London Mathematical Society ISSN 1461–1570

MODULAR POLYNOMIALS FOR GENUS 2

REINIER BRÖKER AND KRISTIN LAUTER

Abstract

Modular polynomials are an important tool in many algorithms involving elliptic curves. In this article we investigate their generalization to the genus 2 case following pioneering work by Gaudry and Dupont. We prove various properties of these genus 2 modular polynomials and give an improved way to explicitly compute them.

1. *Introduction*

The ‘classical’ modular polynomial $\Phi_N \in \mathbf{Z}[X, Y]$ was introduced by Kronecker more than 100 years ago. The polynomial Φ_N is a model for the modular curve $Y_0(N)$ parametrizing cyclic N-isogenies between elliptic curves. As is shown in the examples below, the explicit computation of Φ_N has led to various speed ups in algorithms using elliptic curves.

Examples. 1. Schoof’s original algorithm [25] to count the number of points on an elliptic curve $E/\mathbf{F}_p$ was rather impractical as one had to compute with the *complete* l-torsion of E for various small primes $l \neq p$. The key to the improvements made by Atkin and Elkies [24, Sec. 6–8] is to work with a one-dimensional eigenspace of the Frobenius action on $E[l] \cong \mathbf{Z}/l\mathbf{Z} \times \mathbf{Z}/l\mathbf{Z}$. Instead of using division polynomials of degree $(l^2 - 1)/2$ one can now use the modular polynomial Φ_l of degree $l + 1$. The ‘Schoof-Elkies-Atkin’-algorithm behaves very well in practice, and primes p of several thousand digits are now feasible [13].

2. Both the primality proving algorithm ECPP [9, Sec. 14D] and efficient constructions of cryptographically secure elliptic curves [8, Ch. 18] rely on the computation of the Hilbert class polynomial $H_{\mathcal{O}}$ for a certain imaginary quadratic order $\mathcal{O}$. At the moment, the fastest known algorithm to compute $H_{\mathcal{O}} \in \mathbf{Z}[X]$ is to first compute its reduction modulo various primes p and then apply the Chinese remainder theorem [4, 28]. If we know one root of $H_{\mathcal{O}}$ in $\mathbf{F}_p$, then we can compute the other roots by exploiting the modular polynomials Φ_l for small primes l generating the class group of $\mathcal{O}$. This observation is crucial to the practical behaviour of the ‘CRT-algorithm’.

The algorithms in the examples above have analogues for genus 2, see [15, 12]. Whereas the situation in well understood in genus 1 and algorithms are fast, the computations are still in their infancies in genus 2. Typically, algorithms only terminate in a reasonable amount of time for very small examples. Inspired by the

Received 9 April 2008, revised 4 February 2009; *published* 22 November 2009.
2000 Mathematics Subject Classification 11G18, 14J99

https://doi.org/10.1112/S1461157000001546 Published online by Cambridge University Press

speed ups modular polynomials give in the genus 1 case, we investigate modular polynomials for genus 2 in this paper.

In [17], Gaudry and Schost examine a tailor-made variant of Φ_N in genus 2 to improve point counting on genus 2 curves over finite fields. The polynomial they construct has factorization properties similar to Φ_N, and this enables them to speed up point counting in genus 2 in the spirit of the improvements made by Atkin and Elkies in the genus 1 case.

In this paper, we consider a 'direct' generalization of Φ_N to genus 2. Such a generalization was first defined by Gaudry in his PhD-thesis [14, Ch. 3]. Whereas we have one polynomial Φ_N in the genus 1 case, we now get 3 polynomials P_N, Q_N, R_N for every $N \geqslant 2$. At the time, it was not possible to *explicitly compute* these polynomials P_N, Q_N, R_N in the simplest case $N = 2$. Dupont considered the problem of computing the modular polynomials in this thesis [10, Sec. 10.4] as well. He was able to compute them for $N = 2$, and he gives some partial results for $N = 3$. The resulting polynomials are *huge*. Nevertheless, knowing just a few modular polynomials will speed up the 'CRT-algorithm' [12] to compute class fields of degree 4 CM-fields. This in turn will lead to faster algorithms to construct cryptographically secure Jacobians of hyperelliptic curves. This paper solely focuses on the definitions and properties of modular polynomials for genus 2 however.

We reconsider the polynomials defined by Gaudry and Dupont in this article. We will mostly restrict to the case that $N = p$ is prime. By combining the function field approach of Gaudry with finite symplectic geometry over $\mathbf{F}_p$, we are able to prove Gaudry's conjecture on the degree of the modular polynomials. Furthermore, we prove that the polynomials P_p, Q_p, R_p have coefficients in $\mathbf{Q}(j_1, j_2, j_3)$. We also give a heuristic in Section 6 implying that the bit size of the polynomial P_p grows like p^{12}. We extend Dupont's results in the following way: the algorithm in [10] requires 'guessing' the denominator of the coefficients of P_p, Q_p, R_p. In Section 6 we prove that the denominator is closely linked to the *Humbert surface* of discriminant p^2 describing (p, p)-split Jacobians. Our result considerably helps the computation.

The structure of this article is as follows. After recalling some classical facts on polarized abelian varieties in Section 2, we consider level structures in Section 3, and for primes p we define the 2-dimensional analogue $Y_0^{(2)}(p)$ of the modular curve $Y_0(p)$. In Section 4 we consider functions on $Y_0^{(2)}(p)$ and this leads naturally to the definition of the genus 2 modular polynomials. We explain the moduli interpretation behind P_p, Q_p, R_p, and compute their degrees. By studying the 'Fourier coefficients' of the Igusa j-functions, we show in Section 5 that the genus 2 modular polynomials have rational coefficients. Section 6 focuses on the *computation* of the modular polynomials. In the special case $p = 2$, the modular polynomials are closely linked to the *Richelot isogeny*. We explain the precise relation in Section 7.

2. *Polarized abelian varieties*

We recall some classical facts about complex abelian varieties. For modular polynomials we are only interested in the 2-dimensional case, but as much of the theory generalizes, we work in arbitrary dimension $g \geqslant 1$ in this section.

Let $A/\mathbf{C}$ be a g-dimension abelian variety, and write $A^\vee = \mathrm{Pic}^0(A)$ for its dual. It is well known that every abelian variety admits a *polarization*, i.e., an isogeny

https://doi.org/10.1112/S1461157000001546 Published online by Cambridge University Press

$\varphi : A \to A^\vee$. If φ is an isomorphism, we call A principally polarized. The Jacobian of a curve is the classical example of a principally polarized abelian variety: the choice of a base point on the curve determines a principal polarization.

The complex points $A(\mathbf{C})$ have the natural structure of a g-dimensional complex torus $\mathbf{C}^g/L$. Here, $L \subset \mathbf{C}^g$ is a full lattice. In order to characterize those complex tori $\mathbf{C}^g/L$ that arise as abelian varieties, we define the polarization of a torus. We follow the classical approach via Riemann forms. A skew-symmetric form $E : L \times L \to \mathbf{Z}$ can be extended to a form $E : \mathbf{C}^g \times \mathbf{C}^g \to \mathbf{R}$, and we call E a *Riemann form* if

1. $E(x, y) = E(ix, iy)$ for all $x, y \in \mathbf{C}^g$
2. the Hermitian form $H(x, y) = E(ix, y) + iE(x, y)$ is positive definite.

A torus $\mathbf{C}^g/L$ is called polarizible if it admits a Riemann form. The link with the definition from the previous paragraph is that the Hermitian form H from condition 2 defines a map

$$\varphi_E : (\mathbf{C}^g/L) \longrightarrow (\mathbf{C}^g/L)^\vee$$

sending x to $H(x, \cdot)$. If φ_E is an isomorphism, we say that the torus $\mathbf{C}^g/L$ is principally polarized. The following theorem describes the precise connection between complex abelian varieties and polarizable tori.

THEOREM 2.1. *The category of complex abelian varieties is equivalent to the category of polarizable tori via the functor $A \to A(\mathbf{C})$.*

Proof. See [5, Ch. 4]. □

Let L be a full lattice in $\mathbf{C}^g$ such that the torus $\mathbf{C}^g/L$ is principally polarizable. One can choose a basis of L such that L is given by $\mathbf{Z}^g + \mathbf{Z}^g\tau$ with τ a complex $g \times g$-matrix. The fact that the lattice admits a Riemann form now translates into the fact that τ is an element of the g-dimensional *Siegel upper half plane*

$$\mathbf{H}_g = \{\tau \in \mathrm{Mat}_g(\mathbf{C}) \mid \tau^T = \tau, \mathrm{Im}(\tau) \text{ positive definite}\}.$$

Conversely, for $\tau \in \mathbf{H}_g$ the torus $\mathbf{C}^g/(\mathbf{Z}^g + \mathbf{Z}^g\tau)$ is principally polarizable. The Hermitian form given by $H(x, y) = x\mathrm{Im}(\tau)^{-1}\overline{y}^T$ is by construction positive definite, and the Riemann form is given by $E(x, y) = \mathrm{Im}(H(x, y))$.

Next we consider what happens if we change a basis for the $2g$-dimensional polarized lattice L. By the ‘elementary divisor theorem’, we can choose a basis for L such that the Hermitian form $H : L \times L \to \mathbf{Z}$ is given by the matrix

$$J = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}$$

where 1_g denotes the $g \times g$ identity matrix. The general linear group $\mathrm{GL}(2g, \mathbf{Z})$ stabilizes the lattice L, and the subgroup

$$\mathrm{Sp}(2g, \mathbf{Z}) = \{M \in \mathrm{GL}(2g, \mathbf{Z}) \mid MJM^T = J\} \subseteq \mathrm{GL}(2g, \mathbf{Z})$$

that respects the Hermitian form is called the *symplectic group*. Explicitly, a matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2g, \mathbf{Z})$ is symplectic if and only if the $g \times g$ matrices a, b, c, d satisfy the relations $ab^T = b^Ta$, $cd^T = d^Tc$ and $ad^T - bc^T = 1_g$.

https://doi.org/10.1112/S1461157000001546 Published online by Cambridge University Press

For $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}(2g, \mathbf{Z})$ and $\tau \in \mathbf{H}_g$, the $g \times g$-matrix $c\tau + d$ is invertible. Indeed, if $c\tau + d$ had determinant zero, there would be an element $y \in \mathbf{C}^g$ with $y\mathrm{Im}(\tau)y^T = 0$, contradicting that $\mathrm{Im}(\tau)$ is positive definite. We define an action of the symplectic group $\mathrm{Sp}(2g, \mathbf{Z})$ on the Siegel upper half plane $\mathbf{H}_g$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}, \tag{2.1}$$

where dividing by $c\tau + d$ means multiplying on the right with the multiplicative inverse of the $g \times g$-matrix $c\tau + d$. An explicit check shows that the right hand side of (2.1) indeed lies in $\mathbf{H}_g$.

The map

$$\tau \mapsto A_\tau = \mathbf{C}^g / (\mathbf{Z}^g + \mathbf{Z}^g \tau).$$

induces a canonical bijection between the quotient space $\mathcal{A}_g = \mathrm{Sp}(2g, \mathbf{Z}) \backslash \mathbf{H}_g$ and the set of isomorphism classes of principally polarized g-dimensional abelian varieties. In fact, the space $\mathcal{A}_g$ is a *coarse* moduli space for principally polarized abelian varieties of dimension g.

We close this section by zooming in on the 1-dimensional case, i.e., the case of elliptic curves. An elliptic curve is isomorphic to its dual, so polarizations do not play a real role here. Indeed, every complex torus is polarizable, and the Siegel space $\mathbf{H}_1$ equals the Poincaré upper half plane $\mathbf{H}$. The symplectic group $\mathrm{Sp}(2, \mathbf{Z})$ equals the special linear group $\mathrm{SL}_2(\mathbf{Z})$ in this case. The space $\mathrm{Sp}_2(\mathbf{Z}) \backslash \mathbf{H}$ is in canonical bijection with the set of isomorphism classes of elliptic curves.

3. *Isogenies*

Let $A/\mathbf{C}$ be a 2-dimensional principally polarized abelian variety, and let $N \geqslant 1$ be a positive integer. The N-torsion $A[N]$ of A is, non-canonically, isomorphic to $(\mathbf{Z}/N\mathbf{Z})^4$. The polarization on A induces a symplectic form v on the rank 4 $(\mathbf{Z}/N\mathbf{Z})$-module $A[N]$. We choose a basis for $A[N]$ such that v is given by the matrix

$$\begin{pmatrix} 0 & 1_2 \\ -1_2 & 0 \end{pmatrix},$$

and we let $\mathrm{Sp}(4, \mathbf{Z}/N\mathbf{Z})$ be the subgroup of the matrix group $\mathrm{GL}(4, \mathbf{Z}/N\mathbf{Z})$ that respects v. A subspace $G \subset A[N]$ is called *isotropic* if v restricts to the zero-form on $G \times G$, and we say that A and A' are (N, N)-isogenous if there is an isogeny $A \to A'$ whose kernel is isotropic of order N^2.

The full congruence subgroup $\Gamma^{(2)}(N)$ of level N is defined as the kernel of the reduction map $\mathrm{Sp}(4, \mathbf{Z}) \to \mathrm{Sp}(4, \mathbf{Z}/N\mathbf{Z})$. Explicitly, a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is contained in $\Gamma^{(2)}(N)$ if and only if we have $a, d \equiv 1_2 \bmod N$ and $b, c \equiv 0_2 \bmod N$. The congruence subgroup $\Gamma^{(2)}(N)$ fits in an exact sequence

$$1 \longrightarrow \Gamma^{(2)}(N) \longrightarrow \mathrm{Sp}(4, \mathbf{Z}) \longrightarrow \mathrm{Sp}(4, \mathbf{Z}/N\mathbf{Z}) \longrightarrow 1.$$

The surjectivity is not completely trivial, see [1, Lemma 3.2].

The 2-dimensional analogue of the subgroup $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbf{Z})$ occuring in the equality $Y_0(N) = \Gamma_0(N) \backslash \mathbf{H}$ of Riemann surfaces is the group

$$\Gamma_0^{(2)}(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}(4, \mathbf{Z}) \mid c \equiv 0_2 \bmod N \right\}.$$

From now on, we restrict to the case $N = p$ prime. The reason for this restriction is that the finite symplectic geometry we need in the remainder of this section is much easier for vector spaces over finite fields than for modules over arbitrary finite rings. The following lemma gives the link between the group $\Gamma_0^{(2)}(p)$ and isotropic subspaces of the p-torsion.

Lemma 3.1. *The index* $[\mathrm{Sp}(4, \mathbf{Z}) : \Gamma_0^{(2)}(p)]$ *equals the number of 2-dimensional isotropic subspaces of the* $\mathbf{F}_p$*-vector space* $\mathbf{F}_p^4$.

Proof. We map $\Gamma_0^{(2)}(p)$ to a subgroup $H \subset \mathrm{Sp}(4, \mathbf{F}_p)$. The inclusion $\Gamma^{(2)}(p) \subseteq \Gamma_0^{(2)}(p)$ shows that we have $[\mathrm{Sp}(4, \mathbf{Z}) : \Gamma_0^{(2)}(p)] = [\mathrm{Sp}(4, \mathbf{F}_p) : H]$. The group H is parabolic, and occurs as stabilizer of the 2-dimensional isotropic subspace $\mathbf{F}_p \times \mathbf{F}_p \times 0 \times 0$ of the symplectic space $\mathbf{F}_p^4$. The group $\mathrm{Sp}(4, \mathbf{F}_p)$ permutes the 2-dimensional isotropic subspaces transitively by Witt's extension theorem [2, Thm. 3.9], and the lemma follows. □

Let $S(p)$ be the set of equivalence classes of pairs (A, G), with A a 2-dimensional principally polarized abelian variety and $G \subset A[p]$ a 2-dimensional isotropic subspace. Here, two pairs (A, G) and (A', G') are said to be isomorphic if there exists an isomorphism of abelian varieties $\varphi : A \to A'$ with $\varphi(G) = G'$.

Theorem 3.2. *The quotient space* $\Gamma_0^{(2)}(p)\backslash\mathbf{H}_2$ *is in canonical bijection with the set* $S(p)$ *via* $\Gamma_0^{(2)}(p)\tau \mapsto (A_\tau, \langle(1/p, 0, 0, 0), (0, 1/p, 0, 0)\rangle)$ *where* $A_\tau = \mathbf{C}^2/(\mathbf{Z}^2 + \mathbf{Z}^2\tau)$ *is the variety associated to* τ.

Proof. The group $\Gamma_0^{(2)}(p)$ stabilizes the subspace $G = \langle(1/p, 0, 0, 0), (0, 1/p, 0, 0)\rangle$ of $A[p]$, and the image (A_τ, G) therefore does not depend on the choice of a representative τ.

If A_τ and $A_{\tau'}$ are isomorphic, then there exists $\psi \in \mathrm{Sp}(4, \mathbf{Z})$ with $\psi\tau = \tau'$. If an isomorphism $A_\tau \xrightarrow{\sim} A_{\tau'}$ maps the group G to $G' = \langle(1/p, 0, 0, 0), (0, 1/p, 0, 0)\rangle \subset A_{\tau'}[p]$, then ψ lies in $\Gamma_0^{(2)}(p)$. Hence, our map is injective.

To prove surjectivity, we first note that every 2-dimensional principally polarized abelian variety occurs as some A_τ by Theorem 2.1. The theorem now follows directly from Lemma 3.1. □

As a quotient space, the 2-dimensional analogue of the curve $Y_0(p)$ is

$$Y_0^{(2)}(p) \stackrel{\text{def}}{=} \Gamma_0^{(2)}(p)\backslash\mathbf{H}_2.$$

We close this section by showing how to give $Y_0^{(2)}(p)$ the structure of a quasi-projective variety. Siegel defined a metric on $\mathbf{H}_2$, a generalization of the Poincaré metric in dimension 1, that respects the action of the symplectic group. With this metric, $Y_0^{(2)}(p)$ becomes a topological space. Just as in the 1-dimensional case $Y_0(p)$, it is not compact. There are several ways to compactify it, one of which is the *Satake compactification*

$$Y_0^{(2)}(p)^* = Y_0^{(2)}(p) \cup Y_0(p) \cup \mathbf{P}^1(\mathbf{Q}).$$

By the Baily-Borel theorem [3], the space $Y_0^{(2)}(p)^*$ has a natural structure as a

https://doi.org/10.1112/S1461157000001546 Published online by Cambridge University Press

projective variety V, and the space $Y_0^{(2)}(p) \subset V$ is therefore naturally a quasi-projective variety.

4. *Functions*

The left-action of $\mathrm{Sp}(4, \mathbf{Z})$ on the Siegel upper half plane $\mathbf{H}_2$ induces a natural right-action on the set of functions from $\mathbf{H}_2$ to $\mathbf{P}^1(\mathbf{C})$ via $(fM)(\tau) = f(M\tau)$. The fixed points under this action are called *rational Siegel modular functions*. Igusa defined [**18**, Thm. 3] three algebraically independent rational Siegel modular functions $\mathbf{H}_2 \to \mathbf{P}^1(\mathbf{C})$ that generate the function field K of $\mathcal{A}_2 = Y_0^{(2)}(1)$. The functions j_1, j_2, j_3 that most people use nowadays are slightly different from Igusa's and we recall their definition first.

Let $E_k(\tau) = \sum_{(c,d)}(c\tau + d)^{-k}$ be the 2-dimensional Eisenstein series. Here, the sum ranges over all co-prime symmetric 2×2-integer matrices that are non-associated with respect to left-multiplication by $\mathrm{GL}(2, \mathbf{Z})$. We define

$$\chi_{10} = -43867 \cdot 2^{-12} \cdot 3^{-5} \cdot 5^{-2} \cdot 7^{-1} \cdot 53^{-1}(E_4E_6 - E_{10})$$

and

$$\chi_{12} = 131 \cdot 593 \cdot 2^{-13} \cdot 3^{-7} \cdot 5^{-3} \cdot 7^{-2} \cdot 337^{-1}(3^2 \cdot 7^2 E_4^3 + 2 \cdot 5^3 E_6^2 - 691 E_{12}),$$

where the constants in χ_{10} and χ_{12} should be regarded as 'normalization factors'. We then define

$$j_1 = 2 \cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^6}, \qquad j_2 = 2^{-3}3^3 \frac{E_4\chi_{12}^3}{\chi_{10}^4}, \qquad j_3 = 2^{-5} \cdot 3 \frac{E_6\chi_{12}^2}{\chi_{10}^3} + 2^{-3} \cdot 3^2 \frac{E_4\chi_{12}^3}{\chi_{10}^4}.$$

We have $K = \mathbf{C}(j_1, j_2, j_3)$ and via the moduli interpretation for $\mathcal{A}_2$, the Igusa functions are functions on the set of principally polarized 2-dimensional abelian varieties. The functions j_1, j_2, j_3 have poles at $\tau \in \mathbf{H}_2$ corresponding to products of elliptic curves with the product polarization.

For a fixed prime p, we define three functions

$$j_{i,p} : \mathbf{H}_2 \to \mathbf{P}^1(\mathbf{C}) \tag{4.1}$$

by $j_{i,p}(\tau) = j_i(p\tau)$. These functions arise naturally in the study of (p, p)-isogenous abelian varieties as we have

$$j_{i,p}(A_\tau/\langle(1/p, 0, 0, 0), (0, 1/p, 0, 0)\rangle) = j_i(A_{p\tau}) = j_{i,p}(\tau).$$

LEMMA 4.1. *The functions $j_{i,p}$ defined in (4.1) above are invariant under the action of $\Gamma_0^{(2)}(p)$.*

Proof. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of $\Gamma_0^{(2)}(p)$, and write $c = pc'$ with c' a 2×2-matrix with integer coefficients. We compute

$$j_{i,p}(M \cdot \tau) = j_i(p(M \cdot \tau)) = j_i((pa\tau + pb)/(c\tau + d)) = j_i(B \cdot p\tau),$$

with $B = \left(\begin{smallmatrix} a & pb \\ c' & d \end{smallmatrix}\right)$. It is clear that B is again symplectic, so we have $j_i(B \cdot p\tau) = j_{i,p}(\tau)$. □

The functions $j_{i,p}$ have poles at $\tau \in \mathbf{H}_2$ corresponding to (p, p)-*split* principally polarized abelian varieties, i.e., varieties that are (p, p)-isogenous to a product of elliptic curves with the product polarization.

Lemma 4.2. *For a prime p, the function field of $Y_0^{(2)}(p)/\mathbf{C}$ equals $K(j_{i,p})$ for every $i = 1, 2, 3$.*

Proof. The function field of $\mathcal{A}_2 = Y_0^{(2)}(1)$ equals $K = \mathbf{C}(j_1, j_2, j_3)$ and the function field $\mathbf{C}(Y_0^{(2)}(p))$ is an extension of K of degree $[\mathrm{Sp}(4, \mathbf{Z}) : \Gamma_0^{(2)}(p)]$. The functions $j_{i,p}$ are contained in $\mathbf{C}(Y_0^{(2)}(p))$ by Lemma 4.1. It suffices to show that, for fixed i, the functions $\{j_{i,p}(\alpha\tau)\}_{\alpha\in\Gamma_0^{(2)}(p)\backslash\mathrm{Sp}(4,\mathbf{Z})}$ are distinct. If two of these functions are equal, then the stabilizer $S \subset \mathrm{Sp}(4, \mathbf{Z})$ of $j_{i,p}$ inside $\mathrm{Sp}(4, \mathbf{Z})$ *strictly* contains $\Gamma_0^{(2)}(p)$. The images of S and $\Gamma_0^{(2)}(p)$ under the reduction map $\pi : \mathrm{Sp}(4, \mathbf{Z}) \twoheadrightarrow \mathrm{Sp}(4, \mathbf{F}_p)$ then satisfy

$$\pi(S) \supsetneq \pi(\Gamma_0^{(2)}(p)).$$

The group $\pi(\Gamma_0^{(2)}(p))$ is the stabilizer of an isotropic subspace of $\mathrm{Sp}(4, \mathbf{F}_p)$ and is therefore *maximal* by [**19**, Thm. 4.2]. Hence, $\pi(S)$ equals the full group $\mathrm{Sp}(4, \mathbf{F}_p)$ and S has to equal $\mathrm{Sp}(4, \mathbf{Z})$. This is absurd. □

The pth *modular polynomial* P_p for j_1 is defined as the minimal polynomial of $j_{1,p}$ over $K = \mathbf{C}(j_1, j_2, j_3)$. It has degree $[\mathrm{Sp}(4, \mathbf{Z}) : \Gamma_0^{(2)}(p)]$ and its coefficients are rational functions in j_1, j_2, j_3 with complex coefficients. The evaluation map $\varphi_\tau : \mathbf{C}(j_1, j_2, j_3) \to \mathbf{C}$ sending j_i to $j_i(\tau)$ maps P_p to a polynomial $P_{p,\tau} \in \mathbf{C}[X]$. The roots of $P_{p,\tau}$ are the j_1-invariants of principally polarized abelian varieties that are (p, p)-isogenous to a variety with j-invariants $j_1(\tau), j_2(\tau), j_3(\tau)$.

The functions $j_{2,p}, j_{3,p}$ are contained in $K(j_{1,p}) = K[j_{1,p}]$ and we define $R_p, Q_p \in \mathbf{C}(j_1, j_2, j_3)[X]$ to be the monic polynomials of degree less than $\deg(P_p)$ satisfying

$$j_{2,p} = R_p(j_{1,p}) \qquad\qquad j_{3,p} = Q_p(j_{1,p}). \tag{4.2}$$

The evaluation map φ_τ maps Q_p, R_p to polynomials $Q_{p,\tau}, R_{p,\tau} \in \mathbf{C}[j_{1,p}]$. If $x \in \mathbf{C}$ is a root of $P_{p,\tau}$, then

$$(x, Q_{p,\tau}(x), R_{p,\tau}(x))$$

are j-invariants of a principally polarized abelian variety that is (p, p)-isogenous to a variety with invariants $j_1(\tau), j_2(\tau), j_3(\tau)$.

5. *Field of definition*

A holomorphic map $\psi : \mathbf{H}_2 \to \mathbf{C}$ is called a *Siegel modular form* of degree $w \geqslant 0$ if it satisfies the functional equation

$$\psi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau) = \det(c\tau + d)^w \psi(\tau)$$

for all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}(4, \mathbf{Z})$. The Eisenstein series E_w are Siegel modular forms of degree w. Any Siegel modular form is invariant under the transformation $\tau \mapsto \tau + b$ and therefore admits a *Fourier expansion*

$$\psi = \sum_T a(T) \exp(2\pi i \mathrm{Tr}(T\tau)),$$

where the summation ranges over all 2 × 2 symmetric 'half-integer' matrices, i.e., symmetric matrices with integer entries on the diagonal and off-diagonal entries in $\frac{1}{2}\mathbf{Z}$. The coefficients $a(T)$ are called the Fourier coefficients of ψ. As discovered by Koecher [20], they are zero unless T is positive semi-definite. For $T = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right)$ we have

$$\mathrm{Tr}(T\tau) = a\tau_1 + b\tau_2 + c\tau_3.$$

Writing $q_i = \exp(2\pi i\tau_i)$, we see that we can express a modular form as $\psi = \sum_{k,l,m} c_{k,l,m} q_1^k q_2^l q_3^m$. By Koecher's result, the summation ranges over non-negative k, l and m satisfying $4m - kl \geqslant 0$.

A Siegel modular form is called a *cusp form* if the Fourier coefficients $a(T)$ are zero for all T that are semi-definite but not definite. One of the classical examples of a cusp form is

$$\chi_{10} = -43867 \cdot 2^{-12} \cdot 3^{-5} \cdot 5^{-2} \cdot 7^{-1} \cdot 53^{-1}(E_4E_6 - E_{10}),$$

which appears in the denominator of the Igusa j-functions. If we express χ_{10} in its 'q_i-expansion', every term is divisible by $q_1q_2q_3$. The 'normalization factor' ensures that the $q_1q_2q_3$-term has coefficient 1.

Lemma 5.1. *The Igusa functions j_i have a Laurent series expansion in q_1, q_2, q_3 with rational coefficients.*

Proof. The denominator of all three Igusa functions is a constant multiple of a power of the cusp form χ_{10}. The product $(q_1q_2q_3)^{-1}\chi_{10}$ has a *non-zero* constant term and is therefore invertible in the ring $\mathbf{C}[[q_1, q_2, q_3]]$. This shows that the Igusa functions have a Laurent series expansion.

As the Fourier coefficients of the Eisenstein series are rational [11, Cor. 2 to Thm. 6.3], the coefficients of the Laurent expansion of j_i are rational. □

In genus 1, it is not hard to prove that the Fourier coefficients of the j-function are rational. A deeper result is that they are *integral*. This is no longer true in genus 2: the coefficients of the expansion of the Igusa functions have 'true' denominators.

Theorem 5.2. *For any prime p, the modular polynomials P_p, Q_p, R_p lie in the ring $\mathbf{Q}(j_1, j_2, j_3)[X]$.*

Proof. We only give the proof for P_p, the proof for Q_p and R_p is similar. We can write

$$P_p = \sum_{m \geqslant 0} \frac{\sum_{a,b,c} c_{m,a,b,c} j_1^a j_2^b j_3^c}{\sum_{a,b,c} d_{m,a,b,c} j_1^a j_2^b j_3^c} X^m,$$

and we have to prove that the coefficients $c_{m,a,b,c}$ and $d_{m,a,b,c}$ are rational. We substitute the Laurent series expansion of $j_1, j_2, j_3, j_{1,p}$ into the equation $P_p = 0$. By equating powers of $q_1^a q_2^b q_3^c$, we get a set of linear equations for the $c_{m,a,b,c}$ and $d_{m,a,b,c}$.

Over the complex numbers, this system of equations has a unique solution. As the coefficients of the equations are rational by Lemma 5.1, this solution must be rational. □

Remark 5.3. *We can reduce the polynomials P_p, Q_p, R_p modulo a prime l. A natural question is if these reduced polynomials still satisfy a moduli interpretation as in (4.2). Whereas reduction of modular curves is relatively well understood, the situation is more complicated for general Siegel modular varieties. In* *our situation, the answer is given by a theorem of Chai and Norman [7, Cor. 6.1.1]. They look at the algebraic stack $\mathcal{A}_{2,\Gamma_0^{(2)}(p)}$ and prove that the structural morphism $\mathcal{A}_{2,\Gamma_0^{(2)}(p)} \to \operatorname{Spec} \mathbf{Z}$ is faithfully flat, Cohen-Macaulay and smooth outside p. Concretely, this means that the moduli interpretation (4.2) remains valid modulo primes $l \neq p$.*

6. *Explicit computations*

In this Section we give a method to compute the three modular polynomials $P_p, Q_p, R_p \in \mathbf{Q}(j_1, j_2, j_3)$ and indicate what the computational difficulties are. We begin with the degree of P_p.

Lemma 6.1. *For a prime p, we have $[\mathrm{Sp}(4, \mathbf{Z}) : \Gamma_0^{(2)}(p)] = (p^4 - 1)/(p - 1)$.*

Proof. By Lemma 3.1, we have to count the number of 2-dimensional isotropic subspaces of the symplectic space $V = \mathbf{F}_p^4$.

Any two-dimensional isotropic subspace of V contains $(p^2 - 1)/(p - 1) = p + 1$ lines. Conversely, a line $l \subset V$ is contained in $(p+1)$ isotropic subspaces. To see this, we note that we can need to select a second line m such that $\langle l, m \rangle$ is isotropic of dimension 2. The complement of l is 3-dimensional, and out of the $(p^3 - 1)/(p - 1)$ lines, only $(p^2 - 1)/(p - 1) = p + 1$ yield an *isotropic* subspace.

We see that the number of 2-dimensional isotropic subspaces equals the number of lines in V. This yields the lemma. □

Remark 6.2. *It is easy to give coset representatives for $S = \mathrm{Sp}(4, \mathbf{Z})/\Gamma_0^{(2)}(p)$. In genus 1, we can take the set*

$$\left\{ \begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix} \mid i \in \mathbf{F}_p \right\} \cup \left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\} \tag{6.1}$$

as a set of coset representatives for $\mathrm{SL}(2, \mathbf{Z})/\Gamma_0(p)$. Inspired by the set in (6.1) we write down

$$\left\{ \begin{pmatrix} 1_2 & 0_2 \\ \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right) & 1_2 \end{pmatrix} \mid a, b, c \in \mathbf{F}_p \right\} \cup \left\{ \begin{pmatrix} 0_2 & -1_2 \\ 1_2 & \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right) \end{pmatrix} \mid ac = b^2 \in \mathbf{F}_p \right\}, \tag{6.2}$$

a set of cardinality $p^3 + p^2$. We are missing $p + 1$ matrices. One can check that

$$\left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & a \\ -a & 1 & 0 & 0 \end{pmatrix} \mid a \in \mathbf{F}_p \right\} \cup \left\{ \begin{pmatrix} -1 & -1 & 1 & -1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \end{pmatrix} \right\}$$

is a set of $p + 1$ matrices that is independent of the set in (6.2). We note that this is the same set of matrices that Dupont found in his thesis [10].

To compute R_p and Q_p, we have to write $j_{2,p}$ and $j_{3,p}$ as rational functions in j_1, j_2, j_3 and $j_{1,p}$. For M ranging over the cosets $S = \mathrm{Sp}(4, \mathbf{Z})/\Gamma_0^{(2)}(p)$, the functions $j_{i,p}(M\tau)$ are distinct by Lemma 4.2. Inspired by the formulas in [16, Sec. 7.1] we note that, by Lagrange interpolation, the polynomials

$$F_{k,p}(X) = \sum_{M \in S} \left(\prod_{\substack{B \in S \\ B \neq M}} \frac{X - j_{1,p}(B\tau)}{j_{1,p}(M\tau) - j_{1,p}(B\tau)} \right) j_{2,p}(M\tau)$$

satisfy $F_{k,p}(j_{1,p}(C\tau)) = j_{2,p}(C\tau)$ for $k = 2, 3$ and all $C \in S$. As the coefficients of $F_{k,p}$ are, by construction, invariant under the action of $\mathrm{Sp}(4, \mathbf{Z})$ the polynomials $F_{k,p}$ are contained in $\mathbf{Q}(j_1, j_2, j_3)[X]$. We have $R_p = F_{2,p}(j_{1,p})$ and $Q_p = F_{3,p}(j_{1,p})$.

We have $P_p = \prod_{M \in S}(X - j_{1,p}(M\tau))$ and with

$$\widetilde{F}_{k,p} = \sum_{M \in S} \left(\prod_{\substack{B \in S \\ B \neq M}} X - j_{1,p}(B\tau) \right) j_{2,p}(M\tau) \in \mathbf{Q}(j_1, j_2, j_3)[X]$$

we have $R_p = \widetilde{F}_{2,p}(j_{1,p})/P_p'(j_{1,p})$ and $Q_p = \widetilde{F}_{3,p}(j_{1,p})/P_p'(j_{1,p})$. Here, P_p' denotes the derivative of P_p. We deduce that it suffices to compute the 3 polynomials $P_p, \widetilde{F}_{2,p}$ and $\widetilde{F}_{3,p}$. In Lemma 6.3 below we prove that the denominators of the coefficients of these polynomials are closely related to (p, p)-*split Jacobians*.

We say that a principally polarized abelian variety $A/\mathbf{C}$ is (p, p)-split if there exists an isogeny of degree p^2 between A and the product $E \times E'$ of two elliptic curves with the product polarization. The locus of such A is denoted by $\mathcal{L}_p$. It is well known that $\mathcal{L}_p$ is a 2-dimensional algebraic subvariety of the 3-dimensional moduli space $\mathcal{A}_2$. We have chosen coordinates j_1, j_2, j_3 for $\mathcal{A}_2$, and $\mathcal{L}_p$ can be given by an equation $L_p = 0$ for a polynomial $L_p \in \mathbf{Q}[j_1, j_2, j_3]$.

Lemma 6.3. *The denominators of the coefficients of P_p, $\widetilde{F}_{2,p}$ and $\widetilde{F}_{3,p}$ are all divisible by the polynomial L_p describing the moduli space of (p, p)-split Jacobians.*

Proof. Let $\tau \in \mathbf{H}_2$ correspond to a (p, p)-split Jacobian, and let c be a coefficient of P_p. For some $M \in \mathrm{Sp}(4, \mathbf{Z})/\Gamma_0^{(2)}(p)$, the value $j_{1,p}(M\tau)$ is infinite because the functions j_i have poles at products of elliptic curves. The evaluation of c at τ is a symmetric expression in the $j_{1,p}(M\tau)$'s. Generically, there is no algebraic relation between these values, and the evaluation of c at τ is therefore *infinite*.

Since $j_i(\tau)$ is finite, the numerator of c is finite. We conclude that the denominator of c must vanish at τ, i.e., c is divisible by L_p. The proof for $\widetilde{F}_{2,p}$ and $\widetilde{F}_{3,p}$ proceeds similarly. □

Remark 6.4. *Points on the variety $\mathcal{L}_p$ are in bijection with points on the Humbert surface H_{p^2}, see [23]. It is a traditionally hard problem to compute equations for Humbert surfaces. Up to now, this has only been done for $p = 2, 3, 5$, see [26, 27, 21]. As computing modular polynomials is an even harder problem, it seems unlikely that we will be able to compute many examples in the near future. More precisely, we conjecture that the following is true.*

Conjecture 6.5. *There exists an element $c \in \mathbf{Q}_{>0}$ with the property that the polynomial P_p requires at least cp^{12} bits to write down.*

Heuristic Reason. *The degree of P_p equals $(p^4 - 1)/(p - 1) \approx p^3$ by Lemma 6.1. The numerator of every coefficient of P_p is a polynomial in j_1, j_2, j_3. We expect that the degree in each of the three variables j_1, j_3, j_3 of these polynomials is of order p. Furthermore, by looking at the 1-dimensional case it seems reasonable to assume that these polynomials themselves have coefficients of size at least p. This means that we need at least cp^4 bits to store one coefficient of P_p for some constant $c \in \mathbf{Q}_{>0}$.*

In the case $p = 2$ it is relatively straightforward to compute the polynomial L_2 describing $(2,2)$-split Jacobians. We refer to [26] for its construction. We have

$$\begin{aligned}L_2 = {} & 236196j_1^5 - 972j_1^4j_2^2 + 5832j_1^4j_2j_3 + 19245600j_1^4j_2 - 8748j_1^4j_3^2\\ & -104976000j_1^4j_3 + 125971200000j_1^4 + j_1^3j_2^4 - 12j_1^3j_2^3j_3 - 77436j_1^3j_2^3\\ & +54j_1^3j_2^2j_3^2 + 870912j_1^3j_2^2j_3 - 507384000j_1^3j_2^2 - 108j_1^3j_2j_3^3 - 3090960j_1^3j_2j_3^2\\ & +2099520000j_1^3j_2j_3 + 81j_1^3j_3^4 + 3499200j_1^3j_3^3 + 78j_1^2j_2^5 - 1332j_1^2j_2^4j_3\\ & +592272j_1^2j_2^4 + 8910j_1^2j_2^3j_3^2 - 4743360j_1^2j_2^3j_3 - 29376j_1^2j_2^2j_3^3 + 9331200j_1^2j_2^2j_3^2\\ & +47952j_1^2j_2j_3^4 - 31104j_1^2j_3^5 - 159j_1j_2^6 + 1728j_1j_2^5j_3 - 41472j_1j_2^5\\ & -6048j_1j_2^4j_3^2 + 6912j_1j_2^3j_3^3 + 80j_2^7 - 384j_2^6j_3.\end{aligned}$$

In the remainder in this section we describe the explicit computation of the entire polynomial P_2. Our idea is to use an *interpolation* technique, i.e., compute $P_2(j_1(\tau), j_2(\tau), j_3(\tau)) \in \mathbf{C}[X]$ for sufficiently many $\tau \in \mathbf{H}_2$ and use that information to reconstruct the coefficients of P_2. Unfortunately, we need to know the full denominators of the coefficients of P_2 for this approach to work. The interpolation problem was also considered by Dupont in his thesis [10]. Without knowing Lemma 6.3, he succeeded in computing P_2. The approach outlined below is inspired by Dupont's ideas.

Let $c(j_1, j_2, j_3)$ be a coefficient of P_2. The first step is to compute the degree in j_1, j_2, j_3 of its numerator $n(c)$ and its denominator $d(c)$. We *fix* $y, z \in \mathbf{Q}(i)$ and for a collection of values $x_k \in \mathbf{Q}(i)$ we compute a value $\tau_k \in \mathbf{H}_2$ with

$$(j_1(\tau_k), j_2(\tau_k), j_3(\tau_k)) = (x_k, y, z)$$

by first using Mestre's algorithm [22] to find a genus 2 curve C whose Igusa invariants are (x_k, y, z) and then finding $\tau_k \in \mathbf{H}_2$ corresponding to $\mathrm{Jac}(C)$. We can therefore evaluate the *univariate* rational function $c(x_k, y, z)$. It is now an easy matter to determine the degree in j_1 of $n(c)$ and $d(c)$. Indeed, we check for which values of m, n the matrix $M(m, n) =$

$$\begin{pmatrix} 1 & \dots & x_1^m & -c(x_1, y, z) & \dots & -c(x_1, y, z)x_1^n \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 1 & \dots & x_{m+n+2}^m & -c(x_{m+n+2}, y, z) & \dots & -c(x_{m+n+2}, y, z)x_{m+n+2}^n \end{pmatrix}$$

has non-zero solution-space for arbitrary $x_k \in \mathbf{Q}(i)$. The smallest m, n for which this is the case are the degrees of $n(c)$ and $d(c)$. We find for instance that the constant term of P_2 has a numerator of degree 60 and a denominator of degree 51 in j_1. Likewise, we can find the degrees in j_2 and j_3. The degree in j_2 of the denominators is 42 for all coefficients and we find 30 for the degree in j_3.

As L_2 has degree 7 in j_2 and degree 5 in j_3, we *guess* that L_2^6 divides $d(c)$. We are still missing a polynomial in j_1 of degree > 1 for the denominator. To find this polynomial, a natural idea is to try j_1^α with α the difference between the degree of $d(c)$ and $6 \cdot 5 = 30$. One heuristic reason for this is the following: if $\tau \in \mathbf{H}_2$ corresponds to the product of elliptic curves, then the numerator of c is infinite at τ. Combined with the vanishing of L_2^6 at τ, this would mean that c has a pole of very high order at such τ. To 'compensate' for this, we multiply L_2^6 by j_1^α. One can verify that the denominator is indeed $j_1^\alpha L_2^6$ by taking $x, y, z \in \mathbf{Z}[i]$ and looking at the denominator of $c(x, y, z) \in \mathbf{Q}(i)$.

https://doi.org/10.1112/S1461157000001546 Published online by Cambridge University Press

Having computed the denominator of c, it is an easy matter to compute the numerator. Indeed, we can evaluate $d(c)c$ at any point $\tau \in \mathbf{H}_2$ and apply interpolation techniques to find $n(c)$. As the degrees in j_1, j_2 and j_3 of $n(c)$ are relatively large, this does take a large amount of time. The constant term of P_2 contains 16795 monomials for instance, with coefficients up to 200 decimal digits. It takes more than 50 megabytes to store P_2, Q_2, R_2.

Combined with Conjecture 6.5, the fact that P_2, Q_2, R_2 require more than 50 megabytes to store means that the computation of P_3, Q_3, R_3 will be a major effort. We can guess the cost of the computation by combining the asymptotic growth predicted by Conjecture 6.5 with the 'initial data' provided by P_2. A quick computation yields that we expect that every coefficient of the numerator of P_2 has roughly 56000 monomials with coefficients up to 300 decimal digits. As P_3 has degree $(3^4-1)/(3-1)=40$, this means that we would roughly need 0.7 gigabytes to store the numerator of P_3. The denominator is fairly small, so we would need about 2 gigabytes of memory to store P_3, Q_3, R_3. This is still feasible with currect computers, but we did not attempt the computation.

7. *Richelot isogeny*

In this Section we zoom in on the special case $p=2$, and explain the link between our modular polynomials P_2, Q_2, R_2 and the classical 'Richelot isogeny'. The Richelot isogeny is typically used as a tool for computing the Mordell-Weil group of a Jacobian of a genus 2 curve, and we first explain the construction.

Fix a non-singular curve $C/\mathbf{C}$ of genus 2, and pick an equation

$$Y^2 = f(X)$$

for C, where $f \in \mathbf{C}[X]$ is monic of degree 6. We pick a factorization $f = ABC$ of f into three monic polynomials, each of degree 2. Writing $[A,B] = A'B - AB'$, with A' the derivative of A, we define the curve C' by the equation

$$\Delta Y^2 = [A,B][A,C][B,C]. \tag{7.1}$$

Here, Δ is the determinant of A, B, C with respect to the basis $1, X, X^2$. A simple check shows that the right hand side is again a monic polynomial of degree 6. It is separable if and only if Δ is non-zero.

Lemma 7.1. *The Jacobians of the two curves C and C' defined above are $(2,2)$-isogenous. Furthermore, every $(2,2)$-isogeny from* $\mathrm{Jac}(C)$ *into some principally polarized abelian variety A arises via this construction.*

Proof. The fact that $\mathrm{Jac}(C)$ and $\mathrm{Jac}(C')$ are $(2,2)$-isogenous can be found in [6]. To show that every $(2,2)$-isogeny is a 'Richelot isogeny', we look at the generic case that $\mathrm{Jac}(C)$ is *not* $(2,2)$-split. It then suffices to prove that there are $[\mathrm{Sp}_4(\mathbf{Z}) : \Gamma_0^{(2)}(2)] = 15$ different equations for the curve C'. This is simple combinatorics: we have a priori $6 \cdot 5/2 = 15$ choices for the polynomial A, and then 6 choices for the polynomial B. As the right hand side of (7.1) is invariant under a permutation of A, B, C, we get 15 different equations. □

The connection with the modular polynomial P_2 defined in this paper is as follows. Assume that $\mathrm{Jac}(C)$ is not $(2,2)$-split. The discriminant Δ is then non-

https://doi.org/10.1112/S1461157000001546 Published online by Cambridge University Press

zero for every choice of factorization $f = ABC$. We let φ be the map sending an Igusa invariant j_i to $j_i(\mathrm{Jac}(C)) \in \mathbf{C}$. Lemma 7.1 tells us that the 15 roots of $\varphi(P_2) \in \mathbf{C}[X]$ are exactly the first Igusa invariants of the curves C' in (7.1). There are similar relations for $\varphi(R_2)$ and $\varphi(Q_2)$.

References

1. A. N. Andrianov and V. G. Zhuravlev, *Modular forms and Hecke operators*, AMS Translations of mathematical monographs, vol 145 (AMS, Providence, 1995). 329

2. E. Artin, *Geometric algebra*, Wiley Classics Library (John Wiley & Sons Inc., New York, 1988). 330

3. W. L. Baily and A. Borel, ‘Compactification of arithmetic quotients of bounded symmetric domains’, *Ann. of Math.* 84 (1966) 442–538. 330

4. J. Belding, R. Bröker, A. Enge and K. Lauter, ‘Computing Hilbert Class Polynomials’, *Algorithmic Number Theory Symposium VIII*, Banff, 2008, ed. A. J. van der Poorten and A. Stein (Springer Lecture Notes in Computer Science 5011, Berlin, 2008) 282–295. 326

5. C. Birkenhake and C. Lange, *Complex Abelian Varieties*, Grundlehren der Mathematischen Wissenschaften 302 (Springer, Berlin, 2003). 328

6. J.-B. Bost and J.-F. Mestre, ‘Moyenne arithmético-géometrique et périodes de courbes de genre 1 et 2’, *Gaz. Math. Soc. France* 38 (1988) 36–64. 337

7. C.-L. Chai and P. Norman, ‘Bad reduction of the Siegel moduli scheme of genus two with $\Gamma_0(p)$-level structure’, *Amer. J. Math.* 122 (1990) 1003–1071. 334

8. H. Cohen, G. Frey et al., *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and Its Applications 34 (Chapman & Hall/CRC, Boca Raton, 2006). 326

9. D. A. Cox, *Primes of the form* $x^2 + ny^2$, 1st edn (John Wiley & Sons Inc., New York, 1989). 326

10. R. Dupont, *Moyenne arithmético-géométrique, suites de Borchardt et applications*, PhD-thesis (École Polytechnique, Paris, 2006). 327, 334, 336

11. M. Eichler and D. Zagier, *The theory of Jacobi forms*, Progress in mathematics 55 (Birkhäuser, Boston, 1985). 333

12. K. Eisenträger and K. Lauter, ‘A CRT algorithm for constructing genus 2 curves over finite fields’, *Arithmetic, Geometry and Coding Theory (AGCT-10)*, online at `http://arxiv.org/abs/math.NT/0405305` (2005). 326, 327

13. A. Enge and F. Morain, *SEA in genus 1: 2500 decimal digits*, Announcement sent to the Number theory mailing list, online available at `http://listserv.nodak.edu/archives/nmbrthry.html` (December 2006). 326

14. P. Gaudry, *Algorithmique des courbes hyperelliptiques et applications à la cryptologie*, PhD-thesis (École Polytechnique, Paris, 2000). 327

15. P. Gaudry and R. Harley, 'Counting points on hyperelliptic curves over finite fields', *Algorithmic Number Theory Symposium IV*, Leiden, 2000, ed. W. Bosma (Springer Lecture Notes in Computer Science 1838, Berlin, 2000) 313–332. 326

16. P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng, 'The 2-adic CM-method for genus 2 curves with applications to cryptography', *Advances in Cryptology, Asiacrypt 2006*, Shanghai, 2006, ed. X. Lai and K. Chen (Springer Lecture Notes in Computer Science 4284, Berlin, 2006) 114–129. 334

17. P. Gaudry and E. Schost, 'Modular equations for hyperelliptic curves', *Math. Comp.* 74 (2005) 429–454. 327

18. J.-I. Igusa, 'On Siegel modular forms of genus two', *Amer. J. Math.* 84 (1962) 175–200. 331

19. O. H. King, 'The subgroup structure of finite classical groups in terms of geometric configurations', *Surveys in Combinatorics*, ed. B. S. Webb, London Mathematical Society Lecture Note Series 327 (Cambridge University Press, Cambridge, 2005) 29–56. 332

20. M. Koecher, 'Zur Theorie der Modulfunktionen n-ten Grades, I', *Math. Z.* 59 (1954) 399–416. 333

21. K. Magaard, T. Shaska and T, H. Völklein, 'Genus 2 curves with degree 5 elliptic subcovers', (Form Math., to appear). 335

22. J.-F. Mestre, 'Construction des courbes de genre 2 à partir de leurs modules', *Effective methods in algebraic geometry*, Livorno, 1990, ed. T. Mora and C. Traverso (Birkhäuser Progress in Mathematics 94, Boston, 1991) 313–334. 336

23. N. Murabayashi, 'The moduli space of curves of genus two covering elliptic curves', *Manuscripta Math.* 84 (1994) 125–133. 335

24. R. Schoof, 'Counting points on elliptic curves over finite fields', *J. Théor. Nombres Bordeaux* 7 (1993) 219–254. 326

25. R. Schoof, 'Elliptic curves over finite field and the computation of square roots mod p', *Math. Comp.* 44 (1985) 483–494. 326

26. T. Shaska, 'Genus 2 curves covering elliptic curves, a computational approach', *Lect. Notes in Comp.* 13 (2005) 243–255. 335, 336

27. T. Shaska, 'Genus 2 fields with degree 3 elliptic subfields', *Forum Math. 16* no. 2 (2004) 263–280. 335

28. A. V. Sutherland, 'Computing Hilbert class polynomials with the Chinese Remainder Theorem', available at `http://arxiv.org/abs/0903.2785` (2009). 326

Reinier Bröker reinierb@microsoft.com
Kristin Lauter klauter@microsoft.com

Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA

https://doi.org/10.1112/S1461157000001546 Published online by Cambridge University Press