ACTA ARITHMETICA
XCIII.2 (2000)

Explicit moduli for curves of genus 2 with real multiplication by $\mathbb{Q}(\sqrt{5})$

by

John Wilson (Oxford)

1. Motivation. Let $J_0(N)$ denote the Jacobian of the modular curve $X_0(N)$ parametrizing pairs of N-isogenous elliptic curves. The simple factors of $J_0(N)$ have real multiplication, that is to say that the endomorphism ring of a simple factor A contains an order in a totally real number field of degree $\dim A$. We shall sometimes abbreviate "real multiplication" to "RM" and say that A has *maximal RM by the totally real field* F if A has an action of the full ring of integers of F. We say that a curve C has RM (or maximal RM) by F when the Jacobian $\mathrm{Jac}(C)$ does.

Let us call an abelian variety *modular* if it is isogenous to a simple factor of $J_0(N)$ for some N. Save for some technical restrictions, it is now known that all elliptic curves (that is, RM abelian varieties of dimension 1) are modular. It is also conjectured that all RM abelian varieties are modular [14]. In a recent paper, Taylor and Shepherd-Barron [15] have shown that many abelian surfaces with maximal real multiplication by $\mathbb{Q}(\sqrt{5})$ are modular. (Again, there are some technical conditions to be met.)

It is well known that principally polarized abelian surfaces are either Jacobians, or products. Thus principally polarized abelian surfaces with maximal RM are amenable to a fairly explicit description, if one can determine which curves give these surfaces as Jacobians. Our aim, then, is to attempt to give a description of those curves of genus 2 with maximal RM by $\mathbb{Q}(\sqrt{5})$ both in terms of their moduli and by giving equations for the curves. (We also note that it follows from other work of ours [17, Chapter 4] that an abelian surface with RM is almost always isogenous over the ground field to a principally polarized abelian surface with maximal RM.)

Acknowledgements. I should like to thank Prof. Birch for his supervision of the doctoral thesis of which this work forms a part.

2000 *Mathematics Subject Classification*: 11G10, 11G15.

2. Humbert's criterion. Let C be a curve of genus 2, and let $J = \mathrm{Jac}(C)$. We shall denote by $\dagger$ the canonical Rosati involution on J, and by $\mathrm{End}(J)^{\dagger=1}$ the ring of endomorphisms fixed by the Rosati involution. Also, throughout the following, we shall write $\eta = \frac{1}{2}(1+\sqrt{5})$.

Recall that the bicanonical map $C \to \mathbb{P}^2$ induces a 2-1 map of C onto a plane conic Q, say. Let $P_1, \ldots, P_6$ be the branch points of this map. Then the following theorem, originally due to Humbert [9] (see also [5, Chapter IX] and [11]), characterizes when J has maximal RM by $\mathbb{Q}(\sqrt{5})$.

THEOREM 1 (Humbert's criterion). *There is an embedding of* $\mathbb{Z}[\eta]$ *into* $\mathrm{End}(J)^{\dagger=1}$ *if and only if, for some ordering of the* P_i*, the conic which is tangent to each of the edges of the pentagon* $P_1P_2P_3P_4P_5$ *passes through* P_6*.*

We briefly review the proof of one implication as given in [5] and [11]. Let D be the image of a symmetric embedding $C \hookrightarrow J$. Suppose that $i : \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)^{\dagger=1}$, and let $\varepsilon = i(\eta - 1)$. Now let K be the Kummer surface $K = J/\langle -1 \rangle$, and let H be the image of $\varepsilon^* D$ on K. It is known that K admits an embedding as a quartic surface in $\mathbb{P}^3$ with sixteen nodes (which are the images of $J[2]$) as its only singularities (see [6]; the classic reference is [8]). The divisor H is then a rational cubic curve passing through six of these nodes. Projection through a chosen node to $\mathbb{P}^2$ yields the projective dual of Humbert's criterion.

In the sequel, by an *Humbert configuration* we shall mean a configuration as in Theorem 1, that is a tuple $(Q, R; P_1, \ldots, P_6)$ consisting of two plane conics Q and R and six points $P_1, \ldots, P_6$ on Q such that R passes through P_6 and is tangent to the edges of the pentagon $P_1P_2P_3P_4P_5$. If we say that an Humbert configuration $(Q, R; P_1, \ldots, P_6)$ is an *Humbert configuration for the curve* C, we mean that C is a double cover of Q branched over $P_1, \ldots, P_6$.

We can copy Humbert and make explicit the geometric criterion of Theorem 1. Let us fix a little notation. We let C be a curve of genus 2 over a number field k. Suppose that C admits an Humbert configuration $(Q, R; P_1, \ldots, P_6)$, say, and then choose coordinates $(X : Y : Z)$ on $\mathbb{P}^2$ so that the conic Q which is covered by C has equation

$$Y^2 = XZ.$$

Suppose that the branch points $P_1, \ldots, P_6$ are given by $P_i = (a_i^2 : a_i : 1)$.

Notice that there is only one conic R which is tangent to the five lines P_1P_2, P_2P_3, P_3P_4, P_4P_5, P_5P_1; we require that this conic should pass through P_6. In fact it is no difficult matter to write down the equation of the projective dual R^*. If we take coordinates $(l : m : n)$ on the projective dual $\mathbb{P}^{2*}$ so that R^* has an equation

$$al^2 + bm^2 + cn^2 + 2dmn + 2enl + 2flm = 0$$

then the coefficients are

$$\begin{aligned}
a &= a_1a_2^2a_5^2(a_4^2-a_3^2)+\ldots+a_5a_1^2a_4^2(a_3^2-a_2^2),\\
b &= a_1^2a_2a_5(a_3-a_4)+\ldots+a_5^2a_1a_4(a_2-a_3),\\
c &= a_1^2(a_3-a_4)+\ldots+a_5^2(a_2-a_3),\\
2d &= a_1^2(a_2+a_5)(a_3-a_4)+\ldots+a_5^2(a_1+a_4)(a_2-a_3),\\
2e &= a_1^2(a_2^2+a_5^2)(a_4^2-a_3^2)+\ldots+a_5^2(a_1^2+a_4^2)(a_3^2-a_2^2),\\
2f &= a_1^2[a_3a_4(a_2^2+a_5^2)+a_2a_5(a_3^2-a_4^2)]\\
&\qquad+\ldots+a_5^2[a_2a_3(a_1^2+a_4^2)+a_1a_4(a_2^2-a_3^2)],
\end{aligned}$$

where on each line the missing terms are produced by cycling the subscripts by the 5-cycle (1 2 3 4 5).

To obtain the condition that R passes through P_6 one may consider the case when $P_6=(1:0:0)$, when the condition is simply $bc=d^2$, and then generalize by making the substitution $a_i\mapsto 1/(a_i-a_6)$. We shall denote the resulting condition by $H(a_1,\ldots,a_6)$.

An important fact from our point of view is that, while the group of permutations of the a_i which fix R is the symmetry group of the pentagon $P_1P_2P_3P_4P_5$ (that is, $\mathrm{D}_{10}=\langle(1\ 2\ 3\ 4\ 5),(1\ 2)(3\ 4)\rangle$), the group of permutations in S_6 which fix H is rather larger. This subgroup is precisely the transitive copy of A_5 which is generated by (1 2 3 4 5) and (1 6)(2 5). We call this subgroup $\mathrm{A}_5^{\mathrm{tr}}$. A consequence of this is that for each choice of branch point P_i, there is some conic R_i which passes through P_i and is tangent to the pentagon formed by taking the other branch points in a specific order. (The equation above defines R_6.) Moreover, we can retrieve this ordering because we know that for each $i=1,\ldots,6$ the group of symmetries of the pentagon formed by the branch points other than P_i is just the intersection of $\mathrm{A}_5^{\mathrm{tr}}$ with the stabilizer in S_6 of P_i.

We are now in a position to verify the following, which makes life a little simpler later on.

LEMMA 1. *Let C be a curve of genus* 2 *which admits the Humbert configuration $(Q,R,\{P_i\})$. Then, after reordering the P_i, we may suppose that Q and R meet transversally in four points.*

P r o o f. Our proof is a straightforward, if rather tedious, calculation. For the purposes of the verification, we would recommend the use of a computer algebra package. As a point of notation, if p_1 and p_2 are multivariate polynomials we shall denote by $\mathrm{Res}(p_1,p_2;x)$ the resultant of p_1 and p_2 with respect to the variable x.

We may suppose up to isomorphism that Q has the equation $Y^2=XZ$, and that the branch points of $C\to Q$ are $P_1=(0:0:1)$, $P_2=(1:1:1)$, $P_3=(\lambda^2:\lambda:1)$, $P_4=(\mu^2:\mu:1)$, $P_5=(\nu^2:\nu:1)$ and $P_6=(1:0:0)$, for some λ, μ and ν such that 0, 1, λ, μ and ν are all distinct.

The condition that Q and R both pass through P_6 can be calculated as above, and gives a single condition $H(\lambda, \mu, \nu) = 0$, say. We can also determine the condition $D_1(\lambda, \mu, \nu)$ that Q and R meet in fewer than four points: D_1 is the discriminant (with respect to t) of the quartic equation satisfied by those points $(t^2 : t : 1)$ lying on R.

From the discussion above, we note that the curve C admits at least three further Humbert configurations $(Q, R_2; P_1, P_4, P_6, P_2, P_5, P_3)$, $(Q, R_3; P_1, P_2, P_5, P_6, P_3, P_4)$ and $(Q, R_4; P_4, P_2, P_3, P_1, P_6, P_5)$, say; let the condition that Q meets R_i in fewer than four points be $D_i(\lambda, \mu, \nu)$ for $i = 2, 3, 4$.

We define $p_1(\nu) = \mathrm{Res}(\mathrm{Res}(D_3, D_4; \lambda), D_2; \mu)$ (a polynomial of degree 64), and let $p_2(\nu) = \mathrm{Res}(\mathrm{Res}(H, D_1; \lambda), D_2; \mu)$ (which has degree 32). These polynomials are coprime, and so we conclude that at least one the conics R, R_2, R_3 and R_4 must meet Q in four distinct points. ∎

3. Description of the RM. Now we start from the configuration of Theorem 1 and construct an explicit embedding $j : \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)$. This is mainly useful because it allows us to give a criterion for the multiplication being rationally defined.

Let C be a curve of genus 2 which admits an Humbert configuration $(Q, R; \{P_i\})$, say. Let us fix a geometric isomorphism $\phi : Q \xrightarrow{\sim} \mathbb{P}^1$ such that $\phi(P_6) = \infty$. This gives an equation for C of the form

$$C: \quad Y^2 = f(X) = \prod_{i=1}^{5} (X - a_i), \tag{1}$$

where $a_i = \phi(P_i)$ for $i = 1, \ldots, 5$.

By Lemma 1, we may assume that Q and R meet transversally in four distinct points. Define E to be the incidence relation between Q and the projective dual R^*, that is,

$$E = \{(P, L) \in Q \times R^* \mid P \text{ lies on } L\}.$$

The curve E carries two natural involutions ι and ι', given by $\iota : (P, L) \mapsto (P', L)$, where P' is the residual point of intersection of L and R, and $\iota' : (P, L) \mapsto (P, L')$, where L' is the residual tangent line to R passing through P. It is proved in [7] that E is a nonsingular curve of genus 1. Up to a geometric isomorphism, we may replace E with the Jacobian of E, which is then an elliptic curve; moreover we may suppose that the zero of E covers the point P_6 on Q.

Referring again to [7], there is a point T on E such that the composition $\iota \circ \iota'$ is translation by T, and such that T has order 5. (Observe that this proves Poncelet's theorem; in this instance, given any point P on Q, there is a pentagon with one vertex at P, with every vertex a point of Q, and with every edge tangent to R.) In particular, if we let $\widetilde{P}_1$ be either of the

two points of E lying above P_1, then $\widetilde{P}_1 + (n-1)T$ lies above P_n for each $n = 1, \ldots, 5$.

Now, following Mestre [12], let x be the composition $x : E \to Q \xrightarrow{\phi} \mathbb{P}^1$ (so x is a function on E with double pole at 0), let $f : E \to E$ be the isogeny associated with the subgroup $\langle T \rangle$ and let u be the *abscissa equation*, that is, the function which makes the following square commute:

$$\begin{array}{ccc} E & \xrightarrow{f} & E \\ \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x} \\ \mathbb{P}^1 & \xrightarrow{u} & \mathbb{P}^1 \end{array}$$

Observe that $u(a) = u(b)$ when the line joining the points $\phi^{-1}(a)$ and $\phi^{-1}(b)$ is tangent to R (that is, when a and b are the x-coordinates of points of E whose difference is T). The poles of u are the x-coordinates of points of $\ker f$, so u has double poles at $x(T)$ and $x(2T)$, and no other poles.

Define the curve C' by the equation

$$C' : \quad Y^2 = u(X) - u(a_1).$$

Then C' is a double cover of $\mathbb{P}^1$; by our remarks in the last paragraph, this double cover is branched over $a_1, \ldots, a_5$ and ∞, and so C' is geometrically isomorphic to C. Indeed, if we write $\nu(x) = (x - x(T))(x - x(2T))$ then $(x', y') \mapsto (x', y'\nu(x'))$ defines an isomorphism $C' \xrightarrow{\sim} C$, because the defining equation for C' can be written as

$$C' : \quad Y^2 = \frac{\prod_{i=1}^{5}(X - a_i)}{(X - x(T))^2 (X - x(2T))^2}.$$

Now suppose (x, y) is a generic point of C. There are two tangents to R passing through $\phi^{-1}(x) \in Q$; label the residual points of intersection of these lines with Q as $\phi^{-1}(x_+)$ and $\phi^{-1}(x_-)$ such that if $x = x(P)$ for some $P \in E$ then $x_\pm = x(P \pm T)$. Note that $u(x_+) = u(x) = u(x_-)$ by our earlier remarks, and so $\left(x_\pm, y\frac{1}{\nu(x)}\right)$ both lie on C'. Thus $\left(x_+, y\frac{\nu(x_+)}{\nu(x)}\right)$ and $\left(x_-, y\frac{\nu(x_-)}{\nu(x)}\right)$ both lie on C.

Define a morphism θ from C to the Jacobian J by

$$\theta : (x, y) \mapsto \left[\left(x_+, y\frac{\nu(x_+)}{\nu(x)}\right) + \left(x_-, y\frac{\nu(x_-)}{\nu(x)}\right) - 2\infty\right], \tag{2}$$

where ∞ is the point of C above P_6, and $[D]$ denotes the class of a divisor D on C. Then θ extends by linearity to an endomorphism of $J = \mathrm{Jac}(C)$ since θ commutes with the hyperelliptic involution on C. Let us now prove that $\theta^2 + \theta - 1 = 0$ on J; then $j(\eta) = \theta + 1$ defines an embedding $j : \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)$ as required.

Let (x, y) be a point of C, and choose x_+ and x_- as in the definition of θ. Now there are two tangents to R which pass through $\phi^{-1}(x_+)$: one of these meets Q again at $\phi^{-1}(x)$; the other meets Q again at some new point, which we shall label $\phi^{-1}(x_{++})$. In a similar way, we define x_{--}. Then $\theta^2 + \theta - 1$ maps the divisor class $[(x, y) - \infty]$ to

$$\left[\left(x_{++}, y\frac{\nu(x_{++})}{\nu(x)}\right) + \left(x_+, y\frac{\nu(x_+)}{\nu(x)}\right) + (x, y) + \left(x_-, y\frac{\nu(x_-)}{\nu(x)}\right) + \left(x_{--}, y\frac{\nu(x_{--})}{\nu(x)}\right) - 5\infty\right]. \tag{3}$$

(Observe that, by Poncelet's theorem, the inverse images under ϕ of the points x_{++}, x_+, x, x_- and x_{--} form a pentagon with vertices on Q and edges tangent to R.)

Now consider the function $\nu(x)Y - yX$ on C. This has five zeros and has a five-fold pole at ∞; indeed, formula (3) above is the class of the divisor of zeros of this function. This establishes our claim that $\theta^2 + \theta - 1 = 0$.

We started this section by supposing that C admits an Humbert configuration. Of course, by Theorem 1, this is equivalent to assuming that there is an embedding $i : \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(J)^{\dagger=1}$. We now check that $i = j$.

We shall make use of the explicit description given by Cassels and Flynn [3, Chapter 3] of the Kummer surface K associated with C.

Fix a model for C in the form

$$C: \quad Y^2 = f(X) = \prod_{i=1}^{6}(X - a_i). \tag{4}$$

Now choose a point of J: this is represented by a point $\{(x, y), (u, v)\}$, say, on $C^{(2)}$. Then, from [3, equation 3.1.3], the image of this point on the Kummer surface K is $(1 : x + u : xu : \beta_0(x, u, y, v))$, where the exact form of β_0 will not worry us.

The node on K under the zero of J is at $N_0 = (0 : 0 : 0 : 1)$. From [3, equation 3.1.9], the image of the tangent cone at N_0 under projection through N_0 into the plane $(l : m : n : 0)$ has equation $l^2 = 4mn$. Considering the proof of Theorem 1, this is the dual of Q. Hence we identify the plane $(l : m : n : 0)$ with $(\mathbb{P}^2)^*$, and then Q has equation $Y^2 = XZ$.

We then see that the branch locus of the double cover $C \to Q$ is the set of points $\{(a_i^2 : -a_i : 1) \mid i = 1, \ldots, 6\}$ (see [3, Chapter 3, Section 7]). Thus the image of a point (x, y) under $C \to Q$ is $(x^2 : -x : 1)$. Further, the image of $\{(x, y), (u, v)\}$ under the composition $C^{(2)} \to J \to K \to (\mathbb{P}^2)^*$ is the point representing the chord joining $(x^2 : -x : 1)$ and $(u^2 : -u : 1)$.

Now let $\varepsilon = i(\eta - 1)$ and let $\theta = j(\eta - 1)$ (as defined in equation (2)). Fix a symmetric embedding $C \hookrightarrow J$, and write D for the image of this map (a symmetric theta divisor). The image of $\varepsilon^* D$ under $J \to K \to (\mathbb{P}^2)^*$ is

the conic R^*. By the definition of θ, and by the previous paragraph, a pair $\{(x,y),(u,v)\}$ represents a point of θ^*D precisely when the chord joining $(x^2 : -x : 1)$ and $(u^2 : -u : 1)$ is tangent to R, that is, when the projection of this point to $(\mathbb{P}^2)^*$ lies on R^*. Thus ε^*D and θ^*D have the same projection to $(\mathbb{P}^2)^*$.

Since R^* is birational to its preimage on K, and since each of ε^*D and θ^*D is fixed by multiplication by (-1), we can conclude that $\varepsilon^*D = \theta^*D$. It follows that ε and θ differ only by an automorphism of C.

Bolza [1] has classified the possibilities for the automorphism group of a curve C of genus 2. The reduced automorphism group (that is, $\mathrm{Aut}(C)$ modulo the hyperelliptic involution) falls into one of three cases:

(i) the trivial group (this is the generic case);
(ii) cyclic of order 5 (when $\mathrm{Jac}(C)$ has CM by a fifth root of unity); or
(iii) a group of even order.

In the first two of these cases we must have $\varepsilon = \theta$, since ε and θ both satisfy the equation $T^2 + T - 1 = 0$. Suppose, then, that the third case holds.

Since C has a nonhyperelliptic involution, it has a nontrivial map to an elliptic curve; hence $\mathrm{Jac}(C)$ is isogenous to a product of elliptic curves. Indeed, to have RM, $\mathrm{Jac}(C)$ must be isogenous to the square of some elliptic curve E. There is, then, an isomorphism $\mathrm{Jac}(C) \otimes \mathbb{Q} \cong \mathrm{M}_2(\mathrm{End}(E) \otimes \mathbb{Q})$ such that the Rosati involution becomes $A^\dagger = \overline{A}^{\mathrm{t}}$ (where the overbar denotes complex conjugation).

We know that $\theta = \varepsilon u$ for some $u \in \mathrm{Aut}(C)$, and that $\varepsilon^\dagger = \varepsilon$. Since θ and ε both satisfy $T^2 + T - 1 = 0$, we also have $\det u = 1$ and $\mathrm{Tr}(\theta) = \mathrm{Tr}(\varepsilon)$. Moreover, regarding u as an endomorphism of $\mathrm{Jac}(C)$, a straightforward calculation gives $u^\dagger = u^{-1}$. These equations together are enough to force $u = 1$, that is, $\theta = \varepsilon$.

We now turn to the promised criterion for the RM to be rationally defined. Suppose the curve C is defined over a number field k, and take a model of the form (4) over k.

THEOREM 2. *The embedding j has image contained in $\mathrm{End}_k(J)$ if and only if $\mathrm{Gal}(k(a_1,\dots,a_6)/k)$ is contained in $\mathrm{A}_5^{\mathrm{tr}}$ up to S_6-conjugacy.*

Proof. Let H_i denote the stabilizer in S_6 of a_i $(i = 1,\dots,6)$. A permutation $\sigma \in H_i$ acts on the set of branch points other than P_i and hence induces a new map ${}^\sigma\theta$ as in (2); then ${}^\sigma\theta = \theta$ exactly when σ preserves the conic R_i. Hence, setting $G = \{\sigma \in \mathrm{S}_6 \mid {}^\sigma\theta = \theta\}$, we have $G \cap H_i = \mathrm{A}_5^{\mathrm{tr}} \cap H_i$ for each i. This forces $G = \mathrm{A}_5^{\mathrm{tr}}$. ∎

4. A family of curves from Humbert's criterion. In this section, we use Humbert's criterion (Theorem 1) to produce a family of curves which

parametrizes all curves of genus 2 defined over $\mathbb{Q}$ with maximal RM by $\mathbb{Q}(\sqrt{5})$ and a rational Weierstrass point. We note that families of curves with maximal RM over $\mathbb{Q}(\sqrt{5})$ already exist in the literature—see [12] and [2]—but that our approach is rather more direct.

Suppose that C is a curve of genus 2 defined over a number field k, with maximal RM by $\mathbb{Q}(\sqrt{5})$. Note that by our description of the RM in the previous section, if $(Q, R; \{P_i\})$ is an Humbert configuration for C such that the map $C \twoheadrightarrow Q$ is defined over k, then the field of definition of the conic R is the field of definition of the RM. We shall suppose further that this is contained in k, and that C has a k-rational Weierstrass point.

In this case, we may choose an Humbert configuration $(Q, R; \{P_i\})$ for C such that Q has equation

$$Q: \quad Y^2 = XZ$$

and the point $P_6 = (1 : 0 : 0)$.

We shall make one further supposition, namely that R meets Q transversally at P_6. Let us show that we may ensure this by supposing that k does not contain $\mathbb{Q}(\sqrt{5})$.

If R meets Q tangentially at P_6 then we may choose an equation for the dual conic R^* in the form

$$R^*: \quad al^2 + bm^2 + 2enl + 2flm = 0$$

(where $(l : m : n)$ are coordinates on $(\mathbb{P}^2)^*$); there will be a further condition on the coefficients a, b, e and f ensuring that there is a pentagon whose vertices lie on Q and whose edges are tangent to R. Indeed, we note that by Poncelet's theorem [7], for every point P on Q there is a pentagon with a vertex at P, all of whose vertices lie on Q, and all of whose edges are tangent to R.

Let $(1 : t : t^2)$ be an arbitrary point of Q which is not a point of intersection with R, let $(1 : u_1 : u_1^2)$ and $(1 : u_2 : u_2^2)$ be the residual points of intersection with Q of the two tangents to R which pass through t, and then, for each $i = 1, 2$, let $(1 : s_i : s_i^2)$ be the residual point of intersection with Q of the other tangent to R which passes through $(1 : u_i : u_i^2)$. In this way we obtain a pentagon with vertices $(1 : t : t^2)$, $(1 : u_1 : u_1^2)$, $(1 : s_1 : s_1^2)$, $(1 : s_2 : s_2^2)$ and $(1 : u_2 : u_2^2)$ on Q and edges tangent to R. Then u_1 and u_2 are the roots of a quadratic equation whose coefficients are rational functions in t, a, b, e and f; the numbers s_1 and s_2 are roots of a similar equation. After some algebra, one checks that the condition on a, b, e and f (which is the condition that the chord joining $(1 : s_1 : s_1^2)$ and $(1 : s_2 : s_2^2)$ should be tangent to R) is

$$b^2 + 6be + 4e^2 = 0.$$

Thus, in particular, the field of definition of R contains $\mathbb{Q}(\sqrt{5})$.

To sum up: we suppose that k does not contain $\mathbb{Q}(\sqrt{5})$, and that C is a curve over k with maximal RM by $\mathbb{Q}(\sqrt{5})$ defined over k, and a k-rational Weierstrass point.

Under these hypotheses, we may still choose Q to have the equation $Y^2 = XZ$ and the point P_6 to be $(1:0:0)$; the conics Q and R now meet transversally at P_6. The pentagon with a vertex at P_6 which is inscribed to Q and tangent to R (as given by Poncelet's theorem) will have two repeated vertices, and one of these must lie on a line which is a mutual tangent to Q and R. We may then write the equation of R^* in the form

$$R^*: \quad (m+\lambda n)^2 + 2\mu ln + \frac{1}{\lambda} lm = 0,$$

where λ and μ are suitable elements of k.

Suppose that the point P_1 is $P_1 = (1 : \lambda t : \lambda^2 t^2) \in Q$, and write $P_2 = (1 : \lambda u_1 : \lambda^2 u_1^2)$, $P_3 = (1 : \lambda s_1 : \lambda^2 s_1^2)$, $P_4 = (1 : \lambda s_2 : \lambda^2 s_2^2)$ and $P_5 = (1 : \lambda u_2 : \lambda^2 u_2^2)$. Then C has an equation

$$Y^2 = X(X-t)(X^2 - [u_1+u_2]X + u_1u_2)(X^2 - [s_1+s_2]X + s_1s_2)$$

over $\overline{k}$. One may calculate that u_1 and u_2 satisfy

$$u_1 + u_2 = \frac{2 - 2\mu t - 2t + t^2}{1-t} \quad \text{and} \quad u_1u_2 = 1 - t;$$

s_1 and s_2 satisfy

$$s_1 + s_2 = \frac{2\mu - t}{1-t} \quad \text{and} \quad s_1 s_2 = \frac{2\mu - 1}{t(1-t)}.$$

We now make the following choice of parameters $A, B \in k$:

$$A = 1 - 2\mu, \qquad B = u_1u_2 + s_1s_2 + (u_1+u_2)(s_1+s_2) + t(u_1+u_2+s_1+s_2).$$

Then C has an equation of the following shape:

$$(5) \qquad C_{AB}: \quad Y^2 = X[X^5 + (A-3)X^4 + BX^3 + (5 - 3A + A^2 - 2B)X^2 + (A+B-3)X + A].$$

Thus we have the following proposition.

PROPOSITION 1. *For each choice of $A, B \in k$ such that C_{AB} is nonsingular, the curve C_{AB} has maximal RM by $\mathbb{Q}(\sqrt{5})$ defined over k. Conversely, when k does not contain $\mathbb{Q}(\sqrt{5})$, every nonsingular curve X/k which has a k-rational Weierstrass point and maximal RM by $\mathbb{Q}(\sqrt{5})$ defined over k is isomorphic over k to some C_{AB}.*

We observe that there are curves defined over fields containing $\mathbb{Q}(\sqrt{5})$ which have rationally defined maximal RM by $\mathbb{Q}(\sqrt{5})$ and a rational Weierstrass point, but which do not appear in the family C_{AB}. An example is the curve

$$Y^2 = X^5 - 2,$$

considered as a curve over $\mathbb{Q}(\sqrt{5})$. Note that, however, this is isomorphic over $\overline{\mathbb{Q}}$ to the curve C_{AB} when $A = \frac{1}{2}(1+\sqrt{5})$ and $B = \frac{1}{2}(5-3\sqrt{5})$.

5. The explicit moduli. Before proceeding, we shall introduce some useful shorthand. Suppose that $x_1, \ldots, x_n$ are independent (commuting) variables. Then we shall denote by $\sigma_i(x_1, \ldots, x_n)$, or simply $\sigma_i(x)$ when the range of indices is clear from the context, the ith elementary symmetric function in $x_1, \ldots, x_n$, and by $\tau_i(x)$ the ith power sum $\tau_i(x) = \sum_j x_j^i$. If $f(T)$ is a polynomial in one variable, then we use the shorthand notation $\sigma_i(f(x)) = \sigma_i(f(x_1), \ldots, f(x_n))$, and similarly for $\tau_i(f(x))$.

We shall start from the description of the (coarse) moduli space for curves of genus 2 with an ordering of the Weierstrass points given by considering the space $P_1^6 = (\mathbb{P}^1)^6/\mathrm{PGL}_2$. This space is studied in detail in [4] (see also [15]); in particular the following process constructs a convenient model for P_1^6, namely the Segre cubic $Z \subset \mathbb{P}^5$, which is given by the equations

$$\sum_{i=1}^{6} z_i = \sum_{i=1}^{6} z_i^3 = 0$$

(that is, $\tau_1(z) = \tau_3(z) = 0$).

Any given point of P_1^6 is represented by an ordered sextuple of points $(a_i : b_i) \in \mathbb{P}^1$ $(i = 1, \ldots, 6)$. Write (ij) for the cross-ratio $(a_i b_j - a_j b_i)$, and form the following five numbers:

$$t_1 = (12)(34)(56), \quad t_2 = (13)(24)(56), \quad t_3 = (12)(35)(46),$$
$$t_4 = (13)(25)(46), \quad t_5 = (14)(25)(36).$$

We then make the following linear change of variables to define $P_1^6 \xrightarrow{\sim} Z$:

$$\begin{aligned}
z_1 &= 2t_1 - t_2 - t_3 + t_4 + t_5,\\
z_2 &= -2t_1 + t_2 + t_3 + t_4 - t_5,\\
z_3 &= -t_2 + t_3 - t_4 + t_5,\\
z_4 &= t_2 + t_3 - t_4 - t_5,\\
z_5 &= -t_2 - t_3 + t_4 - t_5,\\
z_6 &= t_2 - t_3 - t_4 + t_5.
\end{aligned}$$

The z_i are cubic forms in the a_i and also in the b_i; each term is of the form $\pm a_{i_1} a_{i_2} a_{i_3} b_{j_1} b_{j_2} b_{j_3}$, where $\{i_1, i_2, i_3, j_1, j_2, j_3\} = \{1, 2, 3, 4, 5, 6\}$.

Working with these explicit forms, one can verify that any permutation $\sigma \in \mathrm{S}_6$ of the points $(a_i : b_i)$ corresponds to the permutation σ^{out} of the coordinates z_i, where $\mathsf{out} : \mathrm{S}_6 \xrightarrow{\sim} \mathrm{S}_6$ is the outer automorphism which maps the close transpositions as follows:

$$(1\ 2) \mapsto (1\ 4)(2\ 3)(5\ 6),$$

$$(2\ 3) \mapsto (1\ 5)(2\ 6)(3\ 4),$$
$$(3\ 4) \mapsto (1\ 4)(2\ 5)(3\ 6),$$
$$(4\ 5) \mapsto (1\ 5)(2\ 3)(4\ 6),$$
$$(5\ 6) \mapsto (1\ 4)(2\ 6)(3\ 5).$$

(It seems at first sight that there is a sign change for odd permutations but, of course, we are free to rescale the z_i.) This means that the permutation action on Z corresponds to choosing different level 2 structures on the same isomorphism class of abelian surface.

Now we turn to curves with RM by $\mathbb{Q}(\sqrt{5})$. It is proved in [5] that the variety $Y \subset \mathbb{P}^4$ given by

$$\sum_{i=1}^{5} y_i = \sum_{i=1}^{5} y_i^3 = 0$$

is a moduli space for principally polarized abelian surfaces A with level 2 structure and an embedding $i : \mathbb{Z}[\eta] \hookrightarrow \mathrm{End}(A)^{\dagger=1}$.

It is then proved in [15, Lemma 2.4] that the map $j : Y \to Z$ induced by their moduli interpretations is given, up to the permutation action of S_6 on Z, by

$$(y_i) \mapsto (4y_1^2 - \tau_2(y) : 4y_2^2 - \tau_2(y) : 4y_3^2 - \tau_2(y) : 4y_4^2 - \tau_2(y) : 4y_5^2 - \tau_2(y) : \tau_2(y)).$$

One can then verify that the image $j(Y) \subset Z$ is contained in the hypersurface $H \subset \mathbb{P}^5$ with equation

$$12z_6^4 - 4\tau_2(z)z_6^2 + \tau_2(z)^2 - 4\tau_4(z) = 0.$$

Indeed, we claim that $j(Y) = Z \cap H$. Note that a hyperplane in $\mathbb{P}^5$ pulls back under j to a diagonal quadric in $\mathbb{P}^4$, and that every diagonal quadric in $\mathbb{P}^4$ arises in this fashion. The intersection of Y with two diagonal quadrics is generically 12 points, and so our claim is justified since the degrees of $j(Y)$ and $Z \cap H$ are equal.

Thus, if we write $s_i = \sigma_i(z_1, z_2, z_3, z_4, z_5)$ (so that $\sigma_i(z) = z_6 s_{i-1} + s_i$), then $j(Y)$ is given by the equations

$$s_1 + z_6 = 0, \quad s_3 = s_1 s_2 \quad \text{and} \quad s_2^2 = 4s_4. \tag{6}$$

From this, we can choose (z_6, s_2, σ_5) as moduli for curves of genus 2 with maximal RM by $\mathbb{Q}(\sqrt{5})$. (We disregard the ordering of the coordinates z_i since this corresponds to the choice of ordering of the Weierstrass points.)

Suppose that C is a curve of genus 2 defined over a number field k, and that C has maximal RM by $\mathbb{Q}(\sqrt{5})$, also defined over k. Then, for any corresponding point $z \in Z$ of the moduli space we may write $z = (z_1 : \ldots : z_6)$ such that $\{z_1, \ldots, z_6\}$ is defined over k (as a set). Moreover, if k' is the field obtained by adjoining to k all coordinates of Weierstrass points on C,

then we have that $\mathrm{Gal}(k(z)/k) = \mathrm{Gal}(k'/k)^{\mathsf{out}}$ in S_6. From Theorem 2, we have $\mathrm{Gal}(k'/k) \subseteq \mathrm{A}_5^{\mathrm{tr}}$ up to S_6-conjugacy, and thus we find that we may choose $z_1, \ldots, z_6$ such that $z_6 \in k$ and $\mathrm{Gal}(k(z)/k)$ is even.

Write Δ for the discriminant of the polynomial $\phi(T) := \prod_{i=1}^{5}(T - z_i)$. Then we know from the previous paragraph that curves of genus 2 over k with RM by $\mathbb{Q}(\sqrt{5})$ defined over k are given by certain choices of $z_6, s_2, \sigma_5 \in k$ such that Δ is a square in k. (Sadly, not every such choice gives such a curve; we shall present an example later.) We can parametrize such triples.

The discriminant Δ is given in terms of z_6, s_2 and σ_5 by

$$5T_4^2 = T_3^2 + T_1^3 T_2^2, \tag{7}$$

where we write

$$\begin{aligned} T_1 &= 2(5s_2 - 8z_6^2), \\ T_2 &= 5s_2 + 2z_6^2, \\ T_3 &= 3125\sigma_5 - 128z_6^5 - 200z_6^3 s_2 - 500z_6 s_2^2, \\ T_4^2 &= 625\Delta/\sigma_5^2. \end{aligned} \tag{8}$$

The variety T (in weighted projective space) whose equation is given in (7) is a rational variety. Note that the formulae in (8) do not give a 1-1 correspondence between points of T and the triples (z_6, s_2, σ_5) in which we are interested, but we can get round this by choosing a parametrization of T carefully. To be precise, let us take three parameters

$$u_1 = \frac{2}{5}z_6, \quad u_2 = \frac{T_4}{10T_1T_2} \quad \text{and} \quad u_3 = \frac{T_3}{10T_1T_2}.$$

This gives a parametrization of T, and also parametrizes the triples (z_6, s_2, σ_5) such that Δ is a square. Explicitly, we have

$$\begin{aligned} 2z_6 &= 5u_1, \\ s_2 &= 10(u_1^2 + 5u_2^2 - u_3^2), \\ \sigma_5 &= 2(27u_1^5 + 225u_1^3u_2^2 - 45u_1^3u_3^2 + 50u_1^2u_2^2u_3 - 10u_1^2u_3^3 \\ &\qquad + 500u_1u_2^4 - 200u_1u_2^2u_3^2 + 20u_1u_3^4 + 200u_2^4u_3 - 80u_2^2u_3^3 + 8u_3^5). \end{aligned}$$

6. Relations with other invariants. In this section we give the relations between the moduli introduced in the previous section, and those defined by Igusa [10], as well as between those introduced here, and those defined by Clebsch (for definitions see [13]).

Given $((a_1 : b_1), \ldots, (a_6 : b_6)) \in (\mathbb{P}^1)^6$, Igusa's invariants are

$$I_2 = \sum_{15\,\text{terms}} (12)^2(34)^2(56)^2,$$

$$I_4 = \sum_{10\text{ terms}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2,$$

$$I_6 = \sum_{60\text{ terms}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2,$$

$$I_{10} = \prod_{i<j}(ij)^2,$$

where the symbols (ij) denote cross-ratios as before, and each sum is over every symmetric conjugate of the summand.

The relations between (I_2, I_4, I_6, I_{10}) and $(z_1, \ldots, z_6)$ are

$$\begin{aligned} I_2 &= \tau_2(z), \\ 32I_4 &= 6\tau_4(z) - \tau_2(z)^2, \\ 64I_6 &= -6\tau_6(z) + 7\tau_2(z)\tau_4(z) - \tau_2(z)^3, \\ 2^{10}I_{10} &= \sigma_5(z)^2. \end{aligned}$$

When $(z_1 : \ldots : z_6) \in j(Y)$, we can rewrite these as

$$\begin{aligned} I_2 &= -2s_2 + 2z_6^2, \\ 16I_4 &= (s_2 + 2z_6^2)^2, \\ 64I_6 &= 36z_6\sigma_5 - 16I_4(3s_2 - 2z_6^2), \\ 2^{10}I_{10} &= \sigma_5^2. \end{aligned}$$

Clebsch's invariants (as defined in [13]) can be written in terms of the invariants introduced here as follows:

$$\begin{aligned} 2^2 3 \cdot 5A &= s_2 - z_6^2, \\ 2^5 3^2 5^4 B &= 7s_2^2 - 4s_2 z_6^2 + 12z_6^4, \\ 2^8 3^2 5^6 C &= -3s_2^3 + 100\sigma_5 z_6 - 26s_2^2 z_6^2 - 4s_2 z_6^4 + 8z_6^6, \\ 2^{11} 3^6 5^{10} D &= 2s_2^5 - 3125\sigma_5^2 + 1900s_2^2\sigma_5 z_6 - 485s_2^4 z_6^2 - 6800s_2\sigma_5 z_6^3 \\ &\quad + 1520s_2^3 z_6^4 + 400\sigma_5 z_6^5 - 120s_2^2 z_6^6 + 160s_2 z_6^8 + 48z_6^{10}. \end{aligned} \tag{9}$$

7. Finding equations for curves. There is a method for constructing an equation for a curve of genus 2 from its invariants described by Mestre [13], which we review here, giving a few examples.

Suppose that C is a curve with maximal RM by $\mathbb{Q}(\sqrt{5})$, with invariants (z_6, s_2, σ_5) and suppose that C has no nontrivial automorphisms. (As remarked earlier, this is the generic case.) Then Mestre gives explicit equations for a plane conic L and plane cubic M such that C is a double cover of L branched exactly over $L \cap M$. Further, if $z_6, s_2, \sigma_5 \in k$, then C has a model over k exactly when $L(k) \neq \emptyset$ [13, Lemme 1].

For convenience we reproduce the formulae from [13] which define L and M. These are given in terms of Clebsch's invariants (see equations (9)).

The conic L has equation $\sum_{i,j=1}^{3} A_{ij}x_ix_j$, where

$$\begin{aligned} A_{11} &= 2C + \tfrac{1}{3}AB,\\ A_{12} &= \tfrac{2}{3}(B^2 + AC),\\ A_{13} &= A_{22} = D,\\ A_{23} &= \tfrac{1}{3}B(B^2 + AC) + \tfrac{1}{3}C\big(2C + \tfrac{1}{3}AB\big),\\ A_{33} &= \tfrac{1}{2}BD + \tfrac{2}{9}C(B^2 + AC). \end{aligned} \tag{10}$$

The cubic M has equation $\sum_{i,j,k=1}^{3} a_{ijk}x_ix_jx_k$, where

$$\begin{aligned} 36a_{111} &= 8(A^2C - 6BC + 9D),\\ 36a_{112} &= 4(2B^3 + 4ABC + 12C^2 + 3AD),\\ 36a_{113} &= 4\big(AB^3 + \tfrac{4}{3}A^2BC + 4B^2C + 6AC^2 + 3BD\big),\\ 36a_{122} &= 36a_{113},\\ 36a_{123} &= 2\big(2B^4 + 4AB^2C + \tfrac{4}{3}A^2C^2 + 4BC^2 + 3ABD + 12CD\big),\\ 36a_{133} &= 2\big(AB^4 + \tfrac{4}{3}A^2B^2C + \tfrac{16}{3}B^3C + \tfrac{26}{3}ABC^2 + 8C^3\\ &\quad + 3B^2D + 2ACD\big),\\ 36a_{222} &= 4\big(3B^4 + 6AB^2C + \tfrac{8}{3}A^2C^2 + 2BC^2 - 3CD\big),\\ 36a_{223} &= 2\big(-\tfrac{2}{3}B^3C - \tfrac{4}{3}ABC^2 - 4C^3 + 9B^2D + 8ACD\big),\\ 36a_{233} &= 2\big(B^5 + 2AB^3C + \tfrac{8}{9}A^2BC^2 + \tfrac{2}{3}B^2C^2 - BCD + 9D^2\big),\\ 36a_{333} &= -2B^4C - 4AB^2C^2 - \tfrac{16}{9}A^2C^3 - \tfrac{4}{3}BC^3 + 9B^3D\\ &\quad + 12ABCD + 20C^2D. \end{aligned} \tag{11}$$

We note that Mestre also gives an invariant R such that the discriminant of L is $2R^2$. In our case, R is a square multiple of the discriminant Δ defined in equation (7). Explicitly,

$$2^{36}3^{18}5^{20} \cdot R = (4z_6^5 + 4z_6^3s_2 + z_6s_2^2 - 2\sigma_5)^2\Delta.$$

Also, C has nontrivial automorphisms exactly when either $A = B = C = 0$ or $R = 0$ [13, remarque 1]. The first of these conditions translates to $z_6 = s_2 = 0$; this point on the moduli space corresponds to the isomorphism class of the curve $y^2 = x^5 + 1$, and here the RM by $\mathbb{Q}(\sqrt{5})$ is never defined over $\mathbb{Q}$ (the discriminant Δ is never a square). There are, however, several curves for which $R = 0$; these are curves such that $\mathrm{Aut}(C)$ contains an involution and, as remarked earlier, the Jacobian of each of these curves is isogenous to the square of some elliptic curve.

We finish with two examples to illustrate this method and a short table of results: Wang [16] has determined all the principally polarized 2-dimensional factors of $J_0(N)$ for $N < 200$, and has, in each case, given invariants for

a curve whose Jacobian is isogenous to the given abelian surface; we list equations for these curves, calculated as described here.

EXAMPLE 1. As has been remarked before, not all of the rational choices for (z_6, s_2, σ_5) which make Δ a square actually correspond to a curve with a model over $\mathbb{Q}$. One example where the obstruction is nontrivial is provided by taking $z_6 = 7/2$, $s_2 = 8$ and $\sigma_5 = 14$. In this case, the invariants A_{ij} are:

$$A_{11} = \frac{-1655981}{2592000000}, \qquad A_{12} = \frac{124837043}{1555200000000},$$
$$A_{13} = A_{22} = \frac{6150111571}{933120000000000}, \qquad A_{23} = \frac{255358687187}{559872000000000000},$$
$$A_{33} = \frac{9642570072739}{335923200000000000000}.$$

We can remove every square factor from the discriminant of L by an integral transformation as follows. If p is a prime such that p^2 divides the discriminant of L, then we can always transform the matrix for L so that it has the following shape modulo p:

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix} \pmod{p}.$$

If p^2 divides the top left entry then we can scale the relevant variable by $1/p$ and remove a factor of p^2 from the discriminant. Failing that, p divides the determinant of the bottom right minor and so we can transform L so that p divides every entry in the matrix except the bottom right entry. Then we may scale the corresponding variable by p and clear a common factor of p, thus removing a factor of p from the discriminant.

Once this has been done, we may imitate the method of Gaussian reduction for positive definite forms, and thereby reduce the size of the coefficients.

Following these procedures, the equation for L may be reduced to

$$x_1^2 - 5x_2^2 - 26x_3^2 - 2x_2x_3 = 0.$$

Now it is a routine matter to check that $L(\mathbb{Q}) = \emptyset$ since this new equation has discriminant $3 \cdot 43$ but has no 3-adic points and no 43-adic points.

EXAMPLE 2. For this example, we start from $z_6 = 5/2$, $s_2 = 18$ and $\sigma_5 = 206$. This isomorphism class has a Jacobian which is a simple factor of $J_0(103)$ and appears in Wang's tables [16].

In this case, Igusa's invariants are:

$$I_2 = \frac{-47}{2}, \quad I_4 = \frac{61^2}{2^6}, \quad I_6 = \frac{-11 \cdot 14593}{2^9} \quad \text{and} \quad I_{10} = \frac{103^2}{2^8};$$

the invariants A_{ij} are:

$$A_{11} = \frac{-219743}{864000000}, \qquad A_{12} = \frac{19108301}{518400000000},$$
$$A_{13} = A_{22} = \frac{-3718418807}{311040000000000}, \qquad A_{23} = \frac{52268246549}{186624000000000000},$$
$$A_{33} = \frac{-9248523360143}{111974400000000000000}.$$

By the methods of the previous example, the equation for L can be reduced to

$$8x_2^2 + 11x_3^2 + 2x_1x_2 + 2x_1x_3 + 4x_2x_3 = 0;$$

after the same change of coordinates, the equation for M becomes

$$1375x_1^3 + 13650x_1^2x_2 + 18150x_1^2x_3 + 1800x_1x_2^2 + 162900x_1x_2x_3 + 44100x_1x_3^2 - 8072x_2^3 + 89544x_2^2x_3 + 340104x_2x_3^2 + 39988x_3^3 = 0.$$

The conic L has an obvious $\mathbb{Q}$-point, namely $(1 : 0 : 0)$. Projecting through this point, the images of $L \cap M$ are the roots of the sextic polynomial

$$34112x^6 - 2688x^5 - 65120x^4 + 118640x^3 - 29420x^2 + 30372x + 34877;$$

scaling x by a factor of 2 gives the polynomial

$$f(x) = 533x^6 - 84x^5 - 4070x^4 + 14830x^3 - 7355x^2 + 15186x + 34877.$$

Now the invariants for the model we have here are

$$I_2 = -2^3 5^{10} 47, \quad I_4 = 2^2 5^{20} 61^2, \quad I_6 = -2^3 5^{30} 11 \cdot 14593, \quad I_{10} = 2^{12} 5^{50} 103^2.$$

Comparing these with the ones we started with, it is at least clear that we have a curve from the correct $\overline{\mathbb{Q}}$-isomorphism class. However, we should prefer to find an equation $y^2 = g(x)$ such that the odd part of the discriminant of g is 103^2; then the conductor of this curve would have no odd factors other than 103. Note that the invariants (z_6, s_2, σ_5) determine only the $\overline{\mathbb{Q}}$-isomorphism class of the curve, whereas the conductor varies with the $\mathbb{Q}$-isomorphism class.

In this case, we might consider a twist defined over $\mathbb{Q}(\sqrt{5})$. Specifically, consider the curve $y^2 = 5f(x)$. The factor of 5^{60} in the discriminant of the right-hand side can be removed by a linear transformation in x, and suitable re-scaling of y. Specifically, we can transform to the equation $y^2 = g(x)$, where

$$\begin{aligned} g(x) &= 5^{-11} f(25x + 18) \\ &= 2665x^6 + 11496x^5 + 20630x^4 + 19718x^3 + 10589x^2 + 3030x + 361. \end{aligned}$$

We note that the discriminant of g is $2^{12}103^2$ and that the odd part of the conductor of this curve is 103^2.

There is now one more technique we use to reduce the size of the coefficients. Let us define the *size* of a polynomial to be the sum of the squares of the coefficients. Now, given an equation $y^2 = g(x)$, we can transform by a linear change in the x-coordinate to ensure that the new coefficient of x^5 is less than 6 times the coefficient of x^6 in modulus. Very often this will reduce the size of the polynomial on the right-hand side as well. Then we are free to reverse the order of the coefficients on the right-hand side (that is, to make the change of coordinates $(x, y) \mapsto (1/x, y/x^3)$) and repeat this process for as long as the size of the right-hand side continues to decrease.

For the equation $y^2 = g(x)$ above, we find that we can transform to

$$y^2 = (4x-1)^6 g\left(\frac{1-3x}{4x-1}\right) = x^6 + 6x^5 - 19x^4 + 22x^3 - 10x^2 + 1.$$

8. Principally polarized factors of $J_0(N)$ with $\sqrt{5}$-multiplication. Wang [16] has determined the 2-dimensional factors of $J_0(N)$ for $N < 200$ and, in the case where the factor is principally polarized, has calculated values of Igusa's invariants which give a curve whose Jacobian is isogenous to the given factor of $J_0(N)$. In the table, N is the conductor, and z_6, s_2, σ_5 are the invariants defined above. Equations for these curves were found using the methods outlined in the examples at the end of the previous section; these are given by taking $y^2 = f(x)$, where f is as tabulated.

N	$2z_6$	$\frac{1}{2}s_2$	$\frac{1}{2}\sigma_5$	$f(x)$
23	15	46	23^3	$x^6 + 2x^5 - 23x^4 + 50x^3 - 58x^2 + 32x - 11$
31	23	$-2 \cdot 31$	-31^2	$x^6 - 2x^5 - 81x^4 + 468x^3 - 689x^2 + 46x - 447$
67	1	9	67	$x^6 + 8x^5 - 18x^4 + 14x^3 - 3x^2 - 2x + 1$
73	5	9	-73	$x^6 - 2x^5 - 3x^4 + 6x^3 + 6x^2 - 16x + 9$
87	5	-6	$3^2 29$	$-x^6 + 2x^4 + 6x^3 + 11x^2 + 6x + 3$
93	9	13	$3^2 31$	$x^6 - 6x^5 + 5x^4 + 6x^3 + 2x^2 - 1$
103	5	9	103	$x^6 + 6x^5 - 19x^4 + 22x^3 - 10x^2 + 1$
107	5	-6	107	$x^6 + 10x^5 - 371x^4 + 3118x^3 - 12010x^2 + 22456x - 16575$
115	1	-3	$5^2 23$	$-x^6 + 6x^5 - 5x^4 + 10x^3 - 2x^2 - 1$
125	5	0	5^3	$3x^6 + 4x^5 - 20x^4 - 80x^3 - 160x^2 - 128x - 64$
133	83	-1722	$-7^2 19$	$-7x^6 - 98x^5 - 409x^4 - 204x^3 + 1111x^2 - 722x + 137$
133	7	9	$7 \cdot 19$	$x^6 - 8x^5 + 10x^4 - 6x^3 + 5x^2 - 2x + 1$
161	7	30	$7^2 23$	$5x^6 - 6x^5 - 37x^4 - 36x^3 + 11x^2 + 42x + 85$
167	9	2	167	$-x^6 + 2x^5 + 3x^4 - 14x^3 + 22x^2 - 16x + 7$
175	1	-14	$5^2 7^2$	$-17x^6 + 26x^5 + 155x^4 - 570x^3 + 770x^2 - 464x + 247$
177	3	4	$3 \cdot 59$	$-3x^6 + 56x^4 + 176x^3 + 272x^2 + 192x + 64$
177	17	684	$-3^2 5^6 59$	$3x^6 - 12x^5 - 10x^4 + 14x^3 - x^2 - 6x + 63$
188	2	15	$2^4 47$	$x^5 + 34x^4 + 463x^3 + 3158x^2 + 10792x + 14785$
191	7	12	191	$x^6 - 6x^5 + 5x^4 + 2x^3 + 2x^2 + 1$

References

[1] O. Bolza, *On binary sextics with linear transformations into themselves*, Amer. J. Math. 10 (1888), 47–70.

[2] A. Brumer, *The rank of* $J_0(N)$, Astérisque 228 (1995), 41–68.

[3] J. W. S. Cassels and E. V. Flynn, *Prologomena to a Middlebrow Theory of Curves of Genus* 2, London Math. Soc. Lecture Note Ser. 230, Cambridge Univ. Press, 1996.

[4] I. Dolgachev and D. Ortland, *Point sets in projective space and theta functions*, Astérisque 165 (1988).

[5] G. van der Geer, *Hilbert Modular Surfaces*, Springer, 1988.

[6] M. R. Gonzalez-Dorrego, $(16,6)$ *configurations and geometry of Kummer surfaces in* $\mathbb{P}^3$, Mem. Amer. Math. Soc. 512 (1994).

[7] P. Griffiths and J. Harris, *A Poncelet theorem in space*, Comment. Math. Helv. 52 (1977), 145–160.

[8] R. W. H. T. Hudson, *Kummer's Quartic Surface*, Cambridge Univ. Press, 1905.

[9] G. Humbert, *Sur les fonctions abéliennes singulières*, J. Math. Pures Appl. (5) 5 (1899), 233–350.

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

[11] B. Jakob, *Poncelet* 5*-gons and abelian surfaces*, Manuscripta Math. 83 (1994), 183–198.

[12] J. F. Mestre, *Familles de courbes hyperelliptiques à multiplications réelles*, in: Progr. Math. 89, Birkhäuser, 1991, 193–208.

[13] —, *Construction de courbes de genre* 2 *à partir de leurs modules*, in: Progr. Math. 94, Birkhäuser, 1991, 313–334.

[14] K. Ribet, *Abelian varieties over* $\mathbb{Q}$ *and modular forms*, in: Algebra and Topology 1992 (Taejon), Korea Adv. Inst. Sci. Tech., Taejon, 1992, 53–79.

[15] N. I. Shepherd-Barron and R. Taylor, *Mod* 2 *and mod* 5 *icosahedral representations*, J. Amer. Math. Soc. 10 (1997), 283–298.

[16] X. Wang, 2*-dimensional simple factors of* $J_0(N)$, Manuscripta Math. 87 (1995), 179–197.

[17] J. Wilson, *Curves of genus* 2 *with real multiplication by a square-root of* 5, Oxford University D. Phil. thesis, 1998.

Magdalen College
Oxford OX1 4AU, UK
E-mail: wilsonj@maths.ox.ac.uk

Received on 5.3.1999
and in revised form on 28.6.1999 (3566)