TOKYO J. MATH.
VOL. 21, NO. 1, 1998

A Construction of Everywhere Good Q-Curves with p-Isogeny

Atsuki UMEGAKI

Waseda University

(Communicated by T. Suzuki)

Abstract. An elliptic curve E defined over $\bar{\mathbf{Q}}$ is called a $\mathbf{Q}$-curve, if E and E^{σ} are isogenous over $\bar{\mathbf{Q}}$ for any σ in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. For a real quadratic field K and a prime number p, we consider a $\mathbf{Q}$-curve E with the following properties: 1) E is defined over K, 2) E has everywhere good reduction over K, 3) there exists a p-isogeny between E and its conjugate E^{σ}. In this paper, a method to construct such a $\mathbf{Q}$-curve E for some p will be given.

1. Introduction.

Let E be an elliptic curve which is defined over the algebraic closure $\bar{\mathbf{Q}}$ of the rational number field $\mathbf{Q}$. An elliptic curve E is called a $\mathbf{Q}$-curve, if E and its Galois conjugate E^{σ} are isogenous over $\bar{\mathbf{Q}}$ for any σ in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. $\mathbf{Q}$-curves are very interesting objects in many aspects of the arithmetic geometry including a generalization of the Taniyama-Shimura conjecture. It is conjectured by Ribet that $\mathbf{Q}$-curves are "modular" in the sense that each should be a factor over $\bar{\mathbf{Q}}$ of the jacobian variety of the modular curve $X_1(N)$ for some N. The following examples for "modular" $\mathbf{Q}$-curves are prototypes of this conjecture. Let $f=\sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight 2 on $\Gamma_1(N)$ which is a common eigenform for the Hecke operators with Nebentypus character χ associated to a real quadratic field K. We denote by K_f the extension over $\mathbf{Q}$ generated by the Fourier coefficients $\{a_n\}$. Then by Shimura [14] we know that there exists an abelian variety A_f defined over $\mathbf{Q}$ attached to f such that its dimension is equal to $d=[K_f:\mathbf{Q}]$ and

$$\mathrm{End}_{\mathbf{Q}}(A_f)\otimes_{\mathbf{Z}}\mathbf{Q}=K_f\,,$$

where $\mathrm{End}_{\mathbf{Q}}(A_f)$ is the endomorphism ring defined over $\mathbf{Q}$ of A_f. Suppose that $d=2$ and χ is a primitive character modulo N. Then we know that the simple components of A_f are $\mathbf{Q}$-curves defined over K, which are called Shimura's elliptic curves. Moreover it is known that they have everywhere good reduction (cf. [2], [9]). Thus it can be said that Shimura's elliptic curves are the simplest nontrivial "modular" $\mathbf{Q}$-curves. We

Received December 12, 1996
Revised September 26, 1997

examine the converse question. Namely for any real quadratic field K, we consider $\mathbf{Q}$-curves E which satisfy the following conditions:

1) E is defined over K,

2) E has everywhere good reduction over K.

Some examples for $\mathbf{Q}$-curves with properties 1) and 2) have been constructed by Cremona [1]. In this paper we discuss a new method to construct such $\mathbf{Q}$-curves. We consider $\mathbf{Q}$-curves E with properties 1), 2) and the additional property

3) E has an isogeny to its conjugate E^{σ} of degree p

for some rational prime p. For $p=2, 3, 5, 7$ and 13, we give a new method to construct $\mathbf{Q}$-curves with properties 1), 2) and 3) systematically.

Here we describe it briefly. For a number field L, a prime ideal $\mathfrak{q}$ of L, a finite extension L' over L and an elliptic curve E over L, we will functorially use the following notation:

$\mathcal{O}_L$: the ring of integers of L,

$v_{\mathfrak{q}}$: the normalized valuation of L with respect to $\mathfrak{q}$, i.e. $v_{\mathfrak{q}}(L)=\mathbf{Z}\cup\{\infty\}$,

$L_{\mathfrak{q}}$: the completion of L with respect to $\mathfrak{q}$,

$\mathrm{D}(L'/L)$: the relative discriminant of L'/L,

$N_{L'/L}$: the norm map of L'/L,

$\mathrm{cond}_L(E)$: the conductor of E over L.

Define a rational function $j(X)$ by

$$(1.1)\qquad j(X)=\begin{cases} 2^6\dfrac{(X+4)^3}{X^2} & \text{if } p=2,\\[2mm] 3^3\dfrac{(X+1)(9X+1)^3}{X} & \text{if } p=3,\\[2mm] \dfrac{(X^2+10X+5)^3}{X} & \text{if } p=5,\\[2mm] \dfrac{(X^2+13X+49)(X^2+5X+1)^3}{X} & \text{if } p=7,\\[2mm] \dfrac{(X^2+5X+13)(X^4+7X^3+20X^2+19X+1)^3}{X} & \text{if } p=13. \end{cases}$$

For any element τ in K with $j(\tau)\neq 0$, 1728, we consider the elliptic curve

$$(1.2)\qquad E_{\tau}: y^2+xy=x^3-\frac{36}{j(\tau)-1728}x-\frac{1}{j(\tau)-1728}$$

defined over K, which has discriminant

$$\Delta(\tau)=\frac{j(\tau)^2}{(j(\tau)-1728)^3}.$$

If p does not split in K, let $\mathfrak{p}$ be the unique prime of K above p. If p splits in K, let $\mathfrak{p}$, $\mathfrak{p}'$ be the primes of K above p. We define the ideal $\mathfrak{a}$ of K by

$$(1.3) \qquad \mathfrak{a}=\begin{cases} \mathcal{O}_K & \text{if } p=2,\,3 \text{ and } p \text{ does not split in } K\,, \\ \mathcal{O}_K \text{ or } \mathfrak{p}^6\mathfrak{p}'^{-6} & \text{if } p=2 \text{ and } 2 \text{ splits in } K\,, \\ \mathfrak{p}^3\mathfrak{p}'^{-3} & \text{if } p=3 \text{ and } 3 \text{ splits in } K\,, \\ \mathfrak{p}^3 & \text{if } p=5\,, \\ \mathfrak{p}^2 & \text{if } p=7\,, \\ \mathfrak{p} & \text{if } p=13\,, \end{cases}$$

and put

$$m_p=\begin{cases} 1 & \text{if } p=2,\,3\,, \\ 5^3 & \text{if } p=5\,, \\ 7^2 & \text{if } p=7\,, \\ 13 & \text{if } p=13\,. \end{cases}$$

Now we state the main theorem, which plays a central role in our construction:

THEOREM 1.1. *Fix a real quadratic field K. The notation is as above.*

a) *Assume that p is equal to* 2. *For the existence of a non-CM* **Q**-*curve with properties* 1), 2) *and* 3), *it is necessary that there exists an element τ in K such that*

$$(1.4) \qquad \tau\mathcal{O}_K=\mathfrak{a}\,, \quad N_{K/\mathbf{Q}}(\tau)=m_p \quad \textit{and} \quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6 \ \textit{for any prime } \mathfrak{q}\,,$$

where u is a unit in K.

b) *Assume that p is equal to* 3, 5, 7, 13. *For the existence of a non-CM* **Q**-*curve with properties* 1), 2) *and* 3), *it is necessary that the rational prime p does not remain prime in K and there exists an element τ in K such that*

$$(1.5) \qquad \tau\mathcal{O}_K=\mathfrak{a}\,, \quad N_{K/\mathbf{Q}}(\tau)=m_p \quad \textit{and} \quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6 \ \textit{for any prime } \mathfrak{q}\,,$$

where u is a unit in K.

c) *Assume that τ satisfies either* (1.4) *or* (1.5). (*We do not have to assume that E_τ is non-CM type.*) *If there exists an element D in K such that*

$$(1.6) \qquad \mathrm{cond}_L E_\tau=\mathcal{O}_L \ \textit{and} \ \mathrm{D}(L/K)^2=\mathrm{cond}_K E_\tau$$

where $L=K(\sqrt{D})$, then there exists a **Q**-*curve with properties* 1), 2) *and* 3). *Moreover the quadratic twist of E_τ by D has properties* 1), 2) *and* 3).

This theorem tells us the necessary and sufficient conditions for the existence of **Q**-curves which we require, and will be proved by using properties of the modular curves as the moduli space of elliptic curves and a parameterization of the points on these curves. In section 2 we explain more precisely an idea for the proof of the theorem and our method to construct such **Q**-curves using it. We prove assertions a) and b) of Theorem 1.1 in section 4. In section 5 we discuss the sufficient conditions for existence and prove the part c) of Theorem 1.1. In section 6 we give some examples for **Q**-curves produced by our method and check their "modularity".

ACKNOWLEDGMENTS. This paper grew out from the author's master thesis. The author expresses sincere thanks to Professors Ki-ichiro Hashimoto and Fumiyuki Momose for kind and warm encouragement during the preparation of this paper.

2. The idea for construction.

In this section we explain our method of construction. Let N be a positive integer, and $\Gamma = \mathrm{SL}_2(\mathbf{Z})$. Define subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$ of Γ by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; c \equiv 0 \pmod N \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; c \equiv 0 \pmod N,\ a \equiv d \equiv 1 \pmod N \right\}.$$

We denote by $X_0(N)$ and $X_1(N)$ the modular curves corresponding to $\Gamma_0(N)$ and $\Gamma_1(N)$, respectively. We recall that they have models defined over **Q**. For any prime number p, any non-cuspidal point of the modular curve $X_0(p)$ corresponds to a triple (E_1, E_2, ϕ) of elliptic curves E_1, E_2 and the isogeny $\phi : E_1 \to E_2$ whose kernel is a cyclic subgroup of order p. Denote by W_p the Atkin-Lehner involution for p. Then W_p induces an involution $(E_1, E_2, \phi) \mapsto (E_2, E_1, \hat{\phi})$ on $X_0(p)$ with the dual isogeny $\hat{\phi}$ of ϕ, which is denoted by the same letter W_p. Moreover we denote by $X_0^*(p)$ the quotient curve of $X_0(p)$ by W_p, which is defined over **Q**. Then we note that any non-cuspidal **Q**-rational point of $X_0^*(p)$ corresponds to a **Q**-curve and conversely any non-CM **Q**-curve corresponds to a **Q**-rational point, as pointed out by Elkies [3]. Therefore for a real quadratic field K, a **Q**-curve E has properties 1) and 3) if and only if the triple (E, E^σ, ψ) is represented by a point on $X_0(p)$, where σ is the generator of the Galois group $\mathrm{Gal}(K/\mathbf{Q})$ and ψ is an isogeny between E and E^σ.

Assume that p is a prime number such that the genus of $X_0(p)$ is zero, namely $p = 2, 3, 5, 7, 13$. Since $X_0(p)$ is isomorphic over **Q** to the projective line $\mathbf{P}^1$, the points of $X_0(p)$ are described by one parameter τ (see Fricke [5]). And we can write the relation between points on $X_0(p)$ and triples (E_1, E_2, ϕ), i.e. we know that the j-invariant of E_1 is equal to $j(\tau)$, where the rational function j is given in (1.1), and the involution W_p acts on the points of $X_0(p)$ by

(2.1)
$$W_p(\tau)=\begin{cases} 1/\tau & \text{if } p=2,3, \\ 5^3/\tau & \text{if } p=5, \\ 7^2/\tau & \text{if } p=7, \\ 13/\tau & \text{if } p=13. \end{cases}$$

If we put $k(X)=j(X)-1728$, then we can write

(2.2)
$$k(X)=\begin{cases} 2^6\dfrac{(X-8)^2(X+1)}{X^2} & \text{if } p=2, \\ 3^3\dfrac{(27X^2+18X-1)^2}{X} & \text{if } p=3, \\ \dfrac{(X^2+22X+125)(X^2+4X+1)^2}{X} & \text{if } p=5, \\ \dfrac{(X^4+14X^3+63X^2+70X-7)^2}{X} & \text{if } p=7, \\ \dfrac{(X^2+6X+13)(X^6+10X^5+46X^4+108X^3+122X^2+38X-1)^2}{X} & \text{if } p=13. \end{cases}$$

We recall that the elliptic curve E_τ given in (1.2) has j-invariant $j(\tau)$ and discriminant

(2.3)
$$\Delta(\tau)=j(\tau)^2/k(\tau)^3 .$$

Now we assume that there exists a **Q**-curve E with properties 1), 2) and 3). If E_τ is isomorphic to E over $\bar{\mathbf{Q}}$, then the Galois action for τ coincides with the action of the involution W_p, i.e. it follows that

(2.4)
$$\tau^\sigma = W_p(\tau) .$$

So one can describe the necessary condition for the existence of such **Q**-curves E by using τ, as in assertions a) and b) of Theorem 1.1.

Using this theorem, we can give an effective procedure to construct such **Q**-curves. At first we fix p and K, and we find a fundamental unit ε of K and a suitable element α in K which generates the ideal $\mathfrak{a}$ given in (1.3) if $\mathfrak{a}$ is principal. Every unit u in K is a power of ε up to sign, so we can write

$$\tau = \pm\alpha\varepsilon^n ,$$

where n is a rational integer. For each n, we calculate $\Delta(\tau)$. If τ satisfies condition (1.4) or (1.5), we check whether there exists an element D in K which actually satisfies condition (1.6). We note that the number of elements in K which have possibility to be D is finite (cf. Remark 5.4). Thus we can obtain **Q**-curves of the type specified.

3. Lemmas.

In this section we show some lemmas to prove our main theorem.

LEMMA 3.1. *Let L be a quadratic field, and E an arbitrary elliptic curve defined over L. Let Δ be the discriminant of E. If there exists an elliptic curve E_0 over L such that E_0 has everywhere good reduction and E_0 is isomorphic to E over the algebraic closure $\bar{L}$ of L, then*

$$v_{\mathfrak{q}}(\Delta) \equiv 0 \pmod{6} \qquad \textit{for any prime } \mathfrak{q} \textit{ of } L\,.$$

PROOF. We suppose that there exists E_0 which satisfies the condition above. If $j(E_0)$ is equal to 0 or 1728, then there exists a prime $\mathfrak{q}$ in L such that E has bad reduction at $\mathfrak{q}$ from Theorem 2 of [13]. So we may assume that $j(E_0) \neq 0$, 1728. Therefore there exists a quadratic extension L' of L such that E and E_0 are isomorphic over L' from [15] chapter X, Proposition 5.4. Let Δ_0 be the discriminant of E_0. Then there exists an element α in L' such that $\Delta = \alpha^{12}\Delta_0$, so it follows that

$$v_{\mathfrak{q}}(\Delta) \equiv v_{\mathfrak{q}}(\Delta_0) = 0 \pmod{6} \qquad \text{for any prime } \mathfrak{q} \text{ of } L\,. \qquad \square$$

LEMMA 3.2. *Let L be a number field and E an elliptic curve defined over L. If E has everywhere good reduction over L, then its j-invariant is an integer of L.*

PROOF. Let $\mathfrak{q}$ be a prime of L. From [15] chapter VII, Proposition 5.5, E has potential good reduction in the completion $L_{\mathfrak{q}}$ of L by $\mathfrak{q}$ if and only if its j-invariant is an integer of $L_{\mathfrak{q}}$. Since this holds for any prime $\mathfrak{q}$, the lemma follows. $\square$

LEMMA 3.3. *Let L be a number field and E an elliptic curve defined over L. For an element D in L, we put $M = L(\sqrt{D})$ and denote by E_D the quadratic twist of E by D. Then the Weil restriction $\mathrm{Res}_{M/L}E$ and the product $E \times E_D$ are isogenous over L.*

PROOF. We put $A = \mathrm{Res}_{M/L}E$. For a rational prime l, let ρ_A (resp. ρ_E) be the l-adic representation over L with respect to A (resp. E). Then it follows that

$$\rho_A = \mathrm{Ind}_M^L(\rho_E|_M) = \rho_E \oplus (\rho_E \otimes \psi)\,,$$

where ψ is the character corresponding to the extension M over L. This means that A is isogenous over L to $E \times E_D$ from [4] chapter IV, Corollary 1.3. This completes the proof of the lemma. $\square$

4. Necessary conditions.

In this section we prove assertions a) and b) of Theorem 1.1. We recall that the prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ defined in section 1 divide p. Moreover we note that we use equations (1.1) and (2.2) many times through this section.

4.1. The case of $p = 2$. PROOF. If τ corresponds to a **Q**-curve, then equation

(2.4) holds, so it follows that

(4.1) $$N_{K/\mathbf{Q}}(\tau)=1$$

from (2.1). At first we assume that 2 remains in K. Then we need that $v_{\mathfrak{p}}(\tau)=0$ from (2.4). Then $v_{\mathfrak{p}}(j(\tau))=6$ and $v_{\mathfrak{p}}(k(\tau))=6+v_{\mathfrak{p}}(\tau+1)$, so $v_{\mathfrak{p}}(\Delta(\tau))=-6-3v_{\mathfrak{p}}(\tau+1)$. From Lemma 3.1, we need that $v_{\mathfrak{p}}(\tau+1)\equiv 0 \pmod 2$. For any prime $\mathfrak{q}$ not dividing 2, if $v_{\mathfrak{q}}(\tau)>0$, then $v_{\mathfrak{q}}(j(\tau))<0$. Therefore we need that

$$v_{\mathfrak{q}}(\tau)=0 \quad \text{and} \quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6$$

from the action of W_2, Lemma 3.1 and Lemma 3.2, so from equation (4.1) it follows that

$$\tau\mathcal{O}_K=\mathcal{O}_K .$$

Now we assume that 2 ramifies in K. As above, we must have $v_{\mathfrak{p}}(\tau)=0$. Then $v_{\mathfrak{p}}(j(\tau))=12$ and $v_{\mathfrak{p}}(k(\tau))=12+v_{\mathfrak{p}}(\tau+1)$, so $v_{\mathfrak{p}}(\Delta(\tau))=-12-3v_{\mathfrak{p}}(\tau+1)$. Thus we need that $v_{\mathfrak{p}}(\tau+1)\equiv 0 \pmod 2$. For other primes $\mathfrak{q}$ not dividing 2, clearly we need that

$$v_{\mathfrak{q}}(\tau)=0 \quad \text{and} \quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6 .$$

From equation (4.1) it follows that

$$\tau\mathcal{O}_K=\mathcal{O}_K.$$

Next we assume that 2 splits in K. If $v_{\mathfrak{p}}(\tau)\geq 7$, then $v_{\mathfrak{p}}(j(\tau))<0$, so we need that $-6\leq v_{\mathfrak{p}}(\tau)\leq 6$. If $v_{\mathfrak{p}}(\tau)=4$, 5, then $v_{\mathfrak{p}}(j(\tau))=12-2v_{\mathfrak{p}}(\tau)$ and $v_{\mathfrak{p}}(k(\tau))=12-2v_{\mathfrak{p}}(\tau)$, so

$$v_{\mathfrak{p}}(\Delta(\tau))=2v_{\mathfrak{p}}(j(\tau))-3v_{\mathfrak{p}}(k(\tau))=-12+2v_{\mathfrak{p}}(\tau)\not\equiv 0 \pmod 6 .$$

If $v_{\mathfrak{p}}(\tau)=-3$, then $v_{\mathfrak{p}}(j(\tau))=3$ and $v_{\mathfrak{p}}(k(\tau))=3$, so $v_{\mathfrak{p}}(\Delta(\tau))=-3\not\equiv 0 \pmod 6$. If $v_{\mathfrak{p}}(\tau)=2$, then $v_{\mathfrak{p}}(j(\tau))=2+3v_{\mathfrak{p}}(\tau+4)$ and $v_{\mathfrak{p}}(k(\tau))=6$, so $v_{\mathfrak{p}}(\Delta(\tau))=6v_{\mathfrak{p}}(\tau+4)-14\not\equiv 0 \pmod 6$. If $v_{\mathfrak{p}}(\tau)=1$, then $v_{\mathfrak{p}}(j(\tau))=7$ and $v_{\mathfrak{p}}(k(\tau))=6$, so $v_{\mathfrak{p}}(\Delta(\tau))=-4\not\equiv 0 \pmod 6$. Therefore from Lemma 3.1 and the action of W_2 we need that $v_{\mathfrak{p}}(\tau)=0$, ± 6. If $v_{\mathfrak{p}}(\tau)=0$, then $v_{\mathfrak{p}}(j(\tau))=6$ and $v_{\mathfrak{p}}(k(\tau))=6+v_{\mathfrak{p}}(\tau+1)$, so $v_{\mathfrak{p}}(\Delta(\tau))=-6-3v_{\mathfrak{p}}(\tau+1)$. If $v_{\mathfrak{p}}(\tau)=\pm 6$, then $v_{\mathfrak{p}}(j(\tau))=v_{\mathfrak{p}}(k(\tau))=0$, so $v_{\mathfrak{p}}(\Delta(\tau))=0$. For other primes $\mathfrak{q}\nmid 2$, clearly we need that

$$v_{\mathfrak{q}}(\tau)=0 \quad \text{and} \quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6 ,$$

so from equation (4.1) it follows that

$$\tau\mathcal{O}_K=\mathcal{O}_K \quad \text{or} \quad \mathfrak{p}^6\mathfrak{p}'^{-6}.$$ □

REMARK 4.1. In order to find τ which satisfies the condition above, we must evaluate the value $v_{\mathfrak{q}}(\Delta(\tau))$ for any prime $\mathfrak{q}$, and it is often difficult to compute $v_{\mathfrak{q}}(\Delta(\tau))$, since the absolute value of a fundamental unit of K becomes very large. Fortunately, it is rather easy for any prime ideal dividing 2. Namely if 2 does not split in K, then it is sufficient to check that

$$v_{\mathfrak{p}}(\tau+1)\equiv 0 \pmod 2 .$$

If 2 splits in K and $\tau\mathcal{O}_K=\mathcal{O}_K$, then it is sufficient to check that

$$v_{\mathfrak{p}}(\tau+1)\equiv v_{\mathfrak{p}'}(\tau+1)\equiv 0 \pmod 2,$$

and if 2 splits in K and $\tau\mathcal{O}_K=\mathfrak{p}^6\mathfrak{p}'^{-6}$, we do not need to evaluate the value $v_{\mathfrak{p}}(\Delta(\tau))$.

4.2. The case of $p=3$. PROOF. If τ corresponds to a **Q**-curve, then equation (2.4) holds, so it follows that

$$N_{K/\mathbf{Q}}(\tau)=1 \tag{4.2}$$

from (2.1). If 3 remains prime in K, then we need that $v_{\mathfrak{p}}(\tau)=0$ from (2.4). Then $v_{\mathfrak{p}}(j(\tau))\geq 3$ and $v_{\mathfrak{p}}(k(\tau))=3$, so

$$v_{\mathfrak{p}}(\Delta(\tau))=2v_{\mathfrak{p}}(j(\tau))-9\not\equiv 0 \pmod 6.$$

This contradicts Lemma 3.1. Therefore 3 does not remain prime in K.

Now we assume that 3 ramifies in K. Then we need that $v_{\mathfrak{p}}(\tau)=0$ from the same reason as above. If $v_{\mathfrak{p}}(\tau)=0$, then $v_{\mathfrak{p}}(j(\tau))=6+v_{\mathfrak{p}}(\tau+1)$ and $v_{\mathfrak{p}}(k(\tau))=6$, so $v_{\mathfrak{p}}(\Delta(\tau))=2v_{\mathfrak{p}}(\tau+1)-6$. Therefore we need that $v_{\mathfrak{p}}(\tau)=0$ and $v_{\mathfrak{p}}(\tau+1)\equiv 0 \pmod 3$. For other primes $\mathfrak{q}$ not dividing 3, clearly we need that

$$v_{\mathfrak{q}}(\tau)=0 \quad \text{and} \quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6,$$

so from equation (4.2) it follows that

$$\tau\mathcal{O}_K=\mathcal{O}_K.$$

Next we assume that 3 splits in K. If $v_{\mathfrak{p}}(\tau)\geq 4$, then $v_{\mathfrak{p}}(j(\tau))<0$. If $v_{\mathfrak{p}}(\tau)=1, 2$, then $v_{\mathfrak{p}}(j(\tau))=3-v_{\mathfrak{p}}(\tau)$ and $v_{\mathfrak{p}}(k(\tau))=3-v_{\mathfrak{p}}(\tau)$, so

$$v_{\mathfrak{p}}(\Delta(\tau))=2v_{\mathfrak{p}}(j(\tau))-3v_{\mathfrak{p}}(k(\tau))=-3+v_{\mathfrak{p}}(\tau)\not\equiv 0 \pmod 6.$$

Moreover, if $v_{\mathfrak{p}}(\tau)=0$, then $v_{\mathfrak{p}}(j(\tau))\geq 3$ and $v_{\mathfrak{p}}(k(\tau))=3$, so

$$v_{\mathfrak{p}}(\Delta(\tau))=2v_{\mathfrak{p}}(j(\tau))-9\not\equiv 0 \pmod 6.$$

Therefore we need that $v_{\mathfrak{p}}(\tau)=\pm 3$ from Lemma 3.1 and the action of W_3. Then $v_{\mathfrak{p}}(j(\tau))=0$ and $v_{\mathfrak{p}}(k(\tau))=0$, so $v_{\mathfrak{p}}(\Delta(\tau))=0$, and the same holds for $\mathfrak{p}'$. For other primes $\mathfrak{q}$ not dividing 3, clearly we need that

$$v_{\mathfrak{q}}(\tau)=0 \quad \text{and} \quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6,$$

so from equation (4.2) it follows that

$$\tau\mathcal{O}_K=\mathfrak{p}^3\mathfrak{p}'^{-3}.$$

□

REMARK 4.2. As in Remark 4.1, it is rather easy to evaluate the value $v_{\mathfrak{q}}(\Delta(\tau))$ in the case where $\mathfrak{q}=\mathfrak{p}$ or $\mathfrak{p}'$. Namely if 3 ramifies in K, then it is sufficient to check that

$$v_{\mathfrak{p}}(\tau+1)\equiv 0 \pmod 3,$$

and if 3 splits in K, then we do not need to evaluate the value $v_{\mathfrak{p}}(\Delta(\tau))$.

4.3. The case of $p=5$. PROOF. If τ corresponds to a **Q**-curve, then equation (2.4) holds, so

$$N_{K/\mathbf{Q}}(\tau)=5^3 \tag{4.3}$$

from (2.1). If 5 remains prime in K, then from (2.4)

$$2v_{\mathfrak{p}}(\tau)=v_{\mathfrak{p}}(\tau)+v_{\mathfrak{p}}({}^{\sigma}\tau)=3\ ,$$

but this cannot occur.

Now we assume that 5 ramifies in K. Then we need that $v_{\mathfrak{p}}(\tau)=3$. If $v_{\mathfrak{p}}(\tau)=3$, then $v_{\mathfrak{p}}(j(\tau))=3$ and $v_{\mathfrak{p}}(k(\tau))=0$, so it follows that $v_{\mathfrak{p}}(\Delta(\tau))=6$. For other primes $\mathfrak{q}$ not dividing 5, clearly we need that

$$v_{\mathfrak{q}}(\tau)=0 \quad\text{and}\quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6\ ,$$

so from equation (4.3) it follows that

$$\tau\mathcal{O}_K=\mathfrak{p}^3.$$

Next we assume that 5 splits in K. If $v_{\mathfrak{p}}(\tau)\geq 4$, then $v_{\mathfrak{p}}(j(\tau))<0$. If $v_{\mathfrak{p}}(\tau)=1$, then $v_{\mathfrak{p}}(j(\tau))=2$ and $v_{\mathfrak{p}}(k(\tau))=0$, so $v_{\mathfrak{p}}(\Delta(\tau))=4$. From the action of W_5 on $X_0(5)$ and Lemma 2.3 we need that $v_{\mathfrak{p}}(\tau)=0, 3$. If $v_{\mathfrak{p}}(\tau)=0, 3$, then $v_{\mathfrak{p}}(j(\tau))=0$ and $v_{\mathfrak{p}}(k(\tau))\geq 0$, so $v_{\mathfrak{p}}(\Delta(\tau))=-3v_{\mathfrak{p}}(k(\tau))$. Therefore $v_{\mathfrak{p}}(k(\tau))\equiv 0 \pmod 2$, and the same holds for $\mathfrak{p}'$. For other primes $\mathfrak{q}$ not dividing 5, we clearly need that

$$v_{\mathfrak{q}}(\tau)=0 \quad\text{and}\quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6\ ,$$

so from equation (4.3) it follows that

$$\tau\mathcal{O}_k=\mathfrak{p}^3\ . \qquad \square$$

REMARK 4.3. As in Remark 4.1, we must evaluate the value $v_{\mathfrak{q}}(\Delta(\tau))$ for any prime $\mathfrak{q}$, fortunately it is rather easy for any prime ideal dividing 5. Namely if 5 splits in K, then it is sufficient to check that

$$v_{\mathfrak{p}}(k(\tau))\equiv v_{\mathfrak{p}'}(k(\tau))\equiv 0 \pmod 2\ ,$$

and if 5 ramifies in K, then we do not need to evaluate the value $v_{\mathfrak{p}}(\Delta(\tau))$.

4.4. The case of $p=7$. PROOF. If τ corresponds to a **Q**-curve, then equation (2.4) holds, so

$$N_{K/\mathbf{Q}}(\tau)=7^2 \tag{4.4}$$

from (2.1). If the rational prime 7 remains prime in K, then we need that $v_{\mathfrak{p}}(\tau)=1$ from (2.4). Then $v_{\mathfrak{p}}(j(\tau))=0$ and $v_{\mathfrak{p}}(k(\tau))=1$, so $v_{\mathfrak{p}}(\Delta(\tau))=-3\not\equiv 0 \pmod 6$. This is contradictory to Lemma 3.1.

We assume that 7 ramifies in K. Then we need that $v_{\mathfrak{p}}(\tau)=2$, so $v_{\mathfrak{p}}(j(\tau))=0$ and $v_{\mathfrak{p}}(k(\tau))=2$. Therefore it follows that $v_{\mathfrak{p}}(\Delta(\tau))=-6$. For other primes $\mathfrak{q}\nmid 7$, clearly we must have

$$v_{\mathfrak{q}}(\tau)=0 \quad\text{and}\quad v_{\mathfrak{q}}(\Delta(\tau))=0 \pmod 6)$$

from Lemma 3.2, so from equation (4.4) it follows that

$$\tau\mathcal{O}_K=7\mathcal{O}_K=\mathfrak{p}^2 .$$

Next we assume that 7 splits in K. If $v_{\mathfrak{p}}(\tau)\geq 3$, then $v_{\mathfrak{p}}(j(\tau))<0$. If $v_{\mathfrak{p}}(\tau)=1$, then $v_{\mathfrak{p}}(j(\tau))=0$ and $v_{\mathfrak{p}}(k(\tau))=1$, so $v_{\mathfrak{p}}(\Delta(\tau))=-3\not\equiv 0 \pmod 6$. Thus we need that $v_{\mathfrak{p}}(\tau)=0, 2$ from the action of W_7 on $X_0(7)$ and Lemma 3.1. If $v_{\mathfrak{p}}(\tau)=0, 2$, then $v_{\mathfrak{p}}(j(\tau))\geq 0$ and $v_{\mathfrak{p}}(k(\tau))=0$, so $v_{\mathfrak{p}}(\Delta(\tau))=2v_{\mathfrak{p}}(j(\tau))$. Therefore it follows that $v_{\mathfrak{p}}(j(\tau))\equiv 0 \pmod 3$. Similarly, for any prime $\mathfrak{q}\nmid 7$, if $v_{\mathfrak{q}}(\tau)>1$, then $v_{\mathfrak{q}}(j(\tau))<0$, so we need that

$$v_{\mathfrak{q}}(\tau)=0 \quad\text{and}\quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6 .$$

From equation (4.4) it follows that

$$\tau\mathcal{O}_K=\mathfrak{p}^2. \qquad \square$$

REMARK 4.4. As in Remark 4.1, it is rather easy to evaluate the value $v_{\mathfrak{q}}(\Delta(\tau))$ in the case where $\mathfrak{q}=\mathfrak{p}$ or $\mathfrak{p}'$. Namely if 7 splits in K, then it is sufficient to check that

$$v_{\mathfrak{p}}(j(\tau))\equiv v_{\mathfrak{p}'}(j(\tau))\equiv 0 \pmod 3 ,$$

and if 7 ramifies in K, then we do not need to evaluate the value $v_{\mathfrak{p}}(\Delta(\tau))$.

4.5. The case of $p=13$.* PROOF. If τ corresponds to a **Q**-curve, then equation (2.4) holds, so

$$N_{N/\mathbf{Q}}(\tau)=13 \tag{4.5}$$

from (2.1). If 13 remains prime in K, then from (2.4)

$$2v_{\mathfrak{p}}(\tau)=v_{\mathfrak{p}}(\tau)+v_{\mathfrak{p}}({}^{\sigma}\tau)=1 ,$$

but this cannot occur.

Now we assume that 13 ramifies in K. Then we need that $v_{\mathfrak{p}}(\tau)=1$. Then $v_{\mathfrak{p}}(j(\tau))=0$ and $v_{\mathfrak{p}}(k(\tau))=0$, so $v_{\mathfrak{p}}(\Delta(\tau))=0$. For other $\mathfrak{q}$ prime to 13, clearly we need that

$$v_{\mathfrak{q}}(\tau)=0 \quad\text{and}\quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6 ,$$

so from equation (4.5) it follows that

$$\tau\mathcal{O}_K=\mathfrak{p} .$$

* In the case of $p=13$, the author finds that Pinch showed the fact that there does not exist a **Q**-curve with properties 1), 2) and 3) (cf. R. G. E. Pinch, *Elliptic curves over number fields*, Doc. Phil. Thesis, Oxford University (1982)).

Next we assume that 13 splits in K. If $v_{\mathfrak{p}}(\tau)\geq 2$, then $v_{\mathfrak{p}}(j(\tau))<0$. Therefore we need that $v_{\mathfrak{p}}(\tau)=0$, 1 from the action of W_{13} on $X_0(13)$. If $v_{\mathfrak{p}}(\tau)=0$, 1, then $v_{\mathfrak{p}}(j(\tau))$, $v_{\mathfrak{p}}(k(\tau))\geq 0$. Similarly, for any other prime $\mathfrak{q}$ not dividing 13, if $v_{\mathfrak{q}}(\tau)>1$, then $v_{\mathfrak{q}}(j(\tau))<0$, so we need that

$$v_{\mathfrak{q}}(\tau)=0 \quad \text{and} \quad v_{\mathfrak{q}}(\Delta(\tau))\equiv 0 \pmod 6 .$$

From equation (4.5) it follows that

$$\tau\mathcal{O}_K=\mathfrak{p} . \qquad \square$$

REMARK 4.5. We must evaluate the value $v_{\mathfrak{q}}(\Delta(\tau))$ for any prime $\mathfrak{q}$, fortunately it is rather easy for any prime ideal dividing 13 as in Remark 4.1. Namely if 13 ramifies in K, then we do not need to evaluate the value $v_{\mathfrak{p}}(\Delta(\tau))$.

5. Sufficient conditions.

We have proved the necessary conditions for the existence of **Q**-curves with properties 1), 2) and 3). Next we discuss the sufficient conditions for the existence of such **Q**-curves. In the following, for a triple (p, K, τ) of a rational prime p, a real quadratic field K and an element τ in K, we say that (p, K, τ) has property $(*)$ if (p, K, τ) satisfies assertions a) or b) of Theorem 1.1. Fix a prime number p. Now for any triple (p, K, τ) with property $(*)$ we consider the case where we can form a **Q**-curve

$$E: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

with everywhere good reduction using the elliptic curve E_τ defined by (1.2). Let $\Delta(\tau)$ be the discriminant of E_τ, and $\mathfrak{q}_1, \cdots, \mathfrak{q}_r$ the primes of K dividing $\Delta(\tau)$. One can rewrite E_τ in the short form

$$E'_\tau: y^2=x^3+c_4x+c_6, \quad c_4, c_6\in\mathcal{O}_K .$$

From the choice of τ,

$$v_{\mathfrak{q}_i}(\Delta(E'_\tau))\equiv 0, 6 \pmod{12}$$

for $i=1, \cdots, r$. Now we consider the quadratic twist

$$E'_{\tau,D}: y^2=x^3+D^2c_4x+D^3c_6$$

of E'_τ by an element D in K. If the class number h_K of K is equal to 1, then one can find a sequence $\{\alpha_i\}_{i=1,\cdots,r}$ of elements in K such that

$$\begin{cases} \alpha_i\mathcal{O}_K=\mathfrak{q}_i & \text{if} \quad v_{\mathfrak{q}_i}(\Delta(E'_\tau))\equiv 6 \pmod{12} , \\ \alpha_i=1 & \text{if} \quad v_{\mathfrak{q}_i}(\Delta(E'_\tau))\equiv 0 \pmod{12} . \end{cases}$$

So if we put $D_0=\prod_i\alpha_i$, then the quadratic twist E'_{τ,D_0} of E'_τ has good reduction at any $\mathfrak{q}$ prime to 6. Thus we know the following:

REMARK 5.1. Assume that $h_K=1$. If we find an element τ in K such that (p, K, τ) has property $(*)$, we can get a **Q**-curve which has good reduction at any prime $\mathfrak{q}$ not dividing 2 or 3 and which also satisfies conditions 1) and 3) in §1.

It remains to check whether $E'_{\tau,D}$ has good reduction at all prime ideals dividing 6. To determine exactly the reduction type of $E'_{\tau,D}$ at $\mathfrak{q}$ dividing 6, we consider the conductors of E over K and L.

PROPOSITION 5.2. *Assume that the triple (p, K, τ) has property $(*)$. We put E_τ as in* (1.2). *For an element D in K, let $E'_{\tau,D}$ be the quadratic twist by D and $L=K(\sqrt{D})$. Then $E'_{\tau,D}$ has everywhere good reduction over K if and only if*

$$\mathrm{cond}_L E_\tau = \mathcal{O}_L \quad \textit{and} \quad \mathrm{D}(L/K)^2 = \mathrm{cond}_K E_\tau .$$

REMARK 5.3. In this proposition, we do not assume that K has class number 1.

PROOF. Denote by A the Weil restriction $\mathrm{Res}_{L/K}(E_\tau)$ of E_τ. Then we recall that A is isogenous to $E_\tau \times E'_{\tau,D}$ over K from Lemma 3.3. From [12] Proposition 1, we know that

$$\mathrm{cond}_K A = N_{L/K}(\mathrm{cond}_L E_\tau) \cdot \mathrm{D}(L/K)^2 .$$

Then

$$\mathrm{cond}_K(E_\tau \times E'_{\tau,D}) = \mathrm{cond}_K E_\tau \cdot \mathrm{cond}_K E'_{\tau,D} ,$$

so it follows that

$$N_{L/K}(\mathrm{cond}_L E_\tau) \cdot \mathrm{D}(L/K)^2 = \mathrm{cond}_K E_\tau \cdot \mathrm{cond}_K E'_{\tau,D} . \tag{5.1}$$

We assume that $E'_{\tau,D}$ has everywhere good reduction. Since it is equivalent to $\mathrm{cond}_K E'_{\tau,D} = \mathcal{O}_K$ that $E'_{\tau,D}$ has everywhere good reduction over K, it is also equivalent to

$$N_{L/K}(\mathrm{cond}_L E_\tau) \cdot \mathrm{D}(L/K)^2 = \mathrm{cond}_K E_\tau . \tag{5.2}$$

We note that E_τ and $E'_{\tau,D}$ are isomorphic over L. If $E'_{\tau,D}$ has everywhere good reduction over K, then $E'_{\tau,D}$ also has everywhere good reduction over L, so $\mathrm{cond}_L E_\tau$ is trivial and

$$\mathrm{D}(L/K)^2 = \mathrm{cond}_K E_\tau .$$

Conversely if $\mathrm{cond}_L E_\tau = \mathrm{cond}_L E'_{\tau,D} = \mathcal{O}_L$ and $\mathrm{D}(L/K)^2 = \mathrm{cond}_K E_\tau$, then $E'_{\tau,D}$ has everywhere good reduction in K from (5.1). So we have completed the proof of Proposition 5.2. □

Clearly assertion c) of Theorem 1.1 follows from Proposition 5.2.

REMARK 5.4. In assertion c) of Theorem 1.1, the number of prime ideals in K which ramify in the extension L/K is finite, since the number of bad primes is finite for any elliptic curves. Thus the number of elements in K which have possibility to be D is finite. Therefore we can determine whether there exists a **Q**-curve with properties 1),

2) and 3).

6. Examples and their modularity.

All the calculations in the following were done on SparcStation with GNU C and PARI-library, version 1.39. The calculation of global minimal models is based on Laska's algorithm (cf. [10], [11]) and the calculation of conductors is based on Tate's algorithm.

Using our method, we can find many triples (p, K, τ) with property $(*)$. We can construct **Q**-curves with properties 1), 2) and 3) as follows.

EXAMPLE 6.1. Let $p=3$ and $K=\mathbf{Q}(\sqrt{997})$. The quadratic field K has a fundamental unit $\varepsilon=84906+2689\sqrt{997}$ and class number 1, and the rational prime 3 splits in K. Put

$$\alpha=\frac{58275188611277+1845593740900\sqrt{997}}{27},$$

then $\alpha\mathcal{O}_K=\mathfrak{p}^3\mathfrak{p}'^{-3}$. For $\tau=\alpha\varepsilon^{-2}=(2021+64\sqrt{997})/27$, we can verify that the triple (p, K, τ) has property $(*)$. Then

$$\mathrm{cond}_K E_\tau=(2^4\cdot 7^2\cdot \pi_{67}^2\cdot \pi_{4597}^2),$$

where $\pi_{67}=(-27+\sqrt{997})/2$ and $\pi_{4597}=2304+73\sqrt{997}$ are prime elements of prime ideals over 67 and 4597 of degree 1, respectively. Moreover

$$D=-7\cdot \pi_{67}\cdot \pi_{4597}=\frac{74011+2331\sqrt{997}}{2},$$

for which $N_{K/\mathbf{Q}}\mathrm{D}(L/K)=2^4\cdot 7^2\cdot 67\cdot 4597$, satisfies condition (1.6). So we can get a **Q**-curve E with properties 1), 2) and 3) whose global minimal Weierstrass equation is defined by

$$y^2+y=x^3+x^2-(129490+4101\sqrt{997})x-\frac{50814489+1609311\sqrt{997}}{2}.$$

This is isomorphic over K to the quadratic twist $E'_{\tau,D}$ of E_τ. Then E has discriminant

$$\Delta=14418057673+456624468\sqrt{997}=\varepsilon^2$$

and j-invariant

$$j=j(\tau)=33308803072+1054900224\sqrt{997}.$$

EXAMPLE 6.2. Let $p=5$ and $K=\mathbf{Q}(\sqrt{461})$. The quadratic field K has a fundamental unit $\varepsilon=(365+17\sqrt{461})/2$ and class number 1, and the rational prime 5 splits in K. Put

$$\alpha = -4788 + 223\sqrt{461},$$

then $\alpha\mathcal{O}_K = \mathfrak{p}^3$. For $\tau = -\alpha\varepsilon = (-31 + \sqrt{461})/2$, we can verify that (p, K, τ) has property $(*)$. Then one can find a $\mathbf{Q}$-curve E with properties 1), 2) and 3) which has the following global minimal Weierstrass equation:

$$y^2 + \frac{3+\sqrt{461}}{2}xy = x^3 + x^2 + (42907827 + 1998409\sqrt{461})x - \frac{58348803105 + 2717574729\sqrt{461}}{2}.$$

Then E has discriminant

$$\Delta = -\frac{4197215256069455887008062 7 + 1954838033345010483647275\sqrt{461}}{2} = -\varepsilon^{10}$$

and j-invariant

$$j = j(\tau) = \frac{-3048867 + 142155\sqrt{461}}{2}.$$

EXAMPLE 6.3. Let $p = 7$ and $K = \mathbf{Q}(\sqrt{497})$. The quadratic field K has a fundamental unit $\varepsilon = 1201887 + 53912\sqrt{497}$ and class number 1, and the rational prime 7 ramifies in K. For $\tau = 7$, one can construct a $\mathbf{Q}$-curve E_1 with properties 1), 2) and 3) which has a global minimal model

$$y^2 + xy = x^3 - x^2 - \frac{12770049 + 572815\sqrt{497}}{2}x - \frac{17560440233 + 787693397\sqrt{497}}{2}.$$

Then E_1 has discriminant

$$\Delta = 694465866194667875 1 + 311510514535059400\sqrt{497} = \varepsilon^3$$

and j-invariant

$$j = j(\tau) = 16581375 = 3^3 \cdot 5^3 \cdot 17^3.$$

For $\tau = -7$ one can also find a $\mathbf{Q}$-curve E_2 with properties 1), 2) and 3) whose global minimal model is

$$y^2 + xy = x^3 - x^2 - \frac{751179 + 33695\sqrt{497}}{2}x - \frac{307946113 + 13813271\sqrt{497}}{2}.$$

Then E_2 has discriminant

$$\Delta = -6944658661946678751 - 311510514535059400\sqrt{497} = -\varepsilon^3$$

and j-invariant

$$j = -3375 = -3^3 \cdot 5^3 .$$

For a real quadratic field K whose discriminant N is one of

28, 56, 77, 161, 301, 497, 553, 749, 889, 1057, 1141, 1253, 1337, 1477, 1673, 1841,

we can get two **Q**-curves which have properties 1), 2) and 3) and j-invariants

$$j = 16581375, \ -3375 .$$

Assume that K has class number 1 and its discriminant is less than 1000. Using our method, we can construct **Q**-curves with properties 1), 2) and 3) for a prime p and a real quadratic field K whose discriminant is equal to N listed in Table 1.

TABLE 1

p	N
2	24, 41, 88, 152, 337, 344, 472, 536, 664, 856, 881
3	109, 997
5	29, 349, 461, 509
7	28, 56, 77, 161, 301, 497, 553, 749, 889

REMARK 6.4. In the case of $h_K \neq 1$, we can also get such **Q**-curves. For example, we can find by our method a **Q**-curve for $p=2$ and $N=257$ (resp. $p=5$ and $N=229$), which is listed in Cremona [1].

The following modularity problem arises naturally:

PROBLEM 6.5. For a prime number p and a real quadratic field K, we assume that there exists a **Q**-curve E with properties 1), 2) and 3). Let N be the discriminant of K, and $S_2^0(N, \chi)$ the space of cusp forms of weight 2 on $\Gamma_1(N)$ with Nebentypus character χ which is a primitive real quadratic Dirichlet character. Is E modular? In other words, does there exist a cusp form f in $S_2^0(N, \chi)$ corresponding to E?

We can check this modularity problem for elliptic curves given in the examples above. For a **Q**-curve E over K with everywhere good reduction, let $A = \mathrm{Res}_{K/\mathbf{Q}} E$ be the Weil restriction of E. Then A is a **Q**-simple abelian variety over **Q** of dimension 2, which is isogenous to $E \times {}^{\sigma}E$ over K. For all primes $\mathfrak{q}$ in K, we denote by $\kappa_{\mathfrak{q}}$ the finite field $\mathcal{O}_K/\mathfrak{q}\mathcal{O}_K$, and denote by $\tilde{E}_{\mathfrak{q}}$ the reduction of E at $\mathfrak{q}$. Then we put

$$c_{\mathfrak{q}} = 1 + \#\kappa_{\mathfrak{q}} - \#\tilde{E}_{\mathfrak{q}}(\kappa_{\mathfrak{q}}) ,$$

and we define a_q, b_q which satisfy the following equation:

$$f_q(u)=\begin{cases} 1-c_{\mathfrak{q}}u^2+q^2u^4 & \text{if } q \text{ remains prime in } K, \\ 1-c_{\mathfrak{q}}u+qu^2 & \text{if } q \text{ ramifies in } K, \\ (1-c_{\mathfrak{q}}u+qu^2)(1-c_{\mathfrak{q}'}u+qu^2) & \text{if } q \text{ splits in } K, \end{cases}$$
$$=(1-a_qu+\chi(q)qu^2)(1-b_qu+\chi(q)qu^2),$$

where $\mathfrak{q}$, $\mathfrak{q}'$ are the primes over the rational prime q and χ is the Dirichlet character corresponding to K. Then we note that a_q and b_q are determined up to order. Then the L-series of A over $\mathbf{Q}$ is defined to be the infinite product

$$L(s, A/\mathbf{Q})=\prod_{q\in P} f_q(q^{-s})^{-1},$$

where P is the set of all rational prime numbers.

On the other hand, if there exists a two-dimensional $\mathbf{Q}$-simple subspace in $S_2^0(N, \chi)$ corresponding to E, then let f_1 and f_2 be the normalized cusp forms which are common eigen forms of the Hecke operators and span the two-dimensional subspace. Then we denote by A_n and B_n the n-th Fourier coefficients of f_1 and f_2, respectively.

In the following, we know the existence of a suitable two-dimensional subspace in $S_2^0(N, \chi)$ and the Fourier coefficients A_n and B_n of the basis from Hasegawa [7].

EXAMPLE 6.6. For Example 6.1, there exists a two-dimensional $\mathbf{Q}$-simple subspace in $S_2^0(997, \chi)$ where χ is the real quadratic character $\left(\frac{997}{\cdot}\right)$. Then we can see the good correspondence as in Table 2.

TABLE 2. Data of L-series (for Example 6.1)

q	$\#\tilde{E}_{\mathfrak{q}}(\kappa_{\mathfrak{q}})$	$c_{\mathfrak{q}}$	a_q, b_q	A_q	B_q	q	$\#\tilde{E}_{\mathfrak{q}}(\kappa_{\mathfrak{q}})$	$c_{\mathfrak{q}}$	a_q, b_q	A_q	B_q
2	1	4	0, 0	0	0	43	1872	-22	$\pm 6\sqrt{-3}$	$-6\sqrt{-3}$	$6\sqrt{-3}$
3	3, 3	1	1, 1	1	1	47	2224	-14	$\pm 6\sqrt{-3}$	$-6\sqrt{-3}$	$6\sqrt{-3}$
5	28	-2	$\pm 2\sqrt{-3}$	$2\sqrt{-3}$	$-2\sqrt{-3}$	53	63, 63	-9	$-9, -9$	-9	-9
7	36	14	0, 0	0	0	59	63, 63	-3	$-3, -3$	-3	-3
11	112	10	$\pm 2\sqrt{-3}$	$2\sqrt{-3}$	$-2\sqrt{-3}$	61	3708	14	$\pm 6\sqrt{-3}$	$-6\sqrt{-3}$	$6\sqrt{-3}$
13	15, 15	-1	$-1, -1$	-1	-1	67	73, 73	-5	$-5, -5$	-5	-5
17	268	22	$\pm 2\sqrt{-3}$	$-2\sqrt{-3}$	$2\sqrt{-3}$	71	75, 75	-3	$-3, -3$	-3	-3
19	16, 16	4	4, 4	4	4	73	72, 72	2	2, 2	2	2
23	27, 27	-3	$-3, -3$	-3	-3	79	87, 87	-7	$-7, -7$	-7	-7
29	832	10	$\pm 4\sqrt{-3}$	$4\sqrt{-3}$	$-4\sqrt{-3}$	83	72, 72	12	12, 12	12	12
31	24, 24	8	8, 8	8	8	89	75, 75	15	15, 15	15	15
37	1404	-34	$\pm 6\sqrt{-3}$	$6\sqrt{-3}$	$-6\sqrt{-3}$	97	96, 96	2	2, 2	2	2
41	1648	34	$\pm 4\sqrt{-3}$	$4\sqrt{-3}$	$-4\sqrt{-3}$						

EXAMPLE 6.7. For Example 6.2, there exists a two-dimensional $\mathbf{Q}$-simple subspace in $S_2^0(461, \chi)$ where χ is the real quadratic character $\left(\frac{461}{\cdot}\right)$. Then we can see the good

correspondence as in Table 3.

Moreover, we can prove that E has modularity from Hasegawa-Hashimoto-Momose [8] in this example.

TABLE 3. Data of L-series (for Example 6.2)

q	$\sharp\tilde{E}_q(\kappa_q)$	c_q	a_q, b_q	A_q	B_q	q	$\sharp\tilde{E}_q(\kappa_q)$	c_q	a_q, b_q	A_q	B_q
2	6	-1	$\pm\sqrt{-5}$	$\sqrt{-5}$	$-\sqrt{-5}$	43	48, 48	-4	$-4, -4$	-4	-4
3	4	6	0, 0	0	0	47	2161	49	$\pm 3\sqrt{-5}$	$-3\sqrt{-5}$	$3\sqrt{-5}$
5	5, 5	1	1, 1	1	1	53	48, 48	6	6, 6	6	6
7	41	9	$\pm\sqrt{-5}$	$\sqrt{-5}$	$-\sqrt{-5}$	59	54, 54	6	6, 6	6	6
11	105	17	$\pm\sqrt{-5}$	$\sqrt{-5}$	$-\sqrt{-5}$	61	55, 55	7	7, 7	7	7
13	144	26	0, 0	0	0	67	66, 66	2	2, 2	2	2
17	15, 15	3	3, 3	3	3	71	5025	17	$\pm 5\sqrt{-5}$	$-5\sqrt{-5}$	$5\sqrt{-5}$
19	20, 20	0	0, 0	0	0	73	68, 68	6	6, 6	6	6
23	30, 30	-6	$-6, -6$	-6	-6	79	6164	78	$\pm 4\sqrt{-5}$	$4\sqrt{-5}$	$-4\sqrt{-5}$
29	804	38	$\pm 2\sqrt{-5}$	$2\sqrt{-5}$	$-2\sqrt{-5}$	83	6729	161	$\pm\sqrt{-5}$	$-\sqrt{-5}$	$\sqrt{-5}$
31	945	17	$\pm 3\sqrt{-5}$	$-3\sqrt{-5}$	$3\sqrt{-5}$	89	101, 101	-11	$-11, -11$	-11	-11
37	1376	-6	$\pm 4\sqrt{-5}$	$4\sqrt{-5}$	$-4\sqrt{-5}$	97	96, 96	2	2, 2	2	2
41	37, 37	5	5, 5	5	5						

EXAMPLE 6.8. For Example 6.3, E_1 and E_2 have CM j-invariants, so we know that they are modular from Shimura [14]. There exists a two-dimensional **Q**-simple subspace in $S_2^0(497, \chi)$ where χ is the real quadratic character $\left(\frac{497}{\cdot}\right)$. Then we can see that two **Q**-curves E_1, E_2 have the same a_q, b_q. Then they have the good correspondence as in Table 4.

TABLE 4. Data of L-series (for Example 6.3)

q	$\sharp(\tilde{E}_i)_q(\kappa_q)$	c_q	a_q, b_q	A_q	B_q	q	$\sharp(\tilde{E}_i)_q(\kappa_q)$	c_q	a_q, b_q	A_q	B_q
2	2, 2	1	1,1	1	1	43	56, 56	-12	$-12, -12$	-12	-12
3	4	6	0, 0	0	0	47	48, 48	0	0, 0	0	0
5	16	10	0, 0	0	0	53	2816	-6	$\pm 4\sqrt{-7}$	$-4\sqrt{-7}$	$4\sqrt{-7}$
7	8	0	$\pm\sqrt{-7}$	$\sqrt{-7}$	$-\sqrt{-7}$	59	60, 60	0	0, 0	0	0
11	128	-6	$\pm 2\sqrt{-7}$	$2\sqrt{-7}$	$-2\sqrt{-7}$	61	62, 62	0	0, 0	0	0
13	14, 14	0	0, 0	0	0	67	4608	-118	$\pm 6\sqrt{-7}$	$-6\sqrt{-7}$	$6\sqrt{-7}$
17	18, 18	0	0, 0	0	0	71	56	16	$8\pm\sqrt{-7}$	$8+\sqrt{-7}$	$8-\sqrt{-7}$
19	324	38	0, 0	0	0	73	5184	146	0, 0	0	0
23	512	18	$\pm 2\sqrt{-7}$	$2\sqrt{-7}$	$-2\sqrt{-7}$	79	88, 88	-8	$-8, -8$	-8	-8
29	32, 32	-2	$-2, -2$	-2	-2	83	6724	166	0, 0	0	0
31	32, 32	0	0, 0	0	0	89	7744	178	0, 0	0	0
37	32, 32	6	6, 6	6	6	97	98, 98	0	0, 0	0	0
41	42, 42	0	0, 0	0	0						

References

[1] J. Cremona, Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction, Math. Proc. Cambridge Philos. Soc. **111** (1992), 199–218.

[2] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, Lecture Notes in Math. **349** (1986), 143–316, Springer.

[3] N. Elkies, Remarks on elliptic K-curves, preprint (1993).

[4] G. Faltings, G. Wüstholtz et al., *Rational Points*, 3rd enlarged edition, Aspects of Math. **E6** (1992), Vieweg.

[5] R. Fricke, *Die Elliptischen Funktionen und ihre Anwendungen*, Teubner (1992).

[6] B. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, Lecture Notes in Math. **776** (1980), Springer.

[7] Y. Hasegawa, Table of cuspforms on $\Gamma_1(N)$ with real quadratic character, unpublished.

[8] Y. Hasegawa, K. Hashimoto and F. Momose, **Q**-curves and QM-curves, preprint.

[9] N. Katz and B. Mazur, *The Arithmetic Moduli of Elliptic Curves*, Princeton Univ. Press (1985).

[10] A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique, Acta Arith. **54** (1989), 75–80.

[11] M. Laska, An algorithm for finding a minimal Weierstraß equation for an elliptic curve, Math. Comp. **38** (1982), 257–260.

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

[13] B. Setzer, Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant, Illinois J. Math. **25** (1981), 233–245.

[14] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Forms*, Publ. Math. Soc. Japan **11** (1971), Iwanami.

[15] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106** (1986), Springer.

[16] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math. **151** (1994), Springer.

Present Address:
Department of Mathematics, School of Science and Engineering, Waseda University,
Okubo, Shinjuku-ku, Tokyo, 169–8555 Japan.