Hyperelliptic Simple Factors of $J_0(N)$ with Dimension at Least 3

Hermann-Josef Weber

CONTENTS

Work carried out at the Institute for Experimental Mathematics, Essen, Germany.

We develop algorithms for three problems. Starting with a complex torus of dimension $g \geq 2$, isomorphic to a principally polarized, simple abelian variety $A/\mathbb{C}$, the first problem is to find an algorithmic solution of the hyperelliptic Schottky problem: Is there a hyperelliptic curve C of genus g whose jacobian variety $\mathcal{J}_C$ is isomorphic to A over $\mathbb{C}$? Our solution is based on [Poor 1994]. If such a hyperelliptic curve C exists, the next problem is the construction of the Rosenhain model $C : Y^2 = X(X-1)(X-\lambda_1)(X-\lambda_2)\dots(X-\lambda_{2g-1})$ for pairwise distinct numbers $\lambda_j \in \mathbb{C} \setminus \{0, 1\}$. Applying the theory of hyperelliptic theta functions we show that these numbers λ_j can easily be computed by using theta constants with even characteristics. If the abelian variety A is defined over a field k (this field could be the field of rational numbers, an algebraic number field of low degree, or a finite field), we show only in the case $k = \mathbb{Q}$ for simplicity, how the method in [Mestre 1991] can be generalized to get a minimal equation over $\mathbb{Z}\left[\frac{1}{2}\right]$ for the hyperelliptic curve C with jacobian variety $\mathcal{J}_C \cong_{\mathbb{C}} A$. This is our third problem. For some hyperelliptic, principally polarized and simple factors with dimension g = 3, 4, 5 of the jacobian variety $J_0(N) = \mathcal{J}_{X_0(N)}$ of the modular curve $X_0(N)$ we compute the corresponding curve equations by applying our algorithms to this special situation.

1. INTRODUCTION

We consider a g-dimensional abelian variety A, with $g \geq 2$, which is principally polarized, simple and defined over the rational numbers $\mathbb{Q}$. For example, A could be an abelian variety with real multiplication defined over $\mathbb{Q}$; that is, the endomorphism ring $\mathrm{End}(A)$ is an order in a totally real field $\mathbb{E}$ of degree $[\mathbb{E} : \mathbb{Q}] = g$. Since the generalized Shimura–Taniyama conjecture asserts that any abelian variety with real multiplication defined over $\mathbb{Q}$ is isogenous to a factor of the jacobian variety $\mathcal{J}_{X_0(N)}$ of

1058-6458/1997 \$0.50 per page

the modular curve $X_0(N)$ for suitable level $N \in \mathbb{N}$, we restrict ourselves to these modular abelian varieties. The following three problems will be solved algorithmically in this paper.

In Section 2 we give a solution, based on [Poor 1994], of the hyperelliptic Schottky problem, by showing that an abelian variety $A/\mathbb{C}$ is isomorphic to the jacobian variety $\mathcal{J}_C$ of a hyperelliptic curve $C/\mathbb{C}$ of genus $g \geq 3$ if and only if a number $n(g)$ of certain even theta constants associated to A vanish (the case $g = 2$ is trivial, since every curve of genus 2 is hyperelliptic).

Section 3 shows how the corresponding Rosenhain model $Y^2 = X(X-1)(X-\lambda_1)\dots(X-\lambda_{2g-1})$, where $\lambda_i \in \mathbb{C} \setminus \{0,1\}$, of the hyperelliptic curve C with $\mathcal{J}_C \cong_{\mathbb{C}} A$ can be computed by the use of certain other even theta constants.

Section 4 generalizes the method introduced in [Mestre 1991] for computing a $\mathbb{Z}[\frac{1}{2}]$-minimal curve equation of the curve C. This method can also be used for other fields of definition, for example finite fields or algebraic number fields with tolerable arithmetic.

In Section 5 we apply these algorithmic solutions to hyperelliptic, principally polarized and simple factors of $\mathcal{J}_{X_0(N)}$ with dimension $g = 3, 4, 5$. The construction of such modular hyperelliptic curves C of genus g is motivated by its use in public key cryptosystems for $\mathrm{Pic}^0(C)(\mathbb{F}_q)$ based on the discrete logarithm problem. Here $\mathbb{F}_q$ denotes a finite field with $q = p^r$ elements and $\mathrm{Pic}^0(C)(\mathbb{F}_q)$ the $\mathbb{F}_q$-rational divisor classes of degree 0 on C. More about this topic can be found in [Weber 1996].

2. THE HYPERELLIPTIC SCHOTTKY PROBLEM

We take the set $\mathcal{H}_g(\mathbb{C})$ of $\mathbb{C}$-isomorphism classes of hyperelliptic curves of fixed genus $g \geq 2$. This set is a coarse moduli space and has the structure of a quasi-projective irreducible algebraic variety with dimension $2g-1$ [Deligne and Mumford 1969]. We identify $\mathcal{H}_g(\mathbb{C})$ with the orbit space

$$\{B \subset \mathbb{P}^1(\mathbb{C}) : \#B = 2(g+1)\}/\,\mathrm{PSL}_2(\mathbb{C}),$$

where the action is given by

$$\gamma \circ P = \frac{a\,\alpha + b}{c\,\alpha + d}$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{C})$ and $P = (\alpha : 1) \in \mathbb{P}^1(\mathbb{C})$. Abel's map $J_{P_0} : C \to \mathrm{Pic}^0(C)$ with $P \mapsto [(P)-(P_0)]$ gives us an embedding (depending on a base point $P_0 \in C$) by sending a moduli point $C \in \mathcal{H}_g(\mathbb{C})$ into the jacobian variety $\mathcal{J}_C \cong_{\mathbb{C}} \mathrm{Pic}^0(C)$. This jacobian variety $\mathcal{J}_C$ is a principally polarized abelian variety with dimension g and polarization divisor $W_{g-1} = J_{P_0}^{(g-1)}(C^{(g-1)})$, that is, the image of the $(g-1)$-fold symmetric product $C^{(g-1)}$ under the surjective map $J_{P_0}^{(g-1)} : C^{(g-1)} \to W_{g-1} \subset \mathrm{Pic}^0(C)$. This divisor W_{g-1} is defined uniquely up to translation. For $g = 2$ the curve C is isomorphic to W_{g-1}. See [Lang 1959] for these results.

We get a morphism $\mathcal{J} : \mathcal{H}_g(\mathbb{C}) \to \mathcal{A}_g(\mathbb{C})$ with $C \mapsto (\mathcal{J}_C, W_{g-1})$, where $\mathcal{A}_g(\mathbb{C})$ is the coarse moduli space of principally polarized abelian varieties with fixed dimension $g \geq 2$. Torelli's theorem states that this morphism is injective, that is, a moduli point $C \in \mathcal{H}_g(\mathbb{C})$ can be uniquely reconstructed from its principally polarized jacobian variety $(\mathcal{J}_C, W_{g-1})$.

We observe that a moduli point $A \in \mathcal{A}_g(\mathbb{C})$ is a complex torus $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\,\mathbb{Z}^g)$ with period matrix $\Omega \in \mathbb{H}_g = \{M \in M_g(\mathbb{C}) : M^t = M,\ \mathrm{Im}(M) > 0\}$. So we get the description $\mathcal{A}_g(\mathbb{C}) = \mathbb{H}_g/\Gamma_g$, where the action of the full modular group $\Gamma_g = \mathrm{Sp}_{2g}(\mathbb{Z})$ is given by

$$\gamma \circ \Omega = (a\,\Omega + b)(c\,\Omega + d)^{-1}$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_g$ and $\Omega \in \mathbb{H}_g$.

The *hyperelliptic Schottky problem* asks for a characterization of the hyperelliptic jacobian varieties in $\mathcal{A}_g(\mathbb{C})$. Since $\mathcal{A}_g(\mathbb{C})(\mathcal{J}(\mathcal{H}_g(\mathbb{C})))$ has codimension $\frac{1}{2}(g-1)(g-2)$, this problem is trivial for $g \leq 2$. That's the reason why the following question is only interesting in the case $g \geq 3$:

Problem 2.1. *Let $A \in \mathcal{A}_g(2)(\mathbb{C})$ be a simple moduli point given as a complex torus $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\,\mathbb{Z}^g)$ with period matrix $\Omega \in \mathbb{H}_g$ (where simple means* *symplectic irreducible). Let* $\mathcal{B} = \{1, 2, 3, \ldots, 2g+1, \infty\}$*. Are there distinct numbers* $\alpha_i \in \mathbb{C} \cup \{\infty\}$*, for* $i \in \mathcal{B}$*, such that the moduli point* $C \in \mathcal{H}_g(\mathbb{C})$ *given by*

$$Y^2 = \prod_{i \in \mathcal{B}} (X - \alpha_i)$$

satisfies $A \cong_{\mathbb{C}} \mathcal{J}_C$*, and* α_∞ *corresponds to the base point* P_0 *of Abel's map* J_{P_0} *under the projection to the projective line* $\mathbb{P}^1$*?*

Our algorithmic solution of this problem is based on [Poor 1994], where the hyperelliptic jacobian varieties are characterized by a number (depending on the genus g) of vanishing even theta constants.

Write $\mathbb{F}_2^{2g}$ for the set of characteristics $\left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right]$ with row vectors $\delta, \varepsilon \in \mathbb{F}_2^g$. If we choose a symplectic basis for the 2-torsion points $A[2]$ of a moduli point $A \in \mathcal{A}_g(\mathbb{C})$ by fixing a level-2-structure $\Psi_2 : \left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right] \mapsto \frac{1}{2}(\varepsilon + \delta\,\Omega)$, we can identify $A[2]$ with $\mathbb{F}_2^{2g}$. We get a pair (A, Ψ_2) from the orbit space $\mathcal{A}_g(2)(\mathbb{C}) = \mathbb{H}_g/\Gamma_g(2)$ with $\Gamma_g(2) = \ker(\Gamma_g \to \mathrm{Sp}_{2g}(\mathbb{F}_2))$.

We attach to every characteristic $\left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right] \in \mathbb{F}_2^{2g}$ a *theta constant*

$$\theta\left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right](\Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi\, i\,((n+\frac{1}{2}\delta)\,\Omega\,(n+\frac{1}{2}\delta)^t + (n+\frac{1}{2}\delta)\,\varepsilon^t)}$$

and get $2^{g-1}(2^g+1)$ *even* or $2^{g-1}(2^g-1)$ *odd* holomorphic functions $\theta\left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right] : \mathbb{H}_g \mapsto \mathbb{C}$, depending on whether $\delta\varepsilon^t = 0$ or $\delta\varepsilon^t = 1$. It follows that all the odd theta constants vanish; that is, $\theta\left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right] \equiv 0$ when $\delta\,\varepsilon^t = 1$. The following result gives us a condition necessary to our Problem 2.1:

Theorem 2.2 [Krazer 1903, p. 459]. *Let* $(A, \Psi_2) \in \mathcal{A}_g(2)(\mathbb{C})$ *be a simple moduli point with torus representation* $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\,\mathbb{Z}^g)$ *and* $A \cong_{\mathbb{C}} \mathcal{J}_C$ *for some moduli point* $C \in \mathcal{H}_g(\mathbb{C})$*. Let* $V(A) = V(A, \Psi_2)$ *be the set of vanishing even theta constants,*

$$V(A) = \left\{\theta\left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right](\Omega) \equiv 0 : \left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right] \in \mathbb{F}_2^{2g},\ \delta\,\varepsilon^t = 0\right\}$$

Then

$$\#V(A) = 2^{g-1}(2^g+1) - \binom{2g+1}{g}.$$

We define $n(g)$ as the number in the right-hand side of this equation.

An *azygetic fundamental system* is a set $\eta = \{\eta_1, \ldots, \eta_{2g+1}\}$ of $2g+1$ pairwise distinct characteristics $\eta_i = \left[\begin{smallmatrix}\delta_i\\ \varepsilon_i\end{smallmatrix}\right] \in \mathbb{F}_2^{2g} \setminus \{0\}$ such that $\delta_i \varepsilon_j^t + \delta_j \varepsilon_i^t = 1$ for all η_i and η_j with $i \neq j$.

Proposition 2.3. (i) *The finite group*

$$\mathrm{Sp}_{2g}(\mathbb{F}_2) \cong \Gamma_g/\Gamma_g(2)$$

acts transitively on the set of azygetic fundamental systems in $\mathbb{F}_2^{2g}$*.*

(ii) *Let*

$$\eta_1^0 = \begin{bmatrix} 1\,0\,0\,0 \ldots 0 \\ 0\,0\,0\,0 \ldots 0 \end{bmatrix}, \quad \eta_2^0 = \begin{bmatrix} 1\,0\,0\,0 \ldots 0 \\ 1\,0\,0\,0 \ldots 0 \end{bmatrix},$$

$$\eta_3^0 = \begin{bmatrix} 0\,1\,0\,0 \ldots 0 \\ 1\,0\,0\,0 \ldots 0 \end{bmatrix}, \quad \eta_4^0 = \begin{bmatrix} 0\,1\,0\,0 \ldots 0 \\ 1\,1\,0\,0 \ldots 0 \end{bmatrix},$$

$$\eta_5^0 = \begin{bmatrix} 0\,0\,1\,0 \ldots 0 \\ 1\,1\,0\,0 \ldots 0 \end{bmatrix}, \quad \eta_6^0 = \begin{bmatrix} 0\,0\,1\,0 \ldots 0 \\ 1\,1\,1\,0 \ldots 0 \end{bmatrix},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\eta_{2g+1}^0 = \begin{bmatrix} 0\,0\,0\,0 \ldots 0 \\ 1\,1\,1\,1 \ldots 1 \end{bmatrix}.$$

Then the set $\eta^0 = \{\eta_1^0, \ldots, \eta_{2g+1}^0\}$ *is an azygetic fundamental system in* $\mathbb{F}_2^{2g}$*.*

Proof. See [Igusa 1972, p. 212] for statement (i) and [Mumford 1983, p. 3.88] for (ii). ☐

To state the following necessity and sufficiency criterion from [Poor 1994] we need some notations. Let $U = \{1, 3, 5, \ldots, 2g+1\} \subset \mathcal{B}$ be the set of odd indices and define $U \bullet S = (U \cup S) \setminus (U \cap S)$ for any set $S \subset \mathcal{B} \setminus \{\infty\}$. (That is, $U \bullet S$ is the symmetric difference of U and S).

Define

$$T_0(2) = \{S \subset \mathcal{B} \setminus \{\infty\} : \#S \equiv 0 \bmod 2\}.$$

Then $T_0(2)$ is a disjoint union $T_0^{=}(2) \cup T_0^{\neq}(2)$, where $T_0^{=}(2) = \{S \subset \mathcal{B} \setminus \{\infty\} : \#(U \bullet S) = g+1\}$ and $T_0^{\neq}(2)$ is defined analogously.

For an azygetic fundamental system η in $\mathbb{F}_2^{2g}$ and a set $S \in T_0^{\neq}(2)$ we put $\eta_S = \sum_{s \in S} \eta_s$ and call

$$W(A, \eta) = \{\theta[\eta_S](\Omega) \equiv 0 : S \in T_0^{\neq}(2)\}$$

the *vanishing set* of some moduli point $A \in \mathcal{A}_g(\mathbb{C})$.

Theorem 2.4 [Poor 1994, Main Theorem 2.6.1]. *For a moduli point $(A,\Psi_2) \in \mathcal{A}_g(2)(\mathbb{C})$ the following two statements are equivalent*:

(i) *A is simple and there is an azygetic fundamental system $\eta = \{\eta_1,\dots,\eta_{2g+1}\}$ such that $V(A) = W(A,\eta)$.*
(ii) *There exists a moduli point $C \in \mathcal{H}_g(\mathbb{C})$ satisfying the conditions of Problem* 2.1.

When (i) *and* (ii) *hold, α_i corresponds to η_i (that is, if P_i is a Weierstrass point with x-coordinate α_i, then $\Psi_2(J_{P_0}(P_i)) = \eta_i$), and α_∞ corresponds to* 0.

Algorithm 2.5. Input. A simple moduli point $A \in \mathcal{A}_g(2)(\mathbb{C})$ of dimension $g \geq 2$ given as a torus $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\,\mathbb{Z}^g)$ with the standard polarization.

Output. An answer $\in \{\text{YES}, \text{NO}\}$ for the question: Is there a moduli point $C \in \mathcal{H}_g(\mathbb{C})$ with $\mathcal{J}_C \cong_{\mathbb{C}} A$? For $g = 2$ the answer is always YES and there's nothing to do.

Step 1. Compute the $2^{g-1}(2^g+1)$ even theta constants $\theta\left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right](\Omega)$ with $\delta\,\varepsilon^t = 0$ and form the set $V(A)$ (where the vanishing of the theta constants only has been proved numerically).

Step 2. If $\#V(A) = n(g)$ continue with Step 3. Otherwise output NO because of Theorem 2.2.

Step 3. Form $W(A,\eta^0)$ with the azygetic fundamental system η^0 from Proposition 2.3. Output YES if $V(A) = W(A,\eta^0)$. Otherwise find, if possible, a matrix $\gamma \in \mathrm{Sp}_{2g}(\mathbb{F}_2)$ such that

$$V(A) = W(A, \gamma \circ \eta^0),$$

and output YES. If there is no such γ, output NO.

3. CONSTRUCTION OF THE ROSENHAIN MODEL OVER $\mathbb{C}$

Take a simple moduli point $(A,\Psi_2) \in \mathcal{A}_g(2)(\mathbb{C})$ given as a torus $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\,\mathbb{Z}^g)$ with an azygetic fundamental system $\eta = \{\eta_1,\dots,\eta_{2g+1}\}$ such that $V(A) = W(A,\eta)$. An application of Theorem 2.4 gives a moduli point C and numbers α_i, for $i = 1,2,\dots,2g+1,\infty$, as in the statement of the same theorem.

Theorem 3.1 [Mumford 1983, Thomae's theorem, p. 3.120]. *The value of $(\theta[\eta_S](\Omega))^4$ is* 0 *for $S \in T_0^{\neq}(2)$ and*

$$c \cdot (-1)^{\#(U\cap S)} \prod_{i\in(U\bullet S)} \prod_{j\notin(U\bullet S)} \frac{1}{(\alpha_i-\alpha_j)}$$

for all $S \in T_0^{=}(2)$, where $c \in \mathbb{C}^*$ is a constant that does not depend on S.

We introduce, for $\mu = 1,\dots,2g-1$, the analytic moduli

$$\lambda_\mu = \frac{\alpha_{\mu+2}-\alpha_1}{\alpha_2-\alpha_1},$$

to get the new model

$$Y^2 = X(X-1)(X-\lambda_1)\dots(X-\lambda_{2g-1}) \qquad (3\text{–}1)$$

for the moduli point $C \in \mathcal{H}_g(\mathbb{C})$ with pairwise distinct numbers $\lambda_\mu \in \mathbb{C}\setminus\{0,1\}$. Equation (3–1) is called the *Rosenhain model* of C.

Problem 3.2. *Compute the Rosenhain model of $C \in \mathcal{H}_g(\mathbb{C})$.*

This problem can easily be solved by using the next result, for which we introduce some more notation. For all $\mu = 1,\dots,2g-1$ write $\mathcal{B}$ as some disjoint union

$$\mathcal{B} = \{1,2,\mu{+}2,\infty\} \cup \mathcal{B}_0^\mu \cup \mathcal{B}_1^\mu,$$

where $\mathcal{B}_0$ and $\mathcal{B}_1$ have $g-1$ elements. Set

$$\begin{aligned} S_1^\mu &= \{1,2\}\cup\mathcal{B}_0^\mu, & S_2^\mu &= \{1,2\}\cup\mathcal{B}_1^\mu,\\ S_3^\mu &= \{1,\mu{+}2\}\cup\mathcal{B}_0^\mu, & S_4^\mu &= \{1,\mu{+}2\}\cup\mathcal{B}_1^\mu,\\ S_5^\mu &= \{2,\mu{+}2\}\cup\mathcal{B}_0^\mu, & S_6^\mu &= \{2,\mu{+}2\}\cup\mathcal{B}_1^\mu. \end{aligned}$$

Finally, for $\nu = 1,\dots,6$ we set $\theta_\nu^\mu = \theta[\eta_{U\bullet S_\nu^\mu}](\Omega)$.

Theorem 3.3. *With the notation just introduced*,

$$\lambda_\mu = \frac{(\theta_1^\mu\,\theta_2^\mu)^4 + (\theta_3^\mu\,\theta_4^\mu)^4 - (\theta_5^\mu\,\theta_6^\mu)^4}{2\,(\theta_1^\mu\,\theta_2^\mu)^4},$$

for $\mu = 1,\dots,2g{-}1$.

Proof. Consider for some $k \in \mathcal{B}\setminus\{\infty\}$ the disjoint decomposition $\mathcal{B}\setminus\{\infty\} = S \cup T \cup \{k\}$ for sets S,T

where S and T each have cardinality g. As an application of Theorem 3.1 we get the identity

$$\frac{(\theta[\eta_{U\bullet(T\cup\{k\})}](\Omega))^4}{(\theta[\eta_{U\bullet(S\cup\{k\})}](\Omega))^4} = (-1)^{k+1}\frac{\prod_{i\in T}(\alpha_i-\alpha_k)}{\prod_{j\in S}(\alpha_j-\alpha_k)}. \tag{3–2}$$

We fix $\mu \in \{1,\dots,2g-1\}$. Then we apply (3–2) with $k=1$ and $S = S_1^\mu \setminus \{1\}$ and $T = S_3^\mu \setminus \{1\}$, obtaining

$$\frac{\theta_3^\mu}{\theta_1^\mu} = \frac{\prod_{i\in S_3^\mu\setminus\{1\}}(\alpha_i-\alpha_1)}{\prod_{j\in S_1^\mu\setminus\{1\}}(\alpha_j-\alpha_1)}. \tag{3–3}$$

If we do the same for $k=1$ and $S = S_2^\mu \setminus \{1\}$ and $T = S_4^\mu \setminus \{1\}$ we get from (3–2) the equation

$$\frac{\theta_4^\mu}{\theta_2^\mu} = \frac{\prod_{i\in S_4^\mu\setminus\{1\}}(\alpha_i-\alpha_1)}{\prod_{j\in S_2^\mu\setminus\{1\}}(\alpha_j-\alpha_1)}. \tag{3–4}$$

Multiplying (3–3) and (3–4) we get

$$\frac{\theta_3^\mu\,\theta_4^\mu}{\theta_1^\mu\,\theta_2^\mu} = \frac{(\alpha_{\mu+2}-\alpha_1)^2}{(\alpha_2-\alpha_1)^2}. \tag{3–5}$$

Applying (3–2) in the same manner to $k=2$ and the cases $S = S_1^\mu \setminus \{2\}$ and $T = S_5^\mu \setminus \{2\}$, on the one hand, and $S = S_2^\mu \setminus \{2\}$, $T = S_6^\mu \setminus \{2\}$, on the other, we get an analogous equation

$$\frac{\theta_5^\mu\,\theta_6^\mu}{\theta_1^\mu\,\theta_2^\mu} = \frac{(\alpha_{\mu+2}-\alpha_2)^2}{(\alpha_1-\alpha_2)^2}. \tag{3–6}$$

We use (3–5) and (3–6) in the easily verified identity

$$\frac{\alpha_{\mu+2}-\alpha_1}{\alpha_2-\alpha_1} = \frac{(\alpha_2-\alpha_1)^2+(\alpha_{\mu+2}-\alpha_1)^2-(\alpha_{\mu+2}-\alpha_2)^2}{2\,(\alpha_2-\alpha_1)^2},$$

and see that our statement is true for the given μ. □

Algorithm 3.4. Input. A simple moduli point $A \in \mathcal{A}_g(2)(\mathbb{C})$ of dimension $g \geq 2$ given as a torus $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\,\mathbb{Z}^g)$ with an azygetic fundamental system η such that $V(A) = W(A,\eta)$.

Output. The Rosenhain model (3–1) for some moduli point $C \in \mathcal{H}_g(\mathbb{C})$ with $\mathcal{J}_C \cong_{\mathbb{C}} A$.

Step. Compute the roots $\lambda_1,\dots,\lambda_{2g-1}$ using Theorem 3.3 and output (3–1).

4. CONSTRUCTION OF A MINIMAL CURVE EQUATION OVER $\mathbb{Z}\left[\frac{1}{2}\right]$

We now state and solve our third problem:

Problem 4.1. *Let $C \in \mathcal{H}_g(\mathbb{Q})$ be a moduli point of genus $g \geq 2$ with projective model*

$$Z^{2g}\,Y^2 = F(X,Z), \tag{4–1}$$

where $F \in \mathbb{C}[X,Z]$ is the binary form of degree $2(g+1)$ given by

$$F(X,Z) = \sum_{i=0}^{2(g+1)} F_i X^i Z^{2(g+1)-i}. \tag{4–2}$$

Decide whether C has an affine model over $\mathbb{Q}$ and, if so, compute a curve equation that is minimal over $\mathbb{Z}\left[\frac{1}{2}\right]$.

Given an element $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{C})$ and a form as in (4–2), we can write

$$F(aX+b, cZ+d) = \sum_{i=0}^{2(g+1)} \tilde{F}_i X^i Z^{2(g+1)-i},$$

where each $\tilde{F}_i$ can be expressed as a polynomial with integer coefficients on the F_i and the entries of γ. Then we can define an action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{C}[X,Z,F_0,\dots,F_{2(g+1)}]$ by setting

$$\begin{aligned}(\gamma\circ\varphi)&(X,Z,F_0,\dots,F_{2(g+1)})\\ &= \varphi(dX-bZ, -cX+aZ, \tilde{F}_0,\dots,\tilde{F}_{2(g+1)}),\end{aligned}$$

for $\varphi \in \mathbb{C}[X,Z,F_0,\dots,F_{2(g+1)}]$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$. The homogeneous polynomials that are invariant under this action form a finitely generated algebra

$$\mathcal{K}_g(\mathbb{C}) \subset \mathbb{C}[X,Z,F_0,\dots,F_{2(g+1)}]$$

over $\mathbb{C}$, called the *covariant algebra of binary forms* of degree $2(g+1)$.

Every covariant $\varphi \in \mathcal{K}_g(\mathbb{C})$ can be characterized by its *order* i, which is its degree in X, Z, and its *degree* e, which is its degree in $F_0,\dots,F_{2(g+1)}$.

Thus we can represent the covariant algebra as a bihomogeneous graded algebra

$$\mathcal{K}_g(\mathbb{C}) = \bigoplus_{i,e\geq 0} \mathcal{K}_g(i,e)(\mathbb{C}).$$

This graded algebra contains a subalgebra

$$\mathcal{I}_g(\mathbb{C}) = \bigoplus_{e\geq 0} \mathcal{K}_g(0,e)(\mathbb{C}),$$

the *invariant algebra of binary forms* with degree $2(g+1)$. This subalgebra is also finitely generated over $\mathbb{C}$. Some of these results can be found in the classical papers of Hilbert.

The right-hand side of (4–2) can be regarded as an element of $\mathbb{C}[X,Z,F_0,\dots,F_{2(g+1)}]$, which we denote by $\mathcal{F}$ and call the *generic binary form*. It is, by construction, a covariant of order $2(g+1)$ and index 1.

The *überschiebung* operation on covariants is defined as follows (see also [Vinberg and Popov 1994, p. 182]). If $\varphi_1,\varphi_2 \in \mathcal{K}_g(\mathbb{C})$ have orders i_1, i_2 and degrees e_1, e_2, and if $h \in \{0,\dots,\min(i_1,i_2)\}$, we set

$$(\varphi_1,\varphi_2)_h = \lambda \sum_{j=0}^{h} \binom{h}{j} \frac{\partial^h \varphi_1}{\partial X^{h-j}\partial Z^j} \frac{\partial^h \varphi_2}{\partial X^{j}\partial Z^{h-j}},$$

with

$$\lambda = \frac{(i_1-h)!\,(i_2-h)!}{i_1!\,i_2!};$$

this is a new covariant with order i_1+i_2-2h and degree e_1+e_2. (The factor λ is traditional.)

Theorem 4.2 [Clebsch 1872, p. 101]. *The covariant algebra $\mathcal{K}_g(\mathbb{C})$ is generated by iterated überschiebungen of the generic binary form*

$$\mathcal{F} \in \mathcal{K}_g(2(g+1),1)(\mathbb{C}).$$

Now we generalize the method of Mestre [1991] to the case where the genus is greater than 2 and the field of definition of the moduli point is $\mathbb{Q}$. Suppose that the automorphism group $\mathrm{Aut}(C)$ of the moduli point $C \in \mathcal{H}_g(\mathbb{C})$ is trivial, which means $\mathrm{Aut}(C) = \{\mathrm{id}, \iota\}$, where ι denotes the hyperelliptic involution. Then Mestre's method (for $g=2$) gives us an affine model over $\mathbb{Q}$, provided that such a model exists.

We now recall results from the classical invariant theory that are fundamental for this method and its generalization. Let $\psi_1,\psi_2,\psi_3 \in \mathcal{K}_g(\mathbb{C})$ be three covariants of order $2 = i_1 = i_2 = i_3$ and degrees $0 < e_1 < e_2 < e_3$. Following [Clebsch 1872, p. 201], we have the following corresponding simultaneous system of generators:

- 3 covariants
$$\varphi_1 = (\psi_2,\psi_3)_1 \in \mathcal{K}_g(2, e_2+e_3)(\mathbb{C}),$$
$$\varphi_2 = (\psi_3,\psi_1)_1 \in \mathcal{K}_g(2, e_3+e_1)(\mathbb{C}),$$
$$\varphi_3 = (\psi_1,\psi_2)_1 \in \mathcal{K}_g(2, e_1+e_2)(\mathbb{C});$$
- 6 invariants $Q_{l,m} = (\psi_l,\psi_m)_2 \in \mathcal{I}_g(e_l+e_m)(\mathbb{C})$, for $l \leq m = 1,2,3$; and
- 1 invariant
$$R_{123} = -\varphi_1 \star \varphi_2 \star \varphi_3 \in \mathcal{I}_g(e_1+e_2+e_3)(\mathbb{C}),$$
with $R_{123}^2 = \frac{1}{2}\det(Q_{l,m})$ for $Q_{2,1} = Q_{1,2}$, $Q_{3,1} = Q_{1,3}$, and $Q_{3,2} = Q_{2,3}$. The operation $\star$ is defined in [Mestre 1991].

Proposition 4.3 [Clebsch 1872, p. 201].

(i) $\sum_{l,m=1}^{3} Q_{l,m}\varphi_l\varphi_m = 0$.
(ii) $R_{123}\mathcal{F} = \sum_{l=1}^{3} (\mathcal{F},\psi_l)_2\varphi_l$.
(iii) *For fixed values of the indeterminates $F_1, \dots, F_{2(g+1)}$, the covariants φ_1, φ_2, and φ_3 are linearly independent if and only if $R_{123} \neq 0$ (here φ_1, φ_2, φ_3, and R_{123} are specialized at the given values).*

Mestre recognized that relation (ii) is a special case of

$$R_{123}^{g+1}\mathcal{F} = \sum_{l_1,\dots,l_{g+1}=1}^{3} H_{l_1,\dots,l_{g+1}} \varphi_{l_1}\cdots\varphi_{l_{g+1}},$$

with

$$H_{l_1,\dots,l_{g+1}} = (\dots((\mathcal{F},\psi_{l_1})_2,\psi_{l_2})_2,\dots,\psi_{l_{g+1}})_2 \in \mathcal{I}_g\bigl(\textstyle\sum_{i=1}^{g+1} e_{l_i} + 1\bigr)(\mathbb{C})$$

for $g \in \mathbb{N}\cup\{0\}$. This led him to the idea that we now describe.

Proposition 4.4 [Mestre 1991, pp. 322 and 324]. *Let C and F be as in Problem 4.1, and consider the specialization of the various covariants discussed above to the given $F_1, \dots, F_{2(g+1)}$. Assume that F has trivial automorphism group. (In this case R_{123} is nonzero). Let $\mathcal{V}(Q)$ be the conic defined by the irreducible quadratic form $Q \in \mathbb{C}[X_1, X_2, X_3]$ such that*

$$Q(X_1, X_2, X_3) = \sum_{l,m=1}^{3} Q_{l,m} X_l X_m,$$

and let $\mathcal{V}(H)$ be the curve of degree $g+1$ defined by the form $H \in \mathbb{C}[X_1, X_2, X_3]$ such that

$$H(X_1, X_2, X_3) = \sum_{l_1,\dots,l_{g+1}=1}^{3} H_{l_1,\dots,l_{g+1}} X_{l_1} \dots X_{l_{g+1}}.$$

Then:

(i) *The map $\Phi : \mathbb{P}^1(\mathbb{C}) \to \mathcal{V}(Q)$ taking $(X{:}Z)$ to $(\varphi_1{:}\varphi_2{:}\varphi_3)$ is an isomorphism defined over $\mathbb{C}$, and it maps the set of $(X{:}Z) \in \mathbb{P}^1(\mathbb{C})$ such that $F(X,Z) = 0$ to the set of $(X_1{:}X_2{:}X_3) \in \mathbb{P}^2(\mathbb{C})$ such that $Q(X_1, X_2, X_3) = H(X_1, X_2, X_3)$.*

(ii) *The moduli point $C \in \mathcal{H}_g(\mathbb{Q})$ possesses an affine model over $\mathbb{Q}$ if and only if the conic $\mathcal{V}(Q)$ has a rational point over $\mathbb{Q}$.*

The *discriminant* $\Delta_g \in \mathcal{I}_g(2(g+1))(\mathbb{C})$ is the invariant of degree $2(g+1)$. Following [Geyer 1974], we have $\mathcal{H}_g(\mathbb{C}) \cong_{\mathbb{C}} \mathrm{Spec}_{\mathbb{C}}(\mathcal{I}_g[\Delta_g^{-1}]_0)$.

The elements of the algebra $\mathcal{I}_g[\Delta_g^{-1}](\mathbb{C})$ are called *absolute invariants* (that is, quotients of invariants with the same degree) *with discriminant power in the denominator*. If we choose an embedding

$$\mathcal{I}_g(\mathbb{C}) \hookrightarrow \mathcal{I}_g[\Delta_g^{-1}](\mathbb{C})$$

and specialize at $F(X,Z) \in \mathcal{H}_g(\mathbb{Q})$, the invariants $Q_{l,m}$ and $H_{l_1,\dots,l_{g+1}}$ are then elements in $\mathbb{Q}$ with restricted denominator and so a conversion from $\mathbb{C}$ to $\mathbb{Q}$ is possible. We will give the precise definition of the embedded coefficients (depending on the genus g) in the last section and fix for these embedded coefficients the same notation.

Lemma 4.5 [Mordell 1969, p. 47]. *Suppose that $Q \in \mathbb{Z}[Z_1, Z_2, Z_3]$ is an irreducible quadratic form with a nontrivial solution $(Z_1^0, Z_2^0, Z_3^0) \in \mathbb{Z}^3 \setminus \{0\}$. Then every other nontrivial solution has the form*

$$(Z_1, Z_2, Z_3) = (h_1(T), h_2(T), h_3(T))$$

with polynomials $h_1, h_2, h_3 \in \mathbb{Z}[T]$ of degree two, depending also on (Z_1^0, Z_2^0, Z_3^0).

Algorithm 4.6. Input. A binary form $F(X,Z) \in \mathbb{C}[X,Z]$ with trivial automorphism group, which corresponds to a moduli point $C \in \mathcal{H}_g(\mathbb{Q})$ of genus $g \geq 2$.

Output. An answer in $\{\mathrm{YES}, \mathrm{NO}\}$ for the question: Has C an affine model over $\mathbb{Q}$? If the answer is YES, output an affine model $Y^2 = h(T) = \sum_{i=0}^{\deg(h)} h_i T^i \in \mathbb{Z}[T]$ with these properties:

(1) $\deg(h) = 2g{+}1$ if C has a $\mathbb{Q}$-rational Weierstrass point, and $2(g+1)$ otherwise.
(2) $\sum_{i=0}^{\deg(h)} |h_i| \in \mathbb{Z}$ is minimal for C.
(3) $|\Delta_g(h(T))| \in \mathbb{Z}\left[\frac{1}{2}\right]$ is minimal for C.

Step 1. Compute the embedded coefficients $Q_{l,m} \in \mathbb{Q}$ for $l \leq m = 1, 2, 3$. They are elements in $\mathbb{Z}[S^{-1}]$, where S denotes the set of primes with bad reduction of the moduli point $C \in \mathcal{H}_g(\mathbb{Q})$.

Step 2. Using Lemma 4.5, compute the parametrization

$$(Z_1, Z_2, Z_3) = (h_1(T), h_2(T), h_3(T)) \tag{4–3}$$

for the irreducible quadratic form $Q(Z_1, Z_2, Z_3) \in \mathbb{Z}[Z_1, Z_2, Z_3]$. Output NO if $(Z_1, Z_2, Z_3) = (0,0,0)$ and YES otherwise.

Step 3. Compute the embedded coefficients

$$H_{l_1,\dots,l_{g+1}} \in \mathbb{Q}$$

for $l_1, \dots, l_{g+1} = 1, 2, 3$. Without loss of generality, they are elements in $\mathbb{Z}[S^{-1}]$. Plug into (4–3) to get a squarefree polynomial

$$h^{(3)}(T) = H(h_1(T), h_2(T), h_3(T)) \in \mathbb{Z}[T]$$

of degree $\deg(h^{(3)}) = 2(g+1)$.

Step 4. Factor $\Delta_g(h^{(3)}(T))$, which has the form

$$|\Delta_g(h^{(3)}(T))| = 2^{\nu_2}\, m^{2(2g+1)(g+1)} \prod_{p\in S} p^{\nu_p}$$

for $\nu_2, \nu_p, m \in \mathbb{N}_0$.

Step 5. Minimize $|\Delta_g(h^{(3)}(T))|$ by iterated computations of roots T_0 of the congruence $h^{(3)}(T) \equiv 0 \bmod n$ for some $n \in \{2, m\} \cup S$ and afterwards by doing the transformation

$$h^{(3)}(T) \mapsto n^{-2(g+1)} h^{(3)}(T_0 + n\,T).$$

The result is a polynomial $h^{(2)}(T)$ with property (3).

Step 6. Minimize $\sum_{i=0}^{\deg(h^{(2)})} |h_i^{(2)}| \in \mathbb{Z}$ by iterated computations of roots $\beta \in \mathbb{C}$ and afterwards by doing the transformation $h^{(2)}(T) \mapsto h^{(2)}(T + \mathrm{Re}(\beta))$ under the assumption $h_{2g+1}^{(2)} \le h_0^{(2)}$. The result is a polynomial $h^{(1)}(T)$ with property (2).

Step 7. Find a root $\gamma \in \mathbb{Z}$ of the polynomial $h^{(1)}(T)$ (if C has a $\mathbb{Q}$-rational Weierstrass point) and apply the transformation $h^{(1)}(T) \mapsto h^{(1)}(T^{-1}+T_0)\,T^{2(g+1)}$ to get a polynomial $h(T) \in \mathbb{Z}[T]$ with property (3). Output the affine model $Y^2 = h(T)$.

Remark 4.7. Only for simplicity have we considered the case that the moduli point $C \in \mathcal{H}_g(k)$ is defined over $k = \mathbb{Q}$. If k is a finite field or a number field of low degree, it's also possible to construct curve equations over these fields. In [Weber 1996] there is an example of a moduli point $C \in \mathcal{H}_2(k)$, which is defined over a real quadratic number field $k = \mathbb{Q}(\sqrt{d})$ with class number $h_k = 1$. The jacobian variety $\mathfrak{J}_C$ of this moduli point is isomorphic to an abelian variety A with complex multiplication.

5. APPLICATION TO MODULAR CURVES

Our aim in this section is to construct (as an application of Algorithms 2.5, 3.4, and 4.6) hyperelliptic curves with real multiplication and genus $g = 3, 4, 5$. The jacobian varieties of these curves are principally polarized, simple factors of the jacobian variety $J_0(N) = \mathfrak{J}_{X_0(N)}$ of the modular curve $X_0(N)$. We recall the definition of this modular curve.

Let $N \in \mathbb{N}$ be a fixed natural number and let $\Gamma_0(N)$ be the subgroup of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ with $c \equiv 0 \bmod N$. The modular curve $X_0(N)/\mathbb{C}$ can be regarded as the orbit space $\mathbb{H}^*/\Gamma_0(N)$, where $\mathbb{H}^* = \{\omega \in \mathbb{C} : \mathrm{Im}(\omega) > 0\} \cup \mathbb{P}^1(\mathbb{Q})$ and the action of $\Gamma_0(N)$ is given by

$$\gamma \circ \omega = \frac{a\,\omega + b}{c\,\omega + d}$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ and $\omega \in \mathbb{H}^*$. If we denote by $S_2(N)$ the space of cusp forms of weight 2 for the group $\Gamma_0(N)$, we get [Shimura 1971] for some fixed newform $f(z) = 1 + \sum_{n=2}^{\infty} a_n e^{(2\pi i\, n/N)\,z} \in S_2(N)$ a simple abelian variety $A_f/\mathbb{Q}$ satisfying these conditions:

- $\mathrm{End}(A_f)$ is an order in the totally real field $\mathbb{E}_f = \mathbb{Q}(a_2, \dots, a_\infty)$ with degree $[\mathbb{E}_f : \mathbb{Q}] = \dim(A_f)$.
- A_f is isogenous to a simple factor of the jacobian variety $J_0(N)$.

Using the programs of X. Wang and M. Müller we can compute the decomposition of $J_0(N)$ into simple factors of dimension $g \ge 1$, the Fourier coefficients of new forms $f \in S_2(N)$, and the period matrices Ω_f of simple factors A_f of $J_0(N)$ with dimension $g \ge 1$. See [Wang 1995] for more details, including the definition of polarization and a criterion to test the principality given a period matrix of dimension $g \ge 2$.

For those modular curves $X_0(N)$ that are hyperelliptic (classified in [Ogg 1974]), affine models in the form $Y^2 = f(T) \in \mathbb{Z}[T]$ have been computed by Gonzàlez Rovira [1991] and independently by M. Shimura [1995], who also considered the nonhyperelliptic case. The methods used in these papers don't leave the arithmetic of the modular curve $X_0(N)$, so they don't allow us to treat simple factors of $J_0(N)$. We show now that by applying our algorithms to hyperelliptic, principally polarized and simple factors of $J_0(N)$, we can construct affine models for these factors and for the cases treated by Gonzàlez Rovira and M. Shimura. The case $g = 2$ was solved in [Wang 1995].

5.1. Three-Dimensional Factors of $J_0(N)$

We explain in detail how our algorithms must be applied to get affine models of hyperelliptic curves $C/\mathbb{Q}$ with real multiplication and genus $g = 3$.

We start with the newform

$$f = 1 + \sum_{n=2}^{\infty} a_n q^n \in S_2(284)$$

whose Fourier coefficients belong to the totally real field

$$\mathbb{E}_f = \mathbb{Q}(\{a_n : n \in \mathbb{N}\}) = \mathbb{Q}(\beta)$$

with irreducible equation $\beta^3 + 3\beta^2 - 3 = 0$. The first few of these coefficients are

$$\begin{aligned}
a_2 &= 0, & a_3 &= \beta,\\
a_5 &= -\beta^2 - 3\beta - 1, & a_7 &= 2\beta^2 + 2\beta - 6,\\
a_{11} &= 2\beta, & a_{13} &= -4\beta^2 - 6\beta + 4,\\
a_{17} &= 4\beta^2 + 6\beta - 6, & a_{19} &= -\beta^2 - 2,\\
a_{23} &= -2\beta^2 + 8, & a_{29} &= 6\beta^2 + 9\beta - 8,\\
a_{31} &= -2\beta - 8, & a_{37} &= -\beta^2 - 4\beta - 2,\\
a_{41} &= -4\beta^2 - 8\beta + 4, & a_{43} &= -\beta^2 - 3\beta + 1,\\
a_{47} &= -4\beta^2 - 8\beta + 8, & & \ldots .
\end{aligned}$$

By Shimura's construction we get an associated simple abelian variety A_f isogenous to a three-dimensional simple factor of the jacobian variety $J_0(284)$ of the modular curve $X_0(284)$. In general a factor A_f is simple over $\mathbb{Q}$ and simple over $\mathbb{C}$ only if the level N is squarefree. If the level N contains a square we have to show that $\mathrm{End}(A_f)$ has no zero-divisors to assume that A_f is simple over $\mathbb{C}$.

A_f is principally polarized and possesses the torus representation $\mathbb{C}^3/(\mathbb{Z}^3 + \Omega_f\,\mathbb{Z}^3)$, where

$$\Omega_f = (w_{ij})_{1 \le i,j \le 3}$$

is the period matrix, whose entries (truncated to five decimal places) are

$$\begin{aligned}
w_{11} &= -1.39675 + 1.71195i,\\
w_{22} &= -0.36574 + 0.28982i,\\
w_{33} &= 1.61009 + 1.33956i,\\
w_{12} = w_{21} &= -0.48286 + 0.49444i,\\
w_{13} = w_{31} &= -0.59993 + 0.16233i,\\
w_{23} = w_{32} &= 0.66735 + 0.30210i.
\end{aligned}$$

We use this torus $\mathbb{C}^3/(\mathbb{Z}^3 + \Omega_f\,\mathbb{Z}^3)$ as an input for Algorithm 2.5. In Step 1 we compute the 36 even theta constants $\theta\left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right](\Omega_f)$ for $\left[\begin{smallmatrix}\delta\\ \varepsilon\end{smallmatrix}\right] \in \mathbb{F}_2^6$ and $\delta\,\varepsilon^t = 0$ and build the set $V(A_f)$. As an abbreviation we use *binary notation* (by rows) for the theta constants; for example, the theta constant $\theta\left[\begin{smallmatrix}1&0&0\\0&0&0\end{smallmatrix}\right](\Omega_f)$ will be denoted by $\theta[4,0](\Omega_f)$.

In Step 2 we notice that because of $V(A_f) = \{\theta[5,5](\Omega_f)\}$ (this has been proven numerically) our condition $\#V(A_f) = n(g) = 1$ is fulfilled.

The canonical azygetic fundamental system $\eta = \{\eta_1^0, \ldots, \eta_7^0\}$ for Step 3 is given by

$$\eta_1^0 = \begin{bmatrix}1&0&0\\0&0&0\end{bmatrix},\quad \eta_2^0 = \begin{bmatrix}1&0&0\\1&0&0\end{bmatrix},\quad \eta_3^0 = \begin{bmatrix}0&1&0\\1&0&0\end{bmatrix},$$
$$\eta_4^0 = \begin{bmatrix}0&1&0\\1&1&0\end{bmatrix},\quad \eta_5^0 = \begin{bmatrix}0&0&1\\1&1&0\end{bmatrix},\quad \eta_6^0 = \begin{bmatrix}0&0&1\\1&1&1\end{bmatrix},$$
$$\eta_7^0 = \begin{bmatrix}0&0&0\\1&1&1\end{bmatrix},$$

and shows us that the vanishing set $W(A_f, \eta^0) = \{\theta[7,5](\Omega_f)\}$ and the set $V(A_f)$ are different. By a computer search we find a transformation matrix $\gamma \in \mathrm{Sp}_6(\mathbb{F}_2)$ with

$$\gamma = \begin{pmatrix}0&0&1&0&0&0\\0&1&1&0&0&0\\1&0&0&0&0&0\\0&0&0&0&1&1\\0&0&0&0&1&0\\0&0&0&1&0&0\end{pmatrix}$$

and $\gamma \circ \eta^0 = \tilde{\eta} = \{\tilde{\eta}_1, \ldots, \tilde{\eta}_7\}$ for

$$\tilde{\eta}_1 = \begin{bmatrix}0&0&1\\0&0&0\end{bmatrix},\quad \tilde{\eta}_2 = \begin{bmatrix}0&0&1\\0&0&1\end{bmatrix},\quad \tilde{\eta}_3 = \begin{bmatrix}0&1&0\\0&0&1\end{bmatrix},$$
$$\tilde{\eta}_4 = \begin{bmatrix}0&1&0\\1&1&1\end{bmatrix},\quad \tilde{\eta}_5 = \begin{bmatrix}1&1&0\\1&1&1\end{bmatrix},\quad \tilde{\eta}_6 = \begin{bmatrix}1&1&0\\0&1&1\end{bmatrix},$$
$$\tilde{\eta}_7 = \begin{bmatrix}0&0&0\\0&1&1\end{bmatrix}$$

such that $W(A_f, \tilde{\eta}) = \{\theta[5,5](\Omega_f)\} = V(A_f)$. So we can produce the output YES and stop.

To apply Algorithm 3.4 we choose the sets

$$S_1^1=\{1,2,4,6\},\ S_2^1=\{1,2,5,7\},\ S_3^1=\{1,3,4,6\},$$
$$S_4^1=\{1,3,5,7\},\ S_5^1=\{2,3,4,6\},\ S_6^1=\{2,3,5,7\},$$
$$S_1^2=\{1,2,3,5\},\ S_2^2=\{1,2,6,7\},\ S_3^2=\{1,4,3,5\},$$
$$S_4^2=\{1,4,6,7\},\ S_5^2=\{2,4,3,5\},\ S_6^2=\{2,4,6,7\},$$
$$S_1^3=\{1,2,3,4\},\ S_2^3=\{1,2,6,7\},\ S_3^3=\{1,5,3,4\},$$
$$S_4^3=\{1,5,6,7\},\ S_5^3=\{2,5,3,4\},\ S_6^3=\{2,5,6,7\},$$
$$S_1^4=\{1,2,3,4\},\ S_2^4=\{1,2,5,7\},\ S_3^4=\{1,6,3,4\},$$
$$S_4^4=\{1,6,5,7\},\ S_5^4=\{2,6,3,4\},\ S_6^4=\{2,6,5,7\},$$
$$S_1^5=\{1,2,3,5\},\ S_2^5=\{1,2,4,6\},\ S_3^5=\{1,7,3,5\},$$
$$S_4^5=\{1,7,4,6\},\ S_5^5=\{2,7,3,5\},\ S_6^5=\{2,7,4,6\}.$$

Then the roots $\lambda_1,\dots,\lambda_5$ of the Rosenhain model (3–1) have the numerical values shown in the table below. The associated binary form

$$F(X,Y)=X(X-Y)\prod_{i=1}^{5}(X-\lambda_i Y)$$

corresponds to a moduli point $\mathcal{C}\in\mathcal{H}_3(\mathbb{Q})$ with trivial automorphism group (in the case of real multiplication the automorphism group is always simple since there are no nontrivial roots of unity in $\mathbb{E}_f$).

This Rosenhain model is then fed into Algorithm 4.6. In Step 1 we define the three covariants $\psi_1=(k,m)_3\in\mathcal{K}_3(2,5)(\mathbb{C})$, $\psi_2=(k,\psi_1)_2\in\mathcal{K}_3(2,7)(\mathbb{C})$ and $\psi_3=(k,\psi_2)_2\in\mathcal{K}_3(2,9)(\mathbb{C})$ with the help of the covariants $k=(\mathcal{F},\mathcal{F})_6\in\mathcal{K}_3(4,2)(\mathbb{C})$ and $m=(\mathcal{F},k)_4\in\mathcal{K}_3(4,3)(\mathbb{C})$. For the überschiebung we use the parameter $\lambda=1/(h!)^2$. Then we get with $I_2=(\mathcal{F},\mathcal{F})_8\in\mathcal{I}_3(2)(\mathbb{C})$ the embedded coefficients

$$Q_{l,m}\mapsto\frac{Q_{l,m}\,I_2^{11-(l+m)}}{\Delta_3^2},\quad\text{for } l,m=1,2,3,$$

as elements in the algebra $\mathcal{I}_3[\Delta_3^{-1}]_0(\mathbb{C})$; we denoted them by $Q_{l,m}$ as well.

Using the procedure `isolve` in Maple we get in Step 2 the irreducible quadratic form $Q(Z_1,Z_2,Z_3)$ in the diagonalized representation shown at the top of the next page. Therefore we output YES, meaning that C has an affine model over $\mathbb{Q}$.

For Step 3 we compute the embedded coefficients (fixing the same notation) of the curve $\mathcal{V}(H)$ by using the embedding

$$H_{l_1,\dots,l_4}\mapsto\frac{H_{l_1,\dots,l_4}\,I_5\,I_2^{12-(l_1+l_2+l_3+l_4)}}{\Delta_3^3}$$

with invariant $I_5=(k,m)_4\in\mathcal{I}_3(5)(\mathbb{C})$. Using the coordinates Z_1,Z_2,Z_3 for X_1,X_2,X_3 that have diagonalized the quadratic form, we plug in the parametrization and get the squarefree polynomial $h^{(3)}(T)$ given at the bottom of the next page.

$$\lambda_1=\frac{(\theta[1,0](\Omega_f)\,\theta[3,0](\Omega_f))^4+(\theta[0,0](\Omega_f)\,\theta[2,0](\Omega_f))^4-(\theta[0,1](\Omega_f)\,\theta[2,1](\Omega_f))^4}{2\,(\theta[1,0](\Omega_f)\,\theta[3,0](\Omega_f))^4}=0.83032-2.04464i,$$

$$\lambda_2=\frac{(\theta[1,2](\Omega_f)\,\theta[3,4](\Omega_f))^4+(\theta[0,2](\Omega_f)\,\theta[2,4](\Omega_f))^4-(\theta[0,3](\Omega_f)\,\theta[2,5](\Omega_f))^4}{2\,(\theta[1,2](\Omega_f)\,\theta[3,4](\Omega_f))^4}=2.41472-1.37352i,$$

$$\lambda_3=\frac{(\theta[5,2](\Omega_f)\,\theta[3,4](\Omega_f))^4+(\theta[4,2](\Omega_f)\,\theta[2,4](\Omega_f))^4-(\theta[4,3](\Omega_f)\,\theta[2,5](\Omega_f))^4}{2\,(\theta[5,2](\Omega_f)\,\theta[3,4](\Omega_f))^4}=-1.37026-0.83267i,$$

$$\lambda_4=\frac{(\theta[5,2](\Omega_f)\,\theta[3,0](\Omega_f))^4+(\theta[4,2](\Omega_f)\,\theta[2,0](\Omega_f))^4-(\theta[4,3](\Omega_f)\,\theta[2,1](\Omega_f))^4}{2\,(\theta[5,2](\Omega_f)\,\theta[3,0](\Omega_f))^4}=-0.15599-1.87981i,$$

$$\lambda_5=\frac{(\theta[1,2](\Omega_f)\,\theta[1,0](\Omega_f))^4+(\theta[0,2](\Omega_f)\,\theta[0,0](\Omega_f))^4-(\theta[0,3](\Omega_f)\,\theta[0,1](\Omega_f))^4}{2\,(\theta[1,2](\Omega_f)\,\theta[1,0](\Omega_f))^4}=2.45210-0.92310i.$$

Roots of the Rosenhain model (3–1) for the example of Section 5.1.

$Q(Z_1, Z_2, Z_3) = -310146482690273725409\, Z_1^2 + Z_2^2 + 113922743\, Z_3^2$,with squarefree coefficients

$$Z_1 = h_1(T) = 5408438734746610874028937383516975917117472 + 4747461825727467669935701410838 5504\, T^2,$$

$$\begin{aligned} Z_2 = h_2(T) = {}& 8809329785683051821276348234733072017105390568980 4927 \\ & -678651961493008988289890255769069630959995973463 4\, T - 77327226800385694902696893760125421287524568 9\, T^2, \end{aligned}$$

$$\begin{aligned} Z_3 = h_3(T) = {}& -3393259807465044941449451278845348154799979867317 \\ & -1546544536007713898053937875202508425750491378\, T + 2978562241487676382098218332791853646641 9\, T^2. \end{aligned}$$

Quadratic form produced by Step 2 of Algorithm 4.6 for the example of Section 5.1.

The factorization of the discriminant in Step 4, which has over 2000 digits, was carried out using the computer algebra program LiDIA [1996]. We get $\Delta_3(h^{(3)}(T)) = -2^{236}\, m^{56}\, 71^3$, with

$$m = 3 \cdot 11 \cdot 59 \cdot 67 \cdot 79 \cdot 149 \cdot 1993 \cdot 7187 \cdot 45757 \cdot 16215770450329.$$

Finally, after minimizing this polynomial in Steps 5, 6, and 7, we get an affine model

$$Y^2 = g(T) = T^7 + 3T^6 + 2T^5 - T^4 - 2T^3 - 2T^2 - T - 1$$

for our moduli point $C \in \mathcal{H}_3(\mathbb{Q})$ with $\mathcal{J}_C \cong_{\mathbb{C}} A_f$.

We have investigated 228 three-dimensional simple factors of $J_0(N)$ up to level $N \leq 500$. Only 26 of them were principally polarized. For those factors that are isomorphic to hyperelliptic jacobians of dimension $g = 3$ we have computed the corresponding curve equations with endomorphism fields $\mathbb{E}_f = \mathrm{End}(A_f) \otimes \mathbb{Q}$ (f denotes here a newform); see Table 1. Our result for $N = 41$ is the same one that appears in [Gonzàlez Rovira 1991;

$h^{(3)}(T) = \sum_{i=0}^{8} h_i^{(3)} T^i \in \mathbb{Z}[T]$, with coefficients

$$\begin{aligned}
h_0^{(3)} &= -124106094710662863340822193234454568071760054258264696428674415577551963836959258872941789\backslash \\ &\qquad 364518841252980669498433795610746275444834342956742139545374780761457 \\
h_1^{(3)} &= -289422967350034912763544130861983992324886848261913393813342090615151077677987075884065004\backslash \\ &\qquad 3454719607674177045023834521821141256574221013218573277132193047 2 \\
h_2^{(3)} &= -290576948995281531407381833896198365369397073243460940310410783006943147014187581943094580\backslash \\ &\qquad 0957829239217185536059666334676678892182574441454273676261388 12 \\
h_3^{(3)} &= 545485656312720261658668387978285496873098732561291294620283260390367935912590603344031205\backslash \\ &\qquad 318845192839825071491392301081283578908740006428287181450 00 \\
h_4^{(3)} &= -538066929523204341945650993919758180851690142972368856289656737999525931488063312198414458\backslash \\ &\qquad 69154050472455044508650092315945426433508854847214556 86 \\
h_5^{(3)} &= 790987028435054085783060904170360181468862221473517625495854403566263530462619899648934171\backslash \\ &\qquad 54241069390269503260365010166118239588650881347639 2 \\
h_6^{(3)} &= -513961847531856347240393860381315890092669916607668216423675988960751605597684364873850531\backslash \\ &\qquad 8162557891826479015620669402185996916506481420 4 \\
h_7^{(3)} &= 221540933088014339204476848833284885332655901902118189341769144664641839349319103761445514\backslash \\ &\qquad 631798792141227274859246713537356082731682 4 \\
h_8^{(3)} &= -574135797825075316615253152523804806529259507348984589893321192177271150962633975074782362\backslash \\ &\qquad 377516749118014555877572926934225668 01
\end{aligned}$$

Polynomial produced by Step 3 of Algorithm 4.6 for the example of Section 5.1.

$N = 41$ curve $= Y^2 = X^8 + 4X^7 - 8X^6 - 66X^5 - 120X^4 - 56X^3 + 53X^2 + 36X - 16$ $\Delta_3 = (-1) \cdot 2^{16} \cdot 41^6$ $\mathbb{E}_f = \mathbb{Q}(\beta)$, with $\beta^3 + \beta^2 - 5\beta - 1 = 0$ $D = 148 = 2^2 \cdot 37$
$N = 95 = 5 \cdot 19$ curve $= Y^2 = 19X^8 - 262X^7 + 1507X^6 - 4784X^5 + 9202X^4 - 10962X^3 + 7844X^2 - 3040X + 475$ $\Delta_3 = 2^{16} \cdot 5^6 \cdot 19^4$ $\mathbb{E}_f = \mathbb{Q}(\beta)$, with $\beta^3 - \beta^2 - 3\beta + 1 = 0$ $D = 148 = 2^2 \cdot 37$
$N = 284 = 2^2 \cdot 71$ curve $= Y^2 = X^7 + 3X^6 + 2X^5 - X^4 - 2X^3 - 2X^2 - X - 1$ $\Delta_3 = (-1) \cdot 71^3$ $\mathbb{E}_f = \mathbb{Q}(\beta)$, with $\beta^3 + 3\beta^2 - 3 = 0$ $D = 81 = 3^4$
$N = 385 = 5 \cdot 7 \cdot 11$ curve $= Y^2 = X^8 + 12X^7 + 68X^6 + 114X^5 + 282X^4 + 176X^3 - 123X^2 - 170X + 25$ $\Delta_3 = (-1) \cdot 2^{16} \cdot 5^4 \cdot 7^{19} \cdot 11^6$ $\mathbb{E}_f = \mathbb{Q}(\beta)$, with $\beta^3 + 4\beta^2 + 2\beta - 2 = 0$ $D = 148 = 2^2 \cdot 37$

TABLE 1. Hyperelliptic curves of genus 3 with real multiplication.

Shimura 1995]. More detailed tables can be found in [Weber 1996].

5.2. Four-Dimensional Factors of $J_0(N)$

In this section we mention only the main algorithmic differences from the case $g = 3$. If we consider a generic four-dimensional hyperelliptic factor A_f of $J_0(N)$, the corresponding vanishing set $W(A_f, \eta^0)$ consists of 10 even theta constants, namely,

$$\theta[13,9](\Omega_f),\ \theta[7,5](\Omega_f),\ \theta[14,11](\Omega_f),\ \theta[7,13](\Omega_f),$$
$$\theta[11,13](\Omega_f),\ \theta[15,5](\Omega_f),\ \theta[14,10](\Omega_f),$$
$$\theta[13,11](\Omega_f),\ \theta[15,10](\Omega_f),\ \theta[11,9](\Omega_f)$$

(recall the binary notation for thetas on page 281). We define covariants $\psi_1 = (\mathcal{F}, k)_8 \in \mathcal{K}_4(2,3)(\mathbb{C})$, $\psi_2 = (m, \psi_1)_2 \in \mathcal{K}_4(2,5)(\mathbb{C})$, and $\psi_3 = (m, \psi_2)_2 \in \mathcal{K}_4(2,7)(\mathbb{C})$ with the help of the covariants

$$k = (\mathcal{F}, \mathcal{F})_6 \in \mathcal{K}_4(8,2)(\mathbb{C}),$$
$$m = (\mathcal{F}, \mathcal{F})_8 \in \mathcal{K}_4(4,2)(\mathbb{C}),$$

and choose for the überschiebung the parameter value $\lambda = (h-1)!/(h!)^3$. Using the invariant $I_2 = (\mathcal{F}, \mathcal{F})_{10} \in \mathcal{I}_4(2)(\mathbb{C})$ we get an embedding

$$Q_{l,m} \mapsto \frac{Q_{l,m} \cdot I_2^{8-(l+m)}}{\Delta_4}$$

for $l, m = 1, 2, 3$ into the algebra $\mathcal{I}_4[\Delta_4^{-1}]_0(\mathbb{C})$. The embedding of the coefficients of the curve $\mathcal{V}(H)$ of degree 5 has the form

$$H_{l_1,\ldots,l_5} \mapsto \frac{H_{l_1,\ldots,l_5} \cdot I_2^{15-(l_1+l_2+l_3+l_4+l_5)}}{\Delta_4^2},$$

for $l_1, \ldots, l_5 = 1, 2, 3$. We found 114 four-dimensional simple factors of $J_0(N)$ up to level $N \leq 500$, and 11 of them were principally polarized. Table 2 includes all curve equations with endomorphism

$N = 47$ $\text{curve} = Y^2 = X^{10} + 6X^9 + 11X^8 + 24X^7 + 19X^6 + 16X^5 - 13X^4 - 30X^3 - 38X^2 - 28X - 11$ $\Delta_4 = 2^{20} \cdot 47^8$ $\mathbb{E}_f = \mathbb{Q}(\beta),\ \text{with } \beta^4 - \beta^3 - 5\beta^2 + 5\beta - 1 = 0$ $D = 1957 = 19 \cdot 103$
$N = 119 = 7 \cdot 17$ $\text{curve} = Y^2 = X^{10} + 2X^8 - 11X^6 - 14X^5 - 40X^4 - 42X^3 - 48X^2 - 28X - 7$ $\Delta_4 = 2^{20} \cdot 7^6 \cdot 17^6$ $\mathbb{E}_f = \mathbb{Q}(\beta),\ \text{with } \beta^4 + \beta^3 - 5\beta^2 - \beta + 3 = 0$ $D = 9301 = 71 \cdot 131$

TABLE 2. Hyperelliptic curves of genus 4 with real multiplication.

$N = 59$ $\text{curve} = Y^2 = X^{12} + 8X^{11} + 22X^{10} + 28X^9 + 3X^8 - 40X^7 - 62X^6 - 40X^5 - 3X^4 + 24X^3 + 20X^2 + 4X - 8$ $\Delta_5 = (-1) \cdot 2^{24} \cdot 59^9$ $\mathbb{E}_f = \mathbb{Q}(\beta),\ \text{with } \beta^5 - 9\beta^3 + 2\beta^2 + 16\beta - 8 = 0$ $D = 138136 = 2^3 \cdot 31 \cdot 557$

TABLE 3. Hyperelliptic curve of genus 5 with real multiplication.

fields $\mathbb{E}_f = \text{End}(A_f) \otimes \mathbb{Q}$ (f denoting a newform) up to level $N \leq 500$. Our result for $N = 47$ is the same one found in [Fricke 1924–28, p. 491; Gonzàlez Rovira 1991; Shimura 1995].

5.3. Five-Dimensional factors of $J_0(N)$

Our method is theoretically useful for all $g \in \mathbb{N}$. In practice we're restricted to the case $g \leq 5$ since the computation of the even theta constants requires in practice a precision of approximately $50\,g$ digits and a great deal of computing time already for $g = 5$ (roughly 55 hours per theta constant on a parallel IBM SP1 with four processors).

The rarity of hyperelliptic factors of $J_0(N)$ for genus $g \geq 5$ is another reason for the restriction to $g \leq 5$. Up to level $N \leq 800$ we found only the five-dimensional simple factor $J_0(59)$, which belongs to the classical hyperelliptic modular curve $X_0(59)$; see Table 3.

We discuss with the algorithmic differences between the case $g = 5$ and the preceding ones. The vanishing set $W(A_f, \eta^0)$ of a generic hyperelliptic factor A_f of $J_0(N)$ consists of 66 even theta constants, corresponding to the following pairs, where (i, j) stands for $\theta[i, j](\Omega_f)$:

$$(30,11), (15,10), (27,9), (15,5), (14,10), (28,20),\\ (11,29), (31,10), (29,20), (22,19), (7,29), (13,27),\\ (26,22), (19,17), (31,20), (28,21), (13,9), (25,21),\\ (26,23), (21,25), (31,5), (14,26), (29,11), (15,21),\\ (25,19), (30,20), (7,5), (21,19), (19,25), (25,23),\\ (30,21), (25,17), (27,22), (28,22), (13,11), (28,23),\\ (11,9), (19,29), (15,26), (23,5), (11,13), (31,23),\\ (23,18), (21,17), (7,21), (30,10), (14,27), (14,11),\\ (26,18), (21,27), (27,13), (23,13), (7,13), (11,25),\\ (29,9), (27,18), (31,17), (26,19), (22,27), (23,26),\\ (31,29), (13,25), (19,21), (22,18), (22,26), (29,22).$$

To define the embedded coefficients of the conic $\mathcal{V}(Q)$ and the curve $\mathcal{V}(H)$ of degree 6 we need the covariants $\psi_1 = (m, n)_3 \in \mathcal{K}_5(2,5)(\mathbb{C})$, $\psi_2 = (n, \psi_1)_2 \in \mathcal{K}_5(2,7)(\mathbb{C})$, and

$$\psi_3 = (n, \psi_2)_2 \in \mathcal{K}_5(2,9)(\mathbb{C}),$$

with

$$k = (\mathcal{F}, \mathcal{F})_6 \in \mathcal{K}_5(12,2)(\mathbb{C}),$$
$$m = (\mathcal{F}, k)_{10} \in \mathcal{K}_5(4,3)(\mathbb{C}),$$
$$n = (\mathcal{F}, \mathcal{F})_{10} \in \mathcal{K}_5(4,3)(\mathbb{C}).$$

For the überschiebung we choose the parameter value $\lambda = 1/(h!)^2$. Then with the help of the invariant $I_2 = (\mathcal{F}, \mathcal{F})_{12} \in \mathcal{I}_5(2)(\mathbb{C})$ we get the embedding

$$Q_{l,m} \mapsto \frac{Q_{l,m}\, I_2^{8-(l+m)}}{\Delta_5}$$

for $l, m = 1, 2, 3$ into the algebra $\mathcal{I}_5[\Delta_5^{-1}]_0(\mathbb{C})$. The other embedded coefficients have the form

$$H_{l_1,\dots,l_6} \mapsto \frac{H_{l_1,\dots,l_6}\, I_3\, I_2^{22-(l_1+l_2+l_3+l_4+l_5+l_6)}}{\Delta_5^3},$$

for $l_1, \dots, l_6 = 1, 2, 3$, with the invariant

$$I_3 = (\mathcal{F}, \mathcal{F})_6 \in \mathcal{I}_5(3)(\mathbb{C}).$$

Our result for $N = 59$ (see Table 3) is the same one found in [Gonzàlez Rovira 1991; Shimura 1995].

ACKNOWLEDGEMENTS

This paper is based on some parts of my thesis [Weber 1996] and I thank my advisor Prof. G. Frey for his help and encouragement. Another thank you is due to M. Müller and X. Wang for their programs and useful discussions and to the anonymous reviewers for their useful comments. All the numerical results were achieved by the use of the computer algebra systems Pari [Batut et al. 1995], LiDIA [LiDIA 1996] and Maple.

REFERENCES

[Batut et al. 1995] C. Batut, D. Bernardi, H. Cohen, and M. Olivier, *User's Guide to Pari-GP* 1.39, Université de Bordeaux, 1995. See ftp://megrez.math.u-bordeaux.fr/pub/pari.

[Clebsch 1872] A. Clebsch, *Theorie der binären algebraischen Formen*, Teubner, Leipzig, 1872.

[Deligne and Mumford 1969] P. Deligne and D. Mumford, "The irreducibility of the space of curves of given genus", *Publ. Math. Inst. Hautes Études Sci.* **36** (1969), 75–109.

[Fricke 1924–28] R. Fricke, *Lehrbuch der Algebra*, Vieweg, Braunschweig, 1924–28.

[Geyer 1974] W. D. Geyer, "Invarianten binärer Formen", pp. 36–69 in *Classification of algebraic varieties and compact complex manifolds*, edited by H. Popp, Lecture Notes in Math. **412**, Springer, Berlin, 1974.

[Gonzàlez Rovira 1991] J. Gonzàlez Rovira, "Equations of hyperelliptic modular curves", *Ann. Inst. Fourier* (*Grenoble*) **41**:4 (1991), 779–795.

[Igusa 1972] J.-I. Igusa, *Theta Functions*, Springer, Berlin, Heidelberg, New York, 1972.

[Krazer 1903] A. Krazer, *Lehrbuch der thetafunktionen*, Teubner, Leipzig, 1903. Reprinted by Chelsea, New York, 1970.

[Lang 1959] S. Lang, *Abelian varieties*, Interscience Tracts in Pure and Applied Mathematics, Interscience Publishers, New York, 1959. Reprinted by Springer, New York, 1983.

[LiDIA 1996] T. L. Group, "LiDIA: a C++ library for computational number theory", software, Technische Universität Darmstadt, Darmstadt, Germany, 1996. See http://www.informatik.th-darmstadt.de/TI/LiDIA.

[Mestre 1991] J.-F. Mestre, "Construction de courbes de genre 2 à partir de leurs modules", pp. 313–334 in *Effective methods in algebraic geometry* (Castiglioncello, 1990), edited by T. Mora and C. Traverso, Progr. Math. **94**, Birkhäuser, Boston, 1991.

[Mordell 1969] L. J. Mordell, *Diophantine equations*, Pure and Applied Mathematics **30**, Academic Press, London, 1969. Reprinted by Chelsea, New York, 1970.

[Mumford 1983] D. Mumford, *Tata Lectures on Theta II*, Birkhäuser, Boston, 1983.

[Ogg 1974] A. P. Ogg, "Hyperelliptic modular curves", *Bull. Soc. Math. France* **102** (1974), 449–462.

[Poor 1994] C. Poor, "The hyperelliptic locus", *Duke Math. J.* **76**:3 (1994), 809–884.

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan **11**, Princeton University Press and Iwanami Shoten, Tokyo, 1971.

[Shimura 1995] M. Shimura, "Defining equations of modular curves $X_0(N)$", *Tokyo J. Math.* **18**:2 (1995), 443–456.

[Vinberg and Popov 1994] È. B. Vinberg and V. L. Popov, "Invariant theory", pp. 123–278 in *Algebraic geometry IV*, edited by A. N. Parshin and I. R. Shafarevich, Encycl. of Math. Sc. **55**, Springer, Berlin, 1994.

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

[Weber 1996] H.-J. Weber, *Algorithmische Konstruktion hyperelliptischer Kurven mit kryptographischer Relevanz und einem Endomorphismenring echt größer als* $\mathbb{Z}$, Dissertation, Essen University, 1996.

Hermann-Josef Weber, Mannesmann Information Technology, Theodorstraße 90, 40472 Düsseldorf, Germany (hermann-josef.weber@it-mannesmann.de)

Received December 2, 1996; accepted in revised form June 6, 1997