



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Hilbert theta series and invariants of genus 2 curves

Kristin Lauter^{a,*}, Michael Naehrig^a, Tonghai Yang^b^a Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA^b Department of Mathematics, University of Wisconsin Madison, Van Vleck Hall, Madison, WI 53706, USA

ARTICLE INFO

Article history:

Received 2 November 2014

Accepted 2 February 2015

Available online xxxx

Communicated by Jerome Hoffman,
Robert Perlis, Ling Long, Karl
Mahlburg, Jorge Morales, Holly
SwisherDedicated to Professor Wen-Ching
Winnie Li*MSC:*

14G35

11F55

11G18

Keywords:

Theta functions

Hilbert moduli space

Genus 2 curves

Invariants

Cryptography

ABSTRACT

In this paper, we compute pull-backs of Siegel theta functions to the Hilbert moduli space and consider their application to generating genus 2 curves for cryptography. We express invariants of genus 2 curves such as the Gundlach invariants and Rosenhain invariants in terms of these Hilbert theta functions. A result of independent interest is a simple formula in terms of these functions for the Eisenstein series of weight 2, which is not the pull-back of any Siegel modular form of level 1. We present an algorithm to compute minimal polynomials for the invariants, including a description of CM points and how to compute them, along with numerical examples.

© 2015 Elsevier Inc. All rights reserved.

* Corresponding author.

E-mail addresses: klauter@microsoft.com (K. Lauter), mnaehrig@microsoft.com (M. Naehrig), thyang@math.wisc.edu (T. Yang).<http://dx.doi.org/10.1016/j.jnt.2015.02.020>

0022-314X/© 2015 Elsevier Inc. All rights reserved.

1. Introduction

Igusa defined three invariants for genus 2 curves which can be used to construct curves for use in cryptography. The Igusa invariants can be computed as special CM values of Siegel modular functions on the Siegel moduli space of principally polarized abelian surfaces. CM points on the moduli space correspond to complex multiplication points where the abelian surface has extra endomorphisms and the endomorphism ring is an order in the ring of integers of a quartic CM field, K . Evaluating the Siegel modular functions at CM points to high precision and recognizing them algebraically is a computationally intensive task.

In [LY], Lauter and Yang introduced invariants of genus 2 curves defined as special values of Hilbert modular functions. These were constructed by pulling back Eisenstein series from the Siegel to the Hilbert moduli space and expressing the Igusa invariants in terms of these pull-backs. Part of the motivation for introducing invariants on the Hilbert moduli space was to improve efficiency for the computation. The invariants on the Hilbert moduli space are more efficient to compute because the CM points have a simpler description, and the evaluation of the exponential functions is more compact, depending essentially on two variables rather than three. In addition, when the Hilbert moduli space is associated to the real quadratic field $F = \mathbb{Q}(\sqrt{5})$, the space of Hilbert modular functions is generated by only two rational functions constructed by Gundlach. Thus the problem of computing invariants for genus 2 curves is reduced to computing and recognizing algebraically just two *Gundlach* invariants, the CM values of the Gundlach rational functions.

In this paper, we present a further improvement to this approach by expressing all the functions to be computed in terms of Hilbert theta functions on the Hilbert moduli space. Igusa invariants for genus 2 curves on the Siegel moduli space can be expressed either in terms of Eisenstein series or in terms of products of theta functions. Theta series converge faster so they are preferable for high-precision computation, but Eisenstein series have a Fourier expansion which is very useful for estimating and controlling precision of computation (see [BL]). We prove (Theorem 2.2) that the pull-back of Siegel theta functions are exactly those Hilbert theta functions. So Igusa invariants can be computed via pullbacks to Hilbert theta functions for any CM field. In addition, we discover a simple formula for the Eisenstein series of weight 2 in terms of Hilbert theta functions, which should be of independent interest. Notice that this Eisenstein series is not the pull-back of any Siegel modular form of level 1.

Hyperelliptic curves can also be constructed from their Rosenhain invariants, whose CM values give the Weierstrass points for a hyperelliptic model of the curve. The advantages of using Rosenhain invariants instead of Igusa invariants was explored in [CDLY]. The formulas for the Rosenhain invariants in terms of theta functions are much simpler than for the Igusa invariants and thus they have much smaller height, requiring less precision to compute and recognize as algebraic numbers. But unfortunately their degree can be larger, and the ratio of the degrees depends on the splitting of the prime 2 in

the CM field K . Since Rosenhain invariants have a very simple expression in terms of theta constants, they can also be pulled back to the Hilbert moduli space for any real quadratic field.

The paper is organized as follows. The next three sections focus on modular forms and maps between the moduli spaces. Sections 2 and 3 present formulas for computing the pull-backs of modular forms from the Siegel to the Hilbert moduli space. In Section 2.4 we show how to pull back Siegel theta functions to Hilbert thetas, thus making it possible to compute pull-backs of Igusa invariants expressed solely in terms of products of theta functions, and this works for the Hilbert moduli space associated to any real quadratic field. In Section 3, we show how to express Gundlach invariants in terms of the Hilbert theta series, allowing for more efficient computation. There are only two Gundlach invariants to be computed, which gives an advantage over computing three Igusa invariants. Unfortunately, the advantages of the two Gundlach invariants are only available when the real quadratic subfield of K is $F = \mathbb{Q}(\sqrt{p})$ ($p = 2, 5, 13, 17$), as the associated Hilbert modular surfaces are projective spaces. Finally, in Section 4, we show how to pull back the Rosenhain invariants and express them in terms of Hilbert theta functions.

The last two sections of the paper focus on the application to computing invariants of genus 2 curves. Section 5 presents a description of the CM points and how to compute them, including a description of the Galois orbits and the CM points with level structure which are needed for computing Rosenhain invariants. Section 5.4 addresses the computational issues which arise when evaluating modular forms at CM points to high precision; Section 5.5 presents an algorithm for computing minimal polynomials of invariants, and Section 6 gives examples of the CM method to compute minimal polynomials for the various choices of invariants. Appendix A addresses the issue of the precision of computation which is important for recognizing the invariants as algebraic numbers.

2. Hilbert and Siegel modular forms

2.1. Siegel modular forms and theta constants

Let $\text{Sym}_2(\mathbb{C})$ be the set of symmetric 2×2 -matrices over $\mathbb{C}$. For $\tau \in \text{Sym}_2(\mathbb{C})$ we denote its imaginary part by $\Im\tau$. Let

$$\mathbb{H}_2 = \{\tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \in \text{Sym}_2(\mathbb{C}) : \Im\tau > 0\}$$

be the Siegel upper half-plane of genus 2. Let I be the 2×2 identity matrix and let

$$\text{Sp}_2(\mathbb{Z}) = \{g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{GL}_4(\mathbb{Z}) : g \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} g^t = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\}$$

be the symplectic group, which acts on $\mathbb{H}_2$ via $g\tau = (A\tau + B)(C\tau + D)^{-1}$.

For a quadruple $m = (m_1, m_2, m_3, m_4) \in \mathbb{Z}^4$ which we write as $m = (m', m'') = ((m_1, m_2), (m_3, m_4))$, i.e. $m', m'' \in \mathbb{Z}^2$, the *Siegel theta constant of characteristic m* is defined as

$$\theta_m(\tau) = \sum_{n \in \mathbb{Z}^2} e\left(\frac{1}{2}\left(n + \frac{m'}{2}\right)\tau\left(n + \frac{m'}{2}\right)^t\right) e\left(\left(n + \frac{m'}{2}\right)\left(\frac{m''}{2}\right)^t\right),$$

where $e(z) = e^{2\pi iz}$. The function $\theta_m(\tau)$ is a Siegel modular form of weight $\frac{1}{2}$ (for the modular group $\Gamma(2)$). Note that

$$\theta_m(\tau) = \pm \theta_n(\tau) \quad \text{if } m \equiv n \pmod{2}.$$

This means that $\theta_m(\tau)$ is well-defined up to sign when we restrict the characteristic m to be a representative of $(\mathbb{Z}/2\mathbb{Z})^4$. From now on, we only consider $m \in (\mathbb{Z}/2\mathbb{Z})^4$. In what follows, the sign ambiguity does not affect our calculation of the Igusa invariants as only θ_m^2 appears in our computations. A quadruple $m = (m', m'')$ as above is *even* if $m'(m'')^t = 0$, i.e., $m_1m_3 + m_2m_4 \equiv 0 \pmod{2}$. There are 10 even quadruples $m \in (\mathbb{Z}/2\mathbb{Z})^4$. It is well-known that $\theta_m \neq 0$ if and only if m is even.

2.2. Igusa invariants in terms of Siegel theta constants

Let C_0 be the set of even quadruples in $(\mathbb{Z}/2\mathbb{Z})^4$. A set $\{l, m, n\} \subset C_0$ of three different even characteristics is called a *syzygous triple* if the sum $l + m + n$ is in C_0 . There are 60 syzygous triples. A set $\{k, l, m, n\} \subset C_0$ of four different even characteristics is called a *Göpel quadruple*, if the sum $k + l + m + n \equiv (0, 0, 0, 0) \pmod{2}$. Let S be the set of all Göpel quadruples. In terms of the above theta constants, Igusa [Ig2, p. 848] defines the following functions:

$$\begin{aligned} \psi_4(\tau) &= 2^{-2} \sum_{m \in C_0} (\theta_m(\tau))^8, & \psi_6(\tau) &= 2^{-2} \sum_{\substack{\{l, m, n\} \subset C_0 \\ \text{syzygous}}} (-1)^{s(l, m, n)} (\theta_l(\tau) \theta_m(\tau) \theta_n(\tau))^4, \\ \chi_{10}(\tau) &= -2^{-14} \prod_{m \in C_0} (\theta_m(\tau))^2, & \chi_{12}(\tau) &= 2^{-17} 3^{-1} \sum_{c \in S} \prod_{m \in C_0 \setminus c} (\theta_m(\tau))^4. \end{aligned}$$

The sign of each summand in the formula for ψ_6 is given in its explicit form in [St, p. 68] and is determined by $(-1)^{s(l, m, n)}$ where

$$\begin{aligned} s(l, m, n) &= l_1 + l_2 + m_1 + m_2 + n_1 + n_2 + l_1m_1 + l_2m_2 + l_4m_2 + l_1m_3 - l_2m_4 \\ &\quad + l_1n_1 - l_3n_1 + m_1n_1 + l_2n_2 + m_2n_2 + m_4n_2 + m_1n_3 - l_2l_3m_1 \\ &\quad - l_2l_4m_2 - l_1l_2m_3 - l_2l_3n_1 - l_3m_1n_1 - l_1m_3n_1 - l_2m_3n_1 \\ &\quad - l_2l_4n_2 - l_4m_2n_2 - l_1l_2n_3 - l_1m_1n_3 - l_2m_1n_3. \end{aligned}$$

The three absolute Igusa invariants as defined in [Ig1] can be written in terms of $\psi_4, \psi_6, \chi_{10}$ and χ_{12} (see also [LY, Section 2.2]) as

$$\begin{aligned} j_1(\tau) &= 2 \cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^6}, \quad j_2(\tau) = -2^{-3} \cdot 3^3 \cdot \psi_4 \frac{\chi_{12}^3}{\chi_{10}^4}, \\ j_3(\tau) &= 2^{-5} \cdot 3 \cdot \left(\psi_6 \frac{\chi_{12}^2}{\chi_{10}^3} + 2^2 \cdot 3 \cdot \psi_4 \frac{\chi_{12}^3}{\chi_{10}^4} \right). \end{aligned} \quad (2.1)$$

2.3. Hilbert theta constants

Let $F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field with fundamental discriminant $D > 0$, ring of integers $\mathcal{O}_F$, and different $\partial_F = \sqrt{D}\mathcal{O}_F$. For convenience, we fix the following $\mathbb{Z}$ -basis $\{e_1, e_2\}$ of $\mathcal{O}_F$ with $e_1 = 1$ and

$$e_2 = \begin{cases} \frac{1-\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod{4}, \\ -\frac{1}{2}\sqrt{D} & \text{if } D \equiv 0 \pmod{4}. \end{cases} \quad (2.2)$$

Let σ be the non-trivial Galois automorphism of F and denote by $\text{tr}_{F/\mathbb{Q}}(t) = t + \sigma(t)$ the standard field trace of $t \in F$ over $\mathbb{Q}$. Let $\mathbb{H}^2$ be the product of two copies of the usual upper half plane $\mathbb{H}$. For $z = (z_1, z_2) \in \mathbb{H}^2$ and $t \in F$, define $tz = t(z_1, z_2) = (tz_1, \sigma(t)z_2)$. We define the trace $\text{tr}_{F/\mathbb{Q}}$ on $\mathbb{H}^2$ as the map $\text{tr}_{F/\mathbb{Q}}(z) = z_1 + z_2$, i.e. for $t \in F$, we have $\text{tr}_{F/\mathbb{Q}}(tz) = tz_1 + \sigma(t)z_2$. When $z = (1, 1)$, one obtains the standard field trace as $\text{tr}_{F/\mathbb{Q}}(t) = \text{tr}_{F/\mathbb{Q}}(t(1, 1)) = t + \sigma(t)$.

The group $\text{SL}_2(F)$ acts on $\mathbb{H}^2$ via $\gamma z = \gamma(z_1, z_2) = (\gamma z_1, \sigma(\gamma)z_2)$, where

$$\gamma z_1 = \frac{az_1 + b}{cz_1 + d}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and $\sigma(\gamma)$ is the matrix obtained by applying σ to the coefficients of γ . For a fractional ideal $\mathfrak{f}_0$ of F , let

$$\text{SL}_2(\mathcal{O}_F \oplus \mathfrak{f}_0) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(F) : a, d \in \mathcal{O}_F, b \in \mathfrak{f}_0, c \in \mathfrak{f}_0^{-1} \right\}.$$

In particular, $\text{SL}_2(\mathcal{O}_F \oplus \mathcal{O}_F) = \text{SL}_2(\mathcal{O}_F)$.

For $(a, b) \in (\mathcal{O}_F/2\mathcal{O}_F)^2$, we define the *Hilbert theta constant with characteristic* (a, b) as

$$\theta_{a,b}(z) = \sum_{u \in \mathcal{O}_F} e \left(\frac{1}{2} \text{tr}_{F/\mathbb{Q}} \left(\left(u + \frac{a}{2} \right)^2 z \right) \right) \cdot e \left(\frac{1}{2} \text{tr}_{F/\mathbb{Q}} \left(\left(u + \frac{a}{2} \right) \frac{b}{\sqrt{D}} \right) \right), \quad (2.3)$$

where $e(z) = e^{2\pi iz}$ as above. The function $\theta_{a,b}(z)$ is a Hilbert modular form of weight $\frac{1}{2}$. We notice that $\theta_{a,b}(z)$ is also only well-defined up to a sign:

$$\theta_{a+2a_1, b+2b_1}(z) = e\left(\mathrm{tr}_{F/\mathbb{Q}} \frac{ab_1}{2\sqrt{D}}\right) \theta_{a,b}(z) = \pm \theta_{a,b}(z).$$

However, this does not affect the calculations in this paper. One can prove that $\theta_{a,b} \neq 0$ if and only if $\mathrm{tr}_{F/\mathbb{Q}}(\frac{ab}{\sqrt{D}}) \in 2\mathbb{Z}$. In this case we call the pair (a, b) *even*.

2.4. Pull back

In this section, we describe the relation between Siegel theta constants and Hilbert theta constants. We show that the Siegel theta constants correspond to Hilbert theta constants via the pull back induced from the following maps. Let

$$R = \begin{pmatrix} e_1 & e_2 \\ \sigma(e_1) & \sigma(e_2) \end{pmatrix}, \quad \gamma^* = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} a & 0 & b & 0 \\ 0 & \sigma(a) & 0 & \sigma(b) \\ c & 0 & d & 0 \\ 0 & \sigma(c) & 0 & \sigma(d) \end{pmatrix}.$$

We define three maps, which are compatible in the sense of [Lemma 2.1](#) and [Theorem 2.2](#) below. For this reason, we use the same notation ϕ for all of them instead of three different symbols. Let

$$\begin{aligned} \phi: \mathbb{H}^2 &\rightarrow \mathbb{H}_2, & z = (z_1, z_2) &\mapsto R^t \mathrm{diag}(z_1, z_2) R, \\ \phi: \mathrm{SL}_2(F) &\rightarrow \mathrm{Sp}_2(\mathbb{Q}), & \gamma &\mapsto \mathrm{diag}(R^t, R^{-1}) \gamma^* \mathrm{diag}((R^t)^{-1}, R), \\ \phi: (\mathcal{O}_F/2\mathcal{O}_F)^2 &\rightarrow (\mathbb{Z}/2\mathbb{Z})^4, & (a, b) &\mapsto (m_1, m_2, m_3, m_4), \end{aligned} \quad (2.4)$$

where

$$(m_1, m_2)^t = R^{-1}(a, \sigma(a))^t, \quad (m_3, m_4)^t = \begin{pmatrix} \sigma(e_2) & -\sigma(e_1) \\ e_2 & -e_1 \end{pmatrix}^{-1} (b, \sigma(b))^t.$$

We have the following lemma.

Lemma 2.1. *Let the notation be as above. Then:*

- (1) For $\gamma \in \mathrm{SL}_2(F)$ and $z \in \mathbb{H}^2$, one has $\phi(\gamma z) = \phi(\gamma)\phi(z)$;
- (2) $\phi^{-1}(\mathrm{Sp}_2(\mathbb{Z})) = \mathrm{SL}_2(\mathcal{O}_F \oplus \partial_F^{-1})$;
- (3) The map ϕ is a bijection from $(\mathcal{O}_F/2\mathcal{O}_F)^2$ to $(\mathbb{Z}/2\mathbb{Z})^4$ such that (a, b) is even if and only if $\phi(a, b)$ is even.

Proof. The proof follows by a direct calculation. For example, for statement (3), if $m = \phi(a, b)$, then we have:

$$(m_1, m_2) = (a, \sigma(a))(R^t)^{-1}, \quad (m_3, m_4)^t = \begin{pmatrix} \sigma(e_2) & -\sigma(e_1) \\ e_2 & -e_1 \end{pmatrix}^{-1} (b, \sigma(b))^t.$$

In particular, ϕ is a bijection. Moreover,

$$(m_1, m_2)(m_3, m_4)^t = \frac{ab - \sigma(a)\sigma(b)}{\det R} = \text{tr}_{F/\mathbb{Q}} \left(\frac{ab}{\sqrt{D}} \right).$$

So m is even if and only if (a, b) is even. $\square$

The lemma shows that the pull-back via ϕ of a Siegel modular form for a congruence subgroup of $\text{Sp}_2(\mathbb{Z})$ is a Hilbert modular form for a congruence subgroup of $\text{SL}_2(\mathcal{O}_F \oplus \partial_F^{-1})$.

Theorem 2.2. *Let the notation be as above. Then*

$$\phi^* \theta_m = \pm \theta_{\phi^{-1}(m)}.$$

Proof. Let $z = (z_1, z_2) \in \mathbb{H}^2$. From the definition of θ_m and the pullback ϕ^* , we obtain

$$\phi^* \theta_m(z) = \sum_{n \in \mathbb{Z}^2} e \left(\frac{1}{2} \left(n + \frac{m'}{2} \right) R^t \text{diag}(z_1, z_2) R \left(n + \frac{m'}{2} \right)^t \right) e \left(\left(n + \frac{m'}{2} \right) \left(\frac{m''}{2} \right)^t \right),$$

where $m' = (m_1, m_2)$ and $m'' = (m_3, m_4)$. Let $(a, b) = (m_1 e_1 + m_2 e_2, m_3 \sigma(e_2) - m_4 \sigma(e_1)) = \phi^{-1}(m)$ as in Lemma 2.1. Then an explicit calculation shows that

$$\left(n + \frac{m'}{2} \right) R^t \text{diag}(z_1, z_2) R \left(n + \frac{m'}{2} \right)^t = \text{tr}_{F/\mathbb{Q}} \left(\left(u + \frac{a}{2} \right)^2 z \right)$$

and

$$\left(n + \frac{m'}{2} \right) (m'')^t = \text{tr}_{F/\mathbb{Q}} \left(\left(u + \frac{a}{2} \right) \frac{b}{\sqrt{D}} \right),$$

where $n = (n_1, n_2)$ and $u = n_1 e_1 + n_2 e_2 \in \mathcal{O}_F$. As n runs through all of $\mathbb{Z}^2$, u runs through all of $\mathcal{O}_F$ and together with the fact that theta constants are well-defined up to their sign, the theorem follows. $\square$

2.5. A variant

In this subsection, we assume that F has a (fundamental) unit $\epsilon > 0$ with $\sigma(\epsilon) < 0$. Such a fundamental unit exists, for example, if D is prime. We will use it for the special case $D = 5$ later. In this case, it is more convenient to use the concept of Hilbert modular forms for $\text{SL}_2(\mathcal{O}_F)$ or its congruence subgroups. Let

$$\theta_{a,b}^\epsilon(z) = \sum_{u \in \mathcal{O}_F} e_{F,\epsilon} \left(\frac{1}{2} \left(u + \frac{a}{2} \right)^2 z \right) e_{F,\epsilon} \left(\frac{1}{2} \left(u + \frac{a}{2} \right) b \right), \quad e_{F,\epsilon}(tz) = e \left(\operatorname{tr}_{F/Q} \left(\frac{t\epsilon}{\sqrt{D}} z \right) \right). \quad (2.5)$$

The function $\theta_{a,b}^\epsilon$ is a Hilbert modular form of weight $\frac{1}{2}$ for the main congruence subgroup $\Gamma(2)$ of $\operatorname{SL}_2(\mathcal{O}_F)$. Let $\alpha = \operatorname{diag}(\frac{\epsilon}{\sqrt{D}}, 1)$, and let

$$\begin{aligned} \phi_0 : \mathbb{H}^2 &\rightarrow \mathbb{H}^2, & (z_1, z_2) &\mapsto (\alpha z_1, \sigma(\alpha) z_2), \\ \phi_0 : \operatorname{SL}_2(\mathcal{O}_F) &\rightarrow \operatorname{SL}_2(\mathcal{O}_F \oplus \partial_F^{-1}), & \gamma &\mapsto \alpha \gamma \alpha^{-1}, \\ \phi_0 : (\mathcal{O}_F/2\mathcal{O}_F)^2 &\cong (\mathcal{O}_F/2\mathcal{O}_F)^2, & (a, b) &\mapsto (a, \epsilon b). \end{aligned}$$

Then ϕ_0 induces a bijection between Hilbert modular forms for subgroups of $\operatorname{SL}_2(\mathcal{O}_F)$ and for the corresponding subgroups of $\operatorname{SL}_2(\mathcal{O}_F \oplus \partial_F^{-1})$. Moreover, one has

$$\phi_0^* \theta_{a,b} = \theta_{a, \epsilon^{-1}b}^\epsilon. \quad (2.6)$$

Now denote $\phi_\epsilon = \phi \circ \phi_0$. Then ϕ_ϵ^* maps Siegel modular forms for a subgroup Γ of $\operatorname{Sp}_2(\mathbb{Z})$ to Hilbert modular forms for $\phi_\epsilon^{-1}(\Gamma)$. Moreover, one can check

$$\phi_\epsilon^{-1}(\operatorname{Sp}_2(\mathbb{Z})) = \operatorname{SL}_2(\mathcal{O}_F), \quad \phi_\epsilon^{-1}(\Gamma(2)) = \Gamma(2),$$

where we use $\Gamma(2)$ for the main congruence subgroup of index 2 in both the symplectic and the Hilbert case. One also has

$$\phi_\epsilon^* \theta_m = \pm \theta_{\phi_\epsilon^{-1}(m)}^\epsilon \quad (2.7)$$

and

$$\phi_\epsilon^{-1}(m) = (m_1 e_1 + m_2 e_2, \epsilon^{-1} m_3 \sigma(e_2) - \epsilon^{-1} m_4 \sigma(e_1)). \quad (2.8)$$

Lemma 2.3. Assume that $\{1, \epsilon\}$ is a $\mathbb{Z}/2\mathbb{Z}$ -basis of $\mathcal{O}_F/2\mathcal{O}_F$, i.e. $\epsilon = x + y \frac{D+\sqrt{D}}{2}$ with y odd.

(1) If $x \equiv 0 \pmod{2}$, then

$$\phi_\epsilon^{-1}(m) = (m_1 + m_2 \sigma(\epsilon), m_3 + m_4 \sigma(\epsilon)).$$

(2) If $x \equiv 1 \pmod{2}$, then

$$\phi_\epsilon^{-1}(m) = (m_1 + m_2 \epsilon, m_3 + m_4 \epsilon).$$

Proof. We check the case $D \equiv 1 \pmod{4}$ and leave the other case to the reader. We remark though that when $D \equiv 0 \pmod{4}$, one has $D \equiv 0 \pmod{8}$ and that $x \equiv 1 \pmod{2}$. Now assume $D \equiv 1 \pmod{4}$ and recall (2.2). When $x \equiv 1 \pmod{2}$, then $\epsilon \equiv \frac{1+\sqrt{D}}{2}$, and so $e_2 = \sigma(\epsilon)$, and $\epsilon^{-1}\sigma(e_2) = 1$, which yields the first part. The second part follows in a similar way. $\square$

3. The Gundlach invariants

In this section, we assume that $D = 5$. We fix $e_1 = 1$ and $e_2 = \frac{1-\sqrt{5}}{2} = \sigma(\epsilon)$ with $\epsilon = \frac{1+\sqrt{5}}{2}$ being a fundamental unit of $F = \mathbb{Q}(\sqrt{5})$. In this case,

$$R = \begin{pmatrix} 1 & \sigma(\epsilon) \\ 1 & \epsilon \end{pmatrix}, \quad \det R = \sqrt{5},$$

and F has narrow class number one. Let

$$\begin{aligned} C_1 &= \{(0, 0), (0, \sigma(\epsilon)), (0, 1), (0, \epsilon), (\sigma(\epsilon), 0), (\sigma(\epsilon), 1), (1, 0), (1, \sigma(\epsilon)), (\epsilon, 0), (\epsilon, \epsilon)\} \\ &= \phi_\epsilon^{-1}(C_0) \end{aligned}$$

be the *even pairs* in $(\mathcal{O}_F/2\mathcal{O}_F)^2$ —the associated theta functions $\theta_{a,b}^\epsilon$ are even theta functions. By Section 2.3, $(a, b) \in C_1$ if and only if $\text{tr}_{F/\mathbb{Q}}(\frac{\epsilon ab}{\sqrt{D}}) \equiv 0 \pmod{2}$. Recall also that a triple of quadruples in C_0^3 is called syzygous if their sum is in C_0 . Similarly, we call a triple in C_1^3 syzygous if their sum is in C_1 . Clearly, the map ϕ_ϵ preserves the ‘syzygous’ property.

For computing the Eisenstein series ψ_6 from Section 2.2, the sign of each summand is determined by $s(l, m, n)$, where $\{l, m, n\} \subset C_0$ is a syzygous triple. Using the bijection ϕ_ϵ , we can express s in terms of a syzygous triple $\{(a, b), (c, d), (e, f)\} \subset C_1^3$ by defining

$$s(a, b; c, d; e, f) := s(\phi_\epsilon(a, b), \phi_\epsilon(c, d), \phi_\epsilon(e, f)).$$

3.1. The Gundlach invariants

We first recall the Gundlach invariants as defined in [Gu] and [LY]. We refer to [LY] for a short summary of Hilbert modular forms on $\text{SL}_2(\mathcal{O}_F)$. For $k \geq 2$, let

$$G_k(z) = 1 + \sum_{t=a+b\frac{1-\sqrt{5}}{2} \in \mathcal{O}_F^+} b_k(t) q_1^a q_2^b \quad (3.1)$$

be the normalized Eisenstein series for $\text{SL}_2(\mathcal{O}_F)$ of weight k , where

$$b_k(t) = \kappa_k \sum_{(\mu) \supset (t)} N(\mu)^{k-1}. \quad (3.2)$$

Here

$$\kappa_k = \frac{(2\pi)^{2k} \sqrt{5}}{(k-1)! 2^k 5^k \zeta_F(k)}$$

is a rational number, (μ) denotes the principal ideal $\mu\mathcal{O}_F$, and $N(\mu) = \#\mathcal{O}_F/(\mu)$. Then

$$\begin{aligned} \theta_6 &= -\frac{67}{2^5 3^3 5^2} (G_6 - G_2^3), \\ \theta_{10} &= 2^{-10} 3^{-5} 5^{-5} 7^{-1} (412751 \cdot G_{10} - 5 \cdot 67 \cdot 2293 \cdot G_2^2 G_6 + 2^2 \cdot 3 \cdot 7 \cdot 4231 \cdot G_2^5) \end{aligned} \quad (3.3)$$

are cusp forms of weight 6 and 10 respectively. Let

$$J_2 = \frac{G_2^5}{\theta_{10}}, \quad \text{and} \quad J_4 = \frac{\theta_6 G_2^2}{\theta_{10}} \quad (3.4)$$

be the two Gundlach invariants defined in [LY]. Then, a theorem of Gundlach [Gu] asserts that they generate the space of meromorphic functions on the Hilbert modular surface $\mathrm{SL}_2(\mathcal{O}_F) \backslash \mathbb{H}^2$. The Igusa invariants are explicit rational functions of J_2 and J_4 when restricting to the Hilbert modular surface (see [LY]). The purpose of this subsection is to compute J_2 and J_4 in terms of theta constants. First, [LY, Theorem 4.4] and (2.7) can be used to obtain the functions G_2^2 , θ_6 and θ_{10} that occur in the formulas for the Gundlach invariants in terms of the Hilbert theta constants via the pullback from Siegel modular forms. This is summarized in the following proposition.

Proposition 3.1. *With notation as above, the below formulas hold:*

$$\begin{aligned} G_2^2 &= 2^{-2} \sum_{(a,b) \in C_1} (\theta_{a,b}^\epsilon)^8, \\ \theta_{10} &= 2^{-12} \prod_{(a,b) \in C_1} (\theta_{a,b}^\epsilon)^2, \end{aligned} \quad (3.5)$$

$$\theta_6 = 2^{-5} 3^{-3} \left(G_2^3 - 2^{-2} \sum_{(*)} (-1)^{s(a,b;c,d,e,f)} (\theta_{a,b}^\epsilon \theta_{c,d}^\epsilon \theta_{e,f}^\epsilon)^4 \right), \quad (3.6)$$

where the summation $(*)$ runs over all syzygous triples $((a,b), (c,d), (e,f)) \in C_1^3$.

Proof. The formulas follow from the representations of ψ_4 , ψ_6 and χ_{10} given by Igusa [Ig2, p. 848] (see Section 2.2 and also [LY, Formulas (2.8)]) together with [LY, Theorem 4.4] and (2.7). Note that in the representation of ψ_6 in [LY, Formulas (2.8)], a factor of 2^{-2} is missing in front of the summation in that formula. $\square$

We remark that $G_4 = G_2^2$ and that we do not obtain the correct sign of G_2 via this approach. The new result of this subsection is an explicit formula for G_2 in terms of the

theta constants and a simpler formula for θ_6 , in which the sum over the 60 syzygous triples is replaced by a sum over the 12-th powers of the ten even theta constants.

Proposition 3.2. *Let*

$$\delta(a, b) = \begin{cases} +1 & \text{if } ab \equiv 0 \pmod{2}, \\ -1 & \text{if } ab \not\equiv 0 \pmod{2}. \end{cases}$$

Then we have

$$G_2 = 2^{-2} \sum_{(a,b) \in C_1} \delta(a, b) (\theta_{a,b}^\epsilon)^4, \\ \theta_6 = 2^{-5} \cdot 3^{-1} (G_2^3 - G_6'),$$

where

$$G_6' = 2^{-2} \sum_{(a,b) \in C_1} \delta(a, b) (\theta_{a,b}^\epsilon)^{12}.$$

Writing out the formulas for $4 \cdot G_2$ and $4 \cdot G_6'$ from above explicitly, gives

$$4G_2 = (\theta_{0,0}^\epsilon)^4 + (\theta_{1,0}^\epsilon)^4 + (\theta_{\epsilon,0}^\epsilon)^4 + (\theta_{\sigma(\epsilon),0}^\epsilon)^4 + (\theta_{0,1}^\epsilon)^4 \\ + (\theta_{0,\epsilon}^\epsilon)^4 + (\theta_{0,\sigma(\epsilon)}^\epsilon)^4 - (\theta_{\epsilon,\epsilon}^\epsilon)^4 - (\theta_{1,\sigma(\epsilon)}^\epsilon)^4 - (\theta_{\sigma(\epsilon),1}^\epsilon)^4, \\ 4G_6' = (\theta_{0,0}^\epsilon)^{12} + (\theta_{1,0}^\epsilon)^{12} + (\theta_{\epsilon,0}^\epsilon)^{12} + (\theta_{\sigma(\epsilon),0}^\epsilon)^{12} + (\theta_{0,1}^\epsilon)^{12} \\ + (\theta_{0,\epsilon}^\epsilon)^{12} + (\theta_{0,\sigma(\epsilon)}^\epsilon)^{12} - (\theta_{\epsilon,\epsilon}^\epsilon)^{12} - (\theta_{1,\sigma(\epsilon)}^\epsilon)^{12} - (\theta_{\sigma(\epsilon),1}^\epsilon)^{12}.$$

Comparing the two formulas for θ_6 in [Propositions 3.1 and 3.2](#), and the formula for the Siegel Eisenstein series ψ_6 in [Section 2.2](#), one obtains the following corollary.

Corollary 3.3. *One has*

$$\phi_\epsilon^* \psi_6 = 3^2 \cdot G_6' - 2^3 \cdot G_2^3.$$

To prove [Proposition 3.2](#), we need the following lemma, which is of independent interest.

Lemma 3.4. *Let $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, and*

$$n(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \alpha \in \mathcal{O}_F, \quad m(\beta) = \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}, \beta \in \mathcal{O}_F^\times.$$

(1) One has

$$\theta_{a,b}^\epsilon(m(\beta)z) = \theta_{\beta a, \beta^{-1}b}^\epsilon(z),$$

$$\theta_{a,b}^\epsilon(wz) = N_{F/\mathbb{Q}}\left(\frac{z}{\epsilon}\right)^{\frac{1}{2}} \theta_{b,a}^\epsilon(z),$$

where $N_{F/\mathbb{Q}}\left(\frac{z}{\epsilon}\right) = \frac{z_1 z_2}{\epsilon \sigma(\epsilon)}$ for $z = (z_1, z_2) \in \mathbb{C}^2$.

(2) One has

$$\theta_{a,b}^\epsilon(n(2\alpha)z) = e_{F,\epsilon}\left(\frac{1}{4}a^2\alpha + \frac{1}{2}\alpha a(1-a)\right) \theta_{a,b}^\epsilon(z),$$

$$\theta_{a,b}^\epsilon(n(\epsilon^{-1})z) = e_{F,\epsilon}\left(\frac{a^2}{8\epsilon} + \frac{a(1-a)}{4\epsilon}\right) \theta_{a,b+a\epsilon^{-1}-\epsilon^{-1}}^\epsilon(z),$$

$$\theta_{a,b}^\epsilon(n(\epsilon)z) = e_{F,\epsilon}\left(\frac{a^2\epsilon}{8} + \frac{a(1-a\epsilon)}{4}\right) \theta_{a,b+a\epsilon-1}^\epsilon(z),$$

$$\theta_{a,b}^\epsilon(n(1)z) = e_{F,\epsilon}\left(\frac{a^2}{8} + \frac{a(\epsilon-a)}{4}\right) \theta_{a,b+a-\epsilon}^\epsilon(z).$$

Proof. A simple expansion gives

$$\theta_{a,b}^\epsilon(z) = e_{F,\epsilon}\left(\frac{ab}{4}\right) e_{F,\epsilon}\left(\frac{a^2}{8}z\right) \sum_{u \in \mathcal{O}_F} e_{F,\epsilon}\left(\frac{1}{2}u^2z + \frac{1}{2}u(az+b)\right) = e_{F,\epsilon}\left(\frac{ab}{4}\right) \theta(\epsilon z, a, \epsilon b),$$

where $\theta(z, a, b)$ is Gundlach's theta function on $\mathbb{H}_0 = \mathbb{H}^+ \times \mathbb{H}^-$ as in [Gu, page 233].

Now the first formula in (1) follows after a substitution $u \mapsto u/\beta$. Gundlach's formula in [Gu, page 234] gives

$$\begin{aligned} \theta_{a,b}^\epsilon(wz) &= e_{F,\epsilon}\left(\frac{ab}{4}\right) N_{F/\mathbb{Q}}\left(\frac{z}{\epsilon}\right)^{\frac{1}{2}} \theta\left(\frac{z}{\epsilon}, b\epsilon, a\right) \\ &= N_{F/\mathbb{Q}}\left(\frac{z}{\epsilon}\right)^{\frac{1}{2}} \theta_{b\epsilon, a\epsilon^{-1}}^\epsilon\left(\frac{z}{\epsilon^2}\right) \\ &= N_{F/\mathbb{Q}}\left(\frac{z}{\epsilon}\right)^{\frac{1}{2}} \theta_{b,a}^\epsilon(z). \end{aligned}$$

The last step follows from the substitution $u \mapsto u\epsilon$ in the summation of the theta function definition.

For (2), one has by definition

$$\begin{aligned} \theta_{a,b}^\epsilon(n(\alpha)z) &= e_{F,\epsilon}\left(\frac{ab}{4}\right) e_{F,\epsilon}\left(\frac{a^2\alpha}{8}\right) e_{F,\epsilon}\left(\frac{a^2}{8}z\right) \\ &\quad \cdot \sum_{u \in \mathcal{O}_F} e_{F,\epsilon}\left(\frac{1}{2}u^2\alpha\right) e_{F,\epsilon}\left(\frac{1}{2}u^2z + \frac{1}{2}u(az + a\alpha + b)\right). \end{aligned}$$

When $\alpha \in 2\mathcal{O}_F$, $e_{F,\epsilon}(\frac{1}{2}u^2\alpha) = 1$, then the first formula in (2) is clear.

When $\alpha = \epsilon^{-1}$, notice that $u^2 + u \equiv 0 \pmod{2}$. So

$$e_{F,\epsilon} \left(\frac{1}{2} u^2 \epsilon^{-1} + \frac{1}{2} u \epsilon^{-1} \right) = e \left(\frac{1}{2} \operatorname{tr}_{F/\mathbb{Q}} \frac{u^2 + u}{\sqrt{5}} \right) = 1,$$

and

$$\begin{aligned} \theta_{a,b}^\epsilon(n(\epsilon^{-1})z) &= e_{F,\epsilon} \left(\frac{a^2}{8\epsilon} \right) e_{F,\epsilon} \left(\frac{ab}{4} \right) e_{F,\epsilon} \left(\frac{a^2}{8} z \right) \\ &\quad \cdot \sum_{u \in \mathcal{O}_F} e_{F,\epsilon} \left(\frac{1}{2} u^2 z + \frac{1}{2} u (az + a\epsilon^{-1} + b - \epsilon^{-1}) \right) \\ &= e_{F,\epsilon} \left(\frac{a^2}{8\epsilon} \right) e_{F,\epsilon} \left(\frac{a(1-a)}{4\epsilon} \right) \theta_{a,b+\epsilon^{-1}a-\epsilon^{-1}}^\epsilon(z). \end{aligned}$$

Similarly, when $\alpha = \epsilon$, a direct calculation verifies for all $u \in \mathcal{O}_F$

$$e_{F,\epsilon} \left(\frac{1}{2} u^2 \epsilon + \frac{1}{2} u \right) = 1,$$

and thus the third formula in (2) holds.

When $\alpha = 1$, one checks that

$$e_{F,\epsilon} \left(\frac{1}{2} u^2 + \frac{1}{2} u \epsilon \right) = 1,$$

and so the fourth formula in (2) holds.

We remark that the third and fourth formulas can also be derived with the help of $n(\epsilon) = m(\epsilon)n(\epsilon^{-1})m(\epsilon^{-1})$ and $n(1) = n(-2\epsilon^{-1})n(\epsilon)n(\epsilon^{-1})$. $\square$

Let

$$\Gamma(2) = \{\gamma \in \operatorname{SL}_2(\mathcal{O}_F) : \gamma \equiv 1 \pmod{2}\}.$$

Then $\Gamma(2)$ is clearly generated by $m(\beta)$, $\beta \in \mathcal{O}_F^\times$ and $\beta \equiv 1 \pmod{2}$, $n(\alpha)$, and $n_-(\alpha)$, $\alpha \in 2\mathcal{O}_F$, where $n_-(\alpha) = wn(-\alpha)w^{-1}$. Let Θ be the subgroup of $\operatorname{SL}_2(\mathcal{O}_F)$ generated by $\Gamma(2)$, w , and all $m(\beta)$ with $\beta = 1, \epsilon^{\pm 1}$ (the so-called theta group). Then [Lemma 3.4](#) implies

Corollary 3.5.

- (1) The function $(\theta_{0,0}^\epsilon)^4$ is a Hilbert modular form for Θ of weight 2.
- (2) For all $(a, b) \in (\mathcal{O}_F/2\mathcal{O}_F)^2$, $(\theta_{a,b}^\epsilon)^4$ is a Hilbert modular form for $\Gamma(2)$ of weight 2.

Proof. It suffices to check that $(\theta_{a,b}^\epsilon)^4|_2\gamma = (\theta_{a,b}^\epsilon)^4$ for generators of $\Gamma(2)$, and in the case $(a,b) = (0,0)$, for generators of Θ . Here

$$f|_k\gamma(z) = N(cz + d)^{-k}f(\gamma(z)), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is the usual weight k slash operator. The verification follows from Lemma 3.4 immediately. For $\beta \equiv 1 \pmod{2}$ and $\beta \in \mathcal{O}_F^\times$,

$$(\theta_{a,b}^\epsilon)^4|_2m(\beta)(z) = N(\beta)^2(\theta_{a,b}^\epsilon)^4(m(\beta)z) = (\theta_{\beta a, \beta^{-1}b}^\epsilon)^4 = (\theta_{a,b}^\epsilon)^4.$$

We leave the other verification to the reader. $\square$

Proof of Proposition 3.2. Corollary 3.5 asserts that $(\theta_{0,0}^\epsilon)^4$ is a modular form for Θ of weight 2. So the trace

$$f = \sum_{\gamma \in \Theta \backslash \mathrm{SL}_2(\mathcal{O}_F)} (\theta_{0,0}^\epsilon)^4|_2\gamma$$

is a modular form for $\mathrm{SL}_2(\mathcal{O}_F)$ of weight 2. Notice that

$$\begin{aligned} \Gamma(2) \backslash \mathrm{SL}_2(\mathcal{O}_F) &= \{n(\alpha) : \alpha = 0, 1, \epsilon^{\pm 1}\} \\ &\cup \{n(\alpha_1)wm(\beta)n(\alpha_2) : \alpha_j = 0, 1, \epsilon^{\pm 1}, \beta = 1, \epsilon^{\pm 1}\}. \end{aligned}$$

For this, one can check that $\Theta \backslash \mathrm{SL}_2(\mathcal{O}_F)$ has a complete set of representatives as follows:

$$n(\alpha), n_-(\alpha) = \begin{pmatrix} 1 & 0 \\ \alpha & 0 \end{pmatrix}, \alpha = 0, 1, \epsilon^{\pm 1}, \quad n_-(\epsilon^{\pm 1})n(1), \text{ and } n_-(1)n(\epsilon). \quad (3.7)$$

Now, a direct calculation using Lemma 3.4 gives

$$f = \sum_{(a,b) \in C_1} \delta(a,b) (\theta_{a,b}^\epsilon)^4.$$

Since $\mathrm{SL}_2(\mathcal{O}_F)$ has only one modular form of weight 2 up to scalar multiples, there is a constant C such that

$$G_2 = C \sum_{(a,b) \in C_1} \delta(a,b) (\theta_{a,b}^\epsilon)^4.$$

Comparing the constant term, one sees that $C = 2^{-2}$. This proves the formula for G_2 .

The same computation as above gives the following modular form of weight 6,

$$g = \sum_{\gamma \in \Theta \backslash \mathrm{SL}_2(\mathcal{O}_F)} (\theta_{0,0}^\epsilon)^{12}|_6\gamma = \sum_{(a,b) \in C_1} \delta(a,b) (\theta_{a,b}^\epsilon)^{12} = 4G'_6, \quad (3.8)$$

which is not a multiple of G_2^3 . The classical result of Gundlach [Gu] (see also [LY, Theorem 4.2]) asserts that $\dim M_6^{\text{Sym}}(\text{SL}_2(\mathcal{O}_F)) = 2$ (space of symmetric modular forms of weight 2 for $\text{SL}_2(\mathcal{O}_F)$). So there are constants A and B such that

$$\theta_6 = A \cdot G_2^3 + B \cdot G_6'.$$

An explicit comparison of the terms in the formula with those in Proposition 3.1 yields the constants $A = -B = 2^{-5} \cdot 3^{-1}$. $\square$

4. Rosenhain invariants

In this section, we describe how to use the pull-back map to express the Rosenhain invariants for genus 2 curves in terms of Hilbert theta functions. For generating genus 2 curves for use in cryptography, there are many different possible combinations of 6 even Siegel theta constants which can be used to construct a Rosenhain model for the curve C ,

$$C: y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3), \quad (4.1)$$

with

$$\lambda_1 = -\frac{\theta_{i_1}^2 \theta_{i_3}^2}{\theta_{i_4}^2 \theta_{i_6}^2}, \quad \lambda_2 = -\frac{\theta_{i_2}^2 \theta_{i_3}^2}{\theta_{i_5}^2 \theta_{i_6}^2}, \quad \lambda_3 = -\frac{\theta_{i_1}^2 \theta_{i_2}^2}{\theta_{i_4}^2 \theta_{i_5}^2}.$$

Several different choices for the combination of even theta constants have appeared in the literature, but here we use the following choice which coincides with van Wamelen [vW]. The characteristics $(i_1, \dots, i_6)$ are as follows:

$$\begin{aligned} i_1 &= (0, 0, 1, 0); & i_2 &= (0, 0, 1, 1); & i_3 &= (0, 1, 1, 0); \\ i_4 &= (1, 0, 0, 0); & i_5 &= (1, 0, 0, 1); & i_6 &= (1, 1, 0, 0) \end{aligned}$$

We propose to evaluate these functions by computing the pull-backs of the theta constants to the Hilbert moduli space. Using the fact that $\phi_\epsilon^* \theta_m = \pm \theta_{\phi_\epsilon^{-1}(m)}^\epsilon$, and that $\phi_\epsilon^{-1}(m) = (m_1 e_1 + m_2 e_2, \epsilon^{-1} m_3 \sigma(e_2) - \epsilon^{-1} m_4 \sigma(e_1))$, we can express the Rosenhain invariants as values of functions of the Hilbert theta constants. For example, using Lemma 2.3 for $D = 5$, we obtain

$$\lambda_1 = -\left(\frac{\theta_{(0,1)}^\epsilon \theta_{(\sigma(\epsilon),1)}^\epsilon}{\theta_{(1,0)}^\epsilon \theta_{(\epsilon,0)}^\epsilon}\right)^2, \quad \lambda_2 = -\left(\frac{\theta_{(0,\epsilon)}^\epsilon \theta_{(\sigma(\epsilon),1)}^\epsilon}{\theta_{(1,\sigma(\epsilon))}^\epsilon \theta_{(\epsilon,0)}^\epsilon}\right)^2, \quad \lambda_3 = -\left(\frac{\theta_{(0,1)}^\epsilon \theta_{(0,\epsilon)}^\epsilon}{\theta_{(1,0)}^\epsilon \theta_{(1,\sigma(\epsilon))}^\epsilon}\right)^2. \quad (4.2)$$

This choice of Rosenhain invariants was used to compute the examples of the Hilbert Rosenhain polynomials in Section 6.

5. CM points and the computation of Igusa invariants

Let K be a CM field, i.e. a totally imaginary quadratic extension of F with CM type $\Phi = \{\sigma_1, \sigma_2\}$. We assume that $\sigma_1|_F = \text{id}$ and $\sigma_2|_F = \sigma$. Fix an element $\xi_0 \in K$ with $\bar{\xi}_0 = -\xi_0$ and $\Phi(\xi_0) = (\sigma_1(\xi_0), \sigma_2(\xi_0)) \in \mathbb{H}^2$. We denote by F^+ the set of totally positive elements in F .

5.1. CM points

The construction of CM points on $X(\mathfrak{f}_0) = \text{SL}_2(\mathcal{O}_F \oplus \mathfrak{f}_0) \backslash \mathbb{H}^2$ of CM type $(\mathcal{O}_K, \Phi)$ is described in [BY, Section 3], which we briefly review here. In general, for a fractional ideal $\mathfrak{f}_0$ of F , let $\text{CM}(\mathcal{O}_K, \Phi, \mathfrak{f}_0)$ be the set of CM points on $X(\mathfrak{f}_0)$ of CM type $(\mathcal{O}_K, \Phi)$. The elements of $\text{CM}(\mathcal{O}_K, \Phi, \mathfrak{f}_0)$ are indexed by equivalence classes $[\mathfrak{a}, r]$ of pairs $(\mathfrak{a}, r)$, where $r \in F^+$ is totally positive and $\mathfrak{a}$ is a fractional ideal of K satisfying

$$\xi_0 \partial_{K/F} \mathfrak{a} \bar{\mathfrak{a}} \cap F = r \mathfrak{f}_0.$$

Two pairs $(\mathfrak{a}_1, r_1)$ and $(\mathfrak{a}_2, r_2)$ are equivalent if there is a $z \in K^\times$ such that $\mathfrak{a}_2 = z\mathfrak{a}_1$ and $r_2 = r_1 z \bar{z}$, i.e. $[\mathfrak{a}, r] = [z\mathfrak{a}, rz\bar{z}]$ for any $z \in K^\times$. Given such a pair, one can write

$$\mathfrak{a} = \mathcal{O}_F \alpha + \mathfrak{f}_0 \beta, \quad \Phi\left(\frac{\alpha}{\beta}\right) \in \mathbb{H}^2, \quad (5.1)$$

with $\xi_0(\bar{\alpha}\beta - \alpha\bar{\beta}) = r$. The point $z = \Phi\left(\frac{\alpha}{\beta}\right) \in \mathbb{H}^2$ is the CM point associated to $[\mathfrak{a}, r]$. It is convenient to introduce the generalized class group $\mathcal{C}(K)$, which is the quotient of

$$\{(\mathfrak{a}, r) : \mathfrak{a} \text{ fractional ideal of } K, r \in F^+, N_{K/F} \mathfrak{a} = r \mathcal{O}_F\} \quad (5.2)$$

by the subgroup of $\{(z\mathcal{O}_K, z\bar{z}) : z \in K^\times\}$. Then it is known that $\mathcal{C}(K)$ acts on $\text{CM}(\mathcal{O}_K, \Phi, \mathfrak{f}_0)$ transitively via

$$(\mathfrak{a}, r)[\mathfrak{b}, s] = [\mathfrak{a}\mathfrak{b}, rs].$$

One also has the following exact sequence

$$1 \rightarrow \mathcal{O}_F^{\times,+} / N_{K/F} \mathcal{O}_K^{\times} \xrightarrow{u \mapsto (\mathcal{O}_K, u)} \mathcal{C}(K) \xrightarrow{(\mathfrak{a}, \alpha) \mapsto \mathfrak{a}} \text{Cl}(K) \xrightarrow{N_{K/F}} \text{Cl}^+(F) \rightarrow 1,$$

where $\text{Cl}^+(F)$ is the narrow class group of F . In particular, if the fundamental unit $\epsilon > 1$ is not totally positive, as is the case when $F = \mathbb{Q}(\sqrt{5})$, one has $\mathcal{C}(K) = \text{Cl}_0(K) = \ker(N_{K/F})$. In this case, one also has an isomorphism

$$\text{CM}(\mathcal{O}_K, \Phi, \mathcal{O}_F) \rightarrow \text{CM}(\mathcal{O}_K, \Phi, \partial_F^{-1}), \quad [\mathfrak{a}, r] \mapsto [\mathfrak{a}, r\sqrt{D}/\epsilon],$$

which is compatible with the isomorphism

$$\mathrm{SL}_2(\mathcal{O}_F) \backslash \mathbb{H}^2 \rightarrow \mathrm{SL}_2(\mathcal{O}_F \oplus \partial_F^{-1}) \backslash \mathbb{H}^2, \quad (z_1, z_2) \mapsto \left(\frac{\epsilon}{\sqrt{D}} z_1, \sigma \left(\frac{\epsilon}{\sqrt{D}} \right) z_2 \right).$$

We denote by $\mathrm{CM}(K)$ the CM points associated to the elements of $\mathrm{CM}(\mathcal{O}_K, \Phi, \partial_F^{-1})$ for all possible CM types, and define the *Gundlach class polynomials* as in [LY] to be:

$$P_2(x) = \prod_{z \in \mathrm{CM}(K)} (x - J_2(z)) \in \mathbb{Q}[x]$$

$$P_4(x) = \prod_{z \in \mathrm{CM}(K)} (x - J_4(z)) \in \mathbb{Q}[x].$$

In the next subsection, we explain that the class polynomials might not be equal to the minimal polynomials in general. This is different from the case of classical singular moduli.

5.2. The reflex field and the Galois orbit of a CM point

For a given CM point $[\mathfrak{a}, r] \in \mathrm{CM}(\mathcal{O}_K, \Phi, \mathfrak{f}_0)$, its Galois orbit may be a proper subset and can be described explicitly by the reflex field $(\tilde{K}, \tilde{\Phi})$ and the type norm map ([Sh] and [BY, page 247]). Recall that $\tilde{K} \subset \mathbb{C}$ is generated by all the type norms $N_{\Phi}(x) = \sigma_1(x)\sigma_2(x)$. To define the reflex CM type $\tilde{\Phi}$, let M be the composite of K and $\tilde{K}$, which is either dihedral over $\mathbb{Q}$ of degree 8 or equal to K itself depending on whether K is non-Galois or cyclic. Extend Φ to a CM type of M

$$\Phi_M = \{\tau \in \mathrm{Gal}(M/\mathbb{Q}) : \tau|_K \in \Phi\}.$$

It can be shown that Φ_M^{-1} is also the extension of a unique CM type $\tilde{\Phi}$ of $\tilde{K}$, the reflex CM type of Φ . Let

$$N_{\tilde{\Phi}} : \mathrm{Cl}(\tilde{K}) \rightarrow \mathrm{Cl}(K), \quad \tilde{\mathfrak{b}} \mapsto \tilde{\sigma}_1(\tilde{\mathfrak{b}})\tilde{\sigma}_2(\tilde{\mathfrak{b}})\mathcal{O}_M \cap \mathcal{O}_K.$$

This map actually gives a map to $\mathcal{C}(K)$, which we still call type norm and denote by $N_{\tilde{\Phi}}$

$$N_{\tilde{\Phi}} : \mathrm{Cl}(\tilde{K}) \rightarrow \mathcal{C}(K), \quad \tilde{\mathfrak{b}} \mapsto (N_{\tilde{\Phi}}(\tilde{\mathfrak{b}}), N(\tilde{\mathfrak{b}})). \quad (5.3)$$

It is convenient at this moment to define the type class group $\mathrm{Cl}(\tilde{K}, \tilde{\Phi})$ as $\mathrm{Cl}(\tilde{K})/\ker(N_{\tilde{\Phi}})$ and define the type class field $H(\tilde{K}, \tilde{\Phi})$ as the associated class field of $\tilde{K}$. According to [Sh, page 112], the CM point $[\mathfrak{a}, r]$ is defined over the type class field $H(\tilde{K}, \tilde{\Phi})$, and the action is given, via class field theory, by

$$[\mathfrak{a}, r]^{\sigma_{\tilde{\mathfrak{b}}}} = (\mathfrak{a} N_{\tilde{\Phi}}(\tilde{\mathfrak{b}}), r N(\tilde{\mathfrak{b}})), \quad (5.4)$$

where $\sigma_{\tilde{\mathfrak{b}}}$ is the Galois element associated to the ideal $\tilde{\mathfrak{b}}$. So we have

Proposition 5.1. *Given $[\mathfrak{a}, r] \in \text{CM}(\mathcal{O}_K, \Phi, \mathfrak{f}_0)$, its Galois orbit over $\tilde{K}$ is the orbit of $[\mathfrak{a}, r]$ under the action of $\text{Cl}(\tilde{K}, \tilde{\Phi})$ via the type norm map.*

One can actually prove that the orbit or equivalently the cycle (formal sum) $\sum_{C \in \text{Cl}(\tilde{K}, \tilde{\Phi})} Cz$ of $z = [\mathfrak{a}, r]$ is defined over $\tilde{F}$ in general and is defined over $\mathbb{Q}$ if $K = \tilde{K}$ is cyclic over $\mathbb{Q}$. Enge and Thomé describe an algorithm in [ET, Algorithm 2] to compute the image group $\text{Im}(N_{\tilde{\Phi}} : \text{Cl}(\tilde{K}) \rightarrow \mathcal{C}(K))$. Using [ET, Algorithm 2], one can compute the minimal polynomial of $f(z)$ over $\tilde{K}$ for a fixed CM point $z = [\mathfrak{a}, r] \in \text{CM}(K, \Phi)$ and a meromorphic Hilbert modular form for $\text{SL}_2(\mathcal{O}_F \oplus \mathfrak{f}_0)$ of weight 0 and coefficients in $\mathbb{Q}$ (and it will actually be defined over $\tilde{F}$):

$$f^{z, \Phi}(x) = \prod_{C \in \text{Cl}(\tilde{K}, \tilde{\Phi})} (x - f(Cz)). \quad (5.5)$$

Let $f^z(x)$ be the minimal polynomial of $f(z)$ over $\mathbb{Q}$, which is either $f^{z, \Phi}$ or the product of $f^{z, \Phi}$ and its conjugate. In particular, when $F = \mathbb{Q}(\sqrt{5})$, $\mathfrak{f}_0$, and $f = J_i$ ($i = 2, 4$) are the Gundlach invariants, it is clear by the definition and Proposition 5.1 that

$$J_i^z(x) | P_i(x), \quad \text{and} \quad \deg \frac{P_i(x)}{J_i^z(x)} = \frac{|\mathcal{C}(K)|}{|\text{Cl}(\tilde{K}, \tilde{\Phi})|}.$$

In general, when f is an Igusa function j_i ($i = 1, 2, 3$) on $\text{SL}_2(\mathcal{O}_F \oplus \partial^{-1}) \backslash \mathbb{H}^2$, one has that $j_i^z(x)$ is a factor of the Igusa class polynomial of $j_i(z)$ (product over all CM points).

Remark 5.2. Since $N_{\tilde{\Phi}} \circ N_{\Phi} = 2$ on $\text{Cl}(\tilde{K})$, the image of the type norm in $\mathcal{C}(K)$ has 2-power index. In particular, if the absolute discriminant $d_K = p^2 q$ with primes $p \equiv q \equiv 1 \pmod{4}$ as considered in [BY], the type norm is surjective and one has $J_i^z = J_i$.

5.3. CM points with level

For Rosenhain invariants, we need CM points with level 2. Let $N > 1$ be a positive integer and let

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathcal{O}_F \oplus \mathfrak{f}_0) : a \equiv d \equiv 1 \pmod{N}, b \in N\mathfrak{f}_0, c \in N\mathfrak{f}_0^{-1} \right\}$$

be the main congruence subgroup, and let $X(N) = \Gamma(N) \backslash \mathbb{H}^2$ be the associated Hilbert modular surface (which of course depends on $\mathfrak{f}_0$). In this case, the set of CM points $\text{CM}(\mathcal{O}_K, \Phi, \mathfrak{f}_0, N)$ is indexed by equivalence classes of $(\mathfrak{a}, r, \alpha, \beta)$, where

- (1) $[\mathfrak{a}, r] \in \text{CM}(\mathcal{O}_K, \Phi, \mathfrak{f}_0)$;
- (2) $\mathfrak{a} = \mathcal{O}_F \alpha + \mathfrak{f}_0 \beta$ and $\Phi(\frac{\alpha}{\beta}) \in \mathbb{H}^2$;
- (3) $\xi_0(\bar{\alpha}\beta - \alpha\bar{\beta}) = r$.

Two such quadruples are equivalent if there are $z \in K^\times$ and $\gamma \in \Gamma(N)$ such that

$$\mathfrak{a}_1 = z\mathfrak{a}_2, \quad r_1 = r_2 z \bar{z}, \quad (\alpha_1, \beta_1)^t = \gamma(\alpha_2, \beta_2)^t.$$

The associated CM point in $X(N)$ is $\tau = \Phi(\frac{\alpha}{\beta})$, which we also denote by $\tau = [\mathfrak{a}, r, \alpha, \beta]$. We can use it to define the class polynomial of the Rosenhain invariants. The natural forgetful map gives a surjective projection from $\text{CM}(\mathcal{O}_K, \Phi, \mathfrak{f}_0, N)$. Each CM point is defined over a class field of $\tilde{K}$, given in [Ya3] using idèles. In particular, the following type class group of level N

$$\text{Cl}(\tilde{K}, \tilde{\Phi}, N) = \frac{\{\text{all fractional ideals of } \tilde{K} \text{ prime to } N\}}{\{\mathfrak{b} : \mathbf{N}_{\tilde{\Phi}}(\mathfrak{b}) = \mu \mathcal{O}_K, \mu \bar{\mu} = \mathbf{N}(\mathfrak{b}), \mu \equiv 1 \pmod{N}\}}$$

acts on $\text{CM}(\mathcal{O}_K, \Phi, \mathfrak{f}_0, N)$ as follows:

$$[\mathfrak{a}, r, \alpha, \beta]^{\sigma_{\mathfrak{b}^{-1}}} = [\mathfrak{a} \mathbf{N}_{\tilde{\Phi}}(\mathfrak{b}), r \mathbf{N}(\mathfrak{b}), \alpha_1, \beta_1]$$

where α_1 and β_1 satisfy

$$\mathfrak{a} \mathbf{N}_{\tilde{\Phi}}(\mathfrak{b}) = \mathcal{O}_F \alpha_1 + \mathfrak{f}_0 \beta_1, \quad \alpha_1 \equiv \alpha \pmod{N}, \quad \beta_1 \equiv \beta \mathbf{N}(\mathfrak{b}) \pmod{N}.$$

Each orbit is defined over $\tilde{F}$, and we can use the orbit of a CM point to define the minimal polynomials of its Rosenhain invariants as we did with Gundlach invariants.

5.4. Computing the CM values of $\theta_{a,b}$ numerically

Let $z = z_{\mathfrak{a}} = (z_1, z_2)$ be a CM point in $\text{SL}_2(\mathcal{O}_F \oplus \partial_F^{-1}) \backslash \mathbb{H}^2$, and write $y_i = \Im(z_i)$. Consider for a positive number $M > 0$ the elliptic region

$$E_M : u_1^2(y_1 + y_2) + 2u_1 u_2(e_2 y_1 + \sigma(e_2) y_2) + u_2^2(e_2 y_1 + \sigma(e_2)^2 y_2) \leq 4M. \quad (5.6)$$

It has area $\text{Area}(E_M) = \frac{4\pi M}{(\det R)y_1 y_2}$. Let $\theta_{a,b}(z, M)$ be the partial theta function which sums only over points in the elliptic region E_M :

$$\theta_{a,b}(z, M) = \sum_{\substack{u=n_1 e_1 + n_2 e_2 \in \mathcal{O}_F \\ (2n_1 + a_1, 2n_2 + a_2) \in E_M}} e\left(\frac{1}{2} \text{tr}_{F/\mathbb{Q}}\left(u + \frac{a}{2}\right)^2 z\right) e\left(\frac{1}{2} \text{tr}_{F/\mathbb{Q}}\left(u + \frac{a}{2}\right) \frac{b}{\sqrt{D}}\right).$$

The partial theta value (for a fixed z) approximates $\theta_{a,b}(z)$, with an error term $\text{Err}_{a,b}(z, M)$ satisfying:

$$|\text{Err}_{a,b}(z, M)| \leq \sum_{\substack{u=n_1 e_1 + n_2 e_2 \in \mathcal{O}_F \\ (u_1, u_2) \notin E_M}} e^{-\frac{\pi}{4}(u_1^2(y_1+y_2)+2u_1 u_2(e_2 y_1+\sigma(e_2) y_2)+u_2^2(e_2^2 y_1+\sigma(e_2)^2 y_2))},$$

where $(u_1, u_2) = (2n_1 + a_1, 2n_2 + a_2)$. The area of the ellipse is approximated by the number of lattice points in the interior

$$\text{Area}(E_t) \approx \#\{(u_1, u_2) \in \mathbb{Z}^2 \cap E_t\},$$

so

$$|\text{Err}_{a,b}(z, M)| \leq \int_M^\infty \frac{d}{dt}(\text{Area}(E_t)) e^{-\pi t} dt = \frac{4}{(\det R) y_1 y_2} e^{-\pi M}. \quad (5.7)$$

In [Appendix A](#), we explain the details and present an algorithm for determining a choice of M which assures that the theta values $\theta_{a,b}(z, M)$ are accurate to a given precision s .

5.5. Algorithm

Input: A primitive quartic CM field K with real quadratic subfield F .

Output: Class polynomials for Gundlach, Rosenhain, or Igusa invariants.

Step 1: Find all the CM points $[\mathfrak{a}, r]$, and write

$$\mathfrak{a} = \mathcal{O}_F \alpha + \partial_F^{-1} \beta, \quad \xi_0(\bar{\alpha} \beta - \alpha \bar{\beta}) = r,$$

with $z_{[\mathfrak{a}, r]} = \Phi(\frac{\alpha}{\beta}) \in \mathbb{H}^2$.

Step 2: Compute $\theta_{a,b}(z_{[\mathfrak{a}, r]}) \approx \theta_{a,b}(z_{[\mathfrak{a}, r]}, M)$ with chosen accuracy parameter M as in [Section 5.4](#) for all even pairs $(a, b) \in (\mathcal{O}_F/2)^2$.

Step 3: Use [Proposition 3.1](#), [Eqs. \(4.2\)](#), or the definition of Igusa invariants in terms of theta functions ([Section 2.2](#)) and $\theta_m(\phi(z_{[\mathfrak{a}, r]})) \approx \theta_{\phi^{-1}(m)}(z_{[\mathfrak{a}, r]}, M)$ to compute approximations to either Gundlach, Rosenhain, or Igusa invariants.

Step 4: Form approximations to the class polynomials for the invariants by repeating steps 1–3 for all CM points and multiplying out the polynomial.

Step 5: Clear the denominators by multiplying the polynomial by either the Bruinier–Yang formula [[BY, Ya1, Ya2](#)] or the Lauter–Viray [[LV](#)] formula. If the precision and the bound M were set high enough in the computation, then the result will be recognizable polynomials with integer coefficients.

Remark 5.3. When F has a fundamental unit $\epsilon > 0$ with $\sigma(\epsilon) < 0$, we can use $\theta_{a,b}^\epsilon$ and the CM points $z_{\mathfrak{a}}$ in $\text{SL}_2(\mathcal{O}_F) \backslash \mathbb{H}^2$ in the above algorithm.

Remark 5.4. When the Hilbert modular surface $\text{SL}_2(\mathcal{O}_F \oplus \partial_F^{-1}) \backslash \mathbb{H}^2$ (or $\text{SL}_2(\mathcal{O}_F) \backslash \mathbb{H}^2$) is rational, e.g. when $D = 5, 8, 13, 17$, $\mathbb{C}(\text{SL}_2(\mathcal{O}_F) \backslash \mathbb{H}^2) = \mathbb{C}(J_1, J_2)$ for two Hilbert rational functions J_1 and J_2 , we can write J_1 and J_2 as rational functions of $\theta_{a,b}$ explicitly. Just as in the case of $D = 5$ for the Gundlach invariants, we recognize CM values J_1 and J_2 as algebraic numbers and then express the pull-backs of the Igusa invariants, $\phi^*(j_i)$, as

explicit rational functions of J_1 and J_2 . When $D = 12$, one can do the same but one needs to replace $\mathrm{SL}_2(\mathcal{O}_F)$ by $\mathrm{SL}_2(\mathcal{O}_F \oplus \partial^{-1})$ as there is no unit $\epsilon > 0$ with $\sigma(\epsilon) < 0$.

6. Examples

In this section, we give concrete numerical examples illustrating the algorithm from the previous section. The results are polynomials which have as their roots either the Gundlach or the Hilbert Rosenhain invariants, obtained from a given quartic CM field K as the input.

6.1. Gundlach and Rosenhain invariants for K Galois of class number 2

We fix the quartic CM field K given by $f = X^4 + 10X^2 + 20$, which means that $K = \mathbb{Q}(\alpha)$ for $\alpha = i\sqrt{5 - \sqrt{5}}$ and $\mathrm{disc}(K) = 128\,000 = 2^{10}5^3$.

Example 6.1 ($K = \mathbb{Q}(\alpha)$, $\alpha = i\sqrt{5 - \sqrt{5}}$, Galois, class number $h = 2$). Approximations to the CM points in the Hilbert space are:

$$\begin{aligned} z_1 &= [1.6625077511098137144i, 2.6899940478558293078i], \\ z_2 &= [0.83125387555490685718i, 1.3449970239279146539i]. \end{aligned}$$

Approximations to the Gundlach invariants (truncated here for space reasons):

$$\begin{aligned} J_2(z_1) &= 47\,239\,200\,000.000000000, \\ J_4(z_1) &= 243\,000.00000000000000, \\ J_2(z_2) &= 1\,606\,611.5702479338843, \\ J_4(z_2) &= 1859.5041322314049587. \end{aligned}$$

The guess $N = 121 = 11^2$ for the denominator was obtained from the denominator bound for θ_{10} from the Brunier–Yang formula.

Polynomials $P_2(X) = N(X - J_2(z_1))(X - J_2(z_2))$, $P_4(X) = N(X - J_4(z_1))(X - J_4(z_2))$:

$$\begin{aligned} P_2 &= 121X^2 - 5\,716\,137\,600\,000X + 9\,183\,300\,480\,000\,000 \\ &= 121(X - 47\,239\,200\,000)(X - 194\,400\,000/121) \\ P_4 &= 121X^2 - 29\,628\,000X + 54\,675\,000\,000 \\ &= 121(X - 243\,000)(X - 225\,000/121) \end{aligned}$$

Coefficients of P_2 :

$$9\,183\,300\,480\,000\,000\,000 = 2^{16} \cdot 3^{15} \cdot 5^{10}$$

$$-5\,716\,137\,600\,000 = 2^{10} \cdot 3^5 \cdot 5^5 \cdot 7351$$

$$121 = 11^2$$

Coefficients of P_4 :

$$54\,675\,000\,000 = 2^6 \cdot 3^7 \cdot 5^8$$

$$-29\,628\,000 = 2^5 \cdot 3^2 \cdot 5^3 \cdot 823$$

$$121 = 11^2$$

Next, we show the minimal polynomials for the Hilbert Rosenhain invariants for the same example as above for comparison.

Example 6.2 ($K = \mathbb{Q}(\alpha)$, $\alpha = i\sqrt{5 - \sqrt{5}}$, Galois, class number $h = 2$). Approximations to the CM points on the Hilbert space are:

$$z_1 = [1.0274862967460155935i, 4.3525017989656430222i],$$

$$z_2 = [0.51374314837300779674i, 2.1762508994828215111i].$$

Approximations to the Rosenhain invariants (truncated here for space reasons):

$$\lambda_1(z_1) = 0.59656940396484372528,$$

$$\lambda_2(z_1) = 0.60458979726548646316,$$

$$\lambda_3(z_1) = 27.793195626142313749,$$

$$\lambda_1(z_2) = 0.071476336699009695572,$$

$$\lambda_2(z_2) = 0.10591819044764272223,$$

$$\lambda_3(z_2) = 0.89132121471838656590.$$

The Rosenhain invariants generate the quartic field $\mathbb{Q}[x]/(r(x))$, where

$$r(x) = x^4 - 72x^3 - 56x^2 + 32x + 16.$$

The minimal polynomials are as follows:

$$\begin{aligned}
\lambda_1(z_1) &: x^4 - 72x^3 - 56x^2 + 32x + 16 \\
\lambda_1(z_2) &: 16x^4 - 432x^3 - 1996x^2 - 1548x + 121 \\
\lambda_2(z_1) &: x^4 - 44x^3 - 44x^2 + 16x + 16 \\
\lambda_2(z_2) &: 16x^4 + 496x^3 - 604x^2 - 1084x + 121 \\
\lambda_3(z_1) &: x^4 - 28x^3 + 4x^2 + 48x + 16 \\
\lambda_3(z_2) &: 16x^4 + 32x^3 - 8696x^2 - 8712x + 14\,641
\end{aligned}$$

As is clear in this example compared with the previous one, the coefficients of the minimal polynomials of the Rosenhain invariants are typically much smaller than the coefficients of the Igusa class polynomials or the Gundlach class polynomials. This is due to the simpler expression for the Rosenhain invariants in terms of squares of theta constants. Rosenhain invariants have another advantage because they directly yield the equation of the hyperelliptic curve via the Rosenhain model given in Eq. (4.1). However, the disadvantage is that the degree can be larger.

6.2. Gundlach invariants for K Galois of class number 8

The next example computes Gundlach invariants for the quartic, Galois CM field K given by $f = X^4 + 660X^2 + 87\,120$, i.e. $K = \mathbb{Q}(\alpha)$ with $\alpha = i\sqrt{330 - 66\sqrt{5}}$ and $\text{disc}(K) = 10\,579\,705\,602\,048\,000 = 2^{16} \cdot 3^6 \cdot 5^3 \cdot 11^6$.

Example 6.3 ($K = \mathbb{Q}(\alpha)$, $\alpha = i\sqrt{330 - 66\sqrt{5}}$, Galois, class number $h = 8$). Approximations to the CM points in the Hilbert space:

$$\begin{aligned}
z_1 &= [1.3090169943749474241 + 5.4634037382557251841i, \\
&\quad 0.19098300562505257590 + 3.3765692045052723164i] \\
z_2 &= [-0.50000000000000000000 + 3.9533560838544895738i, \\
&\quad -0.50000000000000000000 + 0.93326077505201835299i] \\
z_3 &= [1.3090169943749474241 + 1.8211345794185750614i, \\
&\quad 0.19098300562505257590 + 1.1255230681684241054i] \\
z_4 &= [-0.50000000000000000000 + 1.3177853612848298579i, \\
&\quad -0.50000000000000000000 + 0.31108692501733945100i] \\
z_5 &= [1.8090169943749474241 + 2.2936531052298339139i, \\
&\quad 0.69098300562505257590 + 0.73117027997866946194i] \\
z_6 &= [-0.76699731667763988040 + 0.97247609202724360106i, \\
&\quad -0.94352899911183380381 + 0.99840423980404286576i] \\
z_7 &= [1.8090169943749474241 + 0.76455103507661130463i,
\end{aligned}$$

$$0.69098300562505257590 + 0.24372342665955648731i]$$

$$z_8 = [-1.6969011955335404324 + 0.71716715182997753142i,$$

$$-1.7787085605640205432 + 0.62738582842164290444i].$$

Approximations to the Gundlach invariants (truncated here for space reasons):

$$J_2(z_1) = 3\,741\,094\,620\,714\,837\,179\,200,$$

$$J_4(z_1) = -60\,818\,023\,693.106665287,$$

$$J_2(z_2) = 3\,840\,284\,490.5108996511,$$

$$J_4(z_2) = -53\,614.371981364370580,$$

$$J_2(z_3) = 10\,440\,592.275997173850,$$

$$J_4(z_3) = -2441.5717406031621394,$$

$$J_2(z_4) = -64.619455463275423537,$$

$$J_4(z_4) = 4.1454380620345353330,$$

$$J_2(z_5) = 2\,847\,784.6311053302354,$$

$$J_4(z_5) = 1460.2034387263077259,$$

$$J_2(z_6) = -4\,489\,730.4902199749666,$$

$$J_4(z_6) = -7085.6743379368902792,$$

$$J_2(z_7) = 550\,783.66717596136111,$$

$$J_4(z_7) = 770.75072469388249267,$$

$$J_2(z_8) = 18\,868\,649.413927712699,$$

$$J_4(z_8) = -14\,138.890758245058324.$$

The guess $N = 3^2 \cdot 11^4 \cdot 29^2 \cdot 61^2 \cdot 211^2 \cdot 241^2 \cdot 271^2$ for the denominator was obtained from the denominator bound for θ_{10} from the Brunier–Yang formula.

Polynomials $P_2(X) = N \prod_{i=1}^8 (X - J_2(z_i))$, $P_4(X) = N \prod_{i=1}^8 (X - J_4(z_i))$:

$$P_2 = 8\,700\,896\,126\,036\,551\,483\,736\,041X^8$$

$$- 32\,550\,875\,692\,547\,568\,160\,555\,206\,013\,385\,025\,122\,918\,400\,000X^7$$

$$+ 125\,923\,144\,169\,110\,910\,076\,831\,696\,022\,908\,759\,633\,958\,010\,880\,000\,000\,000X^6$$

$$- 3\,532\,308\,132\,779\,706\,667\,907\,638\,602\,077\,212\,120\,324\,453\,171\,200\,000\,000\,000\,000\,000X^5$$

$$+ 18\,896\,258\,614\,901\,229\,917\,530\,949\,381\,166\,658\,369\,177\,393\,928\,601\,600\,000\,000\,000\,000\,000\,000X^4$$

$$+ 78\,004\,698\,176\,565\,486\,371\,972\,347\,519\,396\,339\,488\,310\,620\,585\,984\,000\,000\,000\,000\,000\,000\,000\,000X^3$$

$$- 362\,973\,284\,011\,776\,064\,323\,611\,004\,432\,898\,872\,351\,089\,794\,511\,536\,128\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000X^2$$

Coefficients of P_2 :

Coefficients of P_4 :

$$\begin{aligned} c_{4,0} &= 2^{64} \cdot 3^8 \cdot 5^{26} \cdot 29^3 \cdot 89 \cdot 211 \cdot 1559 \cdot 251 \, 431 \\ c_{4,1} &= 2^{60} \cdot 3^7 \cdot 5^{23} \cdot 283 \cdot 923 \, 284 \, 368 \, 270 \, 711 \, 347 \\ c_{4,2} &= 2^{48} \cdot 3^6 \cdot 5^{19} \cdot 7 \cdot 1 \, 056 \, 061 \cdot 362 \, 022 \, 885 \, 111 \, 720 \, 449 \\ c_{4,3} &= 2^{44} \cdot 3^5 \cdot 5^{16} \cdot 19 \cdot 23^2 \cdot 73 \cdot 152 \, 531 \cdot 29 \, 253 \, 882 \, 917 \, 683 \\ c_{4,4} &= 2^{33} \cdot 3^4 \cdot 5^{12} \cdot 7 \cdot 43 \cdot 127 \cdot 12 \, 907 \cdot 482 \, 413 \cdot 69 \, 446 \, 456 \, 336 \, 729 \\ c_{4,5} &= 2^{25} \cdot 3^3 \cdot 5^9 \cdot 11 \cdot 17 \cdot 53 \cdot 73 \cdot 193 \cdot 797 \cdot 1871 \cdot 1 \, 794 \, 212 \, 865 \, 865 \, 807 \\ c_{4,6} &= 2^{16} \cdot 3^2 \cdot 5^6 \cdot 11^2 \cdot 53 \cdot 671 \, 918 \, 858 \, 429 \, 137 \, 008 \, 360 \, 873 \, 343 \\ c_{4,7} &= 2^9 \cdot 3 \cdot 5^3 \cdot 11^3 \cdot 49 \, 253 \cdot 26 \, 291 \, 379 \, 817 \cdot 1 \, 599 \, 084 \, 712 \, 499 \\ c_{4,8} &= 11^4 \cdot 29^2 \cdot 61^2 \cdot 211^2 \cdot 241^2 \cdot 271^2 \end{aligned}$$

Appendix A. Precision of computation

This section addresses the question of how to compute Hilbert theta constants accurately to a certain precision. In order to determine the number of terms needed to compute theta functions to a certain precision, we roughly follow the method detailed in Weng [We, Section 4] for computing Siegel theta functions precisely.

Throughout this section, we fix a CM point $z = (z_1, z_2) \in \mathbb{H}^2$ that lies in the fundamental domain. In particular, for $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$ we have the condition

$$y_1 \leq y_2 < \epsilon^4 y_1. \quad (\text{A.1})$$

We fix notation as follows. For $n = (n_1, n_2) \in \mathbb{Z}^2$ and $(a, b) = \phi_\epsilon^{-1}(m_1, m_2, m_3, m_4)$, let $E_0 = \frac{1}{2}(n_1 m_3 + n_2 m_4 + \frac{1}{2}(m_1 m_3 + m_2 m_4))$, $E_1 = ((n_1 + m_1/2)^2 + (n_2 + m_2/2)^2)$, and $E_2 = (2(n_1 + m_1/2)(n_2 + m_2/2) + (n_2 + m_2/2)^2)$. Then we can write

$$\theta_{a,b}(z) = \sum_{n \in \mathbb{Z}^2} e(E_0 + E_1 \rho_1 + E_2 \rho_2),$$

where $\rho_1 = (\epsilon z_1 - \sigma(\epsilon) z_2)/\sqrt{5}$ and $\rho_2 = (z_2 - z_1)/\sqrt{5}$. The absolute value of a term $e(E_0 + E_1 \rho_1 + E_2 \rho_2)$ only depends on the imaginary part of $E_0 + E_1 \rho_1 + E_2 \rho_2$ which is equal to the imaginary part of $E_1 \rho_1 + E_2 \rho_2$. We have

$$\text{Im}(E_1 \rho_1 + E_2 \rho_2) = E_1 \cdot \left(\frac{\epsilon}{\sqrt{5}} y_1 - \frac{\sigma(\epsilon)}{\sqrt{5}} y_2 \right) + E_2 \cdot \left(\frac{y_2 - y_1}{\sqrt{5}} \right).$$

Setting $w_1 = \frac{\epsilon}{\sqrt{5}} y_1 - \frac{\sigma(\epsilon)}{\sqrt{5}} y_2$ and $w_2 = \frac{y_2 - y_1}{\sqrt{5}}$, writing out E_1 and E_2 and setting $u_1 = n_1 + m_1/2$, $u_2 = n_2 + m_2/2$, we obtain

$$\text{Im}(E_1 \rho_1 + E_2 \rho_2) = w_1 u_1^2 + (w_1 + w_2) u_2^2 + 2w_2 u_1 u_2.$$

Lemma A.1. *Let w_1, w_2 be as above. Then from (A.1) it follows*

$$0 \leq w_2 < w_1 < (1 + \epsilon) y_1.$$

In particular, for $w = w_2/w_1$, it holds $0 \leq w < 1$.

Proof. The condition on y_1 and y_2 in (A.1) implies $0 \leq w_2 \leq \frac{3+\sqrt{5}}{2} y_1 = (1 + \epsilon) y_1$ and $0 < y_1 \leq w_1 < (1 + \epsilon) y_1$. The lemma follows with $\epsilon > 1$, $\sigma(\epsilon) < 0$, $y_1 > 0$, $y_2 > 0$ from a direct comparison of w_1 and w_2 . $\square$

We rewrite the imaginary part above as

$$\text{Im}(E_1 \rho_1 + E_2 \rho_2) = w_1 (u_1^2 + (1 + w) u_2^2 + 2w u_1 u_2).$$

We are interested in determining the set

$$M_C(z) = \{n = (n_1, n_2) \in \mathbb{Z}^2 \mid \operatorname{Im}(E_1\rho_1 + E_2\rho_2) \leq C\}$$

for a given positive constant C , i.e. we need to find solutions $(u_1, u_2) = (n_1 + m_1/2, n_2 + m_2/2)$, $(n_1, n_2) \in \mathbb{Z}^2$ to the inequality $u_1^2 + (1+w)u_2^2 + 2wu_1u_2 \leq \frac{C}{w_1}$ or equivalently

$$(u_1 + wu_2)^2 + (1+w-w^2)u_2^2 \leq \frac{C}{w_1}.$$

From [Lemma A.1](#), we see that $(1+w-w^2) > 0$ and that all solutions to the inequality lie within the ellipse given by the equation

$$\frac{w_1}{C}(u_1 + wu_2)^2 + \frac{w_1(1+w-w^2)}{C}u_2^2 = 1. \quad (\text{A.2})$$

In order to have any solutions at all, we need $C \geq w_1(1+w-w^2)u_2^2$ and thus

$$|u_2| \leq \sqrt{\frac{C}{w_1(1+w-w^2)}}.$$

For any u_2 in that range, we can now solve for u_1 and obtain the bounds

$$-wu_2 - \sqrt{C/w_1 - (1+w-w^2)u_2^2} \leq u_1 \leq -wu_2 + \sqrt{C/w_1 - (1+w-w^2)u_2^2}.$$

This leads to the following lemma.

Lemma A.2. *The set $M_C(z)$ is the set of all $n = (n_1, n_2) \in \mathbb{Z}^2$ that fulfill the following two conditions:*

$$-\frac{m_2}{2} - \sqrt{\frac{C}{w_1(1+w-w^2)}} \leq n_2 \leq -\frac{m_2}{2} + \sqrt{\frac{C}{w_1(1+w-w^2)}} \quad (\text{A.3})$$

$$\begin{aligned} -\frac{m_1}{2} - w(n_2 + \frac{m_2}{2}) - \sqrt{\frac{C}{w_1} - (1+w-w^2)(n_2 + \frac{m_2}{2})^2} &\leq n_1 \\ &\leq -\frac{m_1}{2} - w(n_2 + \frac{m_2}{2}) + \sqrt{\frac{C}{w_1} - (1+w-w^2)(n_2 + \frac{m_2}{2})^2}. \end{aligned} \quad (\text{A.4})$$

We can now find all elements in $M_C(z)$ by running through all possibilities for n_2 according to the first range, and then depending on the value of n_2 find all corresponding values for n_1 .

For a given precision of s bits, we now wish to determine a constant $C > 0$ such that

$$\left| \sum_{n \in \mathbb{Z}^2 \setminus M_C(z)} e(E_0 + E_1\rho_1 + E_2\rho_2) \right| < 2^{-s}. \quad (\text{A.5})$$

This assures that an approximation to the theta function computed by summing over all elements in the set $M_C(z)$ for such a constant C will be accurate to a precision of s bits.

We have

$$\begin{aligned} \left| \sum_{n \in \mathbb{Z}^2 \setminus M_C(z)} e(E_0 + E_1 \rho_1 + E_2 \rho_2) \right| &\leq \sum_{n \in \mathbb{Z}^2 \setminus M_C(z)} |e(E_0 + E_1 \rho_1 + E_2 \rho_2)| \\ &= \sum_{n \in \mathbb{Z}^2 \setminus M_C(z)} \exp(-2\pi \operatorname{Im}(E_1 \rho_1 + E_2 \rho_2)) \\ &\leq \sum_{k=\lfloor C \rfloor}^{\infty} \mu(k) \exp(-2\pi k), \end{aligned}$$

where

$$\mu(k) = \#\{n = (n_1, n_2) \in \mathbb{Z}^2 \mid k < \operatorname{Im}(E_1 \rho_1 + E_2 \rho_2) \leq k+1\} = |M_{k+1}(z) \setminus M_k(z)|.$$

We estimate $|M_k(z)|$ by the area of the ellipse given by (A.2),

$$|M_k(z)| \approx \pi k / (w_1 \sqrt{1+w-w^2}).$$

Since $M_k(z) \subseteq M_{k+1}(z)$, we can approximate $\mu(k)$ by $|M_{k+1}(z)| - |M_k(z)|$,

$$\mu(k) \approx \pi / (w_1 \sqrt{1+w-w^2}).$$

Therefore, we assume

$$\sum_{k=\lfloor C \rfloor}^{\infty} \mu(k) \exp(-2\pi k) \approx \frac{\pi}{w_1 \sqrt{1+w-w^2}} \sum_{k=\lfloor C \rfloor}^{\infty} \exp(-2\pi k).$$

As in [We], we use the fact that the sum on the right hand side is bounded by the integral

$$\int_{C-1}^{\infty} \exp(-2\pi x) dx = \frac{1}{2\pi} \exp(-2\pi(C-1)).$$

As an upper bound for the absolute value in (A.5) we thus take

$$B = \frac{1}{2w_1 \sqrt{1+w-w^2}} \exp(-2\pi(C-1)).$$

If we ensure $B < 2^{-s}$, then (A.5) is satisfied. We have $B < 2^{-s}$ if and only if

$$C > 1 + \frac{s-1 - \log_2(w_1 \sqrt{1+w-w^2})}{2\pi \log_2(e)}.$$

Using the bounds on w and w_1 , we obtain $B < 2^{-s}$ if

$$C > 1 + \frac{s - 3/2 - \log_2(w_1)}{2\pi \log_2(e)} = 1 - \frac{3}{4\pi \log_2(e)} + \frac{s - \log_2(w_1)}{2\pi \log_2(e)}.$$

The larger w_1 is, the smaller we may choose the bound C and the smaller is the number of terms that are needed to achieve precision s bits.

Appendix B. Supplementary material

Supplementary material related to this article can be found online at <http://dx.doi.org/10.1016/j.jnt.2015.02.020>.

References

- [BL] R. Bröker, K. Lauter, Evaluating Igusa functions, *Math. Comp.* 83 (2014) 2977–2999.
- [BY] B.H. Bruinier, T.H. Yang, CM-values of Hilbert modular functions, *Invent. Math.* 163 (2006) 229–288.
- [CDLY] C. Costello, A. Deines-Schartz, K. Lauter, T.H. Yang, Constructing abelian surfaces for cryptography via Rosenhain invariants, *LMS J. Comput. Math.* 17 (Special issue A) (2014) 157–180.
- [ET] A. Enge, E. Thomé, Computing class polynomials for abelian surfaces, *Exp. Math.* 23 (2014) 129–145.
- [Gu] K.-B. Gundlach, Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $\mathbb{Q}(\sqrt{5})$, *Math. Ann.* 152 (1963) 226–256.
- [Ig1] J.-I. Igusa, Arithmetic variety of moduli for genus two, *Ann. Math.* 72 (1960) 612–649.
- [Ig2] J.-I. Igusa, Modular forms and projective invariants, *Amer. J. Math.* 89 (1967) 817–855.
- [LV] K. Lauter, B. Viray, An arithmetic intersection formula for denominators of Igusa class polynomials, *Amer. J. Math.* 137 (2) (2015) 497–533.
- [LY] K. Lauter, T.H. Yang, Computing genus 2 curves from invariants on the Hilbert moduli space, in: *Elliptic Curve Cryptography*, *J. Number Theory* 131 (5) (2011).
- [Sh] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton Univ. Press, 1998.
- [St] M. Streng, Complex multiplication of abelian surfaces, PhD thesis, Universiteit Leiden, 2010.
- [vW] P. van Wamelen, Examples of genus two CM curves defined over the rationals, *Math. Comp.* 68 (225) (1999) 307–320.
- [We] A. Weng, Constructing hyperelliptic curves of genus 2 suitable for cryptography, *Math. Comp.* 72 (241) (2003) 435–458.
- [Ya1] T.H. Yang, An arithmetic intersection formula on Hilbert modular surfaces, *Amer. J. Math.* 132 (2010) 1275–1309.
- [Ya2] T.H. Yang, Arithmetic intersection on a Hilbert modular surface and Faltings’ height, *Asian J. Math.* 17 (2) (2013) 335–382.
- [Ya3] T.H. Yang, Rational structure of $X(N)$ over $\mathbb{Q}$ and explicit Galois action on CM points, 2014, preprint, 13 pp.