Tôhoku Math. J.
47 (1995), 271–296

SHIMURA CURVES AS INTERSECTIONS OF HUMBERT SURFACES AND DEFINING EQUATIONS OF QM-CURVES OF GENUS TWO

KI-ICHIRO HASHIMOTO AND NAOKI MURABAYASHI

(Received January 17, 1994, revised November 25, 1994)

Abstract. Shimura curves classify isomorphism classes of abelian surfaces with quaternion multiplication. In this paper, we are concerned with a fibre space, the base space of which is a Shimura curve and fibres are curves of genus two whose jacobian varieties are abelian surfaces of the above type. We shall give an explicit defining equation for such a fibre space when the discriminant of the quaternion algebra is 6 or 10.

Introduction. Let A be a simple principally polarized abelian variety of dimension two over the complex number field $\boldsymbol{C}$, and $\mathrm{End}(A)$ the ring of endomorphisms of A. Then, as is well-known, the $\boldsymbol{Q}$-algebra $\mathrm{End}^\circ(A):=\mathrm{End}(A)\otimes_{\boldsymbol{Z}}\boldsymbol{Q}$ is of one of the following types:

(i) a CM-field of degree four, (ii) an indefinite quaternion algebra,

(iii) a real quadratic field, or (iv) the rational number field $\boldsymbol{Q}$.

Let $\mathscr{A}_{2,1}$ be the moduli space of the isomorphism classes of abelian surfaces with principal polarization. The locus of each type in $\mathscr{A}_{2,1}$ has dimension 0, 1, 2, 3, respectively, whose irreducible components in the first three cases are called (i) CM-points, (ii) Shimura curves, and (iii) Humbert surfaces. On the other hand, it is also well-known that the Torelli map gives a birational morphism from $\mathscr{A}_{2,1}$ to the moduli space $\mathscr{M}_2$ of curves of genus two.

In this paper we are concerned with constructing, in a concrete way, an algebraic family of curves of genus two whose jacobian varieties belong to the case (ii) above. Namely, we wish to find out an equation for a fibre space, the base space of which is a Shimura curve and fibres are curves of genus two whose jacobian varieties have quaternion multiplications. Call such curves simply "QM-curves". We shall give defining equations over the rational number field $\boldsymbol{Q}$ for the algebraic family of QM-curves when the endomorphism ring is, generically, a maximal order $\mathcal{O}$ of the indefinite quaternion algebra $\boldsymbol{B}$ over $\boldsymbol{Q}$ which ramifies exactly at $\{2, 3\}$ or $\{2, 5\}$. To the best of our knowledge, not a single concrete example of *simple* QM-curves has been known before. Indeed, it is quite difficult to show that the jacobian variety of a given curve is simple.

The method of our construction is roughly as follows: In a classical work of Humbert [8], one can find general approach, as well as concrete solutions in some

1991 *Mathematics Subject Classification*. Primary 11G15; Secondary 11G18, 14G35, 14H40.

cases, to similar problems for the case (iii), i.e., to construct families of curves of genus two whose jacobian varieties have real multiplication of given discriminants (cf. [1], [18]). Especially, Humbert gives explicit form of "modular equations" for discriminants 5 and 8, in terms of the coefficients of the curves $Y^2 = f(X)$ (see (2), (3) in the text). Our idea is to combine these two equations in a suitable way. Indeed, if one can arrange the coordinate system in such a way that the two real multiplications, with discriminants 5 and 8, generate the order $\mathcal{O}$, then the fibre space we are looking for will be obtained as a component of the intersection of two Humbert's families. We determine possible components by studying quaternion modular embeddings of the upper half plane to the Siegel upper half plane of degree two. Although the calculations needed to find out the components are quite complicated, they can be performed by computer symbolic manipulation.

The main results are given as Theorems 1.3 and 1.7 in §1. As an application, we can give an equation for the universal family of supersingular curves of genus two over the finite field $\boldsymbol{F}_{p^2}$ for $p = 3$, 5. The proofs of the main results will be given in later sections. In §2, we recall briefly some results of Humbert [8] which are basic for our constructions. In §3, we study, in some detail, quaternion modular embeddings of the upper half plane to the Siegel upper half plane of degree two, in the case of maximal orders of the quaternion algebra which ramifies at $\{2, 3\}$, or $\{2, 5\}$. A more general treatment is given in [4]. Finally in §4, we describe briefly how the computation will be performed.

ACKNOWLEDGMENT. The authors thank Akira Kurihara for showing his interest and giving continuous encouragement during the preparation of this paper. They also thank Frans Oort and Don Zagier for valuable suggestions.

1. Statement of the main results. Let $\boldsymbol{B}$ be an indefinite division quaternion algebra over $\boldsymbol{Q}$, and $\mathcal{O}$ a maximal order of $\boldsymbol{B}$. We denote by $D_{\boldsymbol{B}}$ the product of primes at which $\boldsymbol{B}$ ramifies, and call it the discriminant of $\boldsymbol{B}$. Let $\alpha \mapsto \alpha'$ be the canonical involution on $\boldsymbol{B}$, and let $\mathrm{Tr}(\alpha) := \alpha + \alpha'$, $\mathrm{Nr}(\alpha) := \alpha\alpha'$ be the reduced trace and the reduced norm on $\boldsymbol{B}$, respectively. Then $\mathcal{O}^{(1)} := \{\alpha \in \mathcal{O} \mid \mathrm{Nr}(\alpha) = 1\}$ is regarded as a Fuchsian group of $\mathrm{SL}_2(\boldsymbol{R})$ and the compact Riemann surface $\mathcal{O}^{(1)} \backslash \mathfrak{H}$ is identified with the set of $\boldsymbol{C}$-valued points of the Shimura curve $S_{\boldsymbol{B}}$ (cf. [21], [22]). $S_{\boldsymbol{B}}(\boldsymbol{C})$ has the following interpretation. Let ρ be an element of $\mathcal{O}$ such that $\rho^2 = -D_{\boldsymbol{B}}$, $\rho\mathcal{O} = \mathcal{O}\rho$. The existence of such an element can be shown by strong approximation theorem, or by direct construction of $\mathcal{O}$ (cf. [3], [4], [9]). Then the involution of $\boldsymbol{B}$ defined by $\alpha \mapsto \alpha^* := \rho^{-1}\alpha'\rho$ is positive, and satisfies $\mathcal{O}^* = \mathcal{O}$. We have a one-to-one correspondence

$$S_{\boldsymbol{B}}(\boldsymbol{C}) \overset{1:1}{\longleftrightarrow} \left\{ (A, i, \Theta) \;\middle|\; \begin{array}{c} (A, \Theta)\text{: principally polarized abelian surface} \\ i : \mathcal{O} \hookrightarrow \mathrm{End}(A) \\ \text{Rosati involution with respect to } \Theta_{|\mathcal{O}} \text{ is } * \end{array} \right\}.$$

The above isomorphism can be described by the quaternion modular embedding. Indeed, let $\mathfrak{H}$ be the upper half plane and let

$$\mathfrak{H}_2 := \{\tau \in M_2(\boldsymbol{C}) \mid \tau = {}^t\tau,\ \mathrm{Im}(\tau) > 0\}$$

be the Siegel upper half space of degree two. It is known that there is an embedding of analytic spaces $\Psi : \mathfrak{H} \to \mathfrak{H}_2$, $z \mapsto \Omega(z)$, which is compatible with the actions of $\mathcal{O}^{(1)}$ and $Sp(4, \boldsymbol{Z})$ on each space, through an injection $\mathcal{O}^{(1)} \hookrightarrow Sp(4, \boldsymbol{Z})$. See §3 and also [4] for details. Now the following fact is well-known as a very special case of a result of Shimura [22], [23]:

PROPOSITION 1.1. *Let A be a principally polarized abelian variety of dimension two such that*

1. $\mathrm{End}(A) \supseteq \mathcal{O}$
2. *the Rosati involution coincides with the involution $*$ on $\mathcal{O}$.*

Then there exists an element $z \in \mathfrak{H}$ such that A is isomorphic to $A_{\Omega(z)}$ as a principally polarized abelian variety.

DEFINITON 1.2. Notation being as above, A is said to have Quaternion Multiplication by $(\mathcal{O}, *)$, or simply of type QM. A curve C of genus two is called a QM-curve with respect to $(\mathcal{O}, *)$, if its jacobian variety is of tyep QM.

Combining this with Torelli's theorem, we have a rational map

$$S_{\boldsymbol{B}} \to \mathcal{A}_{2,1}(\boldsymbol{C}) \cong Sp(4, \boldsymbol{Z}) \backslash \mathfrak{H}_2 \approx \mathcal{M}_2(\boldsymbol{C})\,.$$

Now the problem we are interested in solving is to describe the image of the Shimura curve $S_{\boldsymbol{B}}$ in $\mathcal{M}_2$ in terms of suitable coordinates on it. More precisely, we look for an equation of the following form:

$$\mathcal{S} : \ Y^2 = f(X; t, s) \in \bar{\boldsymbol{Q}}(t, s)[X]$$

where f is separable of degree 5 or 6 in X, and $\bar{\boldsymbol{Q}}(t, s) = \bar{\boldsymbol{Q}}(S_{\boldsymbol{B}})$ is the function field of S_{B} over the algebraic closure $\bar{\boldsymbol{Q}}$ of $\boldsymbol{Q}$, so that for each point $(t_0, s_0) \in S_{\boldsymbol{B}}(\bar{\boldsymbol{Q}})$ the corresponding curve

$$C_{(t_0, s_0)} : \ Y^2 = f(X; t_0, s_0)$$

is a QM-curve for $\mathcal{O}$ define over $\bar{\boldsymbol{Q}}$.

Here is an answer to this problem in the two cases where $D_{\boldsymbol{B}} = 6$, 10.

THEOREM 1.3. *The case $D_{\boldsymbol{B}} = 6$. The following equations give a family of* QM-*curves of discriminant* 6.

$$\mathcal{S}_6 : \ Y^2 = X(X^4 - PX^3 + QX^2 - RX + 1)\,,$$

with

$$g(t,s)=4s^2t^2-s^2+t^2+2=0\,,$$

$$P=-2(s+t)\,,\quad R=-2(s-t)\,,\quad Q=\frac{(1+2t^2)(11-28t^2+8t^4)}{3(1-t^2)(1-4t^2)}\,.$$

The discriminant of the right hand side of $\mathscr{S}_6$ is

$$\frac{2^4(1+2t^2)^{12}}{3^4(-1+t)^4(1+t)^4(-1+2t)^4(1+2t)^4}\,.$$

Our family $\mathscr{S}_6$ is over the affine curve E_6: $g(t,s)=0$ of genus one, while the genus of the Shimura curve $S_{\boldsymbol{B}_6}$ is zero. This is only to keep the formula in reasonable size. Indeed, our family can be reduced to that over $\boldsymbol{P}^1$, since we have the isomorphisms of fibres

$$C_{(t,s)}\cong C_{(-t,\,-s)}\cong C_{(-t,s)}\,,\qquad (x,y)\leftrightarrow(-x,\sqrt{-1}y)\leftrightarrow\left(\frac{1}{x},\frac{y}{x^3}\right).$$

It is interesting to observe that the base curve E_6 of $\mathscr{S}_6$ has (generic) real points. Recall that the Shimura curves have no real point.

By specializing (t,s) to those points $(t_0,s_0)\in\bar{\boldsymbol{Q}}^2$ such that $g(t_0,s_0)=0$, one can obtain as many QM-curves defined over $\bar{\boldsymbol{Q}}$ as one wishes. However, as shown in the following examples, the curve $C_{(t_0,s_0)}$ may be degenerate, or may be a split curve, i.e., the jacobian variety is isogenous to the product $E\times E$ of an elliptic curve E with complex multiplication. We note that the existence of curves of genus two on the product $E\times E'$ of two elliptic curves was studied by Hayashida [5], Hayashida-Nishi [6].

EXAMPLE 1.4. The fibre of $\mathscr{S}_6$ over $(t,s)=(\sqrt{-2}/2,\sqrt{2}/2)$ is a degenerate curve

$$C^{(6)}_{(\sqrt{-2}/2,\sqrt{2}/2)}\colon\ Y^2=X\left(X-\frac{1+\sqrt{-1}}{\sqrt{2}}\right)\left(X+\frac{1+\sqrt{-1}}{\sqrt{2}}\right)^3.$$

EXAMPLE 1.5. The fibre of $\mathscr{S}_6$ over $(t,s)=(0,\sqrt{2})$ is the curve

$$C^{(6)}_{(0,\sqrt{2})}\colon\ Y^2=X\left(X^4+2\sqrt{2}\,x^3+\frac{11}{3}X^2+2\sqrt{2}\,x+1\right),$$

which splits via a morphism ϕ of degree two

$$\phi\colon C^{(6)}_{(0,\sqrt{2})}\to E\colon y^2=x(1-x)\left(1-\frac{1+2\sqrt{3}-\sqrt{6}}{2}x\right),$$

$$\phi^*(x)=\frac{-2\sqrt{3}\,X}{3X^2+(3\sqrt{2}-\sqrt{3})X+3}\,,\qquad \phi^*(y)=\frac{\sqrt{(1+\sqrt{-2})(\sqrt{3}-\sqrt{-3})(X-1)}}{3X^2+(3\sqrt{2}-\sqrt{3})X+3}\,Y,$$

where E is the elliptic curve with complex multiplication by $\boldsymbol{Z}[\sqrt{-6}]$, whose invariant is $j(\sqrt{-6})=1728(1399+988\sqrt{2})$.

EXAMPLE 1.6. The fibres of $\mathcal{S}_6$ over $(t,s)=(1/4, \sqrt{11}/2)$, $(5/2, \sqrt{-22}/8)$, and $(3/2, \sqrt{-34}/8)$ are the curves

$$C^{(6)}_{(1/4,\sqrt{11}/2)}\colon Y^2=X\left(X^4+\frac{1+2\sqrt{11}}{2}X^3+\frac{99}{20}X^2+\frac{-1+2\sqrt{11}}{2}X+1\right),$$

$$C^{(6)}_{(5/2,\sqrt{-22}/8)}\colon Y^2=X\left(X^4+\frac{20+\sqrt{-22}}{4}X^3+\frac{297}{56}X^2+\frac{-20+\sqrt{-22}}{4}X+1\right),$$

$$C^{(6)}_{(3/2,\sqrt{-34}/8)}\colon Y^2=X\left(X^4+\frac{12+\sqrt{-34}}{4}X^3-\frac{253}{120}X^2+\frac{-12+\sqrt{-34}}{4}X+1\right).$$

One can show that the jacobian varieties of $C^{(6)}_{(1/4,\sqrt{11}/2)}$, $C^{(6)}_{(5/2,\sqrt{-22}/8)}$, $C^{(6)}_{(3/2,\sqrt{-34}/8)}$ are all simple, by calculating congruence zeta functions for their reduction modulo some primes. Let C be one of them, and put $\bar{C}_{\wp}:=C \bmod \wp$, with a prime ideal $\wp$ of K over p such that $\left(\frac{K}{\wp}\right)=+1$, where $K=\mathbf{Q}(\sqrt{11})$, $\mathbf{Q}(\sqrt{-22})$, $\mathbf{Q}(\sqrt{-34})$, respectively. Then $\bar{C}_{\wp}$ is defined over $\mathbf{F}_p$. Let N_m $(m=1,2,\dots)$ be the number of $\mathbf{F}_{p^m}$-rational points of $\bar{C}_{\wp}$. The congruence zeta function of $\bar{C}_{\wp}$ is expressed as

$$Z(\bar{C}_{\wp}/\mathbf{F}_p, u)=\exp\left(\sum_{m=1}^{\infty}\frac{N_m}{m}u^m\right)=\frac{(1-a_{\wp}u+pu^2)(1-b_{\wp}u+pu^2)}{(1-u)(1-pu)},$$

$$a_{\wp}+b_{\wp}=1+p-N_1\,,\quad a_{\wp}^2+b_{\wp}^2=1+4p+p^2-N_2\,,$$

where N_1, N_2, $a_{\wp}$, $b_{\wp}$ are as given in Table 1.

Now suppose that $A:=\mathrm{Jac}(C)$ *were* not simple. Then, since $\mathrm{End}^\circ(A)$ contains $\mathbf{B}$ as a $\mathbf{Q}$-subalgebra, we see that A must be isogenous to the product $E\times E$ of an elliptic curve E with itself which has complex multiplication corresponding to an imaginary quadratic field, say, K. Thus $\mathrm{End}^\circ(A)\cong \mathrm{M}_2(K)$, and it is mapped injectively to $\mathrm{End}^\circ(\bar{A}_{\wp})$, where $\bar{A}_{\wp}$ is the (good) reduction of A mod $\wp$ (cf. [24]). On the other hand, from Table 1 and Tate's theorem (cf. [25], [19]), one can show that $\mathrm{End}^\circ(\bar{A}_{\wp})\cong \mathrm{M}_2(K(\wp))$ with *distinct* imaginary quadratic fields $K(\wp)=\mathbf{Q}(\sqrt{a_{\wp}^2-4p})$ as $\wp$ varies among the primes such that $a_{\wp}=b_{\wp}$ and that $\bar{A}_{\wp}$ is not isogenous to a product of supersingular elliptic curves. When $a_{\wp}=-b_{\wp}$, we can make similar argument replacing the ground field by $\mathbf{F}_{p^2}$ so that $K(\wp)=\mathbf{Q}(\sqrt{a_{\wp}^2(a_{\wp}^2-4p)})$. We conclude that A must be simple.

THEOREM 1.7. *The case* $D_{\mathbf{B}}=10$. *The following equations give a family of* QM-*curves of discriminant* 10.

$$\mathcal{S}_{10}\colon Y^2=X(P^2X^4+P^2(1+R)X^3+PQX^2+P(1-R)X+1)\,,$$

with

TABLE 1. The congruence zeta functions of $C^{(6)}_{(1/4,\sqrt{11/2})}$, $C^{(6)}_{(5/2,\sqrt{-22/8})}$ and $C^{(6)}_{(3/2,\sqrt{-34/8})}$ for a small prime $\wp$.

	p	N_1	N_2	$a_\wp$	$b_\wp$	$a_\wp^2-4p$
$C^{(6)}_{(1/4,\sqrt{11/2})}$	7	8	62	$2\sqrt{2}$	$-2\sqrt{2}$	-20
	19	20	374	$4\sqrt{2}$	$-4\sqrt{2}$	-44
	37	46	1486	-4	-4	-132
	43	44	2006	$2\sqrt{2}$	$-2\sqrt{2}$	-164
	53	46	2990	4	4	-196
	79	80	6302	$8\sqrt{2}$	$-8\sqrt{2}$	-188
	83	84	6822	$10\sqrt{2}$	$-10\sqrt{2}$	-132
$C^{(6)}_{(5/2,\sqrt{-22/8})}$	13	14	158	$4\sqrt{2}$	$-4\sqrt{2}$	-20
	19	20	422	$2\sqrt{2}$	$-2\sqrt{2}$	-68
	23	16	590	4	4	-76
	29	30	894	$4\sqrt{2}$	$-4\sqrt{2}$	-84
	31	28	1078	2	2	-120
	43	44	1958	$4\sqrt{2}$	$-4\sqrt{2}$	-140
	47	52	2390	-2	-2	-184
$C^{(6)}_{(3/2,\sqrt{-34/8})}$	7	8	62	$2\sqrt{2}$	$-2\sqrt{2}$	-20
	23	32	590	-4	-4	-76
	29	38	926	-4	-4	-100
	31	32	1022	$4\sqrt{2}$	$-4\sqrt{2}$	-92
	37	38	1262	$8\sqrt{2}$	$-8\sqrt{2}$	-20
	43	32	1950	6	6	-136
	59	60	3574	$6\sqrt{2}$	$-6\sqrt{2}$	-164

$$g(t,s)=s^2-t(t-2)(2t+1)=0\,,$$

$$P=\frac{4(2t+1)(t^2-t-1)}{(t-1)^2}\,,\qquad R=\frac{(t-1)s}{t(t+1)(2t+1)}\,,$$

$$Q=\frac{(t^2+1)(t^4+8t^3-10t^2-8t+1)}{t(t-1)^2(t+1)^2}\,.$$

The discriminant of the right hand side of $\mathscr{S}_{10}$ is

$$\frac{2^4(t^2-2t-1)^{12}}{t^4(t-1)^8(t+1)^8}\,.$$

As for $\mathscr{S}_6$, our $\mathscr{S}_{10}$ is given as a family over the elliptic curve E_{10}: $g(t,s)=0$, while the genus of the Shimura curve $S_{\boldsymbol{B}_{10}}$ is also zero. $\mathscr{S}_{10}$ can be reduced to that over $\boldsymbol{P}^1$, since the two fibres on $(t,\pm s)$ are easily shown to be isomorphic.

EXAMPLE 1.8. The fibre of $\mathscr{S}_{10}$ over $(t, s)=(1+\sqrt{2}, 1+\sqrt{2})$ is a degenerate curve

$$C^{10}_{(1+\sqrt{2},1+\sqrt{2})}\colon Y^2=2^2(1+\sqrt{2})^6X\left(X+\frac{\sqrt{2}}{2}\right)\left(X-\frac{4-3\sqrt{2}}{2}\right)^3 .$$

EXAMPLE 1.9. The fibre of $\mathscr{S}_{10}$ over $(t, s)=(2, 0)$ is the curve

$$C^{10)}_{(2,0)}\colon Y^2=\frac{1}{9}X(30X^2+20X+3)(120X^2+40X+3),$$

which splits via a morphism ϕ of degree two

$$\phi\colon C^{(10)}_{(2,0)}\to E\colon y^2=x(1-x)\left(1-\frac{1-6\sqrt{2}-3\sqrt{10}}{2}x\right),$$

$$\phi^*(x)=\frac{-2\sqrt{10}X}{60X^2+(30-\sqrt{10})X+3}, \qquad \phi^*(y)=\frac{3\sqrt{-1+\sqrt{10}}(X-\sqrt{5}/10)Y}{60X^2+(30-\sqrt{10})X+3},$$

where E is the elliptic curve with complex multiplication by $\boldsymbol{Z}[\sqrt{-10}]$, whose invariant is $j(\sqrt{-10})=212846400+95178240\sqrt{5}$.

EXAMPLE 1.10. The fibres of $\mathscr{S}_{10}$ over $(t, s)=(-1/3, \sqrt{21}/9)$, $(-3, 5\sqrt{-3})$, and $(2+\sqrt{-5}, 3\sqrt{-5})$ are the curves

$$C^{(10)}_{(-1/3,\sqrt{21}/9)}\colon Y^2=\frac{1}{144}X(25X^4+(25+50\sqrt{21})X^3+575X^2$$
$$+(-60+120\sqrt{21})X+144),$$

$$C^{(10)}_{(-3,5\sqrt{-3})}\colon Y^2=\frac{1}{48}X(9075X^4+3025(3+2\sqrt{-3})X^3-6875X^2$$
$$+220(-3+2\sqrt{-3})X+48),$$

$$C^{(10)}_{(2+\sqrt{-5},3\sqrt{-5})}\colon Y^2=X\left((580+480\sqrt{-5})X^4+\frac{12100+12580\sqrt{-5}}{21}X^3\right.$$
$$\left.+\left(\frac{96200}{441}+\frac{5200\sqrt{-5}}{49}\right)X^2+\frac{550+106\sqrt{-5}}{21}X+1\right).$$

One can show as example 1.6 that $C^{(10)}_{(-1/3,\sqrt{21}/9)}$, $C^{(10)}_{(-3,5\sqrt{-3})}$, $C^{(10)}_{(2+\sqrt{-5},3\sqrt{-5})}$ are simple, by using the results on congruence zeta functions given in Table 2.

Finally, we note that the reduction of a Shimura curve at the prime where $\boldsymbol{B}$ ramifies gives the moduli of supersingular abelian surfaces (cf. [20]). Moreover, it is known that the number of irreducible components of the moduli of such curves is one for $p\leq 11$

TABLE 2. The congruence zeta functions of $C^{(10)}_{(-1/3,\sqrt{21}/9)}$, $C^{(10)}_{(-3,5\sqrt{-3})}$ and $C^{(10)}_{(2+\sqrt{-5},3\sqrt{-5})}$ for a small prime $\wp$.

	p	N_1	N_2	$a_\wp$	$b_\wp$	$a_\wp^2-4p$
$C^{(10)}_{(-1/3,\sqrt{21}/9)}$	17	10	326	4	4	-52
	37	38	1358	$4\sqrt{5}$	$-4\sqrt{5}$	-68
	41	42	1806	$2\sqrt{5}$	$-2\sqrt{5}$	-144
	43	44	1982	$2\sqrt{5}$	$-2\sqrt{5}$	-152
	47	60	2326	-6	-6	-152
	59	60	3558	$4\sqrt{5}$	$-4\sqrt{5}$	-156
	67	68	4718	$2\sqrt{5}$	$-2\sqrt{5}$	-248
$C^{(10)}_{(-3,5\sqrt{-3})}$	13	14	182	$2\sqrt{5}$	$-2\sqrt{5}$	-32
	19	20	398	$2\sqrt{5}$	$-2\sqrt{5}$	-56
	31	40	1054	-4	-4	-108
	37	30	1486	4	4	-132
	43	44	1862	$4\sqrt{5}$	$-4\sqrt{5}$	-92
	61	62	3806	$4\sqrt{5}$	$-4\sqrt{5}$	-164
	67	56	4686	6	6	-232
$C^{(10)}_{(2+\sqrt{-5},3\sqrt{-5})}$	23	24	582	$2\sqrt{5}$	$-2\sqrt{5}$	-72
	29	30	918	$2\sqrt{5}$	$-2\sqrt{5}$	-96
	41	42	1806	$2\sqrt{5}$	$-2\sqrt{5}$	-144
	43	44	1862	$4\sqrt{5}$	$-4\sqrt{5}$	-92
	47	40	2366	4	4	-172
	61	78	3838	-8	-8	-180
	67	48	4558	10	10	-168

(cf. [12]). Thus as a corollary to the above theorems, we obtain the following:

COROLLARY 1.11. *For $p=3$, 5, a one-parameter family of supersingular curves of genus two over the field F_{p^2} with p^2 elements is given by the following equation:*

(i) *For $p=3$*

$$\mathscr{S}_6:\ Y^2=X(X^4-(1-\sqrt{-1})X^3+qX^2+(1-\sqrt{-1})X+1)\,,$$

with a variable

$$q=\frac{(t^4+1)^3}{t^2(t^2-1)^2(t^2+1)^2}\,.$$

(ii) *For $p=5$*

$$\mathscr{S}_{10}:\ Y^2=X(P^2X^4+P^2(1+R)X^3+PQX^2+P(1-R)X+1)\,,$$

with

$$P=\frac{-(2t^2+1)(t^4-t^2-1)}{(t^2-1)^2},$$

$$R=\frac{(t^2-1)}{\sqrt{2}\,t(t^2+1)},\quad Q=\frac{(t^4+1)(t^8-2t^6+2t^2+1)}{t^2(t^2-1)^2(t^2+1)^2}.$$

REMARK 1.12. One can check the above result also by showing the vanishing of the Hasse-Witt matrices for these equations (cf. [17], [26], [12]).

2. A work of Humbert.

Let

$$\tau=\begin{pmatrix}\tau_1 & \tau_2\\ \tau_2 & \tau_3\end{pmatrix}$$

be a point of the Siegel upper half plane $\mathfrak{H}_2$ of degree two. Put $A_\tau=\boldsymbol{C}^2/L_\tau$ with L_τ the lattice generated by the columns of the matrix $(\tau\ 1_2)$. Put

$$a=\begin{pmatrix}1/2\\1/2\end{pmatrix}\quad\text{and}\quad b=\begin{pmatrix}1\\1/2\end{pmatrix}.$$

For z in $\boldsymbol{C}^2$, the 2-dimensional holomorphic theta function with the characteristic determined by a and b is defined by

$$\theta(z)=\sum_{n\in\boldsymbol{Z}^2}\exp(\pi\sqrt{-1}\,{}^t(n+a)\tau(n+a)+2\pi\sqrt{-1}\,{}^t(n+a)(z+b)),$$

where n is written as a column vector and ${}^tv$ denotes the transpose of a column vector v. The following lemma is well-known:

LEMMA 2.1. *Let p, q be column vectors in $\boldsymbol{Z}^2$. Then*

$$\theta(z+\tau p+q)=\exp(-\pi\sqrt{-1}\,{}^tp\tau p-2\pi\sqrt{-1}\,{}^tp(z+b)+2\pi\sqrt{-1}\,{}^taq)\theta(z).$$

Moreover, $\theta(z)$ is an odd function.

We denote by Θ the divisor of zeros of $\theta(z)$ on A_τ. Then (A_τ, Θ) is a principally polarized abelian surface. From now on, we assume that Θ is isomorphic to a curve C of genus two. We recall Humbert's notation for 2-torsion points of A_τ (cf. [8]). Let

$$\xi=\frac{1}{2}\begin{pmatrix}\varepsilon+\lambda\tau_1+\lambda'\tau_2\\ \varepsilon'+\lambda\tau_2+\lambda'\tau_3\end{pmatrix}\pmod{L_\tau}$$

be a 2-torsion point of A_τ with ε, ε', λ, $\lambda'\in\{0, 1\}$. Then Humbert's notation is given in Table 3.

The next lemma follows from Lemma 2.1:

TABLE 3. Humbert's notation.

Notation	ε	ε'	λ	λ'
(11)	0	0	0	0
(12)	0	1	0	0
(21)	1	0	0	0
(22)	1	1	0	0
(31)	0	0	1	0
(32)	0	1	1	0
(41)	1	0	1	0
(42)	1	1	1	0
(13)	0	0	0	1
(14)	0	1	0	1
(23)	1	0	0	1
(24)	1	1	0	1
(33)	0	0	1	1
(34)	0	1	1	1
(43)	1	0	1	1
(44)	1	1	1	1

LEMMA 2.2.

$$\Theta \cap A_\tau[2] = \{(11), (22), (31), (41), (23), (24)\},$$

where $A_\tau[2]$ is the set of 2-torsion points of A_τ.

Let $\phi: A_\tau \to \boldsymbol{P}^3$ be a morphism corresponding to the complete linear system $|2\Theta|$. The image of ϕ is a quartic surface in $\boldsymbol{P}^3$ and can be identified with the quotient space $A_\tau/\langle \iota \rangle$, where ι is the involution of A_τ given by $\xi \mapsto -\xi$. This image is called the Kummer surface of A_τ and is denoted by $\mathrm{Kum}(A_\tau)$. For every $\xi \in A_\tau[2]$, we put

$$\Theta_\xi := T_\xi(\Theta) \quad \text{and} \quad \Theta_\xi^\wedge := \phi(T_\xi(\Theta)),$$

where T_ξ denotes the translation by ξ.

Since $2T_\xi(\Theta) \in |2\Theta|$, there exists a unique hyperplane H_ξ in $\boldsymbol{P}^3$ such that the intersection divisor of H_ξ and $\mathrm{Kum}(A_\tau)$ is equal to the divisor $2\Theta_\xi^\wedge$. H_ξ is called the singular plane of $\mathrm{Kum}(A_\tau)$. From now on, we denote $\phi((ij))$ $(1 \le i, j \le 4)$ by the same notation (ij) and call them double points of $\mathrm{Kum}(A_\tau)$. Then singular planes can be uniquely represented by sixteen symbols kl $(1 \le k, l \le 4)$ such that the following conditions are satisfied:

1. The set of the six double points lying on the singular plane kl is $\{(ij) \mid i = k, j \ne l$ or $i \ne k, j = l\}$.

2. The set of the six singular planes passing through the double point (ij) is $\{kl \mid k = i, l \ne j$ or $k \ne i, l = j\}$.

We choose and fix a hyperplane Π in $\boldsymbol{P}^3$ which does not contain (11). Figure 1 represents

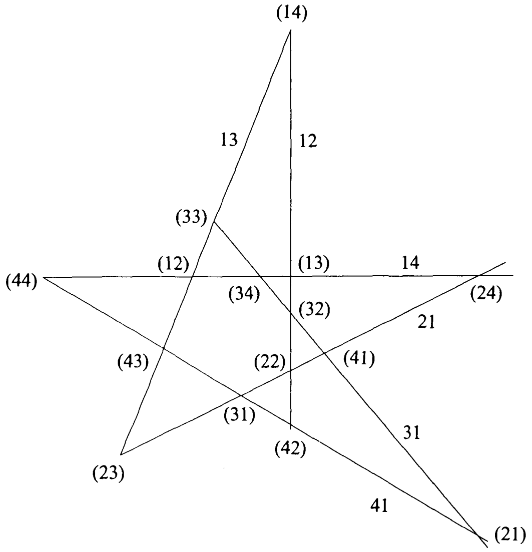

FIGURE 1. The section of singular planes.

the section by Π of the six singular planes of Kum(A_τ) passing through (11). On each line in Figure 1 we mark the symbol of the corresponding singular plane: 12, 13, 14, 21, 31, 41; on the intersection of two lines we mark the symbol of the double point, different from (11), lying on the two corresponding singular planes. Therefore, the point (ij) in Figure 1 is the projection of the double point (ij) from the double point (11) on Π.

REMARK 2.3. Let D be a curve on Kum(A_τ). Then the projection of D from (11) on Π intersects the six lines in Figure 1 at points (ij) or touches them because the singular plane H_ξ touches Kum(A_τ) along the conic $\Theta_\xi^\wedge$.

PROPOSITION 2.4. *There exists a conic Γ in Π which touches the six lines in Figure* 1.

PROOF. Consider the tangent cone to Kum(A_τ)$\subset \boldsymbol{P}^3$ at the double point (11) and let Γ be its section by Π. Then Γ satisfies the above condition. □

We can take a homogeneous coordinate $(x:y:z)$ of $\Pi \cong \boldsymbol{P}^2$ such that Γ is given by the equation $yz=x^2$ and that any three among the six contact points are given by

$$(x:y:z)=(0:0:1),(-1:1:1),(0:1:0)\,.$$

So it may be assumed that the lines 14, 21, 12, 13, 31, 41 are given by the equations

$$y+2a_1x+a_1^2z=0\,,\quad y+2a_2x+a_2^2z=0\,,\quad y+2a_3x+a_3^2z=0\,,$$

$$y=0\,,\quad y+2x+z=0\,,\quad z=0\,,$$

respectively. It is convenient to denote the lines 14, 21, 12, 13, 31, 41 by l_1, l_2, l_3, l_4,

l_5, l_6, respectively.

PROPOSITION 2.5. *C is isomorphic to the curve given by the equation*

$$Y^2=X(X-1)(X-a_1)(X-a_2)(X-a_3)\,. \tag{1}$$

PROOF. Let $\Theta_{(\hat{\hat{1}}2)}$ be the projection of $\Theta_{(\hat{1}2)}$ from the double point (11) to Π. Then $\Theta_{(\hat{\hat{1}}2)}$ is a conic in Π and the degree of the canonical map $\rho\colon C\cong\Theta\to\Theta_{(\hat{\hat{1}}2)}$ is two. By Lemma 2.2, $\Theta_{(\hat{\hat{1}}2)}$ passes through the points (12), (21), (32), (42), (24), (23) in Figure 1 and the coordinates of these points are

$$(-a_1/2:0:1)\,,\quad (1:-2:0)\,,\quad (-(a_3+1)/2:a_3:1)\,,$$
$$(1:-2a_3:0)\,,\quad (-(a_1+a_2)/2:a_1a_2:1)\,,\quad (-a_2/2:0:1)\,,$$

respectively. It is convenient to change the coordinate by

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}=\begin{pmatrix} 1 & 0 & a_1/2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Then the above coordinates are replaced by

$$(0:0:1)\,,\quad (1:-2:0)\,,\quad ((a_1-a_3-1)/2:a_3:1)\,,$$
$$(1:-2a_3:0)\,,\quad (-a_2/2:a_1a_2:1)\,,\quad ((a_1-a_2)/2:0:1)\,,$$

respectively. Therefore $\Theta_{(\hat{\hat{1}}2)}$ is given by the equation

$$4a_3(x')^2+(y')^2+2(a_3+1)x'y'+(a_2a_3-a_1a_2+a_2-a_3)y'z'+2a_3(a_2-a_1)z'x'=0\,.$$

By mapping a point Q of $\Theta_{(\hat{\hat{1}}2)}$ to $t/s\in\boldsymbol{P}^1$, where the line passing through (12) and Q is given by the equation $sx'+ty'=0$, we get

$$(\Theta_{(\hat{\hat{1}}2)},\ \{(12),(21),(32),(42),(24),(23)\})$$
$$\cong\left(\boldsymbol{P}^1,\left\{\infty,\frac{1}{2},\frac{1}{2a_3},-\frac{a_1-a_3-1}{2a_3},\frac{1}{2a_1},\frac{a_2a_3-a_1a_2+a_2-a_3}{2a_3(a_2-a_1)}\right\}\right).$$

By the linear fractional transformation induced by the matrix

$$\begin{pmatrix} -2a_1a_3/(1-a_1) & a_3/(1-a_1) \\ -2a_3/(1-a_1) & -(a_1-a_3-1)/(1-a_1) \end{pmatrix},$$

the latter is isomorphic to

$$(\boldsymbol{P}^1,\{0,1,\infty,a_1,a_2,a_3\})\,.$$

On the other hand, the set of ramification points of $\rho\colon C\to\Theta_{(\hat{\hat{1}}2)}$ is

$$\{(12),(21),(32),(42),(24),(23)\}\,.$$

Hence C is isomorphic to the curve $Y^2=X(X-1)(X-a_1)(X-a_2)(X-a_3)$. □

Now we consider the endomorphism ring $\mathrm{End}(A_\tau)$ of A_τ. Analytically,

$$\mathrm{End}(A_\tau)=\{\alpha\in \mathrm{M}_2(\boldsymbol{C})\,|\,\exists M\in \mathrm{M}_4(\boldsymbol{Z}) \text{ with } (*)\ \alpha(\tau\ 1_2)=(\tau\ 1_2)M\}\,.$$

Let

$$M=\begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Then we see that the above condition $(*)$ is equivalent to

$$\alpha=\tau B+D,\, \alpha\tau=\tau A+C \Longleftrightarrow (**)\ \tau B\tau+D\tau-\tau A-C=0\,.$$

Let E be the Riemann form associated to the polarization Θ. Then E defines an involution $\alpha\mapsto\alpha^\circ$ on $\mathrm{End}(A_\tau)$ called the Rosati involution, which is determined by $E(\alpha z, w)=E(z, \alpha^\circ w)$ (for all $z, w\in \boldsymbol{C}^2$). We have

$$\alpha^\circ=\alpha \Longleftrightarrow {}^tM\begin{pmatrix} 0 & 1_2 \\ -1_2 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 1_2 \\ -1_2 & 0 \end{pmatrix}M$$

$$\Longleftrightarrow A={}^tD\,,\quad B=\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix},\quad C=\begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix}.$$

Put

$$A=\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}.$$

Under the assumption $\alpha^\circ=\alpha$, it follows that

$$(**) \Longleftrightarrow a_2\tau_1+(a_4-a_1)\tau_2-a_3\tau_3+b(\tau_2^2-\tau_1\tau_3)+c=0\,.$$

Then we have

$$\alpha=\tau B+D=\begin{pmatrix} -b\tau_2+a_1 & b\tau_1+a_3 \\ -b\tau_3+a_2 & b\tau_2+a_4 \end{pmatrix},$$

and

$$\begin{aligned} \mathrm{Tr}\,\alpha&=a_1+a_4\,,\\ \det\alpha&=-b\{a_2\tau_1+(a_4-a_1)\tau_2-a_3\tau_3+b(\tau_2^2-\tau_1\tau_3)\}+a_1a_4-a_2a_3\\ &=a_1a_4-a_2a_3+bc\,. \end{aligned}$$

So the characteristic polynomial of α is

$$T^2-(a_1+a_4)T+(a_1a_4-a_2a_3+bc)=0$$

and its discriminant is

$$(a_1+a_4)^2-4(a_1a_4-a_2a_3+bc)=(a_4-a_1)^2-4a_2(-a_3)-4bc\,.$$

DEFINITION 2.6 (cf. [8]). An element

$$\tau=\begin{pmatrix}\tau_1 & \tau_2\\ \tau_2 & \tau_3\end{pmatrix}$$

of $\mathfrak{H}_2$ is said to have a singular relation with invariant Δ if there exist relatively prime integers a, b, c, d, $e\in\boldsymbol{Z}$ such that

1. $a\tau_1+b\tau_2+c\tau_3+d(\tau_2^2-\tau_1\tau_3)+e=0$,
2. $\Delta=b^2-4ac-4de$.

As we have stated above, a singular relation of τ with invariant Δ corresponds to endomorphisms of A_τ fixed by the Rosati involution which have the characteristic polynomial with discriminant Δ. Let

$$N_\Delta=\{\tau\in\mathfrak{H}_2\,|\,\tau\text{ has a singular relation with invariant }\Delta\}\,,$$

and H_Δ the image of N_Δ under the canonical map $\mathfrak{H}_2\to Sp(4,\boldsymbol{Z})\backslash\mathfrak{H}_2$, where $Sp(4,\boldsymbol{Z})$ is the symplectic group over $\boldsymbol{Z}$ and $Sp(4,\boldsymbol{Z})\backslash\mathfrak{H}_2$ denotes the quotient space with respect to the well-known action. H_Δ is called the Humbert surface of invariant Δ. The following result, which is stated explicitly in [1, p. 212] is essentially due to Humbert:

PROPOSITION 2.7. *Each point of H_Δ can be represented by $\tau\in\mathfrak{H}_2$ satisfying an equation $a\tau_1+b\tau_2+\tau_3=0$ with $b^2-4a=\Delta$, $b=0$ or* 1.

PROPOSITION 2.8 (cf. [8]). *If $\tau\in\mathfrak{H}_2$ satisfies the relation $-\tau_1+\tau_2+\tau_3=0$, then there exists a conic D in Π which passes through the five points* (34), (14), (33), (22), (24) *and touches the line l_6 (see Figure* 1). *Conversely, if such a conic D exists, τ has a singular relation with $\Delta=5$.*

PROOF. We shall give a proof for the first part. As we have seen above, the relation $-\tau_1+\tau_2+\tau_3=0$ gives an endomorphism α of A_τ corresponding to the matrix

$$\begin{pmatrix}0 & -1 & 0 & 0\\ -1 & 1 & 0 & 0\\ 0 & 0 & 0 & -1\\ 0 & 0 & -1 & 1\end{pmatrix}.$$

The characteristic polynomial of α is $T^2-T-1=0$. Since

$$\alpha(\{(34),(14),(33),(22),(24),(11)\})=\{(42),(44),(31),(21),(43),(11)\}$$

and the latter set is equal to $\Theta_{(31)}\cap A_\tau[2]$, it follows that

$$\alpha^*\Theta_{(31)}\cap A_\tau[2]=\{(34),(14),(33),(22),(24),(11)\}\,,$$

where $\alpha^*\Theta_{(31)}$ denotes the inverse image of $\Theta_{(31)}$ by α. Let D' be the projection of

$\phi(\alpha^*\Theta_{(31_1)})$ from (11) to Π and D the closure of D'. Since

$$D \cap \{(ij) \text{ in Figure } 1\} = \{(34), (14), (33), (22), (24)\}\,,$$

D necessarily touches the line l_6 by Remark 2.3. As for the intersection number we have

$$(2\Theta, \alpha^*\Theta_{(31_1)}) = (2\Theta_{(31_1)}, \alpha^*\Theta_{(31_1)}) = 2\,\mathrm{Tr}_{K/\boldsymbol{Q}}(\alpha^2) = 6\,,$$

where $K = \boldsymbol{Q}(\sqrt{5})$. Therefore $\phi(\alpha^*\Theta_{(31_1)})$ is a curve of degree three because the degree of ϕ is two. We consider a line l in Π such that l and D meet transversally at points outside $D \setminus D'$ and the set $\mathrm{Sing}(D)$ of singular points of D. Let H be the hyperplane in $\boldsymbol{P}^3$ which contains l and (11). Then we have

$$(D, l) = \sharp\{D \cap l\} \leq \sharp\{H \cap \phi(\alpha^*\Theta_{(31_1)}) \setminus \{(11)\}\} \leq 2\,.$$

So D is a line or a conic. Since D is not a line, D is a conic. Hence D satisfies the conditions in the proposition. □

Using this proposition, Humbert calculated a modular equation for H_5.

THEOREM 2.9 (cf. [8]). *There exists a conic in Π which satisfies the conditions in Proposition* 2.8 *if and only if the identity*

$$\begin{aligned} (2) \qquad & 4(a_1^2a_3 - a_2^2 + a_3^2(1-a_1) + a_2 - a_3)(a_1^2a_2a_3 - a_1a_2^2a_3) \\ & = (a_1^2a_3(a_2+1) - a_2^2(a_1+a_3) + a_2a_3^2(1-a_1) + a_1(a_2-a_3))^2 \end{aligned}$$

holds.

PROOF. Since (24), (22), (14), (33), (34) are $l_1 \cap l_2$, $l_2 \cap l_3$, $l_3 \cap l_4$, $l_4 \cap l_5$, $l_5 \cap l_1$, respectively, their coordinates with respect to $(x:y:z)$ are

$$(-(a_1+a_2):2a_1a_2:2)\,, \quad (-(a_2+a_3):2a_2a_3:2)\,, \quad (-a_3:0:2)\,,$$
$$(-1:0:2)\,, \quad (-(a_1+1):2a_1:2)\,,$$

respectively. Let $p_1x^2 + p_2y^2 + p_3z^2 + p_4xy + p_5yz + p_6zx = 0$ be the defining equation of D. Then

$$p_1 = 4a_1a_2a_3(a_1 - a_2)\,,$$

$$p_2 = a_1^2a_3 - a_1a_3^2 + (a_3^2 - a_2^2 + a_2 - a_3)\,,$$

$$p_3 = a_1a_2a_3^2(a_1 - a_2)\,,$$

$$p_4 = 2((a_2a_3 + a_3)a_1^2 + (-a_2a_3^2 - a_2^2 + a_2 - a_3)a_1 - a_2a_3(a_2 - a_3))\,,$$

$$p_5 = (-a_2^2a_3 - a_2^2 + a_3^2 + a_2)a_1^2 + (-a_2^2a_3^2 - a_3^2)a_1 - a_2a_3(a_2 - a_3)\,,$$

$$p_6 = 2a_1a_2a_3(a_1 - a_2)(a_3 + 1)\,.$$

D touches the line l_6 if and only if the quadratic equation $p_1X^2 + p_4X + p_2 = 0$ has a multiple root, that is, $p_4^2 - 4p_1p_2 = 0$. □

REMARK 2.10. Actually, (2) is not exactly the equation for H_5, but rather that of a component which projects to H_5 under the natural map $\mathcal{M}_{2,2} \to \mathcal{M}_2$, whre $\mathcal{M}_{2,2}$, is the moduli space of genus two curves with level two structure. Indeed, one observes that (2) is not symmetric in the a_i's. A similar assertion applies also to the equation (3) of H_8 below.

Humbert also calculated a modular equation of H_8.

PROPOSITION 2.11 (cf. [8]). *If $\tau \in \mathfrak{H}_2$ satisfies the relation $-2\tau_1 + \tau_3 = 0$, then there exists a curve of degree four and genus one in* Kum(A_τ) *which passes through the double points* (32), (34), (42), (44). *Projecting from* (11) *on Π, we get a conic in Π which passes through the four points in Π corresponding to the above double points and touches the lines l_2 and l_4. Conversely if such a conic exists in Π, then τ satisfies a singular relation with $\Delta = 4$ or* 8.

THEOREM 2.12 (cf. [8]). *Consider a conic $y = x^2$ and its six tangents*

$$l_\delta : y + 2\delta x + \delta^2 = 0 , \qquad \delta = \infty, 0, b_1, b_2, b_3, b_4 .$$

Then there exists a conic which passes through the four points

$$l_{b_1} \cap l_{b_2} , \quad l_{b_2} \cap l_{b_3} , \quad l_{b_3} \cap l_{b_4} , \quad l_{b_4} \cap l_{b_1}$$

and touches l_∞ and l_0 if and only if the identity

$$(3) \qquad (b_1 b_3 - b_2 b_4)^2 \times \{4 b_1 b_2 b_3 b_4 ((b_1 + b_3)(b_2 + b_4) - 2(b_1 b_3 + b_2 b_4))^2 \\ - (b_2 - b_4)^2 (b_1 - b_3)^2 (b_1 b_3 + b_2 b_4)^2\} = 0$$

holds. Moreover, the first factor corresponds to $\Delta = 4$ and the second corresponds to $\Delta = 8$.

3. Quaternion modular embeddings for $D = 6$, 10. We shall describe the concrete form of such embeddings in detail in the two cases $D = 6$, 10 which we need. A general treatment is given in [4].

3.1. The case $D = 6$. Let $\boldsymbol{B}_6$ be the quaternion algebra over $\boldsymbol{Q}$ with discriminant 6 and $\mathcal{O}_6$ a maximal order of $\boldsymbol{B}_6$. One can take the model

$$\boldsymbol{B}_6 = \boldsymbol{Q} + \boldsymbol{Q}i + \boldsymbol{Q}j + \boldsymbol{Q}ij , \quad i^2 = -6 , \quad j^2 = 2 , \quad ji = -ij ,$$

$$\mathcal{O}_6 = \boldsymbol{Z} + \boldsymbol{Z}\frac{i+j}{2} + \boldsymbol{Z}\frac{i-j}{2} + \boldsymbol{Z}\frac{2+2j+ij}{4} .$$

Put $\rho_1 = i$ and consider an involution $\alpha \mapsto \alpha^* := \rho_1^{-1} \alpha' \rho_1$ on $\boldsymbol{B}_6$ where $'$ is the canonical involution on $\boldsymbol{B}_6$. Then one has $\mathcal{O}_6^* = \mathcal{O}_6$. Since $\rho_1^2 = -6 < 0$, the involution is positive: $\mathrm{Tr}(\alpha\alpha^*) > 0$ (if $\alpha \neq 0$). We identify $\boldsymbol{B}_6 \otimes_{\boldsymbol{Q}} \boldsymbol{R}$ with $\mathrm{M}_2(\boldsymbol{R})$ by the isomorphism defined by

$$i \mapsto \begin{pmatrix} 0 & -1 \\ 6 & 0 \end{pmatrix} , \quad j \mapsto \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix} .$$

For an element $z \in \mathfrak{H}$, we define an $\boldsymbol{R}$-linear isomorphism f_z by

$$f_z\colon \boldsymbol{B}_6 \otimes_{\boldsymbol{Q}} \boldsymbol{R} \to \boldsymbol{C}^2\,, \quad \alpha \mapsto \alpha\begin{pmatrix} z \\ 1 \end{pmatrix}.$$

Put $D_z = f_z(\mathcal{O}_6)$. It follows that D_z is a lattice in $\boldsymbol{C}^2$. Define a pairing $E_z\colon \boldsymbol{C}^2 \times \boldsymbol{C}^2 \to \boldsymbol{R}$ by $E_z(f_z(\alpha), f_z(\beta)) = \mathrm{Tr}(\rho_1^{-1}\alpha\beta')$. Then, since $\mathcal{O}_6\rho_1$ is the inverse different of $\mathcal{O}_6$, it induces a nondegenerate pairing $E_z\colon D_z \times D_z \to \boldsymbol{Z}$. Set

$$\omega_1 := f_z(1) = \begin{pmatrix} z \\ 1 \end{pmatrix}, \quad \omega_2 := f_z\left(\frac{i+j}{2}\right) = \begin{pmatrix} \dfrac{\sqrt{2}\,z-1}{2} \\[2ex] \dfrac{6z-\sqrt{2}}{2} \end{pmatrix},$$

$$\omega_3 := f_z\left(\frac{i-j}{2}\right) = \begin{pmatrix} \dfrac{\sqrt{2}\,z-1}{2} \\[2ex] \dfrac{6z+\sqrt{2}}{2} \end{pmatrix}, \quad \omega_4 := f_z\left(\frac{2+2j+ij}{4}\right) = \begin{pmatrix} \dfrac{2(1+\sqrt{2}\,)z+\sqrt{2}}{4} \\[2ex] \dfrac{6\sqrt{2}\,z+2(1-\sqrt{2}\,)}{4} \end{pmatrix}.$$

Then $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ is a $\boldsymbol{Z}$-basis of D_z and we have

$$(E_z(\omega_k, \omega_l)) = \begin{pmatrix} 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

We put $\omega'_1 := -\omega_3$, $\omega'_2 := \omega_4$, $\omega'_3 := -\omega_1$, $\omega'_4 := \omega_3 - \omega_2$. Then $\{\omega'_1, \omega'_2, \omega'_3, \omega'_4\}$ is a symplectic basis, i.e.,

$$(E_z(\omega'_i, \omega'_j)) = \begin{pmatrix} 0 & 1_2 \\ -1_2 & 0 \end{pmatrix}.$$

Also put $(\Omega_1(z)\,\Omega_2(z)) = (\omega'_1\omega'_2\omega'_3\omega'_4)$, and $\Omega(z) := \Omega_2(z)^{-1}\Omega_1(z)$. We have

$$\Omega(z) = \frac{1}{2\sqrt{2}\,z}\begin{pmatrix} \sqrt{2} & \sqrt{2}\,z \\ 1 & -z \end{pmatrix}\begin{pmatrix} \dfrac{\sqrt{2}\,z+1}{2} & \dfrac{2(1+\sqrt{2}\,)z+\sqrt{2}}{4} \\[2ex] \dfrac{-6z-\sqrt{2}}{2} & \dfrac{6\sqrt{2}\,z+2(1-\sqrt{2}\,)}{4} \end{pmatrix}$$

$$= \begin{pmatrix} \dfrac{3}{2}z - \dfrac{1}{4z} & -\dfrac{3\sqrt{2}}{4}z - \dfrac{1}{2} - \dfrac{\sqrt{2}}{8z} \\[2ex] -\dfrac{3\sqrt{2}}{4}z - \dfrac{1}{2} - \dfrac{\sqrt{2}}{8z} & \dfrac{3}{4}z - \dfrac{1}{2} - \dfrac{1}{8z} \end{pmatrix} \in \mathfrak{H}_2\,.$$

Thus we get an embedding $\Psi: \mathfrak{H} \to \mathfrak{H}_2$, $z \mapsto \Omega(z)$. We see immediately that the complex torus $\boldsymbol{C}^2/D_z$ has a structure of an abelian variety, with the principal polarization defined by E_z, and is isomorphic to $A_{\Omega(z)}$. It is easy to check the following lemma:

LEMMA 3.1. *$\Omega(z)$ satisfies the following singular relations parametrized by two independent integers d, $e \in \boldsymbol{Z}$:*

$$-(d+e)\tau_1 + d\tau_2 + (d+2e)\tau_3 + d(\tau_2^2 - \tau_1\tau_3) + e = 0\,.$$

Especially, it satisfies the singular relations

(4) $$-\tau_1 + 2\tau_3 + 1 = 0 \quad \textit{with} \quad \Delta = 8\,,$$

(5) $$\tau_2 - \tau_3 + (\tau_2^2 - \tau_1\tau_3) - 1 = 0 \quad \textit{with} \quad \Delta = 5\,,$$

(6) $$-\tau_1 + \tau_2 + \tau_3 + (\tau_2^2 - \tau_1\tau_3) = 0 \quad \textit{with} \quad \Delta = 5\,.$$

By Lemma 3.1 and Proposition 1.1, we have:

PROPOSITION 3.2. *Let A be as above. Then there exists $\tau \in \mathfrak{H}_2$ such that $A \cong A_\tau$ and that τ satisfies two singular relations* (4), (5) *of Lemma* 3.1.

To combine the modular equations for $\Delta = 5$ and 8, we need some lemmas.

LEMMA 3.3. *Let τ be an element of $\mathfrak{H}_2$ which satisfies the two singular relations* (4), (5) *of Lemma* 3.1. *Let M_i $(i = 1, 2, 3)$ be the matrices in $Sp(4, \boldsymbol{Z})$ given by*

$$M_1 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 1 & 1 & 2 \\ 1 & 1 & 2 & 1 \\ 3 & 2 & 4 & 4 \\ -1 & 0 & -2 & 1 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1 & 1 & -1 & 0 \\ 1 & 1 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

and put

$$\tau' = \begin{pmatrix} \tau'_1 & \tau'_2 \\ \tau'_2 & \tau'_3 \end{pmatrix} := \tau \cdot M_1\,, \quad \tau'' := \tau \cdot M_2\,, \quad \tau'' := \tau \cdot M_3 \in \mathfrak{H}_2\,,$$

where $\tau \cdot N = (\tau B + D)^{-1}(\tau A + C)$ for

$$N = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp(4, \boldsymbol{Z})\,.$$

Then the singular relation (4) *is transformed by M_1 to*

$$-2\tau'_1 + \tau'_3 = 0 \quad (\Delta = 8)\,,$$

and (5) (*resp.* (6)) *is transformed by M_2* (*resp. M_3*) *to*

$$-\tau''_1 + \tau''_2 + \tau''_3 = 0 \quad (\Delta = 5)\,, \quad (\textit{resp.}\ -\tau'''_1 + \tau'''_2 + \tau'''_3 = 0\ (\Delta = 5))\,.$$

This lemma can be checked by direct calculation. One has then $\tau' \cdot M = \tau''$,

$M=M_1^{-1}M_2$. Consider the isomorphism

$$\begin{aligned}\Phi\colon A_{\tau'}&=\mathbf{C}^2/\langle(\tau'\ 1_2)\rangle\\ &=\mathbf{C}^2/\langle(\tau'A+C\tau'B+D)\rangle\to\mathbf{C}^2/\langle(\tau''\ 1_2)\rangle=A_{\tau''}\end{aligned}$$

induced by the matrix $(\tau'B+D)^{-1}$ where $\langle(\tau\ 1_2)\rangle=L_\tau$ and

$$M=\begin{pmatrix}A & B\\ C & D\end{pmatrix}=\begin{pmatrix}4 & 3 & 5 & 6\\ -1 & 0 & -2 & 1\\ -1 & -1 & -1 & -2\\ -1 & -1 & -2 & -1\end{pmatrix}.$$

LEMMA 3.4. *For an element*

$$\xi=\frac{1}{2}\begin{pmatrix}\varepsilon_1+\lambda_1\tau'_1+\lambda'_1\tau'_2\\ \varepsilon'_1+\lambda_1\tau'_2+\lambda'_1\tau'_3\end{pmatrix}\ (\operatorname{mod} L_{\tau'})\in A_{\tau'}[2]\,,$$

we put

$$\Phi(\xi)=\frac{1}{2}\begin{pmatrix}\varepsilon_2+\lambda_2\tau''_1+\lambda'_2\tau''_2\\ \varepsilon'_2+\lambda_2\tau''_2+\lambda'_2\tau''_3\end{pmatrix}\ (\operatorname{mod} L_{\tau''})\in A_{\tau''}[2]\,,$$

where ε_i, ε'_i, λ_i, λ'_i $(i=1, 2)\in\{0, 1\}$. Then we have

$$\begin{pmatrix}\varepsilon_2\\ \varepsilon'_2\\ \lambda_2\\ \lambda'_2\end{pmatrix}=\begin{pmatrix}0 & 1 & 1 & 1\\ 1 & 0 & 1 & 1\\ 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\end{pmatrix}\begin{pmatrix}\varepsilon_1\\ \varepsilon'_1\\ \lambda_1\\ \lambda'_1\end{pmatrix}.$$

This can be proved by direct calculation and we omit the detail.

Put

$$\begin{aligned}(7)\qquad F_1(X, Y, Z)=&4(X^2Z-Y^2+Z^2(1-X)+(Y-Z))(X^2YZ-XY^2Z)\\ &-(X^2Z(Y+1)-Y^2(X+Z)+YZ^2(1-X)+X(Y-Z))^2\,,\end{aligned}$$

$$(8)\qquad F_2(X, Y, Z)=4XYZ((X+Y)(Z+1)-2XY-2Z)^2-(Z-1)^2(X-Y)^2(XY+Z)^2\,.$$

THEOREM 3.5. *Let C be a* QM-*curve of genus two defined over $\mathbf{C}$ with respect to $(\mathcal{O}_6, *)$. Then C has a model with defining equation* (1) *such that*

$$(9)\qquad F_1(a_1, a_2, a_3)=F_2(a_1, a_2, a_3)=0\,.$$

PROOF. Let τ', τ'' be as in Lemma 3.3. By Proposition 3.2 and Lemma 3.3, we have an isomorphism

$$\operatorname{Jac}(C)\cong A_{\tau''}\xleftarrow{\ \Phi\ }A_{\tau'}\,.$$

C has a model given in Proposition 2.5 with τ'' instead of τ. By Proposition 2.11 there exists a curve of degree four and genus one in $\mathrm{Kum}(A_{\tau'})$ passing through (32), (34), (42), (44). Using Lemma 3.4, we see that Φ induces

$$\{(32), (34), (42), (44)\} \xrightarrow{\Phi} \{(34), (41), (13), (22)\} .$$

So we have a curve of degree four and genus one in $\mathrm{Kum}(A_{\tau''})$ passing through (34), (41), (13), (22). Projecting it from (11) on Π, we obtain a conic in Π which passes through

$$l_1 \cap l_3 , \quad l_3 \cap l_2 , \quad l_2 \cap l_5 , \quad l_5 \cap l_1$$

and touches l_4 and l_6. Hence the second factor on the left hand side of the equation in Theorem 2.12 vanishes at $b_1 = a_1$, $b_2 = a_3$, $b_3 = a_2$, $b_4 = 1$. Therefore $F_2(a_1, a_2, a_3) = 0$. On the other hand, by Proposition 2.8 and Theorem 2.9 we have $F_1(a_1, a_2, a_3) = 0$. □

3.2. The case $D = 10$. We can take a model

$$\boldsymbol{B}_{10} = \boldsymbol{Q} + \boldsymbol{Q}i + \boldsymbol{Q}j + \boldsymbol{Q}ij , \qquad i^2 = -10 , \quad j^2 = 13 , \quad ji = -ij$$

$$\mathcal{O}_{10} = \boldsymbol{Z} + \boldsymbol{Z}\frac{1+j}{2} + \boldsymbol{Z}\frac{i+ij}{2} + \boldsymbol{Z}\frac{30j+ij}{13}$$

and consider an involution on $\boldsymbol{B}_{10}$, $\alpha \mapsto \alpha^{**} := \rho_2^{-1}\alpha'\rho_2$, where $\rho_2 = i$. We identify $\boldsymbol{B}_{10} \otimes_{\boldsymbol{Q}} \boldsymbol{R}$ with $M_2(\boldsymbol{R})$ by the isomorphism defined by

$$i \mapsto \begin{pmatrix} 0 & -1 \\ 10 & 0 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} \sqrt{13} & 0 \\ 0 & -\sqrt{13} \end{pmatrix}.$$

Define, for each $z \in \mathfrak{H}$, an $\boldsymbol{R}$-linear isomorphism $f_z \colon \boldsymbol{B}_{10} \otimes_{\boldsymbol{Q}} \boldsymbol{R} \to \boldsymbol{C}^2$, and observe that $D_z := f_z(\mathcal{O}_{10})$ is a lattice in $\boldsymbol{C}^2$. Let $E \colon D_z \times D_z \to \boldsymbol{Z}$ be a pairing as in Section 3.1. Put

$$\omega_1 := f_z(1) , \quad \omega_2 := f_z\left(\frac{1+j}{2}\right), \quad \omega_3 := f_z\left(\frac{i+ij}{2}\right), \quad \omega_4 := f_z\left(\frac{30j+ij}{13}\right),$$

and

$$\omega'_1 := \omega_3 - 6\omega_4 , \quad \omega'_2 := -30\omega_1 - \omega_4 , \quad \omega'_3 := \omega_1 , \quad \omega'_4 := \omega_2 .$$

Then $\{\omega'_1, \omega'_2, \omega'_3, \omega'_4\}$ is a symplectic basis. Set $(\Omega_1(z)\,\Omega_2(z)) = (\omega'_1\ \omega'_2\ \omega'_3\ \omega'_4)$. We have

$$\Omega(z) := \Omega_2(z)^{-1}\Omega_1(z)$$

$$= \frac{1}{13z}\begin{pmatrix} \dfrac{\sqrt{13}-7}{2} + 180z + 5(7+\sqrt{13})z^2 & \dfrac{1-\sqrt{13}}{2} - 360z - 5(1+\sqrt{13})z^2 \\ \dfrac{1-\sqrt{13}}{2} - 360z - 5(1+\sqrt{13})z^2 & -1 - 60z + 10z^2 \end{pmatrix}.$$

LEMMA 3.6. *$\Omega(z)$ satisfies the following singular relations parametrized by two* *independent integers $a, d \in \boldsymbol{Z}$:*

$$a\tau_1+(a-60d)\tau_2-3a\tau_3+d(\tau_2^2-\tau_1\tau_3)+830d=0\,.$$

Especially, it satisfies the singular relations

$$5\tau_1-55\tau_2-15\tau_3+(\tau_2^2-\tau_1\tau_3)+830=0 \quad \textit{with} \quad \Delta=5\,, \tag{10}$$

$$4\tau_1-56\tau_2-12\tau_3+(\tau_2^2-\tau_1\tau_3)+830=0 \quad \textit{with} \quad \Delta=8\,. \tag{11}$$

LEMMA 3.7. *Let τ be an element of $\mathfrak{H}_2$ which satisfies the two singular relations given in Lemma* 3.6. *Put*

$$N_1=\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & -1 & 1 \\ -15 & -14 & 30 & -29 \\ -33 & -34 & 4 & -4 \end{pmatrix}, \quad N_2=\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & -1 & 1 \\ -11 & -12 & -28 & 29 \\ -34 & -33 & -5 & 5 \end{pmatrix}$$

and

$$\tau'=\begin{pmatrix} \tau_1' & \tau_2' \\ \tau_2' & \tau_3' \end{pmatrix}:=\tau\cdot N_1\,, \quad \tau''=\begin{pmatrix} \tau_1'' & \tau_2'' \\ \tau_2'' & \tau_3'' \end{pmatrix}:=\tau\cdot N_2\,.$$

Then the first singular relation in Lemma 3.6 *is transformed by N_1 to*

$$-2\tau_1'+\tau_3'=0 \quad (\Delta=8)\,,$$

and the second is transformed by N_2 to

$$-\tau_1''+\tau_2''+\tau_3''=0 \quad (\Delta=5)\,.$$

Set

$$N=N_1^{-1}N_2=\begin{pmatrix} A & B \\ C & D \end{pmatrix}=\begin{pmatrix} 1 & 2 & 1 & -1 \\ 0 & -1 & -1 & 1 \\ -3 & -3 & 1 & 0 \\ -3 & -3 & 2 & -1 \end{pmatrix}.$$

Consider the isomorphism

$$\begin{aligned}\Phi\colon A_{\tau'}&=\boldsymbol{C}^2/\langle(\tau'\ 1_2)\rangle \\ &=\boldsymbol{C}^2/\langle(\tau'A+C\tau'B+D)\rangle\rightarrow\boldsymbol{C}^2/\langle(\tau''\ 1_2)\rangle=A_{\tau''}\end{aligned}$$

induced by the matrix $(\tau'B+D)^{-1}$.

LEMMA 3.8. *Let notation be as in Lemma* 3.4. *Then we have*

$$\begin{pmatrix} \varepsilon_2 \\ \varepsilon'_2 \\ \lambda_2 \\ \lambda'_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} \varepsilon_1 \\ \varepsilon'_1 \\ \lambda_1 \\ \lambda'_1 \end{pmatrix} .$$

PROOF. This lemma is proved similarly as Lemma 3.4, by

$$\begin{pmatrix} {}^tA & -{}^tC \\ -{}^tB & {}^tD \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \pmod 2 .$$

□

THEOREM 3.9. *Let C be a* QM-*curve of genus two defined over* **C** *with respect to* $(\mathcal{O}_{10}, **)$. *Then C has a model with canonical equation* (1) *such that*

$$F_1(a_1, a_2, a_3) = F_2(a_1, a_2, a_3) = 0 .$$

PROOF.

$$\{(32), (34), (42), (44)\} \xrightarrow{\Phi} \{(23), (12), (31), (44)\}$$

$$\xrightarrow{T_{(21)}} \{(34), (41), (13), (22)\} .$$

□

REMARK 3.10. From a result in [4], it can be shown that the intersection $H_5 \cap H_8$ has no components other than S_6 and S_{10}, except those corresponding to degenerate curves or split ones. This can also be shown by the explicit computations in the next section.

By Theorems 3.5 and 3.9, we thus see that, to construct the family of QM-curves for $\mathcal{O}_6$ and $\mathcal{O}_{10}$, it suffices to solve the systems of equations (9) (cf. Remark 2.10).

4. Intersections of Humbert surfaces H_5 and H_8. Here we sketch briefly the computations to find out the equations $\mathcal{S}_6$ and $\mathcal{S}_{10}$ as the components of $H_5 \cap H_8$.

First we rewrite the equation (1) of our QM-curve in homogeneous form. Namely we study the curves with the equation

$$(12) \qquad Y^2 = X(X-x)(X-y)(X-z)(X-w) .$$

Note that this curve is isomorphic to a similar one which satisfies $xyzw = 1$. Thus we may replace x, y, z by x/w, y/w, z/w where x, y, z, w are subject to the relation $xyzw = 1$, hence by x^2yz, y^2zx, z^2xy, respectively. This amounts to considering the curves with the equation

$$Y^2=X(X^4-PX^3+QX^2-RX+1)\,, \tag{13}$$

with

$$P=x+y+z+w=x+y+z+\frac{1}{xyz}\,,$$

$$Q=xy+yz+zx+w(x+y+z)=xy+yz+zx+\frac{x+y+z}{xyz}\,,$$

$$R=xyz+(xy+yz+zx)w=xyz+\frac{xy+yz+zx}{xyz}\,.$$

We have then

$$F_1(x^2yz, y^2zx, z^2xy)=x^6y^4z^4f_1(x, y, z)\,,$$

$$F_2(x^2yz, y^2zx, z^2xy)=x^4y^4z^6f_{2,a}(x, y, z)f_{2,b}(x, y, z)\,,$$

with

$$\begin{aligned} f_1(x, y, z)= &-y^2+2yz+2xy^4z-z^2-2x^2y^2z^2+2xy^3z^2-2y^4z^2\\ &-x^2y^6z^2+2x^2yz^3-4xy^2z^3-4x^2y^5z^3+2xy^6z^3+2y^2z^4\\ &-x^4y^2z^4+2x^3y^3z^4+4x^2y^4z^4+2xy^5z^4-y^6z^4+2x^4y^6z^4\\ &-4xy^4z^5+2x^5y^4z^5+2y^5z^5-4x^4y^5z^5-y^4z^6-2x^4y^4z^6\\ &+2x^3y^5z^6-2x^2y^6z^6-x^6y^6z^6+2x^2y^5z^7+2x^5y^6z^7-x^4y^6z^8\,, \end{aligned}$$

$$\begin{aligned} f_{2,a}(x, y, z)= &-x+y-2x^2y-2xy^2-x^3y^2+x^2y^3+4xyz+4x^3y^3z+x^2yz^2\\ &-xy^2z^2-2x^3y^2z^2-2x^2y^3z^2+x^4y^3z^2-x^3y^4z^2\,, \end{aligned}$$

$$\begin{aligned} f_{2,b}(x, y, z)= &\,x-y-2x^2y-2xy^2+x^3y^2-x^2y^3+4xyz+4x^3y^3z-x^2yz^2\\ &+xy^2z^2-2x^3y^2z^2-2x^2y^3z^2-x^4y^3z^2+x^3y^4z^2\,. \end{aligned}$$

Observe that $f_1(\sqrt{-1}\,x, \sqrt{-1}\,y, \sqrt{-1}\,z)=-f_1(x, y, z)$, $f_{2,a}(\sqrt{-1}\,x, \sqrt{-1}\,y, \sqrt{-1}\,z)=-\sqrt{-1}f_{2,b}(x, y, z)$. Thus we are reduced to solving the equations $f_1(x, y, z)=0$, $f_{2,a}(x, y, z)=0$, where $f_{2,a}$ has half the size of F_2. This enables one to compute the resultant $\mathrm{Rt}(x, y)$ of them with respect to z which factors, as we expect from Theorems 3.5 and 3.9:

$$\mathrm{Rt}(x, y)=x^2y^6(-x+y)^4(-1+x^3y)^2(-1+xy^3)^2\times \mathrm{Rt}_1(x, y)\,\mathrm{Rt}_2(x, y)\,,$$

$$\begin{aligned} \mathrm{Rt}_1= &\,x^4+4x^3y+6x^2y^2-4x^6y^2+4xy^3+y^4+72x^4y^4+6x^8y^4\\ &-8x^7y^5-4x^2y^6+100x^6y^6-4x^{10}y^6-8x^5y^7+6x^4y^8+72x^8y^8\\ &+x^{12}y^8+4x^{11}y^9-4x^6y^{10}+6x^{10}y^{10}+4x^9y^{11}+x^8y^{12}\,, \end{aligned}$$

$$\begin{aligned}\mathrm{Rt}_2=&x^4-12x^3y+38x^2y^2-4x^6y^2-12xy^3+128x^3y^3+64x^5y^3+y^4\\&+200x^4y^4+6x^8y^4+64x^3y^5+128x^5y^5-104x^7y^5-4x^2y^6\\&-220x^6y^6-4x^{10}y^6-104x^5y^7-128x^7y^7+64x^9y^7+6x^4y^8\\&+200x^8y^8+x^{12}y^8+64x^7y^9-128x^9y^9-12x^{11}y^9-4x^6y^{10}\\&+38x^{10}y^{10}-12x^9y^{11}+x^8y^{12}\,.\end{aligned}$$

Note that Rt_1 is symmetric in x, y. So putting $x+y=2s$, $xy=t$, we obtain a very simple equation

$$\mathrm{St}_1(t,s):=\mathrm{Rt}_1(x,y)=4s^2t^3(-1+t^2)^2+s^4(-1+t^2)^4+4t^4(1+t^2)^2\,,$$

which is easily solved as

$$s=\frac{t(\sqrt{1-t+t^2}+\sqrt{-1}\sqrt{1+t+t^2})}{-1+t^2}\,.$$

Putting

$$a=\frac{-\sqrt{1-t+t^2}}{1+t}\,,\quad b=\frac{\sqrt{-1}\sqrt{1+t+t^2}}{1-t}\,,$$

we thus have a parametric expression

$$P=-2(a+b)\,,\quad R=2(a-b)\,,\quad Q=\frac{1+t^6-9(t^2+t^4)}{t(1-t^2)^2}\,.$$

Here we observe that a^2, b^2 and Q have rational expressions in $u:=t+1/t$. Indded, we easily have

$$a^2=\frac{u-1}{u+2}\,,\quad b^2=\frac{-(u+1)}{u-2}\,,\quad Q=\frac{u(u^2-12)}{u^2-4}\,.$$

Eliminating u from these equalities, we obtain

$$Q=\frac{(1+2a^2)(11-28a^2+8a^4)}{3(1-a)(1+a)(1+2a)(1-2a)}\,,\quad 4a^2b^2+a^2-b^2+2=0\,.$$

This completes the proof of Theorem 1.3.

Next we consider the equation $\mathrm{Rt}_2(x,y)=0$. Putting again $x+y=2s$, $xy=t$, we obtain

$$\begin{aligned}\mathrm{St}_2(t,s):&=\frac{1}{16}\mathrm{Rt}_2(x,y)\\&=s^4(t^2-1)^4-4s^2t(t^2-1)^2(t^2+t-1)(t^2-t-1)+4t^2(t^2+1)^2(t^2-t-1)^2\,,\end{aligned}$$

from which follows

$$s=\frac{\sqrt{t(t^2-t-1)}(\sqrt{t-2}+\sqrt{t(2t+1)})}{1-t^2}.$$

Hence we have

$$P=-2\left(\frac{\sqrt{(t-2)(t^2-t-1)}}{\sqrt{t}(t+1)}+\frac{\sqrt{(2t+1)(t^2-t-1)}}{(t-1)}\right),$$

$$R=2\left(\frac{\sqrt{(t-2)(t^2-t-1)}}{\sqrt{t}(t+1)}-\frac{\sqrt{(2t+1)(t^2-t-1)}}{(t-1)}\right),$$

$$Q=\frac{(t^2+1)(t^4+8t^3-10t^2-8t+1)}{t(t-1)^2(t+1)^2}.$$

Putting $s=\sqrt{t(t-2)(2t+1)}$, and replacing X by $2\sqrt{(2t+1)(t^2-t-1)}X/(t-1)^2$, we easily have an equation

$$Y^2=X(A^2X^4+A^2(1+B)X^3+AQX^2+A(1-B)X+1),$$

with

$$A=\frac{4(2t+1)(t^2-t-1)}{(t-1)^2}, \quad B=\frac{(t-1)s}{t(t+1)(2t+1)},$$

which is birationally equivalent to (13). This completes the proof of Theorem 1.7.

References

[1] G. van der Geer, Hilbert modular surface, Springer-Verlag, Berlin, Heidelberg, 1988.

[2] R. Hartshorne, Algebraic geometry, Springer-Verlag, New York, 1977.

[3] K. Hashimoto, Base change of simple algebras and symmetric maximal orders of quaternion algebras, Memoirs of Sci. & Eng., Waseda Univ. 53 (1989) 21–45.

[4] K. Hashimoto, Explicit form of quaternion modular embeddings, to appear in Osaka Math. J.

[5] T. Hayashida, A class number associated with the product of an elliptic curve with itself, J. Math. Soc. Japan 20 (1968), 26–43.

[6] T. Hayashida and M. Nishi, Existence of curves of genus two on a product of two elliptic curves, J. Math. Soc. Japan 17 (1965), 1–16.

[7] R. W. H. T. Hudson, Kummer's quartic surface, Cambridge Univ. Press, 1990.

[8] G. Humbert, Sur les fonctions abéliennes singulières, Œuvres de G. Humbert 2, pub. par les soins de Pierre Humbert et de Gaston Julia, Paris, Gauthier-Villars (1936), 297–401.

[9] T. Ibukiyama, On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings, Nagoya Math. J. 88 (1982), 181–195.

[10] J. Igusa, Arithmetic variety of moduli for genus two, Ann. of Math. 72 (1960), 612–649.

[11] B. Jordan and R. Livné, Local Diophantine properties of Shimura curves, Math. Ann. 270 (1985), 235–248.

[12] T. Ibukiyama, T. Katsura and F. Oort, Supersingular curves of genus two and class numbers, Comp. Math. 57 (1986), 127–152.

[13] A. Krazer, Lehrbuch der Thetafunktionen, Chelsea, New York, 1970.

[14] R. M. Kuhn, Curves of genus 2 with split jacobian, Trans. Amer. Math. Soc. 307 (1988), 41–49.

[15] A. Kurihara, On some examples of equations defining Shimura curves and the Mumford uniformization, J. Fac. Sci. Univ. Tokyo 25 (1979), 277–301.

[16] A. Kurihara, On p-adic Poincaré series and Shimura curves, International J. of Math. 5, No. 5 (1994), 747-763.

[17] Yu. I. Manin, The theory of commutative formal groups over fields of finite characteristic, Russian Math. Surveys 18 (1963), 1–83.

[18] F. Mestre, Familles de courbes hyperelliptiques multiplications reélles, Arithmetic Algebraic Geometry, Birkhäuser, (1991), 193–208.

[19] D. Mumford, Abelian varieties, Oxford Univ. Press, London, 1970.

[20] M. Ohta, On l-adic representations of Galois groups obtained from certain two dimensional abelian varieties, J. Fac. Sci. Univ. Tokyo 21 (1974), 299–308.

[21] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan, no. 11, Princeton Univ. Press, 1971.

[22] G. Shimura, On the zeta-functions of the algebraic curves uniformized by certain automorphic functions, J. Math. Soc. Japan 13 (1961) 275–331.

[23] G. Shimura, Construction of class fields and zeta functions of algebraic curves, Ann. of Math. 85 (1967), 58–159.

[24] G. Shimura and Y. Taniyama, Complex multiplications of Abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, no. 6, 1961.

[25] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (1966), 134–144.

[26] N. Yui, On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, J. of Algebra 52 (1978), 378–410.

Department of Mathematics
School of Science and Engineering
Waseda University
4–1 Okubo 3-chome, Shinjuku-ku
Tokyo, 169
Japan

Department of Mathematical Sciences
Faculty of Science
Yamagata University
Yamagata, 990
Japan