times = (\mathcal{O}_{K_p}^\times/\mathbb{Z}_p^\times) \cup (\varpi_p \mathcal{O}_{K_p}^\times/\mathbb{Z}_p^\times), \quad \varpi_p = \sqrt{-2n} \in G(\mathbb{Z}_p)\begin{pmatrix} p & \\ & 1 \end{pmatrix} G(\mathbb{Z}_p),$$

we compute the integral

$$\begin{aligned}\int_{K_p^\times/\mathbb{Q}_p^\times} \Psi_p(t)\chi_p(t)dt &= (1+\Psi_p(\varpi_p)\chi_p(\varpi_p))\,\mathrm{Vol}(\mathcal{O}_{K_p}^\times/\mathbb{Z}_p^\times) \\ &= \frac{\mathrm{Vol}(\mathcal{O}_{K_p}^\times/\mathbb{Z}_p^\times)}{1+p^{-1}} \cdot \left(1+\alpha\chi_p(\varpi_p)p^{-1/2}\right) \\ &\quad \cdot \left(1+\alpha^{-1}\chi_p(\varpi_p)p^{-1/2}\right)\end{aligned}$$

By the following formula for local factors:

$$\begin{aligned} L(1,\pi_p,\mathrm{ad}) &= (1-\alpha^2 p^{-1})^{-1}(1-\alpha^{-2}p^{-1})^{-1}(1-p^{-1})^{-1} \\ L(1/2,\pi_p,\chi_p) &= (1-\alpha\chi_p(\varpi)p^{-1/2})^{-1}(1-\alpha^{-1}\chi_p(\varpi)p^{-1/2})^{-1}, \end{aligned}$$

we have

$$\begin{aligned}\frac{\beta_p(f_p)}{(f_p,f_p)} &= \frac{L(1,\eta_p)L(1,\pi_p,\mathrm{ad})}{\zeta_{\mathbb{Q}_p}(2)L(1/2,\pi_p,\chi_p)} \cdot \int_{K_p^\times/\mathbb{Q}_p^\times} \Psi_p(t)\chi_p(t)dt \\ &= \mathrm{Vol}(\mathcal{O}_{K_p}^\times/\mathbb{Z}_p^\times) = p^{-1/2}.\end{aligned}$$

It follows that $\beta_p(f_p)/\beta_{0,p}(f_p) = p^{-1/2}$ for each $p|(n/n_0)$ and $= 1$ for all $p \nmid 2\infty n/n_0$. But $n/n_0 \equiv 1 \bmod 8$ implies that $n/n_0 = \gamma^2$ for some $\gamma \in \mathbb{Q}_2^\times$, i.e. $K_2 \simeq K_{0,2}$. Note that f_2 is a new vector in π_2, i.e. invariant under the 2-component $U_0(32)_2$ of $U_0(32)$ and that the two embeddings of $K_2^\times = K_{0,2}^\times$ into $\mathrm{GL}_2(\mathbb{Q}_2)$ are conjugate by $\begin{pmatrix} 1 & \\ & \gamma \end{pmatrix} \in U_0(32)_2$. Now it is easy to see that $\beta_2(f_2)/\beta_{0,2}(f_2) = 1$. Note that $\pi_\infty = \mathbb{Q}$ is the trivial representation of $\mathbb{H}^\times$, one can also easily check that $\beta_\infty(f_\infty)/\beta_{0,\infty}(f_\infty) = 1$. □

Proof of Proposition 3.5. Recall that for a non-zero integer square-free d, we denote by $\pi^{(d)}$ the automorphic representation corresponding to the elliptic curve $E^{(d)} : dy^2 = x^3 - x$. Then $\pi^{(d)} = \pi^{(-d)}$ and by Lemma 3.1,

$$L(s, \pi, \chi) = L(s, \pi^{(m_0)})L(s, \pi^{(cn/n_0)}), \quad L(s, \pi, \chi_0) = L(s, \pi^{(m_0)})L(s, \pi^{(c)}).$$

Note that the functional equation of $L(s, \pi^{(m_0)})$ (resp. $L(s, \pi^{(2n/m_0)})$) has sign -1 (resp. 1) since $m_0 \equiv m \equiv 5, 6,$ or $7 \bmod 8$ by our assumption. Thus

$$L'(1/2, \pi, \chi)/L'(1/2, \pi, \chi_0) = L(1/2, \pi^{(cn/n_0)})/L(1/2, \pi^{(c)}).$$

Since the special value $L(1/2, \pi^{(c)}) \neq 0$ for $c = 1, 2$, thus $P_0^{\chi_0}(f)$ is torsion if and only if $L'(1/2, \pi^{(m_0)}) = 0$. It follows that if $P^{\chi_0}(f)$ is torsion then $P^\chi(f)$ is torsion. By the class number formula for imaginary quadratic fields, we have that the special value of L-series removed infinite factor

$$L^{(\infty)}(1, \eta) = \pi h_K/\sqrt{8n}, \qquad L^{(\infty)}(1, \eta_0) = \pi h_{K_0}/\sqrt{8n_0},$$

where $L^{(\infty)}$ denotes the L-functions with the factor at infinity removed. Putting everything together, we have that

$$\begin{aligned} \frac{\widehat{h}(P^\chi(f))}{\widehat{h}(P^{\chi_0}(f))} &= \frac{L'(1/2, \pi, \chi)}{L'(1/2, \pi, \chi_0)} \cdot \frac{h_{K_0}^{-2} L(1, \eta_0)^2}{h_K^{-2} L(1, \eta)^2} \cdot \prod_{v|\infty 2n} \frac{\beta_v(f)}{\beta_{0,v}(f)} \\ &= \frac{L(1/2, \pi^{(cn/n_0)})}{L(1/2, \pi^{(c)})} \cdot \frac{n}{n_0} \cdot \prod_{p|(n/n_0)} p^{-1/2} \\ &= \frac{L(1/2, \pi^{(cn/n_0)})/\Omega^{(cn/n_0)}}{L(1/2, \pi^{(c)})/\Omega^{(c)}} = \frac{L^{\mathrm{alg}}(E^{(cn/n_0)}, 1)}{L^{\mathrm{alg}}(E^{(c)}, 1)}, \end{aligned}$$

which completes the proof of Proposition 3.5. □

We have the following estimation of the 2-adic valuation of $L^{\mathrm{alg}}(E^{(cn/n_0)}, 1)$. Note that all prime divisor of n/n_0 are congruent to 1 modulo 8.

Proposition 3.8 (Zhao [28], [29]). *Let $s \geq 1$ be an integer and let $m = p_1 \cdots p_s$ be a product of distinct primes $p_i \equiv 1 \bmod 8$. Then*

1. *the 2-adic additive valuation of $L^{\mathrm{alg}}(E^{(2m)}, 1)$ is not less than $2s - 1$.*
2. *the 2-adic additive valuation of $L^{\mathrm{alg}}(E^{(m)}, 1)$ is not less than $2s-1$ and the equality holds if and only if the ideal class group $\mathcal{A}$ of $\mathbb{Q}(\sqrt{-2m})$ satisfies that $\dim_{\mathbb{F}_2} \mathcal{A}[4]/\mathcal{A}[2] = 1$ and $(\frac{2}{m})_4 \cdot (-1)^{(m-1)/8} = -1$.*

Proof. By Corollary 2 in [28], for any m a product of s distinct odd primes $p_i \equiv 1 \bmod 4$, the 2-adic valuation of $L^{\mathrm{alg}}(E^{(2m)}, 1)$ is not less than $2s - 2$ and is equal to $2s - 2$ if and only if there are exactly an odd number of spanning subtrees in the graph $\widetilde{G}_{-m}$ whose vertices are $-1, p_1, \ldots, p_s$ and whose edges are those $(-1, p_i)$ with $p_i \equiv 5 \bmod 8$ and those $(p_i, p_j), i \neq j$, with $(\frac{p_i}{p_j}) = -1$. Since all primes p_i in the proposition are $\equiv 1 \bmod 8$, the graph $\widetilde{G}_{-m}$ is not connected so that the 2-adic valuation can not reach the lower bound $2s - 2$ and therefore (1) follows. The statement (2) is just Theorem 1 in [29]. □

It is known that the 2-adic valuations of $L^{\mathrm{alg}}(E^{(1)}, 1)$ and $L^{\mathrm{alg}}(E^{(2)}, 1)$ are -3 and -2, respectively (See [2] p.87). In fact, it is also known that the full BSD conjecture holds for $E^{(1)}$ and $E^{(2)}$.

Now Theorem 3.3 follows from Propositions 3.4, 3.5, and 3.8.

4. Induction argument on quadratic twists

We now prove Theorem 1.5 by induction on k. Recall that a non-zero integer m is a congruent number if and only if the Mordell-Weil group $E^{(m)}(\mathbb{Q})$ of the elliptic curve $E^{(m)} : my^2 = x^3 - x$ has rank greater than zero. Note that $E^{(m)} \cong E^{(-m)}$ only depends on the square-free part of m. Let $n = p_0 p_1 \cdots p_k$ be a product of distinct odd primes with $k \geq 0$, $m = n$ or $2n$ such that $m \equiv 5, 6$, or $7 \bmod 8$, and $m^* = (-1)^{(n-1)/2} m$. It is known that $E^{(m)}(\mathbb{Q}) \cong E(\mathbb{Q}(\sqrt{m^*}))^-$, where $E(\mathbb{Q}(\sqrt{m^*}))^-$ is the group of points $P \in E(\mathbb{Q}(\sqrt{m^*}))$ such that $P^\sigma = -P$ where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{m^*})/\mathbb{Q})$ is the non-trivial element. Note that the torsion subgroup of $E(\mathbb{Q}(\sqrt{m^*}))^-$ is $E[2]$. Thus m is congruent if we can construct a point $y \in E(\mathbb{Q}(\sqrt{m^*}))^- \setminus E[2]$. In this section, we will show the Heegner divisor $P^\chi(f) \in E(\mathbb{Q}(\sqrt{m^*}))^-$ defined in section 3 is of infinite order for n satisfying the condition (1.1) in Theorem 1.3 and the abelian character $\chi : \mathrm{Gal}(H(i)/K) \to \{\pm 1\}$ defining the extension $K(\sqrt{m^*})$ over K. In fact, to prove the non-triviality of $P^\chi(f)$, we will construct a point $y_m \in E(\mathbb{Q}(\sqrt{m^*}))$ following Monsky [19] which satisfies $4y_m = P^\chi(f)$, and study its 2-divisibility.

Recall that $K = \mathbb{Q}(\sqrt{-2n})$ and $\varpi = \sqrt{-2n} \in K_2^\times$ is a uniformizer at 2.

4.1. The case $n \equiv 1 \bmod 4$

We first handle the case with $p_0 \equiv 5 \bmod 8$. In this case, $m = n$ and the condition (1.1) in Theorem 1.3 says that the ideal class group $\mathcal{A}$ of $K = \mathbb{Q}(\sqrt{-2n})$ has no order 4 elements, or equivalently that $2\mathcal{A} \cong \mathrm{Gal}(H/H_0)$ has odd cardinality.

Let $P \in X_0(32)$ be the image of $i\sqrt{2n}/8$ under the complex uniformization of $X_0(32) \cong \Gamma_0(32)\backslash(\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}))$. Let $f : X_0(32) \to E$ be a degree 2 modular parametrization. Define

$$z = f(P) + (1 + \sqrt{2}, 2 + \sqrt{2}) \in E(K^{ab})$$

which is actually defined over H by Theorem 2.4, and define

$$y_n = \mathrm{Tr}_{H/K(\sqrt{n})} z \in E(K(\sqrt{n})), \tag{4.1}$$

which is our desired point. It turns out that $4y_n = P^\chi(f)$, the point we defined in Theorem 1.5 and studied in section 3.

Theorem 4.1. *Let $k \geq 0$ be an integer and $n = p_0 p_1 \cdots p_k$ a product of distinct primes with $p_0 \equiv 5 \bmod 8$ and $p_1, \ldots, p_k \equiv 1 \bmod 8$. Then the point*

$$y_n := \mathrm{Tr}_{H/K(\sqrt{n})} z$$

is actually defined over $\mathbb{Q}(\sqrt{n})$ and belongs to $2^{k-1}E(\mathbb{Q}(\sqrt{n}))^- + E[2]$. Moreover, the point $y_n \notin 2^k E(\mathbb{Q}(\sqrt{n}))^- + E[2]$ if the ideal class group of $K = \mathbb{Q}(\sqrt{-2n})$ does not contain any element of order 4.

We start with the case $k = 0$, where the statement $y_n \in 2^{-1}E(\mathbb{Q}(\sqrt{n}))^- + E[2]$ in the theorem is understood as $2y_n \in E(\mathbb{Q}(\sqrt{n}))^-$. When $k = 0$ the above theorem is due to Monsky [19]:

Proposition 4.2. *Let $n = p_0 \equiv 5 \bmod 8$ be a prime. Then the point y_{p_0} satisfies:*

$$\begin{aligned} y_{p_0} &\in E(\mathbb{Q}(\sqrt{p_0})) \setminus E(\mathbb{Q}(\sqrt{p_0}))^- \quad \textit{and} \\ 2y_{p_0} &\in E(\mathbb{Q}(\sqrt{p_0}))^- \setminus \left(2E(\mathbb{Q}(\sqrt{p_0}))^- + E[2]\right). \end{aligned}$$

In particular, $2y_{p_0} \in E(\mathbb{Q}(\sqrt{p_0}))^-$ is of infinite order and therefore p_0 is a congruent number.

Proof. In this case $K(\sqrt{p_0}) = H_0$ and the ideal class group $\mathcal{A}$ of $K = \mathbb{Q}(\sqrt{-2p_0})$ satisfies that $2\mathcal{A} \cong \mathrm{Gal}(H/H_0)$ has odd cardinality. Note that the action of the complex conjugation on $\mathrm{Gal}(H/K)$ is given by inverse and $\mathrm{Gal}(H/K(\sqrt{p_0}))$ is stable under this action. It follows that the point $y_{p_0} = \mathrm{Tr}_{H/K(\sqrt{p_0})} z$ is fixed by the action of complex conjugation and therefore $y_{p_0} \in E(\mathbb{Q}(\sqrt{p_0}))$.

For any $t \in \widehat{K}^\times$, we have that $z_{\varpi t} + z_t = (0,0)$ by Theorem 2.4 (3). Thus

$$y_{p_0} + y_{p_0}^{\sigma_\varpi} = \#\mathrm{Gal}(H/K(\sqrt{p_0})) \cdot (0,0) = \#2\mathcal{A} \cdot (0,0) = (0,0).$$

Since

$$\sigma_\varpi(\sqrt{p_0}) = [(2p_0)_2, \mathbb{Q}^{ab}/\mathbb{Q}](\sqrt{p_0}) = [2_2, \mathbb{Q}^{ab}/\mathbb{Q}](\sqrt{p_0}) = \left(\frac{2}{p_0}\right)\sqrt{p_0} = -\sqrt{p_0},$$

σ_ϖ acts on $K(\sqrt{p_0})$ non-trivially, thus $2y_{p_0} \in E(\mathbb{Q}(\sqrt{p_0}))^-$ but $y_{p_0} \notin E(\mathbb{Q}(\sqrt{p_0}))^-$.

Suppose that $2y_{p_0} \in 2E(\mathbb{Q}(\sqrt{p_0}))^- + E[2]$, say, $2y_{p_0} = 2y' + t$ for some $y' \in E(\mathbb{Q}(\sqrt{p_0}))^-$ and $t \in E[2]$. Then we have that $2(y_{p_0} - y') = t$. Thus $y_{p_0} - y' \in E[4] \cap E(\mathbb{Q}(\sqrt{p_0})) = E[2]$ and then $y_{p_0} \in y' + E[2] \subset E(\mathbb{Q}(\sqrt{p_0}))^-$, a contradiction. In particular, $2y_{p_0} \in E(\mathbb{Q}(\sqrt{p_0}))^-$ is of infinite order and therefore p_0 is a congruent number. □

For each positive divisor d of n divisible by p_0, define

$$y_d := \mathrm{Tr}_{H/K(\sqrt{d})} z \in E(K(\sqrt{d})).$$

Define $y_0 = \mathrm{Tr}_{H/H_0} z \in E(H_0)$.

Lemma 4.3. *Assume $k \geq 1$ and let $\varpi \in K_2^\times$ be the uniformizer $\sqrt{-2n}$. Then*

1. *the point $y_d \in E(\mathbb{Q}(\sqrt{d}))^-$ for each d with $p_0|d|n$.*
2. *the point $y_0 \in E(H_0^+)$, where $H_0^+ = H_0 \cap \mathbb{R} = \mathbb{Q}(\sqrt{p_0}, \ldots, \sqrt{p_k})$, satisfies:*

$$y_0 + y_0^{\sigma_\varpi} = \#2\mathcal{A} \cdot (0,0). \tag{4.2}$$

Moreover these points satisfy the following relation:

$$\sum_{p_0|d|n} y_d = \begin{cases} 2^k y_0, & \text{if } k \geq 2, \\ 2^k y_0 + \#2\mathcal{A} \cdot (0,0), & \text{if } k = 1. \end{cases} \tag{4.3}$$

Proof. Similar to Proposition 4.2, for each d with $p_0|d|n$, $\mathrm{Gal}(H/K(\sqrt{d}))$ is stable under the action of the complex conjugation and therefore $y_d \in E(\mathbb{Q}(\sqrt{d}))$. Moreover, by Theorem 2.4,

$$y_d + y_d^{\sigma_\varpi} = \#\mathrm{Gal}(H/K(\sqrt{d})) \cdot (0,0) = 0$$

since the cardinality of $\mathcal{A}[2]$ is 2^{k+1} and thus $\mathrm{Gal}(H/K(\sqrt{d}))$ has even cardinality $\#2\mathcal{A} \cdot 2^k$. Similarly, y_0 is invariant under the complex conjugation so that $y_0 \in E(H_0^+)$ and satisfies the relation (4.2).

Note that any element σ in $\mathrm{Gal}(H_0/K)$ maps $\sqrt{p_i}$ to $\pm\sqrt{p_i}$ for $0 \le i \le k$, Note also that $\sigma \in \mathrm{Gal}(H_0/K(\sqrt{d}))$ if and only if the cardinality of $\{p|d, \sigma(\sqrt{p}) = -\sqrt{p}\}$ is even. For any $1 \neq \sigma \in \mathrm{Gal}(H_0/K)$, let $n_\sigma = \#\{d, p_0|d|n, \sigma \in \mathrm{Gal}(H_0/K(\sqrt{d}))\}$. Note that $\sigma_\varpi(\sqrt{p_0}) = -\sqrt{p_0}$ and $\sigma_\varpi\sqrt{p_i} = \sqrt{p_i}$ for all $1 \le i \le k$. If $1 \neq \sigma \in \mathrm{Gal}(H/K)$ fixes $\sqrt{p_0}$ and changes exact s elements among $\sqrt{p_1}, \dots, \sqrt{p_k}$, then $n_\sigma = 2^{k-s}\left[\binom{s}{0} + \binom{s}{2} + \cdots +\right] = 2^{k-1}$ and $n_{\sigma\sigma_\varpi} = 2^{k-s}\left[\binom{s}{1} + \binom{s}{3} + \cdots\right] = 2^{k-1}$. Thus

$$\begin{aligned}
\sum_{p_0|d|n} y_d - 2^k y_0 &= \sum_{p_0|d|n} (y_d - y_0) = \sum_{p_0|d|n} \sum_{1\neq\sigma\in\mathrm{Gal}(H_0/K(\sqrt{d}))} y_0^\sigma \\
&= \sum_{1\neq\sigma\in\mathrm{Gal}(H_0/K)} n_\sigma y_0^\sigma \\
&= \sum_{1\neq\sigma,\sigma \text{ fixing } \sqrt{p_0}} (n_\sigma y_0^\sigma + n_{\sigma\sigma_\varpi} y_0^{\sigma\sigma_\varpi}) \\
&= 2^{k-1}(2^k - 1)\#2\mathcal{A} \cdot (0,0).
\end{aligned}$$

The equality (4.3) now follows. □

Proof of Theorem 4.1. We do induction on k. It holds when $k = 0$ by Proposition 4.2. Now assume $k \ge 1$. By Lemma 4.3, we now have

$$y_n + \sum_{p_0|d|n, d\neq n} y_d = 2^k y_0 \bmod E[2]. \tag{4.4}$$

For each d with $p_0|d|n, d \neq n$, let y_d^0 be the point constructed similarly with $\mathbb{Q}(\sqrt{-2n})$ replaced by $\mathbb{Q}(\sqrt{-2d})$. Then $4y_d, 4y_d^0$ are $P^\chi(f)$ and $P^{\chi_0}(f)$ in section 3, respectively. If y_d^0 is torsion, so is y_d. If y_d^0 is not torsion, then the ratio of y_d to y_d^0 in the one dimensional $\mathbb{Q}$-vector space $E(\mathbb{Q}(\sqrt{d}))^- \otimes_\mathbb{Z} \mathbb{Q}$ is $[y_d : y_d^0] = [P^\chi(f) : P^{\chi_0}(f)]$. By induction hypothesis and Theorem 3.3, we know that $y_d \in 2^k E(\mathbb{Q}(\sqrt{d}))^- + E[2]$.

Now write $y_d = 2^k y'_d + t_d$ with $y'_d \in E(\mathbb{Q}(\sqrt{d}))^-$ and $t_d \in E[2]$. Then by (4.4) we have that

$$y_n = 2^k \left(y_0 - \sum_{p_0|d|n, d \neq n} y'_d \right) + t \tag{4.5}$$

for some $t \in E[2]$. Note any proper sub-extension of $H_0^+/\mathbb{Q}$ must be ramified at some odd prime. Thus

$$E[2^\infty] \cap E(H_0^+) = E[2].$$

Consider the (injective) Kummer map

$$E(\mathbb{Q}(\sqrt{n}))/2^{k+1}E(\mathbb{Q}(\sqrt{n})) \longrightarrow H^1(\mathbb{Q}(\sqrt{n}), E[2^{k+1}]),$$

and the exact inflation-restriction sequence

$$\begin{aligned} 1 \longrightarrow H^1(\mathrm{Gal}(H_0^+/\mathbb{Q}(\sqrt{n})), E[2]) \longrightarrow H^1(\mathbb{Q}(\sqrt{n}), E[2^{k+1}]) \\ \longrightarrow H^1(H_0^+, E[2^{k+1}]). \end{aligned}$$

Since $2y_n = 2^{k+1}(y_0 - \sum_{p_0|d|n, d \neq n} y'_d)$ with $y_0 - \sum_{p_0|d|n, d\neq n} y'_d \in E(H_0^+)$, we know that the image of $2y_n$ in the Kummer map belongs to $H^1(\mathrm{Gal}(H_0^+/\mathbb{Q}(\sqrt{n})), E[2])$ and then the image is killed by 2. Thus $4y_n \in 2^{k+1}E(\mathbb{Q}(\sqrt{n}))$, or $4(y_n - 2^{k-1}\widetilde{y}_n) = 0$ for some $\widetilde{y}_n \in E(\mathbb{Q}(\sqrt{n}))$. It follows that $y_n = 2^{k-1}\widetilde{y}_n$ modulo $E[2]$ and then belongs to $2^{k-1}E(\mathbb{Q}(\sqrt{n})) + E[2]$. Moreover, with the relation (4.5), we have that $2^{k-1}(\widetilde{y}_n - 2y_0 + \sum_{d \neq n} 2y'_d) \in E[2]$, which implies that

$$\widetilde{y}_n = 2y_0 - \sum_{d \neq n} 2y'_d + t, \qquad \text{for some } t \in E[2].$$

Note that for any $0 < d|n$ with $p_0|d$, we have that $\sigma_\varpi(\sqrt{d}) = -\sqrt{d}$ and therefore $y_d'^{\sigma_\varpi} = -y'_d$. Thus $\widetilde{y}_n^{\sigma_\varpi} + \widetilde{y}_n = 2(y_0^{\sigma_\varpi} + y_0) = 0$, i.e. $\widetilde{y}_n \in E(\mathbb{Q}(\sqrt{n}))^-$. This shows that $y_n \in 2^{k-1}E(\mathbb{Q}(\sqrt{n}))^- + E[2]$.

Now assume that the ideal class group of $K = \mathbb{Q}(\sqrt{-2n})$ has no order 4 element. Suppose that $y_n = 2^k y'_n + t_n$ for some $y'_n \in E(\mathbb{Q}(\sqrt{n}))^-$ and $t_n \in E[2]$. Then by the relation (4.3) in Lemma 4.2, we have that

$$2^k \left(y_0 - \sum_{p_0|d|n} y'_d \right) \in E[2], \qquad \text{with } y_0 - \sum_{p_0|d|n} y'_d \in E(H_0^+).$$

Again, any proper sub-extension of $H_0^+/\mathbb{Q}$ must be ramified at some odd prime, we have that $y_0 - \sum_{p_0|d|n} y'_d = t$ for some $t \in E[2]$. Thus

$$y_0 + y_0^{\sigma_\varpi} = \sum_{p_0|d|n} (y'_d + y_d'^{\sigma_\varpi}) + (t + t^{\sigma_\varpi}) = 0.$$

But with the assumption that the ideal class group of K has no elements of order 4, we have $y_0 + y_0^{\sigma_\varpi} = (0,0) \in E[2]$ by the equality (4.2) in Lemma 4.3. It is a contradiction. $\square$

4.2. The case $n \equiv 3 \bmod 4$

In this subsection, we assume that $n = p_0 p_1 \cdots p_k$ is a product of distinct primes with $p_0 \equiv 3 \bmod 4$ and $p_1, \ldots, p_k \equiv 1 \bmod 8$.

The genus field of $K = \mathbb{Q}(\sqrt{-2n})$ is $H_0 = K(\sqrt{-p_0}, \sqrt{p_1}, \ldots, \sqrt{p_k})$. Thus $\sqrt{2} \in H_0$ but $i \notin H$. We identify the ideal class group $\mathcal{A}$ of K with the subquotient of $\widehat{K}^\times$ corresponding to $\mathrm{Gal}(H(i)/K(i))$. Recall that we denote by ϖ the uniformizer $\sqrt{-2n}$ in $K_2^\times$ and let $\varpi' = \varpi(1+\varpi) \in K_2^\times$ which is also a uniformizer and $\sigma_{\varpi'}$ fixes i. Let $\varpi'_{p_i} = \sqrt{-2n} \in K_{p_i}^\times$ for $1 \le i \le k$ and let $\varpi'_{p_0} = (\sqrt{-2n})_{p_0}(1+\varpi) \in K_{p_0}^\times K_2^\times$. Note that the condition (1.1) in Theorem 1.3 says that

- if $p_0 \equiv 3 \bmod 8$, then $\mathcal{A}$ has no order 4 elements, or equivalently, $2\mathcal{A}$ has odd cardinality.
- if $p_0 \equiv 7 \bmod 8$, then the class of $\varpi' \in K_2^\times$ in $\mathcal{A}$ is the only non-trivial element in $\mathcal{A}[2] \cap 2\mathcal{A}$. In fact, by Gauss' genus theory, one can check that $\sigma_{\varpi'}\big|_H$ fixes $\sqrt{-p_0}$ and all $\sqrt{p_i}$ for $1 \le i \le k$.

Let $d \equiv 6, 7 \bmod 8$ be a positive divisor of $2n$, then $\sqrt{-d} \in H_0$ is fixed by $\sigma_{\varpi'}$. Let $\chi = \chi_d$ be the character of $\mathcal{A} = \mathrm{Gal}(H(i)/K(i))$ factoring through $\mathrm{Gal}(K(i, \sqrt{-d})/K(i))$ which is non-trivial when $d \neq 2n$. Since $\mathrm{Ker}\chi$ contains the class $[\varpi'] \in \mathcal{A}$ of ϖ', the character χ factors through $\mathcal{A}/\langle[\varpi']\rangle$. For any complete set of representatives $\phi \subset \mathcal{A}$ of $\mathcal{A}/\langle[\varpi']\rangle$, we define

$$y_{d,\phi} = \sum_{t \in \phi} \chi(t) z_t. \tag{4.6}$$

The point $y_{d,\phi}$ is independent of ϕ up to $E[2]$ by Theorem 2.8 (3). More precisely, let ϕ' be a second set of representatives and ϕ^c the complement of ϕ in $\mathcal{A}$. If $\phi' \cap \phi^c$ has even cardinality then $y_{d,\phi'} = y_{d,\phi}$; and if the cardinality is odd, then $y_{d,\phi'} - y_{d,\phi} = (-1,0)$ or $(1,0)$ according as $n \equiv 3$ or $7 \bmod 8$.

We will often ignore the dependence of $y_{d,\phi}$ on ϕ and abbreviate it to y_d. Note that $4y_d = P^\chi(f)$ with $m_0 = d$ in section 3 in then case $n \equiv 3 \bmod 4$.

Recall that $E(\mathbb{Q}(\sqrt{-d}))^-$ denotes the subgroup of points $P \in E(\mathbb{Q}(\sqrt{-d}))$ satisfying $\sigma P = -P$ where σ is the non-trivial element in $\mathrm{Gal}(\mathbb{Q}(\sqrt{-d})/\mathbb{Q})$. Then $E(\mathbb{Q}(\sqrt{-d}))^-$ is isomorphic to the Mordell-Weil group of the elliptic curve $E^{(d)} : dy^2 = x^3 - x$ over $\mathbb{Q}$ and its torsion subgroup is $E[2]$.

Let $m = n$ or $2n$ such that $m \equiv 6$ or $7 \bmod 8$. We will show that y_m is of infinite order under the condition (1.1) in Theorem 1.3 by induction on the number of prime divisors of n. More precisely, the rest of this section will be devoted to proving the following two theorems.

Theorem 4.4. *Let $k \geq 0$ an integer and $n = p_0 p_1 \cdots p_k$ a product of distinct primes with $p_0 \equiv 7 \bmod 8$ and $p_1, \ldots, p_k \equiv 1 \bmod 8$. Then for $m = n$ or $2n$, $y_m \in 2^{k-1}E(\mathbb{Q}(\sqrt{-m}))^- + E[2]$, and if $\dim_{\mathbb{F}_2} \mathcal{A}[4]/\mathcal{A}[2] = 1$ then the point $y_m \notin 2^k E(\mathbb{Q}(\sqrt{-m}))^- + E[2]$.*

Theorem 4.5. *Let $k \geq 0$ be an integer and $n = p_0 p_1 \cdots p_k$ a product of distinct primes with $p_0 \equiv 3 \bmod 8$ and $p_1, \ldots, p_k \equiv 1 \bmod 8$. Then $y_{2n} \in 2^{k-1}E(\mathbb{Q}(\sqrt{-2n}))^- + E[2]$, and if the field $K = \mathbb{Q}(\sqrt{-2n})$ has no order 4 ideal class, then the point $y_{2n} \notin 2^k E(\mathbb{Q}(\sqrt{-2n}))^- + E[2]$.*

The following proposition is the first step for the induction process and is proved in [19], and we repeat its proof here for completeness.

Proposition 4.6. *Let $n = p_0$ be a prime congruent to 3 modulo 4. Let $m = p_0$ or $2p_0$ such that $m \equiv 6, 7 \bmod 8$. Then we have*

$$2y_m \in E(\mathbb{Q}(\sqrt{-m}))^- \setminus \left(2E(\mathbb{Q}(\sqrt{-m}))^- + E[2]\right).$$

In particular, $2y_m \in E(\mathbb{Q}(\sqrt{-m}))^-$ is of infinite order and therefore m is a congruent number.

Proof. Note that the Galois group $\mathrm{Gal}(H(i)/\mathbb{Q})$ is generated by $\mathrm{Gal}(H(i)/K(i))$, the complex conjugation, and the operator $\sigma_{1+\varpi}$.

The element $\sigma_{1+\varpi}$ induces the non-trivial involution on $H(i)$ over H. By Theorem 2.8 (1),

$$y_{m,\phi}^{\sigma_{1+\varpi}} - y_{m,\phi} = \sum_{\phi} (0,0) \tag{4.7}$$

Thus $\sigma_{1+\varpi}$ fixes $2y_m$, i.e. $2y_m$ is rational over H. Moreover, by Theorem 2.8 (2),

$$\overline{y_{m,\phi}} = \sum_{[t]\in\phi} \chi(t)(-z_{t^{-1}} + (1,0)) = -y_{m,\phi^{-1}} + \sum_{\phi}(1,0), \tag{4.8}$$

thus the complex conjugation of $2y_m$ is equal to $-2y_m$. Any $\sigma_s \in \mathrm{Gal}(H(i)/K(i))$ maps $y_{m,\phi}$ to

$$\sum_{\phi} \chi(t) z_{st} = \chi(s) y_{m,[s]\phi}. \tag{4.9}$$

So it takes $2y_m$ to $2y_m$ or $-2y_m$ according to σ_s acts trivially or non-trivially on $\sqrt{-m}$. Thus $2y_m$ is rational over $K(i, \sqrt{-m})$ and therefore rational over $K(i, \sqrt{-m}) \cap H = K(\sqrt{-m})$. Now we claim that $2y_m$ is rational over $\mathbb{Q}(\sqrt{-m})$. This is clear if $m = 2n$. When $m \neq 2n$ choose an element $\sigma \in \mathrm{Gal}(H(i)/K(i))$ mapping $\sqrt{-m}$ to $-\sqrt{-m}$, then both σ and the complex conjugation take $2y_m$ to $-2y_m$, and therefore their composition fixes $2y_m$ and has fixed field $\mathbb{Q}(\sqrt{-m})$ in $K(\sqrt{-m})$. This shows the claim and therefore it follows that $2y_m \in E(\mathbb{Q}(\sqrt{-m}))^-$.

Let us first consider the case with $p_0 \equiv 3 \bmod 8$. Then $m = 2p_0 \equiv 6 \bmod 8$ and ϕ has odd cardinality. We need to show that $2y_m \notin 2E(\mathbb{Q}(\sqrt{-m}))^- + E[2]$. Suppose this is not the case, i.e. $2y_m = 2y + t$ for some $y \in E(\mathbb{Q}(\sqrt{-m}))^-$ and $t \in E[2]$. Then $P := y_m - y$ is a 4-torsion point. Note that $\sqrt{-m} \in H$. Then, by the equation (4.4), we have that

$$\sigma_{1+\varpi}(P) - P = \sigma_{1+\varpi}(y_m) - y_m = \sum_{\phi} (0,0) = (0,0).$$

On the other hand, as we pointed out at the beginning of section 2, $E[4]/E[2]$ is represented by $0, (i, 1-i), (1+\sqrt{2}, 2+\sqrt{2}), (-1-\sqrt{2}, i(2+\sqrt{2}))$. Note that $\sigma_{1+\varpi}$ moves i but fixes $\sqrt{2}$. Thus $\sigma_{1+\varpi}$ acts on any point $Q \in E[4]$ via the complex conjugation. It follows immediately that $\sigma_{1+\varpi}(Q) - Q = 0$ if $Q \equiv 0, (1+\sqrt{2}, 2+\sqrt{2}) \bmod E[2]$ and $\sigma_{1+\varpi}(Q) - Q = (-1, 0)$ otherwise. It is a contradiction.

Assume now that $p_0 \equiv 7 \bmod 8$. Then $m = p_0$ or $2p_0$ corresponding χ non-trivial or trivial. We need to show that $2y_m \notin 2E(\mathbb{Q}(\sqrt{-m}))^- + E[2]$. Suppose this is not the case, i.e. $2y_m = 2y \bmod E[2]$ for some $y \in E(\mathbb{Q}(\sqrt{-m}))^-$. Since ϕ has even cardinality, y_m is rational over H. Then $P := y_m - y \in E[4] \cap E(H) = E[4] \cap E((\mathbb{Q}(\sqrt{2}))$ and therefore $P = 0$ or $(1+\sqrt{2}, 2+\sqrt{2})$ modulo $E[2]$.

Note that $\mathcal{A}[2^\infty]$ is cyclic by Gauss' genus theory. Take an element $[t] \in \mathcal{A} - 2\mathcal{A}$ (for example, a generator of $\mathcal{A}[2^\infty]$), then $\mathcal{A}/([t])$ has odd cardinality. Let ϕ_0 be a set of representatives for the $\mathcal{A}/([t])$ and then we may take $\phi = \bigcup_{i=0}^{m-1} [t]^i \phi_0$ if the order of $[t]$ is $2m$ (thus $[t]^m = [\varpi'])$. Use this ϕ to define y_m. Now we have

$$y_{m,\phi}^{\sigma_t} = \left(\sum_{[t']\in\phi} \chi(t')z_{t'}\right)^{\sigma_t} = \chi(t) \sum_{[t']\in[t]\phi} \chi(t')z_{t'}$$
$$= \chi(t)\left(\sum_{\phi}\chi(t')z_{t'} + \sum_{\phi_0}\chi(t')(z_{\varpi' t'} - z_{t'})\right) = \chi(t)y_{m,\phi} + (1,0)$$

Note that σ_t fixes $\sqrt{-2p_0}$ but moves $\sqrt{2}$ and $\sqrt{-p_0}$. Thus $\sigma_t y = \chi(t)y$ and then

$$P^{\sigma_t} - \chi(t)P = y_m^{\sigma_t} - \chi(t)y_m = (1,0).$$

But we have shown that $P = 0$ or $(1+\sqrt{2}, 2+\sqrt{2})$ modulo $E[2]$. If follows that $P^{\sigma_t} - \chi(t)P = 0$ if $P = 0$ mod $E[2]$ and that $P^{\sigma_t} - \chi(t)P = (-1,0)$ or $0,0)$ if $P = (1+\sqrt{2}, 2+\sqrt{2})$ mod $E[2]$ according to $\chi(t) = 1$ or -1. It is a contradiction. □

We now refine the beginning argument of previous Proposition to obtain the defining field of points y_d's when $k \geq 1$.

Lemma 4.7. *Assume that $k \geq 1$ and that $n = p_0p_1\cdots p_k$ is a product of distinct primes $p_0 \equiv 3$ mod 4 and $p_i \equiv 1$ mod 8 for $1 \leq i \leq k$. Let $d|2n$ be a positive integer $\equiv 6, 7$ mod 8. Then the point $y_d \in E(\mathbb{Q}(\sqrt{-d}))^-$.*

Proof. Note again that the Galois group $\mathrm{Gal}(H(i)/\mathbb{Q})$ is generated by $\mathrm{Gal}(H(i)/K(i))$, the complex conjugation, and the operator $\sigma_{1+\varpi}$. Take a prime $p|n$, then the class $[\varpi'_p] \in \mathcal{A}[2]$ is neither trivial nor equal to $[\varpi']$ since $k \geq 1$. Let $\phi_0 \subset \mathcal{A}$ be a complete set of representatives of $\mathcal{A}/([\varpi'], [\varpi'_p])$ and let $\phi = \phi_0 \cup [\varpi'_p]\phi_0$, which has even cardinality.

(i) Since ϕ has even cardinality, by Theorem 2.8 (1), we have

$$y_{d,\phi}^{\sigma_{1+\varpi}} - y_{d,\phi} = \sum_{\phi}(0,0) = 0.$$

Thus $\sigma_{1+\varpi}$ fixes y_d, i.e. y_d is rational over H.

(ii) The set $\phi^c \cap \phi^{-1}$ is stable under multiplication by $[\varpi'_p]$ and then has even cardinality. It follows that $y_{d,\phi} = y_{d,\phi^{-1}}$. Then by Theorem 2.8 (2), we have

$$\overline{y_{d,\phi}} = \sum_{[t]\in\phi} \chi(t)(-z_{t^{-1}} + (1,0)) = -y_{d,\phi^{-1}} + \sum_{\phi}(1,0) = -y_{d,\phi}.$$

Thus the complex conjugation maps y_d to its negative.

(iii) For any $[t] \in \mathcal{A}$, $[t]\phi = [t]\phi_0 \cup [t\varpi_p']\phi_0$, the set $\phi^c \cap [t]\phi$ is stable under multiplication by $[\varpi_p']$ too and then has even cardinality. Thus for any $\sigma_t \in \mathrm{Gal}(H(i)/K(i))$,

$$y_{d,\phi}^{\sigma_t} = \sum_{\phi} \chi(t') z_{tt'} = \chi(t) y_{d,[t]\phi} = \chi(t) y_{d,\phi},$$

So $y_d^{\sigma_t}$ is equal to y_d or $-y_d$ according to σ_t acts trivially or non-trivially on $\sqrt{-d}$, thus y_d is rational over $K(i, \sqrt{-d})$.

Now by the same argument as the previous Proposition, we have that the point y_d belong to $E(\mathbb{Q}(\sqrt{-d}))^-$. □

We are now going to show separately Theorem 4.4 and Theorem 4.5, which correspond to the case with $p_0 \equiv 7 \bmod 8$ and the case with $p_0 \equiv 3 \bmod 8$.

Let $k \geq 1$ be an integer and $n = p_0 p_1 \cdots p_k$ with $p_0 \equiv 7 \bmod 8$ and $p_i \equiv 1 \bmod 8$ for $1 \leq i \leq k$. Note that $[\varpi'] \in 2\mathcal{A} \cap \mathcal{A}[2]$. Let ϕ_0 be a set of representatives of $2\mathcal{A}/([\varpi'])$. Let ψ be a set of representatives of $\mathcal{A}/2\mathcal{A}$. Then $\phi = \bigcup_{[s]\in\psi} [s]\phi_0$ is a set of representatives of $\mathcal{A}/([\varpi'])$. We use this ϕ to define all y_d's. Let $\beta \in \mathrm{Gal}(H(i)/K(i))$ be an element which moves $\sqrt{2}, \sqrt{p_1}, \ldots, \sqrt{p_k}$. Then β fixes or moves $\sqrt{p_0}$ according to that k is odd or even.

Lemma 4.8. *Assume $k \geq 1$. Let $n = p_0 p_1 \cdots p_k$ with $p_0 \equiv 7 \bmod 8$ and $p_i \equiv 1 \bmod 8$ for $1 \leq i \leq k$. Let $m = n$ or $2n$ such that $m \equiv 6$ or 7 modulo 8. Then we have*

1. *for each positive divisor d of $2n$ congruent to 6 or $7 \bmod 8$, the point $y_d \in E(\mathbb{Q}(\sqrt{-d}))^-$.*
2. *Let $y_0 := \sum_{[t]\in\phi_0} z_t$. Then $y_0 + (-1)^m y_0^\beta$ is rational over the genus subfield $H_0 = K(\sqrt{-p_0}, \sqrt{p_1}, \ldots, \sqrt{p_k})$ of K.*

These points satisfy the following relation:

$$\sum_{\substack{p_0 | d | 2n \\ \nu_0(d) \equiv \nu_0(m) \bmod 2}} y_d = 2^k \left(y_0 + (-1)^m y_0^\beta \right) \tag{4.10}$$

where for any integer d, $\nu_0(d)$ denotes the number of prime divisors of d.

Proof. Note that the Galois group $\mathrm{Gal}(H(i)/H_0)$ is generated by $\mathrm{Gal}(H(i)/H_0(i))$ and the operator $\sigma_{1+\varpi}$. The statement (1) is showed in Lemma 4.7. By Theorem 2.8, for any $[s] \in 2\mathcal{A}$, $y_0 - y_0^{\sigma_s} = 0$ or $(1,0)$ and thus $(y_0 \pm y_0^{\beta})$ is fixed by σ_s and then rational over $H_0(i)$. Since $\sigma_{1+\varpi}$ induces the involution of $H(i)$ over H, Theorem 2.8 also implies that $y_0 \pm y_0^{\beta}$ is rational over H_0. Moreover, we have that

$$\sum_{\substack{p_0|d|2n \\ \nu_0(d)\equiv\nu_0(m) \bmod 2}} y_d = \sum_{[t]\in\phi_0} \sum_{[s]\in\psi} \left(\sum_{\substack{p_0|d|2n \\ \nu_0(d)\equiv\nu_0(m) \bmod 2}} \chi_d(s) \right) (z_t)^{\sigma_s}$$

It is clear that the summation in the last bracket is equal to 2^k for $\sigma_s = 1$, $(-1)^m \cdot 2^k$ for $\sigma_s = \beta$, and 0 otherwise. Thus the equality (4.9) follows. □

Proof of Theorem 4.4. We prove the theorem by induction on k. The initial case $k = 0$ is given by Proposition 4.6. Now assume that $k \geq 1$. For $m = n$ or $2n$, Similar to the case with $p_0 \equiv 5 \bmod 8$, we have the following

1. the point $y_m \in 2^{k-1}E(\mathbb{Q}(\sqrt{-m}))^- + E[2]$, using the equality (4.9);
2. for each positive d with $p_0|d|2n$ and $d \neq n, 2n$, $y_d \in 2^k E(\mathbb{Q}(\sqrt{-d}))^- + E[2]$, i.e. of form $2^k y'_d + t_d$ for some $y'_d \in E(\mathbb{Q}(\sqrt{-d}))^-$ and $t_d \in E[2]$.

Now we show that $y_m \notin 2^k E(\mathbb{Q}(\sqrt{-m}))^- + E[2]$ under the condition $\dim_{\mathbb{F}_2} \mathcal{A}[4]/\mathcal{A}[2] = 1$. Suppose it is not the case, i.e. $y_m = 2^k y'_m + t_m$ for some $y'_m \in E(\mathbb{Q}(\sqrt{-m}))^-$ and $t_m \in E[2]$. Thus the previous lemma implies that

$$P := \left(y_0 + (-1)^m y_0^{\beta} - \sum_{\substack{p_0|d|2n \\ \nu_0(d)\equiv\nu_0(m) \bmod 2}} y'_d \right)$$
$$\in E[2^{k+1}] \cap E(H_0) = E[4] \cap E(\mathbb{Q}(\sqrt{2})).$$

It follows that $P^{\beta} - P = 0$ or $(0,0)$ and $P^{\beta} + P = 0$ or $(-1,0)$.

The assumption $\dim_{\mathbb{F}_2} \mathcal{A}[4]/\mathcal{A}[2] = 1$ implies that $[\varpi']$ is the unique non-trivial element in $2\mathcal{A} \cap \mathcal{A}[2]$. Note that $(y'_d)^{\beta} = (-1)^m y'_d$ and therefore

$$P - (-1)^m P^{\beta} = y_0 - y_0^{\beta^2}.$$

Write $\beta = \sigma_{t_0}$, we claim that $[t_0] \in \mathcal{A}$ has order $4s$ for some integer s. (Proof. Suppose it is not the case, then $[t_0]$ belongs to the subgroup of $\mathcal{A}$

generated by $\mathcal{A}[2]$ and the odd part of $\mathcal{A}$. Since $\mathcal{A}[2] \cong (\mathbb{Z}/2\mathbb{Z})^k$ is generated by $[\varpi_p], p|n$ where $\varpi_p = \sqrt{-2n} \in K_p^\times$, we may write $[t_0] = \prod_{p|n}[\varpi_p]^{\epsilon_p} a$ for some $\epsilon_p = 0$ or 1 and $a \in \mathcal{A}$ is of odd order. Note that $\sigma_{\varpi'_p}(\sqrt{p^*})/\sqrt{p^*} = (\frac{p'}{p})$ if $p' \neq p$ and $= (\frac{n/p}{p})$ otherwise. Let $A = (a_{ij})$ be the $k \times k$ matrixes whose (i,j)-entry is $(\frac{p_j}{p_i})$ and (i,i)-entry is $(\frac{n/p_i}{p_i})$. Let $v = (v_i)$ be the column vector in $\mathbb{F}_2^{k+1}$ with $v_i = 0$ if β fixes $\sqrt{p_i}$ and 1 otherwise. Then $\epsilon = (\epsilon_{p_i}) \in \mathbb{F}_2^k$ is a solution of the equation over $\mathbb{F}_2$: $A\epsilon = v$. But the summation of all rows is a zero row vector and $\sum_i v_i = 1$ by definition of β, a contradiction.)

Thus $[t_0]^{2s} = [\varpi']$ and the group $2\mathcal{A}/([t_0]^2)$ is of odd order. Let ϕ_1 be a set of representatives for the group $2\mathcal{A}/([t_0]^2)$, then we may take $\phi_0 = \bigcup_{i=0}^{s-1}[t_0]^{2i}\phi_1$ to be our set of representative for $2\mathcal{A}/([\varpi'])$ and use it to define y_0. Then

$$y_0 - y_0^{\beta^2} = \sum_{[t]\in\phi_0} z_t - \sum_{[t]\in\phi_0} z_{t_0^2 t} = \sum_{[t]\in\phi_1} (z_t - z_{\varpi' t}) = \#2\mathcal{A}/([t_0]^2)\cdot(1,0) = (1,0).$$

It is a contradiction. □

Finally, we consider the case that $p_0 \equiv 3 \bmod 8$ and $k \geq 1$. Then $\mathcal{A} = 2\mathcal{A} \times \mathcal{A}[2]$ and $[\varpi'] \in \mathcal{A}[2]$. Let ψ be the set of representatives for $\mathcal{A}[2]/([\varpi'])$ consisting of those $[\varpi'_d]$ fixing $\sqrt{2}$, then $\phi := \bigcup_{[s]\in\psi}[s](2\mathcal{A})$ is a set of representatives for $\mathcal{A}/([\varpi'])$. The set ϕ is stable under $[t] \mapsto [t]^{-1}$ and we use ϕ to define all y_d's.

Lemma 4.9. *Assume $k \geq 1$. Let $n = p_0 p_1 \cdots p_k$ be a product of distinct primes with $p_0 \equiv 3 \bmod 8$ and $p_i \equiv 1 \bmod 8$ for $1 \leq i \leq k$. Then we have*

1. *for each positive divisor d of $2n$ divisible by $2p_0$, the point $y_d \in E(\mathbb{Q}(\sqrt{-d}))^-$;*
2. *the point $y_0 := \sum_{[t]\in 2\mathcal{A}} z_t \in E(H_0(i))$ satisfies the following relation:*

$$y_0^{\sigma_{1+\varpi}} - y_0 = \#2\mathcal{A}\cdot(0,0) \tag{4.11}$$

Moreover, these points satisfy the following relation:

$$\sum_{2p_0|d|2n} y_d = 2^k y_0. \tag{4.12}$$

Proof. The statement (1) is showed in Lemma 4.7. The statement (2) follows from Theorem 2.8 (1):

$$y_0^{\sigma_{1+\varpi}} - y_0 = \sum_{[t]\in 2\mathcal{A}} (z_t^{\sigma_{1+\varpi}} - z_t) = \#2\mathcal{A} \cdot (0,0).$$

Moreover,

$$\sum_{2p_0|d|2n} y_d = \sum_{[t]\in 2\mathcal{A}} \sum_{[s]\in\psi} \left(\sum_{2p_0|d|2n} \chi_d(s) \right) z_t^{\sigma_s}.$$

It is clear that the summation in the last bracket is equal to 2^k for $\sigma_s = 1$ and 0 otherwise. Thus the equality (4.11) follows. □

Proof of Theorem 4.5. We prove the theorem by induction on k. The initial case $k = 0$ is given by Proposition 4.6. Now assume that $k \geq 1$. Similar to previous cases, we have that

1. the point $y_{2n} \in 2^{k-1}E(\mathbb{Q}(\sqrt{-2n}))^- + E[2]$, using the equality (4.11);
2. for each positive d with $2p_0|d|2n$ and $d \neq 2n$, $y_d \in 2^k E(\mathbb{Q}(\sqrt{-d}))^- + E[2]$, i.e. of form $2^k y_d' + t_d$ for some $y_d' \in E(\mathbb{Q}(\sqrt{-d}))^-$ and $t_d \in E[2]$.

Now we show that $y_{2n} \notin 2^k E(\mathbb{Q}(\sqrt{-2n}))^- + E[2]$ if the field $K = \mathbb{Q}(\sqrt{-2n})$ has no order 4 ideal class. Suppose it is not the case, i.e. $y_{2n} = 2^k y_{2n}' + t_{2n}$ for some $y_{2n}' \in 2^k E(\mathbb{Q}(\sqrt{-2n}))^-$ and $t_{2n} \in E[2]$. Then as before, we have that

$$\begin{aligned} P := y_{2n}' - y_0 + \sum_{2p_0|d|2n, d\neq 2n} y_d' &\in E[2^{k+1}] \cap E(H_0(i)) \\ &= E[2^{k+1}] \cap E(\mathbb{Q}(i, \sqrt{2})) = E[4]. \end{aligned}$$

Thus we have the formula

$$y_0 = \sum_{2p_0|d|2n} y_d' - P$$

with $P \in E[4]$, and then

$$y_0^{\sigma_{1+\varpi}} - y_0 = \sum_{2p_0|d|2n} ((y_d')^{\sigma_{1+\varpi}} - y_d') - (P^{\sigma_{1+\varpi}} - P) = -\overline{P} + P = 0 \quad \text{or} \quad (-1, 0).$$

But if $\mathcal{A}$ has no order 4 element or equivalently $2\mathcal{A}$ is odd, we have $y_0^{\sigma_{1+\varpi}} - y_0 = (0,0)$ by the equality (4.10) in Lemma 4.9. It is a contradiction. □

5. Proof of main results

In this section, we give proofs of Theorem 1.1, Theorem 1.3, and Theorem 1.5.

Proof of Theorem 1.5. Let $n = p_0p_1\cdots p_k$ be a product of distinct odd primes with $p_i \equiv 1 \mod 8$, $1 \leq i \leq k$, and $p_0 \not\equiv 1 \mod 8$. Let $m = n$ or $2n$ such that $m \equiv 5, 6$ or 7 modulo 8, and $m^* = (-1)^{(n-1)/2}m$. Let χ be the abelian character over K defining the unramified extension $K(\sqrt{m^*})$. Let $P \in X_0(32)$ be the point $[i\sqrt{2n}/8]$ if $n \equiv 5 \mod 8$ and $[(i\sqrt{2n}+2)/8]$ if $n \equiv 6, 7 \mod 8$. Then by Theorem 2.4 and Theorem 2.8, we have $f(P) \in E(H(i))$. We showed in Lemma 3.2 that the point

$$P^\chi(f) = \sum_{\sigma \in \mathrm{Gal}(H(i)/K)} f(P)^\sigma \chi(\sigma)$$

belongs to $E(\mathbb{Q}(\sqrt{m^*}))^-$ by taking $m_0 = m$ there. It is easy to see from the definitions (4.1) and (4.5) of y_m that

$$P^\chi(f) = 4y_m.$$

By Theorem 4.1, Theorem 4.4, and Theorem 4.5, we know that for integers m in Theorem 1.5,

$$y_m \in 2^{k-1}E(\mathbb{Q}(\sqrt{m^*}))^- + E[2] \setminus 2^kE(\mathbb{Q}(\sqrt{m^*}))^- + E[2].$$

It then follows that, by noting that $E[2^\infty] \cap E(\mathbb{Q}(\sqrt{m^*}))^- = E[2]$,

$$P^\chi(f) \in 2^{k+1}E(\mathbb{Q}(\sqrt{m^*}))^- \setminus \left(2^{k+2}E(\mathbb{Q}(\sqrt{m^*}))^- + E[2]\right).$$

In particular, $P^\chi(f) \in E(\mathbb{Q}(\sqrt{m^*}))^-$ is of infinite order and m is a congruent number. This completes the proof of our main result Theorem 1.5. □

By the following lemma, the condition (1.1) in Theorem 1.3 is actually easy to check. This allow us not only to show the existence result Theorem 1.1 but also to construct many congruent numbers.

Lemma 5.1. *Let $n = p_0p_1\cdots p_k$ be a product of distinct odd primes with $p_i \equiv 1 \mod 8$ for $1 \leq i \leq k$ and $p_0 \not\equiv 1 \mod 8$. Let $\mathcal{G}$ be the graph whose vertices set V consists of $p_0, \ldots, p_k$ and whose edges are those p_ip_j, $i \neq j$, with the quadratic residue symbol $\left(\frac{p_i}{p_j}\right) = -1$. Then the condition (1.1) in Theorem 1.3 is equivalent to any one of the following conditions:*

1. *there does not exist a proper even partition of vertices* $V = V_0 \cup V_1$ *in the sense that any* $v \in V_i$ *has even number edges to* V_{1-i}, $i = 0, 1$;
2. *the graph* $\mathcal{G}$ *has an odd number of spanning subtrees.*

Proof. Note that the multiplication by 2 induces an isomorphism $\mathcal{A}[4]/\mathcal{A}[2] \overset{\times 2}{\simeq} \mathcal{A}[2] \cap 2\mathcal{A}$. The condition (1.1) is the same as

$$2\mathcal{A} \cap \mathcal{A}[2] = \begin{cases} 0, & \text{if } n \equiv \pm 3 \bmod 8; \\ \{0, [\varpi]\}, & \text{otherwise.} \end{cases}$$

Note that the group $\mathcal{A}[2]$ consists of $[\varpi_d]$ for all positive divisors $d|n$, that $[\varpi] = [\varpi_n]$ in $\mathcal{A}$, and that $[\varpi_d] \in 2\mathcal{A}$ if and only if

$$\left(\frac{d}{p}\right) = 1, \forall\, p|(n/d) \quad \text{and} \quad \left(\frac{2n/d}{p}\right) = 1, \forall\, p|d.$$

The equivalence between (1) and the condition (1.1) in Theorem 1.3 is then clear. See either [7] Lemma 2.2. or [18] Lemma 2 for the equivalence between (1) and (2). □

By Dirichlet's theorem, we can construct infinitely many numbers n for each given isomorphism class of graph with an odd number of spanning subtrees. Thus Theorem 1.1 follows from Theorem 1.5. We can even obtain the following stronger version.

Theorem 5.2. *Let* $p_0 \not\equiv 1 \bmod 8$ *be an odd prime. Then there exists an infinite set* Σ *of primes congruent to* 1 *modulo* 8 *such that the product of* p_0 *(resp.* $2p_0$*) and primes in any finite subset of* Σ *is a congruent number if* $p_0 \equiv 5, 7 \bmod 8$ *(resp.* $p_0 \equiv 3 \bmod 4$*).*

Proof. Suppose we are given an odd prime $p_0 \not\equiv 1 \bmod 8$. By Dirichlet theorem, we can choose inductively primes $p_1, p_2, \ldots$ satisfying the following conditions:

(i) all $p_i \equiv 1 \bmod 8$,
(ii) the quadratic residue symbol $(\frac{p_i}{p_0}) = -1$, and
(iii) for all $1 \leq j \leq i-1$, $(\frac{p_i}{p_j}) = 1$.

Let Σ be the infinite set $\{p_1, p_2, \ldots\}$. Then the graph with vertices set $\{p_0\} \cup \Sigma$ and edges those $p_i p_j$ satisfying $(\frac{p_i}{p_j}) = -1$, is an infinite star-shape graph. It is now easy to see that the product n of p_0 with primes in any finite subset of Σ satisfies the condition (1.1) in Theorem 1.3. Thus the set Σ is the desired one. □

Finally, we explain how Theorem 1.3 follows from Theorem 1.5. Recall $E' = (X_0(32), [\infty])$ is an elliptic curve defined over $\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 + 4x$.

Lemma 5.3. *Let $n = p_0 p_1 \cdots p_k$ be a product of distinct odd primes with $p_i \equiv 1 \bmod 8$ for $1 \le i \le k$. Let $m = n$ or $2n$ such that $m \equiv 5, 6,$ or $7 \bmod 8$. Let φ be a 2-isogeny from $E^{(m)}$ to $E'^{(m)} : my^2 = x^3 + 4x$ with kernel $\{0, (0,0)\}$, and ψ its dual isogeny. Let $S^{(\varphi)} = S^{(\varphi)}(E^{(m)})$ (resp. $S^{(\psi)} = S^{(\psi)}(E'^{(m)})$) denote the φ-(resp. ψ-) Selmer group. Then the condition (1.1) in Theorem 1.3 implies that*

$$\dim_{\mathbb{F}_2} S^{(\varphi)} = 1 \quad \textit{and} \quad \dim_{\mathbb{F}_2} S^{(\psi)} = 2,$$

and moreover, that the 2-Selmer group $S^{(2)}(E^{(m)}/\mathbb{Q})$ satisfies

$$\dim_{\mathbb{F}_2} S^{(2)}(E^{(m)}/\mathbb{Q}) \Big/ E^{(m)}[2] = 1. \tag{5.1}$$

Proof. These Selmer groups can be computed using [23] Ch.X Proposition 4.9. For example, when $m = n \equiv 5 \bmod 8$, the φ-Selmer group $S^{(\varphi)} \subset H^1(\mathbb{Q}, E^{(m)}[\varphi]) \cong \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ has representatives divisors d (including negative ones) of $2n$ satisfying the condition that the curve

$$C_d : \quad dw^2 = d^2 + 4n^2 z^4$$

over $\mathbb{Q}$ is solvable locally everywhere while ψ-Selmer group $S^{(\psi)} \subset H^1(\mathbb{Q}, E'^{(m)}[\psi]) \cong \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ has representatives divisors d (including negative ones) of $2n$ satisfying the condition that the curve

$$C'_d : \quad dw^2 = d^2 - n^2 z^4$$

over $\mathbb{Q}$ is solvable locally everywhere. Using the equivalence between the condition (1.1) in Theorem 1.3 and (1) in Lemma 5.1, one can check easily by Hensel's Lemma that $S^{(\varphi)}$ consists of only two elements $1, n$ and is then of $\mathbb{F}_2$-dimension 1, and $S^{(\psi)}$ consists of $\pm 1, \pm n$ and then is of dimension 2.

Note that there is an exact sequence:

$$0 \longrightarrow S^{(\varphi)} \longrightarrow S^{(2)}(E^{(m)}/\mathbb{Q}) \longrightarrow S^{(\psi)}.$$

Since the subgroup $E^{(m)}[2] \subset S^{(2)}(E^{(m)}/\mathbb{Q})$ of 2-torsion points provides 2-dimensional image in $S^{(\psi)}$, the last morphism is also surjective and therefore $\dim_{\mathbb{F}_2} S^{(2)}(E^{(m)}/\mathbb{Q}) = 3$. The formula (5.1) follows. □

Proof of Theorem 1.3. Let $m = n$ or $2n$ be as in the Theorem 1.3 and $P^{\chi}(f)$ the Heegner point constructed in Theorem 1.5. By Theorem 1.5, we know that $P^{\chi}(f) \in E(\mathbb{Q}(\sqrt{m^*}))^- \cong E^{(m)}(\mathbb{Q})$ is of infinite order. Via the argument in the proof of Proposition 3.4, the Euler system theory of Kolyvagin implies that the Mordell-Weil group $E^{(m)}(\mathbb{Q})$ has rank one and the Shafarevich-Tate group $Ш(E^{(m)}/\mathbb{Q})$ is finite. By the generalized Gross-Zagier formula ([27] Theorem 1.2) and the non-vanishing of $L(E^{(1)}, 1)$ and $L(E^{(2)}, 1) \neq 0$, the vanishing order of $L(E^{(m)}, s)$ at $s = 1$ is exactly one.

It follows from (5.1) in Lemma 5.3 that

$$\mathrm{rank}_{\mathbb{Z}} E^{(m)}(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(E^{(m)}/\mathbb{Q})[2] = 1.$$

Since we have shown that $\mathrm{rank}_{\mathbb{Z}} E^{(m)}(\mathbb{Q}) = 1$, $Ш(E^{(m)}/\mathbb{Q})[2] = 0$, which implies that $Ш(E^{(m)}/\mathbb{Q})$ has odd cardinality. □

References

[1] B. J. Birch, *Elliptic curves and modular functions*, Symposia Mathematica, Indam Rome 1968/1969, Vol. 4, Academic Press, London, 1970, pp. 27–32.

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

[3] Daniel Bump, *Automorphic Forms and Representations*, Cambridge Studies in Advanced Mathematics 55, 1998.

[4] John Coates and Andrew Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 233–251.

[5] Arian Diaconu and Ye Tian, *Twisted Fermat Curves over Totally Real Fields*, Annals of Math. 162, 2005.

[6] L. E. Dickson, *History of the Theory of Numbers* Volume II. Carnegie Institute, Washington DC (1920), reprinted by Chelsea (1966).

[7] Keqin Feng, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arithmetica, LXXV. 1 (1996).

[8] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in Number theory, Carbondale 1979, M. B. Nathanson, ed., Lecture Notes in Math. 751, Springer, Berlin, 1979, 108–118.

[9] B. Gross, *Kolyvagin's work on modular elliptic curves*, in: L-function and Arithmetic (ed. J. Coates and M. J. Talyor) Cambridge University Press (1991).

[10] B. Gross and D. Zagier, *Heegner points and derivatives of L-series.* Invent. Math. 84 (1986), no. 2, 225–320.

[11] K. Heegner, *Diophantische analysis und modulfunktionen.* Math. Z. 56, (1952), 227–253.

[12] Nicholas M. Katz and Peter Sarnak, *Zeros of zeta functions and symmetry*, Bull. Amer. Math. Soc. (N.S.) 36 (1999), no. 1, 1–26.

[13] Shinichi Kobayshi, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*, Preprint.

[14] Neal Kobliz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, GTM 97, 1993.

[15] V. A. Kolyvagain, *Euler system*, The Grothendieck Festschrift. Prog. in ath., Boston, Birkhauser (1990).

[16] V. A. Kolyvagain, *Finiteness of* $E(\mathbb{Q})$ *and* $Ш(E, \mathbb{Q})$ *for a subclass of Weil curves*, Math. USSR Izvestiya, Vol. 32 (1989), No. 3.

[17] Serge Lang, *Elliptic Functions.* GTM 112, Springer, 1987.

[18] Delang Li and Ye Tian, *On the Birch-Swinnerton-Dyer Conjecture of Elliptic Curves* $E_D : y^2 = x^3 - D^2x$, Acta Mathematica Sinica, English Series 2000, April, Vol. 16, No. 2, pp. 229–236.

[19] P. Monsky, *Mock Heegner Points and Congruent Numbers*, Math. Z. 204, (1990), 45–68.

[20] Jan Nekovář, *The Euler system method for CM points on Shimura curves*, in: L-functions and Galois representations, (Durham, July 2004), LMS Lecture Note Series 320, Cambridge Univ. Press, 2007, pp. 471–547.

[21] B. Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math. 89 (1987), no. 3, pp. 455–510.

[22] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press (1971).

[23] J. Silverman, *Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, 1986.

[24] N. M. Stephens, *Congruence properties of congruent numbers*, Bull. Lond. Math. Soc. 7, (1975), 182–184.

[25] Ye Tian, *Euler System of CM points on Shimura Curves*, thesis at Columbia University, 2003.

[26] J. B. Tunnell, *A classical diophantine problem and modular forms*, Invent. Math. 72, (1983), 323–334.

[27] X. Yuan, S. Zhang, and W. Zhang *The Gross-Zagier formula on Shimura Curves*, Annals of Mathematics Studies Number 184, 2012.

[28] Chunlai Zhao, *A criterion for elliptic curves with lowest 2-power in L(1) (II)*. Math. Proc. Camb. Phil. Soc. 134 (2003), 407–420.

[29] Chunlai Zhao, *A criterion for elliptic curves with second lowest 2-power in L(1)*. Math. Proc. Camb. Phil. Soc. 131 (2001), 385–404.

Ye Tian
Academy of Mathematics and Systems Science
Morningside center of Mathematics
Chinese Academy of Sciences
Beijing 100190
China
E-mail address: ytian@math.ac.cn

Received December 20, 2013