BIRCH AND SWINNERTON-DYER CONJECTURE IN THE COMPLEX MULTIPLICATION CASE AND THE CONGRUENT NUMBER PROBLEM

KAZUMA MORITA

Abstract. For an elliptic curve E over K, the Birch and Swinnerton-Dyer conjecture predicts that the rank of Mordell-Weil group $E(K)$ is equal to the order of the zero of $L(E_{/K}, s)$ at $s = 1$. In this paper, we shall give a proof for elliptic curves with complex multiplications. The key method of the proof is to reduce the Galois action of infinite order on the Tate module of an elliptic curve to that of finite order by using the p-adic Hodge theory. As a corollary, we can determine whether a given natural number is a congruent number (congruent number problem). This problem is one of the oldest unsolved problems in mathematics.

1. Introduction

A natural number N is called a congruent number if it is the area of a rational right-angled triangle. To determine whether N is a congruent number is a difficult problem which can be traced back at least a millennium and is the oldest major unsolved problem in number theory. For example, it is easy to verify that 6 is a congruent number since the sides lengths $(3, 4, 5)$ give the right-angled triangle whose area is 6. Furthermore, 5 and 7 are shown to be congruent numbers by Fibonacci and Euler. On the other hand, Fermat showed that the square numbers are never congruent numbers and, based on this experience, led to the famous Fermat's conjecture. In modern language, a natural number N is a congruent number if and only if there exists a rational point (x, y) with $y \neq 0$ on the elliptic curve $y^2 = x^3 - N^2x$. The Birch and Swinnerton-Dyer conjecture which is one of the millennium problems by Clay Mathematics Institute concerns the rational points on the elliptic curves. The substantial developments are given by Coates-Wiles, Gross-Zagier, Kolyvagin, Rubin, and so on. In this paper, we shall give a proof for elliptic curves with complex multiplications which include the elliptic curves of the form $y^2 = x^3 - N^2x$ and, as a corollary, can determine whether N is a congruent number by the criterion of Tunnell.

Organization. Let E/K be an elliptic curve with complex multiplication over an imaginary quadratic field K. Choose an algebraic closure $\overline{K}$ of K and

Date: May 30, 2019.

1991 *Mathematics Subject Classification.* 11F03, 11G05, 11G40.

Key words and phrases. classical number theory, elliptic curves.

consider the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$. For a prime p, consider the Tate module $\mathbb{V}_p(E)$ over $\mathbb{Q}_p$ and put $V_p(E) = \mathbb{V}_p(E)$ if p splits in K (resp. $V_p(E) = \mathbb{V}_p(E) \otimes_{\mathbb{Q}_p} K_p$ otherwise). Then, by the theory of Lubin-Tate, we have a splitting $V_p(E) = V^{(1)} \oplus V^{(2)}$ of G_K-modules where $V^{(i)}$ is a 1-dimensional vector space. In Section 3.2, we show that $V^{(i)}$ has the Hodge-Tate weight $(0,0)$ or $(1,1)$ in the sense of Section 2. Note that, contrary to the Hodge weights over $\mathbb{C}$, the action of $\mathrm{Gal}(K/\mathbb{Q})$ (and its restriction $\mathrm{Gal}(K_p/\mathbb{Q}_p)$) does not exchange the Hodge-Tate weights (see Remark 3.2 and 3.4). The key method of the proof of the main theorem is to reduce the Galois action of infinite order on the Tate module $V_p(E)$ to that of finite order by using the fact that $V^{(i)}$ has the Hodge-Tate weight $(0,0)$ or $(1,1)$ (see Section 2 for details). This means that the proof of the main theorem is reduced to the methods in the algebraic number theory.

2. Algebraic Hecke character and Algebraic Galois character

In this section, we shall review the basic facts on the class field theory based on [Y]. Let F be a number field and $\mathbb{A}_F$ denote the adele ring of F. For each place v of F, consider its completion F_v. If v is an infinite place of F, denote the connected component of identity of $F_v^\times$ by $F_v^{\times 0}$ and define $F_\infty^{\times 0} = \prod_{v|\infty} F_v^{\times 0}$. Then, the global class field theory claims that the global Artin map Art_F induces the isomorphism

$$\mathrm{Art}_F : \mathbb{A}_F^\times / \overline{F^\times F_\infty^{\times 0}} \simeq G_F^{\mathrm{ab}}$$

where $-$ denotes the closure in $\mathbb{A}_F^\times$. Since the kernel of a continuous character of $\mathbb{A}_F^\times / F^\times$ is a closed set in $\mathbb{A}_F^\times / F^\times$, we have a one-to-one correspondence

$$\{\text{Galois character } R : G_F \to \mathbb{C}^\times\} \leftrightarrow \{\text{Hecke character } \Pi : \mathbb{A}_F^\times / F^\times \to \mathbb{C}^\times, \Pi_{|F_\infty^{\times 0}} = 1\}$$

where this correspondence is given by $\Pi = R \circ \mathrm{Art}_F$. Now, let us consider a p-adic Hecke character $\Pi : \mathbb{A}_F^\times / F^\times \to \overline{\mathbb{Q}_p}^\times$. Since $\overline{\mathbb{Q}_p}^\times$ is totally disconnected, the connected component of the identity on the left hand side is contained in $\mathrm{Ker}\,(\Pi)$ and we obtain $\Pi_{|F_\infty^{\times 0}} = 1$. By the same method above, we have a one-to-one correspondence

$$\{\text{Galois character } R : G_F \to \overline{\mathbb{Q}_p}^\times\} \leftrightarrow \{\text{Hecke character } \Pi : \mathbb{A}_F^\times / F^\times \to \overline{\mathbb{Q}_p}^\times\}.$$

2.1. **Algebraic Hecke character.** Let $\Pi : \mathbb{A}_F^\times / F^\times \to \mathbb{C}^\times$ be a Hecke character and denote its restriction to $F_v^\times$ by Π_v. For an infinite place v of F, we say that Π_v is algebraic if there exist integers $a_\tau \in \mathbb{Z}$ such that we have

$$\Pi_v(x_v) = \prod_{\tau \in \mathrm{Hom}_{\mathbb{R}}(F_v, \mathbb{C})} \tau(x_v)^{a_\tau} \quad (\forall x_v \in F_v^{\times 0}).$$

Furthermore, if Π_v is algebraic for all infinite places v in F, we say that Π is the **algebraic Hecke character** (different from the usual definition) and that the set of integers $(a_\tau)_\tau$ (the number of this set is $[F : \mathbb{Q}]$) is the weights of Π. For an

algebraic Hecke character Π of weights $(a_\tau)_\tau$ and a field isomorphism $\iota : \overline{\mathbb{Q}}_p \simeq \mathbb{C}$, define the p-adic Hecke character Π_ι by

$$\Pi_\iota : x\,(\in \mathbb{A}_F^\times) \mapsto \iota^{-1}\Big(\Pi(x)\cdot \prod_{\tau\in \mathrm{Hom}_{\mathbb{Q}}(F,\mathbb{C})} \tau(x_{v(\tau)})^{-a_\tau}\Big)\cdot \prod_{\tau\in \mathrm{Hom}_{\mathbb{Q}}(F,\overline{\mathbb{Q}_p})} \tau(x_{v(\tau)})^{a_{\iota\circ\tau}} (\in \overline{\mathbb{Q}_p}^\times).$$

The p-adic Hecke character Π_ι factors through $\mathbb{A}_F^\times/F^\times$ and we have $(\Pi_\iota)_v = \iota^{-1}\circ\Pi_v$ for $v\nmid p,\infty$. For a finite place v of F, since Π_v factors through a discrete group, $(\Pi_\iota)_v$ is continuous. On the other hand, for an infinite place v, since $(\Pi_\iota)_v$ factors through a finite group, $(\Pi_\iota)_v$ is also continuous. It follows that Π_ι is a continuous character.

2.2. **Algebraic Galois character.** For an algebraic Hecke character Π of weights $(a_\tau)_\tau$ and a field isomorphism $\iota : \overline{\mathbb{Q}}_p \simeq \mathbb{C}$, define the p-adic Galois character R by $\Pi_\iota = R\circ \mathrm{Art}_F$. Denote its restriction to the Weil group of F_v by R_v and put $\mathrm{Art}_v = \mathrm{Art}_F\mid_{F_v^\times}$. It follows that we have $(\Pi_\iota)_v = R_v\circ\mathrm{Art}_v$. Then, for $v\mid p$ and $\tau\in \mathrm{Hom}_{\mathbb{Q}_p}(F_v,\overline{\mathbb{Q}_p})$, there exist $b_\tau := a_{\iota\circ\tau}\in\mathbb{Z}$ and an open subgroup $U\subset \mathcal{O}_v^\times$ ($\mathcal{O}_v$: the ring of integers of F_v) such that we have

$$R_v\circ\mathrm{Art}_v(x_v) = \prod_{\tau\in\mathrm{Hom}_{\mathbb{Q}_p}(F_v,\overline{\mathbb{Q}_p})} \tau(x_v)^{b_\tau}\quad(\forall x_v\in U).$$

Note that, since the finite component of $\Pi : \mathbb{A}_F^\times/F^\times\to\mathbb{C}^\times$ is a character of a locally profinite group, the finite component of Π is trivial on an open subgroup $\mathbb{U}$ of $\hat{\mathcal{O}}_F^\times := (\mathcal{O}_F\otimes_{\mathbb{Z}}\hat{\mathbb{Z}})^\times$ ($\mathcal{O}_F$: the ring of integers of F). We say that such a p-adic Galois character R is an **algebraic Galois character** and that the set of integers $(b_\tau)_\tau$ (the number of this set is $[F:\mathbb{Q}]$) is the Hodge-Tate weights of R. Conversely, we can obtain the algebraic Hecke character Π from the algebraic Galois character R by reversing the procedure. In particular, it follows from the global class field theory that the algebraic Galois character of Hodge-Tate weights $(0)_\tau$ factors through a finite quotient since the corresponding algebraic Hecke character Π satisfies $\Pi_{\mid F_\infty^{\times 0}} = 1$.

3. Elliptic curve and class field theory

3.1. **Preliminary.** Let E/K be an elliptic curve with complex multiplication over an imaginary quadratic field K. Choose an algebraic closure $\overline{K}$ of K and consider the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$. For the Tate module $\mathbb{V}_p(E)$ over $\mathbb{Q}_p$, put $V_p(E) = \mathbb{V}_p(E)$ if p splits in K (resp. $V_p(E) = \mathbb{V}_p(E)\otimes_{\mathbb{Q}_p} K_p$ otherwise). Then, by the theory of Lubin-Tate, we have a splitting $V_p(E) = V^{(1)}\oplus V^{(2)}$ of G_K-modules where $V^{(i)}$ is a 1-dimensional vector space.

Lemma 3.1. *With notations as above, $V^{(i)}$ has the Hodge-Tate weight* 0 *or* 1.

Proof. Since the weight of an algebraic Hecke character (hence Hodge-Tate weight) does not depend on the choice of prime p, we may assume that the prime p inerts

in K. In this proof, we consider the tensor products over K_p. Let $\mathbb{C}_p$ denote the p-adic completion of an algebraic closure of $\mathbb{Q}_p$. Since, by the comparison theorem of the p-adic Hodge theory ([T], p.180, Cor.2), we have $\mathbb{C}_p \otimes V_p(E) \simeq \mathbb{C}_p \oplus \mathbb{C}_p(-1)$, it suffices to show that we have $\mathbb{C}_p \otimes V^{(1)} \simeq \mathbb{C}_p$, $\mathbb{C}_p \otimes V^{(2)} \simeq \mathbb{C}_p(-1)$ or $\mathbb{C}_p \otimes V^{(1)} \simeq \mathbb{C}_p(-1)$, $\mathbb{C}_p \otimes V^{(2)} \simeq \mathbb{C}_p$. Let α (resp. β) denote an element of $V^{(1)}$ (resp. $V^{(2)}$). Put

$$(*) \qquad g(\alpha) = s\alpha \quad \text{and} \quad g(\beta) = t\beta \quad (g \in G_{K_p},\ s, t \in K_p^{\times}).$$

On the other hand, since $1 \otimes \alpha$ and $1 \otimes \beta$ are elements of $\mathbb{C}_p \otimes V_p \simeq \mathbb{C}_p \oplus \mathbb{C}_p(-1)$, we can write

$$(**) \qquad 1 \otimes \alpha = a\mathbf{1} + b\mathbf{T} \quad \text{and} \quad 1 \otimes \beta = c\mathbf{1} + d\mathbf{T} \quad (a, b, c, d \in \mathbb{C}_p)$$

where $\mathbf{1}$ (resp. $\mathbf{T}$) denotes a basis of $\mathbb{C}_p$ (resp. $\mathbb{C}_p(-1)$) such that we have $g(\mathbf{1}) = \mathbf{1}$ and $g(\mathbf{T}) = \chi(g)\mathbf{T}$ ($g \in G_{K_p}$, χ is the cyclotomic character). From the presentation of $(*)$ and $(**)$, we have

$$g(a)\mathbf{1} + g(b)\chi(g)\mathbf{T} = s(a\mathbf{1} + b\mathbf{T}) \text{ and } g(c)\mathbf{1} + g(d)\chi(g)\mathbf{T} = t(c\mathbf{1} + d\mathbf{T})$$

and it follows that we obtain

$$g(a) = sa,\ g(b)\chi(g) = sb \quad \text{and} \quad g(c) = tc,\ g(d)\chi(g) = td.$$

Assume that we have $b \neq 0$ and then we have $g(ab^{-1}) = \chi(g)ab^{-1}$. Since such an element exists in $\mathbb{C}_p$ if and only if $ab^{-1} = 0$, this means that we have $a = 0$. Therefore, we can obtain $a = 0$ or $b = 0$ (similarly $c = 0$ or $d = 0$) and it follows from $(**)$ that $V^{(i)}$ has the Hodge-Tate weight 0 or 1. □

Remark 3.2. With notations as in the proof of Lemma 3.1, we show that each Hodge-Tate weight does not depend on the embeddings $K_p \hookrightarrow \mathbb{C}_p$. Let $h : K_p \hookrightarrow \mathbb{C}_p$ be the other embedding and $\mathbb{C}_p \otimes_{K_p} V_p(E)$ is equipped with the action of $\mathrm{Gal}(K_p/\mathbb{Q}_p)$ by $\mathbb{C}_p \otimes_{h(K_p)} V_p(E)$. Put $H = \mathrm{Gal}(\overline{K_p}/\mathbb{Q}_p^{\mathrm{ab}})$ and $\Gamma = G_{K_p}/H$. Then, $D := (\mathbb{C}_p \otimes V_p(E))^H = \mathbb{C}_p^H \oplus \mathbb{C}_p^H(-1)$ is equipped with the action of Γ. Since $h \in \mathrm{Gal}(K_p/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)/\Gamma$ commutes with the action of Γ, this induces the Γ-equivariant map

$$h : D \to h(D)\ (\subset \mathbb{C}_p \otimes V_p(E)).$$

Then, we can write

$$(***) \qquad h(\mathbf{1}) = k\mathbf{1} + l\mathbf{T} \quad \text{and} \quad h(\mathbf{T}) = m\mathbf{1} + n\mathbf{T} \quad (k, l, m, n \in \mathbb{C}_p).$$

On the other hand, for an element $g \in \Gamma = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/K_p)$, we have

1). $gh(\mathbf{1}) = g(k)\mathbf{1} + g(l)\chi(g)\mathbf{T} = k\mathbf{1} + l\mathbf{T} = hg(\mathbf{1})$,

2). $gh(\mathbf{T}) = g(m)\mathbf{1} + g(n)\chi(g)\mathbf{T} = \chi(g)m\mathbf{1} + \chi(g)n\mathbf{T} = hg(\mathbf{T})$.

Thus, we obtain $g(l) = \chi(g)^{-1}l$ and $g(m) = \chi(g)m$ and such elements l, m exist in $\mathbb{C}_p$ if and only if $l = m = 0$. It follows from $(***)$ that we have $h(\mathbb{C}_p) = \mathbb{C}_p$ and $h(\mathbb{C}_p(-1)) = \mathbb{C}_p(-1)$ as the action of h on $\mathbb{C}_p \otimes V_p(E) = \mathbb{C}_p \oplus \mathbb{C}_p(-1)$. Therefore, each Hodge-Tate weight does not depend on the embeddings $K_p \hookrightarrow \mathbb{C}_p$. This

means that the Hodge-Tate weights of $V^{(i)}$ as a $\mathbb{Q}_p$-representation are $(0,0)$ or $(1,1)$.

From now on, fix the notation such that $V^{(1)}$ (resp. $V^{(2)}$) has the Hodge-Tate weight 0 (resp. 1). The following is the key lemma which connects the unit elements of the rings of integers of number fields and rational points on elliptic curves.

Lemma 3.3. *In the sense of §2, $V^{(1)}$ (resp. $V^{(2)}$) has the Hodge-Tate weight $(0)_\tau$ (resp. $(1)_\tau$).*

Proof. As in the proof of Lemma 3.1, we may assume that the prime p inerts in K and we consider the Tate module $V_p(E)$ over K_p. First of all, note that we have the one-to-one correspondence between the algebraic Hecke character (the absolute value) $|\cdot|\colon \mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \to \mathbb{R}_{>0}^\times \subset \mathbb{C}^\times$ of weight 1 and the algebraic Galois character (the cyclotomic character) $\chi : G_{\mathbb{Q}} \to \overline{\mathbb{Q}_p}^\times$ of Hodge-Tate weight 1 in the sense of §2. Further, by the base change for a number field $F/\mathbb{Q}$, we also have the one-to-one correspondence between $|\cdot|\circ N_{F/\mathbb{Q}}$ and $\chi_{|F}$ where $N_{F/\mathbb{Q}}$ denotes the norm map from $\mathbb{A}_F^\times$ to $\mathbb{A}_{\mathbb{Q}}^\times$. Let $\sigma^{(i)} : G_K \to \mathrm{Aut}(V^{(i)})$ denote the Galois character obtained from the action of G_K on $V_p(E)$ and let $\sigma_p^{(i)}$ be its restriction to the Weil group of K_p. Denote the ring of integers of K_p by $\mathcal{O}_p$. Since $V^{(1)}$ (resp. $V^{(2)}$) has the Hodge-Tate weight 0 (resp. 1), there exists an open subgroup U of $\mathcal{O}_p^\times$ such that we have ([F], p.143, 3.9.iv)

$$\sigma_p^{(1)}\circ \mathrm{Art}_p(x) = N_{K_p/\mathbb{Q}_p}(1) = 1 \text{ and } \sigma_p^{(2)}\circ \mathrm{Art}_p(x) = N_{K_p/\mathbb{Q}_p}(x) = x\tau(x) \quad (\forall x \in U)$$

where $N_{K_p/\mathbb{Q}_p}$ denotes the norm map from K_p to $\mathbb{Q}_p$ and $1 \neq \tau \in \mathrm{Hom}_{\mathbb{Q}_p}(K_p, \overline{\mathbb{Q}_p})$ (see §2). This means that $V^{(1)}$ (resp. $V^{(2)}$) has the Hodge-Tate weight $(0)_\tau$ (resp. $(1)_\tau$). □

3.2. **Global class field theory and Hecke character.** Let $\sigma^{(i)} : G_K \to \mathrm{Aut}(V^{(i)})$ $(i = 1, 2)$ denote the Galois character obtained from the action of G_K on $V_p(E)$. By the theory of complex multiplication ([S], II.10.5), there exists a Hecke character ω_K over K such that, for a good prime $v \nmid p$, the prime element $\wp_v$ of K and the Frobenius element Frob_v are related by

$$(\sharp) \quad \omega_{K,v}(\wp_v) = \iota \circ \sigma_v^{(1)}(\mathrm{Frob}_v) \quad \text{and} \quad \overline{\omega_{K,v}}(\wp_v) = \iota \circ \sigma_v^{(2)}(\mathrm{Frob}_v)$$

for a field isomorphism $\iota : \overline{\mathbb{Q}}_p \simeq \mathbb{C}$.

Remark 3.4. Since the both sides are connected just by a field isomorphism $\iota : \overline{\mathbb{Q}}_p \simeq \mathbb{C}$, this does not mean that the effect of the complex conjugation changes $\sigma^{(1)}$ to $\sigma^{(2)}$ as a continuous character and we shall normalize the both sides of $(\sharp)$ to obtain the continuous Hecke and Galois characters (see §2).

Let us denote $\omega_K^{(1)} = \omega_K$ and $\omega_K^{(2)} = \overline{\omega_K}$. Since $V^{(1)}$ (resp. $V^{(2)}(1)$) has the Hodge-Tate weight $(0)_\tau$, by making the infinite component of $\omega_K^{(1)}$ (resp. $\omega_K^{(2)}(1)$)

trivial, we can obtain the **algebraic Hecke character** $\omega_{K,a}^{(1)}$ (resp. $\omega_{K,a}^{(2)}(1)$) of the weight $(0)_{\iota\circ\tau}$. Conversely, the Galois character which corresponds to the algebraic Hecke character $\omega_{K,a}^{(1)}$ (resp. $\omega_{K,a}^{(2)}(1)$) becomes the **algebraic Galois character** $\sigma_a^{(1)}$ (resp. $\sigma_a^{(2)}(1)$) of the Hodge-Tate weight $(0)_\tau$ and factors through a finite abelian extension K_1/K (resp. K_2/K) by the global class field theory. In this situation, the effect of the complex conjugation changes $\sigma_a^{(1)}$ (resp. $\omega_{K,a}^{(1)}$) to $\sigma_a^{(2)}(1)$ (resp. $\omega_{K,a}^{(2)}(1)$) as a continuous character.

Remark 3.5. Note that these algebraic characters are different from the former ones up to the normalization and that the former characters never factor through finite quotients since the Galois actions on the Tate module $V_p(E)$ are of infinite order.

Example 3.6. Consider the elliptic curve $y^2 = x^3 - Dx$ ($D \in \mathbb{Z}\backslash\{0\}$) which has the complex multiplication by $K = \mathbb{Q}(i)$. Let p denote the prime ideal of $\mathbb{Z}$ such that p does not divide $2D$. By making the infinite components of the Hecke characters trivial, we shall obtain the algebraic Hecke characters.

a). In the case of $p \equiv 3 \pmod 4$, we have $\omega_K^{(1)}(p) = -p$ and we normalize this character as $\omega_{K,a}^{(1)}(p) = -1$. Then, its normalized complex conjugation $\omega_{K,a}^{(2)}(1)(p)$ is also given by $\omega_{K,a}^{(2)}(1)(p) = -1$.

b). Consider the case of $p \equiv 1 \pmod 4$ and then the prime p decomposes as $p = \pi\bar{\pi}$ where π denotes the element of $\mathbb{Z}[i]$ such that we have $\pi \equiv 1 \pmod{2+2i}$. Let $\wp$ denote the prime ideal $\wp = (\pi)$ in $\mathbb{Z}[i]$. It is known that we have $\omega_K^{(1)}(\wp) = \overline{\left(\frac{D}{\pi}\right)}_4\pi$ or $\left(\frac{D}{\pi}\right)_4\bar{\pi}$ (depending on the choice of $\iota : \overline{\mathbb{Q}}_p \simeq \mathbb{C}$) where $\left(\frac{\cdot}{\pi}\right)_4$ denotes the 4^{th}-power residue symbol. Assume that we have $\omega_K^{(1)}(\wp) = \overline{\left(\frac{D}{\pi}\right)}_4\pi$. In this case, we normalize this character as $\omega_{K,a}^{(1)}(\wp) = \overline{\left(\frac{D}{\pi}\right)}_4$ and its normalized complex conjugation $\omega_{K,a}^{(2)}(1)(\wp)$ is given by $\omega_{K,a}^{(2)}(1)(\wp) = \left(\frac{D}{\pi}\right)_4$.

Since one of these local eigenvalues of normalized Hecke characters is a root of unity (i.e. weight 0), this forces the normalized Hecke L-function to be of weight 0 and thus the normalized Hecke characters factor through global finite Galois extensions.

3.3. **Hecke L-function and Dedekind zeta function.** Since the Galois character $\sigma_a^{(1)}$ is non-trivial, we can show that $L(\omega_{K,a}^{(1)}, s)$ does not have any poles or zeros at $s = 1$. Furthermore, we can deduce that the order of $L(\omega_{K,a}^{(2)}(1), s)\mid_{s=0}$ is the same as that of Dedekind zeta function $\zeta_{K_2}(s)\mid_{s=0}$ ([N], p.502, (8.5)).

4. Rational points and unit elements

Choose a prime p which inerts in K such that the extensions K_1/K and K_2/K are of degree prime to p. Since E has the complex multiplication by K and the

prime p inerts in K, the Tate module $\mathbb{V}_p(E)$ over $\mathbb{Q}_p$ is a one dimensional K_p-vector space. Further, recall that $V_p(E)$ over K_p splits as $V_p(E) = V^{(1)} \oplus V^{(2)}$. The assumption that the extensions K_1/K and K_2/K are of degree prime to p is used in ([Ru], p.24-27).

4.1. **Top exact sequence.** Let $T^{(1)}$ denote a free of rank 1 module over $\mathcal{O}_p$ (the ring of integers of K_p) on which G_K acts via $\sigma_a^{(1)}$ and put $W^{(1)} = (T^{(1)} \otimes \mathbb{Q})/T^{(1)}$. Then, it is known that we have

$$\mathrm{Sel}(K, W^{(1)}) \simeq \mathrm{Hom}(A_{K_1}, W^{(1)})^{\mathrm{Gal}(K_1/K)}$$

where A_L denotes the ideal class group of L ([Ru], p.24). Thus, we have an exact sequence $0 \to \mathrm{Ker}\,(f) \to \mathrm{Sel}(K, W^{(1)}) \xrightarrow{f} \mathrm{Sha}(K, W^{(1)})_{p^\infty} \to 0$ of finite torsion modules over $K_p/\mathcal{O}_p$.

4.2. **Middle exact sequence.** In §3.2, for the Galois representation $\sigma_p := \sigma^{(1)} \oplus \sigma^{(2)}$ of G_K on $V_p(E)$ over K_p, we obtain the normalized Galois representation $\sigma_{p,a} := \sigma_a^{(1)} \oplus \sigma_a^{(2)}$. Write the same notations for their restrictions to $\mathbb{V}_p(E)$. Since the Tate module $\mathbb{V}_p(E)$ over $\mathbb{Q}_p$ is a one dimensional K_p-vector space, we can write $\sigma_{p,a} = \sigma_p \cdot \psi_p$ for some character ψ_p of G_K over K_p. On the other hand, since we have $\mathrm{End}(E) \otimes \mathbb{Q}_p \simeq \mathrm{End}(\mathbb{V}_p(E)) : \sigma \otimes 1 \mapsto \sigma_p$ by the isogeny theorem of Faltings, there exists an element $\psi \in \mathrm{End}(E)$ such that we have $\mathrm{End}(E(\psi)) \otimes \mathbb{Q}_p \simeq \mathrm{End}(\mathbb{V}_p(E)(\psi_p)) : (\sigma \cdot \psi) \otimes 1 \mapsto \sigma_p \cdot \psi_p = \sigma_{p,a}$.

4.3. **Bottom exact sequence.** Let $T^{(2)}$ denote a free of rank 1 module over $\mathcal{O}_p$ on which G_K acts via $\sigma_a^{(2)}$ and put $W^{(2)} = (T^{(2)} \otimes \mathbb{Q})/T^{(2)}$. The following notation is used in ([Ru], p25).

Notation: For a $\mathbb{Z}[G_K]$-module B, we define the χ-component of B by

$$B^\chi = \{b \in (B \otimes_{\mathbb{Z}} \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}_p \mid g(b) = \chi(g)b \ (\forall g \in G_K)\}.$$

With this notation, we have an exact sequence of $K_p/\mathcal{O}_p$-modules ([Ru], p.26)

$$0 \to (\mathcal{O}_{K_2}^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{(\sigma_a^{(2)}(1))^{-1}} \to \mathrm{Sel}(K, W^{(2)}) \to (A_{K_2})^{(\sigma_a^{(2)}(1))^{-1}} \to 0.$$

4.4. **Commutative diagram.**

Lemma 4.1. *We have $H^0(G_K, W^{(2)}) = 0$ and $H^2(G_K, W^{(1)}) = 0$.*

Proof. Since G_K acts on $W^{(2)}$ via the character $\sigma_a^{(2)}$, the G_K-invariant part of $W^{(2)}$ is 0 and thus we obtain $H^0(G_K, W^{(2)}) = 0$. As for $H^2(G_K, W^{(1)})$, since G_K acts on $W^{(1)}$ via the finite character $\sigma_a^{(1)}$, we may assume that the extension K_1/K is the finite cyclic extension and we obtain $H^2(G_K, W^{(1)}) = H^2(\mathrm{Gal}(K_1/K), W^{(1)}) = (W^{(1)})^{\mathrm{Gal}(K_1/K)}/N_{\mathrm{Gal}(K_1/K)}(W^{(1)}) = 0$ where N_G is the norm map $N_G(a) = \sum_{g \in G} ga$. □

With this lemma, we have the vanishing of the cohomology groups $\natural$ and $\sharp$ below and thus we obtain the following commutative diagram of $K_p/\mathcal{O}_p$-modules where all of the horizontal and vertical lines are exact.

$$\begin{array}{ccccccccc}
 & & & & & & \natural = 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Ker}\,(f) & \longrightarrow & \mathrm{Sel}(K, W^{(1)}) & \xrightarrow{f} & \mathrm{Sha}(K, W^{(1)})_{p^\infty} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(\psi)^{G_K} \otimes K_p/\mathcal{O}_p & \longrightarrow & \mathrm{Sel}(K, E(\psi)_{p^\infty}) & \longrightarrow & \mathrm{Sha}(K, E(\psi))_{p^\infty} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\mathcal{O}_{K_2}^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{(\sigma_a^{(2)}(1))^{-1}} & \longrightarrow & \mathrm{Sel}(K, W^{(2)}) & \longrightarrow & (A_{K_2})^{(\sigma_a^{(2)}(1))^{-1}} & \longrightarrow & 0. \\
 & & & & \downarrow & & & & \\
 & & & & \sharp = 0 & & & &
\end{array}$$

Lemma 4.2. *If we have* $\mathrm{ord}_{s=1}L(E(\psi)_{/K}, s) = \mathrm{rank}(E(\psi)^{G_K})$*, this leads to* $\mathrm{ord}_{s=1}L(E_{/K}, s) = \mathrm{rank}(E(K))$.

Proof. This follows from ([Ro], p.127) by reversing the procedure and using the fact that all conjugates $E(\psi)(\psi_c^{-1}) \simeq c^{-1}(E(\psi)(\psi_c^{-1})) = c^{-1}(E(\psi))(\psi^{-1}) \simeq E(\psi)(\psi^{-1}) = E$ ($c \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$) give the same L-functions. □

Lemma 4.3. *The rank of* $\mathcal{O}_{K_2}^\times$ *modulo torsions over* $\mathbb{Z}$ *is equal to that of* $(\mathcal{O}_{K_2}^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{(\sigma_a^{(2)}(1))^{-1}}$ *over* $K_p/\mathcal{O}_p$ *(see the notation in* §4.3*).*

Proof. For simplicity, write $\chi = \sigma_a^{(2)}(1)$ and $B = (\mathcal{O}_{K_2}^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}_p$. Since K_2 is the fixed field of the kernel of the finite character χ, we may assume that the extension K_2/K is the finite cyclic extension. Thus, we can write $B = \oplus B^{\chi^i}$ ([Ru], p.25). If n denotes the rank of B over $K_p/\mathcal{O}_p$, all components B^{χ^i} have the same rank n over $K_p/\mathcal{O}_p$; otherwise the character χ factors through a smaller field. □

4.5. **Main results.**

Theorem 4.4. *For an elliptic curve* E/K *with complex multiplication over an imaginary quadratic field* K*, we have*

$$\mathrm{ord}_{s=1}L(E_{/K}, s) = \mathrm{rank}(E(K)).$$

Proof. As for the left vertical in the commutative diagram above, it follows from the snake lemma that the free rank of $E(\psi)^{G_K}$ is equal to that of the unit group $\mathcal{O}_{K_2}^\times$ (Lemma 4.3). Thus, we have $\mathrm{ord}_{s=1}L(E(\psi)_{/K}, s) = \mathrm{rank}(E(\psi)^{G_K})$ (§3.3) and this leads to $\mathrm{ord}_{s=1}L(E_{/K}, s) = \mathrm{rank}(E(K))$ (Lemma 4.2). □

In particular, if E is defined over $\mathbb{Q}$, since we have $L(E_{/K}, s) = L(E_{/\mathbb{Q}}, s)^2$ and $\mathrm{rank}(E(K)) = 2{\cdot}\mathrm{rank}(E(\mathbb{Q}))$ ([M], §1), we obtain $\mathrm{ord}_{s=1}L(E_{/\mathbb{Q}}, s) = \mathrm{rank}(E(\mathbb{Q}))$.

Therefore, it follows that we can determine whether a given natural number N is a congruent number by the criterion of Tunnell for the equation $E_N : y^2 = x^3 - N^2x$.

Acknowledgments. The paper was not completed without the comments by myriad people including the cerebrated mathematicians. Thanks to them, this paper became much more readable than the first version and I welcome any comments from the readers who learn the standard contents of number theory.

References

[F] Fontaine, J-M.:*Représentations p-adiques semi-stables.* Périodes p-adiques (Bures-sur-Yvette, 1988). Astérisque No. 223 (1994), 113–184.

[M] Milne, J-S.:*On the arithmetic of abelian varieties.* Invent. Math. 17 (1972) 177-190.

[N] Neukirch, J.:*Algebraic number theory.* Grundlehren der Mathematischen Wissenschaften 322. Springer-Verlag, Berlin, 1999. xviii+571 pp.

[S] Silverman, J-H.:*Advanced Topics in the Arithmetic of Elliptic Curves.* volume 151 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1994.

[T] Tate, J.: *p-Divisible Groups, Proceedings of a Conference on Local Fields.* pp 158-183.

[Ro] Rohrlich, D-E.:*The vanishing of certain Rankin-Selberg convolutions.* Automorphic Forms and Analytic Number Theory, Les publications CRM, Montreal, 1990, pp. 123-133.

[Ru] Rubin, K.:*Euler systems.* Annals of Mathematics Studies, 147. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000. xii+227 pp.

[Y] Yoshida, T.:*Automorphic representations and Galois representations (in Japanese).* Proceedings of the 17th Number Theory Summer School, Kyoto, 2009.