Werk

Titel: Q-curves over quadratic fields.

Autor: Hasegawa, Yuji

Jahr: 1997

PURL: https://resolver.sub.uni-goettingen.de/purl?365956996_0094|log30

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

manuscripta math. 94, 347–364 (1997)

manuscripta mathematica
© Springer-Verlag 1997

Q-curves over quadratic fields

YUJI HASEGAWA

Department of Mathematics, Waseda University, 3-4-1, Okubo Shinjuku-ku Tokyo 169, Japan
E-mail: hase@mn.waseda.ac.jp

Received December 12, 1996;
in revised form June 12, 1997

1. Introduction. Let N be a positive integer, and let $X_0(N), X_1(N)$ be the modular curves corresponding to the congruence subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; c \equiv 0 \mod N \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; a \equiv d \equiv 1 \mod N \text{ and } c \equiv 0 \mod N \right\},$$

respectively. Denote by $J_0(N)$, $J_1(N)$ their jacobians. An elliptic curve over $\mathbf{Q}$ is called *modular* if it is isogenous over $\mathbf{Q}$ to a one-dimensional factor over $\mathbf{Q}$ of $J_0(N)$. The celebrated Taniyama–Shimura conjecture predicts that every elliptic curve over $\mathbf{Q}$ is modular. In his Annals paper [17], A.Wiles proved that the conjecture is true for semi-stable elliptic curves over $\mathbf{Q}$. His results has been generalized by many mathematicians for a larger class of elliptic curves over $\mathbf{Q}$, see References in [5].

There is a more general conjecture for some class of abelian varieties over number fields. We will treat one-dimensional cases, i.e., elliptic curves over number fields with some property.

Definition 1.1 (Gross [3], Ribet [12]). Let $E/\bar{\mathbf{Q}}$ be an elliptic curve. Then E is said to be a $\mathbf{Q}$-*curve* if it is isogenous over $\bar{\mathbf{Q}}$ to any of its Galois conjugate ${}^{\sigma}E$, where σ is an element of $G_{\mathbf{Q}} := \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

Conjecture 1.2 (Ribet [12]). *Every* $\mathbf{Q}$*-curve is modular (over* $\bar{\mathbf{Q}}$*) in the sense that it appears as a factor of* $J_1(N)$ *up to isogeny over* $\bar{\mathbf{Q}}$.

An abelian variety A over $\mathbf{Q}$ is called *modular* (over $\mathbf{Q}$) if it is isogenous over $\mathbf{Q}$ to a $\mathbf{Q}$-simple factor of $J_1(N)$. If A is modular over $\mathbf{Q}$, then the $\mathbf{Q}$-algebra $\mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q}$ of endomorphisms of A over $\mathbf{Q}$ is isomorphic to a number field K of degree

$$[K : \mathbf{Q}] = \dim A. \tag{1}$$

1991 *Mathematics Subject Classification.* Primary 11F11; Secondary 14H52,11G05,11F66, 11G40,14K02,14H25,11G30,11G10,14H40,14K15.

An abelian variety A over $\mathbf{Q}$ is said to be *of* GL_2*-type* if it satisfies the property (1) with $K \cong \mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q}$. Thus the modular abelian varieties over $\mathbf{Q}$ are of GL_2-type. Conversely,

Conjecture 1.3 (Modular Conjecture [13][12]). *Every abelian variety of* GL_2*-type is modular.*

It is shown by Ribet [12] that for each $\mathbf{Q}$-curve E, there is an abelian variety of GL_2-type containing E as its simple factor (see section 4). Conjecture 1.2 follows from this together with Conjecture 1.3.

While the significance of studying $\mathbf{Q}$-curves is clear on account of Conjecture 1.2, it seems that there are very few works on $\mathbf{Q}$-curves; no large tables of $\mathbf{Q}$-curves were made, in contrast to elliptic curves over $\mathbf{Q}$.

In this paper, we are interested in constructing $\mathbf{Q}$-curves and algebraic curves over $\mathbf{Q}$ covering $\mathbf{Q}$-curves whose jacobians are of GL_2-type, and of course in checking their modularity.

In section 2, families of $\mathbf{Q}$-curves over quadratic fields are constructed. The process goes on systematically. Namely, we make use of the fact due to Elkies [1] that the $\mathbf{Q}$-curves of degree D are parametrized by the rational points of the modular curve $X_0^*(D)$ (see section 2 for definitions). In particular, we establish the problem of giving all $\mathbf{Q}$-curves of prime degree p over quadratic fields, whenever $X_0(p)$ is of genus zero (especially for $p = 2, 3, 7$). Section 3 treats isogenies $E \to {}^{\sigma}E$ between conjugate $\mathbf{Q}$-curves, to determine the field over which E and ${}^{\sigma}E$ are isogenous. As a consequence of these sections, various families of abelian surfaces of GL_2-type are constructed (section 4). In section 5, we also give three families of hyperelliptic curves over $\mathbf{Q}$ of genus two which cover families of $\mathbf{Q}$-curves and whose jacobians are of GL_2-type. In the final section, we offer many examples for which the modularity is checked.

Throughout this paper, $\mathbf{Q}$-curves are assumed to be of *non*-CM-type (unless specified).

2. Construction of Q-curves. Let D be a *square-free* positive integer. Let $X_0^*(D)$ be the curve over $\mathbf{Q}$ obtained by dividing $X_0(D)$ by all Atkin–Lehner involutions. The result of Elkies [1] says that every $\mathbf{Q}$-curve is isogenous over $\bar{\mathbf{Q}}$ to a $\mathbf{Q}$-curve which corresponds to a non-cuspidal, non-CM $\mathbf{Q}$-rational point of $X_0^*(D)$ for some D. More precisely, (i) a non-cuspidal, non-CM $\mathbf{Q}$-rational point of $X_0^*(D)$ represents a $\mathbf{Q}$-curve of *degree* D' dividing D, i.e., a $\mathbf{Q}$-curve which is isogenous to one of its conjugates with degree D'. and to the other with degree dividing D'; (ii) conversely, any $\mathbf{Q}$-curve of degree D corresponds to a point of $X_0^*(D)(\mathbf{Q})$. A $\mathbf{Q}$-curve corresponding to a point on $X_0^*(D)(\mathbf{Q})$ has a model over a compositum of $\omega(D)$ quadratic fields, where $\omega(D)$ is the number of prime divisors of D. In particular, any $\mathbf{Q}$-curve of prime degree has a model over some quadratic field. For simplicity, we assume in the following that $D = p$ is a prime, and the genus of $X_0(p)$ is zero. Then the relation between the j-function and a uniformizing parameter $t = t_p$ of $X_0(p)$ is known by Fricke [2] (Table 1).

Remark 2.1. For the case of the rational or elliptic modular curves $X_0(D)$, or some of the hyperelliptic modular curves $X_0(D)$, one can also find in [2] a covering

map $X_0(D) \to X_0(1) = \mathbf{P}^1_j$. See also [7].

TABLE 1. Defining equations $j=F_p(t)$ of $X_0(p)$ with $g=0$

p	$F_p(t)$	$t\|W_p$
2	$64\dfrac{(t+4)^3}{t^2}$	$t\|W_2=\dfrac{1}{t}$
3	$27\dfrac{(t+1)(9t+1)^3}{t}$	$t\|W_3=\dfrac{1}{t}$
5	$\dfrac{(t^2+10t+5)^3}{t}$	$t\|W_5=\dfrac{125}{t}$
7	$\dfrac{(t^2+13t+49)(t^2+5t+1)^3}{t}$	$t\|W_7=\dfrac{49}{t}$
13	$\dfrac{(t^2+5t+13)(t^4+7t^3+20t^2+19t+1)^3}{t}$	$t\|W_{13}=\dfrac{13}{t}$

On the other hand, we know that the elliptic curve

$$y^2 = x^3 - 27\frac{j_0}{j_0 - 12^3}x + 54\frac{j_0}{j_0 - 12^3} \tag{2}$$

has j-invariant $j = j_0$. Hence the problem reduces to obtaining those points $t \in X_0(p)$ which project to points of $X_0^*(p)(\mathbf{Q})$. If t itself is $\mathbf{Q}$-rational, then the corresponding elliptic curve is defined over $\mathbf{Q}$, and the problem may be out of interesting. So we assume that t is not $\mathbf{Q}$-rational.

Theorem 2.2. *Let $p = 2$, 3 or 7. For each square-free integer $d(\neq 1)$ and each rational number u, define an elliptic curve $E^{(p)}_{d,u}$ as follows:*

$$\begin{cases} E^{(2)}_{d,u}\colon\ y^2 = x^3 + 6(3\sqrt{d}u - 5)x - 8(9\sqrt{d}u - 7), \\ \qquad\qquad j = 2^6\dfrac{(3\sqrt{d}u - 5)^3}{(\sqrt{d}u - 1)(\sqrt{d}u + 1)^2}, \\ \qquad\qquad \Delta = -2^9 3^6(\sqrt{d}u - 1)(\sqrt{d}u + 1)^2, \end{cases}$$

$$\begin{cases} E^{(3)}_{d,u}\colon\ y^2 = x^3 - 3(4\sqrt{d}u + 5)x + 2(2du^2 + 14\sqrt{d}u + 11), \\ \qquad\qquad j = -2^4 3^3\dfrac{(4\sqrt{d}u + 5)^3}{(\sqrt{d}u - 1)^3(\sqrt{d}u + 1)}, \\ \qquad\qquad \Delta = -2^8 3^3(\sqrt{d}u - 1)^3(\sqrt{d}u + 1), \end{cases}$$

$$\begin{cases} E^{(7)}_{d,u}\colon\ y^2 = x^3 + Ax + B, \\ \qquad\qquad A = -21(du^2 + 27)(15du^2 + 96\sqrt{d}u + 85), \\ \qquad\qquad B = 98(du^2 + 27) \\ \qquad\qquad\qquad \times(27d^2u^4 + 144d\sqrt{d}u^3 + 1170du^2 + 2608\sqrt{d}u + 1539), \\ \qquad\qquad j = -\dfrac{(du^2 + 27)(15du^2 + 96\sqrt{d}u + 85)^3}{(\sqrt{d}u - 1)^7(\sqrt{d}u + 1)}, \\ \qquad\qquad \Delta = -2^{12}3^6 7^3(\sqrt{d}u - 1)^7(\sqrt{d}u + 1)(du^2 + 27)^2. \end{cases}$$

Then every $\mathbf{Q}$*-curve of degree* p *over* $\mathbf{Q}(\sqrt{d})$ *is isomorphic over* $\bar{\mathbf{Q}}$ *to* $E_{d,u}^{(p)}$ *for some* u.

Proof. Since the method is entirely similar, we will only treat the case where $p = 2$. Then we can take $t' = t + 1/t$ as a parameter of $X_0^*(2)$. Writing $t' = 2a \in \mathbf{Q}$, we have

$$t = a \pm \sqrt{a^2 - 1}. \tag{3}$$

Set $a^2 - 1 = db^2$ with d fixed square-free integer. Then a and b are expressed by one parameter u as

$$a = -\frac{du^2 + 1}{du^2 - 1}, \quad b = \frac{-2u}{du^2 - 1}.$$

Substituting these to (3), we have

$$t = -\frac{\sqrt{d}u + 1}{\sqrt{d}u - 1}, \ -\frac{\sqrt{d}u - 1}{\sqrt{d}u + 1}$$

and hence we obtain (up to conjugate) the desired j-invariant. Changing coordinates (x, y) in (2) to

$$(P_d(u)x, \sqrt{P_d(u)^3}y), \quad P_d(u) = \frac{3(3\sqrt{d}u - 5)}{2(9\sqrt{d}u - 7)},$$

we find the equation for $E_{d,u}^{(2)}$. □

The above three cases show that $\mathbf{Q}$-curves of degree $2, 3$ or 7 exist over arbitrary quadratic fields. The situation differs for $p = 5$ and 13, because of the numerator of $t_p | W_p$.

Proposition 2.3. *Let* $p = 5$ *or* 13, *and* $d \neq 1$ *a square-free integer. Then there exists a* $\mathbf{Q}$*-curve of degree* p *over* $\mathbf{Q}(\sqrt{d})$ *if and only if*

$$d = \pm p^{\varepsilon} p_1 \cdots p_r; \ \varepsilon = 0, 1; \ \left(\frac{p}{p_i}\right) = 1 \ \text{ for } \ i = 1, \ldots, r.$$

Proof. The curve $X_0^*(p)$ is parametrized by $t + t|W_p$. Therefore, the existence of such a $\mathbf{Q}$-curve is equivalent to the existence of a rational point (a, b) on the conic $a^2 - p = db^2$. By computing Hilbert symbols $(p, d)_v$ for all $v \leq \infty$ (and $v \neq p$), we obtain the desired result. □

Using the same method as in Theorem 2.2, we have

Theorem 2.4. *Let* $p = 5, 13$, *and assume that* $a, b \in \mathbf{Q}$ *satisfy the relation* $a^2 - p = db^2$. *Then every* $\mathbf{Q}$*-curve of degree* p *over* $\mathbf{Q}(\sqrt{d})$ *has* j*-invariant of the form*

$$j = \begin{cases} 8\dfrac{a+b\sqrt{d}}{a-b\sqrt{d}} \cdot \dfrac{U_5(u)^3}{(\sqrt{d}u + 1)^5(\sqrt{d}u - 1)} & \text{if } p = 5; \\ \dfrac{1}{(a-b\sqrt{d})^6} \cdot \dfrac{((2a+5)du^2 - 4bdu + (2a-5))U_{13}(u)^3}{(\sqrt{d}u + 1)^{13}(\sqrt{d}u - 1)} & \text{if } p = 13, \end{cases}$$

where $u \in \mathbf{Q} \cup \{\infty\}$ *and*

$$U_5(u) = (13a+12b\sqrt{d}+25)du^2 - 2(12a+13b\sqrt{d})\sqrt{d}u + (13a+12b\sqrt{d} - 25);$$

$$\begin{aligned} U_{13}(u) = {} & 2(5(34a^2+143a+117)+12(14a+39)b\sqrt{d})d^2u^4 \\ & - 4(12(28a^2+39a-182)+5(68a+143)b\sqrt{d})d\sqrt{d}u^3 \\ & + 4(5(102a^2-1001)+504ab\sqrt{d})du^2 \\ & - 4(12(28a^2-39a-182)+5(68a-143)b\sqrt{d})\sqrt{d}u \\ & + 2(5(34a^2-143a+117)+12(14a-39)b\sqrt{d}). \end{aligned}$$

First few values of d satisfying the condition of Proposition 2.3 are

$$d = \begin{cases} -1, \pm 5, \pm 11, \pm 19, \pm 29, \dots, & \text{if } p = 5, \\ -1, \pm 3, \pm 13, \pm 17, \pm 23, \dots, & \text{if } p = 13. \end{cases}$$

For instance, we take $(a,b) = (11/5, 2/5), (9/5, 2/5), (11, 2), \dots$ when $p = 5$ and $d = -1, -11, +29, \dots$. Later, we will give families of $\mathbf{Q}$-curves of degree 5 over $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-11})$ and $\mathbf{Q}(\sqrt{29})$.

Remark 2.5. For $p = 2, 3, 7$, we have chosen u so that the value of $t = t(u)$ at $u = \infty$ is rational, so we may ignore the case $u = \infty$. For $p = 5$ and 13, it is clearly impossible to choose such a parameter, so we include the case $u = \infty$.

Remark 2.6. For each family of (j-invariants $j = j_{d,u}^{(p)}$ of) $\mathbf{Q}$-curves given in Theorem 2.2 and Theorem 2.4, it is not difficult to determine all the values of $u \in \mathbf{Q} \cup \{\infty\}$ such that $j_{d,u}^{(p)}$ is a rational, or more generally, CM j-invariant (note that the rationality assumption forces $j_{d,u}^{(p)}$ to be a CM j-invariant; in this case, the corresponding elliptic curve has an endomorphism of degree p). For instance, let $p = 2$, and assume for simplicity that $j_{d,u}^{(p)}$ is rational. Then the endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E (over $\mathbf{Q}$) contains an element of degree 2 if and only if $j(E) = 1728, 8000, -3375$. In fact, we have

$$\begin{aligned} j_{d,u}^{(2)} = j(E_{d,u}^{(2)}) = {} & 1728 \iff u = \infty, \\ & 8000 \iff u = 0, \\ & -3375 \iff u = \pm 5/9,\ d = -7, \end{aligned}$$

where $j_{d,\infty}^{(2)} = \lim_{u \to \infty} j(E_{d,u}^{(2)})$.

3. Isogenies between Conjugate Curves. Let E be a $\mathbf{Q}$-curve of prime degree p defined over a quadratic field k. Then there is a k-rational cyclic subgroup C of order p of E. Since the fundamental involution W_p, which is defined over $\mathbf{Q}$, on $X_0(p)$ acts as $(E, C) \mapsto (E/C, E[p]/C)$, we see that E/C is isomorphic over some quadratic extension of k to the Galois conjugate ${}^{\sigma}E$ of E. We wish to determine the field over which ${}^{\sigma}E$ is isomorphic to E/C. To do this, it is convenient to introduce the so-called division polynomials.

Lemma 3.1. *Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Define a sequence of polynomials $\{\psi_m\}$ in $\mathbf{Z}[A, B, x, y]$ as*

$$\psi_1 = 1, \qquad \psi_2 = 2y,$$
$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$
$$\psi_{2m+1} = \psi_{m+2}\psi_m{}^3 - \psi_{m-1}\psi_{m+1}{}^3 \qquad (m \geq 2),$$
$$2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}{}^2 - \psi_{m-2}\psi_{m+1}{}^2) \qquad (m \geq 3).$$

(i) *Define other sequences $\{\phi_m\}$, $\{\omega_m\}$ of polynomials by*

$$\phi_m = x\psi_m{}^2 - \psi_{m+1}\psi_{m-1},$$
$$4y\,\omega_m = \psi_{m+2}\psi_{m-1}{}^2 - \psi_{m-2}\psi_{m+1}{}^2.$$

Then the image $[m]P$ of $P = (x_0, y_0) \in E$ under the multiplication-by-m-map is given by

$$[m]P = \left(\frac{\phi_m(x_0, y_0)}{\psi_m(x_0, y_0)^2}, \frac{\omega_m(x_0, y_0)}{\psi_m(x_0, y_0)^3}\right).$$

In particular, $P = (x_0, y_0)$ is a non-trivial m-torsion point on E if and only if $\psi_m(x_0, y_0) = 0$.

(ii) *The polynomials ϕ_m, $\psi_m{}^2$ can be regarded as polynomials in one variable x, and have expressions*

$$\phi_m(x) = x^{m^2} + \text{lower order terms},$$
$$\psi_m(x)^2 = m^2 x^{m^2-1} + \text{lower order terms}.$$

If m is odd, then ψ_m itself can be regarded as a polynomial in one variable x of the form

$$\psi_m(x) = mx^{(m^2-1)/2} + \text{lower order terms},$$

and ω_m is written as

$$\omega_m(x, y) = (x^{3(m^2-1)/2} + \text{lower order terms})y.$$

Proof. [15] III, Exer.3.7. □

Let C be a finite subgroup of E. Explicit formula for the isogeny ϕ of E to E/C with kernel $\ker\phi = C$ is determined by Vélu [16], in which the description of the defining equation of E/C in terms of (E, C) is also found.

Lemma 3.2. *Let $E: y^2 = x^3 + Ax + B$ be a $\mathbf{Q}$-curve of degree p defined over a quadratic field k. Let C be the k-rational cyclic subgroup of order p such that E/C is isomorphic (over $\bar{\mathbf{Q}}$) to ${}^\sigma E$. Then the curve E/C can be given by*

$$Y^2 = X^3 + n^2(\sigma A)X + n^3(\sigma B) \tag{4}$$

for some $n \in k^*$ with $N_{k/\mathbf{Q}}n = p^2$.

Proof. We have only to show that $N_{k/\mathbf{Q}}n = p^2$. Let $\phi: E \to {}^\sigma E$ be the isogeny which is the composition of Vélu's one $E \to E/C$ with the evident isomorphism $E/C \ni (X, Y) \mapsto (X/\sqrt{n}^2, Y/\sqrt{n}^3) \in {}^\sigma E$. Then for $p \neq 2$ we have

$$\phi: (x, y) \mapsto \left(\frac{x^p + \dots}{n(x^{p-1} + \dots)}, \frac{x^{3(p-1)/2} + \dots}{\sqrt{n}^3(x^{3(p-1)/2} + \dots)}y\right).$$

Similar formula holds for $p = 2$. Therefore the x-coordinate x' of the point ${}^{\sigma}\phi\circ\phi(x,y)$ is given by

$$x' = \frac{1}{N_{k/\mathbf{Q}}n}\frac{x^{p^2}+\dots}{x^{p^2-1}+\dots}.$$

On the other hand, we have ${}^{\sigma}\phi\circ\phi = \pm[p]$, since ϕ is of degree p. By the above lemma, it follows that $N_{k/\mathbf{Q}}n = p^2$. □

Proposition 3.3. *For $p = 2, 3$ or 7, let $E^{(p)}_{d,u}$ be as in Theorem 2.2. Then its Galois conjugate ${}^{\sigma}E^{(p)}_{d,u}$ is isogenous over $\mathbf{Q}(\sqrt{d}, \sqrt{-p})$ to the original curve $E^{(p)}_{d,u}$. That is, we have $n = -p$ in the notation of Lemma 3.2.*

Proof. Write for simplicity $E = E^{(p)}_{d,u}$. We have a Weierstrass model of E under the form $y^2 = x^3 + Ax + B$, with A, B given in Theorem 2.2.

Let $p = 2$. Then the curve E has a $\mathbf{Q}(\sqrt{d})$-rational subgroup $C = C^{(2)} = \{O, (4,0)\}$ of order 2. For $p = 3, 7$, we see that ψ_p has a factor of degree 1, 3 over $\mathbf{Q}(\sqrt{d})$, respectively; that is, the curve $E = E^{(p)}_{d,u}$ has a $\mathbf{Q}(\sqrt{d})$-rational subgroup $C = C^{(p)}$ of order p defined by

$$\begin{cases} x - 3 = 0 & \text{if } p = 3, \\ x^3 - 21(du^2+27)x^2 - 21(du^2+27)(9du^2 - 32\sqrt{d}u - 173)x \\ \qquad +7(du^2+27)(351d^2u^4 + 864d\sqrt{d}u^3 \\ \qquad\qquad + 1770du^2 - 13024\sqrt{d}u - 28377) = 0 & \text{if } p = 7. \end{cases}$$

Now using the result of Vélu, we find that the curve E/C has a Weierstrass form

$$Y^2 = X^3 + (-p)^2(\sigma A)X + (-p)^3(\sigma B),$$

hence the assertion follows. □

4. Q-curves and abelian surfaces of GL_2-type. Let $k/\mathbf{Q}$ be a finite extension and E a $\mathbf{Q}$-curve defined over k. Following Ribet [12] or Pyle [10], consider a system $\{\mu_\sigma : {}^{\sigma}E \to E\}_\sigma$ of isogenies such that $\mu_\sigma = \mu_\tau$ if ${}^{\sigma}E = {}^{\tau}E$. Then $c(\sigma,\tau) = \mu_\sigma {}^{\sigma}\mu_\tau \mu_{\sigma\tau}{}^{-1}$, viewed as an element of $\mathrm{End}(E)\otimes\mathbf{Q} \cong \mathbf{Q}$, defines a locally constant 2-cocycle c on $G_\mathbf{Q}$ with values in $\mathbf{Q}^*$. By a theorem of Tate, considering $\bar{\mathbf{Q}}^*$ as a trivial $G_\mathbf{Q}$-module, the cocycle c splits in $\bar{\mathbf{Q}}$; namely, c can be written as

$$c(\sigma,\tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1},$$

where $\beta : G_\mathbf{Q} \to \bar{\mathbf{Q}}^*$ is a locally constant function. Let K be the field obtained by adjoining the values of β. As β is locally constant, the extension $K/\mathbf{Q}$ is finite.

Theorem 4.1 (Ribet [12, Thm. 6.1]). *Let E be a $\mathbf{Q}$-curve and $K/\mathbf{Q}$ a finite extension defined as above. Then there exists an abelian variety A of GL_2-type over $\mathbf{Q}$ such that*

(i) $\mathrm{End}_\mathbf{Q}(A)\otimes\mathbf{Q} \cong K$;

(ii) *A is isogenous over $\bar{\mathbf{Q}}$ to a power of E.*

The notion of $\mathbf{Q}$-curve is generalized by Pyle [10] to higher dimensional cases, which she called building blocks. The above theorem holds for building blocks, see [10, Prop. 4.5, Thm. 4.6] for details.

Let k be any quadratic field. We are now interested in $\mathbf{Q}$-curves defined over k such that the restriction of scalars with respect to $k/\mathbf{Q}$ is an abelian surface of GL_2-type.

Proposition 4.2. *Notation being as in Lemma 3.2, assume that there is an element α of k such that $n \cdot N_{k/\mathbf{Q}}\alpha$ is a square in k. Then the twisted curve E_α of E by $\sqrt{\alpha}$ is isogenous over k to ${}^\sigma(E_\alpha)$.*

Proof. By Lemma 3.2 and [16], there is an isogeny $\phi\colon E \to {}^\sigma E$ such that

$$\phi(x,y) = \left(\frac{Q_1(x)}{n \cdot P_1(x)}, \frac{Q_2(x)}{\sqrt{n}^3 P_2(x)} y\right),$$

where P_1, Q_1, P_2, Q_2 are monic polynomials in $k[x]$ with

$$\deg P_1 = \deg Q_1 - 1, \quad \deg P_2 = \deg Q_2.$$

Take a Weierstrass form $y^2 = x^3 + \alpha^2 Ax + \alpha^3 B$ of E_α. Then the isogeny $\phi_\alpha\colon E_\alpha \xrightarrow{\sim} E \xrightarrow{\phi} {}^\sigma E \xrightarrow{\sim} {}^\sigma(E_\alpha)$ corresponding to ϕ is given by

$$\begin{aligned}\phi_\alpha(x,y) &= \left(\frac{\sigma\alpha \cdot Q_1(x/\alpha)}{n \cdot P_1(x/\alpha)}, \frac{\sigma\sqrt{\alpha}^3 \cdot Q_2(x/\alpha)}{\sqrt{n}^3 \cdot P_2(x/\alpha)} \cdot \frac{y}{\sqrt{\alpha}^3}\right) \\ &= \left(\frac{\sigma\alpha \cdot Q_1'(x)}{n\alpha \cdot P_1'(x)}, \frac{\sigma\sqrt{\alpha}^3 \cdot Q_2'(x)}{\sqrt{n}^3 \sqrt{\alpha}^3 \cdot P_2'(x)} y\right),\end{aligned}$$

where P_1', Q_1', P_2', Q_2' are monic polynomials in $k[x]$. Observe that

$$\frac{\sigma\sqrt{\alpha}}{\sqrt{n}\sqrt{\alpha}} = \pm\frac{\sqrt{\sigma\alpha}}{\sqrt{n\alpha}} = \pm\frac{\sigma\alpha}{\sqrt{n \cdot N_{k/\mathbf{Q}}\alpha}},$$

hence we obtain the proposition. □

Combining this with Proposition 3.3, we have

Corollary 4.3. *For $p = 2, 3$ or 7, let $E = E_{d,u}^{(p)}$ be as in Theorem 2.2. Assume that there is an element α of $k = \mathbf{Q}(\sqrt{d})$ such that $-p \cdot N_{k/\mathbf{Q}}\alpha$ is a square in k. Then the twisted curve E_α of E by $\sqrt{\alpha}$ is isogenous over k to ${}^\sigma(E_\alpha)$.*

The next lemma is a direct deduction from [12] [10].

Lemma 4.4. *Let E be a $\mathbf{Q}$-curve over a quadratic field k, furnished with isogeny $\mu_\sigma\colon {}^\sigma E \to E$. Assume that μ_σ is defined over k and of degree p. Let $\hat{\mu}_\sigma\colon E \to {}^\sigma E$ be the dual isogeny of μ_σ. Then we have*

$$K = \begin{cases} \mathbf{Q}(\sqrt{p}) & \text{if } {}^\sigma\mu_\sigma = \hat{\mu}_\sigma; \\ \mathbf{Q}(\sqrt{-p}) & \text{if } {}^\sigma\mu_\sigma = -\hat{\mu}_\sigma, \end{cases}$$

where $K/\mathbf{Q}$ is defined as above.

Proposition 4.5. *Let $E\colon y^2 = x^3 + Ax + B$ be a $\mathbf{Q}$-curve of degree p defined over a quadratic field k. Let C be the k-rational cyclic subgroup of order p such that E/C is isomorphic over k to ${}^\sigma E$. Then $n \in k^*$ in (4) is a square in k, i.e., Vélu's model of the curve E/C is given by*

$$Y^2 = X^3 + n_0^4(\sigma A)X + n_0^6(\sigma B)$$

for some $n_0 \in k^*$ *with* $N_{k/\mathbf{Q}}n_0 = \pm p$. *Furthermore, by letting* μ_σ *be the dual isogeny of the isogeny* $\phi: E \to E/C \xrightarrow{\sim} {}^\sigma E$, *we have* $K = \mathbf{Q}(\sqrt{N_{k/\mathbf{Q}}n_0})$.

Proof. This follows from Lemma 3.2 and Lemma 4.4. (To determine the signature of ${}^\sigma\phi\circ\phi$, i.e., to conclude that ${}^\sigma\phi\circ\phi = [N_{k/\mathbf{Q}}n_0]$, use the y-coordinate of ${}^\sigma\phi\circ\phi(x,y)$ in stead of the x-coordinate; cf. proof of Lemma 3.2.) □

Let K be a quadratic field. By abuse of language, we say in the following that an elliptic curve $\mathscr{E}$ over a quadratic field k is a $\mathbf{Q}$-curve with *quadratic multiplication* by K if it is a $\mathbf{Q}$-curve and $\mathscr{A} = \mathrm{Re}_{k/\mathbf{Q}}(\mathscr{E})$ is of GL_2-type with $\mathrm{End}_{\mathbf{Q}}(\mathscr{A}) \otimes \mathbf{Q} \cong K$.

We are now in a situation to exhibit various families $\{\mathscr{E}_{d,u}^{(\pm p)}\}_u$ of $\mathbf{Q}$-curves over $k = \mathbf{Q}(\sqrt{d})$ with quadratic multiplication by $K = \mathbf{Q}(\sqrt{\pm p})$.

Remark 4.6. The reason why we pick up the following combination of k and K will become apparent in section 6. See also Remark 6.4 and Example 6.5.

TABLE 2. The case of degree 2 ($K = \mathbf{Q}(\sqrt{2})$)

k	$\mathscr{E}_{d,u}^{(2)}$
$\mathbf{Q}(\sqrt{-1})$	$A = -27(3u + 5\sqrt{-1}), \quad B = 54(1+\sqrt{-1})(9u + 7\sqrt{-1})$
$\mathbf{Q}(\sqrt{-7})$	$A = -378(\frac{1+\sqrt{-7}}{2})^2(3\sqrt{-7}u - 5)$ $B = -1512\sqrt{-7}(\frac{1+\sqrt{-7}}{2})^3(9\sqrt{-7}u - 7)$

TABLE 3. The case of degree 2 ($K = \mathbf{Q}(\sqrt{-2})$)

k	$\mathscr{E}_{d,u}^{(-2)}$
$\mathbf{Q}(\sqrt{41})$	$A = 1350(\frac{-7+\sqrt{41}}{2})^2(32 + 5\sqrt{41})^2(3\sqrt{41}u - 5)$ $B = 27000(\frac{-7+\sqrt{41}}{2})^3(32 + 5\sqrt{41})^3(9\sqrt{41}u - 7)$

TABLE 4. The case of degree 3 ($K = \mathbf{Q}(\sqrt{3})$)

k	$\mathscr{E}_{d,u}^{(3)}$
$\mathbf{Q}(\sqrt{-3})$	$A = -3(4\sqrt{-3}u + 5), \quad B = -2(6u^2 - 14\sqrt{-3}u - 11)$
$\mathbf{Q}(\sqrt{-11})$	$A = 33(\frac{-1+\sqrt{-11}}{2})^2(4\sqrt{-11}u + 5)$ $B = -22\sqrt{-11}(\frac{-1+\sqrt{-11}}{2})^3(22u^2 - 14\sqrt{-11}u - 11)$
$\mathbf{Q}(\sqrt{13})$	$A = -39(\frac{-3+\sqrt{13}}{2})^2(\frac{1+\sqrt{13}}{2})^2(4\sqrt{13}u + 5)$ $B = 26\sqrt{13}(\frac{-3+\sqrt{13}}{2})^3(\frac{1+\sqrt{13}}{2})^3(26u^2 + 14\sqrt{13}u + 11)$

TABLE 5. The case of degree 3 ($K = \mathbf{Q}(\sqrt{-3})$)

k	$\mathscr{E}_{d,u}^{(-3)}$
$\mathbf{Q}(\sqrt{109})$	$A = -3(\frac{73+7\sqrt{109}}{2})^2(4\sqrt{109}u + 5)$ $B = -2(\frac{73+7\sqrt{109}}{2})^3(218u^2 + 14\sqrt{109}u + 11)$

TABLE 6. The case of degree 5 ($K = \mathbf{Q}(\sqrt{5})$)

k	$\mathscr{E}_{d,u}^{(5)}$
$\mathbf{Q}(\sqrt{-1})$	$A=27u(11u-2)(2(-9+10\sqrt{-1})u^2-2(9+10\sqrt{-1})u+3)$ $B=54u^2(11u-2)^2$ $\times((13-40\sqrt{-1})u^2+(59+22\sqrt{-1})u+9(-1+2\sqrt{-1}))$
$\mathbf{Q}(\sqrt{-11})$	$A=-297(110u^2-22u+1)$ $\times(11(11-192\sqrt{-11})u^2+2(1067+126\sqrt{-11})u+4(-49+3\sqrt{-11}))$ $B=-6534(110u^2-22u+1)^2(5(2321+738\sqrt{-11})u^2$ $+25(-257+54\sqrt{-11})u-7(37+36\sqrt{-11}))$

TABLE 7. The case of degree 5 ($K = \mathbf{Q}(\sqrt{-5})$)

k	$\mathscr{E}_{d,u}^{(-5)}$
$\mathbf{Q}(\sqrt{29})$	$A=-675(\frac{5+\sqrt{29}}{2})^2(11+2\sqrt{29})(957u^2-290u+22)$ $\times(348(27+5\sqrt{29})u^2-2(1595+296\sqrt{29})u+(269+50\sqrt{29}))$ $B=1350(\frac{5+\sqrt{29}}{2})^3(11+2\sqrt{29})^2(957u^2-290u+22)^2$ $\times(87(512+95\sqrt{29})u^2-(15950+2963\sqrt{29})u+(1426+265\sqrt{29}))$

TABLE 8. The case of degree 7 ($K = \mathbf{Q}(\sqrt{7})$)

k	$\mathscr{E}_{d,u}^{(7)}$
$\mathbf{Q}(\sqrt{-3})$	$A = 9261(\frac{1+3\sqrt{-3}}{2})^2(u+3)(u-3)(45u^2-96\sqrt{-3}u-85)$ $B = 302526\sqrt{-3}(\frac{1+3\sqrt{-3}}{2})^3(u+3)(u-3)$ $\times(243u^4-432\sqrt{-3}u^3-3510u^2+2608\sqrt{-3}u+1539)$

Remark 4.7. The above families $\{\mathscr{E}_{d,u}^{(\pm p)}\}$ may contain "degenerate" cases, by which we mean that either (i) $A = B = 0$ or (ii) $\mathrm{Re}_{k/\mathbf{Q}}(\mathscr{E}_{d,u}^{(\pm p)})$ is isogenous over $\mathbf{Q}$ to a power of an elliptic curve over $\mathbf{Q}$. The former case is determined by

a trivial observation. The latter occurs if and only if $\mathcal{S}_{d,u}^{(\pm p)}$ is isogenous over k to an elliptic curve defined by an equation with rational coefficients. Note also that in this case $\mathcal{S}_{d,u}^{(\pm p)}$ must have complex multiplication. All the degenerate cases in Table 2 – Table 8 are:

$$\begin{aligned}
&\text{Case (i):}\quad (\pm p, d, u) = (5,-1,0),\ (5,-1,2/11),\ (7,-3,\pm 3);\\
&\text{Case (ii):}\quad (\pm p, d, u) = (2,-7,\pm 5/9),\ (3,-3,0),\ (3,-11,\pm 1/4),\\
&\qquad\qquad (5,-1,1),\ (5,-1,-9/13),\ (5,-11,0),\\
&\qquad\qquad (5,-11,2/9),\ (7,-3,\pm 1/5).\ (7,-3,\pm 5/3).
\end{aligned}$$

Remark 4.8. For the case of degree 5, the coefficients A_∞, B_∞ of the equation $\mathcal{S}_{d,\infty}^{(\pm 5)}: y^2 = x^3 + A_\infty x + B_\infty$ can be computed by setting $A_\infty := \lim_{u\to\infty} A/u^4$ and $B_\infty := \lim_{u\to\infty} B/u^6$.

5. Curves of genus two covering Q-curves. In this section, we will give three families of hyperelliptic curves of genus two over $\mathbf{Q}$ covering $\mathbf{Q}$-curves.

5.1. Let u be a rational number. Let $X_u^{(2)}$ be the algebraic curve over $\mathbf{Q}$ defined by

$$X_u^{(2)}: w^2 = z^5 + uz^3 - 64z.$$

This is in fact a hyperelliptic curve of genus two for any $u \in \mathbf{Q}$. The curve $X_u^{(2)}$ has automorphisms

$$\begin{aligned}
&\iota: (z,w) \mapsto \left(\frac{8\sqrt{-1}}{z}, \frac{16(1-\sqrt{-1})}{z^3}w\right).\\
&i: (z,w) \mapsto (-z, \sqrt{-1}w),
\end{aligned}$$

both defined over $k = \mathbf{Q}(\sqrt{-1})$. Let $J_u^{(2)}$ be the jacobian of $X_u^{(2)}$ and consider the element ξ of $\mathrm{End}J_u^{(2)}$ defined by

$$\xi = (i+1)\iota.$$

Since we have $\iota o i = -i o \iota = -^\sigma\iota$ ($\langle\sigma\rangle = \mathrm{Gal}(k/\mathbf{Q})$), it follows that ξ is defined over $\mathbf{Q}$ and $\xi^2 = 2$, i.e., $\mathbf{Q}(\sqrt{2}) \cong \mathbf{Q}(\xi) \subseteq \mathrm{End}_{\mathbf{Q}}(J_u^{(2)}) \otimes \mathbf{Q}$.

Theorem 5.1. *Let $X_u^{(2)}$ be as above. Then the jacobian $J_u^{(2)}$ of $X_u^{(2)}$ is of GL_2-type with real multiplication by $\mathbf{Q}(\sqrt{2})$. The involution ι induces a covering from $X_u^{(2)}$ to a $\mathbf{Q}$-curve $E_u^{(2)}$ over $k = \mathbf{Q}(\sqrt{-1})$ given by*

$$y^2 = x^3 + 27(3u - 80\sqrt{-1})x - 216(1+\sqrt{-1})(9u - 112\sqrt{-1}).$$

Two abelian surfaces $J_u^{(2)}$ and $\mathrm{Re}_{k/\mathbf{Q}}E_u^{(2)}$ are isogenous over $\mathbf{Q}$. In particular, $E_u^{(2)}$ has quadratic multiplication by $\mathbf{Q}(\sqrt{2})$, and $J_u^{(2)}$ is isogenous over k to $E_u^{(2)} \times E_u^{(2)}$.

Proof. The function field of $E_u^{(2)} = X_u^{(2)}/\langle\iota\rangle$ is generated by $z+\iota(z)$ and $w+\iota(w)$. In fact, by taking

$$\begin{aligned}
x &= 3^2(z+\iota(z)) - 12(1+\sqrt{-1}),\\
y &= 3^3(w+\iota(w))/(z+\iota(z)+2(1+\sqrt{-1})),
\end{aligned}$$

we have a Weierstrass form of $E_u^{(2)}$, which is clearly isomorphic over k to $\mathscr{E}_{-1,-u/16}^{(2)}$. It follows that $J_u^{(2)}$ and $\mathrm{Re}_{k/\mathbf{Q}}(\mathscr{E}_{-1,-u/16}^{(2)})$ are isogenous over $\mathbf{Q}$, hence we conclude that $\mathrm{End}_{\mathbf{Q}}(J_u^{(2)}) \otimes \mathbf{Q} = \mathbf{Q}(\sqrt{2})$ (see also Remark 4.7). □

5.2. Let u be a rational number. Let $X_u^{(3)}$ be the algebraic curve over $\mathbf{Q}$ defined by

$$X_u^{(3)}\colon w^2 = z^6 + uz^3 - 27.$$

This is in fact a hyperelliptic curve of genus two for any $u \in \mathbf{Q}$. The curve $X_u^{(3)}$ has automorphisms

$$\iota\colon (z,w) \mapsto \left(-\frac{3}{z}, \frac{3\sqrt{-3}}{z^3}w\right), \quad \zeta\colon (z,w) \mapsto \left(\frac{-1+\sqrt{-3}}{2}z, w\right),$$

both defined over $k = \mathbf{Q}(\sqrt{-3})$. Let $J_u^{(3)}$ be the jacobian of $X_u^{(3)}$ and consider the element η of $\mathrm{End}J_u^{(3)}$ defined by

$$\eta = (2\zeta + 1)\iota.$$

Since we have $\iota\circ\zeta = \zeta^2\circ\iota$, it follows that η is defined over $\mathbf{Q}$. Moreover, we have $\eta^2 = 3$, hence

Theorem 5.2. *Let $X_u^{(3)}$, $u \neq 0$ be as above. Then the jacobian $J_u^{(3)}$ is of GL_2-type with real multiplication by $\mathbf{Q}(\sqrt{3})$. The involution ι induces a covering from $X_u^{(3)}$ to a $\mathbf{Q}$-curve $E_u^{(3)}$ over $k = \mathbf{Q}(\sqrt{-3})$ given by*

$$E_u^{(3)}\colon y^2 = x^3 + 3(2\sqrt{-3}u - 45)x + (u^2 + 42\sqrt{-3}u - 594).$$

Two abelian surfaces $J_u^{(3)}$ and $\mathrm{Re}_{k/\mathbf{Q}}E_u^{(3)}$ are isogenous over $\mathbf{Q}$. In particular, $E_u^{(3)}$ has quadratic multiplication by $\mathbf{Q}(\sqrt{3})$, and $J_u^{(3)}$ is isogenous over k to $E_u^{(3)} \times E_u^{(3)}$.

Remark 5.3. The family $\{E_u^{(3)}\}$ is "equivalent" to $\{\mathscr{E}_{-3,u}^{(3)}\}$ given in Table 4; it is easy to check that $E_{-18u}^{(3)}$ is isomorphic over k to $\mathscr{E}_{-3,u}^{(3)}$.

5.3. Let u again be a rational number and $X_u^{(5)}$ the algebraic curve over $\mathbf{Q}$ defined by

$$\begin{aligned} X_u^{(5)}\colon w^2 =& 2z^6 + 4(-u+1)z^5 + (2u+1)z^4 \\ &+ 4(u-1)(u-2)z^3 - (2u+1)z^2 + 4(-u+1)z - 2 \\ =& (z^3 - (2u-3)z^2 + 2z + 2)(2z^3 - 2z^2 - (2u-3)z - 1). \end{aligned}$$

This curve is in fact of genus two if $u \neq 13/4$. Moreover, it has an involution defined over $k = \mathbf{Q}(\sqrt{-1})$:

$$(z,w) \mapsto \left(-\frac{1}{z}, \frac{\sqrt{-1}}{z^3}w\right).$$

Dividing $X_u^{(5)}$ by this involution, we obtain an elliptic curve $E_u^{(5)}$ over k defined by the equation

$$E_u^{(5)}: y^2 = x^3 + Ax + B,$$
$$A = -3^3(4u-13)(12u^2 - 8(6+5\sqrt{-1})u + (3+40\sqrt{-1})),$$
$$B = 2\cdot 3^3(4u-13)^2 \times (36(1-2\sqrt{-1})u^2 + 14(-11+2\sqrt{-1})u + 11(5+4\sqrt{-1})).$$

Theorem 5.4. *Let u be a rational number such that $u \neq 13/4,\ 1,\ -2/9$, and $X_u^{(5)}$, $E_u^{(5)}$ as above. Then $\{E_u^{(5)}\}$ gives a family of $\mathbf{Q}$-curves over $k = \mathbf{Q}(\sqrt{-1})$ with quadratic multiplication by $\mathbf{Q}(\sqrt{5})$. The jacobian $J_u^{(5)}$ of $X_u^{(5)}$ is isogenous over $\mathbf{Q}$ to $\mathrm{Re}_{k/\mathbf{Q}}E_u^{(5)}$, so it is an abelian surface of GL_2-type with real multiplication by $\mathbf{Q}(\sqrt{5})$, and is isogenous over k to $E_u^{(5)} \times E_u^{(5)}$.*

Proof. Indeed, the curve $E_u^{(5)}$ has a k-rational cyclic subgroup $C_u^{(5)}$ of order 5; the x-coordinates of the points of $C_u^{(5)} \setminus \{O\}$ are the solutions of

$$(2-\sqrt{-1})x^2 - 6(2-\sqrt{-1})^2(4u-13)x + 9\sqrt{-1}(4u-13)(36u^2 + 4(-20+7\sqrt{-1})u + (143+8\sqrt{-1})) = 0.$$

Therefore by [16] we find the equation for $E_u^{(5)}/C_u^{(5)}$

$$Y^2 = X^3 + (1+2\sqrt{-1})^4\cdot\sigma A X + (1+2\sqrt{-1})^6\cdot\sigma B.$$

Now apply Proposition 4.5. (It is not difficult to see that $J_u^{(5)}$ is "degenerate" in the sense of Remark 4.7 if and only if $u = 13/4,\ 1,\ -2/9$.) □

Remark 5.5. (1) The family $\{X_u^{(5)}\}$ is found by K. Hashimoto [6]. He used algebraic correspondences on $X_u^{(5)}$ (but not from the same point of view as in the above two cases) to show that $X_u^{(5)}$ has the properties described in Theorem 5.4. Compared with the previous cases, formulas giving real multiplication are much more complicated.

(2) As in the case of $E_u^{(2)}$ and $E_u^{(3)}$, the family $\{E_u^{(5)}\}$ is "equivalent" to $\{\mathscr{E}_{-1,u}^{(5)}\}$ given in Table 6; if we put $v = (u+1)/(2u)$, then $E_v^{(5)}$ is isomorphic over k to $\mathscr{E}_{-1,u}^{(5)}$. This gives another proof of Theorem 5.4.

Remark 5.6. Write $\mathscr{A}_{d,u}^{(p)} = \mathrm{Re}_{k/\mathbf{Q}}\mathscr{E}_{d,u}^{(p)}$ with $k = \mathbf{Q}(\sqrt{d})$. The above three cases show that the families $\{\mathscr{A}_{d,u}^{(p)}\}$ of abelian surfaces of GL_2-type for $(p,d) = (2,-1)$, $(3,-3)$, $(5,-1)$ can be interpreted up to isogeny over $\mathbf{Q}$ as families $\{J_u^{(p)}\}$ of the jacobian varieties of hyperelliptic curves $X_u^{(p)}$ of genus two. It is highly desirable to construct families of curves over $\mathbf{Q}$ of genus 2 covering $\{\mathscr{E}_{d,u}^{(\pm p)}\}$ for each (p,d) (if possible).

6. Examples. Now we display examples of modular $\mathbf{Q}$-curves. To begin with, we tabulate all the modular abelian surfaces A_f [14] which are ($\mathbf{Q}$-simple) factors of the "new" part of $J_0(N)$ for $N \leq 500$, such that

$$\mathrm{End}(A_f) \otimes \mathbf{Q} = \mathrm{M}_2(\mathbf{Q}).$$

TABLE 9

$N=\prod p_i^{e_i}$	K	k	a_2	a_3	a_5	a_7	a_{11}
$63=3^2\cdot 7$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{-3})$	$\sqrt{3}$	$+$	$-2\sqrt{3}$	$-$	$2\sqrt{3}$
$81=3^4$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{-3})$	$\sqrt{3}$	$-$	$-\sqrt{3}$	2	$-2\sqrt{3}$
$98=2\cdot 7^2$	$\mathbf{Q}(\sqrt{2})$	$\mathbf{Q}(\sqrt{-7})$	$-$	$\sqrt{2}$	$-2\sqrt{2}$	$+$	-2
$117=3^2\cdot 13$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{-3})$	$\sqrt{3}$	$+$	0	2	$-2\sqrt{3}$
$160=2^5\cdot 5$	$\mathbf{Q}(\sqrt{2})$	$\mathbf{Q}(\sqrt{-1})$	$+$	$2\sqrt{2}$	$-$	$-2\sqrt{2}$	$-4\sqrt{2}$
$169=13^2$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{13})$	$\sqrt{3}$	2	$-\sqrt{3}$	0	0
$189=3^3\cdot 7$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{-3})$	$\sqrt{3}$	$+$	$\sqrt{3}$	$-$	$-\sqrt{3}$
$189=3^3\cdot 7$	$\mathbf{Q}(\sqrt{7})$	$\mathbf{Q}(\sqrt{-3})$	$\sqrt{7}$	$-$	$-\sqrt{7}$	$+$	$-\sqrt{7}$
$196=2^2\cdot 7^2$	$\mathbf{Q}(\sqrt{2})$	$\mathbf{Q}(\sqrt{-7})$	$-$	$2\sqrt{2}$	$-\sqrt{2}$	$+$	4
$243=3^5$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{-3})$	$\sqrt{3}$	$-$	$2\sqrt{3}$	-1	$-2\sqrt{3}$
$(320=2^6\cdot 5)$	$\mathbf{Q}(\sqrt{2})$	$\mathbf{Q}(\sqrt{-1})$					
$363=3\cdot 11^2$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{-11})$	$\sqrt{3}$	$+$	-3	$-2\sqrt{3}$	$+$
$363=3\cdot 11^2$	$\mathbf{Q}(\sqrt{5})$	$\mathbf{Q}(\sqrt{-11})$	$\sqrt{5}$	$-$	2	$-2\sqrt{5}$	$+$
$387=3^2\cdot 43$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{-3})$	0	$+$	$2\sqrt{3}$	2	$-3\sqrt{3}$
$392=2^3\cdot 7^2$	$\mathbf{Q}(\sqrt{2})$	$\mathbf{Q}(\sqrt{-7})$	$+$	$2\sqrt{2}$	$2\sqrt{2}$	$-$	-4
$392=2^3\cdot 7^2$	$\mathbf{Q}(\sqrt{2})$	$\mathbf{Q}(\sqrt{-7})$	$-$	$\sqrt{2}$	$2\sqrt{2}$	$+$	6
$416=2^5\cdot 13$	$\mathbf{Q}(\sqrt{5})$	$\mathbf{Q}(\sqrt{-1})$	$-$	$\sqrt{5}$	3	$\sqrt{5}$	$-2\sqrt{5}$
$(441=3^2\cdot 7^2)$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{-3})$					
$484=2^2\cdot 11^2$	$\mathbf{Q}(\sqrt{3})$	$\mathbf{Q}(\sqrt{-11})$	$-$	2	3	$2\sqrt{3}$	$+$

TABLE 10

N	p	d	u
†63	3	−3	13/9
†81	3	−3	1
98	2	−7	−13/49
†117	3	−3	5/9
†160	2	−1	3/4
169	3	13	−11/13

N	p	d	u
†189	3	−3	1/9
‡189	7	−3	4
196	2	−7	−3/7
†243	3	−3	−1/3
363	3	−11	31/11
‡363	5	−11	1/11

N	p	d	u
387	3	−3	3/4
392	2	−7	3
392	2	−7	−11/7
‡416	5	−1	1/5
484	3	−11	4/11

This is achieved by decomposing the space of newforms of weight 2 by means of trace formulas of Hecke operators and using the result of [11] or [9] on the structure of $\mathrm{End}(A_f)\otimes\mathbf{Q}$; the result is summarized in Table 9.

The meaning of symbols are as follows: N is the level of f; $K=\mathrm{End}_{\mathbf{Q}}(A_f)\otimes\mathbf{Q}$ is the $\mathbf{Q}$-algebra of endomorphisms over $\mathbf{Q}$ of A_f; k is the smallest subfield of $\bar{\mathbf{Q}}$ over which all endomorphisms of A_f are defined; a_q for $2\le q\le 11$ with $q\nmid N$ gives the q-th Fourier coefficient of f. If $q|N$, then the sign of the eigenvalue of the Atkin–Lehner involution W_q is given there. (If N is divisible by $q\ge 13$, then the sign of the eigenvalue of W_q is $-,-,-,+$, according to $N=117,169,387,416$.) The case of $N=320$ (resp. $N=441$) is obtained by twisting the case of $N=160$ (resp. $N=63$) by a quadratic character of conductor 8 (resp. 7). Note that a major part of Table 9 is occupied by those abelian surfaces with real multiplication by $\mathbf{Q}(\sqrt{2})$ or $\mathbf{Q}(\sqrt{3})$.

On the other hand, we constructed families of abelian surfaces of GL_2-type from the families of $\mathbf{Q}$-curves (section 4). Let A be an abelian surface of GL_2-

type. It is known that the conductor of $A/\mathbf{Q}$ is of the form N^2 with N a positive integer. If further $A = \mathrm{Re}_{k/\mathbf{Q}}E$ is the restriction of scalars of an elliptic curve E over a quadratic field k, then N is recovered from the conductor of E/k:

$$N = \sqrt{\mathrm{cond}(A/\mathbf{Q})} = \sqrt{\mathrm{N}_{k/\mathbf{Q}}\mathrm{cond}(E/k)} \cdot |\mathrm{discr}(k)|.$$

We also tabulate such abelian surfaces of GL_2-type with conductor $N^2 \leq 500^2$ (Table 10; two cases of $N = 320$ and $N = 441$ are omitted), by giving three parameters p, d, u, see Table 2 – Table 8 for notation.

Observe that there is a precise correspondence between Table 9 and Table 10. One can also find that first few Euler factors of the L-functions of two abelian surfaces A_f and $\mathrm{Re}_{k/\mathbf{Q}}\mathcal{E}^{(p)}_{d,u}$ over $\mathbf{Q}$ coincide for each case. Hence all of them are strongly expected to be modular. Unfortunately, it is in general hard to check the modularity for the case of real multiplication by $\mathbf{Q}(\sqrt{2})$ or $\mathbf{Q}(\sqrt{3})$. A few special cases of them, however, are shown to be modular, using the quotient curve of $X_0(N)$. Indeed, the curves $X^{(3)}_v$ (see section 5) corresponding to $v = -2, 6, -10, -18, -26$ are obtained as quotient curves of $X_0(N)$ with $N = 189$, 243, 117, 81, 63, respectively [4]. Thus, the jacobian $J^{(3)}_v$ of $X^{(3)}_v$, and hence its simple factor $E^{(3)}_v$, which is isomorphic over $\mathbf{Q}(\sqrt{-3})$ to $\mathcal{E}^{(3)}_{-3,u}$ with $v = -18u$, is modular for these values of v. Similarly, the curve $\mathcal{E}^{(2)}_{-1,3/4}$ ($N = 160$) is covered by

$$X^{(2)}_{-12}\colon\ w^2 = z^5 - 12z^3 - 64z = z(z+4)(z-4)(z^2+4),$$

which is a quotient curve of $X_0(160)$ [4], so we conclude that this case is also modular. These six cases are marked "†" in Table 10.

Remark 6.1. Consider the family $\{E^{(3)}_v\}$ over $k = \mathbf{Q}(\sqrt{-3})$ given in section 5. Obviously, we have ${}^{\sigma}E^{(3)}_v = E^{(3)}_{-v}$. For $v = (\pm)26$ and $(\pm)54$, the curve $E = E^{(3)}_v$ has conductor $\mathfrak{p}_3{}^2\mathfrak{p}_7\mathfrak{p}'_7$. In fact, one sees that there is an isogeny $E^{(3)}_{26} \to E^{(3)}_{54}$ over k of degree 2 (take $C = \{O, P\}$ with $P = (-2(5-2\sqrt{-3}), 0)$). Hence $J^{(3)}_{26}$ and $J^{(3)}_{54}$ are isogenous over $\mathbf{Q}$, and have common conductor $N^2 = 63^2$. As mentioned above, $X^{(3)}_{26}$ ($\cong X^{(3)}_{-26}$) is a quotient curve of $X_0(63)$. The absolute invariants of Igusa [8] for $X^{(3)}_{26}$ and $X^{(3)}_{54}$ are given by

$$X^{(3)}_{26}\colon\ (J_2, J_4, J_6, J_{10}) = (3\cdot 439,\ 3\cdot 7^2 827,\ -7^4 11\cdot 181,\ 3^{12}7^6),$$

$$X^{(3)}_{54}\colon\ (J_2, J_4, J_6, J_{10}) = (3^4 37,\ 3^7 7\cdot 41,\ -3^9 7^2 53.\ 3^{21}7^3).$$

On the other hand, the absolute invariants of A_f of level $N = 63$ (see Table 9) are computed numerically by means of modular symbols. and we find that the absolute invariants of A_f and $J^{(3)}_{54}$ coincide. Hence $J^{(3)}_{54}$ is isogenous over $\mathbf{Q}$ to A_f, and isomorphic over $\bar{\mathbf{Q}}$ to A_f.

Next we let $p \geq 5$. Then we have the following criterion:

Theorem 6.2 ([5]). *Let D be a square-free positive integer divisible by a prime $p \geq 5$, and E a $\mathbf{Q}$-curve over a quadratic field k, with quadratic multiplication by $\mathbf{Q}(\sqrt{\pm D})$. Let $A = \mathrm{Re}_{k/\mathbf{Q}}E$ be the restriction of scalars of E. If $A/\mathbf{Q}$ has semi-stable reduction at p, then A is modular.*

There are three cases satisfying this condition for $N \leq 500$ (marked "‡" in Table 10), and clearly Theorem 6.2 applies to them.

Remark 6.3. In section 4, we also gave a family $\{\mathscr{E}_{d,u}^{(-p)}\}$ of $\mathbf{Q}$-curves over $\mathbf{Q}(\sqrt{d})$ with quadratic multiplication by $\mathbf{Q}(\sqrt{-p})$ for three cases: $(p,d)=(2,41),(3,109)$, $(5,29)$. By setting $u = 3/25,\ 1,\ 3/19$ for $\mathscr{E} = \mathscr{E}_{41,u}^{(-2)}$, $\mathscr{E}_{109.u}^{(-3)}$, $\mathscr{E}_{29,u}^{(-5)}$, respectively, we obtain a $\mathbf{Q}$-curve $\mathscr{E}$ over $k = \mathbf{Q}(\sqrt{d})$ with *everywhere good reduction*. Put $\mathscr{A} = \mathrm{Re}_{k/\mathbf{Q}}(\mathscr{E})$. Then we have

$$N = \sqrt{\mathrm{cond}(\mathscr{A}/\mathbf{Q})} = d.$$

One can find a newform f on $\Gamma_1(d)$ with Nebentypus character $\left(\frac{d}{\cdot}\right)$, having Fourier coefficients in $\mathbf{Q}(\sqrt{-p})$. Applying Theorem 6.2 for $p = 5$, we see that $\mathscr{A}$ is in fact modular, i.e., $\mathscr{A}$ is isogenous over $\mathbf{Q}$ to A_f attached to this f. For $p = 2, 3$, one also checks that the Euler factors of the L-functions of two abelian surfaces $\mathscr{A}$ and A_f over $\mathbf{Q}$ coincide for smaller primes.

Remark 6.4. Let D be a square-free composite number. One can also construct a family of $\mathbf{Q}$-curves of degree D over a quadratic field by the same method as in section 2 for some cases (but note that a $\mathbf{Q}$-curve of degree D is in general defined over a compositum of $\omega(D)$ quadratic fields, as mentioned in section 2). For instance, let $D = 10$. Then the following gives a family $\{\mathscr{E}_{-1,u}^{(10)}\}$ of $\mathbf{Q}$-curves of degree 10 over $k = \mathbf{Q}(\sqrt{-1})$:

$$\begin{aligned}
&\mathscr{E}_{-1,u}^{(10)}\colon y^2 = x^3 + Ax + B,\\
&\quad A = 2^2 3^3 \sqrt{-1}(u-1)(3u-1)\\
&\qquad \times \{9(265-54\sqrt{-1})u^6 + 2(-3330+2411\sqrt{-1})u^5\\
&\qquad\quad + 5(1209-2254\sqrt{-1})u^4 + 60(-14+193\sqrt{-1})u^3\\
&\qquad\quad - 5(357+1202\sqrt{-1})u^2 + 6(170+257\sqrt{-1})u - 11(15+14\sqrt{-1})\},\\
&\quad B = -2^4 3^3 (1-\sqrt{-1})(u-1)^2(3u-1)^2\\
&\qquad \times ((2+\sqrt{-1})u - 1)((1+4\sqrt{-1})u - (2+3\sqrt{-1}))\\
&\qquad \times ((1+10\sqrt{-1})u^2 - 8(1+\sqrt{-1})u + (5+2\sqrt{-1}))\\
&\qquad \times \{3(72+161\sqrt{-1})u^4 - 4(207+176\sqrt{-1})u^3 + 6(184+37\sqrt{-1})u^2\\
&\qquad\quad + 4(-153+16\sqrt{-1})u + (120-29\sqrt{-1})\}.
\end{aligned}$$

Write simply $\mathscr{E} = \mathscr{E}_{-1,u}^{(10)}$. Then there is in fact an isogeny $\phi\colon \mathscr{E} \to {}^{\sigma}\mathscr{E}$ of degree 10 over k. Furthermore, one checks that ${}^{\sigma}\phi\circ\phi = 10$ by using Proposition 4.5 (whose statement is naturally generalized to the case of composite degree). This means that $\mathscr{A} = \mathscr{A}_{-1,u}^{(10)} = \mathrm{Re}_{k/\mathbf{Q}}\mathscr{E}$ has real multiplication by $\mathbf{Q}(\sqrt{10})$:

$$\mathrm{End}_{\mathbf{Q}}\mathscr{A} \otimes \mathbf{Q} = \mathbf{Q}(\sqrt{10}).$$

Now set $u = 3/5$. Then $\mathscr{A}$ has conductor $N^2 = 544^2$, and Theorem 6.2 applies. Indeed, one can find a newform f on $\Gamma_0(544)$ with Fourier coefficients in $\mathbf{Q}(\sqrt{10})$, for which $\mathscr{A}$ is isogenous over $\mathbf{Q}$ to A_f.

Finally, we give two more examples of modular $\mathbf{Q}$-curves of degree 13 and 19.

Example 6.5. Consider two elliptic curves E_1, E_2 defined by

$$E_1: y^2 = x^3 + A_1 x + B_1,$$
$$A_1 = -27(25 - 8\sqrt{3}), \quad B_1 = 54(233 - 156\sqrt{3}),$$
$$E_2: y^2 = x^3 + A_2 x + B_2,$$
$$A_2 = 15(-53 + 8\sqrt{-15}), \quad B_2 = 10(1735 - 228\sqrt{-15}).$$

Then E_1 is a $\mathbf{Q}$-curve of degree 13 over $k_1 = \mathbf{Q}(\sqrt{3})$. Indeed, the j-invariant of this curve is obtained by setting $(a, b) = (4, 1)$ and $(p, d, u) = (13, 3, 0)$ in the equation of j given in Theorem 2.4. Furthermore, one can prove that $\mathrm{Re}_{k_1/\mathbf{Q}}(E_1)$ has real multiplication by $\mathbf{Q}(\sqrt{13})$ and has conductor $N^2 = 864^2$. Therefore, by Theorem 6.2, we see that E_1 is modular.

The curve E_2 is a $\mathbf{Q}$-curve of degree 19 over $k_2 = \mathbf{Q}(\sqrt{-15})$. This curve corresponds to a k_2-rational point on the modular curve

$$X_0(19): s^2 = t(t^3 - 16t^2 + 64t - 76), \tag{5}$$

see [2, II, p.414] for the covering $X_0(19) \to \mathbf{P}^1_j$. The equation (5) is transformed into a cubic form

$$S^2 = T^3 + 64\,T^2 + 1216\,T + 5776$$

by setting

$$(t, s) = (-76/T,\ 76\,S/T^2).$$

In fact, we find that E_2 corresponds to a Mordell–Weil generator (456, 684) of the elliptic curve

$$X_0(19)_{-15}: S^2 = T^3 + (-15)\cdot 64\,T^2 + (-15)^2\cdot 1216\,T + (-15)^3\cdot 5776$$

obtained by twisting $X_0(19)$ by $\sqrt{-15}$. (One can show that $X_0(19)_{-15}(\mathbf{Q}) \cong \mathbf{Z}$ with generator (456, 684) by using, e.g., Cremona's algorithm.) Furthermore, one can prove that $\mathrm{Re}_{k_2/\mathbf{Q}}(E_2)$ has real multiplication by $\mathbf{Q}(\sqrt{19})$ and has conductor $N^2 = 1350^2$. Therefore, by Theorem 6.2, we see that E_2 is modular.

Acknowledgments. The author would like to express his thanks to Professor K. Hashimoto for his warmful encouragement. The author also would like to thank A. Umegaki for his help to compute conductors of elliptic curves over quadratic fields.

References

[1] N. Elkies, A remark on elliptic K-curves, preprint.
[2] R. Fricke, "Die Elliptischen Funktionen und ihre Anwendungen", Teubner, 1916.
[3] B. Gross, "Arithmetic on elliptic curves with complex multiplication", Lecture Notes in Math. 776, Springer–Verlag, 1980.
[4] Y. Hasegawa, Modular abelian surfaces and hyperelliptic curves of genus two, preprint.
[5] Y. Hasegawa, K. Hashimoto, F. Momose, Modular conjecture for $\mathbf{Q}$-curves and QM-curves, preprint.
[6] K. Hashimoto, On Brumer's family of RM-curves of genus two, preprint.
[7] T. Hibino and N. Murabayashi, Modular equations of hyperelliptic $X_0(N)$ and an application, to appear in *Acta Arith.*
[8] J. Igusa, Arithmetic variety of moduli for genus two, *Ann. of Math.* **72** (1960), 612–649.

[9] F. Momose, On the l-adic representations attached to modular forms, *J. Fac. Sci. Univ. Tokyo* **28** (1981), 89–109.
[10] E. Pyle, "Abelian varieties over $\mathbf{Q}$ with large endomorphism algebras and their simple components over $\bar{\mathbf{Q}}$", Dissertation of the Univ. of California at Berkeley, 1995.
[11] K. Ribet, Twists of modular forms and endomorphisms of abelian varieties, *Math. Ann.* **253** (1980), 43–62.
[12] K. Ribet, "Abelian varieties over $\mathbf{Q}$ and modular forms", In 1992 Proceedings of KAIST Mathematics Workshop, pp.53–79, Korea Advanced Institute of Science and Technology, Taejon, 1992.
[13] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, *Duke Math. J.* **54** (1987), 179–230.
[14] G. Shimura, On the factors of the jacobian varieties of a modular function field, *J. Math. Soc. Japan* **25** (1973), 523–544.
[15] J. H. Silverman, "The Arithmetic of Elliptic Curves", Graduate Texts in Math. 106, Springer-Verlag, 1986.
[16] J. Vélu, Isogénies entre courbes elliptiques, *C.R. Acad. Sc. Paris* Sér.A **273** (1971), 238–241.
[17] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math.* **141** (1995), 443–551.